(EN) Data Breach: 5 Tips for Organizing Your Crisis Unit

For most organizations, the question of a data breach is not if, but when. This article provides 5 recommendations that organizations should address prior to, and during, a suspected breach.

SaaS & Tech Data Breach Cybersecurity Tips Crisis Unit
May 21, 2024 5 min

For most organizations, the question of a data breach is not if, but when. Regulators and insurance companies are compressing reporting requirements turnarounds. Thus, it is critical that organizations proactively plan for how they will respond to a data breach. **This article provides 5 recommendations that organizations should address prior to, and during, a suspected breach**. Implementing these five will not prevent a breach. However, they will save you significant time and resources as you respond to and address the specific areas of vulnerability.

Membres cités dans l'article

Marie-Noelle Brisson
Co-Founder @ CyberReady LLC
Côte Ouest des USA - Sud

Tip 1: Pre-Breach – The crisis response team should reflect a Holistic Risk Management approach.

If you don't have a response team in place now, put it together ASAP. **Responses should address the physical, behavioral, and technical aspects of the breach and the subsequent response by the company**. Adjust the team as necessary to ensure all appropriate areas are represented and the response is as fast and streamlined as possible. The team should focus on Holistic Risk Management – treating cyber risk the same way you do other corporate risks (operations, financial, market). Use tabletop exercises and have the team respond to simulated breaches.
If a data breach has occurred, it will usually be reported by IT (if network related), HR (if people/behavioral related) or Facilities (if a physical breach).

> *Do you have someone from each of these organizations on your response team? If not, consider adding them so the breach is reported to the team as quickly as possible.*

Finally, update your Business Continuity Plan and Disaster Recovery Plan as appropriate to reflect the work of the response team.

Tip 2: Don't Unplug Anything and Document Carefully What You are Doing

> *It is critical that management and the Board not panic. Respond to data, not emotion. Identify the breach and the vulnerabilities that were exploited, and isolate as needed. Make sure you respond quickly, but accurately, to what has happened.*

Log out of every application including emails, but do not unplug. Unplugging will prevent a thorough documentation of what happened and the implementation of your curative measures.
As you work to contain the breach, make sure you document every step you take. You will need this information as part of your notification plan, as well as to show actionable response should you need to respond to regulators, insurance carrier's questions and legal claims. **GDPR since 2018 and NIS2 by October 2024 impose a 72-hour reporting requirement. Insurance companies in France require a similar reporting timeline. Listed companies in the US also have a 3-day reporting deadline required by the SEC**.

Mobilize your Breach Response Team. The exact steps to take depend on the nature of the breach and the structure of your business. Your team should have been identified and trained on how to respond to various cyber threats.
For a physical breach, you should identify the location and method of breach (i.e. physical theft of data or equipment).
For a behavioral breach, you should identify the method (for example a phishing scheme, email, text, phone), and the individual(s) affected (what name/department/location is the email, text or phone call coming from).
For a technical breach, you should identify the system, software, and servers where the vulnerability was exploited. These systems should be isolated to prevent further contamination.

Tip 3: Secure Physical Operations and Facilities

Immediately upon identification of a breach, check whether unauthorized individuals have gained access to secured physical spaces or compromised IoT (Internet of Things) devices and equipment. Quickly check access control systems including visitor access points, video surveillance, all IoT (Internet of Things) devices and equipment around the office or the home for telecommuters to verify they have not been compromised.

In addition, think about 3rd parties. Are they secure? Check network segmentation to ensure a breach in one area/server can't move to another area/server

This physical security breach can range from unauthorized entry into a corporate office to theft of physical documents or devices containing sensitive information or vandalism The smarter and more connected, the building, the greater the risk that a cyberattack to building systems can result in the shutdown of a facility, threatening property damage and even occupant safety.
Unauthorized entry could come from lost or stolen badges, hackers impersonating repair personnel, or simply tailgating on someone's fob or key card. Physical theft of devices or equipment, or malicious tampering may have occurred with the building infrastructure. Check if power outages may have compromised physical security measures and created vulnerabilities for attackers.

Tip 4: Prepare A List of Affected Parties and Notification Templates

Your response team should have developed a list of key stakeholders who need to be notified in the event of a breach. Notification templates (letters, emails, press releases, etc.) that have been reviewed by Legal should be ready to go. Once the type and extent of the breach is known, these templates should be adjusted (if necessary), completed, reviewed by Legal and then sent to the appropriate stakeholders.

> *Speed is important here, but accuracy is key. It is imperative that affected stakeholders are notified quickly with accurate data and steps they need to take to protect their data. This also will save precious time when it comes to reporting the breach.*

The tabletop exercises noted in Tip 1 are key to the identification of potential affected groups and proper notification of each. An example list of affected parties would include Law enforcement, Employees, Suppliers, Other affected businesses, Clients, SEC (if listed), and Insurer.

Tip 5: Check Your Data Map and Define What is Essential to Recover or Protect

If you have been proactive, you should have a data map, the foundation of data governance. Such a map should track business data engineered in-house or externally collected, employee data, and customer data collected. Sort data in order of value and critical importance and identify what data warrants what level of protection. The response team should have also mapped the data flows and included breach response in both the disaster recovery plan and the business continuity plan. Adjust your data map if necessary.
Having a data map will allow you to zero in quickly on prioritizing which data to protect and recover. When a breach strikes, speed of identification and recovery is of the essence. A data map is an effective tool for this activity.
Hackers post successful breaches on the dark web. Others will try to exploit your systems again using a previously-successful hack.

> *It is amazing the number of companies who are hacked the same way more than once. Lessons learned about a breach are critical to eliminating vulnerabilities and providing increased security against future breaches.*

Conclusion

A complete breach response system doesn't just focus on the current breach. You may have been breached in other places that have not been identified and/or the breach may have hidden itself in other systems. For recovery, always test back-ups before reinstalling. If the breach was software-related, it is possible the software has been dormant on the system long enough to have been included in the backup. If that is the case, restoring from the infected backup will simply recreate the breach.
To improve protection going forward, it is critical to do lessons-learned reviews. Lesson-learned exercises should be part of the response team's tabletop exercises. Basic lessons learned include an assessment of what happened (physical, behavioral or technical breach), why it happened (lax diligence, operational error, brute-force attack) and what steps have been taken and will be taken to make sure this breach doesn't happen again.

With expertise in real estate finance as a valuer, rating analyst, loan servicer, investor, issuer, and lender in the US and in France, and governance experience as a non-executive director, Marie-Noëlle Brisson, Frenchfounders' club member since 2022, co-founded CyberReady, LLC., a company providing holistic management services of cyber risks. She is a designated fellow of the RICS, and a certified director by IFA (Institut Français des Administrateurs). She focuses on data governance and training for C-Suites and Boards.
Dr. Michael Savoie, Ph.D. is a Clinical Professor in Operations and Supply Chain Management at the University of North Texas, CEO and Chairman of the Board of HyperGrowth Solutions, Inc., and Co-Founder of CyberReady, LLC. He has over 30 years of experience working in Cyber Security for U.S. federal agencies and commercial organizations and has developed commercial assessments based on proprietary algorithms that help organizations create holistic, business-oriented, strategies for dealing with cyber risk.

Glossary

FIPS - Federal Information Processing Standards

FISMA - Federal Information Security Modernization Act (FISMA)

GDPR - General Data Protection Regulation (GDPR)

ISO - International Organization for Standardization

NIST – National Institute of Standards and Technology

A REVOIR : Efficacité, mode d'emploi I Paroles d'expert
"Il existe une grande confusion entre agitation et efficacité. Croire que l'urgence ou la vitesse d'exécution sont les bons critères signifie l'acceptation du modèle du hamster dans sa roue. Une autre approche du temps est possible."

Rédigé par
Marie-Noëlle Brisson; Dr. Michael Savoie

Partager l'article