Data breaches in 2017:No relief in sight

BY ROBERT D. CHESLER, MARC D. SCHEIN

THE PONEMON 2016 Cost of Breach Study underscores the need for companies to take all necessary measures to combat the scourge of data breaches.

These include the establishment of a chief information security officer, appropriate data loss prevention controls, encryption where necessary and a robust cyber insurance program. The study found that "Incident response plans and teams in place, extensive use of encryption, employee training, Business Continuity Management involvement or extensive use of Data Loss Prevention reduced the cost of data breach."

The study confirms the resiliency of the hacking plague, and offers no hope that it will cease, or even diminish, in the foreseeable future. In the 11 years that Ponemon has conducted its study, the cost of a data breach has not fluctuated significantly. In 2016, the overall cost of a data breach was about $7 million, and the cost of each single lost record was $221, which are both slight increases from the previous year. The Ponemon Study only included "average" breaches; breaches in excess of 100,000 records were not used in the study. (The average number of breached records in incidents used in the Ponemon Study was 29,611.)

About two-thirds of the cost of a breach represented indirect costs, such as diversion of manpower to deal with the breach and loss of customers. Health care had an average cost per compromised record of $402, while the cost in the hospitality industry was $148. Moreover, unlike in earlier years, data breaches are not limited by a company's size or industry. For example, restaurants and supermarkets have been significant victims of recent breaches.

The threat of data breach and other computer crimes is constantly evolving. "Phishing," by which an outsider passes itself off as a customer or financial institution and causes the transfer of funds to a false account, is rife. Ransomware and cyber extortion, in which the attacker freezes a company's data until it's paid off, have become major threats. No one knows what tomorrow may bring.

IMPACT OF THE INTERNET OF THINGS

This may be the year in which the Internet of Things will create major vulnerabilities in our networks. These connected devices are created to share information that's not necessarily secure, and they're not designed to protect the data they collect. Gartner Research expects there to be more than 20 billion such devices by 2020.

The conclusion of 2016 saw two developments that underscored the growing importance of the Internet of Things. One of the employees at a Vermont utility checked his Yahoo account on his work laptop, which was connected to the utility's network, raising a red flag that suggested the computer was connected to an IP address associated with the hack on the Democratic Party. The good news is thus far there's no sign that the hackers were able to access the nation's power grid. Nonetheless, top political figures as well as businesses fear in 2017 that malware will be used to affect critical infrastructure, such as the power grid, water supply, energy, nuclear reactors and the communication sector.

The U.S. Food and Drug Administration (FDA) issued a formal advisory warning that medical devices such as pacemakers, defibrillators and insulin pumps are easily hackable. Pacemakers first came under scrutiny in August 2016 when a batch ran out of battery three months earlier than they were expected to. "If exploited, the vulnerability could result in permanent impairment, a life-threatening injury, or death," according to the FDA.

CYBER INSURANCE MARKETPLACE: THE WILD WEST

Many companies have turned to their insurance programs to protect themselves against cyber attacks; however, most traditional commercial general liability and property policies don't provide any relief from data breaches. From about 2012 to 2014, litigation raged over whether general liability policies covered data breaches. However, the insurance industry added a broad data breach exclusion by endorsement that eliminates coverage for data breach or network or system failures on policies that contain the exclusion.

As a result, many companies have turned to "cyber insurance." Fitch Ratings estimates that cyber insurance premiums in 2016 totaled in excess of $3 billion and are expected to be around $20 billion in written premium by 2020. The policies are considered to be reasonably priced, and with few exceptions they haven't produced coverage litigation, at least not yet.

More than 60 insurers now offer cyber policies, but no standard policy form exists, and the marketplace is like the Wild West. The policies are highly complex and confusing, with dozens of definitions, exclusions and conditions.

A company must understand its cyber risks and its needs before it approaches the market to transfer those risks. Is it looking for first-dollar coverage or catastrophic coverage? Working with an experienced cyber insurance professional is absolutely essential, and there aren't many of them.

Cyber policies principally provide insurance coverage for data breaches, the first-party and third-party legal responsibilities a company has post-breach, and the associated risks that can include governmental investigations, notification costs, business interruption and class actions.

One feature of cyber policies that has proven to be most useful is event response coverage, which coverage begins when the policyholder discovers the breach. The insurance company provides the policyholder with recommended attorneys — known as data breach coaches — and consultants to address the situation. It also provides coverage for those measures necessary to preserve the company's brand up to the policy limit.

EXCLUSIONS ARE KEY

With the burgeoning growth of ransomware, cyber insurance also can afford cyber extortion coverage and business interruption coverage. This becomes incredibly important when businesses are not able to operate due to their network being locked down (extorted). The business interruption coverage (which does not come standard with all cyber policies) will pay the policyholder for the lost profits that it was not able to collect because its network was compromised. This can be very meaningful for companies who rely heavily on their computer and network.

It's important to review the exclusions in a cyber policy. In view of the growing importance of the Internet of Things, companies should be aware that cyber policies typically preclude insurance coverage for property damage and bodily injury, although it may be possible to negotiate for limited coverage for such risks. However, traditional general liability policies that provide coverage for property damage and bodily injury may apply to such claims. Although general liability policies typically contain a "cyber exclusion," such exclusions usually run to data breach, not physical or bodily injury.

The original focus of data breach was hacking, which remains a pre-eminent threat. However, in 2017, a company must also guard against phishing and cyber extortion, and be cognizant of dangers posed through the Internet of Things. Companies must employ a full panoply of resources to protect themselves, and one of these resources should be cyber insurance.

Robert D. Chesler, a shareholder in Anderson Kill's Newark office, represents policyholders in a broad variety of coverage claims against their insurers and advises companies with respect to their insurance programs. Chesler is also a member of Anderson Kill's Cyber Insurance Recovery group. He can be reached at 973-642-5864.

Marc D. Schein, CIC, CLCS, a risk management consultant for Marsh & McLennan Agency, assists clients by customizing comprehensive commercial insurance programs that minimize or eliminate the burden of financial loss through cost-effective transfer of risk. He can be reached at 516-395-8504.