LOS ANGELES
Daily Journal
www.dailyjournal.com
FRIDAY, JANUARY 16, 2015
PERSPECTIVE

2014: the year of the 'mega breach'

By Eric D. Vandevelde

Government officials and security experts have long warned about the vulnerability of our cyber infrastructure, but last year was a turning point. Target (in December 2013), Neiman Marcus, Michael's, eBay, P.F. Chang's, Home Depot, JPMorgan Chase, and most recently, Sony Pictures, all revealed they were victims of cyberattacks aimed at the core of their business.

What are the lessons to be learned from these attacks? The following are some of the key takeaways.

Cybersecurity Is Not Just IT's Problem

Companies that narrowly consider cybersecurity to be an information-technology problem do so at their own peril. Cybersecurity is also an executive management problem, legal problem, public relations problem, human resources problem, and board room problem. A cybersecurity threat or incident can turn into a much larger crisis.

Every company should have a cross-functional incident response team with appropriate delegated authority to make critical decisions in the event of a major security incident (e.g., shutting down affected servers, cordoning off networks, disabling accounts and resetting passwords, handling media inquiries, working with outside counsel, and potentially notifying law enforcement). While companies should have a CTO, CISO (chief information security officer), or other C-suite executive with primary responsibility for cybersecurity issues, as well as an audit or other board committee with a similar focus, that does not mean other executives or board members can remain on the sidelines.

Cybersecurity must be woven into the company culture, from top to bottom, including through the establishment of computer use and cybersecurity policies, clear escalation procedures, regular employee training, and implementation of data and media access controls.

Hackers Seek More Than Just Credit Card Data

While many hackers seek to exfiltrate credit card numbers and the personal identifying information to exploit such cards, many others, such as "Guardians of the Peace," who attacked Sony, serve as a reminder that companies face threats with varied objectives.

So-called "hacktivists" often seek to embarrass companies by defacing websites, knocking services offline, and publicly posting embarrassing internal data and email communications; foreign (and sometimes domestic) competitors seek to steal trade secrets and other intellectual property; and state-sponsored hackers seek business and military intelligence information.

But even these categories oversimplify the complex, manifold motivations behind many cyberattacks. Even non-retailers must be vigilant because literally every company maintains a wealth of sensitive information that, if stolen or publicly disclosed, could cause significant damage, including trade secrets and other intellectual property, email data, corporate financial data, strategic business planning information, salary and payroll information, and employee personnel files.

For law firms, these concerns are multiplied by the size of their client bases; with each new client comes the attendant responsibility to adequately protect that client's confidential data — there is an ethical obligation to do so. See ABA Model Rule 1.6 cmt. (lawyers must "act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure"); Cal. Standing Committee on Prof. Responsibility and Conduct, Formal Op. Interim No. 08-0002 ("[A]ttorney[s] must take appropriate steps to evaluate: 1) the level of security attendant to the use of a particular technology in the course of representing a client; 2) the legal ramifications to a third party who intercepts, accesses or exceeds authorized use of the electronic information; 3) the degree of sensitivity of the information; 4) the possible impact on the client of an inadvertent disclosure of privileged or confidential information or work product; and 5) whether reasonable precautions may be taken when using the technology to increase the level of security.")

The Eggshell Defense vs. Defense in Depth

Companies today store many types of data across many types of platforms, systems and networks, each of which may present its own unique vulnerabilities. Companies must avoid adopting an "eggshell" defense — hard on the outside, but a gooey mess on the inside — where, once infiltrated, the hacker's most vexing question is often simply what to attack next.

Companies should instead adopt a "defense in-depth" approach, applying multiple, independent layers of security controls throughout the environment, where penetration of one level does not yield access to networks, systems and data protected by other or additional layers of security.

In the past a single defensible perimeter around a centralized server might be sufficient, but that approach provides little protection in a cloud-enabled, bring-your-own-device world where highly mobile employees expect and demand access to the data they need at the time and place of their choosing.

A defense in-depth approach helps prevent a compromised email server from leading to the exfiltration of employee personnel files, a compromised web-server from becoming an open gateway to the company's cloud-based document management system, and the infection of a single employee's laptop with malware from giving hackers root access to the company's critical servers.

Indirect Losses Hurt the Most

Many cyberattacks, even ones targeting financial institutions or payment card information, do not involve the direct theft of money (e.g., by initiating wire transfers or credit card charges). But even non-financially motivated attacks carry enormous financial consequences.

While the short-term costs associated with responding to and remediating a cybersecurity incident can be onerous, the indirect costs, although often difficult to quantify, can be devastating. They include reputational harm, loss of competitive advantage, lost profits, loss of shareholder value, and daunting regulatory and litigation expenses and exposure.

Executives and board members must consider these indirect harms in evaluating cyber risks and deciding when and how to allocate corporate resources toward cybersecurity efforts.

Litigation and Regulatory Scrutiny Is Inevitable

Companies that have suffered a major cybersecurity incident face a barrage of litigation, including consumer class actions (for the actual or expected fraudulent use of consumers' personal information), securities class actions (for the drop in share price), shareholder derivative suits (for management's or the board's alleged failure to provide effective oversight), cost recovery actions by financial institutions (to recoup the costs associated with issuing new credit cards and covering fraud losses), and regulatory enforcement actions, often by the Federal Trade Commission or state attorneys general, who are taking increasingly active roles with respect to data privacy and cybersecurity issues.

These lawsuits are often filed within days a breach disclosure. Sony faces multiple putative class actions by former employees alleging the company failed to adequately safeguard their personal information. Target and Home Depot each face dozens of data privacy-related class actions arising from their disclosed breaches, and their executives have been called to testify before Congress.

Because of the near certainty that regulatory scrutiny and threatened or actual litigation will follow a serious data breach, it is crucial that companies immediately engage outside counsel to coordinate the response effort, allowing counsel and the company to investigate the incident with less fear that their mid-crisis communications, often based on incomplete and evolving facts, can later be used against them.

Cybersecurity experts often say, only half-jokingly, there are only two types of companies in the world: companies that have been hacked, and companies that know they have been hacked. No company can avoid or thwart all attacks. But perfect security is not the goal; the goal is to understand and minimize the risk of an incident and, should one occur, to be prepared to respond to it effectively. Companies must adapt to this new reality, make cybersecurity a priority, and heed the lessons that can be learned from attacks against other companies.

ERIC D. VANDEVELDE
Gibson Dunn & Crutcher

Eric D. Vandevelde, *of counsel at Gibson Dunn & Crutcher LLP, is a former software engineer, and served as deputy chief of the Cyber Crimes Section of the U.S. attorney's office for the Central District of California*