CYBER SECURITY NEED & Cyber Security Detection Frameworks

Author:
Araga Babu Rajendra Prasad Reddy
Research Scholar
Hyderabad
India

ABSTRACT

Cyber Security is the process and techniques involved in protecting sensitive data, computer systems, networks, and software applications from cyber attacks. The cyber attacks are general terminology that covers a large number of topics, but some of the popular are:

- *Tampering systems and data stored within*
- *Exploitation of resources*
- *Unauthorized access to the targeted system and accessing sensitive information*
- *Disrupting the normal functioning of the business and its processes*
- *Using ransomware attacks to encrypt data and extort money from victims*

The attacks are now becoming more innovative and sophisticated that can disrupt the security and hacking systems. So it's very challenging for every business and security analyst to overcome this challenge and fight back with these attacks.

It defines the rules that limit access to information. Confidentiality takes on the measures to restrict sensitive information from being accessed by cyber attackers and hackers.

In an organization, people are allowed or denied access to information according to its category by authorizing the right persons in a department. They are also given proper training about the sharing of information and securing their accounts with strong passwords.

Proper measures should be taken in an organization to ensure its safety. File permissions and user access control are the measures controlling the data breach. Also, tools and technologies should be implemented to detect any change or a breach in the data. Various organizations use a checksum and even cryptographic checksum to verify the integrity of data.

To understand the need for Cyber Security measures and their practices, let's have a quick look at the types of threats and attacks.

Keywords *Cyber-Attack, Cyber-Security, Ransumwear*

1. What Is Cybersecurity?

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.
These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes.

Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

Don't lend your phone to someone you don’t know—they can do damage even in a short time. Shred any printouts of work documents. Use corporate- or IT-approved tools to connect. 4 6 5 Maintain your privacy-safe practices so you’re prepared to work remotely whenever needed. 10 Use privacy screens to shield personal or confidential information from others (yes, even at home). Use virtual backgrounds if you need to shield pictures or information Turn off your home virtual assistant while having private conversations. Top 10 Privacy Tips: Work from home (or anywhere) safely Opt for Multi-factor authentication whenever possible. Get explicit consent from co-workers, family, and friends if using their picture, video, or voice. Don’t use personal information in your passwords or security questions. Need help keeping track of your unique passwords? Use a password manager. 7 9 8 1 3 2 For more information, visit trust.cisco.com

Cybersecurity is the most concerning matter as cyber threats and attacks are overgrowing.

Attackers are now using more sophisticated techniques to target the systems. Individuals, small-scale businesses, or large organizations are all being impacted. So, all these firms, whether IT or non-IT firms, have understood the importance of Cyber Security and focusing on adopting all possible measures to deal with cyber threats.

With the game up for cyber threats and hackers, organizations and their employees should take a step ahead to deal with them. As we like to connect everything to the internet, this also increases the chances of vulnerabilities, breaches, and flaws.

Gone are the days when passwords were enough to protect the system and its data. We all want to protect our personal and professional data, and thus Cyber Security is what you should know to ensure data protection.

So, let's being with defining the term Cyber Security….

What is Cyber Security?

Cyber Security is the process and techniques involved in protecting sensitive data, computer systems, networks, and software applications from cyber attacks. The cyber attacks are general terminology that covers a large number of topics, but some of the popular are:

- Tampering systems and data stored within
- Exploitation of resources
- Unauthorized access to the targeted system and accessing sensitive information
- Disrupting the normal functioning of the business and its processes
- Using ransomware attacks to encrypt data and extort money from victims

The attacks are now becoming more innovative and sophisticated that can disrupt the security and hacking systems. So it's very challenging for every business and security analyst to overcome this challenge and fight back with these attacks.

To understand the need for Cyber Security measures and their practices, let's have a quick look at the types of threats and attacks.

2. Ransomware

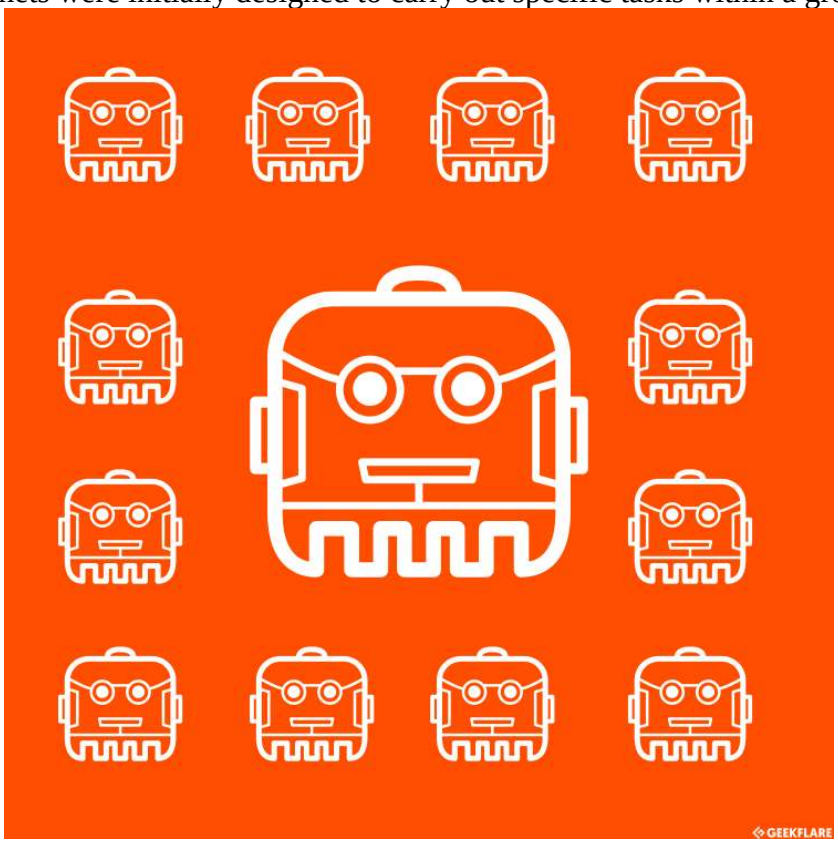
Ransomware is a file encryption software program that uses a unique, robust encryption algorithm to encrypt the files on the target system.

The authors of the Ransomware threat generate a unique decryption key for each of its victims and save it on a remote server. Thus, users cannot access their files by any application.

The ransomware authors take advantage of this and demand a considerable ransom amount from the victims to provide the decryption code or decrypt the data. But such attacks have no guarantee of recovery of data even after paying the ransom.

3. Botnets Attacks

Botnets were initially designed to carry out specific tasks within a group.



It is defined as a network or group of devices connected with the same network to execute a task. But this is now being used by bad actors and hackers that attempt to access the network and inject any malicious code or malware to disrupt its working. Some of the botnet attacks include:

- Distributed Denial of Service (DDoS) attacks
- Spreading spam emails
- Stealing of confidential data

Botnets attacks are generally carried out against large-scale businesses and organizations due to their huge data access. Through this attack, the hackers can control many devices and compromise them for their evil motives.

4. Social Engineering Attacks

Social engineering is now a common tactic used by cybercriminals to gather user's sensitive information.

It may trick you by displaying attractive advertisements, prizes, huge offers, and asking you to feed your personal and bank account details. All the information you enter there is cloned and used for financial fraud, identity fraud, and so.

It is worth saying about the ZEUS virus that is active since 2007 and is being used as a social engineering attack method to steal the victims' banking details. Along with financial losses, Social engineering attacks can download other destructive threats to the concerned system.

5. Cryptocurrency Hijacking

Cryptocurrency hijacking is the new addition to this cyber world.

As digital currency and mining are becoming popular, so it is among cybercriminals. They have found their evil benefit to crypto-currency mining, which involves complex computing to mine virtual currency like Bitcoin, Ethereum, Monero, Litecoin, etc.

Cryptocurrency investors and traders are the soft targets for this attack.

Cryptocurrency hijacking is also known as "Cryptojacking". It is a program designed to inject mining codes silently into the system. Thus the hacker silently uses the CPU, GPU, and power resources of the attacked system to mine for the cryptocurrency.

The technique is used to mine Monero coins particularly. As mining is a complex process, it consumes most of the CPU resources, impacting the system's performance. Also, it is done under all your expenses so that the victim may get a huge electricity bill and internet bill.

It also lessens the lifespan of the affected device.

6. Phishing

Phishing is a fraudulent action of sending spam emails by imitating to be from any legitimate source.

Such mails have a strong subject line with attachments like an invoice, job offers, big offers from reputable shipping services, or any important mail from higher officials of the company.

The phishing scam attacks are the most common cyber attacks that aim to steal sensitive data like login credentials, credit card numbers, bank account information, etc. To avoid this, you should learn more about phishing email campaigns and their preventive measures. One can also use email filtering technologies to avoid this attack.

Along with these, 2019 will seek the potential in biometric attacks, AI attacks, and IoT attacks. Many companies and organizations are witnessing large-scale cyber-attacks, and there is no stop for them. Despite the constant security analysis and updates, the rise of cyber-threat is consistent. Thus, it is worth educating yourself on the basics of cybersecurity and its implementations.

7. The key concept of Cyber Security

Cyber Security is a very broad term but is based on three fundamental concepts known as "**The CIA Triad**".

It consists of Confidentiality, Integrity, and Availability. This model is designed to guide the organization with the policies of Cyber Security in the realm of Information security.

Confidentiality

It defines the rules that limit access to information. Confidentiality takes on the measures to restrict sensitive information from being accessed by cyber attackers and hackers.

In an organization, people are allowed or denied access to information according to its category by authorizing the right persons in a department. They are also given proper training about the sharing of information and securing their accounts with strong passwords.

They can change the way data is handled within an organization to ensure data protection. There are various ways to ensure confidentiality, like two-factor authentication, data encryption, data classification, biometric verification, and security tokens.

Integrity

This assures that the data is consistent, accurate, and trustworthy over its time period. It means that the data within the transit should not be changed, altered, deleted, or illegally being accessed.

Proper measures should be taken in an organization to ensure its safety. File permissions and user access control are the measures controlling the data breach. Also, tools and technologies should be implemented to detect any change or a breach in the data. Various organizations use a checksum and even cryptographic checksum to verify the integrity of data.

To cope with data loss or accidental deletion, or even cyberattacks, regular backups should be there. Cloud backups are now the most trusted solution for this.

Availability

Availability in terms of all necessary components like hardware, software, networks, devices, and security equipment should be maintained and upgraded. This will ensure the smooth functioning and access of Data without any disruption. Also, providing constant communication between the components through providing enough bandwidth.

It also involves opting for extra security equipment in case of any disaster or bottlenecks. Utilities like firewalls, disaster recovery plans, proxy servers, and a proper backup solution should ensure to cope with DoS attacks.

For a successful approach, it should go through multiple layers of security to ensure protection to every constituent of CyberSecurity. Particularly involving computers, hardware systems, networks, software programs, and the shared data.

Cyber Security Detection Frameworks

If you spend enough time in or around the cyber security industry, you will often hear the term "*cyber security framework*" mentioned. In this article, I will be briefly covering several common cyber security detection frameworks used by organizations to help understand adversary behavior during a cyber-attack.

What is a Cyber Security Framework?

A cyber security framework is a collection of standards, guidelines, procedures and best practices intended to help an organization defend itself from cyber attacks or data breaches. They are used by organizations to achieve security objectives and are often mandatory, or at least strongly encouraged, for companies that want to comply with state, industry, and international cybersecurity regulations.

List of Cybersecurity Frameworks.

There are many different types of frameworks that exist within the cybersecurity industry today, which aim to achieve different security objectives. For example, in order to handle credit card transactions, a business must pass an audit attesting to its compliance with the Payment Card Industry Data Security Standards (PCI DSS) framework. Another example would be an organization using the NIST Special Publication 800–53 Revision 5 to implement security and privacy controls. It is also common to see organizations implement more than one framework to achieve their objectives.

9. Technical Security Controls: Encryption, Firewalls & More

9.1 Security Controls

Technical security controls include any measures taken to reduce risk via technological means. They stand in contrast to physical controls, which are physically tangible, and administrative controls, which focus on managing people. Common technical controls include encryption, firewalls, anti-virus software, and data backups.

These types of security control aren't mutually exclusive. Security cameras, for example, are both a technical and a physical control. And password management frequently bridges the gap between technical and administrative controls.

Security controls can also be distinguished based on their goal:

- Preventative controls aim to prevent security incidents;
- Detective controls aim to detect incidents as they happen, or after the fact;
- Corrective controls aim to mitigate the impact once an incident has occurred;
- Deterrent controls aim to deter attackers from making an attempt;
- Compensating controls can be used in case another control won't work.

Technical security controls can serve all of the above purposes. Below, we'll discuss some common technical controls.

9.2 Encryption

Encryption is a protective technical control that scrambles information so that unauthorized users cannot access it. Through encryption, legible "plaintext" is converted into "ciphertext" that appears to be a gibberish of seemingly random characters.

But encryption isn't random. Instead, it uses algorithms and patterns to render the data illegible. If a user has the right key, they can then unscramble the data and access it.

Encryption is a protective control: the goal is to prevent unauthorized users from accessing data.

A firewall monitors incoming and outgoing network traffic and blocks any unwanted traffic. It's essentially a border between one network and another – most often between a private network and the internet.

Once in place, a firewall inspects all traffic going into or out of a network. If a given packet of information breaks the firewall's preset rules, it can then block that packet from passing.

A firewall is a detective and a preventative technical control: it both monitors for threats and prevents them from accessing the network.

Antivirus Software

Antivirus software runs in the background of a device, constantly monitoring for threats. Whenever you download or open a new file, the antivirus software quickly scans it for viruses and other malware.

Periodically, your antivirus software will also run a more comprehensive scan of your device. If it ever detects something fishy, it will typically notify the user and ask what action they'd like to take. Like a firewall, antivirus software is both a detective and preventative control.

Once upon a time, users had to install third-party antivirus software to protect their computers. But these days, firewalls and antivirus software come built into most consumer operating systems by default.

9.3 Password Management

Password management straddles the line between administrative and technical controls. If a company has a clear password policy, that's an administrative control. If the company uses technology to enforce it – say, by requiring passwords to be a certain length – it's also a technical control.

Password requirements are preventative controls by nature. By requiring a password meet a certain level of complexity, the policy prevents simple brute force attacks from cracking the password in a matter of minutes. Multi-factor authentication is also preventative, making it considerably harder for attackers to break into someone's account.

If a password system locks users out after a certain number of attempts, it also counts as a deterrent control. And if the system alerts a user via email or text that multiple failed attempts just occurred, it's also a detective control, alerting the person or organization that an attack may have been attempted.

9.4 Backups

Backups are a great example of a corrective security control. If a server rack goes up in smoke, you could lose key systems or data. But if you have a backup copy of the data, you can restore much or all of the information lost.

There's more than one way to backup data. Some organizations might do a full backup on a daily basis. Others might rely on incremental backups, which only backup files that have changed since the most recent backup.

Note that although backups are certainly a technical control, they may also count as an administrative control if the organization has a clear backup policy in place.

9.5 Physical Security Systems

Physical security systems often coincide with technical controls. Security cameras and motion sensors count as both. These systems can both detect and deter against attacks. A camera is by its nature designed to spot intruders, and the presence of cameras can also discourage people from even making an attempt to break in.

Security isn't just about keeping out trespassers. A fire alarm and sprinkler system mitigates risk just as much as a security system does, qualifying it as a physical and technical corrective security control.

9.6 Governance

The governance building block covers the processes that direct a utility-wide cybersecurity effort and provide accountability for that effort. Cybersecurity governance requires the understanding and action of those at the very top level of the utility, such as the executive director, chief executive officer (CEO), board of directors, and others.

Importance Intersections With Other Building Blocks Process and ActionsEssential DataWebinarRecommended Reading Additional Resources

Power sector cybersecurity *governance* provides oversight for a utility's cybersecurity efforts. Through governance, the utility board of directors, chief executive officer (CEO), executive leadership, and other decision makers seek to balance resource allocation, risk, and business objectives. These leaders must factor in the risk associated with cyberattacks, as well as the need to comply with national, regional, provincial, or state cybersecurity regulations. Their role is to look at cybersecurity holistically, factoring in data about current cyber vulnerabilities as well as the impact of anticipated system upgrades, increased digitalization, and system expansion.

9.7 Importance

If the upper levels of an organization do not demonstrate commitment to cybersecurity, the utility's efforts to improve cybersecurity will enjoy little success (if any). One way to demonstrate that commitment is through allocation of resources to pay for staff time, tools, and, possibly, outside consultation. Cybersecurity governance needs to ensure those resources go where they are really needed—it is easy for organization-wide cybersecurity programs to become "lopsided," investing too much in one area and not enough in another. Cybersecurity governance includes the work of making sure overall security efforts effectively meet the needs of the utility.

Another way for utility leadership to demonstrate commitment is by impressing on staff that everyone has a role to play in cybersecurity. They must communicate this through words as well as actions, leading by example. If staff see leadership flouting cybersecurity policies and guidelines, they will quickly realize that leadership is not serious about this topic. By "walking the walk" as well as "talking the talk," leaders can foster a culture of cybersecurity that will help protect the utility from future cyberattacks. (For more on this topic, see the cybersecurity awareness training building block.)

9.8 Intersections With Other Building Blocks

The **governance** building block provides input (through executive directives) that informs the development of the organizational security policy, the document that defines the utility's cybersecurity efforts. The decision makers of the governance building block determine what cybersecurity will look like; the organizational security policy captures these decisions and presents them as actionable measures to be taken.

Governance must include compliance with all applicable regulations, so a high-level summary of regulatory requirements is provided by the compliance building block.

Governance must set the risk objectives and business requirements that define the scope of the utility's **risk management** building block.

These organizational security policy, compliance, and risk management building blocks have the most interaction with governance; however, the governance building block also relies on data, reports, and other types of information from all other building blocks that might inform high-level decision-making.

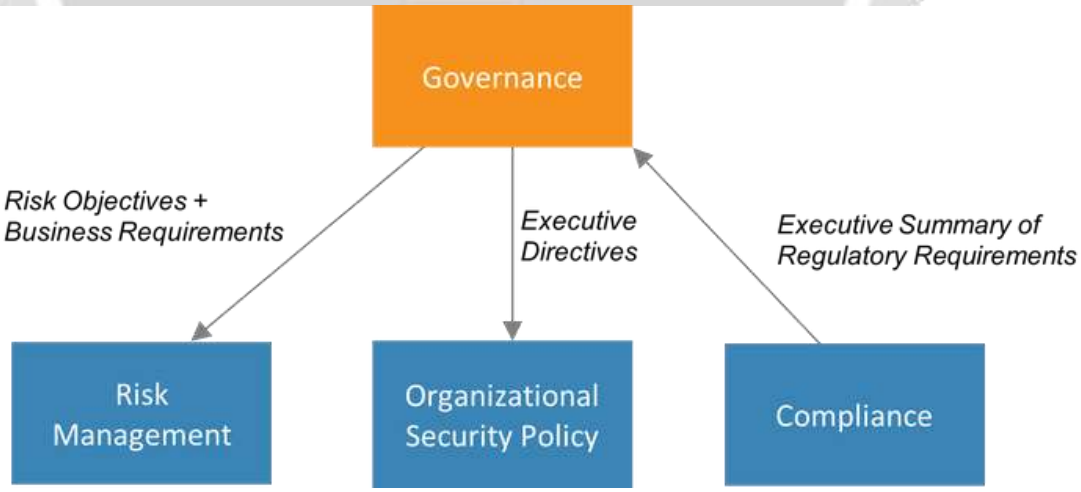


Figure 1. Information passed to and from the governance building block

9.9 Process and Actions

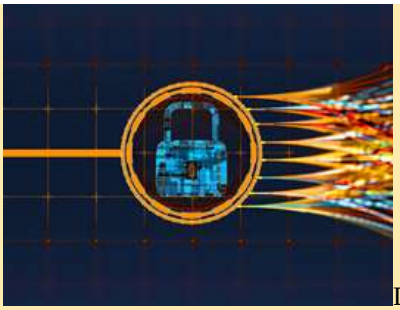
The **governance** building block integrates the work of other building blocks, so there is overlap between the governance processes and actions and those in other building blocks throughout this document. Table 1 maps

governance processes from the Framework for Improving Critical Infrastructure Cybersecurity from the United States National Institute of Standards and Technology (NIST) to the building blocks that provide detail on each. In the context of the NIST framework, these processes are subcategories within the category of governance.

Table 1. NIST Governance Processes

From the NIST *Framework*
"Organizational cybersecurity policy is established and communicated."
"Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners."
"Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed."
"Governance and risk management processes address cybersecurity risks."

Assigning roles and responsibilities (second row in Table 1) is uniquely a cybersecurity governance activity. The utility's high-level decision makers must determine who will execute which parts of their cybersecurity policy and set up the necessary reporting and oversight structures needed to ensure those responsibilities are fulfilled.



DERCF assessments address governance, technical management, and physical security. DERCF can be used for free as a self-assessment tool, and users can take the assessment as an anonymous guest of the system. (In that case, the utility does not need to identify itself by name, and no data associated with the assessment is stored on the DERCF system.) NREL can also guide utilities through DERCF assessments; some utilities appreciate the participation of an outside party that can facilitate the process and communicate results to utility leadership. To learn more about DERCF, visit https://dercf.nrel.gov**.**

This oversight requires a certain level of cybersecurity knowledge on the part of those decision makers. Unfortunately, not all leaders have the necessary knowledge in this area (Rothrock, Kaplan, and Van der Oord 2017). CEOs or board directors do not need to be experts in cybersecurity, but they need enough understanding to make informed decisions. Some commercial entities offer executive and board cybersecurity readiness programs (Tyler Cybersecurity n.d.). Some associations also offer guidance to boards of directors (NACD 2020) with select excerpts from those resources available online (Bew n.d.). These resources offer some ways these decision makers can acquire the requisite knowledge for executing their cybersecurity responsibilities.

For utilities that wish to benchmark the state of their cybersecurity governance, an assessment is available from the National Renewable Energy Laboratory (NREL). The Distributed Energy Resource Cybersecurity Framework (DERCF) assessment tool covers three areas, one of which is governance. See box at above for details.

Essential Data

Utilities should collect or generate the data below for effective governance.

- High-level information on regulatory requirements. This is generated in the **compliance** building block.
- High-level information on risk, threats, and vulnerabilities affecting the utility. This is collected from cyber threat intelligence (CTI) and distilled by the **risk management** building block.
- Budget information. How much can the utility spend on cybersecurity? How much will compliance cost, and how much is left over to mitigate risks not covered by compliance efforts?
- Internal equipment resources. What tools and technology does the utility have for their cybersecurity efforts?
- Internal human resources. What cybersecurity expertise does the utility have in-house for the various cybersecurity activities that need to be performed? Also, how well do all the staff understand the basics of responsible, cyber-safe use of computers? (See the **cybersecurity awareness training** building block.)
- External resources. Where might the utility get outside help such as advice, consultation, and training? These resources could include government agencies, academics, commercial training enterprises, consultants, or not-for-profit entities.

8. Conclusion

1. The above are just a few examples of common technical controls. The National Institute of Standards and Technology lists dozens of security controls in SP 800-53, and even their list is by no means conclusive. Any measure that attempts to mitigate risk through the use of technology qualifies as a technical security control
2. In an organization, to accomplish an effective Cyber Security approach, the peoples, processes, computers, networks, and technology of an organization, either big or small, should be equally responsible. If all components complement each other, it is very much possible to stand against the tough cyber threat and attacks.

9. References

1. **Bew, Robyn. "Five Principles for Stronger Board Oversight of Cybersecurity." BRINK–News and Insights on Global Risk. Accessed January 5, 2019.**
2. **Cybersecurity & Infrastructure Security Agency. "Cybersecurity Governance." Cybersecurity & Infrastructure Security Agency. October 27, 2019.**
3. **Educause. "Information Security Governance." Accessed January 4, 2019.**
4. **NIST. 2018. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*.**
5. **ANSI Webstore. "ISO/IEC 38500:2015 - Information Technology - Governance of IT for the Organization." Accessed January 4, 2019.**
6. **Atkinson, Sean. "Breaking the Divide Between Governance and Operational Cybersecurity." Center for Internet Security. April 10, 2018.**
7. **Bodeau, Deb, Steve Boyle, Jenn Fabius-Greene, and Rich Graubart. 2010. *Cyber Security Governance: A Component of MITRE's Cyber Prep Methodology.* MITRE Corporation.**

8. **Box. "Simplify Your IT Governance Strategy." Accessed January 4, 2019.**
9. **Burke, Brandon. "Governance vs Compliance." April 3, 2019.**
10. **Fontaine, David, and John Stark. "Cybersecurity: The SEC's Wake-up Call to Corporate Directors." The Harvard Law School Forum on Corporate Governance (blog). March 31, 2018.**
11. **Swinton, Seth, and Stephanie Hedges. "Cybersecurity Governance, Part 1: 5 Fundamental Challenges." Insider Threat Blog (blog). July 25, 2019.**
12. **Veltsos, Christophe. "Board Directors Need to Get Involved With Cyber Risk Governance." Security Intelligence. August 24, 2017.**