AIATrust
Where smart architects manage risk®

Cyber Threats Are Real

Synopsis: The Threat is Real: Cyber Attacks Against Architectural Firms

Many architectural firms are tempted into believing they're safe from cyberattacks because they don't consider their data to be "sensitive" enough to attract criminals. Cybercriminals are sophisticated, deliberate and efficient in how they monetize their efforts. If you use the internet for any reason – even if just for basics such as email, submitting invoices or sharing designs – you are at risk – and cyber risk is a problem for every professional services firm.

A risk report published by the AIA Trust is filled with real case studies and highlights how very attractive architectural firms are to cyber criminals, the most successful attack vectors currently in use, and the potential regulatory and reputational impact in the event of a data privacy violation. A defensible cyber security strategy provides a framework to create a safer, more cyber resilient organization. But in the event of an incident or breach, it also helps you develop a validated, auditable narrative to reply to the question: "*How does your firm manage cyber risk?"*

The authors combine extensive technical and legal experience to recommend actionable steps firms can take in order to develop a defensible security strategy, including governance, policies, infrastructure, people, and relationships. Having responded to thousands of cyber incidents, the authors also examine key practices such as the transfer of risk via cyber insurance, multifactor authentication, and third-party risk and how they can benefit architectural firms.

The report gives an overview of recent trends in cyber risk for any firm that might be harboring a false sense of security that it is at low risk for an attack. These risks include a business email compromise, a major threat that can affect anyone with an email account, and a ransomware attack for which every business is a target, particularly those with lax security.

Importantly, the report discusses security measures that all firms should consider, starting with the five pillars of defensible cyber security which include governance, policies and procedures, infrastructure and standards, and people and training. Specific practices are prioritized for firms to more effectively protect their data and their bottom line.

The report clarifies that an architectural firm is as likely a target for cyber-attackers as any enterprise in any business sector – your data IS valuable and may even be used as a springboard into a client's environment. Ultimately, gaining a better understanding of the risks you face along with greater insight into how to defend and protect what you work for, is an ongoing goal.

Published by the AIA Trust, TheAIATrust.com