Breach Response: How to Prepare for the Inevitable

Assuming an attack has occurred leads to the best defense.

EVEN THOUGH CATASTROPHIC DATA BREACHES ARE MUCH IN THE NEWS, many companies don't expect to suffer a breach themselves so don't bother to prepare a plan. Unfortunately, data breaches are increasingly likely to be the rule rather than the exception for organizations of all types. Having a comprehensive plan at the ready and an expert team identified can determine whether your company responds quickly and effectively to a breach — or suffers the consequences. And those consequences can be severe. While headline-grabbing breaches inflicted losses on organizations worth hundreds of millions of dollars, the mean cost of cybercrime was $12.7 million per company in 2014, a significant figure that has nearly doubled from $6.5 million in 2010, according to the Ponemon Institute.[1]

The current vulnerability landscape

Even more troubling, the cybercrime ecosystem has become highly sophisticated. No longer is the nemesis of businesses the lone hacker in a basement looking for thrills. Instead, an organized, specialized and monetized cybercrime marketplace worth $104 billion annually has emerged. From this marketplace, it's possible to readily obtain online employee profiles from which to create social engineering exploits. Skills spanning a wide spectrum are for sale, and many players, ranging from criminals to hacktivists to nation states, are involved. In contrast, only $46 billion is being spent to stop attacks.[2] Advantage, attackers.

Despite the changing landscape, the most prevalent attacks are aimed at familiar targets. The top exploit in 2014 according to HP Security Research (HPSR) was a Microsoft Windows exploit. That's not to say new threats are not appearing, however. Mobile malware emerged in 2014 as a consistent and serious threat, rather than a novelty. Other new

targets emerged as well, such as point-of-sale (PoS) systems and physical devices that make up the Internet of Things (IoT), according to the Hewlett-Packard *Cyber Risk Report 2015*.[3] Long story short, both new and old technology is vulnerable.

Whatever the vulnerability, the longer it takes to detect, contain and resolve, the higher the cost. According to Ponemon, the mean number of days required to resolve cyber attacks is 45, with an average cost of $35,647 per day. That adds up to $1.6 million over the 45-day remediation period.[4]

Breach response: The right mindset

Faced with these facts, there is no excuse for pretending that while others may be breached, your company is safe. In contrast, operating as if a breach has already occurred often leads to the positive results of early detection and effective damage control. This can lead to significant savings, because companies spend the most money relating to breaches on recovery and detection. With this in mind, it should not come as a surprise that organizations deploying security intelligence systems reap the biggest ROI, realizing a 30% better incremental return than any other investment. Organizations following this approach saved $5.3 million more than their peers.[5]

Time to Resolution

Some attacks take longer to resolve and are more costly than others, according to Ponemon Institute.
(average days to resolve in 2014) SOURCE: Ponemon, p. 14

65.5 days
Malicious insider attacks

49.8 days
Malicious code attacks

45.1 days
Web-based attacks (hackers)

Governance activities are also important in breach response. Indeed, certain governance activities — such as team building — can reduce the cost of cybercrime. There is evidence that organizations see the wisdom of this approach. Among enterprise security governance activities, the formation of a senior-level security council and the appointment of a high-level security officer tied for first place in prevalence, with 53% taking part in both.[6]

Breach response: The team

Like a SWAT team or a first-rate fire department, your breach response team should have specialists in several areas. Each member should understand his or her role and how it fits with the roles of others. Every company is different, so the makeup of the breach response team will differ from company to company. However, a team generally should include these members:

- CIO or equivalent
- CSO or equivalent
- IT specialists in networking, database, applications and mobile technology, preferably with forensics expertise
- Legal department representative
- Compliance expert
- Customer service specialist
- Investor relations specialist
- Public relations specialist

Team members should regularly take part in breach response drills. Financial services and military organizations may want to run drills without prior notification. And since the first 24 hours following the discovery of a breach are the most critical, the drills should focus on this time period, utilizing a checklist for the accomplishment of key milestones.

In addition to his or her primary responsibility, each team member should be designated as backup to another team member. Some organizations may find the use of an outside consultant or "breach coach" to be helpful in assigning roles and leading drills.

Worth noting is the importance — and scarcity — of skilled IT staff. When a breach occurs, the security expertise of IT staff will be of the utmost importance. However, it's generally recognized that skilled security professionals are in short supply. That may be because only 32% of organizations view IT security as a career path and 40% of IT security jobs were unfilled in 2014.

A savvy organization will seek to fill its IT security positions with the most skilled candidates available.[7]

Breach response in action

When a breach occurs, it's important for the company as a whole to understand that much is at stake — up to and including corporate survival. It is imperative, therefore, that the breach response team be fully empowered with the authority to take charge of anything within the company that might relate to the breach.

The first objective must be to find the attacker. In this stage, Security Information and Event Management (SIEM) software is often essential. Logs must be reviewed for behavior that indicates an attack has occurred. Malicious IP addresses must be identified and blocked, and firewall rules updated accordingly. Security patches must be applied as necessary. The patching process may call for the cooperation of the entire company, since production systems may need to be taken offline in order for the patches to be applied. After these procedures are complete, it is necessary to retest to make sure the vulnerability was taken care of — and that a variant of the exploit is not present. Very often an attack occurs before a patch has been created. In such "zero day" attacks, it is of the utmost importance to block the attack until a patch is available.

Web and Mobile Apps Suffer from Misused Security Features

Web and mobile applications had issues involving authentication, access control and confidentiality.

SOURCE: HP *Cyber Risk Report 2015*, p. 67

86%
Web apps

97%
Mobile apps

Mobile Targets

In 2014, Android was by far the most attractive mobile OS target, followed distantly by iOS and Windows CE. That's a major change from 10 years earlier, when Symbian was the No. 1 OS target, followed by Windows CE.

2014's most attractive mobile OS target

#1 iOS

#2 

#3 Windows CE

Communication is critical

Once the breach has been discovered and mitigated, it is necessary for management to communicate effectively with employees, customers, investors and the public at large. Each of these constituencies must be given straightforward and credible answers to these questions: What happened? What does it mean to me? Despite the breach, can I trust and believe in the company?

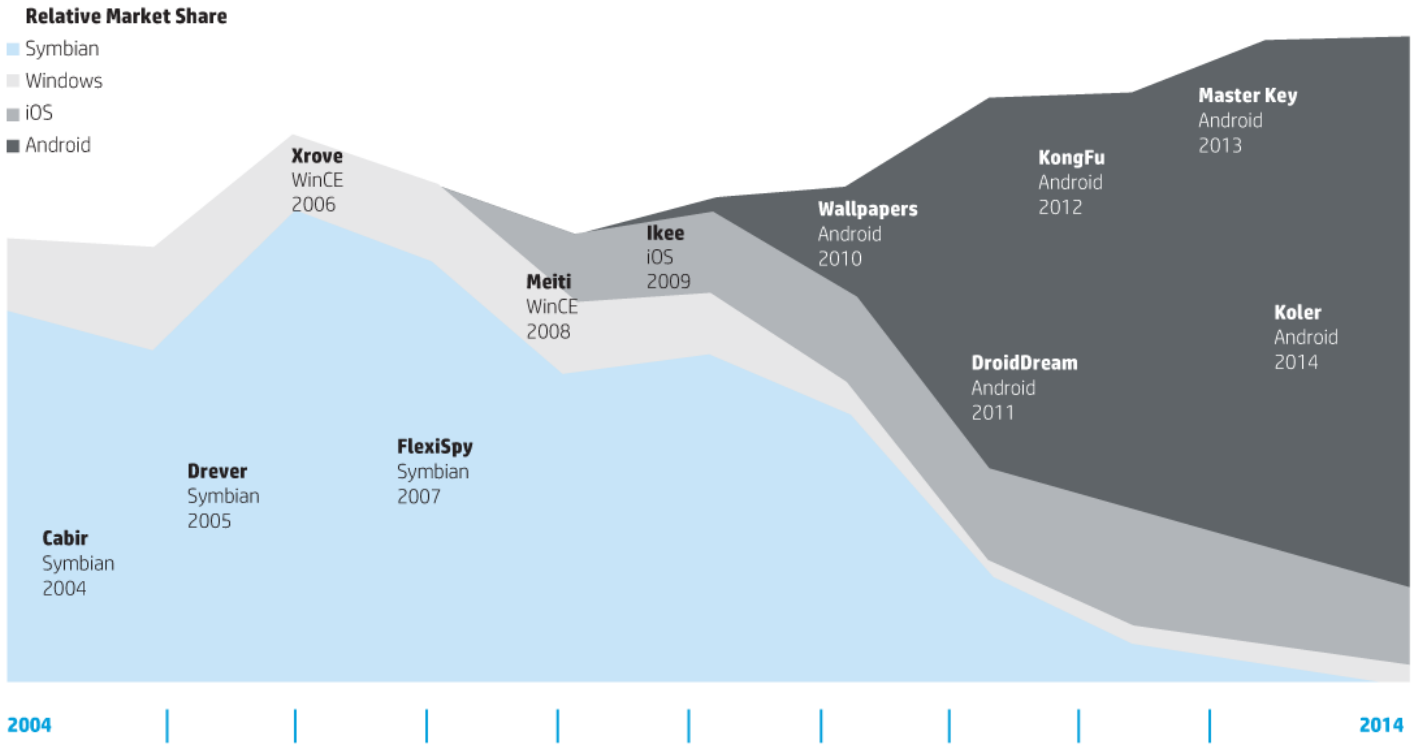
For example, employees need to understand with clarity the seriousness of the situation, how they can help if necessary, and that their company has the situation under control.

Retail customers need to understand their credit card and other personal information is safe and that it is safe to continue shopping. If data has been compromised, they need to know exactly what steps are being taken to protect their data and to compensate for any losses.

One watchword of good crisis communications is never to underplay the seriousness of the situation or to give assurances that can't be backed up. Stating the "facts" of a situation only to change them later adds the perception of incompetence or dissimulation to the very damaging reality of the breach. Because most people understand that anyone or any business can be the target of an attack, there may be a reservoir of sympathy already present from which a company may benefit by a forthright and completely truthful public disclosure.

10 Years of Mobile Malware

10 years of mobile malware; as market share changes, so do malware targets. SOURCE: HP *Cyber Risk Report 2015*



[1] *2014 Cost of Cyber Crime Study: United States,* Ponemon Institute, p. 5.

[2] *Breaking the Cyber Attack Lifecycle,* Hewlett-Packard Co., p. 8.

[3] *Cyber Risk Report 2015,* HP Security Research, p. 4.

[4] Ponemon, p. 13.

[5] *Breaking the Cyber Attack Lifecycle,* Hewlett-Packard Co., p. 16.

[6] Ponemon, p. 22.

[7] *Breaking the Cyber Attack Lifecycle,* p. 17.

Notification: Legal requirements

Data breach notification laws have proliferated across the country, with nearly all states now having laws on the books. The legal department team member must be thoroughly versed in the laws of the states in which the company does business. Although the provisions vary from state to state, if data is encrypted or redacted, disclosure generally is not required. When disclosure is required, requirements differ significantly. As reported in CSO Online, Baker & Hostetler LLP, a national law firm with a focus on privacy law, notes that deadlines for notification range from five days in Connecticut to 45 days in Ohio, Vermont and Wisconsin.

Be ready with the right team

If experience in combating data breaches has taught anything, it is that it is unwise to assume a breach will not occur. Likewise, it is unwise to rely on just one technology to secure data. Instead, a balanced approach that relies on people, process and technology has a far greater chance of success. Above everything, organizations must be ready and waiting with a breach response plan that covers all scenarios and a team with clearly defined and well-rehearsed roles for each member. Having the right plan in place, and being able to execute effective breach response with a skilled team, will enable your company to minimize financial losses and recover quickly if — or when — a breach occurs.

For more information, see
www.hp.com/go/esp