OVERVIEW

As high-profile data breaches continue to increase in their frequency and severity, planning for incident response is becoming a boardroom discussion. It’s encouraging to know that board members and c-level executives are becoming more aware of cybersecurity risks. According to a recent report, 68 percent of risk management professionals said cyber risks were a significant concern for directors, and 75 percent said they were for executives — with both categories showing an increase from 2014.

If organizations don’t take cyber security risks and incident response seriously, the consequences are often dire. When Target experienced their massive breach, in which up to 40 million customer payment cards, the company’s IT security team received an alert that pinpointed a probable intrusion in their network but failed to investigate. Cyber attackers stole card data for over two weeks. Everyone learned about the breach from Brian Krebs’s blog, who discovered large numbers of stolen payment cards for sale on the Dark Web. Target failed in letting the banks know which cards were compromised, thereby letting scammers continue to make fraudulent transactions. At the same time, customers found it impossible to reach Target due to jammed lines, further exacerbating an already poor incident response.

Despite the growing awareness of cyber security risks, fewer than a quarter of companies have taken adequate measures to protect data. According to a global survey of over 1,700 security professionals, 88% of respondents reported that the security capabilities in place at their organizations did not adequately meet their data security needs. Underscoring the problems with cyber threats, one report found that 1 million new threats were being released on a daily basis while another report found that 83% of large enterprises were being targeted by cyber attackers.

But planning is still lacking, notwithstanding the growing number of security threats. According to a recent joint Cloud Security Alliance (CSA) and Skyhigh Networks report, 82.2% of companies have some form of an incidence response plan, but less than half have a comprehensive incidence response plan that includes security remediation, legal, public relations, and customer support.

Now imagine you’ve just been informed of a data breach. The details are scant and you have little insight into the total number of records breached. The breach could be a minor incident,
or it could pose an existential threat to the company, to your job security, or both. Your team is scrambling to respond to the attack. If you know the source of the breach, you might be busy securing vulnerable infrastructure, but it’s just as likely that the source of the breach isn’t known and much of the focus in the initial hours or days is spent figuring out what went wrong. Attempting to formulate a breach response plan in the midst of the chaos surrounding a breach can be disastrous. This checklist contains vital information to help organizations prepare an effective incident response plan ahead of time.

INCIDENT RESPONSE STEPS

The best incident response requires your organization to already understand how much sensitive data is being stored, where the data is stored, the types of data (personal data, health data, intellectual property, or customer data), how it’s being secured in transit and at rest, who has access, and who is actively accessing information. The response plan should include a crisis communications plan, pre-determined list of PR firms, law firms, and forensics vendors that specialize in data breach response, and a well trained and prepared crisis response team comprised of key individuals from human resources, customer support, legal, IT security, and engineering departments.
1. DETECT BREACH

Detecting a data breach can often be the hardest part of the incident. Hackers go to great lengths to hide their footprint so they have ample time to access the most important of data or inflict the greatest amount of damage.

According to one report\(^6\), the average targeted malware compromise was present for 205 days before detection, the longest presence was 2,982 days, and 69 percent were discovered by external parties, not internal IT security functions.

The difficulty in detecting a breach is due to the vast amount of false alerts being triggered on a daily basis. In almost every publicized case of a breach or intrusion, alerts and alarms did go off in the various monitoring systems, but security analysts largely ignored the alerts due to the overwhelming number of false positives.

Many organizations have started to use user and entity behavior analytics (UEBA) to detect breaches and anomalous activities. UEBA helps companies detect potential threats by building baseline behavioral models for normal activity and continuously look for patterns of behavior that deviate, even in non-obvious ways, from the norm.

2. INSPECT AND PROTECT

Once a breach has been detected, organizations should assemble their incident forensics team to begin the long and arduous task of finding the root cause and source of the breach and implement the correct security measures to stop the damage and secure their infrastructure. Larger organizations should have a short list of third-party forensics vendors to help them accelerate this process.

Generally, the sooner a company can accurately assess the scope of the breach and the types of data stolen, the better the outcome will be for their customers and stakeholders.

3. GATHER AND MOBILIZE THE CRISIS COMMUNICATION TEAM

The crisis communication team should include members of the human resources, legal, public relations, and customer support and should be headed by someone who will act as an intermediary between executives and the rest of the team members. The CISO and the CIO should act as advisors to the team.

For example, you may designate a team lead that will be responsible for managing key tasks and the timelines. They may also be in charge of identifying the needed budget for the response, and document every step that is taken during the incident response process.

The communication team is responsible for all levels of communication, both internal and external. They determine the channels and methods of communication, any legal requirements around how the breach should be communicated, who should be notified and in which order, as well as how much information should be divulged.

The legal members of the team will help shape the incident response in such a way to help ensure minimal legal risks.

The PR members of the team generally outline the best methods of communicating the breach.

\(^6\) M-Trend 2015: A View from the Front Lines, Mandiant
ensure information isn’t leaked to the media without the company’s knowledge, and identify negative press coverage and respond promptly.

The HR and customer support team members generally formulate the appropriate approach towards responding to customer inquiries. They will need to understand how to alter their role from their usual day-to-day activities, and start the process of setting up a dedicated phone line for incident response.

4. CONTACT LAW ENFORCEMENT

In the case of a large breach of sensitive data, local authorities as well as the FBI should be notified. The incident response and forensics team should understand their legal obligations throughout the process so that they’re in compliance with legal requirements and directives. Everything should be documented. If systems are terminated, backups should be retained.

5. CONTACT THIRD-PARTY VENDORS

Depending on the severity of the breach and the type of data stolen, organizations should have contractual agreements in place with reputable identity protection service providers, credit monitoring vendors, and vendors specializing in data breach response.

The organization should look to outsource much of the notification process, including identity/address verifications, writing notification letters/emails, printing, and promptly mailing them to the affected parties.

6. NOTIFY STAKEHOLDERS

It’s not uncommon for organizations to fumble their notification process. Many high-profile data breaches are followed by poor notification processes that range from long delays in notifying customers to using inadequate communication channels to announce the breach.

Employ the help of legal counsel to determine who should be notified and how much information needs to be divulged. In some cases, such as when stolen data was encrypted, notification may not be necessary.

Any delay in notifications could severely worsen the effects of the incident for the company. Opportunistic attackers will be quick to send out phishing emails to customers, as it happened in the case of the Target breach, if official notifications are delayed.

Notifications should be communicated via:

- Email and physical mail
- Website and blog
- Social media
- Press release
- A dedicated website for the breach
- Customer portals

7. EXPAND CUSTOMER SUPPORT

Organizations should have contractual agreements in place with staffing agencies that can be brought in to support the expected increase in customer inquiries. In the midst of a data breach, the last thing customers should have to deal with are long wait times and unresponsive customer care specialists. The
benefits of being responsive can’t be overstated because the PR fallout that can result from poor customer care may prove to be as damaging as the breach itself.

Though nothing can fully prepare an organization to deal with a data breach, frequently auditing and reviewing your response plan can avoid some of the common mistakes made when responding to an incident. Team members should go through regular training, and organizations should hold systematic incident response drills and practice runs. The incident response team spearheads post-breach activities; however, every employee has a responsibility to follow data security and privacy best practices. Data security should be an organization-wide tenet and thus must be communicated as such to employees of all levels.

**FIRST 48 HOURS – YOUR INCIDENT RESPONSE CHECKLIST**

When organizations adopt an “assume breach” philosophy and take steps to prepare for an incident, they’re less likely to panic and make damaging mistakes when a breach occurs. Keep the following items in mind as you go through the first 48 hours after discovering a data breach.

- Document in detail the date/time and how the data breach was discovered, who discovered it, and when the incident response procedure began.
- Immediately notify all members of the crisis communication and forensics team, third-party vendors as well as executives.
- Preserve all physical evidence surrounding the location of the breach. Certain regulations, such as HIPAA-HITECH have requirements around the physical security of systems.
- Protect unaffected systems from further data loss by disconnecting them from affected systems while bringing affected systems offline.
- Perform a thorough forensic investigation of all unaffected systems to ensure they are not breached.
<table>
<thead>
<tr>
<th></th>
<th>Protect yourself from further liability; document everything, including the circumstances under which the breach was discovered, types of data lost, affected parties, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Employ an independent third-party vendor to interview internal employees who discovered and initially responded to the data breach.</td>
</tr>
<tr>
<td></td>
<td>Dispatch the forensics teams (both internal and external) to begin investigating the breach and document their findings. Fix the issue that caused the breach.</td>
</tr>
<tr>
<td></td>
<td>Begin the notification process after consulting with the legal team to determine the notification process and priorities.</td>
</tr>
<tr>
<td></td>
<td>Contact law enforcement agencies and begin temporarily expanding the customer support team and setup the incident response hotline.</td>
</tr>
</tbody>
</table>