PREPARING FOR A DATA BREACH: NOT IF, BUT WHEN

BY PETAR BESALEV, SENIOR VICE PRESIDENT OF CYBERSECURITY AND PRIVACY SERVICES AT A-LIGN

When preparing for breaches, companies should think in terms of "WHEN a breach happens, we will do this" instead of "We will do this IF a breach happens." As data breaches are being discovered and reported more frequently, it is critical for organizations to recognize that establishing and implementing a security breach response plan is an integral part of their cybersecurity preparedness.

DEFINING A DATA BREACH

News stories regarding security or data breaches appear almost daily. Networks have been accessed, confidential data has been leaked and customers have had their information stolen. Security threats come in many forms, but there is some confusion around what actually constitutes a data breach and what they mean for business owners.

A data breach can be defined as an incident in which security defenses are bypassed and information is accessed without authorization. Data breaches can range from minor incidents (the hacking of one individual) to massive, such as the 2017 Equifax incident when hackers stole personal information from more than 143 million Americans.

Data breaches are occurring more often, especially to businesses and organizations. A 2019 report from Hiscox found that 53 percent of companies experienced a cyberattack in 2018, a 15 percent increase from the year before.

Though these attacks are being detected more frequently, many businesses still are not prepared. In a 2018 cybersecurity resilience study from IBM, almost 80 percent of business leaders admitted to not having a formal incident response plan in place for their organization

RESPONDING TO A DATA BREACH

So, what happens if you or one of your vendors suffers from a data breach?

The affected company must first determine what kind of breach has occurred — common types include cases of employee negligence, unauthorized access, phishing, ransomware and physical theft of devices. The organization then must assess the impact of the breach to the organization. When assessing the impact of the breach, three aspects to should be considered: defining the technical impact, defining the business impact and defining the privacy impact.

While not an exhaustive list, the following questions can help guide the organization in assessing the potential impact of the breach:

Technical impact:

- What system(s) have been affected?
- What is the identified point of entry?
- What deficiencies and/or vulnerabilities exist within the current monitoring and detection activities?

Business impact:

- Has this caused an impact on business operations?
- Is the business still able to continue operations?
- Is third-party assistance needed?
- Has there been a breach to "sensitive" or "confidential" data?

Privacy impact:

- What regulations and/or state-specific items is the entity concerned about?
- How many users were affected?
- Where are the majority of the data subjects located?
- Was the data encrypted?
- Is this data likely to cause a high-risk to the rights and freedoms of data subjects?

After the impact of the breach has been defined, the company must notify relevant parties. This step should be completed as soon as possible, as most states and many countries have legislation in place requiring the notification of security breaches involving sensitive information. Unfortunately, completing this task can quickly get complicated.

Notification requirements not only include impacted customers and businesses, but also reporting requirements to federal authorities. The requirements for notifying affected parties vary based on the state or territory where those individuals reside, so it is important to have the requirements of each state on hand in order to minimize response time.

International organizations must also take note of requirements and laws pertaining to security breaches impacting citizens of multiple countries.

This process can sound lengthy and intimidating. However, by being prepared for a breach before it occurs, companies can streamline their response and minimize the impact on normal operations.

PREPARING FOR A DATA BREACH

As with anything else, preparation and practice are keys to minimizing the impact of a security breach. It may not be possible to predict exactly what a breach will look like or when a breach may occur, but there are several steps companies should take to ensure they can respond to the unexpected.

ESTABLISH A BREACH TEAM

All members of an organization should have a basic level of knowledge on what to do and who to contact in the event of a breach. However, designating a specific group of individuals who are trained to lead the organization's response to a breach will simplify the process. The members of the breach team may vary, based on what is logical for the organization, but should typically include forensics experts, incident handlers, executives with crisis management experience, legal counsel and media relations experts.

AWARENESS TRAINING

While the breach team will be the internal experts on security breach response plans, awareness training sessions for all employees is still crucial. After all, an organization's security is only as good as the least knowledgeable person with access to internal networks and databases. Training sessions should educate all employees on the policies and procedures in place to prepare for cyber threats and explain their roles in responding to a security incident. Every organization should also continuously update employees on new scams or potential risks as they arise and provide tips on how to avoid falling victim to them.

PENETRATION TRAINING

Penetration testing is a simulated cyberattack against an organization's computer system to test the security of its current technologies and systems. The goal of penetration testing is to identify such vulnerabilities before a malicious source can take advantage. These tests should be run on everything that could potentially be compromised, including servers, firewalls, routers, switches, web applications and wireless technologies. Penetration tests should be conducted on a semi-annual or quarterly basis in order to ensure outdated practices are not being relied upon.

VULNERABILITY SCANS AND ASSESSMENTS

Vulnerability scans and assessments provide detailed reports with explanations about any possible holes in a security system. They also can provide recommendations on how organizations can address the vulnerabilities identified. These scans and assessments should be conducted monthly on all information systems within an organization.

Internal SOC team or third-party monitoring
Ideally, an organization should have an internal security operations center (SOC) team monitoring systems and technologies continuously. An internal SOC team ensures timely detection of and response to security incidents and breaches. If that is not possible, an organization may consider working with a third-party security monitoring service (MSSP) to monitor systems within an organization.

"IF, NOT WHEN"

When preparing for breaches, companies should think in terms of "WHEN a breach happens, we will do this" instead of "We will do this IF a breach happens." As data breaches are being discovered and reported more frequently, it is critical for organizations to recognize that establishing and implementing a security breach response plan is an integral part of their cybersecurity preparedness.

EXTERNAL BREACH CHECKLIST

Breaches at other organizations can still impact your data – if you've been affected by an external breach, here's what to do.

DEFINE THE TECHNICAL IMPACT TO YOUR ORGANIZATION

- [ ] What system(s) have been affected?
- [ ] What is the identified point of entry?
- [ ] What deficiencies and/or vulnerabilities exist within the current monitoring and detection activities?

DEFINE THE IMPACT TO YOUR ORGANIZATION

- [ ] Has this caused an impact on the organization's operations?
- [ ] Is the organization still able to continue operations securely?
- [ ] Is third-party assistance needed? 4. Has there been a breach to "sensitive" or "confidential" information?

DEFINE THE PRIVACY IMPACT TO YOUR ORGANIZATION

- [ ] What regulations and/or state-specific items are we concerned about?
- [ ] How many users were affected?
- [ ] Where are the majority of the data subjects located?
- [ ] Was the data encrypted?
- [ ] Is this data likely to cause a high-risk to the rights and freedoms of data subjects?

NOTIFY RELEVANT PARTIES*

- [ ] Identify impacted customers and organizations
- [ ] Determine if federal authorities must be contacted
- [ ] Keep state requirements on hand, as compliance laws vary
- [ ] Keep international requirements on hand, as breaches may impact citizens of multiple countries

* Complete this step as soon as possible to ensure compliance.

PETAR BESALEV is the Senior Vice President of Cybersecurity and Privacy Services at A-LIGN. He oversees all security service offerings including PCI DSS, Penetration Testing, ISO 27001, HIPAA/HITECH, FISMA, and FedRAMP. Petar has provided IT security, audit, consulting and compliance services for Fortune 500 companies in multiple industries. Prior to joining A-LIGN, Petar was an IT Risk and Assurance Senior Manager with Ernst and Young (EY).

TALK TO AN EXERT

SCHEDULE A TIME FOR YOUR PERSONAL, NO-COST CONSULTATION.

SCHEDULE NOW

Reprinted with permission, FICPA. Florida CPA Today: Summer 2019 – Florida CPA Today | Volume 35, Number 3 (Pages 26-28)