MICHAEL CORCIONE
PARTNER
HKA

Best Practices Can Help Owners Mitigate Growing Vendor and Third-Party Cybersecurity Risk

Introduction
Technological advances over the last decade have benefitted myriad market sectors, including construction project owners in both the public and private sectors. Threats to the safe, secure use of technology have evolved just as quickly.

Cyber-attackers are becoming increasingly sophisticated, moving from one industry to another as businesses and entire markets assess and shore up their vulnerabilities. Cyber-attackers also are constantly changing their tactics as new vulnerabilities arise. When one route of access is blocked, they look for others.

In recent years, cyber-attackers have begun targeting vendors and third parties that public and private owners rely upon to operate and serve their customers or stakeholders. Cyber-attackers have preyed upon vendors' cyber weaknesses to gain access to the systems of hospitals, banks and financial services firms, major retailers, utilities, transportation systems and water treatment plants and other critical infrastructure.

While technology has played a central role in owners' success, it also has opened new areas of risk, especially when owners use outside vendors or third parties to perform certain functions or manage certain systems. And, while some owners' security controls may be well hardened, those of their vendors may be more easily breached, leaving owners scrambling to find ways to simultaneously embrace technological innovation while ensuring that doing so doesn't expose them to new, unanticipated risks. It's a balancing act that isn't easy, but is achievable through careful planning, objective monitoring, and diligent management.

Section 1 –Growing Cybersecurity Risks for Public and Private Owners

1.1 Recent Cybersecurity Attacks

Cyberattacks are growing exponentially across the globe, with a marked increase in 2020 and 2021. As stated by the Center for Strategic and International Studies (CSIS), cybercrime cost governments and businesses more than $945 billion during 2020—nearly double the losses reported just two years earlier, in 2018[1] The trend shows no sign of slowing down in 2021, as private companies and government entities throughout the world continue to be pummelled by cyberattacks from a handful of known threat actors. Owners in the US are no exception and have been directly and indirectly impacted by a host of cyberattacks.

In February, Hyundai's subsidiary, Kia Motors, reportedly was hacked with ransomware, causing widespread IT and systems outages. Although a hacker gang said it demanded 20 million, Hyundai has not acknowledged the hack or the ransom.[2]

Also in February, just two days before the National Football League's Super Bowl LV, a cyber-attacker compromised a remote-access program at a water treatment plant in nearby Oldsmar, Florida, in an attempt to poison the town's water supply.[3]

HKA

In March, insurer CNA was targeted by a ransomware attack that encrypted computers of remote-working employees, amongst an estimated 15,000 devices.[2]

The U.S. Department of State was targeted in March, when suspected Russian hackers breached the department's secure email server, stealing thousands of emails and contained information.[3]

Also in March, Microsoft revealed vulnerabilities in their email software as cyber threat actors attempted to steal data and information from more than 30,000 worldwide organizations. Many of these targeted organizations include government agencies, defense contractors, legislative bodies, law firms, and infectious disease researchers. [3]

In April, computer manufacturer Quanta, one of Apple's primary business partners, was attacked by hackers who demanded a $50 million ransom and threatened to release sensitive Apple-related documents if it wasn't paid. Quanta refused to negotiate, however, and Apple has yet to acknowledge the breach.[2]

In mid-April, a hacker group claimed to have stolen 500 GB of confidential data, including financial information and contracts from the Houston Rockets basketball team. Although the group threatened to make the stolen documents public, no ransom payment was made.[2]

The Metropolitan Transportation Authority in New York also was reportedly targeted in April, but the agency reported that hackers were ultimately unable to gain access.3 In addition, hackers in April exploited remote access and VPN vulnerabilities to target defense contractors and other organizations in the US and other locations.[3]

In late April, the largest refined oil pipeline system in the US, the Colonial Pipeline, was the target of a ransomware attack, which cost owners nearly $5 million and led to a days-long shutdown of the pipeline and concerning fuel shortages in the eastern United States. The gang behind the attack reportedly targeted the firm's internal business network and their billing system.[2]

In the same month, it was revealed that threat actors targeted the secure remote-access devices of many organizations, including Verizon and the Metropolitan Water District of Southern California. This remote-access platform is popular among government agencies and private firms. While the hack had been discovered in April, most of the details and scope was made public in June.[3]

In May, the same group that allegedly attacked the Colonial Pipeline targeted Brenntag, a German chemical and ingredients distribution company. Approximately 150 GB of data was stolen, for which Brenntag paid $4.4 million in Bitcoin to recover.[2]

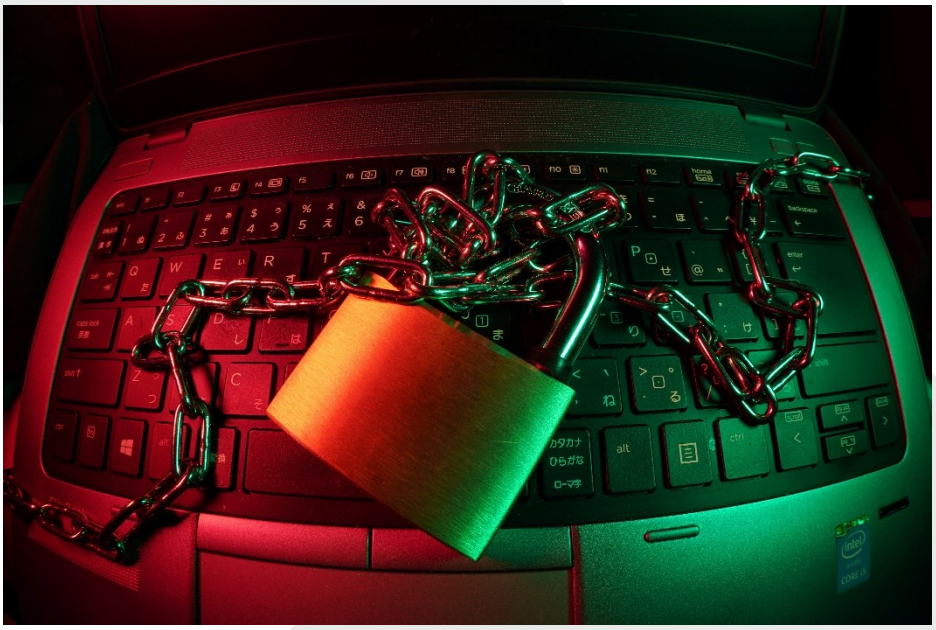
Computer company Acer also was attacked in May, when threat actors gained access to Acer's files through a detected vulnerability in a Microsoft Exchange server. They demanded a $50 million ransom—the largest ransom demanded to-date.[2]

Brazil-based JBS Foods, the world's largest processor of fresh beef and pork and a primary source of meat for the US, was the victim of a cyberattack in May as well. The same group that reportedly attacked Acer was paid $11 million in Bitcoin by JBS as ransom making the payment the largest paid to-date.[2]

HKA

In June, officials in both the US and Britain announced that between 2019 and 2021, hackers with ties to Russia had attempted to access the systems of hundreds of government and private sector organizations worldwide. Access was attempted through organizations' Microsoft Office 365® cloud-based platforms, officials said.[3]

In July, US-based information technology firm Kaseya reported that it had been the victim of a cyberattack that affected between 800 and 1,500 small businesses throughout the world. Hackers demanded $70 million to free the paralyzed computers and release stolen data. Kaseya makes software tools, primarily for IT providers retained by smaller businesses that don't have in-house resources.[4]



1.2 Cyber Threat Landscape

The cyber threat landscape is primarily comprised of threat-actors, vulnerabilities, and attack points. Threat-actors include nation states, "hacktivists," criminal organizations, terrorists, competitors, and malicious or negligent employee or other insiders.

Vulnerabilities are weakness that threat-actors will seek out and try to compromise. Vulnerabilities can be computer system weaknesses including a lack of patching or outdated software, poor access controls such as weak passwords and not using multi-factor authentication, and poor end-user knowledge.

Attack points are the number of targets a threat actor can comprise to expose risk. The more connection points, applications, devices, users, vendors and third parties being used, the higher the likelihood that a threat-actor will expose—and exploit—a vulnerability.

Motivated attackers will try various methods to achieve their mission. Understanding your organization's threat landscape is critical to reducing your cyber-risk. It is also crucial to understand that, when engaging with vendors and third parties, their threat landscapes become part of yours.

1.3 Overview of Third-Party / Vendor (Supply Chain) Risks

The proliferation of technology and adoption of the Internet of Things has greatly enhanced the design, procurement, and construction procurement

processes, making it easier for disparate stakeholders to remotely communicate and collaborate on project goals and accommodate changes. This proliferation also has led to a marked increase in outsourcing, especially in the IT realm.

Today, vendors and third parties are engaged, and their technological advancements are employed, to support every aspect of the design and construction processes. IT firms and tools, for example, can help owners store and disseminate project data, assess projects' progress, and virtually manage all facets of the design and construction processes. These firms, and other third-parties, each have their own set of retained subconsultants and vendors, which creates a vast network of shared resources and information. While these interconnected networks carry great benefits in terms of information and resource-sharing, they also create concerning vulnerabilities.

Cyber-attackers are perpetually looking for new vulnerabilities to compromise, as well as security vulnerabilities and weaknesses in those vulnerabilities that will allow them access sensitive data, key systems, and business processes. The more vendors and third parties that are used, the more potential there is for attackers to find a way into an owner's data and systems.

Tremendous amounts of data—including highly sensitive data—flows through these technology mediums, and unauthorized access to, or malicious use of, this data can be catastrophic.

It's important to note that today's technology solutions are provided by companies of all shapes and sizes. There are very large players, such as Microsoft, CISCO, Amazon, and Google, which provide operating systems, network connectivity and Cloud services. Notably, while these companies have very robust security programs, they are not beyond compromise.

Smaller companies also are key players in the technology ecosystem and are typically involved in providing "specialty and emerging technology" solutions. These solutions include Artificial Intelligence, digital payment systems, biometrics, and custom applications, among others. While smaller companies may not possess the capital and resources of their larger counterparts, their size doesn't necessarily make them or their products more vulnerable to cyber-attacks.

Typically, both public and private owners employ a variety of technological tools from both large and small vendors. However, each of these technologies needs to "talk" to the others to achieve peak value and optimization. While this interconnectedness is vital, it also increases both overall complexity and the likelihood of vulnerabilities and weaknesses, which, in turn, increases risk. Since large and small companies will have varying levels of security controls, and all must be risk-rated and vetted accordingly.

Section 2 –Managing and Mitigating Risks

Risk management of vendors and third parties is essential but can involve significant effort. Organizations often like to think that outsourcing services and technology tools effectively transfers risk while reducing functions they must perform or manage directly. However, this is not the reality. Turning over management and control of vital technologies to a third party reduces owners' ability to foresee and remediate potential challenges and increases their overall risk. It is essential, therefore, that owners establish and maintain comprehensive vendor and third-party risk management programs to complement their outsourcing programs.

2.1 Best Practices

Vendor and third-party risk management programs must start with a solid policy and supporting procedures. The policy must identify how an organization will assess, manage, monitor, remediate and, in some cases, accept risks. Since all vendors and third parties aren't equal in terms of their security protocols, the owner's risk management policy must outline how it will risk-rate its vendors. Traditional "High," "Medium," and "Low" risk categories are standard. These categories also can be expanded to included "Extreme" and "Insignificant," and the range of categories typically depends on the quantity of vendors and third parties to be managed.
The formula for risk-rating vendors has many components, but the heaviest weighting comes from two categories: 1) What is the vendor or third party's access to the organization's most sensitive data, key systems, and business processes? The more access, the higher the risk. 2) What is the maturity level of the vendor or third party? Maturity is a reflection of several characteristics, including the length of time the vendor has been in business, its size, and the history of the product or service it offers.

Generally, the more mature a company is in these categories, the more secure they're likely to be. However, those criteria are never a guarantee, and many additional factors need to be considered. For instance, a company may have been in existence for many years, but has it kept up on its security investments? The assessment also should cover such key questions as: 1) how does the company perform its own internal risk assessments, 2) what does its employee training program entail, 3) what are its cyber-incident response and business continuity plans, as well as recovery plans, and 4) how does it manage its own vendor and third-party risk? (Which, essentially, becomes a "fourth-party" risk for the owner.)

Risk assessments also should encompass reviewing the company's financial posture, reputation, and compliance with laws and regulations. It also may be prudent to request a copy of the company's cyber- and information-security policies and procedures to gain a clearer sense of the company's overall program. On-site visits also may be a good idea, especially if the company is providing data-hosting services.

> "To effectively manage and minimize risk, both public and private owners must establish and maintain—and continually improve—a comprehensive program that manages risk at all levels and at all touch points. This is not an easy task but, with systematic planning and implementation, it is achievable"

Often, a leading question for a vendor and third-party risk assessment is "Does the company have any third-party attestations? The most common third-party attestation is a System and Organization Controls (SOC) report. There are several types of SOC reports. An "SOC 1 Type 1" report is an independent snapshot of the company's control landscape on a given day, and focuses on financial controls. An "SOC 1 Type 2" report adds an historical element, showing how controls were managed over time. SOC 1 reports have evolved from earlier attestations established by the American Institute of Certified Public Accounts (AICPA) Auditing Standards Board.

The AICPA also has developed an SOC 2 report, which focuses on a company's internal controls for cyber- and information-security, availability, processing integrity, confidentiality, and privacy. These SOC 2 reports have become standard for assessing cyber- and information-security. They are provided by accounting firms and their cost can be significant. So, companies

that have them performed (which should be annually) are demonstrating a solid commitment to having a strong cyber- and information-security program. Notably, if a vendor or third party provides a SOC 2, it should not be used to simply "check the box;" and should be carefully reviewed, as these reports may provide valuable insights into a company's weaknesses. It also is helpful to be aware of the company providing the SOC report and know whether the firm is reputable.

It is important to note that the world and variations of independent attestations continues to evolve. Effective vendor and third-party risk management policies should contain guidelines on reporting, what is standard in the industry and tools to continually monitor the industry for changes.

2.2 Regulations

Vendor and third-party risk management programs are not only sound business practice; they also are required in nearly every industry. Regulations span a wide range of authoritative bodies, and some have been around for more than a century. Other regulations are more recent, and newer ones are on the horizon.

The 1863 False Claims Act, which predates almost every technology in use today, has broad implications for cybersecurity. The False Claims Act is a whistle-blower law enacted to identify fraud perpetrated against the US government. The Act also allows any person to sue an entity that has committed fraud against the US government. The plaintiff bringing the suit is eligible to receive a percentage of the successful settlement and protection from retaliation by the defendant, including being fired.

Despite its age, the False Claims Act continues to be highly relevant today. Two recent False Claims Act cases highlight both vendors and their cybersecurity responsibilities:

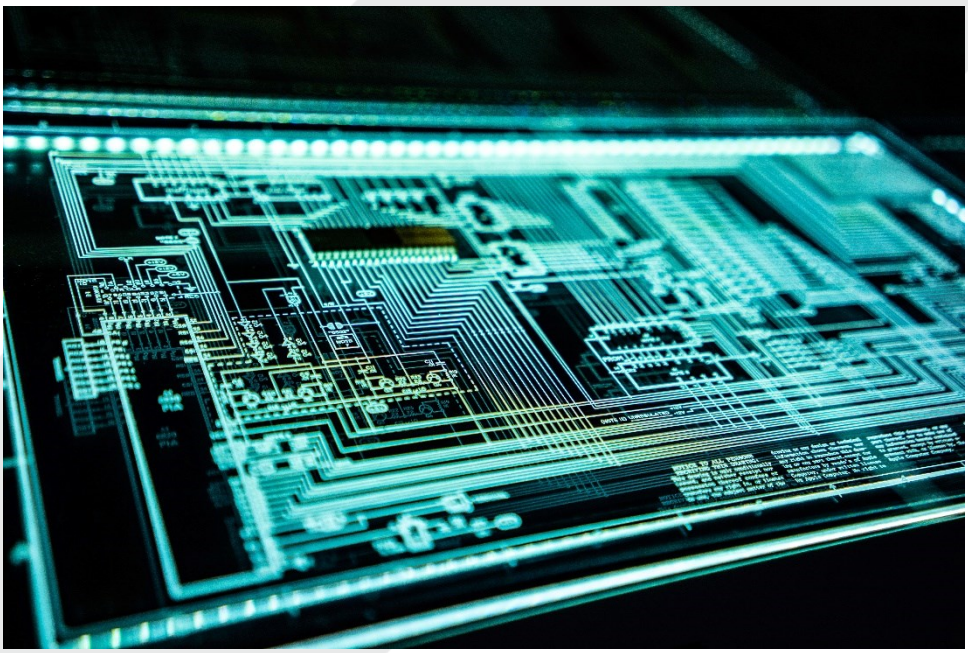
In July 2019, Cisco Systems settled a claim brought by a whistle-blower, alleging that it had knowingly sold video surveillance software with vulnerabilities to various governments. Cisco's settlement of the case constituted the first pay-out related to cybersecurity standards under the False Claims Act. Whistle-blower James Glenn, who worked for a Danish firm that was a Cisco vendor, had brought the suit eight years earlier, in 2011. In it, he alleged that Cisco's product was vulnerable to hacking and could enable cyber-criminals to gain administrative control of an entire network. Glenn alleged that he had warned Cisco about the flaw but said the company did nothing to correct it. Notably, Cisco acquired the firm that made the video surveillance software—and upgraded it—two years after Glenn brought his suit. Before selling the software to Cisco, the company had sold it to such clients as the Washington DC Police Department, Los Angeles International Airport, and the US military. In total, the case listed 15 buyers at the state level, plus the federal government.[5]

A second case was filed in California by a whistle-blower on behalf of NASA and the Department of Defense against Aerojet Rocketdyne Holdings, Inc. The whistle-blower, a former employee of the Aerojet Rocketdyne's cybersecurity department, alleged that the company committee fraud when it entered into federal contracts despite not meeting cybersecurity requirements with which government contractors must comply. Aerojet Rocketdyne maintained that it had informed the government of its non-compliance and asked the United States District Court for the Eastern District of California to dismiss the case. In May 2019, the Court rebuffed Aerojet Rocketdyne's motion to dismiss, which, in effect, upheld the argument that a government contractor can face FCA claims if it falsely

implies certifications of compliance with federal cybersecurity regulations—even if it had disclosed non-compliance to the agency. Although the US District Court ruling did not assign liability, it did open the door for future FCA litigation based on implied cybersecurity certifications.[6]

Data privacy is another element of cyber-security involving vendor and third parties that is highly scrutinized and strictly regulated. In May 2018, the European Union implemented the General Data Protection Regulation (GDPR), which changed the general concept of data privacy with articles on Data Subject Rights (DSR). The DSR component of the GDPR grants specific rights to individuals whose personally identifiable information (PII) is being collected, used, stored, and shared. The DSR articles also empower those individuals to exercise those rights, which include the right to be informed, the right of access, the right of recertification, the right to erasure, the right to restrict processing, the right to data portability and the right to object, as well as rights related to automated decision-making and profiling. Any organization that handles the PII of European citizens must comply with the GDPR and, if an individual exercises a DSR, the data collector must comply in a timely manner and promptly provide notice of that compliance to the individual.

The GDPR has become standard for the global privacy regulations, and other jurisdictions have followed. In the US, the State of California has implemented a new privacy law, the California Consumer Privacy Act (CCPA), and New York has the "New York Privacy Act." Every state in the US and most countries have some level of privacy regulation, and all have some form of breach notification requirement. These requirements can be very costly and time-consuming, and fines for non-compliance can be steep. Emerging privacy regulations mandate that firms which receive, share and outsource PII-processing to vendors and third parties must ensure that those vendors and third parties are compliant with the regulation.



Another new regulation that will impact owners is the "Internet of Things" (IoT) Cybersecurity Improvement Act of 2020, which was passed by the United States Congress on December 4, 2020. This bill requires the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) to take specific steps to increase cybersecurity for IoT devices.

The Internet of Things (IoT) is the network of physical objects, or "things," that are embedded with sensors, software and other technologies which connect to the internet and allow the exchange of data and information. IoT devices include a vast number of consumer, enterprise and industrial sensors and everyday objects. The most common IoT devices are cell phones, tables, watches and computers, which are used by people to connect and share their data.

The IoT Improvement Act requires NIST to develop and publish standards and guidelines on behalf of the federal government regarding the appropriate use and management of IoT devices that are owned and controlled by government agencies. As is the case with most cybersecurity regulations, the requirements will likely soon filter down to best practices for commercial projects in the private sector.

As new technologies arise, they also will be subject to specific regulations based on their use and implementation. Technologies that collect, use and store PII will be particularly scrutinized. Biometrics, which are being used with increasing frequency at headquarters and jobsites, is a good example of technology driving regulation. Health and safety concerns are pushing for more "touchless" facial recognition and eye retina-reading systems to be implemented. Several states already have enacted regulations regarding the proper use of biometric data, and others are expected to regulate the technology soon.

2.3 Industry Guidelines

The quickly evolving nature of both the technologies and their regulation means that owners and their vendors need to stay on top of both cybersecurity and privacy regulations, including those that are current and those on the horizon.

Industry organizations can help. The International Air Transport Association (IATA), which represents, leads, and serves the airline industry, for example, provides the civil aviation industry with valuable guidance and the latest updates on cybersecurity standards and regulations. The IATA's latest report, published in January 2021, includes crucial cybersecurity developments as well as links to knowledge centers of some of the world's leading industry watchdogs.[7]
Once areas of potential weakness are identified, they should be prioritized for mitigation based upon the level of threat they present and possible ramifications, with threats that can affect the entire organization or large portions of its operations at the top of the remediation list.

2.4 Risk Management Tools

Once vendor and third-party risk management policies and procedures are established, the most important element is assessing and managing the risk. As discussed earlier and depending on its size, an owner often relies on hundreds, if not thousands, of vendors to operate and serve its clients, customers or constituents. Potential vendors should be required to have established, "mature" cybersecurity plans in place and show that those plans meet industry standards and, ideally, have been reviewed and certified by a reputable external auditor.

Vendors also should be required to formally attest to the maturity of their cyber-protections before contracts are signed, and be willing police themselves and make similar attestations at specific intervals throughout the life of their contracts, as well as allowing a "right-to-audit" by the customer.

Owners themselves also should employ their own vendor controls, including systems for risk-rating, due diligence, on-boarding, continuous monitoring and off-boarding. Managing these activities and processes is far from easy, however, and the days of tracking activities with spreadsheets and shared document drives are long past.

Employing advanced management tools can help. In fact, there is an emerging category of vendor and third-party risk management software programs on the market, with a wide range of capabilities and features. (Notably, these additional vendors also need to undergo the same scrutiny as everyone else.)

In most cases, one solution alone may not be enough. Prudent owners should begin by developing a list of requirements and conduct a thorough evaluation of the solution(s) that best suit their needs. This evaluation should encompass a detailed outline of all the owner's requirements, as well as its budget, resources, and capabilities.

Governance, Risk and Compliance (GRC) software is a valuable foundational tool for managing vendor and third-party risk. GRC programs are highly customizable, and are designed to manage, monitor, track, review and report on compliance with established policies and procedures.

Risk Assessment tools also can be vital to managing vendor and third-party risk. These tools assess risk based on a vendor's product or services and its risk rating. They do, however, require the robust collection of key data. Once this data is entered and assimilated, risk assessment tools can produce a host of illuminating risk information. Consistent, thorough review of this information is essential.

Monitoring software is a newer tool that boosts vendor and third-party risk management by complementing existing processes. Monitoring programs oversee internet-facing IP addresses and domains to evaluate the performance of specific security controls. They also monitor public information for reports of data breaches, as well as the "dark web" for threat-related chatter by nefarious characters.

Training can be an invaluable tool in on-boarding new vendors and in managing overall vendor risk. Training can be easily tailored to meet each group's specific needs and place in the owner's ecosystem, can be accomplished virtually or in-person, can be ongoing and offered as often as deemed appropriate. Training also can be easily updated as new technologies—and new risks—emerge.

The Chief Information Security Officer, (CISO) who's primary role is to monitor and manage cybersecurity for the entire organization, plays a key role in managing vendor and third-party cyber-risk. They oversee the entire risk management spectrum and the respective vendors and third parties, from assessment, implementation, management, and termination. Depending on the owner's size, a CISO might have a sizable team, or in many cases leverages third-party service providers for specific subject matter expertise.

Conclusion

Technological advances and the integration of emerging solutions within owners' infrastructure and their ecosystems are moving at a rapid pace. Owners also are likely to increasingly rely on a multitude of vendors and third parties, which, in turn, will continue to cultivate prime targets for cyber-attackers.

Cyber-attackers aren't going away. Cybercrime is a huge, growing and increasingly sophisticated business, with no end in sight. In addition, there is no single "silver bullet" that will eliminate all vendor and third-party risks. To effectively manage and minimize risk, both public and private owners must establish and maintain—and continually improve—a comprehensive program that manages risk at all levels and at all touch points. This is not an easy task but, with systematic planning and implementation, it is achievable.

References

[1]https://www.washingtonpost.com/politics/2020/12/07/cybersecurity-202-global-losses-cybercrime-skyrocketed-nearly-1-trillion-2020/

[2]https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php

[3]https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[4]https://www.reuters.com/technology/hackers-demand-70-million-liberate-data-held-by-companies-hit-mass-cyberattack-2021-07-05/

[5]https://www.reuters.com/article/us-cisco-systems-claim/cisco-whistleblower-gets-first-false-claims-payout-over-cybersecurity-idUSKCN1UQ2W2 and https://apnews.com/article/2e56253a512a4622997e8b6e9b1d0e9b)

[6]https://resources.infosecinstitute.com/topic/the-false-claims-act-and-cybersecurity-are-third-party-vendors-putting-you-at-risk/ and https://news.bloombergtax.com/coronavirus/aerojet-rocketdyne-must-face-allegations-of-lax-cyber-compliance?context=article-related)

[7]Compilation of Cyber Security Regulations, Standards, Guidance for Civil Aviation: https://www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/compilation_of_cyber_regulations_standards_and_guidance_1.1.pdf

If you require any further information, please contact Michael Corcione at michaelcorcione@hka.com.