Systems Engineering
Get Ahead of IT

A Systems Engineering White Paper

Preparing for a Data Breach

Get Ahead of IT

Ph: 888.624.6737 · syseng.com · info@syseng.com · An Employee Owned Company

We must use disruptive events, like the Equifax data breach, to reflect on our own security posture and capabilities. While there are things Equifax could-have and should-have done better to protect its data (keeping up-to-date on patching), the company's handling of the breach has been met with widespread frustration and criticism. Being prepared to handle a data breach is critical to successfully responding to an incident without making a bad situation worse.

With the majority of cybercriminals focused on the US, it is becoming increasingly important for organizations to plan and prepare for a breach. While many organizations are implementing technologies to defend against cybercrime, most aren't actually prepared for a breach itself.

A data breach is the intentional or unintentional release of an individual's personally identifiable information (PII) or other valuable information, such as intellectual property (IP) to an untrusted environment. PII and IP information are lucrative and the criminals will do whatever it takes to obtain it.

When cybercriminals are successful and a data breach occurs, it can be a chaotic and confusing time for many organizations, particularly those who fall short of putting the right security measures in place. Many organizations will expect their IT team to handle all aspects of a breach response. However, there is more to responding to a breach than just containment.

While avoiding a breach is always the goal, the risks due to lost and stolen devices or malware attacks are real. The following are steps you can take to mitigate the potential impact:

- **Assemble your team**. Build a team who have defined responsibilities and delegate authority to them. A common response to a data breach is the onset of panic causing the organization to micromanage the data breach response team and their responsibilities. Organizations need to remember that these members were selected because of their competency at a time when panic and confusion did not rule the moment. Let them do what they were trained to do.
- **Get some help**. Whether in-house or outsourced, get legal counsel involved early to understand your legal and compliance requirements. Also, review your business, E&O and cyber insurance coverage to ensure you are covered for a breach. In addition, look to your public relations team to help with communication and, if necessary, involve a computer forensic firm as some breaches are too big and complicated to handle on your own.
- **Provide clear communication**. Decide who you are communicating to, what you are telling them, when the right time to make an announcement is, and how it should be communicated. Sometimes the containment plan (disconnecting servers, shutting down internet access or phone systems, taking down websites, etc...) can disrupt normal communication paths. Your data breach response strategy should consider a backup plan to communicate with employees, customers or anyone who needs to be involved. Choose the person who will collect and disseminate information, and have them be the single point of contact for all communications.

- **Don't wait for perfect information.** While you may want to have all the facts, it is rare that this will happen during a data breach event. Typically, a breach may contain bits of information, but not enough to paint a full picture. Decisions may need to be made based on the imperfect information you have in front of you. Sometimes waiting too long could make the situation worse. It's an imperfect process.
- **Plan!** If you have a plan, blow the dust off and update it, or start one. It doesn't have to be perfect the first time out, but make sure to have one in place. Also, practice it! Get a third party to help you role play to see how effective it is and where the holes might be. If the situation does arise, your organization will be in a much better position to endure it.

Responsibility for a security breach goes beyond IT. While IT deals with the breach itself, members throughout the organization, whether in-house or outsourced, need to be actively involved and take a role in the other responsibilities that materialize as a result. In addition, contact your finance and insurance companies as well as any vendors and/or business partners who may be instrumental in dealing with a breach. Finally, contact local authorities and, if applicable, regulatory boards to notify them of the crime.

Building a Comprehensive Security Foundation

Criminals use various tactics and methods to penetrate your organization such as spear phishing, exploiting system vulnerabilities or even social engineering over the phone (also known as vishing). Organizations need to put a comprehensive security foundation in place to protect against the numerous techniques cybercriminals use. At Systems Engineering, we use the National Institute of Standards and Technology (NIST) Cybersecurity Framework[1] as a reference for improving critical security infrastructure. The steps included in this approach are as follows:

Identify

- Develop an organizational understanding to identify the data, systems, personnel and facilities in your business and their relative importance to reach your business objectives.
  - In particular, locate your PII or IP information and assure access is limited to those with a business reason to do so. Also, document the various places your PII and IP exists, including backup.

Protect

- Develop and implement the appropriate safeguards to protect data and systems from unauthorized access and to assure your employees understand their role in minimizing the risk of a breach.
  - A layered approach to network security is your best defense to limit hackers from penetrating your network.

Detect

– Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event when it happens.
  - Too often an attack and the data breach itself are completed long before the business knows something has happened. It is critical to have security experts actively reviewing and analyzing system activity and security events 24x7.

Respond

– Have a plan in place which guides you through the steps of activating your response team, communicating with authorities and stakeholders, analyzing the extent of the breach, containing the risk and mitigating the impact.
  - It is essential to plan your response to a breach in advance; you should role play and practice the plan to identify and fill any gaps that come up. If needed, hire a facilitator to help keep your practice on track.

Recover

– Develop and implement the appropriate activities to address any reputational fallout that may result from a breach and to cover the extraordinary costs of such an event.
  - Do you have a marketing or public relations firm included in your response plan? Do you have proper cyber insurance in place to cover both first and third-party losses?

In summary, data breaches are wide-spreadspread and show no sign of letting up. Those organizations who put together a comprehensive breach response plan and practice it are better positioned to face any incident.

To combat breaches and reduce the number of incidents, build a comprehensive technology security foundation to include security experts watching the flow of traffic in and out of your network 24x7. In addition, it is crucial to implement security awareness training. Having a workforce educated on threats such as social engineering, spear phishing and ransomware attacks can reduce your breach risk.

References

[1] NIST Framework for Improving Critical Infrastructure Cybersecurity

About Systems Engineering

Systems Engineering is a leading IT strategy and managed services provider serving over 500 legal, healthcare, financial services, and government clients nationwide. Established in 1988, Systems Engineering is an employee owned company committed to delivering engineering excellence and superior customer service. Our team of 100+ network engineers, security professionals, data management experts, field service technicians and account managers are available 24×7, 365 days per year to meet the needs of our clients. From network design, installation and training to a full complement of managed security, data management, business consultation and help desk support services, Systems Engineering helps clients Get Ahead of IT. For more information, please visit syseng.com or call 888.624.6737.