

## Five Steps to Protect Against Cyber Threats

Written by: Tamika Bass, Cybersecurity Director, Gannett Fleming

In today's ever-changing digital world, we continuously protect ourselves against cyber threats and look for ways to increase our security posture to preserve business continuity. Cybersecurity impacts all industries, and the architecture, engineering, and construction (AEC) industry is just as vulnerable. This blog presents ways to implement enterprise risk management processes.

### What is Cybersecurity Risk Management?

Cybersecurity risk management identifies, analyzes, evaluates, and addresses an organization's cybersecurity and data privacy threats and potential risks. Think of it as a strategy: implementing risk management strategies to mitigate and promptly address the most critical threats.

#### FIVE STEPS TO EFFECTIVE RISK MANAGEMENT

##### Step 1. Identify Risks

To effectively manage against security risks, you must identify them. First, you need to establish your valuable and critical assets, such as data networks, computer systems, devices, etc. You must also determine potential environmental risks and other cybersecurity threats, which you can do using ad-hoc findings, a formal risk assessment, penetration testing, vulnerability management, and future risk evaluation.



##### Step 2. Perform a Risk Assessment

This involves gathering information about your assets, vulnerabilities, and existing controls, and developing a risk register – a tracking document. A formal assessment determines and identifies areas that are susceptible to cyber attacks.

##### Step 3. Treat Risks

Treating risks includes:

- » **Remediation:** Implementing controls.
- » **Mitigation:** Reducing impact.
- » **Transfer:** Shifting risk.
- » **Acceptance:** Acknowledging tolerance level.
- » **Avoidance:** Removing exposure.

#### Step 4. Monitor Risks

Once you have identified and treated the risks, the next step is to monitor them. You should regularly – monthly – review your risk register to determine which cyber risks exist, your treatment strategy, and what plans of action and milestones (POAMs) are open. A POAM outlines the steps and milestones for remediation. Monitoring involves tracking the progress of these POAMs.

Another aspect is ensuring the implementation of your risk response plan. Regular assessments are also crucial to identifying new environmental risks. Risk management is ongoing, especially in cybersecurity, where unknown threats constantly emerge.

#### Step 5. Communicate Risks

Communicating risks is arguably the most important step. You must effectively communicate to senior leadership: be clear, concise, and stick to the facts. Help them understand the risks, treatments, action plans, and associated costs. The decision to remediate or accept a risk often depends on its impact and cost.

### TOP THREE RISKS FOR CYBERSECURITY IN AEC

#### Data Breach

Like a security breach, a data breach involves unauthorized access to confidential data. AEC firms store sensitive information, including building or system design, construction plans, client data, and employee and other sources of personal data. Protecting data confidentiality is paramount. Data breach impacts can include:

- » Intellectual property theft.
- » Financial loss.
- » Reputational damage.
- » Legal consequences.

#### Business Email Compromise

Business email compromise (BEC) incidents are on the rise. BEC is a sophisticated fraud scheme that targets businesses using wire transfers as a payment method, resulting in approximately \$8 million and rising in global daily losses. Cybercriminals identify organizations, often AEC firms, and initiate a grooming process.

Cybercriminals use numerous communication methods, including phone calls, emails, and texts. If you, as the victim, are convinced that this is a legitimate business transaction, you follow the wiring instructions and send the funds to the new account.

#### Phishing

Phishing involves sending fraudulent communications that appear to come from a reputable source, intending to steal sensitive data or deliver malware. It's one of the most common methods used to target AEC professionals.

There are various types of phishing attacks: email, voicemail, and smishing (text-based), with 90% occurring via email. Attackers use these methods to deceive individuals into giving up sensitive information or taking malicious actions. The impact on a firm can include:

- » Financial losses
- » Unauthorized access to sensitive project or client data.
- » Disruptions to operations.

Watch for red flags in all your emails, regardless of organizational or personal information threats. Cybercriminals often cast a wide net – they are looking to steal information, infect your machine with malware, or find ways to make money by selling your information on the dark web.

#### Ransomware Attacks

Ransomware is a type of malicious software designed to block access to your computer system or files until you pay a ransom. Cybercriminals like AEC firms because of the critical nature of infrastructure projects. They know that you rely on data to conduct your work, and if they can block access to that data, they believe you will pay the ransom to regain it.

Ransom demands are not always exorbitant; cybercriminals are more likely to receive payment if their demands are reasonable and affordable, which many businesses quietly pay to protect their operations. The true cost of a ransomware attack comes from losing access to your network and information. Consider how long you can survive without access to your computer and the data you need for your work. Additionally, think about how long it might take to recover lost data.

## MITIGATING AEC RISKS

### Proactive Approach

Developing and implementing a comprehensive cybersecurity policy is essential. This policy outlines what employees can and cannot do concerning information systems, ultimately protecting your organization. You should also conduct regular assessments to be able to treat them effectively.


Some say cybersecurity officials conduct too many assessments, even if we haven't fixed all the previous findings. However, it's crucial not to ignore or leave risks untreated because they can be exploited, significantly impacting an organization.

### Technology and Training

Investing in the latest proven security technologies is vital. It goes back to the cost of remediation versus the cost of acceptance. While investing in security technologies comes at a cost, it's an investment in keeping your organization safe. Providing regular training to all employees is equally essential. Training helps enhance awareness and the ability to recognize potential threats.

Just like the safety culture in the AEC industry, we need to emphasize a "see something, say something" mindset for cybersecurity. Reporting any suspicious activity or potential security threats is crucial. For example, if you spot phishing emails, report them promptly, allowing the IT department to take action promptly and mitigate them.

### Collaboration

Embracing collaboration is another significant piece of the puzzle. Collaborating and working together with cybersecurity experts strengthens defense mechanisms. Sharing information about threats and best practices within the industry is essential for a proactive cybersecurity approach. 



---

### About the Author

---

The cybersecurity director at Gannett Fleming, Tamika Bass has more than 15 years experience specializing in business continuity, disaster recover, IT security, and knowledge transfer. Tamika applies methods for assessing and mitigating risk, analyzing impacts, and managing incidents, as well as IT security experience including security auditing, governance risk and compliance, ITGRC implementation, and business continuity planning. Tamika can be reached at [tbass@gfnet.com](mailto:tbass@gfnet.com).

---

### About the Article

---

This article was written for the online [Gannett Fleming Blog](#). Founded in 1915, [Gannett Fleming](#) has been a driving force in shaping infrastructure and improving communities in more than 65 countries, specializing in natural resources, transportation, water, power, and facility-related projects. The company embraces sustainability and innovation in projects and internal activities and achieves results while being responsible stewards of the environment. A results-driven firm, Gannett Fleming is consistently ranked in the top one percent of engineering firms worldwide..

Any views and opinions expressed in this article may or may not reflect the views and opinions of the Construction Management Association of America (CMAA). By publishing this piece, CMAA is not expressing endorsement of the individual, the article, or their association, organization, or company.