$1.50 VOL. 39 NO. 25 www.ocbj.com JUNE 20-26, 2016

ORANGE COUNTY BUSINESS JOURNAL

Cybersecurity Strategies for Small and Middle-Market Companies

By Mike Hornak, Partner, and Marc Boiron, Associate, Rutan & Tucker

RUTAN

RUTAN & TUCKER, LLP

The rise of cyber incidents has resulted in a focus on best practices to prevent, plan for and respond to those incidents. Large companies are able to implement most of those best practices; however, the limited resources of small and middle-market companies require that those companies rely on practices which, albeit not best practices, nonetheless will help protect the companies and their boards of directors from liability, and protect company assets and third party assets from cyber events.

Many small and middle-market companies ignore even the most basic cybersecurity, relying on the mistaken notion that only larger companies are the targets of cyberattacks. The available data is to the contrary. As large companies implement best practices in cybersecurity, cybercriminals increasingly target smaller companies that have not implemented adequate security practices. When cyber data is stolen, those companies may ultimately be subject to litigation based on theories of negligence, breach of contract, and breach of federal or state statutes, among others claims.

Any cybersecurity strategy for small and middle-market companies must consider the consequences of the inevitable cybersecurity event, including litigation risk, lost cyber assets, disruption of the business, and lost customers and clients. The governing body and senior management should be involved in determining the company's cybersecurity strategy, including the resources that will be allocated to cybersecurity.

Small and middle-market companies can take a few inexpensive steps to decrease the likelihood that those companies will face a data breach, or at least mitigate the consequences of a breach. Below are but a few of those inexpensive steps.

Training

There are limited cybersecurity measures that are as cost-effective as employee training to prevent a broad range of breaches that result from or are contributed to by employee error. Employee-related data breaches can be reduced through a mandatory training program that can be inexpensive to establish and maintain and can be carried out internally, combined with web-based training programs. A good training program should be updated from time to time, incorporated into the employee onboarding process and provided to existing employees no less than annually.

Although a good training program has many facets and will differ by industry, key aspects include (i) making employees aware of the various types of cybersecurity threats, (ii) informing employees on how and when to report cybersecurity threats, and (iii) instructing employees on key points of access to the company's data (such as unauthorized software installation, accessing public Wi-Fi, inserting removable media, downloading or uploading corporate data to mobile devices, and phishing emails). In-person cybersecurity training should be considered because employees typically pay more attention and ask more questions than when training is provided online; however, online updates or reminders

Mike Hornak

Mike Hornak is co-chair of Rutan & Tucker's Cybersecurity, Privacy, and Corporate Governance practice group. His expertise extends to intellectual property disputes (including cybersecurity), shareholder and partner governance, the defense of consumer and shareholder class actions, and commercial litigation. He also advises clients on data protection schemes and the practical and legal responses to data breaches. Mr. Hornak is a frequent speaker and panelist on cybersecurity and privacy issues. He can be reached at mhornak@rutan.com or 714.641.3472.

Marc Boiron

Marc Boiron is a member of the Cybersecurity, Privacy and Corporate Governance Practice Group and focuses his practice on advising boards of directors and companies on cybersecurity matters and emerging and mid-market companies in the areas of California and Delaware corporate laws, securities laws, mergers and acquisitions, restructurings, recapitalizations, leveraged buyouts and strategic alliances. Marc can be reached at mboiron@rutan.com or 714.338.1861.

$1.50 VOL. 39 NO. 25 www.ocbj.com JUNE 20-26, 2016

ORANGE COUNTY BUSINESS JOURNAL

regarding cybersecurity are a useful supplement to in-person training programs.

Passwords and Multi-Factor Authentication

All companies should require that strong passwords be used on all systems and networks on which their data is accessible, though it is preferable for companies to require multi-factor authentication on those systems and networks. If passwords are used, then the company should require that all passwords be of a minimum length; include capitalized letters and special characters or numbers; be changed no less than every 90 days; and be different from any password the employee uses for personal emails, website access, or online shopping.

Multi-factor authentication, which generally requires that a password and a pin number generated on a cell phone or password token be entered to gain access to a system or network, provides greater security than passwords without adding significant costs. Cybercriminals are unlikely to be able to access a system or network with multi-factor authentication unless they have access to all of the pieces required for authentication, which (unlike passwords) protects the system from information obtained by keyloggers.

Notwithstanding the benefits of multi-factor authentication over passwords and their importance in a cybersecurity strategy, cyber data remains vulnerable to, among other things, spoofing, spyware, trojan horses and worms; therefore, multi-factor authentication cannot, alone, protect a company's cyber data.

Encryption

Data encryption is generally considered to be the backbone of any cybersecurity strategy and should be part of the cybersecurity strategy of all small and middle-market companies. Encrypting data is a process that makes data previously readable and usable by people unreadable and unusable by people. Therefore, unless a cybercriminal is able to decrypt encrypted data, obtaining access to the encrypted data is not valuable to the criminal.

In addition to protecting company and customer data, a meaningful benefit of encryption is that encryption of data may eliminate, or substantially reduce, the persons and governmental entities to whom formal notice of a data breach is required under the existing web of conflicting federal and state statutes and regulations.

Different quality encryption software exists. Companies with larger cyber budgets should consider high-end encryption software but, for some small and middle-market companies that do not have sufficient resources to pay for higher-end encryption software, free encryption software is available. Before relying on free encryption software, companies should ensure that the software meets any regulatory and other compliance standards applicable to them.

Insurance

As with commercial general liability insurance, cybersecurity insurance is becoming a virtual necessity. Depending on the policy, cybersecurity insurance may provide broad coverage, including for costs related to: legal defense, obtaining legal advice on notification and regulatory requirements, sending notifications, settlements, judgments, regulatory penalties and fines, public relations, lost profits (but not lost intellectual property), credit monitoring services, and forensic discovery. Companies will need to decide the appropriate type of coverage based on the costs and risks they face.

Notwithstanding the recent decision of the United States Court of Appeals for the Fourth Circuit, which found that the commercial general liability policy at issue required an insurer to defend a company in a class-action lawsuit that arose out of the inadvertent posting of patients' medical records online, small and middle-market companies should not rely on general liability policies to provide protection against cybercrimes. Most modern general liability insurance policies specifically exclude cybersecurity coverage, though some providers permit cybersecurity coverage to be added to its general liability insurance policies.

Small and middle-market companies that consider obtaining cybersecurity insurance should recognize that policies are far from uniform. Given the broad range of available coverage and the relative novelty of cyber insurance policies, the costs of, and coverage and exclusions in, those policies range drastically. The cost of cyber insurance can range from approximately $1,000 annually for $1,000,000 of coverage to $40,000 or more annually for the same amount of coverage.

The uncertainty of cybersecurity liability policies should not deter small and middle-market companies from obtaining cybersecurity coverage because it provides important protection to those companies when firewalls, anti-spyware, passwords, multi-factor authentication, encryption and/or other cybersecurity measures fail.