Prepared for Berkley DP by:

BDP® BETTER BY DESIGN a W. R. Berkley Company

Kroll®

The Top Cyber Security Risks for Architectural & Engineering Firms

Kroll routinely applies the three tenets of information security: confidentiality, integrity, and availability of data to the unique requirements of each client. This framework assists Kroll in identifying what assets are most critical to a corporation. Protection of corporate data and information networks relies on a rigorous application of this triad. Furthermore, an inquiry focused on these concepts allows a principled approach to safeguarding a corporation's data and allows corporate decision makers the clarity they need while controlling the desire to protect everything all the time. In essence it forms the basis for a robust risk management program.

In the case of architectural and engineering firms, data availability is certainly at the forefront of these concerns. With the evolution of BIM software, the level of collaboration between architects, contractors, subcontractors, and engineers is unprecedented. While this has undoubtedly had many positive benefits, it has also given rise to new challenges that architectural and engineering firms are, in many cases, considering for the first time. Firms are now generating and storing large amounts of data on their internal networks and access to that data is crucial to meeting client objectives. While the increased appetite for sharing access to this data has in large part caused concerns about confidentiality to dissipate, it has given rise to greater concern about maintaining the integrity of critical project data. What is more, nearly all firms house personally identifiable information (PII) data that needs to be protected as a compromise could lead to required data breach notification under state breach notification laws.

With this in mind, Kroll acknowledges the top seven cyber security risks posed to architectural and engineering firms that could impact their access to information, the integrity of that information, and in some cases the confidentiality of that information.

Risk#1: Critical project data could be lost due to malicious code in your network. The actions of a malicious third party could either render your data inaccessible, cause your data to be altered or, worse yet, completely destroyed. This would impact your ability to meet client objectives and deadlines and result in the loss of intellectual property. Although you may not consider your firm a target for a malicious attack, the reality of today's cyber environment is that every company is at risk – especially in circumstances where you are opening your network to outside parties who can introduce malicious code unwittingly. Savvy attackers who gain access to the data your firm's day-to-day business relies upon (even if it's not something you consider confidential) can encrypt this data using ransom-ware and extort your organization for money in order to regain access to this information.

Risk #2: A malware infection can compromise your network integrity and be difficult to detect. We've seen an increase in the use of polymorphic and wormlike viruses that are created to continuously change the way the malicious code appears so that it is harder to detect. The end result is that your

Certain Kroll companies provide investigative services. State licensing information can be found at www.kroll.com/compliance. These materials have been prepared for general information purposes only and do not constitute legal or other professional advice. Always consult with your own professional and legal advisors concerning your individual situation and any specific questions you may have. 01/03/2014

network could be compromised, allowing unauthorized third parties to have access to sensitive firm information such as project files, client information, or even company financial accounts. This not only poses a risk to your firm; sophisticated malware can create liability issues by leveraging your network to compromise and infect other networks (e.g., clients, partners, etc.) with which you may be integrated.

Risk #3 A Distributed Denial of Service (DDoS) attack could render your network inaccessible. A DDoS, attack occurs when an attacker uses multiple computers to barrage a victim's network with meaningless data connections thereby preventing real communications from getting through to the victim. This essentially makes the victim's computers and network unavailable to users. Such an attack could make critical information inaccessible to firms, contractors, subcontractors, and their clients. This type of attack is another common extortion scenario when attackers recognize that a loss of access to the information on a network is more costly to an organization than paying a sum to the attacker to end the DDoS attack.

Risk #4 Failure to back-up your data can lead to an inability to recover after an attack. Many cyber-attacks result in the loss of data and proprietary information, much of which can't be re-created. In the age of soft blueprints, it is important that you have confidence that your back-up processes work and comply with the statute of limitations for maintaining project record documentation, as well as complying with subpoena requests and contractual obligations to your client.

Risk #5: A compromised network could negatively impact your reputation. Clients make business decisions on the basis of a strong reputation, and part of your reputation includes the integrity of the project data your firm maintains. It is critical to ensure the plan information accessed from your systems can be trusted. Cyber-attacks such as fake emails that appear to be sent from your site, website defacement, or email hijacking can affect not only your firm's reputation, but it may also directly affect your clients. For instance, if a malicious third party is using your email system to send infected links to your clients, the reputational damage could be fairly significant. Not only that, the fact that clients now know your network has been infected could call into question the integrity of the design data your firm is trusted to protect.

Risk #6 Disgruntled employees can cause significant data loss. Your in-house team of architects and/or engineers has a legitimate need for systems access, but a disgruntled employee can cause problems ranging from deleting important files to sharing proprietary or confidential client information with unauthorized third parties. Kroll has worked cases where a terminated employee maintained access to data because access credentials had not been disabled. A rogue employee with access to your design software could wreak havoc in a number of ways, including tampering with the integrity of design documents, deleting critical design data, etc. You should also consider what other information these employees may have had access to that is critical to the operations of your business, such as passwords to company bank accounts and payroll systems.

Certain Kroll companies provide investigative services. State licensing information can be found at www.kroll.com/compliance. These materials have been prepared for general information purposes only and do not constitute legal or other professional advice. Always consult with your own professional and legal advisors concerning your individual situation and any specific questions you may have. 01/03/2014

Risk #7: The loss of sensitive employee data could impact your bottom-line. All firms have sensitive data. While the availability of access to project data is undoubtedly the foremost concern for architects and engineering professionals, there are secondary concerns that need to be considered because they are tied to regulatory obligations regardless of industry. Even the smallest firms maintain some personally identifiable information (PII), typically employee information that includes identifiers such as dates of birth or Social Security numbers. This type of information is directly tied to state breach notification laws that, in the event that your firm experiences a breach of PII, you will be required to comply with.

About Kroll

Kroll, the global leader in risk mitigation and response, delivers a wide range of solutions that span investigations, due diligence, compliance, cyber security and physical security. Clients partner with Kroll for the highest-value intelligence and insight to drive the most confident decisions about protecting their companies, assets and people.

Kroll is recognized for its expertise, with 40 years of experience meeting the demands of dynamic businesses and their environments around the world. Headquartered in New York with offices in 29 cities across 17 countries, Kroll has a multidisciplinary team of 700 employees. Learn more at krollcybersecurity.com.

About the Author

Timothy P. Ryan is a Managing Director with Kroll and the Cyber Investigations Practice Leader for North America. Tim joined Kroll's Cyber Investigations Practice after a distinguished career as a Supervisory Special Agent with the Federal Bureau of Investigation (FBI), where he supervised the largest Cyber Squad in the United States and also led one of the FBI's largest computer forensic laboratories. An expert in responding to all forms of computer crime, attacks, and abuse, Tim has led complex cyber investigations involving corporate espionage, advanced computer intrusions, denial of service, insider attacks, malware outbreaks, Internet fraud and theft of trade secrets. Tim is an adjunct professor at Seton Hall University School of Law.

Certain Kroll companies provide investigative services. State licensing information can be found at www.kroll.com/compliance. These materials have been prepared for general information purposes only and do not constitute legal or other professional advice. Always consult with your own professional and legal advisors concerning your individual situation and any specific questions you may have. 01/03/2014