eSENTIRE®

CHECKLIST

Architecture, Engineering and Construction:

The Three Biggest Cybersecurity Risks and How to Protect Your Data

Whether the motivation is financial, personal or for bragging rights, cybercriminals can compromise systems that drive operations and expose the data of a company and its business partners. The 2020 Verizon DBIR included construction industry data for the first time this year, recording 37 incidents, 25 with confirmed data disclosure[1]. The architecture, engineering and construction industries do not necessarily make headlines for cyberattacks, but cybersecurity should still be a business priority to protect operational risks and lucrative data.

Contruction, and related businesses, depend on high cash flow – they have to deliver project deadlines in order to be able to pay sub-contractors throughout a project life cycle. Cyberattacks can potentially shut down projects and cause business disruption losses, as well as lead to forensic investigations, PR costs, legal claims, damages and legal-defense costs.

These industries are increasingly relying on technology and the use of online networks to share project/client data and to connect to third-party supplier networks, often doing so remotely from job sites. With these advances, comes operational efficiency but also risk. As technology adoption increases, architecture, engineering and construction companies end up vulnerable to cybercriminals looking for opportunities, but most do not have the knowledge or resources within their IT departments to focus on cybersecurity, making them an easy target.

Lack of regulations begets limited guidance

Architecture, engineering and construction are not highly regulated industries, and since they are not an obvious target, there is little cybersecurity guidance out there. Some of the biggest annual reports that track cybersecurity do not even cover these verticals when breaking down their industry data. Yet, the threats exist as long as companies rely on technology and remote connectivity in order to conduct business. Architecture and construction industries have always focused on physical security, as job sites are often plagued by theft and vandalism but, failure to address cybersecurity threats can result in business disruption, unplanned costs and reputational damage if a breach occurs.

Biggest risks to the industry

Risk #1: Not prioritizing cybersecurity

Vandalism and theft of expensive equipment at job sites has always been a big concern for the industry, costing millions of dollars in losses each year and resulting in companies investing large budgets for physical security, such as security guards, tracking systems for equipment assets, fences and locks around job sites. Adequate budgets for cybersecurity are often overlooked simply because companies do not view themselves as high-risk targets, but a lack of investment in cybersecurity is precisely what makes these companies an attractive target for cybercriminals.

A ransomware attack that threatens to divulge clients' financial information will not only affect companies financially if they pay up, it could result in lost business and a damaged reputation if they don't.

Risk #2: Mobile workforce

The businesses of architecture, engineering and construction often take place outside the confines of a corporate headquarters at various job sites and locations. Workers utilize laptops, tablets and mobile phones to connect to company and supplier networks, accessing and exchanging critical business data. As in any industry, there are several cybersecurity issues to address with regards to mobile workers utilizing either a company-issued or a personal BYOD outside of the office. Weak passwords, unpatched software, third-party software tools, public Wi-Fi and theft of devices stored at job sites are all risks that need to be mitigated.

[1] 2020 Verizon Data Breach Investigations Report

Risk #3: Confidential information disclosure and third parties

Projects involve highly confidential information shared amongst collaborating parties (blueprints, bid information, building specifications, architectural drawings, employee records and financial information) that can prove valuable to cybercriminals and make companies a target for phishing and ransomware attacks. A high reliance on the exchange of information with suppliers and other third parties introduces another layer of risk. Architecture, engineering and construction companies cannot control what happens on supplier and business partner networks. So, it is imperative to have strong security controls in place.

Minimizing risk and protecting your data

While the risks of a distributed workforce and collaboration with third parties cannot be avoided, they can be mitigated by addressing the first risk of not prioritizing cybersecurity for your business. The increasing reliance on technology to conduct business in the construction-related industries creates a complex sprawl of disparate systems that need protection. Companies must assess their risks and build comprehensive security strategies to safeguard their business.

Security checklist:

□ **Assess security program maturity and policies**

- Perform an assessment of your current security program's overall maturity. Review policies, incident response planning and your overall security architecture, then align your security strategy and risk profile with your business objectives.

□ **Test prevention, detection and response capabilities**

- Perform a simulated attack to test your current defense measures and identify weaknesses in your external and internal security posture.

□ **Test user risk**

- Implement security awareness training to keep your employees up to date with the evolving threat landscape and turn them into your front line of defense. Test and track their progress with simulated phishing exercises.

□ **Identify and manage vulnerabilities**

- Perform routine scanning of internal and external vulnerabilities to put your security program to the test, solidify your defenses and stay on top of the ever-evolving threat landscape.

□ **Implement controls that detect attacks that bypass preventative measures**

- Protect your mobile (and in-office) endpoints with next-generation antivirus and endpoint detection and response capabilities that go beyond automated blocking of known threats. Endpoint security controls that can identify suspicious behavior and stop new and fileless attacks, with machine learning capabilities to detect threats that preventative technologies miss, are crucial to organizations with a distributed workforce.

□ **Conduct third-party vendor risk assessments**

- Develop a pragmatic vendor risk management program, including vendor classification and due diligence questionnaires in order to mitigate any risk that may currently exist and/or be introduced by new vendors.

Ready to get started? We're here to help.

Reach out and schedule a meeting to learn more.

eSENTIRE®

eSentire, Inc., founded in 2001, is the category creator and world's largest **Managed Detection and Response (MDR)** company, safeguarding businesses of all sizes with the industry-defining, cloud-native Atlas platform that removes blind spots and enables 24x7 threat hunters to contain attacks and stop breaches within minutes. Its threat-driven, customer-focused culture makes the difference in eSentire's ability to attract the best talent across cybersecurity, artificial intelligence and cloud-native skill sets. Its highly skilled teams work together toward a common goal to deliver the best customer experience and security efficacy in the industry. For more information, **visit www.esentire.com** and follow **@eSentire**.