Data Breach Response Guide

This document is ATTORNEY ADVERTISING MATERIAL and does not constitute legal advice.
Introduction

Data breaches are no longer a phenomenon experienced by large retailers and multinational financial institutions. Data breaches are becoming commonplace in today's world. Regardless of the type or size of your business - no one is immune. Experiencing a breach may be inevitable, but the reputational and financial harm often associated with them doesn't have to be. Organizations can greatly reduce the cost of a data breach by having a well thought out incident response plan, a strong IT security platform and a team of professionals pre-selected to respond should the need occur. This Response Guide will outline the recommended steps your organization should take before a data breach occurs and what should be done if one does occur.

This Response Guide will aid you in the development of an incident response plan and what to do during the first 24 hours of a breach.

Please take a moment to review this guide, and if you don't have an incident response plan, use this to help create one. It could mean the difference between a breach that causes a brief disruption and one that jeopardizes the very existence of the business. Please consult with one of our attorneys if you have any questions or concerns.

Life Cycle of a Data Breach

1. Discover the Breach
   The most costly breaches are malicious or criminal attacks, such as hacking. Negligent employees also significantly contribute to data breaches.

2. Engage Legal Counsel
   The laws surrounding data breaches are complex. Without proper guidance, early missteps in communication and procedure will be costly.

3. Investigate & RemEDIATE
   Early detection means you can limit the amount of data compromised.

4. Assemble Internal Response Team
   Having key team members like a Chief Information Security Officer (CISO) and investing in talent in your IT department can reduce the cost of a data breach by 35%.

5. Contact Law Enforcement (If Applicable)
   Data breach laws vary state by state so be sure to retain legal counsel before making any outward statements to law enforcement.

6. Employ Outside Vendors
   Consider vendors such as forensics, data breach resolution, law, and PR firms.

7. Prepare for Public Announcement
   Begin Notification Process. If necessary, purchase Identity Theft Protection Services and credit monitoring for affected persons. While the cost of the announcement, brand reputation and more will add up, delaying the announcement will only make it worse.

8. Mail/Email Notifications
   Consumers want to see facts about the breach, information about the risks they may face, steps they can take to protect themselves and an offer for credit monitoring or identity protection included in a breach notice. Keep in mind that the number of records affected necessary to report a data breach varies by state.

9. Respond to Inquiries
   There will be plenty of questions from the media, your customers and law enforcement agents. This is when having the right legal counsel and PR firm is important.

10. Handle Litigation & Fines
    Customers affected by the breach will want to hold somebody responsible — that somebody unfortunately is usually the victimized business.

11. Resume Business as Usual
    While the time for recovery varies by the type of business and the nature of the breach, if your company stays in front of each part of the data breach life cycle, business can return to normal.
Data Breach Planning and Preparedness

Why do you need a data breach preparedness plan?

Businesses of all shapes and sizes from every industry are becoming more aware to the threat of a data breach. As a result, many are taking steps to proactively assemble a data breach response team, combining internal stakeholders and external resources, so that they can be prepared in the event that they experience a breach.

Implementation of an effective personal information security breach response plan enables organizations to fulfill their responsibilities to those individuals and entities that entrust the organization with personal information. Following a security breach response plan should enable organizations to comply promptly with legal requirements that apply to the organization as an owner and custodian of personal information, and to reduce the risk of a data security breach that causes serious harm to the organization’s reputation and finances, especially because of an inadequate response.

A key requirement for the breach preparedness plan is having an understanding of how data is collected, retained and destroyed. Organizations must be able to quickly determine the nature and scope of an incident, take immediate steps to contain it, ensure that forensics evidence is not accidentally ruined and subsequently notify regulators, law enforcement officials and the impacted users of the loss. The scope of an organization’s plan should include impact assessment regarding the loss of intellectual property, brand reputation, regulatory compliance, and business continuity.

Once developed, the breach preparedness plan should be distributed and communicated to all relevant employees, data partners and vendors to help ensure an effective 24/7 incident response capability.

A data breach can take a toll on a company of any size. Having a breach preparedness plan in place can help you act quickly if one occurs. Acting quickly can help to prevent further data loss, significant fines and costly customer backlash.

Bring Your Response Team Together

A breach response team should consist of a cross-section of company personnel, including legal, privacy/compliance, IT, information security and other relevant stakeholders from the company’s various business units. External members should include outside legal counsel, computer forensic specialists, and a crisis management firm.

Engage the Decision-Makers

Having a management-level executive with broad decision-making authority on the incident response team is ideal; this individual’s broad authority can help the breach response process move more quickly. Your incident lead should be able to:

• Manage and coordinate your company’s overall response efforts and team.
• Outline the budget and resources needed to handle a breach.
• Summarize the steps needed to assess the scope of a breach.
• Analyze response efforts post-breach to better prepare the company and team for the next incident.
Data Breach Planning and Preparedness (cont.)

Here is a quick look at the other members you will want on your team and what their responsibilities might entail:

Information Technology & Security
The IT and security team members play a central role in helping to identify what information was compromised, because they are most familiar with the network systems and the security controls in place. In most cases, however, rather than conducting the forensic investigation, the internal IT and security staff may primarily assist the outside forensic team with their investigation. Even though the IT and security staff possess an intimate knowledge of their organization’s network systems and security controls, many lack the specialized skill set and training to perform digital forensic investigation. You’ll want someone from IT and/or security on your response team to:
• Train personnel in data breach response, secure the affected premises, including safely taking infected machines offline and preserving evidence.
• Work closely with a forensics firm to identify the compromised data and remove the hacker’s presence without compromising evidence.

Legal, Compliance & Privacy
Your outside legal counsel with expertise in this area should be your incident response leader. Identifying the notification, legal and regulatory requirements of the breach response is also a responsibility of the legal team. This includes determining if there is an obligation, contractually or under applicable laws and regulations, to notify external organizations, clients or business partners and, if so, what the content of the notification must be. Rely on internal and/or external legal, privacy and compliance experts to shape your data breach response and help minimize the risk of litigation and fines. Your legal representatives will need to:
• Have the expertise and knowledge to “quarterback” the organization’s data breach response.
• Evaluate whether affected parties need to be notified, including, but not limited to, individuals, government agencies, and law enforcement.

Communications/PR
Your PR and communications team will be an integral part of your response efforts. If your breach is substantial enough, you may need to notify the media, which will require a certain fact that is best handled by your communication department. These people will need to:
• Determine best practices and tactics for crisis management prior to the breach itself.
• Handle any information leaks regarding a breach, monitor media outlets, quickly respond to any negative press during a breach, and manage social media.

Customers/Clients & HR
Data breaches may affect both your customers and your employees, so appoint representatives from both customer service and HR to your response team to provide needed support. After a data breach, customers have lots of questions, especially if they suspect that they are victims of fraud. Your organization’s customer service staff has a crucial role to play in the breach remediation process: rebuilding customer trust. Your representatives should:
• Create simulation training for your customer service representatives that demonstrates how their roles would change during a data breach.
• Outline a plan for setting up a data breach hotline for customers and/or employees if a breach occurs. Determine in advance if you’ll use internal or external resources.

Law Enforcement
Depending on the type and severity of a data breach, you may need to involve law enforcement.
• Consult with your legal counsel before involving law enforcement.
• Identify which state and federal authorities, including the FBI and Secret Service, to contact in the event of a data breach involving criminal activity.
• Inform every member involved in the response and handling efforts of law enforcement directives.

Trainings & Simulations
Having a data breach response plan in place is critical. However, employees who are not made aware of their responsibilities when handling sensitive information or answering questions about steps to protect customer information can be the company’s weakest link.
• Make data security a daily routine for all employees, and regularly train your staff on proper protocols.
• Implement and update company-wide technology guidelines that consider all forms of devices.
• Invest in a solid IT and security infrastructure, and bring in experts to help you do so.
• Monitor and limit the data available to employees and vendors.

This document is ATTORNEY ADVERTISING MATERIAL and does not constitute legal advice.
Responding to a Data Breach

The first 24 hours after you discover a data breach are critical to restoring security, minimizing harm, obtaining and preserving evidence and complying with contractual and legal obligations. This Day One Checklist provides executives and in-house counsel of organizations with prioritized key steps to take in response to a cyber incident/data breach and key warnings as to what not to do.

Day One Checklist

Panicking can result in ill-advised decisions that can be extremely costly. Delaying your response to a data breach can be equally devastating. Accept that it’s happened and immediately contact your legal counsel for guidance on initiating these critical steps:

- Notify the incident response team and ensure team members know their respective responsibilities.
- Establish a timeline of events, including creating a tangible record of the day/time of the breach’s discovery and of the moment the response began. Continually update it to document every aspect of the breach, including the chain of discovery, the type of materials, the systems affected, etc.
- Move the impacted machines offline, but do not turn the machines off or explore the system until after the forensics unit arrives, do not run antivirus programs/utilities, and do not reconnect affected systems.
- Notify forensic experts (via legal counsel) to advise your organization how to stop data loss, secure evidence and prevent further harm. They are also trained to preserve evidence (including that which may exist only in temporary memory) and manage the chain of custody, minimizing the chance that evidence will be altered, destroyed, lost or rendered inadmissible in court.
- Preserve all affected system log files including firewall, VPN, mail, network, client, web, server and intrusion detection system logs. These logs are critical for assessing the origins of the attack, its duration and the volume of data exfiltrated during the breach.
- Increasingly cyberattacks are aimed at gathering log-in credential and password combinations. After a cyber/data breach, personnel should be required to change passwords and be issued new physical authentication/access devices (tokens, badges, key cards).
- Assess the situation using the information you’ve uncovered and the help of your various data security teams.
- With guidance from legal counsel, determine whether law enforcement needs to be notified, and whether there are also obligations to notify service providers, payment card networks or other contractual parties. Additionally, review insurance policies (ideally with the assistance of your broker and an experienced insurance lawyer) to determine whether insurers should be notified to preserve coverage rights.
Responding to a Data Breach (cont.)

Once you have begun or completed the eight initial steps, stop briefly, take a breath, and assess your progress. Ensure your preparedness plan is on track and continue with these next steps:

Move Ongoing Forensics Work Forward

- Rely on your forensics team to detect and delete hacker tools.
- Determine if you have other security gaps or risks and address them.
- Put clean machines online in place of affected ones.
- Analyze backup, preserved or reconstructed data sources.
- Ascertained the number of suspected people affected and type of information compromised.
- Begin to align compromised data with customer names and addresses for notification.

Identify and Act on Legal Obligations

- Work with legal counsel to identify state and federal regulations governing your industry and the type of data lost.
- Determine all persons and entities that need to be notified, i.e. customers, employees, the media, government agencies, regulation boards, etc.
- Ensure all notifications occur within any mandated timeframes.

Plan and Manage the Team

Data security is not an individual effort. It requires the help of a variety of teams and individuals. Make sure that you are prepared for a breach well before it ever occurs, so that the steps outlined above can be paired and compared with a response plan that gives you the best opportunity to handle the breach effectively.

Notification Process

You don’t have an unlimited amount of time. Generally, your business has about 60 days to let affected individuals know that a breach has occurred, assuming notification is required by law. Certain state laws and federal regulations shrink the timeline to 30 or 45 days, meaning there’s no time to waste in verifying addresses; writing, printing and mailing notification letters; and setting up a call center and other services for affected individuals.

Changing Regulations

More and more U.S. states and countries around the world require organizations to disclose instances of data loss or theft when they occur. Regulations specify which data is relevant, what volume of records constitutes a breach, what must be disclosed, within what timeframe, and to whom. The goal of these requirements is not to punish companies, but rather to protect consumers, enabling them to take swift action to limit their risk. While regulations initially focused on credit card records and other financial data, in many cases their scope has expanded to cover healthcare records and other personal data.

- Law enforcement is a top priority in many breaches, and they may delay notification if it interferes with an investigation.
- The timing, content and scope of the notification depends on where the affected individuals reside, not where the business is located. Multiple state laws may apply to one data breach.
- Different states have different requirements, and these variances can often be extreme. Consult with legal counsel to determine which laws are applicable to you, and which notification standards are required. Failing to meet these requirements could lead to disastrous consequences for your business.

Jon Breyer is head of Lindquist & Vennum’s Privacy and Data Security practice group and counsels clients on data security and privacy laws, including representing businesses and individuals who have fallen victim to data security breaches and those targeted by litigation and government investigations stemming from highly publicized data security cases.

This document is ATTORNEY ADVERTISING MATERIAL and does not constitute legal advice.