AIA Trust
Where smart architects manage risk®

An Architect's Guide to Managing Cyber Threats

By Kevin Collins, RPLU, Associate AIA
Senior Vice President, Victor O. Schinnerer & Company

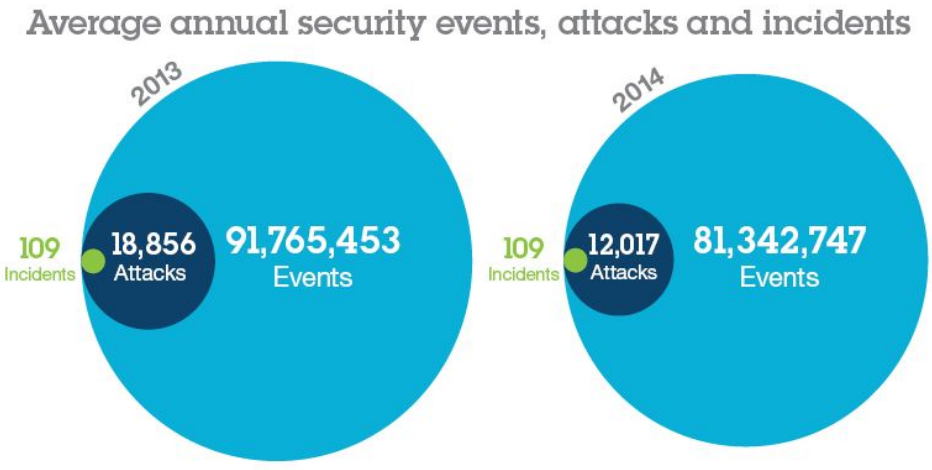
It can happen to anyone. Cyber attacks are everywhere and they're happening more frequently. Many of the notable data breaches that have occurred over the last few years were the result of attacks that exposed credit card data and volumes of personally identifiable information. These breaches potentially compromised the safety of the affected organizations and endangered the security of millions of individuals who were exposed to possible identity theft.

As an architect, if you don't think you need cyber protection or don't believe someone would want to hack into your system, you may already be in trouble. It's tempting to think that since you are an architectural firm and not part of one of the most frequently attacked industries that transact business online, you may not have much to worry about. Unfortunately, that thinking is dangerous.

Design firms of all sizes and segments are at risk and are being attacked. For example, a prominent design firm in Seattle was held up by ransomware. An architectural firm in Maryland was tricked into sending their insurance premium to a hacker. Another architecture firm suffered a loss of more than $500,000 in billable hours after two ransomware attacks rendered the firm's files unusable for days until the data was restored.

Different types of cyberattacks:

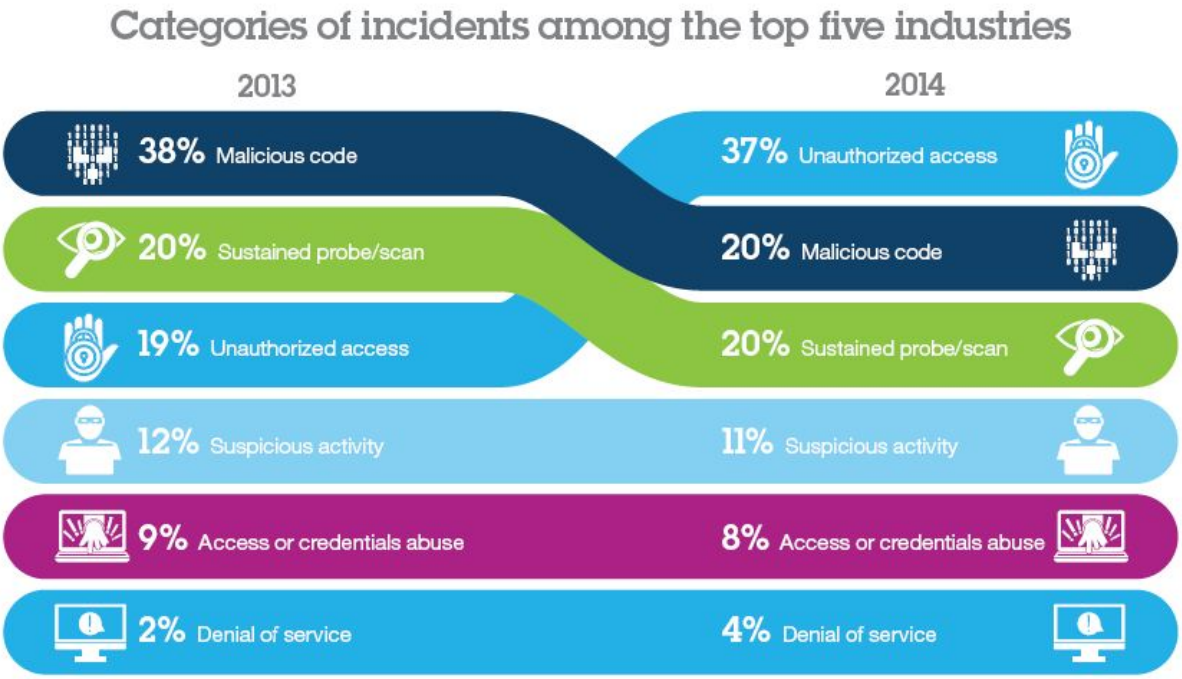
- Security event: an event on a system or network detected by a security device or application.
- Security attack: a security event that has been identified by correlation and analytic tools as malicious, activity that is attempting to collect, disrupt, deny, degrade or destroy information system resources or the information itself.
- Security incident: an attack or security event that has been reviewed by an analyst and deemed worthy of further investigation.



IBM 2015 Cyber Security Intelligence Index

Over the past five to ten years, malicious code and sustained probes and scans accounted for most of the security incidents. However, all that changed in 2014 when certain types of unauthorized access incidents rocketed to the top, accounting for 37 percent of the total. However, with an ever-expanding array of malware for which attackers may choose—including viruses, worms, Trojans, spyware and adware—it seems fairly certain that malicious code incidents will continue to wreak havoc for the foreseeable future.

Attackers are typically interested in finding the path of least resistance and these methods are capable of providing that. The simple failure to keep up with needed patches and consistently updating your systems may be the simple driver that creates the opportunity for bad actors to infect your system.



Source: IBM 2015 Cyber Security Intelligence Index

In a world where more and more companies, people and devices are connected to the Internet, greater focus must be placed on security and privacy. While the Internet has opened us up to a world of possibilities and global connectivity to millions, the very strength of the network – the speed, openness and access – creates a myriad of vulnerabilities. Additionally, securing a business' network grows infinitely more complex as information pours in from thousands of devices through public web-based and cloud service providers.

Architectural firms must educate their employees, clients, and vendors about these risks and take the appropriate actions to protect their information. Please follow these security essentials to create a more secure environment for your practice:

Security Essentials

1. *Build a risk-aware culture*

Whether you open a dubious attachment, click on an unknown link, use an infected flash drive, or fail to install a security patch on your laptop, everyone is at risk. Educate your employees about cyber risks and the measures that they can take to protect themselves and the company.

2. *Manage and report all incidents*

Report all cyber and other potential attacks. Security breaches that occur at different companies or different locations may be related, but this can only be discovered if incidents are reported and analyzed.

3. *Defend the workplace*

Ensure all devices connected to a network – from a laptop to a printer to a smart TV – are up to date with the latest security software and follow all cyber security management and policy enforcement.

4. *Security by design*

One of the biggest vulnerabilities in information systems – and wastes of money – comes from implementing services first and adding on security as an afterthought. Build security into your network from the beginning and maintain regular tests to track conformance and compliance.

5. *Keep it clean*

Cyber criminals target people and businesses that are using old, out of date software. Maintain a comprehensive security system and install necessary updates and patches as they are released.

6. *Control network access*

Companies that channel registered data through monitored access points will have a far easier time spotting and isolating malware.

7. *Security in the clouds*

If your company utilizes public cloud data centers, ensure you have the tools and procedures in place to monitor possible threats and isolate your data from other companies in that data center.

8. *Patrol the neighborhood*

Ensure your vendors and clients are also aware of your risk-aware culture.

9. *Protect the company's crown jewels*

Every company has crown jewels, whether it is scientific data, acquisitions documents, or clients' financial and personal information. Whenever your company carries out an inventory, critical data should get special treatment – guarded, tracked and encrypted as if the company's survival depends on it.

10. *Track who's who*

Ensure you have procedures in place to manage the access and permissions of your employees. If an employee leaves, you must have the control to revoke any access they have to company, client and vendor information.

Source: IBM Security Intelligence 2015

Although dealing with risks such as professional liability, client expectations and solving difficult design issues are often easier to address, more interesting, or may be more top-of-the-mind for every architectural firm, reminding yourself that you are a business and are not immune to the risks of technology and cybercrime is a great first step to addressing these risks proactively.

Implement the 10 steps listed above. You may also want to consider cyber liability insurance to protect your firm. Find out what you need to know about cyber liability coverage in the Architect's Guide to Buying Cyber Liability Coverage – to help transfer your cyber risks, evaluate the cyber liability policy options available to you, and select the best match in terms of limits and coverage to meet your needs.

Insurance underwriter, Victor O. Schinnerer & Company, Inc., works with the AIA Trust to offer AIA members quality risk management coverage through the AIA Trust Professional Liability Insurance Program, Business Owners Program, and Cyber Liability Insurance Program to address the challenges that architects face today and in the future. Detailed information about both these programs may be found on the AIA Trust website, TheAIATrust.com.