ProWriters
A VICTOR COMPANY | VICTOR

Why Architects and Engineers Need Cyber Insurance

Images of architects and engineers (A&E) perched on stools at drafting tables, moving pencils and T-squares over paper blueprints, fail to capture today's reality. Now, these professionals rely on computers and digital tools to design, analyze, and manage construction projects.

Using such technology as building information modeling (BIM), computer-aided design (CAD), finite element analysis (FEA) software, project management platforms, and even augmented reality (AR) and virtual reality (VR), architects and engineers can create more complex and innovative designs, improve efficiency, and collaborate with colleagues and clients in real time.

But even as technology revolutionizes the A&E industry, it exposes design professionals and their businesses to serious cyber threats.

A 2023 study from Dodge Construction Network and Egnyte revealed 59% of architects, engineers, and contractors had experienced a cyber security threat in the previous two years.

Cyber Risk and Exposures in the A&E Industry

As a high-cash-flow and deadline-driven industry, the A&E sector is particularly susceptible to both cyber attacks and their disruptive consequences. Among the cyber risks today's architects and engineers face are:

- **Data breaches**
  Architectural and engineering firms store vast amounts of client information, project details, and proprietary designs. Consequently, they are prime targets for hackers looking to steal sensitive data for financial gain. Data breaches can have severe repercussions, including legal issues, financial losses, damaged reputation, and compromised client trust.

- **Ransomware attacks**
  In ransomware attacks, hackers encrypt a firm's data and demand a ransom in exchange for the decryption key. Ransomware attacks can cause significant disruption to operations and result in the loss of critical project data if proper backups are not in place.

- **Phishing scams**
  Cyber criminals often use deceptive emails or malicious websites to trick individuals into revealing login credentials or other sensitive information. These scams can lead to unauthorized access to confidential data, financial theft, or the installation of malware on the firm's network.

- **Attacks on the Internet of Things (IoT)**
  "Smart" devices and building technologies, such as connected HVAC systems and security cameras, can be vulnerable to cyber attacks if not properly secured. Hackers can exploit the IoT to gain unauthorized access to a firm's network or disrupt building operations.

Real-World A&E Claims and Examples

- Architecture, engineering, and construction (AEC) firms are more than twice as likely as those in other industries to be the target of ransomware attacks.
- The AEC industry is the second-most-targeted for email fraud, seeing an average of 61 attacks per company over a three-month period.
- In 2023, Miami-based home builder Lennar experienced a data breach in which the names and Social Security numbers of 7,448 customers were exposed. Lennar offered the affected customers 24 months of free credit monitoring services, as well as guidance on reporting incidents and placing a fraud alert or security freeze on a credit file.
- In 2022, Sheppard Robson—one of the UK's biggest architectural practices, employing nearly 400 people—was hit by a ransomware attack and extortion attempt, and it was forced to disconnect all its systems from the internet. In ransomware attacks, the threat actors forward links to the data they steal to their victims' business partners and workers, where the data can be viewed and downloaded from a "shaming blog."

In 2023, cyber security firm Cisco Talos warned mostly French-speaking architects, engineers, and graphic designers in several countries, including the U.S. and Canada, that hackers could be targeting their computers with cryptocurrency-mining malware. Why? AEC professionals commonly need computers with high GPU power for their legitimate software applications—the same kind of powerful computers needed to mine cryptocurrency.

Cyber Insurance Helps to Mitigate Your Risk

The importance of Cyber Insurance for architects and engineers can't be overstated.

With the increasing frequency and sophistication of cyber attacks, having a robust Cyber Insurance policy in place is essential for protecting your firm and ensuring you can continue to provide the high-quality services on which your clients rely.

Cyber Insurance can cover the frequently and frighteningly high costs associated with data breaches, ransomware attacks, and other cyber incidents, including:

- Costs associated with business interruption
- Expenses for data recovery and system repair
- Notification and crisis management expenses
- Legal costs and settlement expenses