Cyberattack: best practices for organizations after a data breach

Being ready to manage a data breach is an extension of staying competitive and is a necessary reality of being in business today. Cyberattacks are on the rise in parallel with the increasingly digital nature of global commerce. According to a 2018 study from Juniper Research[1], cybercriminals are expected to steal an estimated 33 billion records in 2023—a significant increase from the 12 billion records forecasted to be stolen in 2018[2]. This is a rising trend that needs to be addressed at every level of the organization, from service staff up through senior leadership. So how can businesses start thinking about what to do before an incident occurs?

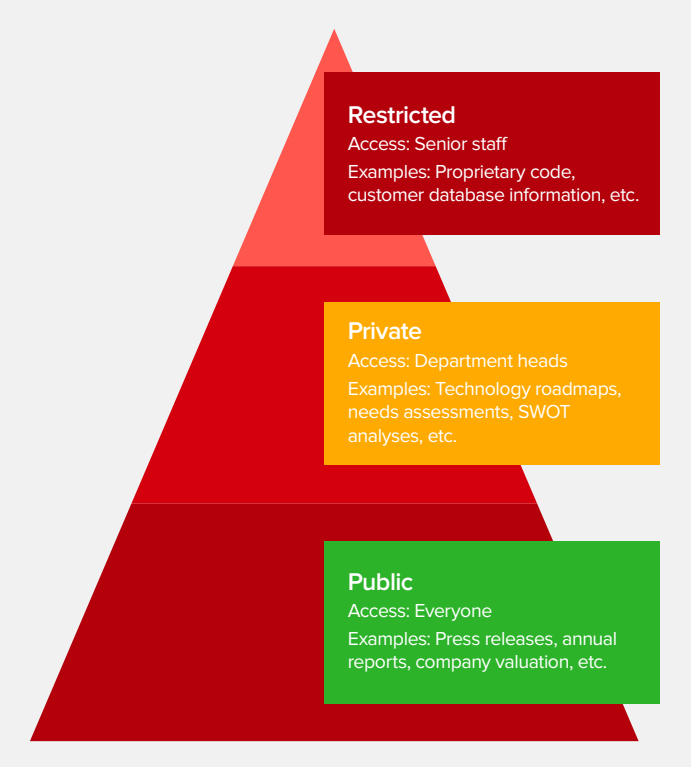
This white paper offers a practical approach to preparing for a data breach. It will identify the parties that should have agency in the preparation process, outline how communications should be structured and managed, and touch upon how business data should be layered into a cybersecurity plan.

Know what you're protecting: data classification

When preparing for a data breach, it's vital to know how company data is structured, where it can be accessed, and who has access. In addition to creating safeguards around data as a preventative measure, data classification is an important process in meeting legal requirements after a breach has occurred. Proper data classification can save an organization from liability around fines and other penalties associated with the theft of business and consumer data[3].

Organizing company data into a coherent and organized model is an important measure to take to make sure that when an incident occurs, teams can identify what's happening in order to address it as quickly as possible. It's also an effective way to clearly identify and protect the company's most valuable business data.

A data classification hierarchy that is well-defined, allocated, and regularly re-assessed will help organizational leaders to understand what they're protecting. Here's a sample of an effective data classification structure:



Key vulnerabilities that lead to data breaches

Data breaches can come from any angle, and can threaten the integrity of any system that's not properly equipped. Some of the most common areas of vulnerability for company and consumer data include:

1. **The point of sale**—Newer systems protect company and consumer data more effectively because of P2P encryption and other protocols, but many older systems don't. Outdated POS solutions can pose a serious liability when those kinds of vulnerabilities are exploited by criminals.
2. **Unpatched security solutions**—When security safeguards are not updated on a regular basis, resistance to viruses and other invading programs (which are updated regularly) becomes less effective.
3. **IoT devices**—As the internet of things (IoT) expands what an organization can do for its customers and for data analytics, the increased number of potentially exploitable access points into a system makes safeguarding business data more difficult.
4. **Staff**—Without proper security training, employees at all levels can represent a vulnerability. By falling prey to phishing scams, opening malicious attachments, losing company hardware, or unintentionally communicating with criminals, any staff member can accidentally facilitate cybercrime.

Once a company knows where its valuable data lies, it can deal with attacks in a more focused and effective manner. From here, it becomes easier to create a plan for dealing with potential incidents.

Developing an incident response plan

In the light of the growing threat of cyberattacks across a range of industries, businesses need to plan for the worst while hoping for the best. Protecting the integrity of customer and company data is not easy, and requires executive team buy-in, proactive leadership, regular pen testing, a "security-first" corporate culture, and other preventative measures. Still, it's vital to acknowledge the increasing likelihood of data breaches by creating an effective response plan in the event of an attack.

Creating a response plan for the possibility of a data breach isn't just an exercise in damage control and PR. It's a strategy for saving money. The *2018 Ponemon Global Cost of Data Breach Study*[4] suggests that an incident response team can save an organization $14 per record on average, with the average cost per record as the result of a breach being $148—just over 9%. This adds up significantly depending on the nature of the breach.

Incident response plan characteristics

The goals of an incident response action team are threefold:

1. Isolate and reduce the damage of the breach
2. Document all actions taken during the response process in detail
3. Manage clear and effective communications with all stakeholders and affected parties

Incident response plans should be designed for as much clarity as possible. This makes a plan more efficient and less ambiguous when dealing with a data breach.

With the three points above in mind, here are some of the most common and useful elements to include in an incident response plan:

- A list of likely scenarios and associated action items for each
- An up-to-date personnel list with a strict division of labor
- A clear methodology for collecting and presenting legal evidence of actions taken after a breach
- A detailed communication plan specific to relevant parties—customers, the media, et al.

Forming a data breach incident action team

Before an attack, it's important for the whole team in an organization to know who its key allies are when addressing both the immediate and long-term effects of a breach. This goes beyond just the affected areas of the company technology platform. Forming an action team will help to unify and consolidate company expertise when planning proactive measures in the aftermath of a data breach.

Some of the personnel involved will include IT leadership, their teams, as well as in-house and third-party security personnel. But an action team will also include company legal counsel, communications and marketing departments, operations staff, and third-party service providers like financial institutions and insurance companies.

Key tasks during and after a breach

IT teams will typically be in damage containment and repair mode during a breach. But other parties on the action team will be busy, too. Here are some of the key tasks that members of the team will need to address after a cyberattack:

- **Create documentation**—Company legal counsel should follow up on an incident with accurate documentation that adheres to regional and national laws around security incidents.

- **Stabilize operations**—The COO and team will be responsible for implementing pre-determined strategies that enable the company to continue business operations during what may potentially be an extended period before a system is fully restored and secured again.
- **Keep lines of communication open**—Investor relations firms as well as the marketing and communications department will play a vital role in addressing incoming questions from company stakeholders, customers, and the press.
- **Minimize damage and take preventive measures**—Security experts both in-house and third-party will help to ensure that loopholes in the system are closed after an attack, and that the system is free of "backdoors" for attackers to re-enter.

Communications guidelines after a breach

Clear and succinct communications during and immediately after a security breach are vital. These will extend to both internal and external parties, very often including the media. Developing effective messages to speak to specific audiences will require collaboration with marketing and communications teams, investor relations firms, and company legal counsel.

What comes out of that collaboration should then be included in the company incident response plan, and follow some basic best practices aligned with the following approaches and actions:

- Be honest, clear, and concise about the facts
- Take ownership of the problem with all parties
- Underscore company commitment to data security and system integrity
- List specific actions taken or that will be taken to resolve the crisis, complete with timelines

Effective communications are the means to take control of the narrative after a breach. Planning and crafting that messaging is crucial to minimizing any damage. All of the above should guide the creation of company-wide emails, communications with external stakeholders, and all published content including blog posts, dedicated landing pages, and press releases.

Vendor risk management (VRM)

Managing relationships between staff and the technology partners will play a significant role when dealing with the aftermath of a data breach. This should begin at the planning stages, as technology partners should value security just as much as the organization in question does.

Vendor risk management (VRM) is the process of ensuring that partnerships with service providers and IT suppliers do not create potential for security issues and subsequent business disruption. High-profile and brand-damaging data breaches can be more effectively avoided if vendors that access an organization's network are required to sign contracts or other agreements that mandate their compliance with organizational security policies.

To manage this effectively, organizations should include the following in all vendor agreements:

- Organizations must require vendors to meet and possibly exceed their own security standing
- Vendor security protocols must be documented, reviewed, and updated on a regular basis
- Vendors must provide evidence of security compliance on an annual basis
- Organizations must reserve the right to audit and update security requirements based on the ever-changing security landscape

Data security should be a cooperative effort between the organization and its partners. In addition to being good practice in general, formal agreements are extremely valuable during and after a security incident to minimize damage and even liability.

Creating a more secure business

When it comes to building a comprehensive approach to data security, the first order of business is to create a set of principles and action items that will guide the way toward a safer technology infrastructure. By fostering an environment that prioritizes security, you can minimize and prevent the cyberattacks that stand to harm your business the most.

Managing a data breach: key takeaways

- Hope for the best, plan for the worst
- Organize company data via an accessible and coherent data classification structure to identify the company's most important data
- Recognize internal and external allies when it comes to a data breach and form an action team that includes them before an incident
- Create a detailed incident response plan, including a communications strategy for every stakeholder
- Document every action during an incident, with detailed timelines
- Form relationships and create formal agreements with vendors who share company values around data security

Finding the right technology partner to help ensure better cybersecurity

To better create a healthy working relationship with a technology partner, it's important to begin with the selection process. Here are some traits to look for in a potential technology partner.

- The partner always ensures that the latest security features are applied to all applications, and are scaled to evolve as trends shift
- The partner manages automatic and regular updates to security measures
- The partner carefully monitors end-of-life hardware applications
- The vendor can demonstrate that their products are compliant when it comes to secure data management and processing

Creating awareness and practical actions to prepare for a data breach requires vigilance, specialized expertise, and teamwork at all levels, including with technology partners. To learn more, talk to us at Infor® about how we approach security requirements to serve a wide range of industries.

References
[1] "Cybercrime & the Internet of Threats 2018," Juniper Research, 2018.
[2] "10 cyber security facts and statistics for 2018," Norton, 2018.
[3] "2018 Ponemon Institute Cost of a Data Breach Study," Ponemon Institute, July 2018.
[4] Joshua Aguiar, "Data Classification and Protecting Information," September 27, 2018.

Learn more ›

Follow us :

infor Gold Channel Partner

GODLAN

641 Avenue of the Americas, New York, NY 10011

INFDTP2303848-en-US-0420-1

Godlan, Inc.
15399 Canal Road
Clinton Township, MI 48038
586-464-4400
info@godlan.com
www.Godlan.com