June 2014

Contact:
Timothy J. Toohey
Partner
213.417.5324
ttoohey@mpplaw.com

Privacy and Data Security Trends and Design Professionals

Although we are only half-way into the year, 2014 is shaping up to be a banner year for privacy and security issues. Data breaches, like the ones affecting Target, Michaels, and Nieman-Marcus, are almost a daily news occurrence. Because design professionals, like everyone else in our information-intensive economy, communicate and collaborate electronically, they too are vulnerable to cyber-attacks. Even if they do not perceive themselves a target, architects and engineers may be subject to such attacks because they hold and process information that is of perceived value to others, including client design, specification and engineering data. Foreign-based hackers may target them precisely because professionals believe that they are "below the radar" and have put fewer defensive measures in place than their clients. In this environment, design professionals need to be aware of the pattern of attacks on data and take measures to minimize their risk.

Breaches on the Rise

The number and severity of "breaches," which result in disclosure of data, and cyber "incidents," which compromise the integrity or confidentiality of information assets, continues to rise. The Verizon 2014 Data Breach Investigations Report, which surveyed a total or 63,437 security incidents and 1,367 breaches from 2013, found that almost every economic sector has been subject to an increasing number of both data breaches and incidents. The Verizon report further highlights the fact that both "professionals," including architects, engineers and related services and other professionals, and others in the construction industry, including contractors, are significant sources of security incidents. Only the public sector, finance and retail had more security incidents in 2013 than did professionals. The report also indicates that the main types of attacks on professionals are "denial of service attacks" and "cyber espionage." Contractors suffered considerably fewer attacks than professionals, but had much more varied attack vectors, including insider misuse, theft/loss, cyber-espionage and cyber-espionage.

Types of Attacks

Denial of service (DoS) attacks typically compromise the availability of networks and systems through network and computer applications. DoS attacks are launched by a variety of actors, including foreign governments and private entities, to slow or shut down traffic by legitimate users. The typical

mechanism for a DoS attacks is directing massive amounts of traffic to a legitimate site from a compromised device called a "bot" or a network of devices called a "botnet." Although DoS attacks do not usually result in extraction of data from the attacked computers, they may be part of a broader effort launched to either gain publicity about a particular business or its practices by shutting down traffic to a site. Analysts advise that even low profile businesses, including architecture and engineering firms, may be subject to attacks by "hactivists," particularly if they are involved in a controversial project, such as an airport or a power plant.

In contrast to DoS attacks, cyber espionage often results in loss or "exfiltration" of data through unauthorized system access by state-affiliated spies, particularly from East Asia and Eastern Europe. Although professionals are not the only targets of cyber espionage, they had in 2013 the second highest number of known attacks, after public entities.

Cyber espionage attacks typically occur through the use of malware and social engineering, particularly "spear-phishing" e-mails that includes information obtained from social networks, such as the names of colleagues, references to recent company developments, or personal information about the purported sender or user. For example, a user may receive a seemingly genuine e-mail from a known sender that prompts the user to open an attachment or click a link within the message that appears to be genuine, such as an Excel spreadsheet containing recent sales figures. When the user clicks the link, the file then installs malware on the entity's system that opens a backdoor allowing the attackers to extract internal operating materials, secrets, plans, designs and credentials from the company's computer network. In contrast to the "phishing" attacks of some years ago, which often contained crude spelling errors and other mistakes, modern spear-phishing attacks are sophisticated and the e-mail messages may seem genuine. As troubling as the attacks themselves is the fact that cyber espionage attacks are particularly difficult to discover. The Verizon report found in 2013 that 62% of the attacks took months and that 5% took years to discover.

The US Department of Justice's May 19, 2014 indictment of five Chinese military hackers for cyber espionage highlights the vulnerability of design professionals to such attacks. The indictment alleges that a Chinese hacker "stole confidential and proprietary technical and design specifications for pipes, pipe supports, and pipe routing within [power] plant buildings" from Westinghouse to advantage a Chinese state-owned enterprise. Although the spies took information directly from Westinghouse, design professional firms are also likely victims of such attacks because they have plans, diagrams and

specifications of interest to foreign authorities. Although companies are understandably reluctant to self-report such attacks, one consultant has cited an example of an executive at an engineering firm who received an e-mail purporting to be from the CFO of the company. Although the e-mail contained spelling errors, it transmitted a zip file attachment that launched malware into the system. Because of the sophistication of these attacks and the fact that design professionals are the custodians of data that is of interest to state-sponsored actors, they need to develop robust risk management techniques to prepare themselves for attacks.

Action Items for Designers

The first thing that design professionals should do to fend off the risk of attacks is to implement fundamental good practices. These practices include patching all software, using and updating anti-virus (AV) software, training users on proper use of networked systems, segmenting networks so that users do not have access to the entire network, keeping logs of network activity, and implementing other technical protective measures. Most importantly, design professionals should realize that they are not immune from attack and scrutinize e-mails carefully. When in doubt, do not open questionable e-mails, particularly those with attachments.

The second thing that design professionals should do is to adopt internal policies and procedures to prepare them to address security risks and to deal with any incidents and attacks that occur. For example, architecture and engineering firms and their counsel should undertake an internal privacy and data security policy assessment to determine if there are any gaps in the internal procedures and systems needed to prevent and detect data breaches and incidents. Depending upon the scope of their operations, design professionals should also assess whether their data transfer mechanisms include adequate safeguards to ensure security of proprietary and personal information and to comply with their contractual and legal obligations. Firms should also consider adopting a data breach incident response plan to help minimize the risks associated with unauthorized access to information so that they can efficiently respond to any incident or breach.

Finally, in conjunction with other professional advisers, including insurance brokers and counsel, design professionals should also review their insurance coverage to ensure that they are adequately covered in the event of a data incident. Design professionals may wish to contact Dealey Renton & Associates', which provides information relating to available cyber insurance coverage and its benefits.

About the Author

Tim Toohey is partner with Morris Polich & Purdy LLP in Los Angeles and is the head of the firm's Cyber, Privacy and Data Security team. He is a US and EU Certified Information Privacy Professional (CIPP/US and CIPP/EU). Tim is the author of Understanding Privacy and Data Protection: What You Need to Know to be published in early 2014 by Thomson Reuters/Aspatore.