wyliecrump

CYBER RISK AND DESIGN PROFESSIONALS

It has been years since design professionals transitioned from drafting tables to design software, and now the rapid emergence of AI and cloud-powered technologies promises to enhance project design and delivery while minimizing delays.

While these advancements offer numerous benefits, integrating technology into core processes also introduces new risks, particularly in cybersecurity.

High-profile incidents at large corporations often dominate the headlines, but it's crucial to recognize that small and medium-sized enterprises (SMEs) are frequently the targets of cybercriminals. In fact, according to NetDiligence[1], 98% of total claims originate from SMEs. Although the costs of attacks may be lower proportionally, they can still be devastating, with the average cost of a cyber incident in the last five years being $205,000 USD.

This highlights the vulnerability of smaller firms, which may not fully recognize their exposure and often lack the robust security measures that larger organizations implement. Given their reliance on technology, firms offering professional services are frequently targeted, representing 1,630 claims, or approximately 15% of the 10,464 claims analyzed. The most prevalent sources of malicious attacks are ransomware and business email compromise. Ransomware attacks occur when a hacker uses malicious code to lock you out of your system and demands a ransom payment to restore access.

Business email compromise, or social engineering, involves tricking an employee into making a fraudulent payment or divulging confidential information via email. Not all cyber incidents are malicious or targeted; a lost or stolen mobile device, inadvertent disclosure of sensitive information, or third-party software outages can also significantly impact your business or trigger regulatory reporting requirements.

A cyber incident can also lead to indirect costs such as project delays or missed bids, while eroding the reputation you have worked hard to build. Therefore, it's crucial to review your workflow to identify potential areas of risk and establish best practices for managing those exposures—utilizing internal controls, third-party vendors, or specialized cyber insurance.

WORKFLOW AND INFORMATION:

Design professionals rely heavily on computer systems to produce and distribute design documents, manage timelines, and collaborate with various parties throughout a project's lifecycle. Considering your firm's workflow, what would happen if you were unable to access your primary system?

Design professionals are often entrusted with the confidential and proprietary information of clients, subconsultants, partners, and employees, and have a duty to safeguard it. Taking inventory of the information you collect and how it is utilized is crucial to identifying the potential impact of a cyber incident on your business, employees, and clients. The larger and more complex a project, the more data is generated, increasing the need for stakeholder coordination. Consequently, these projects increasingly rely on technological tools for efficient management, including Building Information Modeling (BIM), Virtual Design and Construction (VDC), Artificial Intelligence (AI), Computational Design, and Virtual Reality (VR).

[1] *Source: NetDiligence-Cyber-Claims-Study-2024-Report-1.pdf*

If a threat actor gains access to one of these systems or a shared data environment, it could result in delays and significant financial losses, along with reputational damage. Geographic location also plays a role in data breach reporting obligations, which can vary widely across international borders and even between provinces or states. Companies operating in different jurisdictions must navigate varying notification timelines, reporting procedures, and data rights. Noncompliance with these regulations can result in substantial fines, legal penalties, and reputational damage.

RISK MITIGATION

In today's digital landscape, it's impossible to avoid cyber exposure while remaining relevant, making the mitigation of cyber risk a critical aspect of maintaining business continuity. Threats are constantly evolving, but implementing safeguards, staff training, and an incident response plan can help reduce vulnerabilities and make your firm a less attractive target. Collaborate with your internal IT team or a third-party provider to develop tailored cybersecurity measures. Basic security measures include keeping software up to date, regularly backing up and encrypting essential information, and utilizing multi-factor authentication and strong password requirements.

Not all data breaches result from targeted attacks; a lost or stolen device can lead to the loss of confidential information. Mobile device management, data encryption, and limiting access to authorized individuals can all help mitigate these risks. Contracts can also pose unexpected exposure risks, as they may include clauses related to data protection and notification. It's essential to review specific clauses and ensure your current protocols are adequate. Additionally, stay informed about legislative requirements in the jurisdictions where you operate.

Given the increasing prevalence of cyberattacks, experts generally agree that it's not a matter of if, but when your firm will be impacted. Even the most robust security measures can fall victim to attacks or human error. Establishing an incident response plan can minimize potential downtimes and reduce the impact of an attack by outlining what to do and who to contact. At a minimum, a plan should address contingencies for system access, data recovery—including crucial design documents—assess the extent of the breach, and outline stakeholder communication.

This is where cyber insurance can prove invaluable. It covers expenses and liabilities your practice may incur while also providing incident response services. Most policies include access to a breach coach who can coordinate legal, IT, and PR experts to manage your claim efficiently and reduce recovery time. This peace of mind allows you to focus on what you do best: delivering innovative and effective designs to clients.

CONCLUSION:

In conclusion, as design professionals increasingly rely on advanced technologies, the importance of robust cybersecurity measures cannot be overstated. The risks posed by cyber threats are ever-evolving, making it essential for firms to proactively assess their vulnerabilities and implement comprehensive risk mitigation strategies. By prioritizing cybersecurity and leveraging tools like cyber insurance, design firms can safeguard their assets, maintain client trust, and ensure continuity in their operations. The future of design hinges not only on innovation but also on the ability to protect that innovation in an increasingly digital landscape.

If you have questions specific to your business, or would like additional information, please reach out to your Wylie-Crump Advisor.

Jason Harrison, FCIP, CRM
Senior Associate, Wylie-Crump Limited

Jason Harrison is a Senior Associate with Wylie-Crump Limited and is focused on providing insurance advisory services to design professional firms and contractors. Jason spent 18 years as an underwriter prior to joining Wylie-Crump Limited with experience in design, construction and manufacturing.