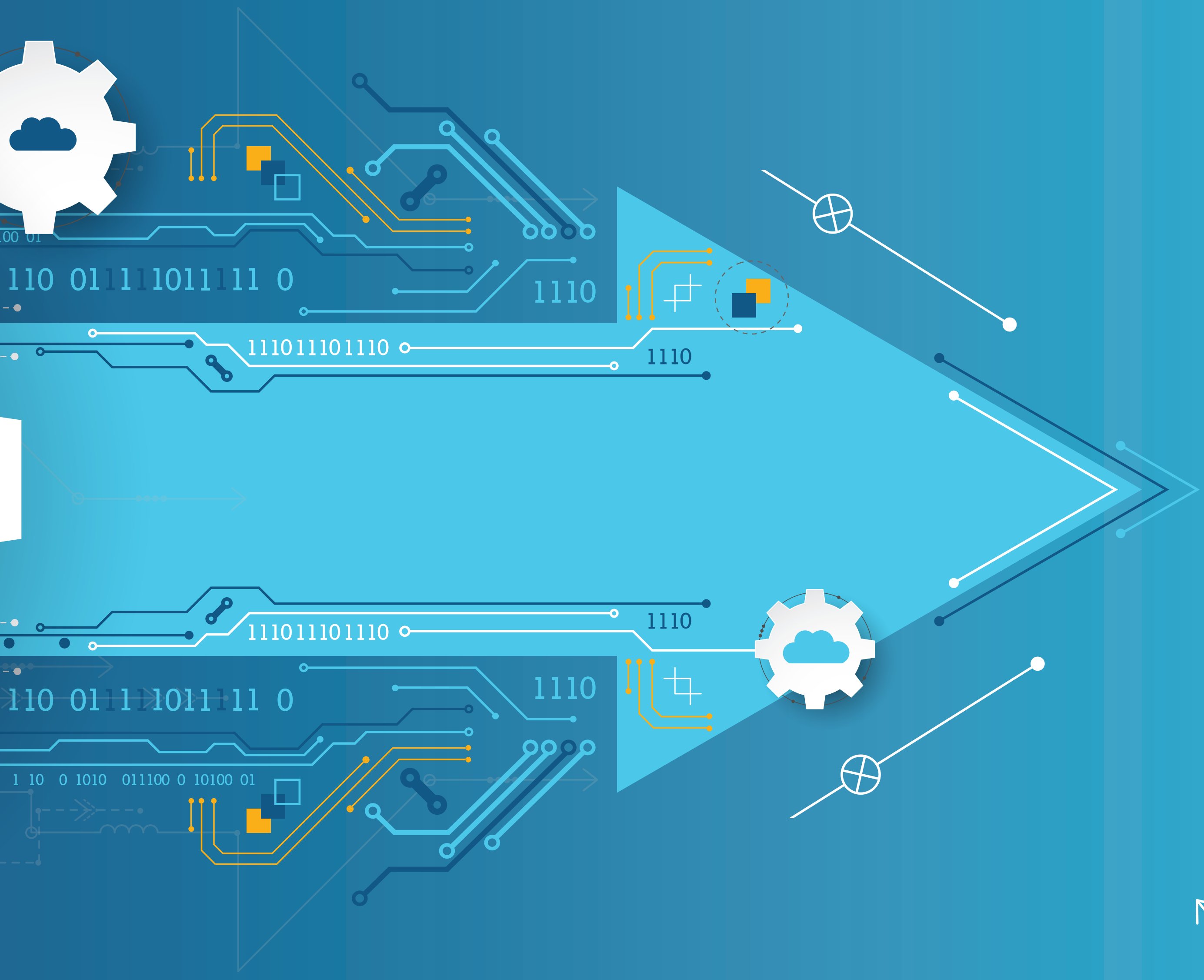
The Role of the CFM in CYBERSECURITY Risk Management

By Joe Harper, Jennifer Miloszewski,
Tom Skoog & Damien Strohmier

With increasing speed and consistency,

DATA BREACHES AND FINANCIAL LOSSES DUE TO CYBERSECURITY INCIDENTS ARE OCCURRING ACROSS COMPANIES OF ALL TYPES – AND THE CONSTRUCTION INDUSTRY IS NOT EXEMPT.

Misappropriations, ransoms, corporate embarrassment, and weeks of administrative downtime can cripple a closely held business.



Cybersecurity is an enterprise risk management concern. And, since construction financial managers (CFMs) understand the business risks and potential impacts to an organization if a breach were to occur, they are, to some extent, responsible for their companies' cybersecurity controls and response plans. The responsibility is in large part assembling the right team of resources and experts to ensure the company is safe. However, it is our belief that effective CFMs need some level of understanding of the cybersecurity threats, defenses, and insurance. (We acknowledge that the "level" is up for debate.)

This article will review how cybersecurity has impacted the construction industry and will work through the facets of an IT risk assessment including current threats, controls, and a response plan.

EXHIBIT 1: PROBABILITY

Probability	Definition
Probable	Risk will occur
Possible	Risk likely to occur
Improbable	Risk unlikely to occur

EXHIBIT 2: IMPACT

Impact	Definition
Intolerable	Critical effect on confidentiality, integrity, or availability
Tolerable	Moderate effect on confidentiality, integrity, or availability
Acceptable	Little to no effect on confidentiality, integrity, or availability

EXHIBIT 3: OVERALL RISK

		Impact		
		Acceptable: Little to no effect	**Tolerable:** Moderate effect	**Intolerable:** Critical effect
Probability	**Improbable:** Risk unlikely to occur	Low	Low	Medium
	Possible: Risk likely to occur	Low	Medium	High
	Probable: Risk will occur	Medium	High	High

The Impact to Construction

The construction industry has not been spared from the exploits of cybercriminals. Verizon's *2020 Data Breach Investigations Report* (DBIR) identified construction as a new category in 2020. The DBIR collected data on more than 157,000 incidents and 108,000 breaches and found that organized groups are targeting the construction industry for financial gain.[1]

Web applications and crimeware represent 95% of all incidents in construction.[2] Cybercriminals are using stolen credentials and waiting for the right opportunity to access confidential information or divert payments from contractors.

The construction industry is also in the early stages of standardizing the integration of smart devices – such as thermostats, water heaters, and power systems – that involve more access to internal and client networks. These new internet of things (IoT) devices create a larger attack surface than previously existed.

While construction has not historically faced federal cybersecurity regulations, in November 2020, the U.S. Department of Defense (DOD) initiated the Cybersecurity Maturity Model Certification (CMMC) framework that phases in certain cybersecurity requirements for DOD contractors.

Contractors that rely on revenue from the DOD will be required to implement over 200 cybersecurity controls over a five-year implementation period. Additionally, those required to comply with this mandate will have to hire an independent third party to assess and report their level of compliance with these requirements.

Where to Start

To begin establishing a cybersecurity risk management program, start by identifying and understanding risks and then sourcing and measuring them to determine how to manage them down to an acceptable level.

Identify & Understand

A CFM trying to understand cyber risks should begin by identifying and understanding what data and information are used in the business and within its data systems. The following questions can serve as a starting point to this understanding by classifying data from less to more critical:

1) What do we deem as confidential? Do we have confidential information? Does any of this data have regulatory protection requirements? Where is this data stored? Do outside entities/business partners/vendors have this data in their systems? Examples of such system data may include:

- *Employee information* – payroll and other personal and financial employee information. If that information were to be exposed, the employer has obligations under state and federal law to inform the affected personnel.
- *Construction data* – owner's plans and specifications; *Davis-Bacon Act* data, which includes subcontractor employee data; and other confidential or proprietary data of the owner, designer, or a supplier. You may have a contractual obligation to keep that data secure. In addition, construction plans may include security system information, which can be used for a later, more traditional attack on the physical assets of the business.
- *Valuable company data* – intellectual property, trade secrets, company financial information, and other confidential company data that could be used by a competitor.

2) If our systems were breached and data was changed, what would the impact be to the company?

3) If our data or systems became unavailable, what would be the impact to our day-to-day operations?

4) What can compromise the confidentiality of our data?

5) What can cause a loss of availability?

6) What can challenge the integrity of our data?

This list is a starting point, and CFMs should consider asking their IT staff or service providers to assist in helping them to better understand their data and systems.

Source & Measure Risk

Threats and vulnerabilities that can turn into risks can be categorized into several macro level events, including environmental and physical threats, natural threats, human threats, and technical threats. Inside each of these macro level threats are dozens of more specific incidents that can negatively impact your cyber position.

Risk levels are determined by the *probability* that a threat will occur (Exhibit 1) and the *impact* of loss or harm to company data (Exhibit 2). This methodology to determine *overall risk* (Exhibit 3) will be familiar to project management, as similar heat maps are used to assess risk on jobs.

Current Controls & Readiness Assessment

Once you have identified all threats to the confidentiality, integrity, and availability of your data and systems as well as measured the risk, you can then ask specific and informed questions of your IT resources to determine your company's readiness, such as:

- How are we protecting against the loss of our systems due to a natural disaster?
- How are we limiting the ability of ransomware or malware into our systems?
- What have we done to limit the chance of an employee doing something they shouldn't do?
- Have we adequately restricted access to our information?
- Have we reduced the chances of someone accidentally jeopardizing our systems?

Questions around risk may seem limitless, but as you continue through this process, it is likely that additional questions will start to fall into low-risk categories.

Cybersecurity Framework

To aide in your risk assessment process, there are several security standards and guidelines that CFMs can use in understanding the strength of their cybersecurity protection measures. One of these standards is the Cyber Security Framework (CSF) from the National Institute of Science and Technology (NIST).[3]

The framework's core consists of five areas: *identify*, *protect*, *detect*, *respond*, and *recover*. These five areas provide a high-level, strategic look at the organization's readiness and risk tolerance and can serve as a road map for policy creation, strategic defense, and necessary response. The CSF promotes the identification and response of the *layers of risk* as well as the categories and subcategories (discrete outcomes) for each function:

1) *Identify* – Asset management, business environment, governance, risk assessment, risk management strategy, and supply chain management

2) *Protect* – Identity management, authentication and access control, awareness training, data security, information protection processes and procedures, maintenance, and protective technology

3) *Detect* – Anomalies and events, security continuous monitoring, and detection processes

4) *Respond* – Response planning, communications, analysis, mitigation, and improvements

5) *Recover* – Recovery planning, improvements, and communications[4]

For all of the former auditors reading this, consider the CSF as a standardized audit program. At the end of the process, the cybercrime prevention team will have a road map of preparedness and risk appetite. The results may then be presented to company leadership with the intention of obtaining organizational approval of the overall plan, including risk assessment.

Please note that the defense process is not static. Cybercrime statistics, current trends, etc., are updated continuously. Unfortunately, cybercriminals are constantly evolving with increasing resources, so the defense plan, training, monitoring, and awareness must continue to grow and evolve as well.

It's important for CFMs to be aware of cybercrime tentacles. For instance, consider something as simple as creating a "preferred vendor program" in which subcontractors and vendors that meet certain criteria are paid by ACH instead of check. Such a program would benefit the company by reducing the number of checks written, processing effort, time, and mailing costs; this type of program also prevents advertising the company bank account, routing number, check signer, etc., to would-be criminals.

However, simply initiating ACH payments from your primary bank and using earning credits to offset ACH fees generally requires a company to keep vendor and subcontractor bank account and routing information electronically. Keeping your customer's credit card information on the network increases a company's exposure. In the unfortunate event of a breach, not only will there be a negative impact on your company, but also its subcontractors, vendors, and, in the case of credit card information, your customers.

To offset the additional exposure, you may look to house bank information on a third-party payment solution's site instead of it being stored on the company intranet. However, those services generally cost the subcontractor and vendor a couple points, negating the benefits of attaining the "preferred" status. They also generally have a cash back component to the company, again, negating the spirit of the program. Those third-party payment programs may be best suited to the nonpreferred subcontractors and vendors. A company may be left with obtaining cyber insurance to offset the liability.

The Importance of Response Plans

While it's imperative to be vigilant in cybercrime prevention (or lessen the likelihood or impact of a breach), some of the most secure networks in the world have been breached. The final element of your cybersecurity risk management program is to develop a detailed incident response plan for not if but *when* a breach occurs.

Preparation

Compile a list of all your assets including, but not limited to, servers, networks, applications, and critical endpoints (like C-level laptops), and rank them by level of importance. Next, monitor their traffic patterns to create baselines for later comparisons. Also, create a communication plan with guidance on who to contact, how, and when based on each incident type. Don't forget to get buy-in from everyone on this contact list to prevent confusion later.

Determine which security events and at what thresholds should be investigated, and then create an incident response plan for each type. It can be improved through security event simulations where you identify holes in your process, but it will also be improved after actual events. The point is to get a process in place.

Detection & Analysis

Once a security incident has been identified, go into research mode. Gather everything you can on the incident and analyze it. Determine the entry point and the extent of the breach. Determine how many files or systems have been potentially infected because of the breach. This will be made substantially easier if you have elected to engage an outside security monitoring service.

Containment, Eradication & Recovery

Containment patches the threat's entry point, and eradication aims to remove the threat. If the threat gained entry from one system and proliferated into others, then examine each one. Recovery aims to get the system operational if it went down or simply back to business as usual if it didn't.

Post-Incident Activity

Lastly, take the time to learn from your experience so you can better respond to future security events. This should include a lessons learned/root cause analysis, not unlike what is completed at the end of a large construction project. All interested parties (CFM, IT, cyber insurance firm, security vendors, etc.) should participate in the analysis, and relevant policies and procedures should be reviewed and updated as necessary to prevent future incidents.

Conclusion

Cybersecurity is an enterprise risk management concern and the responsibility of the CFM. Now is the time to establish preventative policies and resources to protect the business. By spending more time identifying an organization's cyber-related risks, a CFM will be able to establish appropriate controls that mitigate those risks, along with an incident recovery plan that allows the business to resume operations quickly and prevent lost resources. ■

Endnotes

1. "2020 Data Breach Investigations Report." Verizon. 2020. *enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf.*
2. Ibid.
3. "Cybersecurity Framework." National Institute of Standards and Technology. *www.nist.gov/cyberframework.*
4. "Framework for Improving Critical Infrastructure Cybersecurity." National Institute of Standards and Technology. April 16, 2018. *nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.*

JOE HARPER, CPA, CCIFP, is CFO of Greater Dayton Construction Group, a commercial and residential builder in Beavercreek, OH. He is responsible for the accounting and finance operations, as well as financial strategy for the company. Joe currently serves as the Chair for CFMA's Education Steering Committee as well as on several education task forces. He is Past President of CFMA's Central Ohio and Greater Cincinnati Chapters.

Phone: 740-607-1449
E-Mail: jharper@gdcg.com
Website: www.gdcg.com

JENNIFER MILOSZEWSKI, CPA, is a Director and the Construction Niche Leader at Blue & Co., LLC in Lexington, KY, where she provides assurance services

Top 10 Immediate & Practical Considerations

One common reaction from CFMs to the Cyber Security Framework (CSF) might be that "we don't have the resources to do all of this." However, part of the risk assessment process is to direct resources to the most critical areas. Here are some immediate and practical things that CFMs can inquire of their IT teams as first layers of defense:

1) *Patching* – Ensuring timely patches are installed is arguably the number one defense against malware and ransomware infecting your networks.

2) *Know your data* – Police your data, and only retain what is appropriate to conduct business.

3) *Stay current with technology* – Ensure your operating systems are up to date and you are not relying on unsupported software. For example, computers running on Microsoft 7 or earlier versions are no longer supported; do not use them in your organization if they are connected to your network, as they are an open door for cybercriminals.

4) *Train, train, and train some more* – Most breaches are because an employee unintentionally provided unauthorized access to your system. Remind your employees about cybersecurity best practices and help them identify "red flags" in e-mails so they don't put the organization at risk. Acceptable use training will keep employees up to date and aware of phishing schemes. Training is not foolproof, but it will reduce the risk of cybercrimes.

5) *Look for monitoring help* – It is difficult for small- and medium-sized contractors to have the resources to monitor security incidents and events. If your organization is not large enough to have a robust internal IT staff, then partner with an outside cyber monitoring service, as they have 24/7 staffing, the latest monitoring technologies, and significant experience in dealing with cyber events.

6) *Manage your vendor risk* – Ask your outside partners, banks, CPA, attorney, subcontractors, payroll processors, etc., how they protect their data.

7) *Get insured* – Make sure your cybercrime/cyber insurance policy is well thought out and fits within your overall plan. Partner with an experienced cybercrime/cyber insurance agency.

8) *Implement passwords and encryption* – Ensure users are forced to use strong passwords and, if possible, multi-factor authentication (MFA). Use MFA in every financial area and on every access to the internet.

9) *Rely on your experts* – Confirm that your outside CPA is up to speed on current cyber threats and responses.

10) *Back up data* – Verify that backed up data can be restored. Backups should be off-site, off network, or stored in the cloud and encrypted.

and consults with contractors on financial and operational matters. Jennifer is the President of CFMA's Bluegrass Chapter and has presented at CFMA's Annual Conference & Exhibition and at the Ohio Valley Construction Conference.

Phone: 859-410-2380
E-Mail: jmiloszewski@blueandco.com
Website: www.blueandco.com

TOM SKOOG is a Principal at Blue & Co., LLC in Westerville, OH. He is responsible for the management of the firm's cybersecurity and data management service lines. Tom consults with clients on issues related to cyber and data security, data management, data reporting, and analytics and systems management.

Phone: 614-220-4131
E-Mail: tskoog@blueandco.com
Website: www.blueandco.com

DAMIEN STROHMIER, CCIFP, is Senior Manager at Blue & Co., LLC in Cincinnati, OH. He is a construction financial consultant and assurance provider that utilizes field labor experience and knowledge of construction operations to assist clients in executing their strategic plans. Damien serves on Allied Construction Industries' Young Professionals and Entertainment Committee. He is the multi-year presenter of financial leadership sessions for the Indiana Subcontractor Association and Indiana Constructors, Inc.

Phone: 812-584-4188
E-Mail: dstrohmier@blueandco.com
Website: www.blueandco.com