This past year has highlighted the need for businesses to be laser focused on the cyber threats posed by today's cyber space landscape. As if the dual threats of COVID-19 and its devastating impact on our nation's economy weren't enough of a catastrophe, a third and very real threat is now invading the computer systems of every private and public sector enterprise in our country, including those in the construction industry. Cyber criminals are working overtime to create chaos using spear-phishing scams and malware schemes to take advantage of the coronavirus pandemic. Cyber hackers employing two variants of ransomware — Maze and Ryuk — are launching devastatingly successful attacks under the shadow of COVID-19.

Cyber threats have become more acute as employees of all companies, including those in the construction industry, have been forced into working from home. This has created a target rich environment for cyber hackers. Cyber threats to the construction industry are nothing new. What is new is the ferocity, frequency and sophistication of the cyber attacks.

Cyber criminal activity is now the greatest threat to every business and public sector entity in the United States. And as construction executives are now realizing, the industry is far from being immune or exempt from attacks perpetrated by cyber criminals. Much like any other industry that relies on the internet to communicate externally with clients, customers, and vendors, and internally with employees, the construction industry is under the constant threat of cyber attacks.

An alert issued in April 2020 by our Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) noted that the attacks have often involved malicious phishing or ransomware attacks. In a ransomware attack, the cyber attacker locks up a company's computer system and demands payment to restore access for the user. According to CISA Assistant Director Bryan Ware, "As the COVID-19 outbreak continues to evolve, bad actors are using these difficult times to exploit and take advantage of the public and business." Cyber criminals are taking advantage of the understandable fear created by COVID-19 to lure computer users, especially those working from home, into clicking on links to malicious emails. The malicious emails often appear to be sent from reputable organizations such as the Centers for Disease Control and Prevention (CDC).

As organizations in the construction industry — engineers, architects, construction managers, general contractors, subcontractors, suppliers — are doing more on-line than ever before, are more connected than ever before, and are more digitally integrated than ever before, they are more vulnerable than ever before. And much like companies in other industries that believe the security provided by conventional cyber security measures such as firewalls and anti-virus software provide a safe harbor, the construction industry has learned from recent experience that its cyber security is simply not all that secure.

The cold hard facts of cyber crime — the cost of a data breach — are sobering.

- ***Global cyber crime damage will cost an estimated $6 trillion by 2021*** *(Source: Cybersecurity Ventures)*
- ***Sixty percent (60%) of small business shut down within six months of a cyber attack*** *(Source: Inc.com)*
- ***Thirty-eight percent (38%) increase in cyber security incidents between 2016 and 2017*** *(Source: IBM Security Intelligence)*
- ***The "Internet of Things" is exploding — from 2 billion connected devices in 2006 to a projected 200 billion connected devices in 2020*** *(Source: Intel.com)*
- ***Cyber attacks are now the fastest growing crime in the U.S., and the attacks are increasing in size, sophistication and cost*** *(Source: Cybersecurity Ventures)*

The Cyber Threat of Ransomware—Maze and Ryuk—Invading Under Cover of COVID-19

Ransomware is a growing cyber threat that is spreading virulently across all sectors of the world's economy. The FBI began warning U.S. companies in 2019 about ransomware attacks in which the cyber hacker, disguised as a federal or state government agency, penetrates a company's cyber defenses, steals valuable company data, and then encrypts it to further extort the target of the attack. In a later advisory, the FBI warned private sector enterprises to be vigilant against the Maze ransomware. Maze is very effective in its ability to fool the target company through its spoofing of government agencies, well-known security vendors, and other seemingly trustworthy sites and thereby infiltrate the victim's defenses.

In 2020, cyber hackers employing Maze ransomware successfully breached the cyber defenses of a wide range of companies in every sector of our economy and the economies of most industrialized countries. According to CyberEdge ***2020 Cyberthreat Defense Report***, ransomware attacks and payments continued to rise, resulting in 62 percent of organizations being victims in 2019, up from 56 percent in 2018 and 55 percent in 2017. The catalyst for this dramatic rise over the past three years has been the payments received by the hackers from the victims.

In April 2020, Cognizant, one of the largest consulting and tech companies in the Fortune 500, was hit with a Maze ransomware attack. In a cyber breach that must fall under the heading of "Physician, Heal Thyself," Chubb, one of the largest cyber security insurance carriers, become a target of a data breach. In March 2020, hackers using Maze ransomware launched an attack on Chubb for the purpose of stealing the carrier's data.

Ransomware—Maze and Ryuk—Is Now Aimed at the Construction Industry

The February 2020 Maze ransomware attack on Canadian construction giant Bird Construction, is a case in point. A 100-year old publicly traded company with operations throughout Canada and in the U.S., the Maze ransomware hacker claimed to have successfully stolen 60 GB of data from the company. The cyber attack resulted in the encryption of the company's files.

At about the same time cyber criminals deploying Maze ransomware penetrated the cyber defenses of Bird Construction, the construction subsidiary of the Paris-based Bouygues Group was the target of a successful cyber attack perpetrated by the same Maze hackers. With over $32 billion in global revenue, Bouygues construction unit is ranked No. 10 on Engineering News Record's list of Top 250 Global Contractors. As a result of the cyber attack, Bouygues' entire computer network was affected. The company had to temporarily shut down all of its servers.

In March 2020, EMCOR Group, a U.S. Fortune 500 company that provides mechanical, electrical, and fire protection construction services to clients across all markets, disclosed that it was hit by a Ryuk ransomware attack that took down some of its IT systems. According to the company, the cyber attack did not involve data theft, however, EMCOR did not specify if had paid the ransom demand. EMCOR adjusted its estimated 2020 earnings projections to account for the downtime caused by the cyber attack.

During 2020, cyber attacks have increased about 40 percent as the COVID-19 pandemic has emboldened cyber criminals to act with impunity. Spear-phishing attempts have soared by an astonishing 600 percent since the end of February. Those phishing attacks include traditional impersonation scams coupled with extortion attacks. Cyber criminals are taking advantage of the understandable fear that has affected those people concerned about their health and the economic stress of job vulnerability. With most employees working from home, the usual reluctance to

open personal emails is much less and the lure of opening personal emails dealing with health issues is much greater. Cyber criminals are using fear to create a sense of urgency in the targeted victim to reduce security awareness.

The Fundamentals — Cyber Risks

Along with the exponential advancements in Information Technology in the construction industry there has been a concomitant increase in cyber risk. Cyber risks are generally caused by cyber threats. Broadly speaking, cyber risks are the potential for damage, loss, or disruption to business operations that can occur from using information systems. The cyber risks include:

- ***Business Operational Risk***: The possibility for net operating losses caused by the failure of key business systems, processes, procedures or people.
- ***Reputational Risk***: The possibility for loss or damage that is the direct result of harm caused to an entity's reputation or public image.
- ***Legal and Compliance Risk***: The possibility for loss or damage that is the direct result of legal action being instituted against an entity based on the entity's negligence or failure to comply with regulatory requirements.

Cyber Criminals Exploiting COVID-19

As the cyber threat landscape has evolved, so has the sophistication and types of cyber criminals that threaten an organization's cyber security. Today's cyber criminals run the gamut from unscrupulous hackers who lurk in cyber space ready to take advantage of the slightest vulnerability of an organization's cyber defenses to nation-states with the economic and technical resources to launch complex and sophisticated cyber attacks designed to breach the most robust cyber defenses.

- ***Lone Wolves***: Operating as solo hackers, lone wolves are motivated by a wide variety of incentives that range from financial gain to ego rewards.
- ***Hacktivists:*** Hacktivists tend to engage in cyber hacking to express some social, political or religious agenda. The hacktivist can cause substantial damage to an organization by vandalizing its internet presence and/or harming its reputation on-line.
- ***Criminal Organizations:*** The criminal gangs of cyber space have as their primary motivation financial gain. Data theft and data ransom are the goals. The potential upside is substantial. That is why cyber space is increasingly the turf of Mafia-like organized criminal groups that are capitalizing on vulnerabilities in cyber defenses.
- ***Nation-States***: Cyber attacks launched by nation-states range from strategic intelligence-gathering and espionage of military targets to destructive attacks designed to have a devastating impact on the infrastructure of the target country. In contrast to criminal organizations, nation-state hackers are aligned with the foreign policy agendas and espionage goals of the nation-states. The axis of nation-states involved in cyber espionage includes China, Russia, North Korea and Iran.

The Fundamentals — Cyber Risk Management

Today's cyber threat landscape should serve as a red flag that the traditional approach to cyber security, while important for securing business systems and assets from conventional attack vectors, falls far short in thwarting a cyber adversary whose means, methods and techniques are continually and rapidly evolving. A traditional approach, such as a fixed fortification like the Maginot Line, cannot adapt to the continual changes in the cyber threat landscape.

Cyber risk management, in contrast, is a holistic strategy that is highly adaptive to the universe of cyber threats, both external and internal, and provides a methodology for evaluating their potential impact, their likely attack vectors, and the technology needed to counter these threats. Cyber risk management strengthens cyber resilience by incorporating aspects of risk mitigation that ensures the security of a company's information systems. Cyber risk management includes:

- ***Threat Intelligence***. Evaluating cyber threats through an understanding of threat intelligence.
- ***Critical Business Systems and Assets***. Identifying critical business systems and assets which are essential to the continued operation of an organization.
- ***Technologies.*** Deploying up-to-date cyber security technologies.
- ***Incidence Response Plan.*** Executing an Incidence Response Plan when faced with a cyber attack.

The Fundamentals —The CIA Triad — Confidentiality, Integrity, Availability

No organization's cyber security can successfully function unless it protects and integrates three critical functions: the ***Confidentiality***, the ***Integrity***, and the ***Availability*** of its information systems. Referred to as the ***CIA Triad***, the development of cyber security must ensure that the procedures are fully aligned with an organization's business objectives and corporate strategy.

- ***Confidentiality***. Keeping sensitive information private and access controlled is the first prong of the CIA Triad. To maintain confidentiality, the use of passwords, personal identification numbers, access control lists, and a written security policy requiring strict compliance, are but a few of the necessary safeguards.
- ***Integrity***. The second prong of the CIA Triad refers to the trustworthiness of an organization's information. As data is moved around an organization and between the organization and authorized third parties, it is critical that steps are taken to ensure that the data cannot be altered or corrupted by cyber criminals.
- ***Availability***. Unless an organization's data is readily available through fully operational information systems, its business objectives are compromised. This raises the potential for an adverse impact to a firm's reputation and the risk of losing clients or worse.

The Fundamentals — The NIST Cyber Security Framework — Five Core Functions

In response to increased threats to our nation's critical infrastructure, the National Institute of Standards and Technology (the "***NIST***") developed a framework for organizations to assess their readiness to thwart and respond to a cyber attack. The NIST Cybersecurity Framework was designed to provide guidance to both public and private sector entities for evaluating their capability to effectively mitigate cyber attacks. The five interdependent core functions include:

- ***Identify***. The core function involves understanding an organization's resources that support critical business systems and assets. This includes: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy.
- ***Protect***. The Protect Function supports the capacity of an organization to limit the adverse impact of a cyber attack. This includes: Access Control; Awareness Training; Data Security; Information Protection Processes and Procedures; Protective Technology.
- ***Detect***. The Detect Function implements key activities needed to discover and identify the occurrence of a cyber event. This includes: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.
- ***Respond***. This core function develops and executes key activities to react in the event of a cyber security event. The Respond Function provides the capacity to contain and/or quarantine the adverse impact of a cyber incident. This includes: Response Planning; Communications; Analysis; Mitigation; Improvements.
- ***Recover***. The Recover Function develops and implements those key activities required to restore key business systems and assets that may have been adversely impacted by the cyber event. This includes: Recovery Planning; Improvements; Communications.

In sum, the NIST Cyber Security Framework provides the necessary guidance for construction industry organizations when assessing their cyber security core competencies. Identifying critical business assets and systems is the next step.

Cyber Resilience—Protecting Critical Business Systems and Assets

Cyber attacks subject key company assets to encryption and/or destruction. For engineering and construction companies, these mission critical assets include:

- ***CADD Systems***. The use of computers to aid in the creation, modification, analysis, or optimization of a design is now common in the construction industry. CADD software is used to increase the productivity of the designer, improve the quality of design, improve communications through documentation, and to create a database for manufacturing. CADD output is often in the form of electronic files for print, machining, or other manufacturing operations.
- ***Project Control and Management Systems.*** The capability to efficiently manage the design and construction process is essential to the successful completion of constructed facilities. Cost Control, Schedule Control, and Quality Control systems comprise the three-legged stool that enables project managers for engineering and construction companies to efficiently manage and execute the design and construction process. Taken together, Cost Control, Schedule Control, and Quality Control comprise the Project Control and Management Systems.
- ***Project Extranets***. Project Extranets are generally referred to as the "weakest link" in an organization's information infrastructure. Because the chain is only as strong as its weakest link, an organization's cyber security is only as strong as its Project Extranets. Cyber criminals will look for the weakest security and focus its attack resources on the weakest point. For companies in the construction industry, that weakest point is also an integral part of the design and construction process. Project Extranets allow clients, contractors, design professionals, subcontractors and suppliers to share project related data at any point along the design-construction continuum. By linking project participants together in a network, access to the information and data necessary for the design and construction process is made much more efficient. Project Extranets can significantly reduce the transaction costs that are associated with the design-construction process.

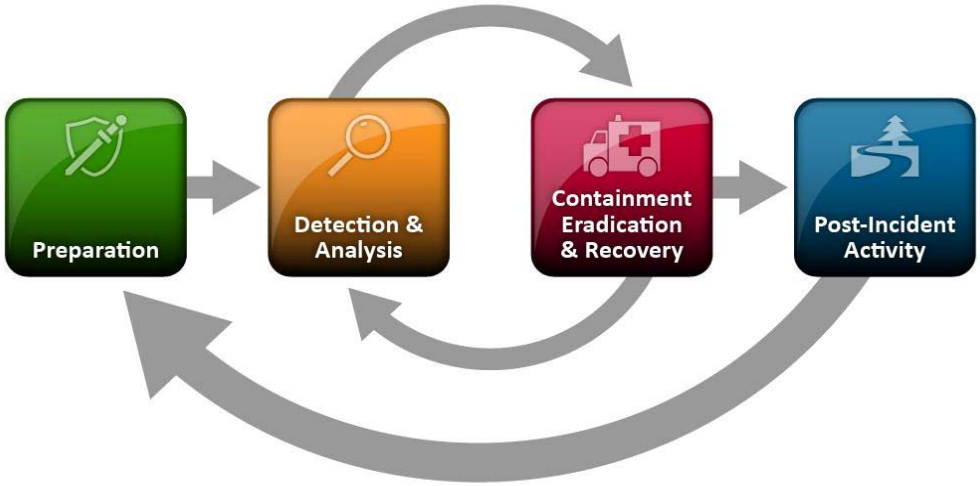
Cyber Resilience—A Holistic Approach to Cyber Risk Management

Perimeter defenses combined with technology alone — much like the "fixed fortifications" of the Maginot Line — are not the silver bullet needed to defeat the universe of rapidly evolving threats from the cyber risk landscape. Those organizations that have been the most successful in thwarting cyber attacks — and effectively responding once the attacks have occurred — are deploying a holistic approach to cyber risk management. The holistic approach combines technical, human and physical factors in the detection, prevention, and improvement of cyber security vulnerabilities.

Expanding cyber defenses beyond technology alone involves a broad-based cyber risk management approach starting with the NIST Cyber Security Framework. This approach includes a risk and threat assessment which identifies those areas of an organization that need additional resource allocation. For these purposes, the NIST Cyber Security Framework should be used to identify an organization's vulnerabilities, to determine an organization's cyber resiliency — and to create a reference point against which to realistically evaluate the status of an organization's cyber security.

Cyber Resilience—Implementing an Effective Incident Response Plan

Cyber risk management incorporates aspects of risk mitigation that ensure the security of an organization's information systems. The capability of implementing an Incident Response Plan in the event of a cyber attack is a critical element of any organization's cyber security. Key steps in an Incident Response Plan should include:



Incidence Response Life Cycle —The NIST Incidence Handling Guide

- ***Step 1.1 — Prevention***: This initial step includes the technical and non-technical measures that an organization should take to prevent a cyber attack. Technical measures include controls such as: Antivirus Software, Anti-Spam Software, an Intrusion Prevention System, Firewalls / DMZ, and Vulnerability Scanners. Non-technical measures include updated Threat Intelligence and Data Governance protocols.
- ***Step 1.2 — Planning***: The individuals within an organization involved in the Incident Response Plan and their roles should be identified and their responsibilities defined. Key individuals and their roles include the Chief Operating Officer (COO), the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), the Computer and the Security Incidence Response Team (CSIRT) Manager.
- ***Step 1.3 — Preparation***: This step includes the reporting mechanisms, the preparation of checklists, and the auditing procedures. Also included in this step are the training exercises the Incident Response Team will undergo.
- ***Step 2.1 — Detection***: Deployment of the following technical tools is an integral part of the detection defense of a cyber attack: Intrusion Detection System (IDS), Security Information and Event Management (SIEM), System and Application Logs, File Integrity Checking Software, Network Analyzers, and Vulnerability Scanners.
- ***Step 2.2 — Analysis***: Following a determination that a cyber event was not a false positive, the analysis should proceed as follows: First, determine the focus of the attack, the potential threat to Critical Business Systems and Assets. Next, focus on the nature and scope of the attack, i.e., was the end goal to insert malware, to hold the Critical Business Systems and Assets hostage by inserting ransomware. This should be supplemented by an analysis of the extent of penetration of the attack. Finally, the analysis should answer the question of the attack origin, if possible, and how far back into cyber space can the attack be traced.

- ***Step 3.1 — Containment***: Based on the nature and scope of the cyber attack as determined in Step Five, the next step involves (a) verifying that the cyber event has not impacted any Critical Business Systems and Assets, and (b) disabling, compartmentalizing and isolating any affected files.
- ***Step 3.2 — Communication***: In consultation with in-house and/or outside counsel, determining the timing and extent of communications with external and internal stakeholders.
- ***Step 3.3 — Eradication***: The Incidence Response Team, led by the CISO and the CSIRT Manager, should take responsibility for removing the threat from an organization's internal system.
- ***Step 3.4 — Recovery***: This key step will determine the cyber resilience of the Incidence Response Plan.
- ***Step 4.0 — Post-Event Analysis***: This final step is necessary to ensure that the lessons learned from the cyber event are incorporated into the Incidence Response Plan, thereby improving the cyber resilience of the Incidence Response Plan. Questions to be answered include:
    - ***Specifically what happened and when?***
    - ***How well did management respond?***
    - ***What data was needed sooner?***
    - ***Did any actions impede the recovery?***
    - ***What should management have done differently to better respond?***
    - ***What corrective actions could prevent similar future incidents?***
    - ***What indicators should provide red-flag warnings to detect future incidents?***
    - ***What additional tools are needed to detect, analyze, and mitigate future incidents?***

Cyber Resilience—Tactics, Techniques and Procedures

As construction industry organizations respond to the latest threats in the cyber landscape caused by cyber criminals taking advantage of the work-from-home protocols implemented as a result of COVID-19, an understanding of cyber threat intelligence solutions is more crucial than ever. Cyber criminals are developing more complex and sophisticated means, methods and techniques of attack. The velocity and sophistication of cyber attacks too often outpaces the ability of cyber defenses to respond in kind. With construction industry organizations — engineers, architects, construction managers, general contractors, subcontractors, suppliers — doing more on-line than ever before, more connected than ever before, and more digitally integrated than ever before, the cyber risks to businesses are increasing exponentially. Faced with the likelihood for significant operational, financial, reputational, and legal losses, construction organizations must ramp up their counter intelligence and cyber security by gaining an in-depth understanding of how threat agents launch their attacks. The reality of data breaches in 2021 is not a question of "***if, but when***." And the biggest question for construction industry organizations remains — how to maintain the ***Confidentiality***, the ***Integrity***, and the ***Availability*** of their Critical Business Systems and Assets while dealing with 24/7 cyber attacks under cover of the COVID-19 pandemic.