MGM

MANION GAYNOR & MANNING LLP

201 Spear Street, 18th Floor
San Francisco, CA 94105

415 512 4381 *main*
415 512 6791 *fax*
www.mgmlaw.com

Don't Make Your Business a Target for Hackers

By David M. Fox

Sony. J.P. Morgan Chase. Home Depot. Target. Starbucks. Anthem. Turbo Tax. Ashley Madison. The U.S. Government. All have fallen victim to security breaches due to hackers or thieves. All have been sued in class actions as a result. Apple, which recently disclosed that its App Store had been hacked, is sure to follow. Attackers have absconded with intellectual property, architectural specifications, drawings, financial information, credit card numbers, Social Security numbers, personnel files, medical records, and private communications, causing stress to the customers, employees, and business partners of these entities and costing the entities themselves millions of dollars.

While the breaches of these large entities have dominated the headlines, hackers are increasingly targeting small businesses. Hackers can be anyone from a disgruntled former employee to an online prankster to a criminal organization. According to Chris Wysopal, chief technology officer, chief information security officer, and co-founder of Veracode, a leading data security firm, hackers have "taken note" of every business's reliance on software and are "compromising systems at an alarming rate."[1] Symantec, an Internet security firm, estimated that 60% of cyber-attacks in 2014 were directed at small and mid-size businesses.[2] According to First Data, 90% of breaches impact small businesses. On average, the cost of a data breach to a small business is $36,000.[3]

As these attacks have wreaked havoc on the business community, the plaintiffs' bar has cashed in and is increasing its efforts to extract settlements from "data breach" defendants.
Small businesses should not delude themselves into thinking that the plaintiffs' bar is only after large corporations. Even businesses with few employees can have extensive exposure. For example, a restaurant may serve hundreds of people per day, with many of those customers using credit cards. A business may possess the Social Security numbers of dozens of former employees. A doctor's office will have sensitive medical records, likely in electronic form, of dozens, if not hundreds, of patients. A company may also store valuable intellectual property on

[1] Chris Wysopal, *Software Security: On the Wrong Side of History*, RECODE (Aug. 13, 2015), http://recode.net/2015/08/13/software-security-on-the-wrong-side-of-history/.

[2] Symantec, *Internet Security Threat Report: Vol. 20* (Apr. 2015), *available at* http://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf.

[3] First Data Market Insight, *Small Businesses: The Cost of a Data Breach Is Higher than You Think*, at 1 (2014), *available at* https://www.firstdata.com/downloads/thought-leadership/Small_Businesses_Cost_of_a_Data_Breach_Article.pdf

its server—potentially belonging to a client. These are all targets for hackers that could result in costly litigation.

What Employers Can Do

Many hackers find their targets simply by searching the internet for unsecured sites, and small businesses bear the brunt of these attacks. By taking some simple, affordable (oftentimes free) steps, employers can protect themselves, make their systems unattractive to hackers and disgruntled employees, prevent corporate espionage, and stay out of the courtroom:

- **Enact strong password requirements:** Each employee should have her own computer account requiring a login and password. Passwords should be complex (more than six characters, containing at least one number, upper and lower case letters, and a special character) and expire periodically so that one misplaced password does not indefinitely expose the business to potential breaches. Businesses should require different passwords for different applications so that any breach can be contained to a limited portion of the enterprise's data.[4] These password requirements should carry over to any mobile devices.

- **Secure the internet:** Employers should institute download controls to prevent employees from downloading spyware or malware that could expose the business's data. Web filtering software like Barracuda can be employed to prevent employees from visiting dangerous websites. Anti-virus software should also be installed to identify and neutralize threats.

- **Secure the workplace and devices:** The workplace should also be physically secure. If an employer provides laptops to its employees, they should be labeled and assigned. All devices should be encrypted. There are many free programs that can encrypt devices. For example, BitLocker is a popular encryption tool that is included on all Microsoft computers. Retail businesses should make sure their point-of-sale systems are used exclusively for customer transactions, with no access to the greater internet permitted. Additionally, if a business engages a cloud provider to host its data, it is vital to obtain a clear understanding of the steps that such provider is taking to keep that data secure.

- **Encryption**: Employers should employ encryption keys on plans, specifications and other intellectual property. By encrypting the information, it ensures the confidentiality of such information as it flows over networks, as it is stored, and as it is used – either within the architectural/engineering firm or at remote locations.

- **Educate employees:** Education is also a valuable tool to prevent breaches. Employees should be informed on how to recognize phishing attempts and corrupt emails. A breach will often occur because an employee clicks on a malicious link or attachment. Teaching employees to recognize and report these threats will minimize the danger from these

[4] These passwords can be securely stored with password manager software.

hacking attempts. It is critically important to create not only legal obligations for employees to safeguard the company's confidential information, but also to impress upon them the importance of doing so. Employees should be reminded of their obligation to maintain the secrecy of the company's proprietary information through regular training and audits.

- **Protect electronically stored confidential information:** There is simply no reason for employees who are not working on a particular project to have access to confidential information relating to the project, or for employees who are working on a section of the project to have access to all of the project's intellectual property. Steps can almost always be taken to limit access to confidential information to only those who need to see it.

- **Have a sound system in place at the end of employment relationship:** An employer should always conduct an exit interview with departing employees and require an attestation that he or she is not taking any confidential and/or proprietary information to a new employer. It is absolutely critical for a company to learn the departing employee's future plans and, more specifically, if the departing employee intends to join a competitor or start his or her own company. Review of email history and internet access of departing employee by an outside security consultant can assist an employer in discovering corporate espionage.

- **Consider engaging a security consultant:** A business can also hire a professional to test the business's perimeter security, and/or to assist in crafting a workable, cost-effective security solution.

Even with best practices for protecting intellectual property, architectural/engineering firms are still vulnerable to having their confidential information, intellectual property rights and trade secrets misappropriated. Accordingly, it is crucial that an architectural/engineering firm not only continuously re-evaluate its practices, but also that it consult with security and legal counsel to make sure it is protecting its valuable information in a manner that preserves all available legal protections. By being proactive, an employer can protect its data, its employees, its customers, and in the long run, its bottom line.

David M. Fox is an associate at Manion Gaynor & Manning LLP. He maintains a diverse civil litigation practice, concentrating in complex commercial litigation, employment litigation, intellectual property litigation, and products liability. Dave's employment litigation experience includes representing businesses in Wage Act, discrimination, retaliation, trade secret, and non-competition/non-solicitation actions at the state and federal levels. Dave has also litigated cases involving data security.

MANION GAYNOR & MANNING LLP

About Manion Gaynor & Manning LLP

Manion Gaynor & Manning LLP provides innovative, responsive and aggressive representation for clients facing high-stakes litigation. We navigate complex, high-stakes, multi-jurisdictional matters without unnecessary process, inefficiency or expense. We are the law firm of choice for numerous Fortune 500 companies and some of the most iconic brands in American business. Clients value our guidance on sophisticated matters ranging from complex commercial and business disputes, toxic tort and products liability, professional liability, intellectual property, real estate, employment, to white collar and regulatory issues. With fully integrated offices in Boston, Los Angeles, New Orleans, San Francisco, Wilmington, Hattiesburg, Lake Charles, and Providence, we have the requisite infrastructure to handle the most complex cases. Find us at mgmlaw.com.