Cybersecurity Policy for Public and Private Sector Entities

Paul F. Ayres
Christopher M. Bowen
Blake Carriere
Richard P. Clifton
Jeffery S. Hasley
Greg L. Kohn
Caleb L. Lacey
David E. Lilly
Marvin S. Massey III
Thomas G. Pledger
Thomas E. Smith
Charles W. Teel
Steven P. Van Sciver

Academic Advisor:
Danny W. Davis, LTC, US Army (ret); Ph.D.

PSAA 675 Capstone, Fall 2019

In partial fulfillment of the requirements for the Executive Master of Public Service and Administration with a concentration in Homeland Security.

ACKNOWLEDGMENTS

The authors wish to thank Dr. Danny Davis and the staff and faculty of the Bush School of Government and Public Service for their advice and guidance on this paper and on our path to graduation. The authors also wish to thank our families and friends for helping us along this journey. It wasn't always easy, but the end for this chapter of our lives closes at the end of this paper. Lastly, this paper could not have been done without the teamwork of the 13 motley fools who began this paper in June 2019. Thanks to each for the support and assistance given as we worked and struggled to come to a good product.

TABLE OF CONTENTS

NOMENCLATURE

1FA	single-factor authentication
2FA	two-factor authentication
APT	advanced persistent threat
BYOD	bring your own device
CEA	Cybersecurity Enhancement Act
CFR	Code of Federal Regulations
CIS	Center for Internet Security
CSIP	Cybersecurity Strategy and Implementation Plan
CSIS	Center for Strategic and International Studies
DCCC	Democratic Congressional Campaign Committee
DDoS	direct denial of service
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DoD	Department of Defense
DoJ	Department of Justice
EO	executive order
FBI	Federal Bureau of Investigation
Fed. Reg.	Federal Register
FIOP	Federal Interagency Operational Plan
GAO	Government Accountability Office
GPU	graphics processing unit
GRU	Main Intelligence Directorate (Russia)
HSM	hardware security module
IEC	International Electrotechnical Commission
IOS	International Organization for Standardization
IoT	Internet of Things

ISA	International Society for Automation
ISACA	Information Systems Audit and Control Association
ISC	International Strategy for Cyberspace
IT	information technology
ITSSP	Information Technology Sector-Specific Plan
MFA	multifactor authentication
MPS	Ministry of Public Security
MSS	Ministry of State Security
NCCIC	National Cybersecurity and Communications Integration Center
NCS	National Cyber Strategy
NGO	nongovernmental organization
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NPG	National Preparedness Goal
NSS	National Security Strategy
OMB	Office of Management and Budget
PLA	People's Liberation Army
PPD	presidential policy directive
PRC	People's Republic of China
Pub. L.	public law
SEC	Securities and Exchange Commission
TAC	Texas Association of Counties
US	United States
USB	Universal Serial Bus
USC	United States Code

INTRODUCTION

Advancements in technology have numerous proven benefits to society, however these advancements have not come without challenges. Cybersecurity is no longer solely an issue for governments and large corporations, it is a problem which must be addressed by organizations at all levels. The aim of this project is to develop a policy which can be used by organizations to ensure their information technology systems are secure from internal and external threats. The policy is designed to be reviewed by the executive level leadership, adapted to the organization's specific threat environment, and applied throughout the organization at all levels.

To provide the necessary context for a cybersecurity policy, the group conducted a literature review in an effort to provide background information in four areas: 1) current approaches to cybersecurity within the United States, 2) descriptions of common threat vectors, 3) methods of vulnerability reduction, and 4) minimizing the impact of a cyberattack.

First, the group presented current cybersecurity policy, jurisdictional boundaries/limitations, and responsibilities of the U.S. federal government. The federal government recognizes the important role the cyber domain plays in societal and economic security. In response to the prevalence of cyber threats to the United States' national security, the federal government has published numerous documents to frame the issue in an attempt to prevent exploitation

through increased awareness and preparedness. Due to the majority of cyber infrastructure residing within the public sector, the government understands the importance of public-private cooperation in the cyber domain. Many of the nation's strategies and policies encourage public and private entities to form partnerships across the information spectrum to defend against cyberattacks.

Second, the group focused its efforts on the identification of three different threat vectors: non-state actors, state actors, and insiders. While each actor has different motivations, they may employ similar means to obtain access to cyber networks. Organizations can take steps to promote domain awareness and counteract malicious attacks. The fast pace of cybersecurity makes it a challenge for organizations to stay current on the variety of threats that exist, but dedicating adequate resources and implementing best practices can significantly bolster an organization's cybersecurity program.

Third, the group determined that at a minimum, organizations should incorporate the physical, technical, and social aspects of cyber threat detection and prevention in their policies. Organizations are coming under increased attack from hostile cyber actors both outside and inside their networks and the need for cyber security cannot be overemphasized. There are many network vulnerabilities that need to be considered when developing a cyber security policy or assessing an existing one.

Fourth, the group recognized that it is not a matter of if, but when an organization will be attacked. To minimize the damage caused by a cyberattack, an organization needs to be prepared to detect, respond, and then recover from the attack. The group provided a series of steps that an organization can take in order to minimize the effects of a cyberattack.

Utilizing the information researched during the literature review, the group identified a gap in our nation's resilience against cyberattacks: the small private-sector organization. The group then developed a cybersecurity policy that would address the requirements of small private-sector organizations. Additionally, the policy helps to identify, define, and determine cyber security situations faced by small organizations and provides some best practices with the use of personal electronic devices at this type of organization.

This cybersecurity policy, using the context of the literature review described above, will facilitate the communication of cybersecurity activities and outcomes across the organization’s enterprise – from the implementation/operations level to the executive level. It provides not only the scope and limitations of the policy, but also provides specific roles and responsibilities for key leaders within an organization, the frequency of policy review, the applicability across the members of the organization, as well as recommendations for training and educating the members of the organization.

Additionally, the policy provides definitive guidance for visitors, vendors, third parties, and interns in the use of information technology systems of the organization and the parameters for exemptions to policy. Finally, the policy provides guidance on implementation, the use of common cyber terminology, and specific guidance on technologies and techniques for cybersecurity.

This document is intended to serve a diverse audience, including senior level management, administrative and support personnel, auditors, end-users, information security professionals, information technology management, and field personnel.

PROPOSED CYBERSECURITY POLICY

Purpose

1. This policy provides information on how to secure networked technologies critical to achieving the mission and vision of the organization. A breach in cybersecurity has the potential to be detrimental to the organization and cause significant setbacks in strategic goals. This policy provides the most current information on how to prevent the damages associated with a cyberattack while maintaining confidentiality, integrity, and availability. While there is no such thing as 100% prevention of the effects of a cyberattack, this policy focuses on minimizing the potential for catastrophic damage to the organization.

Scope

1. This policy applies to all employees (full-time and part-time), interns, visitors, and external stakeholders who access the organization's network.

2. This policy provides definitive guidance for users with both local and remote network connections.

3. This policy provides definitive guidance for users of both organization-owned and personally owned devices.

4. While the organization may not directly communicate all portions of this policy to external stakeholders (vendors and contractors), the decision to accept their services should include their ability to integrate with the organization's applicable cybersecurity policies.

Limitations

1. This policy is only as effective as the capability, skill sets, education, and personality traits of employees. Each member of the organization shall strive for the full implementation of this policy.

2. This policy will be reviewed annually for necessary revisions and updates, to include technological updates, vulnerability assessments, and trends in recent cyberattacks.

3. This policy is not all-inclusive or static. Additional policies, sections, appendices, or procedures will be added as necessary. This may include 1) acceptable use of networked technologies, 2) methods and levels of access control, 3) changes/updates in technology and development of new technologies, 4) securing sensitive/confidential information, 5) provisions for secure remote access and email communications, 6) responding to and recovering from a cybersecurity incident, and 7) planning for the continuity of business operations.

4. To ensure that violations of this policy are enforced, this cybersecurity policy will be integrated with the organization's discipline policy. Violations of the organization's cybersecurity policy by visitors and external stakeholders will be adjudicated on a case by case basis, keeping in line with the organization's discipline policy.

Roles and Responsibilities

5. General Responsibilities

    a. Any system user granted remote access privileges to the organization's network are responsible for ensuring remote access connections are secure.

    b. All system users will use secure passwords with two-factor authentication.

c. System users are prohibited from using unsecure networks to access the organization's network.

d. System users must ensure any personally owned devices used to access the organization's network have the latest critical updates and antivirus software installed.

e. All members of the organization are required to use due diligence to ensure that only authorized users are granted access to organization systems and networks. Members of the organization are never to give their login credentials to anyone, including other members of the organization.

6. Human Resources

a. The receipt and acknowledgement of this policy will be documented during the on-boarding process of new employees and each time the employee receives continuing education on this policy.

b. HR is responsible for coordinating training events to ensure all employees receive adequate training on cybersecurity related policies.

c. Documentation of policy related training received by employees will be retained by HR for a period consistent with applicable state and federal regulations.

7. Chief Information Officer

a. Ensure that all organization computers, servers and remote access devices are up-to-date and fully compatible with one another and the system.

b. Create and implement information integration plan and distribute plan to all responsible parties and stakeholders.

c. Establish process for testing security and integrity of organization cybersystems and oversee testing and validation of systems.

8. Information Technology Director

a. Develop cybersecurity guidelines for all organization members that establish standards for privacy, security and protection of organization data and oversee implementation of guidelines.

b. Establish internal controls for cybersecurity and process for validating these controls and oversee implementation of controls.

c. Manage the development and implementation of the organization's cybersecurity policy and standards.

d. Establish a process to ensure all system users comply with the organization's cybersecurity policy and oversee implementation of process.

e. Develop actionable plan for ensuring standardization of all organization hardware and software and oversee implementation of plan.

9. Information Technology Project Manager

a. Implement organization's cybersecurity protocols for data protection, system usage and cloud access.

b. Oversee development and implementation of all organization information technology projects.

c. Secure information technology projects and grant access only to personnel with the necessary authority and clearance level.

d. Will engineer visitor access points in a way that prevents unauthorized use and has the ability to quarantine/isolate the visitor network.

10. Information Technology Technician

a. Maintain and repair organization's software and data processing hardware systems.

b. Build, install, repair and troubleshoot organization networks.

c. Install and operate virus detection software on organization data processing equipment.

11. Interns

a. Sign and comply with organization network connection and non-disclosure agreements.

b. Limit usage of organizational computers and servers to only what is authorized by this policy.

c. Protect user IDs and system access to ensure that no unauthorized individuals gain access to the organization's servers.

12. Visitors, Vendors and Other Third Parties

a. Visitors, vendors, and third parties not directly involved in providing technology services or protecting this organization's technology assets will not receive a copy of this policy.

b. Visitors, vendors, and third parties will access only portions of the network specifically authorized by the Information Technology Director.

c. Visitors, vendors, and third parties will only access the organization's network using devices authorized and controlled by the Information Technology Director. Independent contractors are not allowed to bring their own devices to connect to the organization's network. All visitors and vendors need to seek approval for their devices before connecting to the network.

d. Employees may only assist visitors with connecting to networks specifically designed for guests/visitors. Employees will not provide additional information on how to access restricted portions of the network.

e. Visitors will only use access points that have been designated by the Information Technology Department as visitor access points.

Implementation

1. Members of this organization will follow these policies and take precautions to prevent cyberattacks. Implementing this policy means that each member of the organization is a responsible steward of the computer network and accountable for their activities while using the system. Without such individual action, cybersecurity policies are meaningless and lack influence on the overall security of systems within the organization.

2. This policy will be provided to visitors, vendors, and third party contractors as necessary.

3. For individuals with the need to access this policy, it should be easy to access, easy to understand and provide a means for employees, organization members and consultants to provide feedback.

4. Regular and active involvement of senior executives and leaders is necessary and required to ensure success. Senior leaders must ensure technical and operational line departments and their personnel are implementing the policy to ensure the security objectives are met.

5. When conducting an annual financial review of the implementation of this policy, the following steps will be considered:

    1. identify the organization's information and data assets;
    2. identify the financial cost of if the assets are lost, damaged, or compromised;
    3. identify the cost of implementing the cybersecurity policy, to include associated costs resulting from modification of existing procedures where applicable;
    4. estimate the risk to the organization's information and data assets;
    5. estimate the benefits from implementation of the policy in terms of avoiding the losses projected in step 2 in conjunction with the risk estimate in step 4; and
    6. compare the expected benefits in step 5 with the expected costs in step 3.

6. During the annual financial review of the implementation of the cybersecurity policy, executives will also consider the intangible cost of a successful cyberattack to the reputation and standing of the organization.

7. The IT department will conduct an impact assessment for new technology (hardware and software) considered for cybersecurity used by this organization. Items that must be highlighted within this analysis will include the impact on changes to organizational performance and an assessment of the technology's security related qualities.

8. All departments have a role in protecting the organization's data and information. Those sections within the organization that handle financial matters (budgeting, contracting, and purchasing) need to be especially attentive to the implementation of this policy to protect not only this organization, but also the relationships with vendors and independent contractors with whom this organization interacts.

Common Terminology

1. Terminology used in cybersecurity changes on a regular basis with new and emerging threats. Therefore, routine training that is provided to employees and interns will include a review of terminology that is common to the current threat environment.

2. Understanding the common terminology used in cybersecurity will reduce misunderstandings when discussing cyber and IT security issues. This shared understanding allows the security directives to be more effective across all organizational levels and sections.

3. To support cybersecurity training, the organization's employees at all levels need to understand the meaning and importance of common cybersecurity terminology. This shared understanding of common terminology is also important in areas such as risk management. Because it is the responsibility of the chief financial officer or compliance officers, financial security purchasing such as insurance policies against cyberattacks requires that these leaders have a clear understanding of common cybersecurity terms.

4. Several websites track and maintain updated lists of current cybersecurity terminology. A definitive glossary of cybersecurity terms usable for the purposes of this policy can be found in the National Institute of Standards and Technology - Computer Security Resource Center (NIST CSRC) at https://csrc.nist.gov.

Frequency of Policy Review

1. This organization's cybersecurity policy shall be reviewed on an annual basis. However, additional reviews (quarterly, monthly) shall be initiated based on the current threat environment and directly related to the potential of an actual cyberattack directed against this organization.

2. Updates should allow for protecting not only the organization's data, but also the various connected devices other than workstations, smartphones, and tablets, to include all other connected devices commonly classified as part of the Internet of Things.

3. This cybersecurity policy must be reviewed to address new threats, new technical considerations, and account for new business practices. Organizational leaders must commit time and financial resources to the effort.

4. Cybersecurity policy reviews should always consider personal devices within the workplace:
    a. identification of areas where personal devices are not allowed;
    b. determination of the types and models of personal devices which are allowed to be used within the organization's workspace.

5. Cybersecurity policy reviews should determine if current cybersecurity training meets the needs of both the workforce and the organization.

6. Just as cybersecurity policy evolves, the threats are also evolving. Reviews of the organization's cybersecurity policy are not complete without systematic testing of the safeguards in place. The policy's procedures and directives should be validated to ensure objectives are met and for identifying areas where changing the policy is required.

Applicability

1. The organization requires all users to exercise care with the operation and use of its information systems. The organization has to have clear guidelines to what cybersecurity policies the organization wants to implement and avoid duplicating the same work, which leads to time wasted and inefficiency. The structure of this publication facilitates communication of cybersecurity activities and outcomes across the organization's enterprise – from the implementation/operations level to the executive level. This document is intended to serve a diverse audience, including senior level management, administrative and support personnel, auditors, end-users, information security professionals, information technology management, and field personnel. In addition, this policy applies to all networks managed by the organization

2. Audience

    a. Staff who may benefit from a review of the security controls in this document include:

        i. Individuals that have access to systems, including end users.

        ii. Individuals with information system, security, and/or risk management and oversight responsibilities (e.g., chief information officers, senior information security officers, information system managers, information security managers);

        iii. Individuals with information system development responsibilities (e.g., program managers, system designers and developers, information security engineers, systems integrators)

        iv. Individuals with information security implementation and operational responsibilities (e.g., mission/business owners, information system owners, common control providers, information owners/stewards, system administrators, information system security officers); and

v. Individuals with information security assessment and monitoring responsibilities (e.g., auditors, system evaluators, assessors, independent verifiers/validators, analysts, information system owners).

Authorized users of information systems

1. With the exception of information published for public consumption, all users of organization's information systems must be formally authorized by appointment as a member of staff, an intern, or by another process specifically authorized by the Chief Information Officer (CIO). This cybersecurity policy applies to all senior management, employees, stockholders, consultants, and service providers who use the organization's assets. Authorized users will be in possession of a unique user identity. Any password associated with a user identity must not be disclosed to any other person.

2. The organization's cybersecurity policy applies to all individuals accessing, using, holding, or managing the organization's information resources. This includes contractors performing custodial care on network or IT systems, along with other third-parties performing services for the organization.

3. At a minimum the officers, directors, and senior management should have a clear understanding of the risks posed by the technology used in the operation of the organization. Clear guidance from the leadership on risk management practices is necessary to guide the direction of the organization. The leadership must provide active oversight in monitoring and cybersecurity mitigation activities.

Confidential Information

1. Authorized users will pay due care and attention to protect the organization's information in their personal possession. Confidential,

personal or private information must not be copied or transported without consideration of:

2. permission of the information owner

3. the risks associated with loss or falling into the wrong hands

4. how the information will be secured during transport and at its destination.

5. All of the organization's information will be protected from unauthorized access to help maintain information's confidentiality and integrity. The information owner will classify and secure information within their jurisdiction based on the data classification guidelines in the "Information Management and Security Procedural Document" according to the information's value, sensitivity to disclosure, consequences of loss or compromise and ease of recovery.

6. Information will be readily available for authorized use as needed by the user in the normal performance of their duties. Appropriate processes will be implemented to ensure the reasonable and timely recovery of all of the organization's information, applications and systems, regardless of computing platform, should that information become corrupted, destroyed, or unavailable for a defined period.

7. Willful or negligent disregard of this policy may be investigated and dealt with under the organization's Disciplinary Procedure.

Exemptions

1. Cybersecurity is paramount in this organization. We go to great lengths and spend a significant amount of money and resources to ensure the security of our information systems. As such, any and all exemptions to our established policies will require clear justification and several levels of review prior to final approval or disapproval. The process for obtaining an exemption applies to all employees of this organization (full-time or

temporary), as well as contractors, interns, and guests who require access to organizational networks.

2. Exemptions to organizational IT cybersecurity policies shall be limited to requests submitted and endorsed by your division chief, or their deputy, and forwarded to the information technology department for a thorough risk assessment. Once the risk assessment has been completed, the request, justification, and the results of the risk assessment will be forwarded to the Chief Information Officer for final disposal, largely due to the risk the organization is taking for ignoring its own policy.

3. The Chief Information Officer's decision will be final and is not subject to review or dispute. Approved exemptions will be documented, in writing, and implemented by the IT department. Denied exemptions will be returned to the requester, also in writing. If further consideration is required, and an exemption still necessary, a new request may be made with additional justification and the process will remain the same. Information technology system administrators must also submit requests for exemptions through channels, even if the exemption will improve their ability to accomplish their job. No employee can authorize their own exemptions.

4. The following are possible reasons for exemptions:
    a. There is an organizational need to be exempted from this policy:
    b. Compliance with the current policy is considered too costly and inefficient
    c. The existing policy adversely impacts other requirements making compliance detrimental to organizational goals
    d. Administrators conducting their legitimate job responsibilities
        i. Accessing restricted websites to determine whether continued employee access is a violation of the organizational policy
        ii. Assumes established organizational policy outlines the authority of the IT department to monitor equipment, systems, and network traffic at any time
    e. Variations in devices and platforms:
        i. Desktop computers that remain on the network may have reason for exemption if protected behind organizational firewalls

ii. Laptop and portable devices may be ineffective unless granted an exemption

5. Time critical emergency situations may arise that require immediate action making the exemption approval process inappropriate. Any member of the organization must thoroughly consider the potential consequences of their actions when responding in an emergency situation. As soon as feasible, after knowingly violating organizational cybersecurity policy, employees must report the deviation to their immediate supervisor and the information technology office. This is meant as a preventative measure, NOT punitive, to limit potential damage to organizational systems and networks. Knowingly failing to report a deviation will be handled differently and may result in dismissal from the organization.

6. Recommendations for policy changes in regards to exemptions should be elevated through the division chief, in coordination with the IT branch, and approved by senior executive management prior to implementation.

Training and Education

1. In order to maintain a cybersecurity culture throughout the organization, all personnel within the organization will be required to participate in cybersecurity awareness training. Current personnel will be required to participate in organization approved cybersecurity awareness training within one month of the adoption of this policy. New employees shall participate in organization approved cybersecurity awareness training within one month of starting with the organization.

2. Individuals requiring access to the organization’s network or technology who are not part of the organization must also undergo training prior to being given access. This includes, but is not limited to, guests of the organization and independent contractors.

3. Because cyberthreats continuously evolve over time, ongoing education of the organization's personnel is critical to maintain good cybersecurity practice within the organization. Supplementary training materials, such as

audiocasts, videos, screensavers, posters, factsheets, and monthly newsletters will be updated and made available throughout the year to personnel. Personnel will be expected to stay up to date on the information that is provided to them. Ongoing training should be done on an annual basis for all personnel while those with a specific job function that requires them to handle sensitive information should participate in training every 90 days.

4. The organization will conduct periodic penetration testing to assess training of personnel and their collective awareness of cybersecurity risk. This will be done in a way that disguises the penetration testing to appear as a normal part of an employee's daily tasks and does not disrupt the organization's daily operations. Personnel who respond inappropriately to the penetration testing shall be required to attend remediation training to reinforce awareness of the organization's cybersecurity practices.

5. Cybersecurity awareness training will cover a wide variety of areas that will be continuously updated to meet current threats in the cybersecurity arena. These areas shall include, but are not limited to:

    a. Usage of Removable Media
    b. Email and Social Media Hoaxes and Scams
    c. Social Engineering
    d. Malware Awareness (types of malware) and Malware Protection (tools used for malware protection)
    e. Data Management
    f. Physical Security and Access Controls
    g. Clean Desk Practices
    h. Cybersecurity Best Practices While Away from The Office

6. Training methodology may involve an interactive process that exposes personnel to current threats and trends within the cybersecurity arena. Additional training by cybersecurity professionals who are familiar with the organization's policies will be done on a routine basis. Training may also be augmented by online courses either developed internally or provided by a qualified third party.

Technologies and Techniques for Cybersecurity

The scope of this document is limited in order to keep it general and easily implementable as it is written. Topics for individual organizational evaluation and inclusion include the following technologies and techniques. These should be evaluated based on organizational processes and fiscal means of the organization.

1. Authentication of Users
    a. Through network policies, all users should be required to use passwords of eight characters in length at a minimum. Passwords should be required to use:
        i. lower case letters
        ii. upper case letters
        iii. numbers
        iv. special characters
    b. Passwords should be rotated at least quarterly.
    c. To supplement the use of passwords and reduce potential risk to unauthorized access of user accounts, Two Factor Authentication Methods (2FA) should be required on all user accounts. 2FA methods that are permitted are:
        i. Time-based One-Time Passwords (TOTP)
        ii. Hardware Tokens
        iii. SMS or Email Delivered One Time Security Codes
    d. Where key authentication is to be used
        i. Shared keys should be computed using a Diffie-Hellman key exchange with Elliptic-curve algorithms (ECDH).
        ii. Public/Private Key Exchanges should use RSA 2048bit at a minimum. Though RSA 4096bit is recommended.
2. Remote Access of Networks or Data
    a. Virtual Private Network (VPN) service should be hosted by the organization on their premises. All VPN connections should be encrypted using at least AES 256bit encryption to protect data in

transit. All users should be authenticated using the same requirements for authenticating users on the network.

b. Use of the organization's VPN should be considered the same as the onsite network for the organization.

3. Sensitive Data Storage
    a. To maintain sensitive data's confidentiality and integrity data should:
        i. Have appropriate read/write access applied using network and operating system access controls.
        ii. Be encrypted while at rest using AES 256bit encryption.
        iii. Be encrypted while in transit using AES 256bit encryption with a shared key that is computed using Diffie-Hellman key exchange with Elliptic-curve algorithms or through an encrypted message using RSA 2048bit encryption or better.
        iv. Be securely backed up both onsite and off site with a trusted third party contractor.
    b. The use of personal cloud storage accounts to store and transfer sensitive data owned by the organization is prohibited. Instead the organization will provide one of two options to personnel:
        i. A third party cloud storage service (such as Dropbox or Google Drive) with individual accounts for all authorized personnel with the same user authentication requirements used on the organization's network.
        ii. An on premises cloud storage (such as Nextcloud) with the same user authentication requirements used by the organization, which will store the data securely.
    c. Anonymous, unauthenticated, or public URL access to files stored in any cloud storage service is prohibited.
4. Use of Personal Devices
    a. While it is unreasonable to prohibit the use of personal devices such as laptops, desktops, smartphones, tablets, smartwatches, and other personal devices while on the premises of the organization, it is important to limit and control access of those devices to the organization's network and data.

b. No personal device will be permitted access to the organization's network without strict device provisioning policies and device registration through mobile device management (MDM) software.
c. For a device to be allowed to be registered it will have at a minimum these capabilities and system settings:
    i. Automatic screen locking after one minute or less of inactivity.
    ii. Ability to be locked with a PIN, password, biometric access, or security token.
    iii. Full storage encryption.
    iv. Ability to be remotely locked and wiped by both the owner of the device and the organization in the event the device is stolen or lost.
    v. An operating system that continues to receive security updates and patches from the operating system manufacturer while the device is registered.
d. The owner of the personal device must adhere to the following policies in order to maintain the security of their registered device:
    i. Only the owner may access the personal device, and not family, friends, or associates who are not part of the organization.
    ii. Any password or PIN used to unlock the device must adhere to the organization's password requirements.
    iii. The owner may not modify or remove the code of the operating system of the device or the device management software without prior approval from the organization's IT department.
    iv. The owner may only download software applications (apps) from the official store of the operating system of their device if and only if the software has gone through a testing process maintained by that store. No third party sources of software, or pirated software, will be permitted on their device.
    v. In the event that the device is lost, stolen, disabled, or otherwise made not accessible or usable to the owner, the owner will notify the IT department immediately so that

they may remotely wipe the device and revoke access for that device to the network.

vi. The device may only be synchronized with or backed-up to workstations that are owned by the organization or workstations that have up to date anti-malware software as defined by the organization.

EXECUTIVE SUMMARY

With high-profile cyberattacks targeting the government, for-profit, and nonprofit sectors, the topic of cybersecurity and how to mitigate the effects of these attacks has become a bigger concern for organizations of all types in recent years. When facing a variety of cyber threats in the world, from individual bad actors to organized crime to state actors, it is important to be aware of the existing relevant literature in the field of cybersecurity in order to develop an effective cybersecurity plan to protect any organization against attacks and to mitigate the damages caused by successful attacks.

This literature review seeks to inform the development of an effective cybersecurity policy with existing policy documents and industry best practices that are most relevant to cyberattacks and their effects on organizations by sorting the material using the framework developed by the United States (US) National Institute of Standards and Technology (NIST), which organizes the function and categories of cybersecurity activities into five key areas: identify, protect, detect, respond, and recover. For the purpose of this literature review, these areas have been consolidated into the following sections:

I) *Core Documents*, covering various relevant policy documents and recommendations from relevant government agencies and industry best practices

II) *Identify Threats*, outlining the various types of cyber threats an organization might face

III) *Protect and Detect*, detailing the various measures that can be taken to both protect an organization's information technology (IT) and detect either internal or external attacks on its network

IV) *Respond and Recover*, presenting ways to respond to a detected attack and to recover from damages caused by the attack

SECTION I: CORE DOCUMENTS

Summary

The US historically has been considered a land of great opportunity, with the concept of individual liberty guaranteed by the US Constitution (1789). Over time, the US has become known as a safe refuge for oppressed people and as a symbol of freedom due, in part, to the industrial and technological advancements that have vastly improved the quality of life for citizens.

Advancements in technology have numerous proven benefits to society, but these advancements have not come without challenges. In a matter of 50 years, IBM mainframe computer networks the size of a warehouse have been condensed into the smart phones that most of us carry in our pockets. In the same time frame, bad actors have found ways to exploit advanced technologies and cause great harm to others. Basic computing skills are the only requirement to disrupt operations or exploit computer-network vulnerabilities from anywhere in the world utilizing internet access. The US recognizes the importance of the cyber domain and its role in societal and economic security. In response, the US has published numerous documents to frame the issue and attempt to prevent exploitation through increased awareness and preparedness. National and international strategies broadly delineate the problem, while departmental documents identify

specific government agencies charged with preparing for and responding to cyber incidents directly impacting the country.

Recognizing that the cyber domain is an area of critical risk faced by the nation, US presidents over the last 25 years have issued numerous policy directives and executive orders (EOs) increasing expenditures for the acquisition of cybersecurity resources. Because the majority of cyber infrastructure resides within the public sector, the government understands the importance of public-private cooperation in the cyber domain. Without voluntary participation from the private sector, a completely secure cyber domain will remain elusive, and bad actors will continue to infiltrate information infrastructures. Many of the nation's strategies and policies encourage public and private entities to form partnerships across the information spectrum to defend against cyberattacks.

Introduction

Strategies are developed to provide guidance to political, economic, and military agencies to ensure maximum support of US governmental policies in peace or war. Three specific strategies have been developed by the administrations of President Obama and President Trump addressing the cyber domain as a risk and placing emphasis on senior leaders ensuring cybersecurity:

- International Strategy for Cyberspace (ISC): Prosperity, Security, and Openness in a Networked World (published May 2011)

- National Security Strategy (NSS) of the United States of America (published December 2017)
- National Cyber Strategy (NCS) of the United States of America (published September 2018)

These documents directly address the need to focus on critical infrastructure and network security to prevent devastating impact to the economy.

The US Department of Homeland Security (DHS), through the National Preparedness Goal (NPG), has developed policies for the protection of the cyber domain. This, together with the National Infrastructure Protection Plan (NIPP), the Information Technology Sector-Specific Plan (ITSSP), and the Protection Federal Interagency Operational Plan (FIOP), provides a framework for planning for and responding to cyber threats to mitigate the impact of a successful attack.

Several presidential policy directives (PPDs) and EOs have focused on cybersecurity in the last 20+ years. In the years from President Clinton to President Trump, an ever-increasing emphasis on cyber threats has been evident in the urgency of the language used in White House documents. The threat is real and evolves daily with adversaries who “have increased the frequency and sophistication of their malicious cyber activities” (from p. 1 of the NCS, published September 2018).

Literature Review

Strategies

National Security Strategy

One of the key tenets of the NSS is to "protect the American people, the homeland, and the American way of life" (from p. 4, published December 2017). As part of the NSS, the US "will protect our critical infrastructure and go after malicious cyber actors" (from p. 4, published December 2017). Bad actors are on the rise around the world and can have a devastating impact on the economy through disruption and exploitation of financial networks or through destruction of critical infrastructure such as the nation's electrical grid network.

The NSS (published December 2017) discusses various domains requiring protection, including land, air, sea, and space. In recent years, cyberspace has been added as a domain. The strategy also addresses our national response to cybercrimes and state-sponsored cybercriminals. The document recognizes the ability of adversaries to inflict damage upon the nation's infrastructure, methods of command and control, and communication networks without crossing territorial borders.

The NSS (published December 2017) addresses how to assess cyber risk and prioritize protective efforts, capabilities, and defenses to ensure uninterrupted, secure communication under all conditions. The document acknowledges that

economic and personal transactions depend on reliable and secure internet to help build personal wealth. With American culture influenced heavily by wealth and prosperity, the nation has naturally embraced the contributions of the cyber domain. A subset of the cyber domain within the NSS is the theft of intellectual property and technology through sophisticated, malicious cyber activities. The NSS concedes that the US has been complacent for too long.

Malicious actors "use cyberattacks for extortion, information warfare, disinformation, and much more" (from p. 31 of the NSS, published December 2017). A disinformation attack by a bad actor can be critical to an organization's future credibility if the attack is successful. The NSS states that the US will be "risk informed, but not risk averse, in considering our options" for response to cyberattacks (from p. 32, published December 2017).

National Cyber Strategy

Identifying the cyber threat as part of the NSS spawned the NCS. According to the NCS, "ensuring the security of cyberspace is fundamental" to protecting national security and promoting prosperity (from p. 1, published September 2018). Released by President Trump, the NCS is the first comprehensive strategy document addressing the criticality of the cyber threat to both public and private organizations. The strategy outlines how the US will respond to adversaries who would exploit, disrupt, or destroy the nation's cyber infrastructure. Additionally,

the strategy specifically addresses how the nation will protect networks, systems, functions, and data; nurture a secure digital economy; deter and punish those who exploit cyberspace for malicious purposes; and extend the benefits of a secure internet overseas.

In order to protect the American way of life, the NCS (published September 2018) seeks to secure federal networks, information, and critical infrastructure while combatting cybercrime and increasing incident reporting. Recognizing the importance of the cyber environment in today's society, the strategy seeks to capitalize on American ingenuity and incentivize innovation in security measures and intellectual property protection. Education on cyber threats is a key component of the strategy, as is enhancing the cybersecurity workforce. Making sure all potential users are aware of the threat is crucial to securing against potential damage from an attack.

The NCS also encourages direct attribution against those who seek to exploit or disrupt cybersecurity with severe consequences against malicious actors. It is important that the US government foster and implement international cooperation in the cyber domain. Universal adherence to cyber norms will help stabilize cyberspace and, along with shared intelligence and incident reporting, will help counter threats to cybersecurity. Through international cooperation with like-

minded countries and civil societies, the strategy seeks to "promote an open, reliable, and secure internet" (from p. 1 of the NCS, published September 2018).

International Strategy for Cyberspace

As the US has realized the global impact of cyberspace, the Obama administration promoted the ISC, which identifies cybersecurity as an obligation that governments and societies must take on willingly to ensure continued innovation, to drive markets, and to improve lives. The strategy expands the US vision for prosperity, security, and openness in a networked world by involving international partners. Overall, there is a commitment to preserve the best of cyberspace while safeguarding US principles by reflecting the nation's "core commitments to fundamental freedoms, privacy, and the free flow of information" (from p. 5 of the ISC, published May 2011).

The ISC (published May 2011) "seeks to develop solutions that are dynamic and adaptable, while rewarding innovation, entrepreneurship, and industriousness" (from p. 5). It seeks to "build and sustain an environment in which norms of behavior guide states' actions, sustain partnerships, and support the rule of law in cyberspace" (from p. 8). The strategy also encourages private-sector collaboration because the private sector holds a majority interest in the functionality of cyber networks.

Cybersecurity is a global issue that must be addressed by all nations, and the ISC (published May 2011) encourages multinational participation in cybersecurity exercises. It also encourages sharing of best practices among international agencies to take full advantage of new technologies and help establish effective policy.

Plans

National Preparedness Goal

The NPG is a "secure and resilient Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk" (United States Department of Homeland Security 2015, 1; hereafter US DHS). The greatest risks identified in the goal "include events such as natural disasters, disease pandemics, chemical spills and other manmade hazards, terrorist attacks and cyber-attacks" (US DHS 2019). The NPG recognizes that "cyber-attacks can have catastrophic consequences, which in turn, can lead to other hazards, such as power grid failures or financial system failures . . . cascading hazards increase the potential impact of cyber incidents" (US DHS 2015, 4). Additionally, the document emphasizes that "cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk" (US DHS 2015, 4). Further, the

document highlights that “cybersecurity poses its own unique challenges” and “represents a core capability integral to preparedness efforts across the whole community” (US DHS 2015, 5).

Cybersecurity is one of 32 core capabilities falling within the DHS mission area of protection (US DHS 2015). As defined in the NPG, cybersecurity is the process to “protect (and, if needed, restore) electronic communications systems, information, and services from damage, unauthorized use, and exploitation” (US DHS 2015, 9). Two specific preliminary targets exist for this core capability. The first is to implement risk-informed guidelines, regulations, and standards to ensure the security, reliability, integrity, and availability of critical information, records, and communications systems and services through collaborative cybersecurity initiatives and efforts. The second is to implement and maintain procedures to detect malicious activity and to conduct technical and investigative-based countermeasures, mitigations, and operations consistent with established protocols against malicious actors to counter existing and emerging cyber-based threats (US DHS 2015). Finally, the NPG stresses that preparedness planners “must also consider integrating cyber preparedness throughout core capabilities in every mission area” (US DHS 2015, 5).

Protection Federal Interagency Operational Plan

DHS has published a large collection of interagency operational plans for each mission area. As detailed above, cybersecurity is one of the core capabilities falling within the mission area of protection. Another core capability that has significance within the mission area of protection is access control and identity verification, as outlined in the FIOP (US DHS 2016b). As highlighted in this document, "access control and identity verification include the application of a broad range of physical, technological, and cyber measures to control admittance to critical locations and systems, limiting access to authorized individuals to carry out legitimate activities" (US DHS 2016b, B2-1).

The FIOP details 11 critical tasks that support cybersecurity protection coordinating activities, one of which is critical infrastructure security and resilience. Collaboration between government entities and the private sector are essential to ensure that information is shared on potential threats and that best practices are distributed to the owners and operators of critical infrastructure and to other private entities and organizations. An example of one of the critical tasks is to "implement countermeasures, technologies, and policies to protect physical and cyber assets, networks, applications, and systems that could be exploited to do harm" (US DHS 2016b, B8-1). Another private-sector example is to "formalize partnerships with governmental and private sector cyber incident or

emergency response teams to accept, triage, and collaboratively respond to incidents in an efficient manner" (US DHS 2016b, B8-1). Additionally, DHS will "collaborate with partners to develop plans and processes to facilitate coordinated incident response activities" (US DHS 2016b, B8-1). These critical tasks help ensure that DHS and the private sector work together to make critical information, records, and communications systems and services reliable and secure.

Information Technology Sector-Specific Plan

DHS is the sector-specific agency for the critical infrastructure sector of IT and is responsible for developing the ITSSP, which is an annex to the NIPP. The ITSSP acknowledges that "government and industry partnerships are critical to creating a continuous risk reduction system . . . effective collaboration among public and private sector partners is imperative to ensure the protection and resilience of IT Sector functions" (US DHS 2016a, iii). DHS has identified several priorities to guide security and resilience efforts, three of which are significant: 1) the NIST Framework for Improving Critical Infrastructure Cybersecurity, 2) situational awareness and information sharing, and 3) partnership and engagement (US DHS 2016a).

The US continuously faces cyberattacks against both public and private organizations and agencies. In addition to the strategies and protection plans highlighted above, several core PPDs, EOs, and government cybersecurity-

focused regulations and documents have been published to describe how the US responds and reacts to cyberattack. Tying together the multinational efforts to secure cyberspace in a singular framework has proven difficult but not insurmountable.

National Institute of Standards and Technology

Ashton Momot (2018) declared that cybersecurity threats change rapidly, requiring industry best practices to keep pace. Documentation and sharing of best practices lag behind the threat and often are outdated by the time of publication. This is where NIST fills the gap and specializes in forming standards, best practices, and publications to keep up with the ever-changing threat. While NIST provides pseudoregulatory guidance for government agencies, it only makes recommendations and suggestions of best practices for the public and private sectors. Updating documentation regularly through special publications, NIST remains at the forefront of helping harden cybersecurity posture (Momot 2018). The most commonly referenced material provided by NIST is its Framework for Improving Critical Infrastructure Cybersecurity.

The Cybersecurity Enhancement Act (CEA) of 2014 (Pub. L. No. 113–274, 15 USC 7421) updates the role of NIST to identify and establish a cybersecurity framework for voluntary use by critical infrastructure owners and users. It "amends the NIST Act to permit the Secretary of Commerce, through the Director

of the NIST, to facilitate and support the development of a voluntary, consensus-based, industry-led set of standards and procedures to cost-effectively reduce cyber risks to critical infrastructure (Homeland Security Digital Library 2019). The CEA of 2014 specifically prohibits the NIST director from prescribing specific solutions or designing services in a particular manner, and it prohibits standards developed through voluntary reporting to become regulation used by federal, state, tribal, or local agencies to regulate activity of any entity. "Through CEA, the NIST must identify 'a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including security measures and controls that may be voluntarily adopted by critical infrastructure owners and operators to help them identify, assess, and manage cyber risks'" (National Institute of Standards and Technology 2018, v; hereafter NIST).

NIST builds on the framework established by President Obama's 2013 EO 13636, Improving Critical Infrastructure Cybersecurity (78 Fed. Reg. 33), without placing additional regulatory guidance on businesses. The framework is a risk-based approach to managing cybersecurity risk and consists of three parts. The first part is the *Framework Core*, which captures cybersecurity activities, desired outcomes, and applicable regulations. It presents industry standards, guidelines, and practices in a manner that bridges cybersecurity concerns across the organization, from the tactical to the strategic levels (user to executive). It consists

of five concurrent or consecutive functions: identify, protect, detect, respond, and recover (NIST 2018).

Second is the *Framework Tiers*, which establishes different levels of how the organization views and accepts risk. Here the organization must consider its current risk management practices, threat environment, legal and regulatory requirements, business objectives, and organizational constraints. The third part is the *Framework Profile*, which characterizes how an organization views its cybersecurity readiness. To achieve the desired framework profile, an organization must self-assess to consider the current threat environment, degree of cyber security it requires, and the amount of financial commitment required to achieve the desired profile (NIST 2018).

Presidential Policy Directives and Executive Orders

Presidential Policy Directive 8

PPD-8, National Preparedness, supplied by President Obama on March 30, 2011, directs strengthening the security and resilience of the US through systematic preparation for the threats that pose the greatest risk to the security of the nation, which includes cyberattacks. The directive also institutes the NPG to identify core capabilities necessary for protection of critical infrastructure and a method to track progress toward that goal. PPD-8 directs the preparedness system to include

an integrated framework covering prevention, protection, mitigation, response, and recovery.

Presidential Policy Directive 21

PPD-21, Critical Infrastructure Security and Resilience, directed by President Obama on February 12, 2013, identifies 16 critical infrastructure sectors, including IT (cyber), and focuses on security and resilience. PPD-21 specifically calls for protection against cyber threats and directs the federal government to work directly with state, local, tribal, and territorial entities to protect critical infrastructure. It remarks that the combined efforts of all stakeholders will reduce vulnerabilities, minimize consequences, identify and disrupt threats, and hasten response and recovery efforts.

Three strategic imperatives are found within PPD-21. The first imperative is to refine and clarify the relationships across the federal government to advance the national unity of effort to strengthen critical infrastructure security and resilience. The second is to enable effective information exchange by identifying baseline data and systems for the federal government. The final imperative is to implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.

Presidential Policy Directive 41

PPD-41, United States Cyber Incident Coordination, directed by President Obama on July 26, 2016, outlines the federal government's response to any cyberattack, regardless of being against the government or private sector. PPD-41 requires DHS and the Department of Justice (DoJ) to publish contact information for public use for assistance in reporting cyber incidents to proper authorities. PPD-41 informs definitions, sets the guiding principles for incident response, identifies concurrent lines of effort, and establishes the significant-cyber-incident response architecture. The directive also reaffirms that protection of the IT (cyber) sector is a collaborative effort among government agencies, private organizations, and the public. The directive builds on and is complementary to PPD-8, reinforces preparedness for cyberattacks against a broad range of targets within the US, and provides direction to an organization for reporting cyber incidents to proper authorities.

Executive Order 13010

Following the bombing of the World Trade Center in 1993 and the Alfred P. Murrah federal building in 1995, President Clinton helped increase the nation's focus on protection of the most vital infrastructures and critical assets by signing EO 13010, Critical Infrastructure Protection, in 1996 (61 Fed. Reg. 138). The order recognizes that threats to "critical infrastructures fall into two categories:

physical threats to tangible property ('physical threats'), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ('cyber threats')" (p. 37347 of 61 Fed. Reg. 138). The focus on physical and cyber protections increased through subsequent administrations, usually in response to a successful threat activity directed against the US (such as 9/11) or against specific organizations.

Executive Order 13231

President G.W. Bush emphasized the importance of cybersecurity in 2001 through EO 13231, Critical Infrastructure Protection in the Information Age (66 Fed. Reg. 202). He understood that "the information technology revolution has changed the way business is transacted, government operates, and national defense is conducted . . . those three functions now depend on an interdependent network of critical information infrastructures" (p. 53063 of 66 Fed. Reg. 202). Additionally, he emphasized that the US must "protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible" (p. 53064 of 66 Fed. Reg. 202). EO 13231 also establishes the President's Critical

Infrastructure Protection Board, charged with working alongside the private sector in developing "voluntary standards and best practices" (p. 53064 of 66 Fed. Reg. 202), as well as creating an environment for information sharing. The order directs the board to "work with industry, State and local governments, and non-governmental organizations (NGO[s]) to ensure that systems are created and well managed to share threat warning, analysis, and recovery information" (p. 53065 of 66 Fed. Reg. 202). Finally, the order establishes a National Infrastructure Advisory Council, with one of its mandates being to "propose and develop ways to encourage private industry to perform periodic risk assessments of critical information and tele-communications systems" (p. 53069 of 66 Fed. Reg. 202).

Executive Order 13636

In 2013, President Obama signed EO 13636, Improving Critical Infrastructure Cybersecurity (78 Fed. Reg. 33). He stated that "repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity . . . the cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we [the US] must confront" (p. 11739 of 78 Fed. Reg. 33). He stressed that the US needs "to enhance the security and resilience . . . and to maintain a cyber-environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties" (p. 11739 of 78 Fed. Reg. 33).

President Obama further emphasized that the government and private sector need to continue developing their partnership "to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards" (p. 11739 of 78 Fed. Reg. 33). Additionally, he highlighted that the government has to "increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats" (p. 11739 of 78 Fed. Reg. 33).

Significantly, this EO directs the establishment of a baseline framework used to reduce cyber risks. As stated in the order, NIST would develop a cybersecurity framework to provide "a prioritized, flexible, repeatable, performance-based, and cost-effective approach . . . to help owners and operators of critical infrastructure identify, assess, and manage cyber risk" (p. 11741 of 78 Fed. Reg. 33). Additionally, the framework would "include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks" and "shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible" (p. 11741 of 78 Fed. Reg. 33).

EO 13636 also directs the US government, in coordination with sector-specific agencies, to establish "a voluntary program to support the adoption of the Cybersecurity Framework . . . and the Secretary [of Homeland Security] shall

coordinate establishment of a set of incentives designed to promote participation in the program" (p. 11741 of 78 Fed. Reg. 33).

Executive Order 13691

EO 13691, Promoting Private Sector Cybersecurity Information Sharing, signed by President Obama in 2015 (80 Fed. Reg. 34), provides that organizations engaged in information-similar cybersecurity-related risks are invaluable in their role in the collective cybersecurity of the US. Organizations must have the ability to share information or report cyber incidents and risks to proper authorities in as near real time as possible. EO 13691 encourages voluntary participation to establish mechanisms and improve capabilities to partner with the federal government in protecting IT. Information sharing must be conducted in a manner that protects the privacy and civil liberties of individuals, protects business confidentiality, and safeguards the information being shared.

Executive Order 13718

EO 13718, Commission on Enhancing National Cybersecurity, signed by President Obama in 2016 (81 Fed. Reg. 29), establishes a commission on cybersecurity within the Department of Commerce. The commission is charged with making recommendations to the government and private sector on how to bolster protection of systems and data. Some methods include advanced identity management, authentication, and cybersecurity of online identities. The order

determines that cybersecurity is to become a core element in the development of the Internet of Things (IoT) and cloud computing. Additionally, the order recommends increased quantities, quality, and expertise of the cyber workforce, including training and education, in both the government and private sectors. It also seeks to improve the broad-based knowledge and education of the general public in commonsense cybersecurity practices.

EO 13718 also directs the commission to make recommendations regarding governance, procurement, and management for federal civilian IT systems, applications, services, and infrastructure, including identifying the framework for which IT services should be procured, modernized, and shared across all agencies. It also recommends a governance model for managing risk, enhancing resilience, and ensuring proper response and recovery.

Finally, EO 13718 directs the commission to seek input from private-sector organizations that have experienced significant cyber incidents and share information with other private-sector organizations about cyber incidents and best practices used to protect IT systems.

Executive Order 13757

EO 13757, Taking Additional Steps to Address the National Emergency with Respect to Malicious Cyber-Enabled Activities, also signed by President Obama in 2016 (82 Fed. Reg. 1), amends EO 13691 freezes the assets of several entities

and organizations that have engaged in malicious cyber activity against the US, persons of the US, or US interests, regardless of whether the malicious cyber activity originated inside the US or outside in part or in whole, and prevents these assets from being transferred to any US citizen. Entities and individuals listed in the annex to this order have or are suspected to have committed a cybercrime or pose a significant threat to the US.

Executive Order 13800

EO 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, signed by President Trump in 2017 (82 Fed. Reg. 93), was issued in response to the Executive Branch identifying an IT weakness and vulnerability across the government due to antiquated hardware and software. To combat the vulnerabilities, the EO charges agencies to provide a risk management report to the Office of Management and Budget (OMB). OMB is directed to use the reports to ensure that adequate protections are in place to secure the Executive Branch cyber enterprise. Additionally, OMB is directed to resource any unmet budgetary needs and to establish a recurring process for review.

Further, the EO addresses the protection of critical infrastructure related to cybersecurity and those areas of "greatest risk of attack that could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security" (p. 22394 of 82 Fed. Reg. 93). In the

order, President Trump emphasizes deterrence and protection, as well as international cooperation and workforce development to create a stronger, cyber-aware talent pool in both the public and private sectors.

Executive Order 13870

EO 13870, America's Cybersecurity Workforce, signed in 2019 by President Trump (84 Fed. Reg. 90), recognizes the need for a talented cyber workforce, both in the public and private sectors. The EO seeks to capitalize on the mobility of cyber-smart workers between the public and private sectors while strengthening the overall workforce through peer mentoring and training. It also directs the establishment of an annual cybersecurity competition with individual and team events, software reverse engineering and exploitation, and other disciplines. The order also awards decoration equivalents to civilians for performance and achievements in cyber operations.

The overall intent of EO 13870 is to enhance the workforce in the cyber realm and incentivize cybersecurity best practices by providing a learning environment conducive to a dynamic and diverse workforce, as well as to establish measures of effectiveness demonstrating the impact of a cyber-secure workforce.

Executive Order 13873

The most recent relevant EO is EO 13873, Securing the Information and Communications Technology and Services Supply Chain, signed in 2019 by

President Trump (84 Fed. Reg. 96). It recognizes adversaries who are increasingly exploiting vulnerabilities in information and communication technology impacting our economy, infrastructure, and emergency services. Through the EO, the president declares this as a direct threat to national security, foreign policy, and our economy; the potential for sabotage from exploitation is defined in the EO as a "national emergency" (p. 22689 of 84 Fed. Reg. 96).

Additionally, EO 13873 prohibits actions that pose an undue risk of sabotage or subversion or that could have potentially catastrophic effects on the security of US infrastructure or national security. Finally, the EO restricts who can do business in the information and communication technology realm.

Public Laws

The National Cybersecurity Protection Act of 2014 (Pub. L. 113-282) establishes the National Cybersecurity and Communications Integration Center (NCCIC) within DHS. According to the stipulations of the law, the functions of the center include being the "federal civilian interface for the . . . sharing of information related to cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities" and "providing shared situational awareness to enable real-time, integrated, and operational actions across the Federal Government and non-Federal entities to address cybersecurity risks and incidents to Federal and non-Federal entities" (p. 3067 of Pub. L. 113-282). Additionally, the NCCIC is

responsible for “coordinating the sharing of information related to cybersecurity risks and incidents” and “facilitating cross-sector coordination . . . including cybersecurity risks and incidents that may be related or could have consequential impacts across multiple sectors” (p. 3067 of Pub. L. 113-282).

Another relevant public law is the Consolidated Appropriations Act, 2016 (Pub. L. 114-113). Within the Consolidated Appropriations Act, 2016, is the Cybersecurity Act of 2015. This broad grouping includes the Cybersecurity Information Sharing Act of 2015, the National Cybersecurity Protection Advancement Act of 2015, the Federal Cybersecurity Enhancement Act of 2015, and the Federal Cybersecurity Workforce Assessment Act of 2015. While these may seem outdated, Section 401 of the Consolidated Appropriations Act, 2016, specifically addresses a study on the use of mobile devices by government employees. It states that “the Secretary of Homeland Security, in consultation with the Director of the NIST, shall complete a study on threats relating to the security of the mobile devices of the Federal Government; and submit an unclassified report to Congress . . . that contains the findings of such study, the recommendations developed,” and “the deficiencies” (p. 2977 of Pub. L. 114-113).

Conclusion

Technological advancements in the last 30 years have greatly improved the quality of life for most Americans and countless citizens of other countries around the world. The internet has created avenues for international communication and commerce never before dreamed of. However, with great advancements in technology, there is always a bad actor willing to exploit vulnerabilities wherever they can be found. The US has recognized the increasing requirement to secure the cyber domain from attack or exploitation and has published numerous documents outlining how to proceed.

The strategy documents for national security, national cyberspace, and international cyberspace give a broad outline of the threat and describe necessary actions to combat the hazards. There is an increasing sense of urgency in the strategy documents as the cyber domain expands to include the cloud. DHS has taken the lead in developing plans for the protection of critical infrastructure and cyber networks to mitigate the damage caused by successful attacks. Response and recovery efforts are crucial to ensuring minimal disruption from a cyber incident.

Every president since Bill Clinton has promulgated at least one EO specifically addressing the criticality of the nation's cyber infrastructure and networks. Each mentions the need to expand the cyber awareness of all employees in both the

public and private sectors and encourages information sharing among all users to help establish best practices and security for all. The majority of cyber-related EOs have only been issued in the last six years under President Obama and President Trump.

A cybercriminal can be a large corporate or governmental entity intent on stealing intellectual property for personal use and exploitation, or it can be a lone wolf, a single entity, intent on doing harm or stealing someone else's hard-earned money. Either way, the bad actors must be stopped, and increased awareness of threats in the cyber domain is the first step.

SECTION II: IDENTIFY THREATS

Summary

In order for organizations to mitigate the risk of cyber exploitation effectively, they must be cognizant of the multitude of threats that exist in their area of operation. Recognizing these threats and identifying the actors behind them allows the organization to build up its defenses. Cyberattacks can be perpetrated by a variety of actors, both internal and external. This paper categorizes them into three groups: nonstate actors, state actors, and insiders.

Nonstate actors include hacktivists, cyber terrorists, organized cybercriminals, and corporations. Each actor has different motivations, but they may use similar means to gain access to cyber networks. It is also important to recognize the potential for nation-states to contract with nonstate actors to attack on their behalf.

State actors include the governing bodies of nation-states. For the purpose of analysis, this paper discusses two predominant state actors: Russia and China. While any nation-state may decide to exploit cyber vulnerabilities, these two actors provide ample examples of the capabilities of nation-states and the interest they have in the affairs of the US.

This section concludes with an overview of one of the most overlooked but extremely dangerous threats: the insider. These actors are trusted to access an

organization's most sensitive information, but they choose to leak that information for personal gain or in cooperation with other types of actors.

Regardless of the actor, organizations can take steps to promote domain awareness and counteract malicious attacks. The fast pace of cybersecurity makes it a challenge for organizations to stay current on the variety of threats that exist, but dedicating adequate resources and implementing best practices can significantly bolster an organization's cybersecurity program.

Introduction

While the internet has undoubtedly transformed our world for the better in countless applications, it also has transformed itself into a warfare domain, where perpetual combat between adversaries continually wages. Although cyber adversaries do not wear uniforms or wave flags to denote affiliation, there exists an unquestionable contention for guarded information, sensitive network systems, and even military superiority among nonstate actors, state actors, and—arguably the most potentially damaging entity of them all—witting or unwitting insiders. This portion of the literature review focuses on these three categories of adversary, who our team believes pose the most considerable threat to the integrity of an organization's information network infrastructure.

The first portion of this section covers the threat posed by nonstate actors, who are inarguably the most versatile of the three primary threats We provide a brief

overview of some of the most prolific forms in which this threat can emerge, paying specific attention to the subcategories that we believe pose the most considerable threat to an organization's cybersecurity.

We then move on to a more conventional antagonist, state actors. While the list of state actors who have proven themselves to be a legitimate threat to western organizations is substantial, this portion of the literature review focuses on the two countries identified in the current National Defense Strategy as the most dangerous: the Russian Federation and the People's Republic of China (United States Department of Defense 2018). Finally, we conclude our literature review with the pernicious danger that stems from within the inner sanctum of an organization: the insider threat. In this section, we delve into the factors that could serve as indicators for identifying individuals who exhibit traits common with saboteurs, followed by the potential for prominent organizations to become the victim of economic espionage. The insider threat section concludes with a presentation of the legal framework for how the US defines espionage of this nature.

Literature Review

Nonstate Actors

The term *nonstate actor* can be defined as any individual or group not associated with a government organization. This broad definition includes a variety of actor

types, all of whom have different motives, victims, and tactics. Because of the variances among them, nonstate actors should not be construed as an all-inclusive term by which a policy can remain stagnant. When creating policies to mitigate the threat posed by nonstate actors, policymakers should not coalesce all forms of nonstate actors into the same category because of the variance of their organizations, abilities, and methodologies.

Sigholm (2016) broke up and categorized the various nonstate actors known to operate in the cyber realm. Sigholm (2016) also acknowledged the overly broad categorization of nonstate actors, describing cyberspace as "a global domain" where "different actors exist in parallel, with varying needs, goals and intentions" (9). The author found it beneficial to create subcategories of nonstate actors and organized them by 1) the extent of organizational structure and use of networking, 2) the motivating factors of the cyberattack, 3) the victims targeted, and 4) the methods or strategies employed (Sigholm 2016). Segmentation of nonstate actors into subcategories provides policymakers with a more comprehensive understanding of the threat environment. Organizations may choose to write a cybersecurity policy that prioritizes the types of attacks to which they are more susceptible.

There are a variety of nonstate actors who utilize vulnerabilities in cybersecurity to achieve their objectives. Nonstate actors may include individual criminals,

organized crime networks, terrorist organizations, hacktivist groups, and groups with opposing political views. Table 1 provides an idea of the global domain in which anyone can be a target for any given reason using a variety of methods (Sigholm 2016). The combinations are nearly endless and always changing, which is why cybersecurity is so difficult to achieve.

Actor	Motivation	Target	Method
Ordinary citizens	None (or weak)	Any	Indirect
Script kiddies	Curiosity, thrills, ego	Individuals, companies, governments	Previously written scripts and tools
Hacktivists	Political or social change	Decision-makers or innocent victims	Protests via webpage defacements or direct-denial-of-service (DDoS) attacks
Black-hat hackers	Ego, personal animosity, economic gain	Any	Malware, viruses, vulnerability exploits
White-hat hackers	Idealism, creativity, respect for the law	Any	Penetration testing, patching
Gray-hat hackers	Ambiguous	Any	Varying
Patriot hackers	Patriotism	Adversaries of own nation-state	DDoS attacks, defacements
Cyber insiders	Financial gain, revenge, grievance	Employer	Social engineering, back doors, manipulation
Cyber terrorists	Political or social change	Innocent victims	Computer-based violence or destruction
Malware authors	Economic gain, ego, personal animosity	Any	Vulnerability exploits
Cyber scammers	Financial gain	Individuals, small companies	Social engineering
Organized cybercriminals	Financial gain	Individuals, companies	Malware for fraud, identify theft, DDoS for blackmail
Corporations	Financial gain	Information and communications technology-based systems and infrastructures (private or public)	Range of techniques for attack or influence operations
Cyber-espionage agents	Financial and political gain	Individuals, companies, governments	Range of techniques to obtain information
Cyber militias	Patriotism, professional development	Adversaries of own nation-state	Based on the group capabilities

Table 1. Nonstate Actors in Cyber Conflict (Recreated from Sigholm 2016)

In order to remain brief and relevant to the threats posed to prominent organizations, this literature review focuses on hacktivists, cyber terrorists, organized cybercriminals, and corporations. Cyber insiders and cyber-espionage agents are addressed in another portion of this literature review. This section concludes with a discussion about nonstate actors being subcontracted to conduct cyberattacks on behalf of a nation-state.

Hacktivists

Hacktivism is a virtual means of protest in which the actor uses the cyber platform to express a political ideology or agenda (Sigholm 2016). Hacktivists tend to believe that their skills can be used to advance ethics and human rights, yet their methods are ethically questionable (Sorrell 2015). Hacktivists leverage their skillset to gain power over specific issues. The nature of cyberspace provides them the opportunity to transcend the physical boundaries and controls of nation-states and organizations (Sorrell 2015).

The group Anonymous is widely known as a network of hacktivists who work cooperatively to attack certain targets (Olson 2012). Members of hacktivist groups often communicate and coordinate their activities through nonmainstream social media platforms such as 4chan, 711chan, Encyclopedia Dramatica, and the Internet Relay Chat (IRC) network (Bernstein *et al*. 2011). These forums serve as a place to anonymously recruit, communicate with, and verify the skills of

participants, as well as to share malware (Bernstein *et al.* 2011). This concept allows individual hacktivists to find and contribute to any cause they wish to support.

Hacktivists differ from other types of nonstate actors because they intentionally make their attacks known to the public (Sigholm 2016). The anonymity that they can achieve through collective action takes some of the personal responsibility out of the act (Bernstein *et al.* 2011). The theories of group dynamics still apply to the cyber platform: as a group increases in size, individual members of the group feel less responsible for any actions or decisions made collectively by the group (Thackray and McAlaney 2018). Hacktivists typically want the public to know about the cyberattack in order to draw attention to their agenda (Mansfield-Devine 2011). The occurrence of a cyber breach alone is cause for embarrassment, but hacktivists typically harden the blow by publicly disseminating confidential or defaming documents. Some examples of the tactics used by hacktivists include "web site defacements, internet resource redirects, denial-of-service attacks, information theft, web site parodies, virtual sit-ins and various forms of cyber- sabotage" (Sigholm 2016, 14).

When considering the political arena in which think tanks and political research organizations exist, the perception of credibility becomes paramount to maintaining influence. Hacktivists have the ability to disrupt and defame a think

tank, utilizing the target organization's own networks and domain. One example is Jeremy Hammond, who was arrested in 2012 after he was able to breach Stratfor, a security think tank with connections to DHS and the Department of Defense (DoD). The breach of the think tank's network was "not just embarrassing for a prominent purveyor of intelligence, but also potentially worrisome for Stratfor's clients" (Trumbull 2011, para. 5). Immediately following the breach, multiple donors and clients were being targeted (Connelly 2011).

Cyber Terrorists

Terrorism is defined by the US as "the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives" (from p. 51 of 28 CFR 0.85). While cyberattacks certainly have the ability to coerce a government or intimidate the civilian population, they generally fail to meet the "use of force or violence" component of the definition. For this reason, some argue that cyberterrorism doesn't exist (Escobar 2019).

Intelligence sources have confirmed that terrorist organizations have an interest in using cyberattacks to accomplish their objectives (Coats 2018). While they may not appear to possess the typical idiosyncrasies of traditional terror attacks, cyberattacks can have a significant impact on society and government. Take, for instance, the introduction of ransomware to government officials, law

enforcement agencies, healthcare systems, school districts, and other critical infrastructure (Cybersecurity and Infrastructure Security Agency 2019). This type of ransomware attack could disrupt basic functions of society for prolonged periods of time, especially if response procedures are not in place.

Beyond crippling critical infrastructure, terrorist organizations can exploit vulnerabilities in cyberspace to gather intelligence and conduct counterintelligence operations (Sigholm 2016). Even if the cyberattack itself doesn't meet the criteria to be classified as terrorism, the information gathered from government and law enforcement networks can contribute to a successful attack. Ransomware may also provide the terrorist organization with the funding and material resources necessary to carry out a traditional attack. The lack of violence associated with cyberattacks should not detract from the significant contributions they make to the overall objectives of terrorist organizations.

Organized Cybercriminals

Organized cybercriminals are a branch of traditional organized crime with an objective of economic gain (Sigholm 2016). This method of financial gain is appealing because it adds a layer of anonymity and reduces the physical risks of typical criminal acts (Sigholm 2016). Law enforcement agencies have found it difficult to offensively pursue cyber-related crimes, as they provide "low thresholds for entry" and "easy access to large groups of potential targets"

(Sigholm 2016, 19–20). The actor may be a standalone cybercrime organization or may serve as an accessory to a drug cartel, human-trafficking organization, or terrorist organization. The high-profit margins associated with cyberattacks, along with the current lack of distinct territories or market boundaries, have certainly contributed to the increase of organized cybercrime within the past decade.

Much like their terrorist counterparts, criminal organizations are interested in any intelligence they can gather from government or law enforcement entities. Mexican drug cartels have been known to kidnap computer and IT experts, forcing them to work for the cartel (Abreu 2012). In 2015, drug cartels demonstrated the ability to hack into surveillance drones being used by US Customs and Border Protection to feed inaccurate location information to law enforcement (Thompson 2015). The acquisition of intelligence and the ability to furnish false intelligence has the potential to put law enforcement at risk and make organized criminal operations more effective. In addition, the illicit revenue from cyberattacks has the potential to enable the funding of other types of criminal activity that have a direct impact on homeland security.

Private Corporations

Corporations are typically expected to be law-abiding organizations, but that does not exempt them from being motivated by profit margins, a desire for political influence, or market domination (Sigholm 2016). The same can be said for think

tanks and other political research organizations. Private corporations that operate in a capitalist economy are no stranger to identifying their competition and seeking to eliminate that external threat. Corporate espionage is the practice of organizations gathering intelligence on their competitors. The intelligence gathering can be achieved in several ways, such as posing as an employee, accessing physical files, wiretapping, recording meetings, hacking, or attacking with malware (Fruhlinger 2018). Organizations with strong political influence are likely to see corporate espionage attacks from groups with opposing political perspectives. In some situations, nation-states may request a private corporation to conduct cyber operations for the government's benefit. One example of this is Google's Chinese subsidiary being forced to conduct cyberattacks against Google and other private corporations in the US (Buley and Greenberg 2010). There have also been instances of state-sponsored espionage occurring under the guise of a private corporation.

Nonstate Actors Subcontracted to Nation-States

Naturally, there are political and diplomatic risks associated with cyberattacks. Nation-states may not have the resources or desire to be the bad actor and may hire a nonstate actor to do the work for them. Nonstate actors are frequently approached by nation-states that "seek to benefit from their experience and

leverage their cyber know-how" (Sigholm 2016). Table 2 describes the benefits and drawbacks of nation-states utilizing nonstate actors for cyberspace operations.

Benefits	Drawbacks
Gaining the initiative—element of surprise	No direct control of nonstate actors
Plausible deniability	Risk of unintended collateral damage
Ability to choose target and attack vector	Targeting of own resources
Determinate scale and duration of attack	Escalation to conventional war
Exploitation of legal uncertainties	Labeling as sponsor of terrorism
Possibility of rapid attacking-by-proxy	Backlashes (blackmailing etc.)

Table 1. Benefits and Drawbacks of Using Nonstate Actors in Cyberspace Operations (Recreated from Sigholm 2016)

State Actors

China

In his 5th-century military strategy treatise *The Art of War*, legendary Chinese military general and tactician Sun Tzu theorized that "all warfare is based on deception" (Tzu 2002). This ancient wisdom holds true in the modern era, as countless cyberattackers from the People's Republic of China (PRC) continue to conduct maliciously clandestine cyber-espionage attacks against the nation's adversaries. While it is unknown when the PRC began to wage its cyber-based information-gathering campaign, some experts believe that the Chinese government began significantly increasing its cyberattack capabilities around

2007. After the infamous 2007 attack on the Pentagon, an unnamed DoD official was quoted as saying that "the PLA [People's Liberation Army] has demonstrated the ability to conduct attacks that disable our system . . . and the ability in a conflict situation to re-enter and disrupt on a very large scale" (Sevastopulo 2007, para. 9). The same official later revealed that the PLA had, in addition to the Pentagon, penetrated the networks of US defense companies and American think tanks (Sevastopulo 2007). This cyberattack served as a shot across the bow for the American intelligence community; cyber actors subordinate to the Chinese government had carried out one of the most successful advanced persistent threat (APT) attacks in history, and this was only the beginning.

The purpose of an APT attack is to steal data, disrupt operations, or destroy infrastructure. Unlike most cybercriminals, APT attackers pursue their objectives over long periods of time, most often ranging from a few months to multiple years (FireEye 2019). When conducting an APT attack, the aggressors must often adapt to cyber defenses and frequently retarget the same victim (FireEye 2019). Because of the tactic's inconspicuous nature and historical effectiveness, Chinese state-sponsored cyber actors have adopted the APT attack as one of their most utilized forms of data exfiltration. One of the more infamous APT malware strains developed and utilized by Chinese state-sponsored hackers is a cyber-espionage tool known as ICEFOG.

The first variant of ICEFOG, known as ICEFOG Old, was first discovered in 2011 (Kaspersky 2013). Over the next seven years, in response to China's intended targets adapting to the malicious virus, five different strains of ICEFOG were discovered. FireEye senior researcher Chi-en (Ashley) Shen believes that the ICEFOG variants are primarily utilized as an intelligence-gathering tool for the PRC (Cimpanu 2019). In the book *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, the author described how ICEFOG infiltrates a target's network: "Through phishing emails and infected attachments, the ICEFOG controllers can upload basic system information about infected computers, which will then allow them to run commands on the infected system. The attacker is enabled to steal files and execute commands on certain types of servers. Unlike other attacks, computers infected by ICEFOG do not automatically download files but are instead individually commanded" (Cheng 2016).

Another strategy, known as a "watering hole," is a known staple of state-sponsored Chinese cyber actors. A watering hole attack is a security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit. The goal is to infect a targeted user's computer and gain access to the network at the target's place of employment (Rouse 2015). Like ATP attacks, watering hole attacks can be time-consuming for the cyber actor, but also very effective if carried out with

meticulous planning. Watering hole attacks are set up to target a specific individual or group of individuals. During a watering hole attack, the cyber actor monitors the type of websites frequently visited by the intended victim, effectively profiling the victim's online pattern of life. Once the cyber actor concludes a successful profile of the intended victim to the extent that they know the victim's online pattern, the cyber actor then seeks out vulnerabilities within the preferred websites of the victim. Once a vulnerability within a frequently visited website is identified, the cyber actor injects a malicious JavaScript or HTML code that redirects the target to a separate site where the malware is hosted (Rouse 2015).

Although the Chinese government carried out its first major cyberattack on the US government in 2007, the Chinese military did not address the concept of cyber warfare until 2013, with the publication of *The Science of Military Strategy*. Based on the information contained in this PRC government document, McReynolds (2015) synthesized the Chinese cyber posture with the following three entities:

- The PLA's specialized military network warfare forces (军队专业网络战力量), which are military operational units specially employed for carrying out network attack and defense

- PLA-authorized forces (授权力量), which are teams of network warfare specialists in civilian organizations such as the Ministry of State Security (MSS), the Ministry of Public Security (MPS), and others that have been authorized by the military to carry out network warfare operations
- Nongovernmental forces (□ 间□ □), which are external entities that spontaneously engage in network attack and defense

In 2017, CrowdStrike's Falcon Intelligence group reported that Chinese actors had been discovered conducting espionage-driven targeted attacks against at least four western think tanks and an additional two NGOs (Kozy 2017). It is generally believed that these attacks were conducted by Chinese government-sponsored hacker groups. The attacks began in an effort to gain access through internet-facing websites using the web shell now widely known as the China Chopper (Gallagher 2017). Once in, the attackers used credential-stealing tools such as Mimikatz, which focuses on Microsoft Active Directory. These brash cyberattacks against western think tanks are likely indicative of China attempting to increase its international prestige in research and innovation (Gallagher 2017). Given the amount of importance that China places on being accepted as a major contributor to academic research and technology innovation, there is no reason to believe that China will decrease its cyber-based information operations in the future. Any organization conducting groundbreaking research and development is

very likely to be a well-sought-after target for Chinese state-sponsored cyber-espionage groups.

Russia

The year 2007 marked the arrival of large-scale state-sponsored cyberattacks against the foundations and infrastructure of sovereign countries. As mentioned previously, the PRC government waged a considerably destructive cyber campaign against the US DoD in 2007. Around the same time, the Russian Federation was also flexing its newly formed cyber capabilities with a large-scale DDoS attack on the country of Estonia. The Russian state-sponsored cyberattacks were part of a wider political conflict between Estonia and Russia over the relocation of a Soviet-era monument in Tallinn, Estonia's capital city (Ottis 2008). This attack, and the many to follow in the subsequent years, is indicative of Russia's increasing proclivity to utilize cyberattacks as a form of retaliation for countries that act or speak out against Russia.

A 2017 article for *Foreign Policy* described Russia's inclusion of cyber warfare in their national defense strategy as "meld[ing] cyber into broader strategies that combine hacks with information war, hybrid war, or old-fashioned conventional war in a bid to advance Moscow's aims" (Tamkin 2017, para. 8). The Russian offensive strategy of initiating cyber-warfare attacks as an act of retaliation against nongovernment entities has become an increasingly dangerous issue for

companies, NGOs, and think tanks. In August 2018, Microsoft discovered Russia conducting cyberattacks against the Hudson Institute and the International Republican Institute, both conservative think tanks based out of Washington, DC. Prior to the attacks, the Hudson Institute had recently published multiple studies concerning the rise of kleptocracy, especially in Russia, and had been critical of the Russian government, according to *The New York Times* (O'Brien 2018). Cyber actors located within Russia, with arguable ties to the Russian government, carried out the cyberattacks that followed the publication of the Hudson Institute's antikleptocracy articles. Speaking at the Hudson Institute later that year, Director of National Intelligence (DNI) Dan Coats singled out the Russian government as one of the "most aggressive" purveyors of cyber warfare, highlighting the country's reported efforts to use hacking and information campaigns to influence US elections (Shoorbajee 2018, para. 4).

The Russian government believes that exploiting the relative ambiguity of cyber warfare on its perceived adversaries is an effective and legitimate strategy to shape world order and persuade other organizations and governments to refrain from speaking out against the Russian government. The Russian government's strategy of weaponizing the internet allows it to carry out offensive assaults on its adversaries halfway around the world without having to physically move militia or weapons. In addition, clandestine cyberattacks allow Russia to evade attribution for the country's assaults on sovereign nations. It is highly suspected

that a Russian Main Intelligence Directorate (GRU)–linked group, known as APT 28 or Fancy Bear, carried out the 2018 Hudson Institute attack (O'Brien and Bing, 2018). Appropriately, the Hudson Institute concluded that the Russian intention with this attack was to gather information about, and compromise or otherwise disrupt, the Hudson Institute's long-standing democracy-promotion programs, in particular, its initiatives to expose the activities of foreign kleptocratic regimes (Hudson Institute 2018). Because of its cyberattacks primarily being utilized to control the public narrative concerning Russian affairs, Moscow's current cyber-warfare strategy is the epitome of Prussian general Carl von Clausewitz's (1918) sagacious axiom, "war is the mere extension of politics through other means".

Spear Phishing

The cyber group that conducted the 2018 attacks on the Hudson Institute and the International Republican Institute utilized various spear-phishing campaigns in order to exfiltrate the information it sought. Spear phishing is an email or electronic-communication cyberattack targeted toward a specific individual, organization, or business. Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user's computer (Kaspersky 2019). In these particular cyberattacks, employees of the aforementioned think tanks received emails containing links to malicious websites that were designed to appear legitimate to the intended victim. At the time of the attack, Microsoft reported that the company had identified and shut down 84

fraudulent websites owned by Fancy Bear for the purpose of ongoing spear-phishing operations (O'Brien and Bing 2018). Spear phishing is not a new methodology, but Russian groups such as Fancy Bear are famous for adapting older methodologies and incorporating new innovations that make their capabilities considerably more effective and dangerous.

In late 2018, the global threat intelligence team at Palo Alto Networks, Unit 42, intercepted a series of weaponized documents that use a technique to load remote templates containing a malicious macro, which is a common telltale sign of a phishing document (Falcone and Lee 2018). However, although the email looked like a typical phishing document on the surface, it concealed a new unconventional malicious technology within. According to Falcone and Lee (2018), Fancy Bear utilized the following innovative methodology:

> . . . the C2 servers for several of these documents were still operational allowing for retrieval of the malicious macro and the subsequent payloads. Analysis revealed a consistent first-stage payload of the well-documented Zebrocy Trojan. Additional collection of related documents revealed a second first-stage payload that we have named 'Cannon'. Cannon has not been previously observed in use by the Sofacy group and contains a novel email-based C2 communication channel. Email as a C2 channel is not a new tactic, but it is generally not observed in the wild as often as HTTP or

> HTTPS. Using email as a C2 channel may also decrease the chance of detection, as sending email via non-sanctioned email providers may not necessarily construe suspicious or even malicious activity in many enterprises. (para. 2)

According to SANS Institute Director of Research Allen Paller, 95% of all attacks on enterprise networks in 2013 were the result of successful spear phishing (Weinberg 2013). One of the reasons that spear phishing is so popular among state-controlled cyber-espionage groups is the relatively low cost of a spear-phishing campaign versus other cyber-espionage methodologies. Considerable insight into Russian utilization of spear-phishing campaigns was presented in the *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, informally known as the Mueller Report (Mueller 2019). Spear phishing was one of the primary tools that Russian GRU military unit 74455 utilized to hack the campaign of presidential candidate Hillary Clinton (Mueller 2019). The following excerpt from the Mueller Report reveals how one spear-phished Democratic Congressional Campaign Committee (DCCC) employee's email account led to further exploitation of the DCCC network: "By no later than April 12, 2016, the GRU had gained access to the DCCC computer network using the credentials stolen from a DCCC employee who had been successfully spear phished the week before. Over the ensuing weeks, the GRU traversed the network, identifying different computers connected to the DCCC network. By

stealing network access credentials along the way (including those of IT administrators with unrestricted access to the system), the GRU compromised approximately 29 different computers on the DCCC network" (Mueller 2019, 38).

The Mueller Report goes on to describe how multiple entities, employees, and volunteers working on the Clinton campaign were also the victims of the GRU spear-phishing campaign against the Clinton presidential campaign in 2016 (Mueller 2019). The number of victims who were tricked into giving the Russians access to sensitive networks is indicative of the simplicity of conducting spear-phishing attacks; once the malicious technology is created, all a cyber actor needs to do is find a human vulnerability. Another reason that spear phishing is a popular methodology for Russian-controlled cyber groups such as Fancy Bear is the relative ease of carrying out a campaign of this nature due to the lack of operational security demonstrated by younger employees.

Symantec's (2016) *Internet Security Threat Report* indicated spear-phishing attacks as beginning to incorporate less mass-spam mails to large target groups of employees at once. In a change of *modus operandi*, Russian cyber actors' new approach includes selecting fewer recipients with a more coordinated approach. This method takes much more investigating of the intended target, but has been favored because of its relatively greater success over a period of time due to the specifically tailored phishing emails and websites to lure in victims. Cyber actors

are likely to continue employee spear-phishing methodologies regardless of the measures undertaken by organizations because of the likelihood of finding one vulnerable individual within the organization who can be exploited as an entry into the entire network.

The Russian threat to think tanks continues to grow every year because of a rise in geopolitical tensions between Russia and western nations. The most brazen example of the rise in cyber hostility toward western think tanks is Microsoft's February 2019 announcement of 104 breach attempts of democratic institutions, think tanks, and nonprofit organizations in Europe, presumably conducted by Russian-backed cyber groups (Burt 2019). In this particular volley of attacks, Microsoft Vice President for Customer Security and Trust Tom Burt reported that Russia had targeted accounts in Belgium, France, Germany, Poland, Romania, and Serbia via spear-phishing campaigns designed to gain access to employee credentials and deliver malware (Burt 2019). Once again, Fancy Bear is likely to be the culprit behind these spear-phishing attacks. As tensions rise and western think tanks continue to publish research and articles with narratives counter to Russia, the amount of cyberattacks toward think tanks and similar organizations are surely to rise, with potentially worse ramifications beyond the exfiltration of information.

Insider Threats

Threats by state and nonstate actors are significant and can receive front-page headlines when they occur. A third category can cause equally serious losses as do hacktivists and nation-states, as well as can erode trust within an organization: the insider threat. An insider threat encompasses malicious actions taken by a trusted insider to either harm the organization, benefit the insider, or both (Greitzer and Hohimer 2011). These acts can attack computers, computer networks, or IT by espionage, sabotage, or leaking of proprietary or classified data (Greitzer and Hohimer 2011).

The insider threat is not new in general, nor is it new to computer and information systems in particular. The DoD inspector general found that 87% of identified intrusions into DoD computer systems resolve to employees or others with internal access (Greitzer and Hohimer 2011). A review of 141 confirmed data breaches investigated in 2009 by the US Secret Service found 46% as being caused by trusted insiders—and 90% of those insider breaches were malicious and deliberate (Greitzer and Hohimer 2011). According to the Computer Emergency Response Team Insider Threat Center, over one-fourth of insiders exhibit behavior warranting scrutiny, including increased cellular phone use at the workplace, outbursts at coworkers, and isolation from colleagues (Greitzer and Hohimer 2011). When these employees are reprimanded for poor performance or

announce their intention to resign or leave the organization, the insider threat risk increases (Greitzer and Hohimer 2011). Malicious insiders can act on their own behalf or in cooperation with a nonstate or state actor.

The challenge for organizations is to identify potential insider threats before they occur. According to the Federal Bureau of Investigation (FBI) (2019), employees who possess the following personal factors may be exhibiting traits that have been found in insider threat cases:

- Feelings of anger or revenge and wanting to retaliate against the organization
- Disagreements with coworkers or managers
- Lack of recognition or dissatisfaction with their job
- Allegiance to another person, company, country, or cause
- Vulnerability to blackmail or engaging in self-destructive behavior steaming from illegal drug use, gambling, affairs, or alcohol abuse
- Marital or family problems
- Displaying an above-the-rules attitude
- A desire to integrate themselves with individuals or organizations that would benefit from insider information

According to Bunn and Sagan (2016), there is a universal framework of six points or questions to analyze the potential of insider threats, whether the organization is trying to protect nuclear material, pharmaceuticals, or the assets of a casino.

- What is the procedure to screen insiders and later rescreen as their career progresses to ensure they are trustworthy? This check can range from basic criminal-history checks at a minimum to a thorough background investigation covering all aspects of a person's adult life. Regardless of the degree of screening utilized, the organization has to balance the degree of intrusion into the privacy of employees with access to sensitive material and the potential damage an employee could exact (Bunn and Sagan 2016).
- Staff must be trained and motivated to minimize their susceptibility to becoming insider threats, as well as to identify and report suspicious activity or security lapses. Organizations can show how they value employees through good pay or compensation and respecting their opinions and concerns. Additionally, training programs can show employees how to recognize potential insider threats. This can involve the use of controlled mock attacks to test cyber defenses or the use of red teams to attempt to access physical installations or gain information through controlled threat and other security issues. Training should

emphasize the need to report concerns to proper officials (Bunn and Sagan 2016).

- How are the company's valuable assets secured, controlled, monitored, and accounted for? Regardless of the industry or setting, almost every organization has measures to secure its valued assets or information, which normally include monitoring the asset, regular review or accounting measures, and determining which employees require access (Bunn and Sagan 2016).
- Interaction between employees and the valued assets or information should be monitored and limited and should occur in a protected environment. Establishment of criteria such as a two-person rule when accessing the material, the use of closed-circuit television cameras, and retaining the assets in a secured room or housing information on a limited access network are all ways to protect against insider threats (Bunn and Sagan 2016).
- Procedures should be established to address potential insider threats suspected within the organization. An organization should have guidance in place to investigate potential security violations and insider threats in a discreet manner that will neither disrupt the organization's work or workforce nor unnecessarily impact employee morale (Bunn and Sagan 2016).

- A plan should be made, security measures should be tested and assessed, and the results should be reviewed for lessons learned and identification of gaps or areas for improvement. This can involve the use of controlled mock attacks to test cyber defenses or the use of red teams to attempt to access physical installations or gain information through controlled social engineering (Bunn and Sagan 2016).

Employees of most businesses and organizations are likely carrying an ever-present cellular phone or other personal electronic device, complete with photographic and video capability, which a malicious insider could use to photograph or video documents and record meetings (Jaffee 2017). These devices also commonly connect to organizational networks via wireless network or Universal Serial Bus (USB) drive and could be used to download proprietary files or receive organizational data emailed to the device on a private account for a malicious purpose. To counter malicious insiders from corrupting, deleting, or exfiltrating data, network-monitoring software programs can be utilized to detect abnormal activity, such as downloading large volumes of documents or actions that violate organizational policy, such as accessing personal information of donors (Punithavathani, Sujatha, and Jain 2015).

To combat the insider threat from cellular phones, USB drives, and other peripheral devices that can enter the workplace under a bring-your-own-device

(BYOD) system, Gewirtz (2011) recommended that an organization take the following steps:

1. Use an automated defensive system in the computer and an information storage network that are capable of not only detecting intrusions, but also identifying and neutralizing devices attempting to access the network physically or remotely through the ether (Gewirtz 2011).
2. Ensure passwords are mandated to change regularly, and when an employee departs the organization for any reason, promptly terminate their passwords and accompanying accounts (Gewirtz 2011).
3. Implement multifactor authentication (MFA) that uses a separate authentication device, which significantly increases the difficulty in accessing the network or password-protected secure areas within the network to those without the authentication device (Gewirtz 2011).
4. Save and examine computer and information network traffic patterns for anomalies such as unexpected data transmission or unknown reasons for lack of activity (Gewirtz 2011).

Many nonprofit organizations and some businesses rely on interns as a significant and productive part of their workforce. Despite their limited status, interns need to hold to the same status for IT policy as other employees. This is the standard for students in prestigious internships such as the US Congress. Congressional interns

are required to complete information security training if they have access to official networks or use the resources of the Congressional Research Service (Eckman 2019). The need for vigilance in this area is supported by research showing that employees such as contractors and temporary workers who may not have long-term associations with the organization have a higher propensity to disregard information-security rules and policies (Sharma and Warkentin 2019). Lockheed Martin has several policies in place that could be applied to the situation at many other organizations. These policies include network segmentation, which limits employee access to sensitive and proprietary information, and an annual internal audit of the cybersecurity program (Jaeger 2017). Lockheed Martin also holds training and security reviews to inform the workforce on the security procedures, internal monitoring, and audits performed by the company, with attendance recorded in case an employee's knowledge of the procedures becomes relevant to future employment or legal action (Jaeger 2017).

Economic Espionage

Economic espionage will be a persistent threat to organizations and businesses in the 21st century. The threat is particularly focused on the information industry, a sector that includes journalists, lawyers, human rights workers, think tanks, and those who value these groups' access to politicians and policymakers (Timberg

and Nakashima 2013). Hackers from China search for those who have influence in political and policy decision-making to understand how the US will view a developing issue (Timberg and Nakashima 2013). The information industry may also be targeted by Chinese hackers and other groups because they believe that institutions like think tanks and news organizations are government bodies, as they are in the PRC or other countries around the world (Timberg and Nakashima 2013).

Economic espionage is defined by 18 USC 1831 and 1832. Under both economic espionage statutes, the government must prove the following:

- that the defendant stole or, without authorization of the owner, obtained, destroyed, or conveyed information
- that the defendant knew that the information was proprietary
- that the information was actually a trade secret
- (in an act of economic espionage) that the defendant knew that the offense would benefit or was intended to benefit a foreign government, instrumentality, or agent (United States Department of Justice 2019a; hereafter, US DoJ)

The elements of economic espionage require an organization to take active steps to protect its information. To satisfy the second proof on the aforementioned list,

an organization must protect its valuable data as a trade secret and mark the information as proprietary, have security measures to protect the information, and have employees sign confidentiality agreements stating that the theft of protected and proprietary information is prohibited (US DoJ 2019a). The third proof, proving that the information was a trade secret, requires companies to take reasonable steps to keep the information secret and requires that the information has independent economic value (US DoJ 2019a).

Nonstate or private-sector economic espionage is addressed by 18 USC 1832. Under the fourth proof on the aforementioned list, the government must prove that the espionage was intended to benefit a person or entity other than the owner of the trade secret (US DoJ 2019b). Similarly, the government also needs to prove that the espionage would cause injury or disadvantage to the owner of the trade secret (US DoJ 2019b). The final element of 1832 that the government must prove is that the trade secret relates to or is included in a product produced for or placed in interstate or foreign commerce (US DoJ 2019b).

Conclusion

The cyber threats faced by governments, businesses, and policy institutes are vast, ranging from foreign-government organizations to terrorists and individual hackers to malicious insiders. Threats can evolve and morph over time, but the one constant is the need for organizations to understand the threat in order to

protect data, products, and themselves. During the Cold War, superpowers battled each other with proxies and in the figurative shadows of the world, in part for deniability, but also because it was effective in its time. While armies may not be facing each other in the field, conflicts between nation-states have been extended to the cyber realm for the same reasons as the Cold War—deniability and effectiveness. Nonstate actors such as the terrorists of old often used bombs to bring attention to their cause and attack their political or ideological enemies. Now, a terrorist group can use a cyberattack to target opponents, causing economic or political damage at critical times with great publicity, all from hundreds or thousands of miles away. In the past, espionage often involved the physical handling of documents—photographing or copying them and then exfiltrating them from the workplace. A malicious insider in the cyber realm can move documents numbering in the thousands with a few clicks of a mouse, possibly securely and without rousing any suspicion if the right security and IT protocols are not in place.

The types of measures required to prevent and defeat these modern cyber threats varies. One solution could be software designed to detect intrusion. Training designed to alert employees to cyber threats and to provide instruction on how to handle events such as unknown email attachments could prevent future phishing attacks. Screening employee backgrounds and reviewing work habits could help detect insider threats. The common thread to these and other means to secure an

organization's IT infrastructure is that all must be part of the strategy, which requires the organization to have information security measures in place that are enforceable, understood by employees, and able to be implemented by leadership.

SECTION III: PROTECT AND DETECT

Summary

Organizations are coming under increased attack from hostile cyber actors, both outside and inside their networks. The need for cybersecurity cannot be overemphasized, and there are many elements of network vulnerabilities that need to be considered when developing a cybersecurity policy or assessing an existing one. At a minimum, any security approach should incorporate the physical, technical, and social aspects of cyber-threat detection and prevention. There are many useful sources of information, lessons learned, and best practices that relate to the detection of cyberattacks and protective measures against such attacks. This portion of the literature review highlights several such sources, which can inform and guide an organization's cybersecurity policy.

Introduction

Detecting potential threats and protecting cyber infrastructure against such threats are critical elements of any public or private organization's cybersecurity program. Such threats can be either external or internal to the organization, and both types of threats can result in the catastrophic loss or destruction of sensitive or proprietary data. At the national level, PPD-8, National Preparedness, establishes cybersecurity as one of the core capabilities of the NPG. The mission of cybersecurity is to "protect (and, if needed, restore) electronic communications

systems, information, and services from damage, unauthorized use, and exploitation" (US DHS 2015, 9). EO 13010 (Critical Infrastructure Protection in 1996) and EO 13231 (Critical Infrastructure Protection in the Information Age in 2001) expand on this goal by establishing the need to protect cyber information or communications systems that control critical infrastructures systems from "electronic, radio-frequency, or computer-based attacks" (p. 37347 of 61 Fed. Reg. 138).

Public, governmental, and private organizations are witnessing their cyber systems become increasingly susceptible to a number of vulnerabilities ranging from system hacking to poor practices that leave company information exposed (Walters 2018). Srinivasan and Simna (2017) stated that several elements of cybersecurity include application (software and firmware) security, information security, and network and operational security.

Connecting to the internet poses significant potential risks to both organizational security and personal privacy if systems are not protected by safeguards such as the most up-to-date software patches, protective software such as antivirus programs and firewalls, strong passwords, and secure connections that restrict access to organizational computer systems (Massachusetts Institute of Technology 2019). Cyber threats, as well as the measures to protect against them, can be physical, technical, and/or social.

Literature Review

Physical Aspects of Cybersecurity Protection and Detection

Physical aspects are tangible; they can be held, touched, seen, and transported independent of the system with which they are used. Physical prevention measures include building security, dual-factor authentication (2FA), and password requirements. Physical threats can include damage or destruction of equipment, compromised passwords, and illegal circumventing of 2FA measures.

Buildings, Automation Systems, and Access Control

Cyber threats to an organization's physical campus or building include unauthorized access, destruction, disclosure, and denial of services. According to Goldstein and Wilshusen (2014) for the Government Accountability Office (GAO), the number of cyber incidents reported to DHS involving industrial control systems (including building and access control systems) increased 74% between fiscal years 2011 and 2014. Thanks to the IoT, modern businesses and organizations have significantly more modes of entry into internal computer systems that can be exploited by a malicious cyber actor. As an example, "in 2013, the retailer Target experienced a breach in its payment card data, which the company believes occurred after intruders obtained a heating, air conditioning, and ventilation system vendor's credentials to access the outermost portion of its network" (Goldstein and Wilshusen, 14). In another incident in 2009, "a security

guard at a Dallas-area hospital loaded a malicious program onto the hospital's computers, one of which controlled the heating, air conditioning, and ventilation control system for two floors, which, according to court records, could have affected patients' medications and treatments" (Goldstein and Wilshusen 2014, 15).

The GAO report by Goldstein and Wilshusen (2014) identified several potential consequences of cyberattacks on building systems, including but not limited to allowing unauthorized access to facilities, damage to temperature-sensitive equipment such as servers and data centers, causing fire alarms or sprinkler systems to activate inappropriately (or conversely, fail to activate in an emergency), disabling facilities by lack of power or environmental services, and providing back-door access to information systems.

Password-Based Authentication

Most organizations rely on username- and password-based authentication to control access to computer networks, a function known as single-factor authentication (1FA). Organizations often rely solely on 1FA controls because they are easy to establish and maintain and are very low-cost. However, recent cyberattacks have exposed the vulnerabilities inherent in 1FA systems. An inherent limitation of these password-only mechanisms is that the server has to

store a sensitive verifier table that contains the passwords of all the registered users.

Even if passwords are properly stored in salted hash, once the authentication server is compromised, an overwhelming fraction of users' passwords will be exposed for two reasons: "1) Human memory is inherently limited and unstable, and the distribution of user-chosen passwords are highly skewed; and 2) Password cracking hardware (e.g., GPUs [graphics processing units]) and algorithms (e.g., Markov-Chain-based) are constantly being improved" (Wang and Wang 2016). Even the most complex username and password requirement protocols are necessarily limited by the fact that the password has to be stored *somewhere*, leaving it vulnerable to being compromised.

> These days it is no news to hear that millions of user accounts are breached in an on-line hacking incident. Some quite recent password data breaches include Adobe (150 million), Evernote (50 million), Anthem (40 million), Rockyou (32 million), Tianya (30 million), Dodonew (16 million), 000webhost (15 million), Gmail (4.9 million), and Phpbb (255 K), just to name a few. Some services (e.g., Anthem and Phpbb) even have been breached more than once during the last five years. What makes things worse is that users tend to reuse the same password (or slight variations) to access multiple servers, a compromise of one server will

lead to the failure of all other servers, which is described as the "domino effect" of password re-use. (Wang and Wang 2016)

Two-Factor and Multifactor Authentication

To overcome the weaknesses of 1FA, many organizations such as universities, hospitals, and financial institutions are moving to 2FA or even MFA, whereby a user must know a password (1FA), possess a token (such as a smart card or mobile device), and/or have the right biometrics (such as fingerprint matching or facial recognition). Newer, more advanced authentication methods are continually being developed with artificial intelligence technology, allowing even greater security. "Google is considering using machine learning to take factors like users' online behaviors and routines into account for authentication, and banks are looking at behavioral biometrics like how individuals use a mouse in order to determine the identity of the user" (Pomputius 2019).

2FA and MFA processes are rapidly becoming the standard by which organizations authenticate end users who access their systems. "While two-factor authentication for digital devices and software is not an old concept, the increasing prevalence of multi-level authentication at large institutions like health care systems and universities shows that the technology is not going to disappear any time soon. Although 2FA is not the final solution for cybersecurity, it is more secure than passwords alone" (Pomputius 2019.

Technical Aspects of Cybersecurity Protection and Detection

The technical elements of an organization's cyber-network system include everything that is programmed into, attached to, or used externally with that system—from software programs and hardware to physical and virtual networks with their nodes to personal devices. All of these system elements have their own unique set of vulnerabilities that need to be mitigated for and protected against to prevent unauthorized access, damage, or, at worst, use as conduits for malicious activity by internal or external attackers. IBM describes a cyber network as an infrastructure through which information flows through nodes that follow protocols or rules that are programmed into them as they transmit or receive packets of data (IBM 2010). The physical elements of a network include servers, hard drives, mainframe computers, routers, switches, bridges, and hubs (IBM 2010).

Software Programs and Hardware

Antivirus and antimalware programs (software) are the means by which computers detect and provide protection against most cyber threats. In a recent article, Rubenking (2019) pointed out that Kaspersky and McAfee are some of the best antivirus programs, whereas Sophos and Malwarebytes are very effective antimalware programs. Many of these software programs perform both antivirus and antimalware functions and can also protect systems and networks against

spyware and adware intrusions. To help facilitate the decision-making process on which software programs to select, Nurhayati, Gautama, and Naseer (2018) conducted a basic analysis of protective software. They grouped 16 variables related to software capabilities into five factors to provide the most optimal program to choose:

- Security: antispyware, internet security, antitrojan, antiworm, antispam, and virus detection
- Performance: loading speed, ease of use, memory use, scanning speed, and accuracy
- Internal: price, data, and user identity protection
- Time: program installation time
- Capacity: amount of space required on hard disk and ability to detect viruses before download (Nurhayati, Gautama, and Naseer 2018).

The decision on which programs to use belongs ultimately to the organization. Although there is no one-size-fits-all program, the organization must decide what software to use that addresses its security concerns. The factors developed by Nurhayati, Guatama, and Naseer (2018) provide organizations with a possible starting point to help them to make a more informed decision on which network protection software to procure.

Firewalls are another critical element of a computer system's or network's security that block unauthorized access to an organization's computer system or network while still allowing users to communicate externally. Kaplesh and Goel (2019) highlighted that firewalls can be configured to prevent employees from transmitting sensitive information outside the system, lock out specific websites, and prevent access by computers outside the network. Some software programs even include firewall capabilities that provide an additional layer of security in concert with antivirus and antimalware elements. Most operating system software programs such as Windows include their own antivirus programs and firewalls specifically designed to work with other related software.

If operating systems are not updated routinely, any software protective measures used will lose their effectiveness. Additionally, because system management programs phased out by their manufacturers cease receiving critical updates, they become more vulnerable to malicious cyberattacks. A survey conducted by Spiceworks (2019) found that 79% of businesses surveyed continue to use some version of Windows 7, which will cease being supported by Microsoft in 2020, and 32% are still using Windows XP, an operating system that has not received any critical updates since 2014.

System hardware measures include biometric devices such as fingerprint readers and facial recognition scanners, encrypted USB drives, external hard drives,

secure workstations, and hardware security modules (HSMs) such as Common Access Cards. While biometric devices and software are very effective cybersecurity tools, Rebner (2019) pointed out that they should be just one part of a multilayered security protocol that also incorporates behavioral analysis to confirm legitimate system users or spot imposters. Rebner (2019) emphasized that such measures are passive in nature and do not require the system user to take any additional steps. Systems that incorporate biometric analysis learn from legitimate users by analyzing their behaviors and physiological markers and are able to more readily spot an attacker trying to mimic authorized users (Rebner 2019). Many organizations and government agencies are requiring their employees to use only agency-approved devices like encrypted USB drives and portable hard drives when uploading or downloading data on agency networks. Secure workstations are used with larger network systems with multiple servers and thousands of authorized users who are granted varying levels of administrative access.

HSMs are external security devices that generate, store, and protect cryptographic keys used to access the network and can provide another layer of network security (IBM 2018). Microsoft's (2015) TechNet wiki describes an HSM as an external standalone device that connects to a server and performs cryptographic authentication functions such as random number generation, key generation, digital signatures, and key archiving and recovery. HSMs also help speed up

cryptographic and authentication processes, thereby reducing the load on servers and administrators (Microsoft 2015).

Physical and Virtual Networks

Networks are composed of computers, mainframes, servers and peripherals connected together to allow for the transfer of data. The increasing use of cloud servers has opened an entirely new area for data storage and more effective network management—also serving as a potential gold mine for hackers if these servers are not protected adequately. With their own servers and storage, physical networks are the most commonly used. Virtual networks are becoming more popular, particularly with small organizations or businesses that cannot afford to build their own networks.

Network firmware and hardware such as nodes, routers, chipsets, and hubs are potential weak points in any information system because they serve as the primary means through which information is routed into, out of, and through the network, and many of these nodes are often wireless. These nodes are also vulnerable to attack from within through preprogrammed chipsets or malicious USB drives. These could be used to manipulate the system with exploits such as back doors and trojans that are built into or programmed onto the hardware components. Most software programs only target threats coming from outside into the network and, thus, are unable to detect malware present on hardware that is introduced to

the network from within (Alves and Morris 2018). Using secure hardware from trusted sources can help protect system hardware against attack and reduce the risk that outside devices, such as USB drives connected directly to the network, can be used to introduce malicious programs.

Kaur, Gill, and Dhaliwal (2016) warned that network nodes are particularly susceptible to attack from internal or external sources and can constitute one or more of the following:

- Black hole attacks force a node to discard all packets instead of forwarding
- Gray hole attacks discard some packets and forward others specified by attacker
- Sinkhole attacks force compromised nodes to accept all traffic from a source designated by the attacker but mask this traffic to appear like legitimate node activity
- Wormhole attacks occur when data packets are essentially drilled through the network to another spot through a low-latency link; such attacks could also include malicious programs
- Message tampering involves incoming messages being changed before they are forwarded to other nodes (Kaur, Gill, and Dhaliwal 2016).

To prevent internal and external attacks, Kaur, Gill, and Dhaliwal (2016) recommended that network nodes be programmed with trust-based routing features that enable them to assess whether the candidate router is trustworthy or not and then decide whether it is safe to transmit packets to or from the routers. Donovan (2017) advised that network administrators monitor user activity on their systems to both prevent the loss of sensitive data and detect potential insider threats.

Washenko (2019) discussed Microsoft's recent announcement of a new cloud storage called Personal Vault that will be available soon to its OneDrive cloud users. This virtual storage method requires some form of 2FA such as fingerprint matching and/or facial recognition.

Rao, Kurariya, and Akuli (2015) suggested that networks should be mapped to determine where their vulnerabilities are so that an effective security program can be established that will address and remediate those vulnerabilities. Rao, Kurariya, and Akuli (2015) stated that network infrastructures should be clearly defined with equipment model specifications, location, firewall configuration, routers, switches, ports, and wireless access points. Rao, Kurariya, and Akuli (2015) suggested several measures to protect networks, including regular updating of cyber-network software and firmware, physically securing network nodes, and extensive use of encrypting all network processes that carry sensitive data.

Personal Devices

Hackers are constantly testing organizations' servers and seeking ways to circumvent prohibition of personal devices and system safeguards. For example, the Texas Association of Counties (TAC) (2019) sent out a notice recently to counties throughout Texas alerting them to just such an attempt; counties have reported receiving USB drives through the mail to county offices with TAC labels on them. The notice from TAC warned counties not to use these USB drives as they were not sent by TAC and very likely have some form of malicious programming loaded on them (Texas Association of Counties 2019).

Personal devices, when connected to organizational systems, can create vulnerabilities for such systems and can be used by hostile actors to download sensitive data or upload malicious programs on networks. The most effective way for organizations to protect their systems is to prohibit the use of any personal devices in the workplace. Such measures are not always practical or enforceable, so putting strong encryption protocols on the system itself can prevent any unauthorized uploading or downloading. Personal devices include cellular phones, laptops and tablets, USB drives, and external portable hard drives. Cellular phones have evolved from simple flip phones with few capabilities and very little memory to virtual minicomputers that can copy and produce documents, access the internet, upload and download files and produce high-quality photographs and

videos and transmit them over the internet instantly. Laptop (portable) computers are very powerful and versatile devices that can possess the computing and storage capacity to copy entire networks in minutes. Tablets such as the iPad and Microsoft Surface Go and Surface Pro are essentially smaller portable computers that can be folded and hidden in a book or even a jacket pocket. USB drives are small enough to be easily hidden or carried on a key chain but can be used to either download sensitive files in seconds or upload malicious software like trojans or viruses. Portable hard drives function like a USB drive but can hold far more data, up to 4 terabytes.

Social Aspects of Cybersecurity Protection and Detection

The protection and detection functions of the NIST (2018) Framework for Improving Critical Infrastructure Cybersecurity contain social elements that must be addressed by an organization to ensure cybersecurity and business continuity. These elements include awareness, training, information protection processes, and continuous security monitoring, with the following elements outlined in the framework:

- All users are informed and trained
- Privileged users understand their roles and responsibilities
- Third-party stakeholders (e.g., suppliers, customers, and partners) understand their roles and responsibilities

- Senior executives understand their roles and responsibilities
- Physical and cybersecurity personnel understand their roles and responsibilities
- Protection processes are improved
- Response plans (incident response and business continuity) and recovery plans (incident recovery and disaster recovery) are in place and managed
- Response and recovery plans are tested
- Cybersecurity is included in human resource practices (e.g., deprovisioning, personnel screening)
- A vulnerability management plan is developed and implemented
- Personnel activity is monitored to detect potential cybersecurity events (NIST 2018)

Within these elements are subcategories that focus on enhancing cybersecurity resiliency through established standards with input from government, business professionals, cybersecurity experts, and academia, as well as the relevant categories from the Framework for Improving Critical Infrastructure Cybersecurity (where applicable) (NIST 2018).

Awareness and Training

A recent study looked at the human factor as a security threat to critical infrastructure. In the study, social engineering was identified as a growing threat,

including for organizations that offer critical and emergency services (Ghafir *et al.* 2018). To combat this, organizations must ensure that all employees are aware and trained on trending cybersecurity threats (NIST 2018). Employees who are well trained and knowledgeable regarding current cybersecurity risks are more likely to remain vigilant. Awareness mitigates vulnerabilities and further ensures organizational resiliency.

Through awareness and training, employees should understand their specific roles as related to the security of the organization's IT infrastructure (NIST 2018). "Many employees simply do not know their role in helping to keep their organization secure and the impact they can have, both positive and negative" (Fox 2018, para. 3). An organization's resiliency is directly related to the human tendency of naiveté. As employees engage with more new clients, the organization increases its risk of falling victim to social engineering. "Social engineering is defined as a method that seeks to exploit a weakness in human nature and take advantage of the naivety of the average person" (Aldawood and Skinner 2019, 1). Humans' natural tendency to trust others creates a substantial challenge to social engineering awareness programs. Social engineering is nothing new, but it can be mitigated within an organization through appropriate training and awareness programs.

To efficiently counter social engineering threats, organizational information systems require the integration of technology and managerial efforts to increase and improve employee awareness. Ineffective or inadequate training and awareness campaigns can be a waste of organizational resources. “The limitation to prevent socially engineered attacks through training and awareness programs occurs in the process of social communication” (Aldawood and Skinner 2019, 3). “Social engineers employ a variety of tactics to trap their targets into performing actions of their choice” (Ghafir *et al.* 2018, 4989). Such tactics include psychological manipulation, obedience to authority, and exploiting naiveté.

An organization is also obligated to increase the awareness of its clients and customers on cybersecurity risks, especially through social engineering (NIST 2018). As Aldawood and Skinner (2019) noted, “hackers leverage the confirmation prejudice and exploit intellectual dissonance to target like-minded groups and influence specific groups of people to outdo training and awareness programs of personnel” (3). A hacker may utilize these business relationships to their advantage, especially if they are able to obtain information that would embarrass the targeted organization. Encouraging employees to help the organization remain competitive in the industry may open opportunities to fall for a social engineering trap. Competition requires social interaction with customers and clients for the organization to be successful and achieve its goals. Ironically,

such relationships may lead to informal communication, which further places employees at risk of falling victim to social engineering threats and attacks.

Information Protection Processes

Employees should not be solely accountable for cybersecurity awareness (NIST 2018). Organizational leadership for promoting cybersecurity requires strategic vision, passion for coordination, and courage to drive culture (Chabinsky 2013). Chief executives should be the drivers of cybersecurity change to effectively change the mindset of an entire organization. “Developing mature business processes requires support from the top down” (Phillips & Tanner 2019). Heightening the levels of cybersecurity vigilance and protection from social engineering requires effort from all levels of employees within a workplace environment. “Business environmental factors include interactive work locations of an employee within a firm as well as outside areas” (Aldawood and Skinner 2019, 3). Locations that are frequently utilized by employees should be monitored and guarded from unauthorized persons. Visitors should always check in with the front desk personnel of the organization and be escorted if moving within the facility. “The internal environment of an organization is comprised of the firm-specific limitations to the extent that training and awareness programs will be helpful in controlling socially engineered attacks within the enterprise” (Aldawood and Skinner 2019, 4). If a visitor or stranger is observed wandering

the facility, every employee should recognize the risk of a social engineering threat and follow the proper protocols to resecure the organization.

Cybersecurity training should always be improved to facilitate the transfer and application of learning for employees (NIST 2018). “Currently, delivery of security awareness [programs] is mainly through two broad modes, namely computer-based training and instructor-led training” (Ghafir *et al.* 2018, 4981). Social engineering defense training should be a blend of both styles to make the greatest impact to improving the cybersecurity culture within an organization. Aldawood and Skinner (2019) confirmed through their research that the impact of training and awareness programs on employees is greatly enhanced when the content is interactive and compelling (Aldawood and Skinner 2019). Training and awareness programs are known to improve organizational resiliency.

Cybersecurity response plans should be in writing and understood by all employees (NIST 2018). Schute (2018) recommended that organizations seeking successful cybersecurity training must explain the dangers, select a security officer, keep training short and stimulating, and reduce internal risks. By understanding how a breach may impact the organization, employees are more likely to stay alert. “A 2016 study reported that organizations that include cyber security within their Business Continuity Management plans can significantly reduce the average time to address a data breach and have the infrastructure and

procedures to minimize the risk of a similar incident in the future" (Krishan 2018). Having a plan in place helps define the expectations of each employee on how to respond in the event of an incident. "Business continuity plans contribute to reducing organization consequences and enhancing an organization's ability to continue essential operations after an incident" (Fisher, Norman, and Klett 2017). Without a business continuity plan, organizations place themselves at risk of ineffective or delayed response to a critical incident, such as a data breach.

Cybersecurity response plans should be tested to ensure the transfer and application of awareness training. "Within an organization, cyber security and incident response strategies are designed to mitigate the impact of a cyber incident" (Phillips and Tanner 2019). It is never good when an organization's first run through a response plan is during an actual disaster. Response exercises help organizations act quicker and more confidently when a disaster does strike. "It is imperative that organizations develop coordinated business continuity and incident response plans to prepare for the rise of malicious threats" (Phillips and Tanner 2019). Coordination during response activities is critical to ensure that all facets of an organization are carrying out their respective tasks during a disaster to maximize risk mitigation.

Along with response plans, human resource development should maintain consistent and frequent training with cybersecurity awareness as a business

practice to reduce organizational liability through personnel (NIST 2018). "Cyber-awareness may be ingrained in your IT team, but it is not something the average employee is usually focused on. However, an employee's online behavior directly impacts their employer's business" (Fox 2018, para. 4). If an employee's personal accounts are hacked, information that may embarrass the employee and the organization may be released. Social networking, even on private and personal accounts, should always be used professionally because derogatory or inflammatory information may be brought to light that could be detrimental to the organization.

Cybersecurity plans should contain frequent threat assessment and vulnerability management plans to diminish an organization's known weaknesses (NIST 2018). "The goal is to allow leaders to identify and prioritize risk, so resources can be efficiently distributed to meet organizational objectives. Risk tolerance and resource allocation are the responsibility of each organization so the use of internal and external expertise can be critical in making wise decisions" (Miller and Griffy-Brown 2018). Organizational executives need to decide what risks they are willing to tolerate. Social engineering is one of the easiest ways to infiltrate an organization's network and should be placed in high regard for the vitality of the organization. Failure to do so places the company at greater risk of a data breach.

Continuous Security Monitoring

As part of the detect function of the Framework for Improving Critical Infrastructure Cybersecurity, organizations should monitor personnel activity to ensure continued compliance of cybersecurity policies (NIST 2018). Fox (2018) recommended developing engaging training content, testing and measuring compliance through phishing simulations, and reporting results to stakeholders and key business decision-makers. Carrying out cybersecurity audits is the best way to ensure that employees are following sound awareness practices for the organization. As an organization, it is vital to consider user education and security awareness training. This allows the organization to test the employee's alertness to cybersecurity and the training's effectiveness at decreasing user mistakes over time.

Conclusion

Various methods of cyber-threat protection must be employed by organizations to increase the chance of resiliency. Organizations should not rely on just one form of cybersecurity. All three measures of physical, social, and technical security should be leveraged. Vulnerabilities in any of these three areas will be exploited by bad actors. Physical security measures cover site security and controlled access to cyber assets, even personal devices, within an organization. Technical security measures ensure that software is up-to-date, firewalls are being used, and users

have strong passwords to maintain the privacy of the organization's data. Social security measures consist of training and awareness programs to maintain vigilance with cyber safety and preventing accidental breaches of cybersecurity. Poor performance in any of these three areas leaves organizations vulnerable for exploitation from bad actors. Without policies in place to detect potential threats, whether internal or external, organizations will remain unnecessarily vulnerable, thus placing their employees, their clients, and their own reputation at risk.

SECTION IV: RESPOND AND RECOVER

Summary

This section of the paper covers what methods should be employed when an organization is attacked via the cyber world. In this day and age, an organization cannot operate without utilizing the internet to run necessary functions. An example of this is executive leadership utilizing email to communicate with staff members on a daily basis. Emails can be and often are the main form of communication between executive leadership and staff members. Cyber hackers know this and are ready exploit vulnerable employees who are not following organization procedures when operating on their organization-issued laptop or desktop. With that said, it is not a matter of *if*, but *when* an organization will be attacked through the internet. In order for an organization to minimize the damage caused by a cyberattack, the organization needs to be prepared to detect, respond to, and then recover from the attack. This section also covers steps for an organization to take in order to minimize the fallout with stakeholders that may occur as a result of the cyberattack.

Introduction

The NIST Framework for Improving Critical Infrastructure Cybersecurity is an excellent guiding document for utilization in planning the various stages of preparing for, detecting, responding to, and recovering from a cyberattack.

According to McAfee Vice President of Threat Research Dmitri Aleprovitch, "of the world's biggest firms, there are just two kinds: those that know they have been compromised, and those that still have not realized they have been compromised" (Bright 2011, para. 8). This quote can be expanded beyond businesses to think tanks and universities. Multiple think tanks in the US and across the world have reported cyberattacks by state-sponsored agencies, largely attributed to China (McKenzie and Grigg 2018). Taking these facts into consideration, it is prudent that any organization or business should prepare to respond to a successful cyberattack.

Literature Review

The Cybersecurity Strategy and Implementation Plan (CSIP), as outlined in a 2015 memorandum from the Executive Office of the President Office of Management and Budget to the heads of executive departments and agencies (M-16-04), defines *recovery* as "the development and implementation of plans, processes, and procedures for recovery and full restoration, in a timely manner, of any capabilities or services that are impaired due to a cyber event" (from p. 17 of M-16-04). The NIST Guide for Cybersecurity Event Recovery defines an *event* as "any observable occurrence in a system or network," while an *incident* is defined as a violation of policies and best practices (Bartock *et al.* 2016, 1). For this

section, both terms refer to an occurrence that results in the successful compromise of one or more information systems.

The aftermath of a cyberattack can be lengthy and painful. While analysis of the initial damage is a crucial step in the response stages, keeping an open line of communication with company personnel and stakeholders is critical for both reputation management and business recovery. According to the Ponemon Institute's most recent study on the cost of cybercrime, "globally, the average cost of dealing with each cyber incident is approximately $9.5 million. In the U.S., this is inflated by a whopping $17.36 million per incident, and in the U.K., it rose by 14% in 2016 to $7.21 million" (Hawkins 2018, 12). Research for this study determined that the real cost of a cyberattack is related directly to the length of the recovery process. As the recovery progresses, the price continues to escalate. This finding puts into focus the importance of speed when it comes to recovery. The Ponemon Institute's research data showed that the average cost of a cyberattack falls from $9.5 million to $7.7 million if recovery is attained within 30 days. However, the average cost rises to $12.2 million if recovery takes longer than 90 days (Hawkins 2018).

Many organizations are placing greater emphasis on detection and response for cyberattacks. This emphasis has also created a greater awareness of the responsibility for planning for business recovery. Because it is not a matter of *if* a

cyber event will occur, but *when*, IT has become such a vital part of providing core business capabilities, making it is imperative for a plan to be in place to resume normal operations in a secure and timely fashion when cyber events occur.

Recovery involves both assets and people. It is imperative for an organization to prioritize its people, the organization's process, and technology assets based on their relative importance. This prioritization is important because not all assets have the same potential impact on the organization if they become unavailable or experience degraded capability. The prioritization step is critical given the cost of protection; the highest priority should be placed on assets that must be recovered to support the mission (Bartock *et al.* 2016). As mentioned earlier, the identity function of the NIST Framework for Improving Critical Infrastructure Cybersecurity suggests that the organization identify the critical systems that must be recovered first as part of the response activity. This identification determines the assets and the security dependencies that will be in the recovery guidance and playbook (Bartock *et al.* 2016).

NIST refers to recovery as one part of the risk management process lifecycle. The recovery process can be broken down into two phases focused on separate tactical and strategic outcomes. The initial period of tactical recovery involves the execution of the previously discussed recovery playbook that should be in place

before a cyber event. The second phase, which is more strategic, focuses on the continuous planning and improvement functions designed to decrease the likelihood and impact of future incidents. This strategy is based on the lessons learned from the current event and other methods learned from similar organizations (Bartock *et al.* 2016).

To help with the recovery plan process, NIST developed a list of topics for a typical plan:

- Service-level agreements—Pre-established external engagement contract support that can assist and augment the organization's recovery team in the event of a significant cyber event
- Authority—Documented name and point-of-contact information for two or more management staff members who may activate the plan
- Recovery team membership—Contact information for team members who have reviewed, trained, and exercised for implementation of the plan
- Specific recovery details and procedures—Specific recovery activities to be performed by the recovery team, including methods to provide for alternate means of processing
- Out-of-band communications—A method to communicate with critical personnel and assets, including external parties like incident response and recovery teams, when existing systems are down or inaccessible

- Communication plan—Any specific notification or escalation procedures that apply to the incident; these may involve some outside of the organization, such as legal, public relations, and human resources personnel who could be needed to manage expectations and information disclosure about the incident and recovery progress
- Offsite storage details—Information regarding the storage of specific records or media at an offline or offsite location; incidents involving the threat of ransomware are of particular interest for this section
- Operational workarounds—Predetermined procedures designed as a workaround if the information system is not able to be restored within the desired recovery time
- Facility recovery details—Information relevant to the recovery process of a physical facility such as an office location or a data center
- Infrastructure, hardware, and software—Details regarding access to the infrastructure, hardware, and software during the recovery process (Bartock *et al.* 2016)

Deciding when to start the recovery process can be difficult for an organization. Essential personnel must agree on the timing because it can be critically important to achieving a successful recovery. For example, "starting recovery before the investigation response has achieved key understandings of the adversary's

footprint and objectives may alert the adversary that an infiltration has been discovered, triggering a change in tactics that would defeat the recovery operation" (Bartock *et al.* 2016, 10). This change in tactic could make it challenging to discover which systems have been impacted.

Proper timing for recovery requires a coordinated response to achieve a balance between effective investigation and business restoration. This balance comes from a decision that weighs the need to identify the root cause versus the need to quickly regain operational readiness. The organization should have in place a method to define the conditions under which the recovery plan is to be initiated, assign the authority to begin the process, and a notification method for predetermined recovery personnel to be called in.

Recovery does not always mean a return to normal operations. The immediate need may not be complete restoration. In the early stages of recovery, "resilience might mean that a given resource is able to continue operation in a diminished capacity, such as during a DoS [denial-of-service] attack or a destructive attack on a group of systems" (Bartock *et al.* 2016, 10). Limiting damage to the reputation of an organization and its stakeholders is of utmost importance. The designated recovery teams may be able to learn from internal resources or from other similar organizations that have in place methods for adapting to the incident. The method could include a partial restoration as an interim measure. NIST points out that, in

situations involving a cyberattack, recovery may have many levels, and while regaining operational readiness is the goal, occasionally it may be best to take a step backward before moving forward, such as taking a key system offline to perform recovery measures before conducting recovery actions on other systems (Bartock *et al.* 2016).

The NIST Framework for Improving Critical Infrastructure Cybersecurity provides five categories for recovery: response planning, communications, analysis, mitigation, and improvements. Each of these categories is then broken into subcategories with guiding documents for resourcing and planning provided by NIST. Response planning is ensuring that the planned process and procedures are current and updated to enable execution during a detected cybersecurity incident. A benefit of constant planning is that it enables the organization to explore "what if" scenarios, which could be based on recent cyber events that have happened at similar organizations. This planning allows the organization the opportunity to develop a customized playbook.

The playbook gives the organization the chance to evaluate potential scenarios in terms of potential impact, planned response activities, and the resulting recovery processes before an actual cyber event occurs. Working through such situations can help identify potential gaps in security that should be addressed before a crisis, which could reduce the impact of an event on the organization. According

to Bartock *et al.* (2016), "such scenarios also help to exercise both technical and non-technical aspects of recovery such as personnel considerations, legal concerns, and facility issues" (4).

The communications category works to ensure that the response of all parties, both internal and external, will be coordinated. This category is broken down into five actions: ensuring that personnel are informed of roles, the incident is reported as required, information is shared, coordination with stakeholders occurs, and information is shared externally to achieve broader situational awareness. As new and significant threats emerge, personnel should be made aware of any threats and should be informed of any environmental changes. Personnel can be made aware of new emerging threats through recurring training mandated by the organization (Dunkerley 2018).

Analysis is performed to ensure that an effective response-and-recovery process is occurring. There are five subcategories to analysis: investigating notifications of events, understanding the impact and reach of events, conducting forensics, categorizing the incident so that the selected and effective response is executed, and developing effective responses and mitigations for vulnerabilities identified by both internal and external sources (Huergo 2018).

The fourth category of response is mitigation, which is an effort to prevent the expansion of, minimize the impact from, and resolve the active event. Mitigation

is broken down into three actions: when an incident is contained and mitigated, when identified vulnerabilities are diminished, and when identified vulnerabilities are accepted and documented.

The last category for response is improvements. Improvements are the continual analysis of response activities and incorporating lessons learned from all phases of the NIST Framework for Improving Critical Infrastructure Cybersecurity. The improvements category consists of two actions; incorporating lessons learned and updating the plan and documentation (Huergo 2018).

One way to initiate improvement by employees is to conduct awareness training on a regular basis. A one-time, mandatory training session does little to improve employee awareness. Employees must be reminded periodically about current information security threats and acceptable behavior in various situations. Placement of posters on bulletin boards in high-traffic areas, such as cafeterias, elevators, and hallways, is one method to remind personnel of the importance and practice of information security (Kolb and Abdullah 2009). Mandated cybersecurity awareness training improves an organization's situational awareness, which lowers the likelihood of an attack against the organization.

NIST and its framework break down the response category into five critical functions and provide actions for an organization before, during, and after an incident. =NIST provides sources to assist developing and supporting each action

involved in an organization's comprehensive response plan. Sources include the Center for Internet Security (CIS), the Information Systems Audit and Control Association (ISACA), the International Society for Automation (ISA), and the International Organization for Standardization (IOS) working with the International Electrotechnical Commission (IEC). The CIS, ISACA, ISA, IOS, and IEC have each published various guiding documents to support a cyber-incident response.

Moving from a theoretical discussion of planning for response to an analysis of real-world responses, a framework of understanding must be built in order to comprehend the necessary response. First, it is critical to note that not all organizations that have been the subject of a cyber incident are aware of the attack. Second, not all organizations that are aware will announce that they have suffered an attack. This failure or hesitance to announce an incident can be under guidance from law enforcement or from fear of hurting stock prices or scaring off investors by an organization's board of directors. Third, the requirements for notification of an individual's stolen personally identifiable information are complex and varies across states and territories (Newman 2018).

The Securities and Exchange Commission (SEC) does have a reporting requirement, but it is rarely enforced (Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 17 CFR 229, 249). According to the

Privacy Rights Clearinghouse, almost 5,000 cyberattacks occurred between 2011 and 2017 (Newman 2018), while DHS has reported an average of 4,000 ransomware attacks daily (Dudley 2019). Meanwhile, SEC has only been notified by 106 companies during the same time period and only investigated a few tardy notifications resulting in zero enforcement actions (Newman 2018). For researchers, this means that the vast majority of incidents are conducted in private, leaving only a few high-profile cases available for study and analysis.

The critical first step is identification of a cyberattack. Unfortunately, as seen by the cyber incidents against Sony (Lee 2014) and the City of Baltimore (Stewart 2019), the first notification provided was when computers displayed ransom notes or other threats to a hacker-controlled internal network. Think tanks have been targeted including the Center for Strategic and International Studies (CSIS). Although CSIS admitted to being targeted and to the technique used, whether the attack was successful has not been announced, nor was how CSIS became aware of the fake websites (Sullivan 2019). Microsoft has also taken down fake websites targeting the US Senate, the Hudson Institute, and the International Republican Institute (O'Sullivan 2019).

Cyber actors have become all too sophisticated with the manner in which they attack. Unlike the attacks against Sony and the City of Baltimore, attacks can happen without any notification. Bad actors may hide their presence without any

trace of who they are or where they came from. It has become nearly impossible to determine if someone has been hacked simply by observing someone's cyber activity (Ruefle *et al.* 2014). The prevalence of cyber-attacks show the difficulty for preventatively identifying ongoing attacks, making the majority of responses reactive.

To add further difficulty to identifying an attack, most nonprofits have a heavy internet presence that connect the nonprofit with their stakeholders electronically. The electronic working relationship between the organization and the stakeholders leaves the organization and its stakeholders vulnerable to attack. As a result, a stakeholder's information may be compromised and accessible to bad actors, making it essential for employees to know and understand when or if they have been attacked (Ruefle *et al.* 2014).

Once an event has been identified, the next critical step is mitigating the negative impacts. Mitigation technique is largely dependent on the type of attack and against what type of computer system. In attacks against think tanks using fake websites to get login credentials, the organizations have used the judicial system to have Microsoft gain control of the fake websites (O'Sullivan 2019). In an attack against Maersk, to mitigate the spreading attack, the company's IT department took down the internal network to isolate the damage (Greenberg 2018). A recently developed approach for responding to ransomware attacks is the

process of hiring a third party to break the encryption (Dudley 2019) or by negotiating with the cyberattacker, sometimes using a cybersecurity insurance policy for funding (Sussman 2018) Unfortunately, good encryption is difficult to break, and the company hired to break the encryption may find it more cost-effective to negotiate, thus fueling future attacks.

An additional mitigation technique that assists in the recovery process is to isolate the incident immediately. Mitigation and segregation are needed to prevent the spread of malware to other buildings and installations not already affected. A hacker leaves a significant amount of malware on the system, including the first malware installed—a callback routine that automatically tries to reconnect to the attacked server if the system is disconnected or rebooted. Mitigation blocks the intruder and denies the opportunity to do further damage (Ayala 2016). This step can assist an organization with isolating any damage that may have transpired.

The last step in the NIST model for response is to continue making improvements. This requires that an organization keep abreast of historical and ongoing attacks of websites that could be mistaken for legitimate sites and of ongoing and developing social engineering techniques. In addition to maintaining situational awareness of attacks and nefarious activities, it is essential that organizations keep all systems up to date, reducing the threat of known exploitations, such as those that affected the City of Baltimore (Stewart 2019). In

order to help the community and society, it is necessary to announce ongoing and identified cyberattacks, thus enabling others to identify the technique and develop and implement effective countermeasures. Sharing attacks can assist with weakening the impact of future attacks.

History is an important aspect to combat further cyberattacks by developing an appropriate response and then conducting a thorough recovery. In order to assist organizations with cybersecurity response and recovery, it is essential to know the history of previous attacks so that organizations can avoid the mistakes of others during the response-and-recovery period. Over the past several decades, cybersecurity proponents have presented a shifting and sometimes ambiguous case for exactly what is being threatened and by whom. During the 1980s, the main threat was espionage via the exploitation of increasing use of computers and networks by the US. Then, in the 1990s, an attack against the US infrastructure proved concerning to the government. Immediately following the 9/11 attacks, the threat assessment shifted to nonstate terrorist attacks via cybersecurity. Recent policy documents identify a combination of state actors working directly or indirectly via nonstate proxies (e.g., patriotic hackers or organized crime) to target information in the form of private intellectual property and government secrets (Lawson 2011). An individual who views himself or herself as a patriot hacker should be concerning to any think tank. The political association of the think tank

should be considered irrelevant, given the fact that individuals associated with both political parties consider themselves patriots.

Conclusion

The number of cyberattacks has increased exponentially over the past decade, increasing the probability that any organization has been subjected to an attack, is currently under attack, or will be under attack soon. This likelihood places the need for a response that is planned, understood, and ready to be executed. An effective plan will continually be refined, address the changing nature of the threats, ensure that IT systems are properly maintained and secured, and create multiple adaptable mitigation strategies.

Research conducted on cybersecurity attacks has proven that most organizations will experience a cyberattack; it is not a question of *if* it will occur, but *when* it will happen. When it comes to recovery, it is critical for organizations to have a documented and exercised plan in place. This section provides some valuable suggestions for developing a plan that has been proven to work by organizations such as NIST. Protecting the reputation of the company and the privacy of its stakeholders should be a top priority of this plan. In 2019, most individuals understand that a cyberattack is imminent, but they will not fathom an organization unprepared to respond.

LITERATURE REVIEW CONCLUSION

The arena of cybersecurity and cyber threats is an ever-evolving area of study that goes back decades—ever since the first network of computers was developed and later exploited by hackers. This volume of information has to be looked at carefully when developing a strategy to combat the cyber threats faced by organizations in both the private and public sectors. The starting point for every organization is the core documents that have been created by the relevant government agencies and private-sector organizations. From these documents, the path is clear on how to build an organization's efforts to prevent and mitigate damages from what is considered an inevitable cyberattack. Organizations must be aware of the actual threats that they face from state actors, organized criminals, and individuals. Once the relevant threats have been identified, the organization must implement practices among their personnel and their technology to both protect their critical infrastructure and detect attacks that are in progress, recognizing that it is impossible to prevent all attacks. Therefore, it is important to have plans in place to both respond to a cyberattack and quickly recover from any successful attack to mitigate the damages that may be done to the organization. By analyzing the relevant literature on these core functions of cybersecurity, an effective cybersecurity plan can be developed for a wide variety of organizations.

BIBLIOGRAPHY

Abreu, José. 2012. "Mexican Drug Cartels and Cyberspace: Opportunity and Threat." *INFOSEC,* March 21. https://resources.infosecinstitute.com/mexican-cartels/#gref/.

Aldawood, Hussain, and Geoffrey Skinner. 2019. "Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues." *Future Internet* 11 (73): 1–16. doi: 10.3390/fi11030073.

Alves, Thiago, and Thomas Morris. 2018. "Hardware-based Cyber Threats." Proceedings of the 4th International Conference on Information Systems Security and Privacy: 259–266. doi: 10.5220/0006577202590266.

Ayala, Luis. 2016. Cyber-Physical Attack Recovery Procedures: A Step-by-Step Preparation and Response Guide. Berkeley, CA: Apress Media.

Bartock, Michael, Jeffrey Cichonski, Murugiah Souppaya, Matthew Smith, Greg Witte, and Karen Scarfone. 2016. *Guide for Cybersecurity Event Recovery,* special publication 800-184. Gaithersburg, MD: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf/.

Bernstein, Michael S., Andrés Monroy-Hernández, Drew Harry, Paul André, Katrina Panovich, and Greg Vargas. 2011. "4chan and /b/: An Analysis of Anonymity and Ephemerality in a Large Online Community." Paper presented at the Fifth International AAAI Conference on Weblogs and Social Media. Barcelona. https://www.aaai.org/ocs/index.php/ICWSM/ICWSM11/paper/view/2873/4398

Bright, Peter. 2011. "Operation Shady RAT: five-year hack attack hit 14 countries." *Ars Technica*, August 3, 4:10pm. https://arstechnica.com/information-technology/2011/08/operation-shady-rat-five-year-hack-attack-hit-14-countries/.

Buley, Taylor, and Andy Greenberg. 2010. "Google China Hackers' Unexpected Backdoor." *Forbes*, January 14, 6:50pm. https://www.forbes.com/2010/01/14/google-china-mcafee-technology-cio-network-hackers.html#3a0e91812903/.

Bunn, Matthew, and Scott D. Sagan. 2016. *Insider Threats*. Ithaca, NY: Cornell University Press.

Burt, Tom. 2019. "New steps to protect Europe from continued cyber threats." *EU Policy Blog* [blog], February 20. https://blogs.microsoft.com/eupolicy/2019/02/20/accountguard-expands-to-europe/.

Chabinsky, Steven. 2013. "The Top Three Cyber Security Leadership Qualities." *Security*, June 1. https://www.securitymagazine.com/articles/84377-the-top-three-cyber-security-leadership-qualities/.

Cheng, Dean. 2016. Cyber Dragon: Inside China's Information Warfare and Cyber Operations. Santa Barbara, CA: ABC-CLIO.

Cimpanu, Catalin. 2019. "Ancient ICEFOG APT malware spotted again in new wave of attacks." *ZDNet*, June 7, 8:30am. https://www.zdnet.com/article/ancient-icefog-apt-malware-spotted-again-in-new-wave-of-attacks/.

Coats, Daniel R. 2018. *Worldwide Threat Assessment of the US Intelligence Community*. Washington, DC: Office of the Director of National Intelligence. https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

Connelly, Eileen AJ. 2011. "Stratfor hacking victims targeted after comments." *The Washington Times*, December 26. https://www.washingtontimes.com/news/2011/dec/26/stratfor-hacking-victims-targeted-after-comments/

Cybersecurity and Infrastructure Security Agency. 2019. Ransomware. *Department of Homeland Security: CISA* [website]. https://www.us-cert.gov/ransomware.

Donovan, Kevin. 2017. "10 Cybersecurity Best Practices for IT, IS, Network & Data Security." *ObserveIT* [blog], April 25. https://www.observeit.com/blog/10-best-practices-cyber-security-2017/.

Dudley, Renee. 2019. "Sting catches ransomware firm negotiating with 'hackers.'" *Salon*, July 5, 12:00am.

https://www.salon.com/2019/07/04/sting-catches-another-ransomware-firm_partner/.

Dunkerley, Dawn. 2018. *CompTIA Security+: Exam Sy0 501,* 5th edition. New York, NY: McGraw-Hill Education.

Eckman, Sarah J. 2019. *Internships in Congressional Offices: Frequently Asked Questions,* report R44491. Washington, DC: Congressional Research Service. https://fas.org/sgp/crs/misc/R44491.pdf

Escobar, Sofia Liemann. 2019. "What could cyberterrorism look like? And is there such a thing?" *Medium,* January 23. https://medium.com/wonk-bridge/cyberterrorism-ff9285c32224/.

Falcone, Robert, and Bryan Lee. 2018. "Sofacy Continues Global Attacks And Wheels Out New 'Cannon' Trojan." *Unit 42,* November 20, 6:00am. https://unit42.paloaltonetworks.com/unit42-sofacy-continues-global-attacks-wheels-new-cannon-trojan/.

Federal Bureau of Investigation. 2019. *The Insider Threat: An introduction to detecting and deterring an insider spy*. Washington, DC: Federal Bureau of Investigation. https://www.dni.gov/files/NCSC/documents/products/Insider_Threat_Brochure.pdf/.

FireEye. 2019. "Advanced Persistent Threat Groups: Who's who of cyber threat actors." *FireEye* [website]. https://www.fireeye.com/current-threats/apt-groups.html.

Fisher, Ronald, Michael Norman, and Mary Klett. 2017. "Enhancing infrastructure resilience through business continuity planning." *Journal of Business Continuity & Emergency Planning* 11 (2): 163–173.

Fox, Dan. 2018. "Making Employees More Cyber-Aware." *Risk Management,* June 1, 6:04am. http://www.rmmagazine.com/2018/06/01/making-employees-more-cyber-aware/.

Fruhlinger, Josh. 2018. "What is corporate espionage? Inside the murky world of private spying." *CSO*, July 2, 3:28am. https://www.csoonline.com/article/3285726/what-is-corporate-espionage-inside-the-murky-world-of-private-spying.html/.

Gallagher, Sean. 2017. “Chinese hackers go after think tanks in wave of more surgical strikes.” *Ars Technica,* December 21, 4:45pm. https://arstechnica.com/information-technology/2017/12/chinese-hackers-go-after-think-tanks-in-wave-of-more-surgical-strikes/.

Gewirtz, David. 2011. “Beware: The Insider Cyber-Threat.” *The Journal of Counterterrorism & Homeland Security International* 17 (4): 8–9.

Ghafir, Ibrahim, Jibran Saleem, Mohammad Hammoudeh, Hanan Faour, Vaclav Prenosil, Sardar Jaf, Sohail Jabbar, and Thar Baker. 2018. “Security threats to critical infrastructure: the human factor.” *Journal of Supercomputing* 74 (10): 4986-5002. doi: 10.1007/s11227-018-2337-2.

Goldstein, Mark L., and Gregory C. Wilshusen. 2014. *Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems,* report GAO-15-6. Washington, DC: United States Government Accountability Office. https://www.gao.gov/assets/670/667512.pdf/.

Greenberg. Andy. 2018. “The Untold Story of NotPetya, the Most Devastating Cyberattack in History,” *Wired*, August 22, 5:00am. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Greitzer, Frank L., and Ryan E. Hohimer. 2011. “Modeling Human Behavior to Anticipate Insider Attacks.” *Journal of Strategic Security* 4 (2): 25–48. doi: 10.5038/1944-0472.4.2.2.

Hawkins, Nick. 2018. “Resistance, response and recovery.” *Computer Fraud & Security,* 2018 (2): 10–13. doi: 10.1016/S1361-3723(18)30014-9.

Homeland Security Digital Library. 2019. “Public Law 113-274: Cybersecurity Enhancement Act of 2014.” *Homeland Security Digital Library* [website]. https://www.hsdl.org/?abstract&did=765286/.

Hudson Institute. 2018. “Hudson Institute Statement on Russian Cyberattacks.” *Hudson Institute* [website]. https://www.hudson.org/research/14510-hudson-institute-statement-on-russian-cyberattacks/.

Huergo, Jennifer. 2018. “NIST Releases Version 1.1 of its Popular Cybersecurity Framework.” *NIST News*, April 16. https://www.nist.gov/news-

events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework/.

IBM. 2010. “What are the basic elements of a network?” *IBM Knowledge Center* [website]. https://www.ibm.com/support/knowledgecenter/zosbasics/com.ibm.zos.znetwork/znetwork_14.htm/.

IBM. 2018. “Hardware Security Module (HSM).” *IBM Knowledge Center* [website]. www.ibm.com/support/knowledgecenter/en/SS3JSW_5.2.0/com.ibm.help.security.doc/SI_HSM.html/.

Jaeger, Jaclyn. 2017. “Identifying inside threats to cyber-security.” *Compliance Week,* January 24, 2:45am. https://www.complianceweek.com/identifying-inside-threats-to-cyber-security/2793.article/.

Jaffee, Larry. 2017. “Always Connected Comes with Risks: What insider threats exist with use of BYOD mobile devices for work? Larry Jaffee explains how organizations can mitigate potential risks.” *SC Magazine* February: 20–23.

Kaplesh, Pooja, and Anjuli Goel. 2019. “Firewalls: A study on Techniques, Security and Threats.” *Pramana Research Journal* 9 (4): 312–323. https://www.pramanaresearch.org/gallery/prj-p690.pdf/.

Kaspersky. 2013. *The ‘ICEFOG’ APT: A Tale of Cloak and Three Daggers*. Woburn, MA: Kaspersky Lab Zao. https://media.kaspersky.com/en/icefog-apt-threat.pdf/.

Kaspersky. 2019. “What is Spear Phishing? – Definition.” *Kaspersky* [website]. https://usa.kaspersky.com/resource-center/definitions/spear-phishing/.

Kaur, Jugminder, Sandeep S. Gill, and Balwinder S. Dhaliwal. 2016. “Secure Trust Based Key Management Routing Framework for Wireless Sensor Networks.” *Journal of Engineering* 2016. doi: 10.1155/2016/2089714.

Kolb, Nancy, and Faisal Abdullah. 2009. “Developing an Information Security Awareness Program for a Non-Profit Organization.” *International Management Review* 5 (2): 103–107.

Kozy, Adam. 2017. "An End to ‘Smash-And-Grab’ and a Move to More Targeted Approaches.” *CrowdStrike* [blog], December 20.

https://www.crowdstrike.com/blog/an-end-to-smash-and-grab-more-targeted-approaches/.

Krishan, Robee. 2018. “Corporate Solutions to Minimize Expenses from Cyber Security Attacks in the United States.” *Journal of Internet Law* 21 (11): 16–19.

Lawson, Sean. 2011. *Beyond Cyber-Doom: Cyberattack Scenarios and the Evidence of History,* working paper no. 11-01. Arlington, VA: Mercatus Center. https://www.mercatus.org/system/files/beyond-cyber-doom-cyber-attack-scenarios-evidence-history_1.pdf/.

Lee, Timothy B. 2014. “The Sony hack: How it happened, who is responsible, and what we've learned.” *Vox*, December 17. https://www.vox.com/2014/12/14/7387945/sony-hack-explained/.

Mansfield-Devine, Steve. 2011. “Anonymous: serious threat or mere annoyance?” *Network Security* 2011 (1): 4–10. doi: 10.1016/S1353-4858(11)70004-6.

Massachusetts Institute of Technology. 2019. “Top 10 Safe Computing Tips.” *MIT Information Systems and Technology* [website]. https://ist.mit.edu/sites/default/files/u21/top10tips.pdf/.

McKenzie, Nick, and Angus Grigg. 2018. “‘Watering hole’ attacks: How China's hackers went after think tanks and universities.” *The Sydney Morning Herald,* December 3. https://www.smh.com.au/national/watering-hole-attacks-how-china-s-hackers-went-after-think-tanks-and-universities-20181203-p50jxj.html/.

McReynolds, Joe. 2015. “China’s Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy.” *China Brief* 15 (8). https://jamestown.org/program/chinas-evolving-perspectives-on-network-warfare-lessons-from-the-science-of-military-strategy/#.Vb7q6f9RHTg/.

Microsoft. 2015. “Hardware Security Module (HSM).” *Microsoft TechNet* [wiki]. https://social.technet.microsoft.com/wiki/contents/articles/10576.hardware-security-module-hsm.aspx/.

Miller, Howard, and Charla Griffy-Brown. 2018. “Developing a Framework and Methodology for Assessing Cyber Risk for Business Leaders.” *Journal of Applied Business and Economics* 20 (3): 34–50.

Momot, Ashton. 2018. “Introduction to NIST and the NIST Cybersecurity Framework.” *Twinstate Technologies Blog* [blog], February 7. https://blog.twinstate.com/introduction-to-nist-and-the-nist-cybersecurity-framework/.

Mueller, Robert S., III. 2019. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*. Washington, DC: United States Department of Justice. https://www.justice.gov/storage/report.pdf/.

National Institute of Standards and Technology. 2018. *Framework for Improving Critical Infrastructure Cybersecurity*. Gaithersburg, MD: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf/.

Newman, Craig A. 2018. “When to Report a Cyberattack? For Companies, That’s Still a Dilemma.” *The New York Times*, March 5. https://www.nytimes.com/2018/03/05/business/dealbook/sec-cybersecurity-guidance.html/.

Nurhayati, Ai, Aditya Gautama, and Muchammad Naseer. 2018. “Decision making model design for antivirus software selection using Factor Analysis and Analytical Hierarchy Process.” *MATEC Web of Conferences* 154. doi: 10.1051/matecconf/201815403006.

O’Brien, Brendan. 2018. “Russian hackers targeted US conservative think-tanks, says Microsoft.” *Public Radio International*, August 21, 7:45am. https://www.pri.org/stories/2018-08-21/russian-hackers-targeted-us-conservative-think-tanks-says-microsoft/.

O’Brien, Brendan, and Christopher Bing. 2018. “Russian hackers targeted U.S. Senate, think tanks: Microsoft.” *Reuters,* August 21, 1:21am. https://www.reuters.com/article/us-usa-russia-hackers/russian-hackers-targeted-u-s-conservative-think-tanks-says-microsoft-idUSKCN1L60I0/.

Olson, Parmy. 2012. We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency. Boston, MA: Little, Brown and Company.

O’Sullivan, Donie. 2019. “Russian group suspected in DNC hack targeted Washington think tank.” *CNN*, January 30, 8:13pm. https://www.cnn.com/2019/01/30/politics/fancy-bear-microsoft-csis-think-tank/index.html/.

Ottis, Rain. 2008. “Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective.” Proceedings of the 7th European Conference on Information Warfare and Security: 163–168. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf/.

Phillips, Rick, and Brandon Tanner. 2019. “Breaking down silos between business continuity and cyber security.” *Journal of Business Continuity & Emergency Planning* 12 (3): 224–232.

Pomputius, Ariel F. 2019. “A Review of Two-Factor Authentication: Suggested Security Effort Moves to Mandatory.” *Medical Reference Services Quarterly* 37 (4): 397–402. doi: 10.1080/02763869.2018.1514912.

Punithavathani, D. Shalini, K. Sujatha, and J. Mark Jain. 2015. “Surveillance of anomaly and misuse in critical networks to counter insider threats using computational intelligence.” *Cluster Computing* 18 (1): 435–451. doi: 10.1007/s10586-014-0403-y.

Rao, J. Durga Prasad, Satyendra Kurariya, and Ram Krishna Akuli. 2015. “A Brief Study on Measures to Improve Cyber Network Security.” *IJCA Proceedings on National Conference: Potential Research Avenues and Future Opportunities in Electrical and Instrumentation Engineering*: 20–22. https://research.ijcaonline.org/acewrm2015/number2/acewrm6031.pdf/.

Rebner, Susan. 2019. “Behavioral Biometrics Are Key for Cybersecurity.” *Inc.*, June 27. https://www.inc.com/young-entrepreneur-council/behavioral-biometrics-are-key-for-cybersecurity.html/.

Rouse, Margaret. 2015. “Definition: watering hole attack.” *SearchSecurity* [website], August. https://searchsecurity.techtarget.com/definition/watering-hole-attack/.

Rubenking, Neil J. 2019. “The Best Antivirus Protection for 2019.” *PC Magazine*, September 23, 10:11am. https://www.pcmag.com/roundup/256703/the-best-antivirus-protection/.

Ruefle, Robin, Audrey Dorofee, David Mundie, Allen D. Householder, Michael Murray, and Samuel J. Perl. 2014. “Computer Security Incident Response Team Development and Evolution.” *IEEE Security & Privacy* 12 (5): 16–26. doi: 10.1109/MSP.2014.89.

Schute, Debra A. 2018. “Four tips for successful cybersecurity training.” *Medical Economics* 95 (20): 34–35.

Sevastopulo, Demetri. 2007. “Chinese hacked into Pentagon.” *Financial Times*, September 3. https://www.ft.com/content/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac/.

Sharma, Shwadhin and Merrill Warkentin. 2019. “Do I really belong?: Impact of employment status on information security policy compliance.” *Computers & Security* 87. doi: 10.1016/j.cose.2018.09.005.

Shoorbajee, Zaid. 2018. “U.S. intelligence chief lays out threats to U.S. infrastructure, efforts to protect it.” *CyberScoop*, July 13. https://www.cyberscoop.com/dan-coats-hudson-institute/.

Sigholm, Johan. 2016. “Non-State Actors in Cyberspace Operations.” *Journal of Military Studies* 4 (1): 1–37. doi: 10.1515/jms-2016-0184.

Sorell, Tom. 2015. “Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous.” *Journal of Human Rights Practice* 7 (3): 391–410. doi: 10.1093/jhuman/huv012.

Spiceworks. 2019. *The Future of Network and Endpoint Security*. Austin, TX: Spiceworks. https://www.spiceworks.com/marketing/network-security/pdf-report/.

Srinivasan, J., and S. Simna. 2017. “Disaster Recovery, An Element Of Cyber Security - A Flick Through.” *International Journal of Management* 8 (4): 125–133. http://www.iaeme.com/MasterAdmin/UploadFolder/IJM_08_04_016/IJM_08_04_016.pdf/.

Stewart, Emily. 2019. “Hackers have been holding the city of Baltimore's computers hostage for 2 Weeks.” *Vox*, May 21, 5:50pm. https://www.vox.com/recode/2019/5/21/18634505/baltimore-ransom-robbinhood-mayor-jack-young-hackers/.

Sussman, Bruce. 2018. “Ransomware Paid: Organization Demands POC from Hackers.” *SecureWorld*, November 28, 9:50am. https://www.secureworldexpo.com/industry-news/ransomware-paid-hacker-negotiation/.

Symantec. 2016. *Internet Security Threat Report*, vol. 21. Mountain View, CA: Symantec Corporation. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf/.

Tamkin, Emily. 2017. "10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?" *Foreign Policy*, April 27, 8:30am. https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/.

Texas Association of Counties. 2019. "Warning: Dangerous USBs being Sent to Counties." *Texas Association of Counties* [website], August 2. https://tac.informz.net/informzdataservice/onlineversion/ind/bWFpbGluZ2luc3RhbmNlaWQ9ODcyMDkyMCZzdWJzY3JpYmVyaWQ9MTExMTExMzYxNw==/.

Thackray, Helen, and John McAlaney. 2018. "Groups Online: Hacktivism and Social Protest." In *Psychological and Behavioral Examinations in Cyber Security*, eds. John McAlaney, Lara A. Frumkin, and Vladlena Benson, 194–209. Hershey, PA: IGI Global.

Thompson, Cadie. 2015. "Drug traffickers are hacking US surveillance drones to get past border patrol." *Business Insider*, December 30, 8:34am. https://www.businessinsider.com/drug-traffickers-are-hacking-us-border-drones-2015-12/.

Timberg, Craig and Ellen Nakashima. 2013. "Has China hacked most of Washington?" *Waterloo Region Record*, February 21: B6.

Trumbull, Mark. 2011. "Intelligence firm Stratfor reels after data breach. What did hackers get?" *The Christian Science Monitor*, December 26. https://www.csmonitor.com/USA/2011/1226/Intelligence-firm-Stratfor-reels-after-data-breach.-What-did-hackers-get/.

Tzu, Sun. 2002. *The Art of War*. Mineola, NY: Dover Publications.

United States Department of Defense. 2018. Summary of the 2019 National Defense Strategy of The United States of America: Sharpening the American Military's Competitive Edge. Washington, DC: United States Department of Defense.

https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf/.

United States Department of Homeland Security. 2015. *National Preparedness Goal*, 2nd ed. Washington, DC: United States Department of Homeland Security. https://www.fema.gov/media-library-data/1443799615171-2aae90be55041740f97e8532fc680d40/National_Preparedness_Goal_2nd_Edition.pdf/.

United States Department of Homeland Security. 2016a. *Information Technology Sector-Specific Plan: An Annex to the NIPP 2013*. Washington, DC: United States Department of Homeland Security. https://www.dhs.gov/sites/default/files/publications/nipp-ssp-information-technology-2016-508.pdf/.

United States Department of Homeland Security. 2016b. *Protection Federal Interagency Operational Plan,* 1st ed. Washington, DC: United States Department of Homeland Security. https://www.fema.gov/media-library-data/1472581208497-42ba23c551f5a502c4f0eab69c3c741b/Protection_FIOP_1st_v3.pdf/.

United States Department of Homeland Security. 2019. "National Preparedness Goal." *Homeland Security* [website], October 2. https://www.dhs.gov/national-preparedness-goal/.

United States Department of Justice. 2019a. "Elements of the Offense Under 18 U.S.C. § 1831." In *Criminal Resource Manual*, 1124–1128. Washington, DC: United States Department of Justice. https://www.justice.gov/jm/criminal-resource-manual-1124-elements-offense-under-18-usc-1831/.

United States Department of Justice. 2019b. "Elements of the Offense Under 18 U.S.C. § 1832." In *Criminal Resource Manual*, 1129–1135. Washington, DC: United States Department of Justice. https://www.justice.gov/jm/criminal-resource-manual-1129-elements-offense-under-18-usc-1832/.

von Clausewitz, Carl. 1918. *On War*. London, UK: Kegan Paul, Trench, Trubner & Co.

Walters, Riley. 2018. "Private Sector Cyber Incidents in 2017." *The Heritage Foundation*, January

3. https://www.heritage.org/cybersecurity/report/private-sector-cyber-incidents-2017/.

Wang, Ding, and Ping Wang. 2016. “Two Birds with One Stone: Two-Factor Authentication with Security Beyond Conventional Bound.” *IEEE Transactions on Dependable and Secure Computing* 15 (4): 708–722. doi: 10.1109/TDSC.2016.2605087.

Washenko, Anna. 2019. “Microsoft OneDrive gets a more secure Personal Vault, plus additional storage options.” *Ars Technica*, June 25, 5:37pm. https://arstechnica.com/gadgets/2019/06/microsoft-beefs-up-cloud-storage-security-with-onedrive-personal-vault/.

Weinberg, Neal. 2013. “How to blunt spear phishing attacks.” *Network World*, March 6, 6:00am. https://www.networkworld.com/article/2164139/how-to-blunt-spear-phishing-attacks.html/.

ANNOTATED BIBLIOGRAPHY

Ablon, Lillian, Martin C. Libicki, and Andrea A. Galay. 2014. "Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar." Washington, DC: RAND Corporation. https://www.rand.org/pubs/research_reports/RR610.html.

Discusses the growth of the black market industries associated with cybercrime and the market for tools on how to conduct crimes in the cyber environment. Also includes discussion on the sale of data received through nefarious means. The market for hacker tools has grown while access to the markets is getting tougher.

Abomhara, Mohamed and Geir M. Køien. 2015. “Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders, and Attacks.” Journal of Cyber Security and Mobility 4 (1): 65-88. https://doi.org/10.13052/jcsm2245-1439.414.

Comprehensive overview of IoT; security threats, attacks, and vulnerabilities; primary security and privacy goals; and intruders, motivations, and capabilities.

Amerding, Taylor. 2019. "The 18 biggest data breaches of the 21st century." Framingham, MA: CSO. https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (June 6, 2019).

Describes major data breaches of organizations ranging from Adobe and Verisign to the US Office of Personnel Management. CSO site also has an extensive data base of articles relating to data protection.

Annansingh, Fenio. 2018. "Bring Your Own Security Risks With BYOD." Theory and Practice in Modern Computing. http://content.ebscohost.com/ContentServer.asp?T=P&P=AN&K=131764671&S=R&D=aps&EbscoContent=dGJyMNLe80SeqLM4yOvqOLCmr1GeqLBSr624S7CWxWXS&ContentCustomer=dGJyMPGus0m0q7JQuePfgeyx43zx.

Discusses the threat of BYOD to organizations and security of data on a mobile device. Addresses the issue of company owned IT or Personal IT and the ability to enforce security protocols.

Ball, Molly. 2013. “The Fall of the Heritage Foundation and the Death of Republican Ideas.” The Atlantic. September 25. https://www.theatlantic.com/politics/archive/2013/09/the-fall-of-the-heritage-foundation-and-the-death-of-republican-ideas/279955/ (July 16, 2019)

This article discusses the rise of Heritage Foundation power in the mid-1980’s and the perceived fall from grace in the 2010-2012 eras. It notes that Heritage was the powerful intellectual backbone of the GOP and served as the chief policy-makers and strategists the conservative movement.

Barth, Bradley. 2017. "Report: Chinese cyber spies targeted Western think tanks with spy tools, DDos attacks in Q4". SC Magazine. https://www.scmagazine.com/home/security-news/apts-cyberespionage/report-chinese-cyberspies-targeted-western-think-tanks-with-spy-tools-ddos-attacks-in-q4/.

Brief article that discusses hostile actions by China-based cyber actors that involved Direct Denial of Service (DDoS) attacks on several US think tanks and non-governmental organizations in 2017.

Beaghley, Sina. 2018. “Have a Victim Response Plan for Data Breaches.” Washington, DC: Wall Street Journal Cybersecurity Bulletin. https://www.rand.org/blog/2018/10/have-a-victim-response-plan-for-data-breaches.html.

Focuses on the timely notification to victims of data breaches and having an organizational plan for protecting the consumer

Blythe, John M., and Lynne Coventry. 2018. "Costly but Effective: Comparing the Factors that Influence Employee Anti-Malware Behaviours." Computers in Human Behavior 87 (2018): 87-97.

QUOTED FROM ABSTRACT: A cross sectional survey examined an extended version of Protection Motivation Theory (PMT) to identify factors that influence employees' intentions to perform three anti-malware behaviors. 526 employees completed an online survey that measured an employees' threat (severity and susceptibility) and coping (self-efficacy, response efficacy and response costs) appraisal. The survey also extended PMT to include additional factors of experience, psychological ownership, organizational citizenship and security responsibility. Factors were found

to have differing effects on employees' intentions to engage in anti-malware behaviors indicating the importance of targeted behavioral analyses. From PMT, coping appraisal was more predictive of security behaviors than threat appraisal. Specifically, across all behaviors, response costs were identified as a key factor that may be a barrier to behavior whereas response efficacy was a key facilitator. Moreover, additional factors to extend PMT contributed unique variance to predicting each anti-malware behavior. The study highlights the importance of identifying key factors prior to intervention development and demonstrates the benefit of expanding on behavioral theories to account for factors that may be important for the cybersecurity context.

Borrett, Martin, Roger Carter, and Andreas Wespi. 2014. "How is Cyber Threat Evolving and What Do Organizations Need to Consider?" Journal of Business Continuity & Emergency Planning. Vol 7, No. 2, 163-171. https://www.ingentaconnect.com/content/hsp/jbcep/2014/00000007/00000002/art00008

Attempts to identify future cyber threats to organizations, the evolution of the threats, and potential means to counter a growing and persistent problem.

Bradley, Nick. 2015. "The Threat Is Coming From Inside the Network: Insider Threats Outrank External Attacks." June 1. Security Intelligence. https://securityintelligence.com/the-threat-is-coming-from-inside-the-network/ (July 13, 2019)

This article discusses how the rise of social media, cloud computing, mobility, and big data are making it harder to detect insider threats while providing more ways to pass protected information. Importantly noted, the disgruntled employee who is terminated but retains access privileges can create back doors before leaving, providing him an opportunity for malicious activity after he is gone. Spam email used to just be an annoyance; however it has become a legitimate attack vector designed to trick inadvertent insiders to open an attachment and launch an attack. Bradley notes that IBM data and research indicates that every organization is under attack and must develop rigorous practices, enterprises, scrutinize users and networks for both security and compliance and enforce policies to protect networks.

Bullock, Jane A., George D. Haddow, and Damon P. Coppola, 2016. Introduction to Homeland Security, Fifth Ed, Elsevier Press, Waltham, MA

Book delves into all facets of Homeland Security with an entire chapter dedicated to cybersecurity and infrastructure protection. Discusses cybercrimes and rogue insiders as well as Department of Homeland Security efforts to protect infrastructure. Also looks at the public/private cooperation necessary to ensure national security, and information sharing with our international partners.

Burt, Tom. 2019. "New Steps to Protect Europe from Continued Cyber Threats". Blog. EU Policy Blog. https://blogs.microsoft.com/eupolicy/2019/02/20/accountguard-expands-to-europe/.

Microsoft VP of Security disclosing recent attacks against think tanks.

Center for Strategic and International Studies. 2019. Significant Cyber Incidents. CSIS. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents (June 29, 2019)

This site provides a complete timeline of cyber incidents since 2006 with special emphasis on attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars.

Cheng, Dean. 2016. Cyber Dragon: Inside China's Information Warfare and Cyber Operations: Inside China's Information Warfare and Cyber Operations. ABC-CLIO, Incorporated.

Provides general background info on Chinese military cyber actor tactics, techniques and procedures (TTPs) and more specifically on advanced persistant threat (APT) attacks.

Chertoff, Michael, 2009. Homeland Security: Assessing the First Five Years, University of Pennsylvania Press, Philadelphia, PA

Book written by former Secretary of Homeland Security and addresses critical issues remaining to be evaluated by his successors. Warns against complacency and encourages realistic threat assessment. A specific chapter on cybersecurity and the damage that can occur should there be an effort made against the infrastructure, particularly the electrical grid of the nation.

Cimpanu, Catalin. 2019. "Ancient ICEFOG APT Malware Spotted Again In New Wave Of Attacks | Zdnet". Zdnet. https://www.zdnet.com/article/ancient-icefog-apt-malware-spotted-again-in-new-wave-of-attacks/.

Article provides background information on ICEFOG malware.

Cisco. 2016. “Ransomware - Anatomy of an Attack.” YouTube. https://www.youtube.com/watch?v=4gR562GW7TI (May 28, 2019).

Short video that shows an example of a socially engineered attack on a company using little to no software development expertise.

Coffman, Andrew. 2011. “State Cybersecurity”. University of Mississippi, National Center for Justice and the Rule of Law. https://olemiss.edu/depts/ncjrl/pdf/StateCybersecurity.pdf (Accessed 3 July 2019).

Peer reviewed paper that details four main areas of focus for state cybersecurity plans; securing systems, securing data, developing knowledge and dealing with the aftermath of security breaches. Author references both the Multi-State Information Sharing and Analysis Center and the National Cybersecurity and Communications Integration Center as resources for states developing or revising cybersecurity policies.

Computer Weekly. 2011. Bring-your-own-device (BYOD) and legal/regulatory compliance. 2011. ComputerWeekly.com. November, 2011. https://www.computerweekly.com/podcast/Bring-your-own-device-BYOD-and-legal-regulatory-compliance (July 4, 2019)

Bring your own devices is an increasing issue in the workplace. These BYOD devices pose a host of compliance concerns for employers. While there are myriad concerns about the use of BYOD on employer networks and systems, some of the main concerns are: these devices have huge storage capacity with instant access to the internet, social networks, email, all of which is outside the control of the employer. In the U.S. and U.K., organizations have adopted “concierge services” that provision the BYOD devices for use on employer networks and systems after the employer installs security software and the employee agrees to have data being stored monitored. Bottom line up front: it’s best to prohibit the use of BYOD, however if allowed, the employer must have policies, procedures and training for the employees.

Crawford, Liam. 2016. “State Cybersecurity Principals & Best Practices”. IT Alliance for Public Sector, June 13, 2016. https://www.itic.org/dotAsset/6b96ecc0-53d8-4068-b2a5-4fd79676c9ed.pdf

Talking paper that describes six steps that state governments and industry can implement to help them build stronger cybersecurity policies. Principles outlined in this talking paper are derived from cybersecurity best practices exhibited by state and federal agencies that have proven effective in protecting these agencies from cyber threats.

Cybersecurity and Infrastructure Security Agency (CISA). 2019. Security Tip (ST05-012) Supplementing Passwords. Originally released July 27, 2010; last revised June 24, 2019. https://www.us-cert.gov/ncas/tips/ST05-012 (July 13, 2019)

Security tip from CISA (Department of Homeland Security) encouraging users to add multifactor authentication to supplement passwords to protect networks. In keeping passwords secure, users should have “salt and hash” passwords and strong authentication recovery mechanisms. Employers should implement account lockout policies and the ability to automatically disable accounts after predetermined periods of inactivity.

Cybersecurity Insider. 2019. "2019 Insider Threat Solutions Guide." https://www.cybersecurity-insiders.com/2019-insider-threat-solutions-guide (July 13, 2019).

This source highlights the threat from insiders (persons with authorized access) who intentionally or unknowingly expose vulnerabilities in employers’ systems. The article evaluates the insider threat through the lens of visibility, intelligence, detection, response and remediation, ease of deployment and impact on user experience, scalability and agility of the solution, and data privacy features.

Davis, John S., Jonathan William Welburn, Benjamin Boudreaux, Jair Aguirre. 2018. “When Cyber Attacks Occur, Who Should Investigate?” United Press International. 6 Dec 2018 https://www.rand.org/blog/2018/12/when-cyber-attacks-occur-who-should-investigate.html.

Discusses whether or not cyber-attacks should be attributed to any particular person or organization and proposes a centralized, non-governmental body investigates and decides whether to go public

Department of Homeland Security. 1996. Executive Order 13010: Critical Infrastructure Protection. Homeland Security Digital Library, July 15, 1996. https://www.hsdl.org/?view&did=1613.

Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. Threats to these critical infrastructures fall into two categories: physical threats to tangible property ("physical threats"), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats"). Because many of these critical infrastructures are owned and operated by the private sector, it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation. Order continues with details on establishment, membership, committee structure, and mission of the President's Commission on Critical Infrastructure Protection.

Department of Homeland Security. 2001. Executive Order 13231: Critical Infrastructure Protection in the Information Age. Homeland Security Digital Library, October 16, 2001. https://www.hsdl.org/?view&did=620.

The order created a federal "critical infrastructure protection" board and charged it with recommending policies and coordinating programs for protecting information systems for critical infrastructure. The Board's wide ambit includes outreach to the private sector and state and local governments, information sharing, incident coordination and crisis response, recruitment of Executive Branch security professionals, coordination of research and development, law enforcement coordination, and international cooperation. Executive Order 12472 is revoked.

Department of Homeland Security. 2013. Executive Order 13636: Improving Critical Infrastructure Cybersecurity. Homeland Security Digital Library, February 19, 2013. https://www.hsdl.org/?view&did=731040.

"Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security

challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties. We can achieve these goals through a partnership with the owners and operators of critical infrastructure to improve cybersecurity information sharing and collaboratively develop and implement risk-based standards."

Department of Homeland Security. 2015. Executive Order 13691: Promoting Private Sector Cybersecurity Information Sharing. Homeland Security Digital Library, February 20, 2015. https://www.hsdl.org/?view&did=762390

"By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows: Section 1. Policy. In order to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible. Organizations engaged in the sharing of information related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States. The purpose of this order is to encourage the voluntary formation of such organizations, to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organizations to partner with the Federal Government on a voluntary basis. Such information sharing must be conducted in a manner that protects the privacy and civil liberties of individuals, that preserves business confidentiality, that safeguards the information being shared, and that protects the ability of the Government to detect, investigate, prevent, and respond to cyber threats to the public health and safety, national security, and economic security of the United States. This order builds upon the foundation established by Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), and Presidential Policy Directive-21 (PPD-21) of February 12, 2013 (Critical Infrastructure Security and Resilience)."

Department of Homeland Security. 2016. Executive Order 13718: Commission on Enhancing National Cybersecurity. Homeland Security Digital Library, February 9, 2016. https://www.hsdl.org/?view&did=790114

"[I]n order to enhance cybersecurity awareness and protections at all levels of Government, business, and society, to protect privacy, to ensure public safety and economic and national security, and to empower Americans to take better control of their digital security, it is hereby ordered as follows: Section 1. Establishment. There is established within the Department of Commerce the Commission on Enhancing National Cybersecurity (Commission). Sec. 2. Membership. (a) The Commission shall be composed of not more than 12 members appointed by the President. The members of the Commission may include those with knowledge about or experience in cybersecurity, the digital economy, national security and law enforcement, corporate governance, risk management, information technology (IT), privacy, identity management, Internet governance and standards, government administration, digital and social media, communications, or any other area determined by the President to be of value to the Commission. […] Sec. 3. Mission and Work. The Commission will make detailed recommendations to strengthen cybersecurity in both the public and private sectors while protecting privacy, ensuring public safety and economic and national security, fostering discovery and development of new technical solutions, and bolstering partnerships between Federal, State, and local government and the private sector in the development, promotion, and use of cybersecurity technologies, policies, and best practices. The Commission's recommendations should address actions that can be taken over the next decade to accomplish these goals."

Department of Homeland Security. 2016. Executive Order 13757: Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities. Homeland Security Digital Library, December 28, 2016. https://www.hsdl.org/?view&did=797652.

"All property and interests in property that are in the United States, that hereafter come within the United States, or that are or hereafter come within the possession or control of any United States person of the following persons are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in: [...] (ii) any person determined by the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to be responsible for or complicit in, or to have

engaged in, directly or indirectly, cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that have the purpose or effect of: (A) harming, or otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector; (B) significantly compromising the provision of services by one or more entities in a critical infrastructure sector; (C) causing a significant disruption to the availability of a computer or network of computers; (D) causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain; or (E) tampering with, altering, or causing a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions; and (iii) any person determined by the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State: (A) to be responsible for or complicit in, or to have engaged in, the receipt or use for commercial or competitive advantage or private financial gain, or by a commercial entity, outside the United States of trade secrets misappropriated through cyber-enabled means, knowing they have been misappropriated, where the misappropriation of such trade secrets is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economy of the United States; (B) to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, any activity described in subsections (a)(ii) or (a)(iii)(A) of this section or any person whose property and interests in property are blocked pursuant to this order[.]"

Department of Homeland Security. 2016. National Cyber Incident Response Plan. Homeland Security Digital Library, December 2016. https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

National Cyber Incident Response Plan (December 2016): As described in the executive summary, “the National Cyber Incident Response Plan (NCIRP or Plan) was developed…to articulate the roles and responsibilities, capabilities, and coordinating structures that support how the Nation responds to and recovers from significant cyber incidents posing risks to critical infrastructure” (2016, 4). Further, “the

NCIRP…serves as the primary strategic framework for stakeholders to understand how federal departments and agencies and other national-level partners provide resources to support response operations… [and] how the Federal Government will organize its activities to manage the effects of significant cyber incidents" (DHS 2016, 4).

Department of Homeland Security. 2017. Study on Mobile Device Security. April. https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf.

Department of Homeland Security (DHS) Study on Mobile Device Security: As highlighted in the executive summary, "special care must be taken in the use of these devices because the default level of security is optimized for consumer ease of use" (DHS 2017, i). Further, DHS found that "Government mobile devices—despite being a minor share of the overall market—represent an avenue to attack back-end systems containing data on millions of Americans in addition to sensitive information relevant to government functions" (DHS 2017, i). Finally, this study "lists mobile security best practices collected from NIST, other government agencies, non-government organizations and private industry… [and] provides recommendations for assessing some of the risks posed by weaknesses in U.S. networks that appear to be unaddressed by industry" (DHS 2017, ii).

Department of Homeland Security. 2017. Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. Homeland Security Digital Library. May 11, 2017. https://www.hsdl.org/?view&did=800953

"The executive branch operates its information technology (IT) on behalf of the American people. Its IT and data should be secured responsibly using all United States Government capabilities. The President will hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises. In addition, because risk management decisions made by agency heads can affect the risk to the executive branch as a whole, and to national security, it is also the policy of the United States to manage cybersecurity risk as an executive branch enterprise."

Department of Homeland Security. 2019. Executive Order 13870: America's Cybersecurity Workforce. Homeland Security Digital Library, May 2, 2019. https://www.hsdl.org/?view&did=824839".

From the Document: "America's cybersecurity workforce is a strategic asset that protects the American people, the homeland, and the American way of life. [...] The United States Government must enhance the workforce mobility of America's cybersecurity practitioners to improve America's national cybersecurity. [...] The United States Government must support the development of cybersecurity skills and encourage ever-greater excellence so that America can maintain its competitive edge in cybersecurity. [...] The United States Government must create the organizational and technological tools required to maximize the cybersecurity talents and capabilities of American workers--especially when those talents and capabilities can advance our national and economic security. [...] In accordance with Executive Order 13800, the President will continue to hold heads of executive departments and agencies (agencies) accountable for managing cybersecurity risk to their enterprises, which includes ensuring the effectiveness of their cybersecurity workforces."

Department of Homeland Security. 2019. Executive Order 13873: Securing the Information and Communications Technology and Services Supply Chain. Homeland Security Digital Library, May 15, 2019. https://www.hsdl.org/?view&did=825242

From the Document: "[F]oreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services, which store and communicate vast amounts of sensitive information, facilitate the digital economy, and support critical infrastructure and vital emergency services, in order to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people. I further find that the unrestricted acquisition or use in the United States of information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign adversaries to create and exploit vulnerabilities in information and communications technology or services, with potentially catastrophic effects, and thereby constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. This threat exists both in the case of individual acquisitions or uses of such technology or services, and when

acquisitions or uses of such technologies are considered as a class. [...] In light of these findings, I hereby declare a national emergency with respect to this threat."

Donovan, Kevin. 2017. "10 Cybersecurity Best Practices for IT, IS, Network & Data Security". Observe IT, April 25, 2017. https://www.observeit.com/blog/10-best-practices-cyber-security-2017/.

Brief article that provides ten essential best practices for enhancing cybersecurity in organizations.

Drage-Arianson, Kristina, and Don Crouch. 2018. "Cybersecurity: Building Resilience from the Inside Out." Environmental Manager 65-68.

Short journal article that argues the importance of organizations to recognize the real threat imposed on cybersecurity. The authors propose that cybersecurity should be proactive within the organization, not something that occurs after an attack has been made. The article also talks about the complex nature of cyber threats and how antivirus software becomes obsolete far too soon. As organizations continue to accept business through the use of digitalization, they also increase their vulnerabilities. The authors recommend intelligence-sharing to identify and deal with vulnerabilities as well as training to increase employee awareness.

Dudley, Renee. "Sting Catches Ransomware Firm Negotiating with "hackers"." Salon. July 03, 2019. Accessed July 05, 2019. https://www.salon.com/2019/07/04/sting-catches-another-ransomware-firm_partner/.

Describes how the actions of a company paying to decrypt their ransomware affected computers was actually negotiating with the bad actors.

Eckman, S.J. @016. "14. Are there mandatory trainings for interns?" Congressional Research Service: Report, May 6: 9. http://eds.b.ebscohost.com.srv-proxy1.library.tamu.edu/eds/pdfviewer/pdfviewer?vid=5&sid=503f7c5b-cc30-4d0a-974b-b61fc7aae5e7%40pdc-v-sessmgr01 (June 29, 2019).

Sets forth the policy for Congressional interns, both paid and unpaid, as it applies for information security training. Training is required if an intern

will have access to computer networks. Additional trainings are required if an intern is paid or if they have access to resources at the Library of Congress or the Congressional Research Service.

Ehrenkranz, Melanie. 2019. “Researchers Reveal That Anonymized Data Is Easy To Reverse Engineer”. Gizmodo. https://gizmodo.com/researchers-reveal-that-anonymized-data-is-easy-to-reve-1836629166.

Researchers explore how inadequate current techniques to anonymize datasets are for cybersecurity.

Falcone, Robert, and Bryan Lee. 2018. "Sofacy Continues Global Attacks And Wheels Out New ‘Cannon’ Trojan". Unit42. https://unit42.paloaltonetworks.com/unit42-sofacy-continues-global-attacks-wheels-new-cannon-trojan/.

New Chinese developments in adapting older tactics, techniques and procedures (TTPs) with new capabilities/methodologies.

Findlaw, 2019. Privacy in the Workplace: Overview https://employment.findlaw.com/workplace-privacy/privacy-in-the-workplace-overview.html.

Discusses the right to privacy while in the workplace on company provided computers and phones as well as the use of monitoring agreements.

FireEye. 2019. "Advanced Persistent Threat Groups". Fireeye. https://www.fireeye.com/current-threats/apt-groups.html.

Advanced Persistent Threat group’s background information.

Flynn, Jim. 2019. "The Reality of the Local Government Cybersecurity Skill Gap". Government Technology, June 15, 2019. https://www.govtech.com/workforce/The-Reality-of-the-Local-Government-Cybersecurity-Skill-Gap.html

Focuses on the critical cybersecurity skill gap that exists in local government IT teams and departments. Briefly discusses the growing threat of cyber-attacks and describes steps that local governments can take to reduce this threat and narrow the gap.

Fortinet, 2016. "Security. From the Inside Out: New Breach Defense Strategies." Computer Weekly. 2016. http://content.ebscohost.com/ContentServer.asp?T=P&P=AN&K=115361333&S=R&D=ofm&EbscoContent=dGJyMNLe80SeqLM4yOvqOLCmr1GeqLBSr6%2B4SLWWxWXS&ContentCustomer=dGJyMPGus0m0q7JQuePfgeyx43zx

Article argues that "perimeter defense" of the organizations networks is no longer sufficient and fails to protect against the internal threats. Recommends internal segmentation as a possible security solution and firewalls within the organization as well. Network defenses must continue to evolve to meet the threats of today and plan for tomorrow. Internal Segmentation Firewalls (ISFW).

Freedman, Andrew. 2015. “Managing Personal Device Use in the Workplace: How to Avoid Data Security Issues and the Dig Yourself out of Your Failed BYOD Policy.” Suffolk Journal of Trial Appellate Advocacy, 20, 284-313. https://heinonline-org.srv-proxy1.library.tamu.edu/HOL/Page?handle=hein.journals/sujoriapv20&id=284&collection=journals&index(June 27, 2019)."

Freedman reviews applicable laws, statutes, and employer-employee contracts and their impact or lack of impact on the use of BYOD in the workplace. Impacts of policies are examined and suggestions for utilization of BYOD securely in the workplace are explored.

Fruhlinger, Josh. 2018. “The Mirai Botnet Explained: How IoT Devices Almost Brought down the Internet.” CSO Online. https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html, June 9, 2019.

Discuss an Internet of Things (IoT) hack that created a BotNet which conducted a Direct Denial of Service (DDoS) attack on the US East Coast.

Gallagher, Sean. 2017. "Chinese Hackers Go After Think Tanks In Wave Of More Surgical Strikes." Ars Technica. https://arstechnica.com/information-technology/2017/12/chinese-hackers-go-after-think-tanks-in-wave-of-more-surgical-strikes.

Article discusses Chinese use of techniques that focus on specific individuals or organizations, and the process of moving away from mass spam email type phishing campaigns.

Garamone, Jim. 2018. “Cyber Tops List of Threats to U.S., Director of National Intelligence Says." Department of Defense News, Defense Media Activity, February 13. https://dod.defense.gov/News/Article/Article/1440838/cyber-tops-list-of-threats-to-us-director-of-national-intelligence-says/ (June 29, 2019).

Director of National Intelligence, Daniel Coats, testified before a Senate Select Committee on Intelligence highlighting the cyber threats from Russia, China, Iran, and North Korea. Coats stated that both state and non-state actors and our adversaries are using cyber as an instrument of power to shape "societies and markets, international rules and institutions, and international hotspots to their advantage."

Gatlan, Sergiu. 2019. "New Extenbro DNS Changer Trojan Blocks Security Domains". Bleeping Computer. https://www.bleepingcomputer.com/news/security/new-extenbro-dns-changer-trojan-blocks-security-domains/.

A newly discovered DNS-changer Trojan dubbed Extenbro has been observed while blocking access to websites of security software vendors to prevent its victims from getting rid of the adware it dumps on their computers.

Gerstein, Daniel M. 2019. "Three 'New Rules' Worth Considering for the Internet" TechCrunch, May 9, 2019. https://www.rand.org/blog/2019/05/three-new-rules-worth-considering-for-the-internet.html.

Discusses "security by design" where the design phase incorporates security principles to prevent attacks. Seeks to ensure our internet infrastructure is up to date and modernized. Business models need to be changed to prevent internet providers from sharing personal data with advertisers.

Gewirtz, David. 2011. “Beware the Insider Cyber-Threat.” Journal of Counterterrorism and Homeland Security International.” Volume 17, no. 4, 8-9. http://eds.a.ebscohost.com.srv-

proxy1.library.tamu.edu/eds/pdfviewer/pdfviewer?vid=1&sid=6cab88dd-6a02-4ff0-808e-fa2f48d0316f%40sessionmgr4006 (July 26, 2019).

Basic recommendations for protection against insider threats with personal electronic (BYOB) devices.

Ghafir, Ibrahim, Jibran Saleem, Mohammad Hammoudeh, Hanan Faour, Vaclav Prenosil, Sardar Jaf, Sohail Jabbar, and Thar Baker. 2018. "Security Threats to Critical Infrastructure: the Human Factor." The Journal of Supercomputing, Vol 74, October: 4986-5002. https://link-springer-com.srv-proxy2.library.tamu.edu/article/10.1007/s11227-018-2337-2 (July 5, 2019).

Social engineering is recognized as a significant threat to information security which is hard to defend against. The article details several types and methods of social engineering attacks are reviewed such as obedience to authority and psychological manipulation. Preventative measures which have been successful have focused on training and awareness campaigns. Types of training examined include computer or web based training, favored by IT professionals, and traditional instructor-led training, favored by managers.

Goel, Sanjay, Kevin Williams, and Ersin Dincelli. 2017. " Journal of the Association for Information Systems, January 1: 22-44." http://eds.b.ebscohost.com.srv-proxy1.library.tamu.edu/eds/pdfviewer/pdfviewer?vid=1&sid=e826cc12-b694-454f-967c-c146b951aa7b%40pdc-v-sessmgr06 (July 5, 2019).

Article details the use of phishing as a human or social engineering attack. Details how phishing emails can be designed to target specific organizations or individuals and what kind of lure is most effective for the designed response. Authors conducted research using a non-malicious phishing campaign against third and fourth year university students.

Granville, Kevin. 2018. “Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens.” The New York Times. https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html (June 9, 2019).

Discuss the Cambridge Analytica / Facebook scandal. Which shows a weakness in third party venders having access to user’s data, creating an

exploitable point and lack of accountability by Facebook of its agreements.

Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." Wired. December 07, 2018. Accessed July 05, 2019. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Describes the NotPetya cyberattack which affected multiple industry and governments. The article goes into detail on how a major logistical company recovered from the attack.

Greenberg, Andy. 2018. “Hackers Remotely Kill a Jeep on the Highway-With Me in It.” Wired. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (June 9, 2019).

Discuss the remote hacking of vehicle operating at speed and the ability of hackers to disable critical safety systems and capabilities

Greitzer, Frank L. and Ryan E. Hohimer. 2011. "Modeling Human Behavior to Anticipate Insider Attacks." Journal of Strategic Security, Vol IV, Issue 2: 25-48. http://eds.b.ebscohost.com.srv-proxy1.library.tamu.edu/eds/pdfviewer/pdfviewer?vid=5&sid=6f59a281-c513-435a-b3f3-101b5a86b3ea%40sessionmgr103 (July 6, 2019).

Article focuses on the insider threat to organizations and notes that approximately 87 percent of Department of Defense (DoD) IT intrusions were done by employees or others inside the organization. Article further identifies behaviors which can be detected when monitoring of a network occurs.

Guerra, Domingo. 2017. "How to Manage Personal Device Risk." Risk Management, Risk and Insurance Management Society, Inc., December 2017. http://content.ebscohost.com/ContentServer.asp?T=P&P=AN&K=126540938&S=R&D=bft&EbscoContent=dGJyMNLe80SeqLM4yOvqOLCmr1GeqK9SsKu4SLKWxWXS&ContentCustomer=dGJyMPGus0m0q7JQuePfgeyx43zx

Article addresses the state of corporate policies on BYOD and the risks associated with personal devices with or without direct access to networks.

Offers a suggestion that all devices, private or corporate-owned should be protected and managed.

Harwell, Drew. 2019. "Hacked Documents Reveal Sensitive Details of Expanding Border Surveillance." The Washington Post. June 21, 2019. Accessed July 04, 2019. https://www.washingtonpost.com/technology/2019/06/21/hacked-documents-reveal-sensitive-details-expanding-border-surveillance/.

Article describes that subcontractors access to networks can be the weak point which hackers will exploit and extract data.

Hern, Alex. 2018. "Russian hackers targeting conservative US thinktanks, Microsoft says". The Guardian, August 21, 2018. https://www.theguardian.com/us-news/2018/aug/21/russian-hackers-targeting-more-us-political-groups-microsoft-says.

Article reveals attempts by Russian hacking group to target organizations such as the Hudson Institute and International Republican Institute by mimicking them with fake websites. Such sites could deceive authorized users of the legitimate sites to log in to the fake sites and thereby compromise their login and authentication information.

Herrera, Andrea Vaca, Mario Ron, and Carlos Rabadão. "National Cyber-Security Policies oriented to BYOD (Bring Your Own Device): Systematic Review." Iberian Conference on Information Systems and Technologies. http://content.ebscohost.com/ContentServer.asp?T=P&P=AN&K=127421183&S=R&D=aps&EbscoContent=dGJyMNLe80SeqLM4yOvqOLCmr1GeqK9SsKu4S7eWxWXS&ContentCustomer=dGJyMPGus0m0q7JQuePfgeyx43zx.

Article discusses the security challenges of BYOD and possible policy guidelines to help protect the organization from the multitude of threats, risks, and systems controls for BYOD. Lost or Stolen devices; non-employee access; Malware; Insecure Applications are just a few of the risks. Offers best practices for consideration when establishing policy.

Hill, Michael. 2019. China Still Poses Major Cyber Threat Despite Drop in U.S. Attacks. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/china-still-major-cyber-threat/ (June 29, 2019).

Article describes how, despite a recent curtail in Chinese state-sponsored cyber intrusions targeting the U.S., U.K., Canadian, and Japanese governments, China remains active in the cyber arena and remains a serious cyber-threat to the U.S. and countries around the world. China is likely in the midst of a multi-year maturation of their cyber programs and will emerge with better organization, communications, and execution.

Homeland Security News Wire. 2019. Cybersecurity. http://www.homelandsecuritynewswire.com/topics/cybersecurity.

The Homeland Security News Wire is the homeland security industry's largest online daily news publication, authoritative, in-depth analysis and coverage of the day's most important homeland security stories. This is a great starting point for many cybersecurity related articles related to government, business, science, and technology.

Hudson Institute. 2018. "Hudson Institute Statement on Russian Cyberattacks - By Hudson Institute". Hudson.Org. https://www.hudson.org/research/14510-hudson-institute-statement-on-russian-cyberattacks.

Hudson Institute addresses their recent hack orchestrated by Russian state sponsored cyber actors.

Hyman, Jon. 2018. "Insiders Are Serious Threats to Cybersecurity in an Organization." November 29. Worforce. https://www.workforce.com/2018/11/29/insiders-are-serious-threats-to-cybersecurity-in-an-organization/ (July 13, 2019).

Employees are any company's weakest link in the cybersecurity world. This article addresses both the negligent employee who doesn't know or understand the risks of his actions and the malicious insider with motive and access. Cybercriminals use the dark web to recruit insiders to gain access to data, make illegal trades, or generate profit. There are three types of insider threats: 1) the negligent employee, 2) the disgruntled employee, and 3) the malicious employee. Each poses the same risks but have different motivators. Each is also difficult to predict and discover before their actions result in damage. The article acknowledges that companies are investing in expensive deterrence, detection, inventories, policies, pre-employment background checks, termination processes that include removing access to cyber systems, designed for protection from their own employees.

Imgraben, James, Alewyn Engelbrecht, and Kim-Kwang Raymond Choo. 2014. "Always Connected, But Are Smart Mobile Users Getting More Security Savvy? A Survey of Smart Mobile Device Users." Behavior & Information Technology, Vol 33, No. 12: 1347-1360. http://eds.b.ebscohost.com.srv-proxy2.library.tamu.edu/eds/pdfviewer/pdfviewer?vid=8&sid=ea5db762-c3a3-4336-877f-a98237f289e1%40pdc-v-sessmgr03 (June 29, 2019).

Survey of students and academics identifies habits of smart phone use by device operating system, user age, and education level. The survey identified potential security threats and lapses in common security protocols in the survey population. Suggestions to mitigate identified risks are discussed in the article.

InfraGard. 2019. Costs Associated with Cyber Intrusions - Cost of a Data Breach Study: Global Overview. 2018. Costs Associated with Cyber Intrusions - 2018 Cost of a Data Breach Study: Global Overview.

Results from a global study about the costs related to cyber hacks. The study recruited 477 organizations worldwide and interviewed more than 2,200 individuals knowledgeable about the data breach incident in these organizations. It shows key findings and makes some recommendations for mitigating a breach.

International Organization for Standardization. 2005. ISO/IEC 27000 family – Information security management systems. https://www.iso.org/isoiec-27001-information-security.html (July 4, 2019).

Family of standards to assist organizations manage the security of assets entrusted by third parties. ISO/IEC 27001 is the best known of these standards provides a model for “establishing, implementing, operating, developing, monitoring, reviewing, maintaining, and improving an information security management system. It is a top-down, risk based approach that defines security policy, scope of ISMS, conduct risk assessment, manage identified risks, select control objectives, prepare statement of applicability. ISO 27001 does not mandate specific information security controls, but provides a checklist for users. Additional information was found at https://whatis.techtarget.com/definition/ISO-27001.

International Strategy for Cyberspace. 2011. "Prosperity, Security, and Openness in a Networked World". Obama White House Archives, May 2011.

https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf

"The foundation of the United States' international cyberspace policy is the belief that networked technologies hold immense potential for our Nation, and for the world. Over the last three decades we, the United States, have watched these technologies revolutionize our economy and transform of our daily lives. We have also witnessed offline challenges, like exploitation and aggression, move into cyberspace. As we adapt to meet those challenges, we will lead by example. The United States will pursue an international cyberspace policy that empowers the innovation that drives our economy and improves lives here and abroad. In all this work, we are grounded in principles essential not just too American foreign policy, but to the future of the Internet itself. [...] Our policies flow from a commitment to both preserving the best of cyberspace and safeguarding our principles. Our international cyberspace policy reflects our core commitments to fundamental freedoms, privacy, and the free flow of information."

Jaeger, Jaclyn. 2017. “Identifying Inside Threats to Cyber-Security.” Compliance Week. Volume 14, Issue 158, 62-65. http://bi.galegroup.com.srv-proxy1.library.tamu.edu/global/article/GALE|A535031011/16624133f8f709ac40f6959c7ea32a5a?u=txshracd2898 (July 26, 2019).

Examples of cyber security measures used by Lockheed Martin to protect against the inside threat.

Kaila, Urpo, and Linus Nyman. 2018. "Information Security Best Practices: First Steps for Startups and SMEs." Technology Innovation Management Review 8 (11): 32-42.

QUOTED FROM ABSTRACT: "This article identifies important first steps toward understanding and implementing information security. From the broad selection of existing best practices, we introduce a lightweight yet comprehensive security framework with four useful first steps: identifying assets and risks; protecting accounts, systems, clouds, and data; implementing a continuity plan; and monitoring and reviewing. This article is intended primarily for startups and less mature companies, but it is likely to be of interest to any reader seeking an introduction to basic information security concepts and principles as well as their implementation."

Kaspersky Labs. 2013. "The ICEFOG APT: A Tale of Cloak and Three Daggers". https://media.kaspersky.com/en/icefog-apt-threat.pdf.

Article discusses history of the malicious ICEFOG advanced persistent threat (APT).

Kaspersky. 2019. "What Is Spear Phishing?" Usa.Kaspersky.Com. Accessed July 25. https://usa.kaspersky.com/resource-center/definitions/spear-phishing.

Background information on spear phishing methodology.

Kessler, Gary C. 2014. "The Impact of Cyber-Security on Critical Infrastructure Protection: The Advanced Persistent Threat". Westview Press, Boulder, CO. 2014.

Article discusses Advanced Persistent Threats to the cyber sphere. Advanced in their capabilities; persistent in that they are not some random attack, but relentless pursuit of information directed at a specific target; threat indicates the capability and intent to do harm as the attacks are specific and intentional by people who are motivated and well-funded.

Kohen, Isaac, 2018. Employee Monitoring Ethics: Considerations and Impacts. https://itsecuritycentral.teramind.co/2018/01/18/employee-monitoring-ethics-considerations-and-impacts/.

Article explores the ethics, legal considerations, and impacts of employee monitoring.

Kozy, Adam. 2017. "An End to 'Smash-And-Grab' And a Move to More Targeted Approaches." CrowdStrike, December 20, 2017. https://www.crowdstrike.com/blog/an-end-to-smash-and-grab-more-targeted-approaches.

CrowdStrike's Falcon Intelligence group reported that China (PRC)-based actors had been discovered conducting espionage-driven targeted attacks against at least four Western think tanks and an additional two non-governmental organizations (NGOs).

Lee, Timothy B. "The Sony Hack: How It Happened, Who Is Responsible, and What We've Learned." Vox. December 18, 2014. Accessed July 05, 2019. https://www.vox.com/2014/12/14/7387945/sony-hack-explained.

Describes the technique and repercussions of the Sony Hack. Provides a useful list of best practices for a corporation in planning and updating scyber security policy.

Lewis, James A. 2006. "Cybersecurity and Critical Infrastructure Protection". Center for Strategic and International Studies, January, 2006. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/0601_cscip_preliminary.pdf.

Article addresses cybersecurity and cyber terrorism, treating the cyber realm as a potential target of a terrorist plot designed to create a political change by military or psychological actions. In theory, disruption of the cyber spectrum could be considered a weapon of mass destruction.

Libicki, Martin C. 2012. "Cyber Operations Can Supplement a War, but They Cannot Be the War" The International Economy, 1 December 2012. https://www .rand.org/blog/2012/12/cyber-operations-can-supplement-the-war-but-they-cannot.html.

Article addresses the fact that while cyber warfare can be disruptive, it is not destructive and usually the owner of the information has not lost the information or its use. It is just an inconvenience that another organization may have the same information now. While the information is proprietary, the owner hasn't necessarily lost its use. Quite different than actual warfare where the enemy attempts to destroy your infrastructure.

Lie, Eric; Macmillan, Rory; Keck, Richard. 2009. "Cybersecurity: The Role and Responsibilities of an Effective Regulator". 9th ITU Global Symposium for Regulators. Beirut, Lebanon, November 2009. http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf.

Background paper that provides framework for discussion on role of information communication technology (ICT) regulators in cybersecurity.

Lohrmann, Daniel J. "A New Look at Insider Threats" PublicCIO, ERepublic, Folsom, CA. http://content.ebscohost.com/ContentServer.asp?T=P&P=AN&K=99942758&S=R&D=bcr&EbscoContent=dGJyMNLe80SeqLM4yOvqOLCmr1GeqK9SsKy4SLKWxWXS&ContentCustomer=dGJyMPGus0m0q7JQuePfgeyx43zx.

Offers three suggestions on where to begin with security. Access Controls; Acceptable use policies; and security teams who offer real world examples. The idea is to get the masses "behind" security policies without scaring everyone who is trying to do a good job.

Lyngaas, Sean. 2019. “As Europe prepares to vote, Microsoft warns of Fancy Bear attacks on democratic think tanks.” Cyber Scoop, February 20, 2019. https://www.cyberscoop.com/european-think-tanks-hack-microsoft-fancy-bear-russia/ (June 29, 2019).

Microsoft has detected hacking attempts on democracy-focused think tanks from the Russian hacking group that breached the Democratic National Committee in 2016. Russian military intelligence hackers, a group known as Strontium or more commonly Fancy Bear or APT28, have conducted over 100 counts of malicious cyber activity against think tank employees in six European countries. Most attempts were unsuccessful; however there is a real threat of continuing Russian interference in free elections of democratic nations.

Mazer, Murray. 2007. "Making a Security and Compliance Investment: How to Value What You Pay For." Journal of Investment Compliance 8 (3): 75-78, September 18, 2007.

QUOTED FROM ABSTRACT: "Purpose – The purpose of the paper is to emphasize the need for technology and people investments in security and compliance and to show the cost of not making such investments. Design/methodology/approach – The paper describes direct and indirect costs of database intrusions and data thefts, shows ways in which the cost of technology can be justified, and shows examples of how return on investment (ROI) can be calculated. Findings – The paper finds that, in today’s data-sensitive climate, automation of stronger data protection practices has become an essential activity. Originality/value – This paper is a practical reminder that security does not come without investment in appropriate automated systems along with related policies and other safeguards. Keywords Investments, Securities, Data security"

McKee, Mike. 2018. Accidental Insiders Pose a Serious Threat to Your Organization. April 10. Infosecurity-Magazine.com. https://www.infosecurity-magazine.com/opinions/accidental-insiders-serious-threat/ (July 13, 2019)

Article describes how accidental insiders pose just as significant threat to organizations and their systems as malicious or disgruntled insiders. It is important to understand what the insider threat looks like and put plans in place to detect and prevent unintentional insider threats before they leak information. Employers should be aware of policy violations, employees sidestepping regulations, use of consumer cloud computing or storage like Dropbox or Google Drive, careless personal security, and available options to decrease the threat and build resiliency.

McKenzie, Nick. 2019. "'Watering Hole' Attacks: How China's Hackers Went after Think Tanks and Universities." The Sydney Morning Herald. December 03, 2018. Accessed July 04, 2019. https://www.smh.com.au/national/watering-hole-attacks-how-china-s-hackers-went-after-think-tanks-and-universities-20181203-p50jxj.html.

Provides evidence of China specifically targeting Think Tanks for the process of stealing information. Additionally describes the technique, fishing hole, currently being used by China in these attacks. Describes how Chinese hackers created fake websites with similar URL names and links. Further describes how these Think Tanks discovered the attempts and worked with proper authorities to have the websites removed.

McReynolds, Joe. 2015. "China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy - Jamestown". Jamestown Foundation, April 16, 2015. https://jamestown.org/program/chinas-evolving-perspectives-on-network-warfare-lessons-from-the-science-of-military-strategy/#.Vb7q6f9RHTg.

Author provides a synthetization of the current Chinese cyber posture as presented in their publicly provided national security strategy document

Microsoft Defender ATP Research Team. 2018. "Analysis of cyberattack on U.S. think tanks, non-profits, public sector by unidentified attackers." Microsoft, December 3. https://www.microsoft.com/security/blog/2018/12/03/analysis-of-cyberattack-on-u-s-think-tanks-non-profits-public-sector-by-unidentified-attackers/ (June 29, 2019)

Reuters recently reported a hacking campaign focused on a wide range of targets across the globe. These attacks have targeted public sector institutions and non-governmental organizations like think tanks and research centers, as well as educational institutions and private-sector

corporations in the oil and gas, chemical, and hospitality industries. Third party security researchers attribute the attacks to Yttrium, also known as Cozy Bear or APT29, however there is insufficient evidence for an affirmative link. Approximately 47% of attacks have targeted think tanks/research centers.

Mikolic-Torreira, Igor; Henry, Ryan; Snyder, Don; Beaghley, Sina; Pettyjohn, Stacie L.; Harting, Sarah; Westerman, Emma; Shlapak, David A.; Bishop, Megan; Oberholtzer, Jenny; Skrabala, Lauren and Weinbaum, Cortney. 2016. "A Framework for Exploring Cybersecurity Policy Options", Santa Monica, Calif. RAND Corporation, RR-1700-WFHF, 2016. (Accessed June 27, 2019). https://www.rand.org/pubs/research_reports/RR1700.html

Peer review research paper that explores the challenges of motivating system users and customers of organizations to utilize cybersecurity methods. This paper goes further to provide IT professionals with a framework upon which they can build an effective cybersecurity program.

Miller, Maggie. 2019. “Louisiana declares state emergency after cyberattacks on school districts”. The Hill, July 26, 2019. https://thehill.com/homenews/state-watch/454928-louisiana-declares-state-emergency-after-cyber-attacks-on-school

The declaration comes after three local school districts were hit by what local media have described as ransomware attacks, where hackers take over and encrypt vital cyber systems and demand a ransom to release the data.

Moore, Michelle. 2019. “Inside the Government Cybersecurity Landscape: Federal vs. State Level Challenges”. Tripwire, May 1, 2019. https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/government-cybersecurity-federal-state/.

Article compares state and federal cybersecurity issues and goals for each to reduce cyber threats, challenges faced by both levels of government and differences between state and federal cyber threats. The author included hyperlinks to referenced sites related to cybersecurity such as the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA) and the Center for Internet and Society.

Mueller, Robert. 2019. "Report On The Investigation Into Russian Interference In The 2016 Presidential Election". Washington, D.C.: Department of Justice, March 2019. https://www.justice.gov/storage/report.pdf.

The Mueller report on Russian interference in the 2016 Presidential election. Lays out how Russians hacked the DCCC.

Musthaler, Linda. 2016. "A new approach to detecting compromised credentials in real-time". Network World, IT Best Practices, April 15, 2016. https://www.networkworld.com/article/3056823/a-new-approach-to-detecting-compromised-credentials-in-real-time.html

Article that briefly describes a proposed method of programming data bases to scan for abnormal data flows resulting from the fraudulent use of credentials such as passwords and authentication.

National Governor's Association. 2017. "Developing a Cybersecurity Strategy". NGA Governor's Guide to Cybersecurity, 2017. https://www.nga.org/bestpractices/divisions/hsps/statecyber/

An information portal on the NGA Governor's website that is set up like a talking paper and offers basic guidance to state governor's offices on how to develop a strategy guide for cybersecurity. Provides two best practice examples of Iowa and Virginia where these states passed legislation addressing cybersecurity issues.

National Institute of Standards and Technology (NIST). 2018. "Framework for Improving Critical Infrastructure Cybersecurity". (https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf) Version 1.1 (updated 2018 version: https://www.hsdl.org/?view&did=809529)

"Version 1.1 of this Cybersecurity Framework refines, clarifies, and enhances Version 1.0, which was issued in February 2014. It incorporates comments received on the two drafts of Version 1.1. [...] The United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. Similar to financial and reputational risks, cybersecurity risk affects a company's bottom line. It can drive up costs and affect revenue. It can harm an organization's ability to innovate and to gain and maintain customers. Cybersecurity can be an important and

amplifying component of an organization's overall risk management. [...] The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The Framework consists of three parts: the Framework Core, the Implementation Tiers, and the Framework Profiles."

Newcomb, Alyssa. 2019. "Hackers Used a Cheap Raspberry Pi Computer to Breach NASA." Fortune. June 20, 2019. Accessed July 04, 2019. http://fortune.com/2019/06/20/hackers-raspberry-pi-computer-nasa/?xid=gn_editorspicks.

Describes how a RasberryPi (IOT device) attached to NASAs network was utilized as an access point for Hackers. Hackers would have access to the entire network and attached networks through this device.

Newman, Craig A. 2018. "When to Report a Cyberattack? For Companies, That's Still a Dilemma." The New York Times. March 05, 2018. Accessed July 05, 2019. https://www.nytimes.com/2018/03/05/business/dealbook/sec-cybersecurity-guidance.html.

Discusses SEC reporting cyberattack reporting requirements. Then goes on to show that very few companies are actually reporting cyberattacks, with very little negative impacts from the SEC or stock holders.

Norton. 2016. "2016 Internet Security Threat Report". Symantec, Vol 21, April 2016. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

Report indicates that spear phishing attacks are beginning to utilize less mass spam email methodologies and instead utilizing more focus campaigns that single out specific individuals and organizations.

Obama, Barack. 2011. "Presidential Policy Directive 8: National Preparedness". The White House, March 30, 2011. (https://www.hsdl.org/?view&did=7423)

"This directive is aimed at strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters. Our national preparedness is the shared responsibility of all levels of government, the

private and nonprofit sectors, and individual citizens. Everyone can contribute to safeguarding the Nation from harm. As such, while this directive is intended to galvanize action by the Federal Government, it is also aimed at facilitating an integrated, all-of-Nation, capabilities-based approach to preparedness. Therefore, I hereby direct the development of a national preparedness goal that identifies the core capabilities necessary for preparedness and a national preparedness system to guide activities that will enable the Nation to achieve the goal. The system will allow the Nation to track the progress of our ability to build and improve the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation."

Obama, Barack. 2013. "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience". The White House, February 12, 2013. (https://www.hsdl.org/?view&did=731087)

"This Presidential Policy Directive (PPD) sets forth principles governing the Federal Government's response to any cyber incident, whether involving government or private sector entities. For significant cyber incidents, this PPD also establishes lead Federal agencies and an architecture for coordinating the broader Federal Government response. This PPD also requires the Departments of Justice and Homeland Security to maintain updated contact information for public use to assist entities affected by cyber incidents in reporting those incidents to the proper authorities."

Obama, Barack. 2016. "Presidential Policy Directive 41: Directive on United States Cyber Incident Coordination". The White House, July 26, 2016. (https://www.hsdl.org/?view&did=797544)

"This Presidential Policy Directive (PPD) sets forth principles governing the Federal Government's response to any cyber incident, whether involving government or private sector entities. For significant cyber incidents, this PPD also establishes lead Federal agencies and an architecture for coordinating the broader Federal Government response. This PPD also requires the Departments of Justice and Homeland Security to maintain updated contact information for public use to assist entities affected by cyber incidents in reporting those incidents to the proper authorities."

O’Brien, Brenden. 2018. "Russian Hackers Targeted US Conservative Think-Tanks, Says Microsoft". Public Radio International. https://www.pri.org/stories/2018-08-21/russian-hackers-targeted-us-conservative-think-tanks-says-microsoft.

Article describes Russian State attacks on American conservative think tanks as retribution for authoring multiple articles speaking out against kleptocracies

Oboba, Osonde A. 2018. “Keeping Artificial Intelligence Accountable to Humans” TechCrunch. 20 August 2018. https://www.rand.org/blog/2018/08/keeping-artificial-intelligence-accountable-to-humans.html

Article addresses further that there is bias in AI and we cannot rely on these tools for perfection and decision making. We are creating intelligence in our own image. AI systems are only as good as the data used to train them.

O'Sullivan, Donie. "Russian Group Suspected in DNC Hack Targeted Washington Think Tank." CNN. January 31, 2019. Accessed July 05, 2019. https://www.cnn.com/2019/01/30/politics/fancy-bear-microsoft-csis-think-tank/index.html.

Second article discussing Russian State attacks on American conservative think tanks.

Ottis, Rain. 2008. "Analysis Of The 2007 Cyber Attacks Against Estonia From The Information Warfare Perspective". Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence. http://Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.

Background info on Russian cyber actors DoSing Estonia due to the removal of a Soviet statue in Talinn, Estonia. It was the first major cyber-attack on a sovereign nation by Russia.

PC Magazine. 2019. “Password-stealing malware attacks rose by 60% in 2019: Kaspersky report”. PCMag, July 29. 2019. https://in.pcmag.com/internet/131680/password-stealing-malware-attacks-rose-by-60-in-2019-kaspersky-report

Password Stealing Ware (PSW) grabs data directly from the web browser and most often these data includes sensitive information like access details

to online accounts, financial information like saved passwords, card details, autofill data etc.

Porche III, Isaac R. 2019. "Fighting and Winning the Undeclared Cyber War." Inside Sources, 23 Jun 2019. https://www.rand.org/blog/2019/06/fighting-and-winning-the-undeclared-cyber-war.html

Highlights vulnerabilities from a lack of effective software security, improper configuration and maintenance of operating systems, and open network connections with weak enforcement of remote login policies such as Wi-Fi hotspots.

Power, Richard and Dario Forte. 2006. "Thwart the Insider Threat: A Proactive Approach to Personal Security." Computer Fraud & Security. Vol. 2006, Issue 7, 10-15. https://www-sciencedirect-com.srv-proxy1.library.tamu.edu/science/article/pii/S1361372306704006

Article includes a 20-question checklist on personnel security controls which also suggest practices an organization can use to detect or thwart insider threats.

Preveil Admin. 2017. "Protecting Think Tanks Against a Cyber Onslaught". Preveil, 2017. https://www.preveil.com/blog/protecting-think-tanks-cyber-onslaught/

Article focuses on potential weak points for think-tanks' network security processes such as "super-users" who are granted administrator-level access and the need for end-to-end encryption that protects data at all stages of system use.

Privacy Rights Clearinghouse. 2014. “Bring Your Own Device (BYOD)…At Your Own Risk." https://www.privacyrights.org/consumer-guides/bring-your-own-device-byod-your-own-risk#2.%20employer%20byod%20concerns.

This source explains BYOD for both employers and employees. It lists some concerns for employers surrounding BYOD. The article shows what employees might expect in a BYOD policy. At the end, it offers some tips for implementing a BYOD policy.

Privacy Rights Clearinghouse. 2019. "Workplace Privacy and Employee Monitoring." https://privacyrights.org/consumer-guides/workplace-privacy-and-employee-monitoring.

This source discusses employer and employee rights concerning computers, email, telephones, mobile devices, and social media.

Rebner, Susan. 2019. "Behavioral Biometrics Are Key for Cybersecurity" by Young Entrepreneur Council. Inc., June 27, 2019. https://www.inc.com/young-entrepreneur-council/behavioral-biometrics-are-key-for-cybersecurity.html

Discusses the evolving nature of biometric security measures for cybersecurity and user access of information technology

"Regulatory Considerations for BYOD Polices". Hanover Research, November, 2012. https://www.attachmate.com/solutions/in-response-to-your-mobility-demands/MobileDeviceManagement/RegulatoryConsiderationsforBYODPolicies.pdf (July 4, 2019)

This white paper highlights the impact of specific regulations governing healthcare and financial industries, along with potential security solutions offered by vendors of mobile device management (MDM) software. In the U.S., strict enforcement and penalties in the healthcare and financial sectors have led to voluntary compliance standards and best practices. The report lists U.S. regulations for the healthcare and financial industries but there is applicability for best practices for use of BYOD.

Riesco, R., and V. A. Villagrà. 2019. "Leveraging Cyber Threat Intelligence for a Dynamic Risk Framework." International Journal of Information Security (Springer Berlin Heidelberg) Volume 18, Issue 6, pgs 1-25, December 2019. https://doi.org/10.1007/s10207-019-00433-2.

QUOTED FROM ABSTRACT: One of the most important goals in an organization is to have risks under an acceptance level along the time. All organizations are exposed to real-time security threats that could have an impact on their risk exposure levels harming the entire organization, their customers and their reputation. New emerging techniques, tactics and procedures (TTP) which remain undetected, the complexity and decentralization of organization assets, the great number of vulnerabilities proportional to the number of new type of devices (IoT) or still the high

number of false positives, are only some examples of real risks for any organization. Risk management frameworks are not integrated and automated with near real-time (NRT) risk-related cybersecurity threat intelligence (CTI) information. The contribution of this paper is an integrated architecture based on the Web Ontology Language (OWL), a semantic reasoner and the use of Semantic Web Rule Language (SWRL) to approach a Dynamic Risk Assessment and Management (DRA/DRM) framework at all levels (operational, tactic and strategic). To enable such a dynamic, NRT and more realistic risk assessment and management processes, we created a new semantic version of STIX™v2.0 for cyber threat intelligence as it is becoming a de facto standard for structured threat information exchange. We selected an international leading organization in cybersecurity to demonstrate new dynamic ways to support decision making at all levels while being under attack. Semantic reasoners could be our ideal partners to fight against threats having risks under control along the time, for that, they need to understand the data. Our proposal uses an unprecedented mix of standards to cover all levels of a DRM and ensure easier adoption by users.

Rosner, Eric. 2017. "Cyber Federalism: Defining Cyber's Jurisdictional Boundaries". Master's Thesis, Department of National Security Affairs, Naval Postgraduate School, Monterey, CA: Office of Management and Budget, pgs 1-128, December 2017. https://archive.org/details/cyberfederalismd1094556794

"QUOTED FROM ABSTRACT: Cybersecurity was once a federal government responsibility because cyber had limited impact on state and local entities, but today's cyber risks to critical infrastructure and public services affect all levels of government. This thesis explores the current state of cybersecurity in the United States and examines what role each level of government—federal, state, and local—should play in protecting against and responding to a significant cyber incident. It evaluates current state and local cyber capabilities and outlines the capabilities these governments must develop to play a larger role in this growing homeland security mission. The research concludes that state and local governments should have an important role in cyber preparedness and cyber incident response, but many of these entities lack the capabilities necessary to play a meaningful role. Furthermore, current policies fail to provide clear jurisdictional boundaries between levels of government. Therefore, this thesis recommends that the nation develop a legal framework to improve jurisdictional boundaries, prioritize cyber investments at the state and local

level, and improve cyber education. These steps will strengthen state sovereignty and improve the nation's cyber posture."

Rouse, Margaret. 2015. "What Is Watering Hole Attack? - Definition from Whatis.Com". Searchsecurity, August 2015. https://searchsecurity.techtarget.com/definition/watering-hole-attack.

Background information on Watering Hole attacks

Sanjay, Katkar. 2016. "4 Steps to Mitigating Third-Party Vendor Cyber-Security Threats". Security Magazine, March 22, 2016. https://docs.google.com/spreadsheets/d/12SOwEbtvvwZtY7Vf928Di6yMW-v4SaBJ/edit#gid=73556766

Brief article provides practical suggestions for reducing the risk of third-party entities with access to organizational cyber systems becoming a vulnerability. Discusses the value of requiring third-party entities to sign service agreements that requires they comply with organizational policies regarding cyber use and access.

Sauter, Mark A. and James J. Carafano, 2012. Homeland Security. 2nd Ed. New York: McGraw-Hill

Chapter on cybersecurity and protection of cyberspace and digital technology discusses the interdependencies of critical infrastructure in cyberspace warning against insider and outsider attacks, malicious software and human engineering. Discusses methods of combatting cyber threats such as authentication and password protection, technical and software defenses, and security practices such as backing up data on an off-site server.

Schulzke, Marcus. 2018. "The Politics of Attributing Blame for Cyberattacks and the Costs of Uncertainty." Perspectives on Politics 16 (4): 954-968, December 14, 2018. https://politicalsciencenow.com/the-politics-of-attributing-blame-for-cyberattacks-and-the-costs-of-uncertainty/

QUOTED FROM ABSTRACT: Attribution is one of the most serious challenges associated with cyberattacks. It is often difficult to determine who launched an attack and why, which hinders efforts to formulate appropriate responses. Although the attribution problem has been discussed extensively in research on cybersecurity, it is generally approached as a technical challenge for security professionals and

politicians. I contend that it is vital to take the attribution problem beyond this elite focus by considering how attributional challenges can interfere with the public's efforts to understand security challenges and evaluate government actions. Faced with uncertainty and the confusion of attempting to understand novel cyber threats, citizens frequently lack the information they need to reliably identify the culprits behind attacks—or sometimes even to know whether an attack has taken place. I show that attributional uncertainty immediately following cyberattacks encourages dependence on a narrow range of elite frames and the assignment of blame to familiar enemies. Over time this promotes conspiratorial thinking and poses a risk to democratic accountability. When seen in light of these broader costs, the attribution problem becomes a vital political concern with implications that reach beyond the scope of elite-focused cybersecurity research.

Sevastopulo, Demetri. 2007. "Chinese Hacked Into Pentagon | Financial Times". Financial Times, September 2007. https://www.ft.com/content/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac.

Background information on the first major Chinese cyber-attack on the United States.

Shane, Scott. 2019. "How a Secret U.S. Cyber weapon Backfired." The New York Times. https://www.nytimes.com/2019/06/04/podcasts/the-daily/nsa-hacking-tool-baltimore.html (June 7, 2019).

Describes the Baltimore attack and the likely source being a weakness identified by the NSA almost a decade prior, using tools stolen from the NSA.

Sharma, Shwadhin and Merrill Warkentin. 2018. "Do I Really Belong? Impact of Employment Status on Information Security Policy Compliance." Computers & Security, November 19: 1-13. https://www-sciencedirect-com.srv-proxy2.library.tamu.edu/science/article/pii/S0167404818304024 (June 27, 2019).

Article focuses on how an employee's status or position in an organization can impact their adherence to information security policies. The authors examined the influx of contractors and temporary employees serving in positions of trust, but with a lower level of institutional investment, in many organizations and examined how can their commitment to abiding to security policies could be obtained. The article also examines if traditional

incentives for compliance and punishments for violations of security policies are effective for temporary, short-term employees.

Shelhart, Mark. 2018. “Why Cyberdefenses Are Worth the Cost.” Journal of Accountancy 226 (5): 1-8, November 1, 2018. http://search.ebscohost.com.srv-proxy2.library.tamu.edu/login.aspx?direct=true&db=bft&AN=132866418&site=eds-live.

Article provides tips for non-profits and other organizations to reduce the risk of potential data breaches. It notes that the most common motivation for an attack is information and money. Nonprofits host an array of potentially valuable information, from donor lists and profiles to employee and client files containing Social Security numbers and other sensitive data. Also points out that many NP’s that are hit by ransomware may prefer to pay the ransom versus the risk of downtime or possible damage to their reputation.

Shoorbajee, Zaid. 2018. "U.S. Intelligence Chief Lays Out Threats to U.S. Infrastructure, Efforts to Protect It". Cyberscoop, July 13, 2018. https://www.cyberscoop.com/dan-coats-hudson-institute/.

Article focuses on Director of National Intelligence Dan Coats' views on Russia being the most aggressive cyber actor.

Smith, Kevin J. and Shira Forman. 2014. “Bring Your Own Device-Challenges and Solutions for the Mobile Workforce” Employment Relations Today. 40(4) 67-73, January 23, 2018; United States: John Wiley and Sons, Ltd. https://online library-Wiley-com.srv-proxy1.library.tamu.edu/doi/epdf/10.1002/err.21436

Article addresses the challenges of Bring Your Own Device (BYOD) in the modern workplace and the advantages/disadvantages and a checklist of possible things to include in the policy.

Stewart, Emily. "Hackers Have Been Holding the City of Baltimore's Computers Hostage for 2 Weeks." Vox. May 21, 2019. Accessed July 05, 2019. https://www.vox.com/recode/2019/5/21/18634505/baltimore-ransom-robbinhood-mayor-jack-young-hackers.

Describes a ransomware attack on the city of Baltimore that occurred in May of 2019 and how the city responded to this cyber-attack.

Sussman, Bruce. "Ransomware Paid: Organization Demands POC from Hackers." Cybersecurity Conferences & News. November 28, 2018. Accessed July 05, 2019. https://www.secureworldexpo.com/industry-news/ransomware-paid-hacker-negotiation.

Describes how a city suffering from a ransomware cyberattack negotiated, paid, and confirmed receipt of a safe decryption tool.

Tamkin, Emily. 2017. "10 Years After The Landmark Attack On Estonia, Is The World Better Prepared For Cyber Threats?" Foreign Policy. https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/.

Utilized author's quote "melding cyber into broader strategies that combine hacks with information war, hybrid war, or old-fashioned conventional war in a bid to advance Moscow's aims".

Tashea, Jason. 2018. "Any piece of technology that stores information could be compromised—even obsolete devices that get thrown out with the garbage" ABA Journal 104 (11): 34, November 1, 2018. http://www.abajournal.com/magazine/article/technology_compromised_obsolete_devices/

QUOTED FROM ABSTRACT: In the normal course of business, they were rolled out the front door along with the electronic health care information of more than 344,000 people, according to a 2013 settlement with the U.S. Department of Health and Human Services. UNDERSTANDING THE RISKS In 2012, the ABA Model Rules of Professional Conduct increased attention on technology's role in legal ethics. "Most lawyers are not trained to deal with the issues associated with inadvertent loss of information or unauthorized loss of information," says John Barkett, a partner at Shook, Hardy & Bacon in Miami and a member of the ABA Standing Committee on Ethics and Professional Responsibility, referencing the updated Model Rule 1.6(a) on confidentiality.

Tchao, E. T., Richard Y. Ansah, and Seth D. Kotey. 2017. "Barrier Free Internet Access: Evaluating the Cyber Security Risk Posed by the Adoption of Bring Your Own Devices to e-Learning Network Infrastructure." International Journal of Computer Applications, Vol. 176, October: 53-62. https://arxiv-org.srv-proxy2.library.tamu.edu/abs/1710.08795? (June 27, 2019).

Assessment of BYOD use on a WLAN network at an academic institution. The network, set-up for BYOD, security risks, and recommendations for mitigation are included in the article. Security recommendations include network segregation, monitoring of the WLAN, user authentication, and mobile device management.

Tehan, Rita. 2018. "Cybersecurity: Legislation, Hearings, and Executive Branch Documents." Congressional Research Service, February 1, 2018. https://www.hsdl.org/?view&did=808139

Congressional Research Service - Cybersecurity: Legislation, Hearings, and Executive Branch Documents: This document details the efforts by Congress (both the Senate and the House of Representatives) efforts to develop and pass legislation relating to cybersecurity. Additionally, there are timelines and synopses of the executive actions done within the cybersecurity realm as well as Congressional hearings on cybersecurity. Rita Tehan emphasized that "Congress has held cybersecurity hearings every year since 2001" (2018, i).

Texas State Legislature. 2015. "Summary Brief: Cybersecurity in Texas and the Texas Cybersecurity, Education and Economic Development Council". Texas Cybersecurity, Education and Economic Development Council (TCEEDC). https://capitol.texas.gov/tlodocs/84R/handouts/C4802016012013001/4e5c0fb0-9e48-41b8-9a7e-1ca41689c18a.PDF

Summary brief provided to the 85th Session of the Texas state legislature by the TCEEDC in 2015 on cybersecurity with three areas of focus: state cybersecurity infrastructure, cybersecurity industry in Texas and state's cybersecurity educational needs. Brief includes committee findings and updates on progress with recommendations made by the TCEEDC in 2012 regarding cybersecurity measures and policies in Texas.

"The DoD Cybersecurity Policy." 2019. CSIAC, October 30, 2019. https://www.csiac.org/resources/the-dod-cybersecurity-policy-chart/ (June 1, 2019).

The goal of the DoD Cybersecurity Policy Chart is to capture the tremendous breadth of applicable policies, some of which many cybersecurity professionals may not even be aware, in a helpful organizational scheme. The use of color, fonts and hyperlinks are all designed to provide additional assistance to cybersecurity professionals

navigating their way through policy issues in order to defend their networks, systems and data. At the bottom center of the chart is a legend that identifies the originator of each policy by a color-coding scheme. On the right-hand side of the Cybersecurity Policy Chart, there are boxes, which identify key legal authorities, federal/national level cybersecurity policies, and operational and subordinate level documents that provide details on defending the DoD Information Network (DoDIN) and its assets. Links to these documents can be found in the Chart.

The Hacker News. 2018. “Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer". https://thehackernews.com/2018/04/iot-hacking-thermometer.html (June 7, 2019).

Describes how a casino was hacked through an Internet of Things (IoT), Wi-Fi capable fish tank thermostat and had data stolen.

Timberg, Craig and Ellen Nakashima. 2013. “Has China Hacked Most of Washington?” Waterloo Region Record, February 21, 2013 http://eds.b.ebscohost.com.srv-proxy2.library.tamu.edu/eds/detail/detail?vid=10&sid=fb087ba5-56e8-41b1-99ac-46cd14a7340d%40pdc-v-sessmgr04&bdata=JnNpdGU9ZWRzLWxpdmU%3d#AN=Q4K378483047213&db=n5h (July 19, 2019).

Brief article that highlights the cyber espionage threat facing law firms, the information industry and think tanks.

Tkacik, John J. 2008. ""Trojan Dragon: China's Cyber Threat."" Executive Summary Backgrounder. The Heritage Foundation. No. 2106. February 8, 2008. 1-14. www.heritage.org/research/AsiaandthePacific/bg2106.cfm

Focuses on the threat from PRC cyber actors and attacks. Offers solutions to mitigate the threat.

Trump, Donald A. 2019. "Executive Order 13870: America's Cybersecurity Workforce". The White House, May 2, 2019. https://www.hsdl.org/?view&did=824839"

From the Document: "America's cybersecurity workforce is a strategic asset that protects the American people, the homeland, and the American way of life. [...] The United States Government must enhance the workforce mobility of America's cybersecurity practitioners to improve

America's national cybersecurity. [...] The United States Government must support the development of cybersecurity skills and encourage ever-greater excellence so that America can maintain its competitive edge in cybersecurity. [...] The United States Government must create the organizational and technological tools required to maximize the cybersecurity talents and capabilities of American workers--especially when those talents and capabilities can advance our national and economic security. [...] In accordance with Executive Order 13800, the President will continue to hold heads of executive departments and agencies (agencies) accountable for managing cybersecurity risk to their enterprises, which includes ensuring the effectiveness of their cybersecurity workforces."

Trump, Donald A. 2018. "National Cyber Strategy of the United States of America" The White House, September 2018. (https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf)

"America's prosperity and security depend on how we respond to the opportunities and challenges in cyberspace. Critical infrastructure, national defense, and the daily lives of Americans rely on computer-driven and interconnected information technologies. As all facets of American life have become more dependent on a secure cyberspace, new vulnerabilities have been revealed and new threats continue to emerge. Building on the National Security Strategy and the Administration's progress over its first 18 months, the National Cyber Strategy outlines how the United States will ensure the American people continue to reap the benefits of a secure cyberspace that reflects our principles, protects our security, and promotes our prosperity."

U.S. Congress. 2014. P.L. 113-282: The National Cybersecurity Protection Act of 2014. December 18, 2014. https://www.hsdl.org/?view&did=765281

Public Law 113-282 – The National Cybersecurity Protection Act of 2014: This law established the national cybersecurity and communications integration center (NCCIC) within the Department of Homeland Security (DHS). According to the stipulations of the law, the functions of the center includes several parameters including being the “Federal civilian interface for the…sharing of information related to cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities…[and] providing shared situational awareness to enable real- time, integrated, and operational actions across the Federal Government and non-Federal

entities to address cybersecurity risks and incidents to Federal and non-Federal entities" (P.L. 113-282, 2014, 3067). Additionally, the NCCIC is responsible for "coordinating the sharing of information related to cybersecurity risks and incidents… [and] facilitating cross-sector coordination… including cybersecurity risks and incidents that may be related or could have consequential impacts across multiple sectors" (P.L. 113-282, 2014, 3067).

U.S. Congress. 2015. Public Law 114-113: Consolidated Appropriations Act, 2016. December 18, 2015. https://www.congress.gov/114/plaws/publ113/PLAW-114publ113.pdf and https://www.dni.gov/index.php/ic-legal-reference-book/cybersecurity-act-of-2015

Public Law 114-113 – Consolidated Appropriations Act of 2016: Division N of the Consolidated Appropriations Act of 2016 is the Cybersecurity Act of 2015. This broad grouping includes the Cybersecurity Information Sharing Act of 2015, National Cybersecurity Protection Advancement Act of 2015, Federal Cybersecurity Enhancement Act of 2015, and the Federal Cybersecurity Workforce Assessment Act of 2015. While this may seem like outdated information, Section 401 of this Act specifically addresses a study on the use of mobile devices by government employees. It stated that "the Secretary of Homeland Security, in consultation with the Director of the National Institute of Standards and Technology, shall complete a study on threats relating to the security of the mobile devices of the Federal Government; and submit an unclassified report to Congress…that contains the findings of such study, the recommendations developed … [and] the deficiencies" (P.L. 114-113 2015, 2977).

United States Department of Justice. 2019. "Elements of the Offense Under 18 U.S.C. § 1831". Criminal Resource Manual, 1124-1128. https://www.justice.gov/jm/criminal-resource-manual-1124-elements-offense-under-18-usc-1831. (July 19, 2019).

Federal laws pertaining to economic espionage by state actors.

United States Department of Justice. 2019. "Elements of the Offense Under 18 U.S.C. § 1832". Criminal Resource Manual, 1129 - 1135. https://www.justice.gov/jm/criminal-resource-manual-1129-elements-offense-under-18-usc-1832 (July 20, 2019).

Federal laws pertaining to economic espionage by non-state or private sector actors.

United States of America. Securities and Exchange Commission. 17 CFR Parts 229 and 249, February 26, 2018. Commission Statement and Guidance on Public Company Cybersecurity Disclosures. Release Nos. 33-10459; 34-82746.

Provides guidance from the United States Government on requirements of companies with publicly traded stocks to report suffering a cyberattack.

Vaas, Lisa. 2013. “Doctors Disabled Wireless in Dick Cheney's Pacemaker to Thwart Hacking.” Naked Security. https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/ (June 9, 2019).

Discuss the need to disable the former Vice President's Wi-Fi enabled pacemaker as a security risk.

Valdes, Manuel. 2012. “If You Want A Job, You May Have To Turn Over Your Facebook Password.” Business Insider. https://www.businessinsider.com/empoyers-ask-for-facebook-password-2012-3 (June 9, 2019).

Reporting on companies demanding Social Media Logins during hiring process.

Vashisth, Akanksha and Avinash Kumar. 2013. "Corporate Espionage: The Insider Threat." Business Information Review. Volume 30, No. 2, 83-90, June 2013. https://journals-sagepub-com.srv-proxy1.library.tamu.edu/doi/pdf/10.1177/0266382113491816

Article contains an overview of economic espionage and its definition. The authors then attempt to explain the factors which can cause individuals to commit economic espionage by using data models. The intersection between the individual and the organizational environment is also addressed as a possible factor.

Villasenor, John. 2015. "Corporate Cybersecurity Realism: Managing Trade Secrets in a World Where Breaches Occur." AIPLA Quarterly Journal, volume 43, Spring/Summer 2015. https://heinonline-org.srv-

proxy1.library.tamu.edu/HOL/Page?collection=journals&handle=hein.journals/aiplaqj43&id=344&men_tab=srchresults

Focuses on corporate trade secrets and legal protections in the USA and internationally and then moves into an examination of cybersecurity and trade secrets. Provides recommendations for corporations to protect their trade secrets from cyber and insider threats.

Wall, Andy. 2018. "Security Assurance and the Ethics of Background Checks." ITNOW. Volume 60, Issue 3, 40-41, September 2019. https://academic-oup-com.srv-proxy1.library.tamu.edu/itnow/article/60/3/40/5088167

Article reviews the reasons for employee screening, discusses related ethical issues related to screening and background checks, and describes steps organizations can take to ensure the screening process is necessary, ethical, and fairly applied.

Washenko, Anna. 2019. "Microsoft is adding a protected section to its cloud storage". Izod Media, June 26, 2019. https://izodnews.com/2019/06/26/microsoft-onedrive-gets-a-more-secure-personal-vault-plus-additional-storage-options-ars-technica/

Brief article that discusses security updates to Microsoft's OneDrive cloud storage system, including a two-factor authentication system that logs the user out automatically after a period of inactivity.

Weinberg, Neal. 2013. "How to Blunt Spear Phishing Attacks". Network World, March 6, 2013. https://www.networkworld.com/article/2164139/how-to-blunt-spear-phishing-attacks.html.

Utilized statistic concerning the prevalence of spear phishing in successful network intrusions.

Wieners, Eva 2019. "What is a Baseline Study?" https://proposalsforngos.com/what-is-a-baseline-study/

Article defines a baseline study and how to compare research results to the baseline.

Wong, Wayne. 2012. "BYOD: The Risks of Bring Your Own Device." Risk Management 59 (5): 9, June 1, 2012. http://eds.b.ebscohost.com.srv-proxy1.library.tamu.edu/eds/pdfviewer/pdfviewer?vid=1&sid=a03f78f8-e15c-4e4f-a726-e6ffd7e3d59b%40sessionmgr103

Short journal article with 5 tips for organizations wishing to allow BYOD devices in the workplace: 1) Have a Policy & Communicate It; 2) Know Regulatory Requirements; 3) Back Up Often; 4) Be Aware of Your "Personas"; and 5) Know Who Owns What.

Worktime. 2019. "USA Employee Monitoring Laws: What Are Employers Allowed and not Allowed Doing in the Workplace?" Worktime, August 19, 2019. https://www.worktime.com/usa-employee-monitoring-laws-what-can-and-cant-employers-do-in-the-workplace

Article supports the employer's right to ensure workers are doing what they are paid to do but cautions against privacy invasions into personal phone calls even on company phones. Again, the article discusses the use of monitoring agreements.

Young, Douglas. 2019. "The Promise and Peril of AI: Q&A with Douglas Yeung". RAND Corporation, Washington DC, February 27, 2019. https://www.rand.org/blog/rand-review/2019/02/the-promise-and-perils-of-ai-qa-with-douglas-yeung.html

Article addresses artificial intelligence and the concern that there is bias in any intelligence. Programmers are biased and therefore cannot create an unbiased AI tool. Concern is as a civilization we begin relying on AI and do not consider the bias that is programmed into these decision assist tools.

Zimmermann, Verena, and Karen Renaud. 2019. "Moving from a 'Human-as-Problem" to a "Human-as-Solution" Cybersecurity Mindset." International Journal of Human-Computer Studies Vol 131, November 2019, pgs 169-187. https://www.sciencedirect.com/science/article/pii/S1071581919300540

"QUOTED FROM ABSTRACT: Cybersecurity has gained prominence, with a number of widely publicized security incidents, hacking attacks and data breaches reaching the news over the last few years. The escalation in the numbers of cyber incidents shows no sign of abating, and it seems appropriate to take a look at the way cybersecurity is conceptualized and to consider whether there is a need for a mindset change. To consider this question, we applied a "problematization" approach to assess current conceptualizations of the cybersecurity problem by government, industry and hackers. Our analysis revealed that individual human actors, in a variety of roles, are generally considered to be "a problem". We also

discovered that deployed solutions primarily focus on preventing adverse events by building resistance: i.e. implementing new security layers and policies that control humans and constrain their problematic behaviors. In essence, this treats all humans in the system as if they might well be malicious actors, and the solutions are designed to prevent their ill-advised behaviors. Given the continuing incidences of data breaches and successful hacks, it seems wise to rethink the status quo approach, which we refer to as “Cybersecurity, Currently”. In particular, we suggest that there is a need to reconsider the core assumptions and characterizations of the well-intentioned human’s role in the cybersecurity socio-technical system. Treating everyone as a problem does not seem to work, given the current cyber security landscape. Benefiting from research in other fields, we propose a new mindset i.e. “Cybersecurity, Differently”. This approach rests on recognition of the fact that the problem is actually the high complexity, interconnectedness and emergent qualities of socio-technical systems. The “differently” mindset acknowledges the well-intentioned human’s ability to be an important contributor to organizational cybersecurity, as well as their potential to be “part of the solution” rather than “the problem”. In essence, this new approach initially treats all humans in the system as if they are well-intentioned. The focus is on enhancing factors that contribute to positive outcomes and resilience. We conclude by proposing a set of key principles and, with the help of a prototypical fictional organization, consider how this mindset could enhance and improve cybersecurity across the socio-technical system."

Zurkus, Kacy. 2019. “Security Considerations in a BYOD Culture”. DarkReading/TheEdge, July 19, 2019. https://www.darkreading.com/edge/theedge/security-considerations-in-a-byod-culture/b/d-id/1335178

Article describes email phishing that makes Outlook look different on a smartphone.