Dickie McCamey
ATTORNEYS AT LAW

12/23/2014 | Articles

The Inevitable Data Breach: Pray for Peace, Prepare for War

“You cannot create an impenetrable fort,” said Eddie Schwartz, former chief information security officer for the RSA Security Division of EMC Corporation. “No matter what you do there’s going to be some exploit that’s going to work against you, and most of all by the human factor. So you have to get better at detecting those problems and closing that window of vulnerability faster.

“We have to accept we live in a time where every organization is going to get breached, no matter what they do. It’s just inevitable.”

Schwartz should know. RSA bills itself as “the premier provider of security, risk, and compliance solutions, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges.” In 2011, attackers stole digital information related to the company’s SecureID products, which are used by other companies to secure their own networks.

Estimates put the cost of the breach around $100 million. That’s not to mention the immediate and potential long-term reputational damage.

No matter how tightly locked down an organization’s computer systems and networks are, they are still subject to the human factor. In the RSA attack, according to Schwartz, an email from somebody that an end user inside RSA thought they knew was the starting point of the attack. This is known as spear phishing.

The answers to several key questions reveal just how vulnerable your corporation might be without even realizing it.

- Where is your data?
- What types of data do you have?
- How much data do you need to operate your business?
- What is your data retention policy?
- Is archived data vulnerable?
- Is your data encrypted?
- Can mobile data be remotely wiped?
- What happens to old devices which may contain data?
- Is your cloud data being properly secured?
- Has counsel reviewed your vendor agreements?

Companies need to take the proper steps to fully prepare for a breach, knowing that it’s a matter of “when” and not “if” an attack will take place.

Planning for a Breach

As with any potential crisis, having a plan in place to manage a data breach is critical. Yet many organizations mistakenly put planning for something that “might” not happen low on the priority list. Remember, it’s not a matter of whether a data breach will occur, but when. So planning in the form of a breach plan – as well as comprehensive

data breach insurance that covers a broad range of costs, including fines and penalties – is essential.

Soliciting key stakeholder input while developing the plan is important, and training employees to implement the plan – including conducting an outside security audit and/or a penetration attempt – will ensure smoother execution of the plan.

Today's hackers are sophisticated. Many times, rather than attempt a "front door" breach, they will identify circuitous or indirect routes into the target, which is why staged penetration attempts are important. Known as human engineering penetration attempts, these hacks are creative and examples can be simple: a key ring with several keys is left in the employee parking lot. A thumb drive is also attached to the ring. An employee finds the keys, brings them into the building and in an attempt to identify whose keys they might be, puts the thumb drive into a computer. The hackers have now embedded malicious software to create an opening into the system. And just like that, the system is breached. Employees untrained about these kinds of attempts can unknowingly open the door to the system.

The Legal Team's Role

A core response team needs to be in place in advance, with one overall leader and representatives from information technology, legal, and public relations. Among its responsibilities, the team advises company leadership on state and federal legal requirements. Today, the 47 different state notification laws, with federal laws layered on top of those, make management of a breach for large companies like Home Depot and Target complex.

Data Breaches: The Next Asbestos Class Action

The legal team also works with outside regulatory agencies and law enforcement. In this process, the team uses attorney-client privilege to protect sensitive communications. Preparation for litigation and fighting class action certification are also among the legal team's other important responsibilities. In today's cyber security environment, plaintiff's attorneys see data breaches as the next asbestos class action.

Consider the Target breach. Weeks after news of the breach broke, a Pittsburgh heating, ventilation and air conditioning subcontractor emerged as the likely route through which Target's security systems were penetrated. It's been reported that the successful "spear phishing" attempt occurred through the subcontractor's electronic billing, contract submission and project management data connection to Target.

As one of the many likely fallouts from the breach, the North Districts Community Credit Union in Pennsylvania sued Target for the cost of reissuing debit cards and dealing with fraudulent charges. An individual and a bank became the first in Wisconsin to file a class action suit against Target over the breach.

Responding to a Breach

To discover a breach, employees need to know the telltale signs.

- Has the system been accessed at unusual times?
- Were different credentials used to log onto their computer?
- Are there data outflow anomalies?

When a breach is detected or suspected, the response team needs to come together immediately and the plan needs to be executed. At the same time, there is critical information to record: date and time of discovery of the breach; which systems were affected; when was the response plan put into place; when were law enforcement and regulatory agencies notified.

There are things not to do, too. One of the most important is to not shut down the system believed to be breached. Crucial information about the system's vulnerability may be lost. Shutting down may also trigger implanted malicious software and make remediation difficult by hindering the ability of experts to fully understand the scope of the breach. Planning for isolation of affected systems and transition to clean equipment should be part of the plan.

Meeting Legal Obligations

Consulting the legal team about how best to meet legal obligations is a top priority. Counsel can help company leadership determine whether the data that were breached triggers a response obligation. Counsel can also help leadership analyze notification responsibility and create a complete list of individuals who must be notified. The list may include customers, employees, regulatory agencies, the attorney general, and credit reporting agencies.

Other legal obligations include:

- Assigning responsibility for notification
- Making timely and proper disclosure in accordance with requirements
- Documenting notifications as they occur
- Working with data breach resolution vendor to ensure process proceeds smoothly

A Top Goal of Data Breach Mitigation: Avoid Litigation

In preparing for a breach, the response plan must be regularly reviewed. All employees need to be trained on the plan. And your organization needs the added protection of data breach insurance for the day when, despite all the preparations, something does go wrong.

When a breach occurs, a top priority is avoiding litigation. Regular meetings with in-house and outside counsel are critical to discuss the status of breach response and ensure that no new responsibilities have been uncovered.

Counsel should always be present during meetings with law enforcement and regulatory agencies and should also be consulted to discuss ways to tailor a breach response to avoid possibility of class action certification.

Your company can find some measure of peace if it takes the necessary steps to prepare for a data breach, which today is inevitable. Those preparations must involve experienced, effective legal counsel.