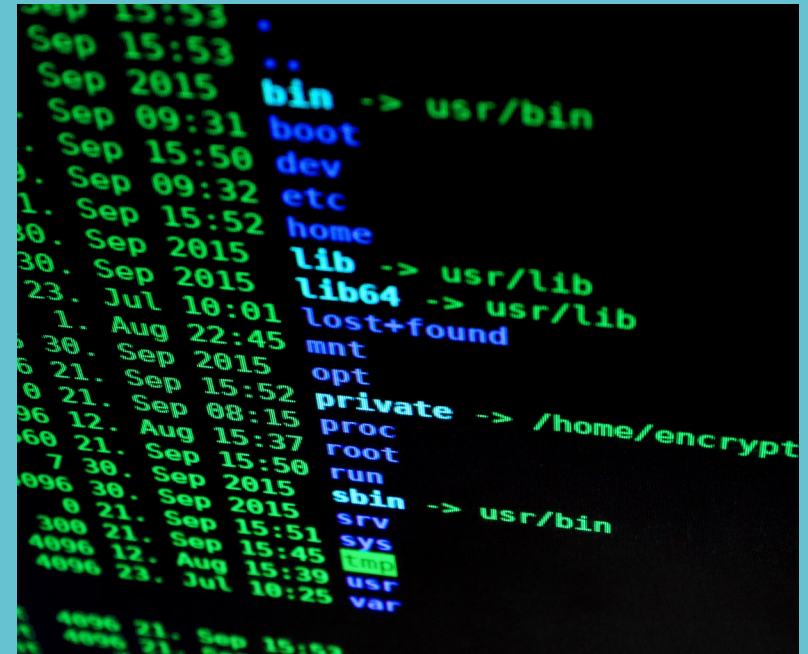


Data Breach Response

A Checklist for Preparing Your Business

Table of Contents

Secure Your Operations	3
Contain the Breach	3
Assess Your Losses	4
Identify What Data Was Stolen	4
Mobilize Your Incident Response Team.....	5
Fix Vulnerabilities	6
Update and Harden Your Infrastructure.....	6
Check Your Network Segmentation	6
Think About Service Providers	6
Notify Appropriate Parties	7
Determine Your Legal Requirements	7
Notify Law Enforcement	7
Notify Managers and Internal Employees	7
Notify Affected Businesses	7
Notify Individuals	8
Conduct a Security Post-Mortem	9
Appendix A: Additional Resources	11



Data breaches are common. And how you respond to one can go a long way in maintaining your business reputation and keeping you from losing the trust of your customers and partners.

As with any crisis, a quick and decisive response is critical. But, most breaches go undetected for a long time – over 200 days according to the latest statistics. The longer a breach goes undetected, the more harm it can do to your business.

This eBook was intended to help businesses like yours to guide you in the steps to take once you suspect a breach has occurred and to remain calm while you take actions to contain it. Although the answers vary from case to case, this guidance can help you make smart, sound decisions.

Secure Your Operations

The only thing worse than a data breach is multiple data breaches. Take steps so it doesn't happen again. Move quickly to secure your systems and fix vulnerabilities that may have caused the breach.

Contain the Breach

While you may be tempted to delete everything after a data breach occurs, preserving evidence is critical to assessing how the breach happened and who was responsible. The first step you should take after a data breach is to determine which servers have been compromised and contain them as quickly as possible to ensure that other servers or devices won't also be infected. Take all affected equipment offline immediately — but don't turn any machines off until the forensic experts arrive.

Here are a few immediate things you can do to attempt to contain the breach:

- Disconnect your internet
- Disable remote access
- Reconfigure firewall access control rules
- Install any pending security updates or patches
- Change passwords
- Add two-factor or multi-factor authentication (2FA/MFA) on any account that allows it
- Secure physical areas potentially related to the breach.

You should take care to change all affected or vulnerable passwords immediately. If an attacker stole credentials, your system will remain vulnerable until you change those credentials. Create new, strong passwords for each account, and refrain from reusing the same passwords on multiple accounts. That way, if a data breach happens again in the future, the damage may be limited.



Do not destroy evidence.

Don't destroy any forensic evidence in the course of your investigation and remediation.



Assess the Your Losses

What kind of data was breached in your business? Was it financial information of your customers or employees? Or did attackers steal other information that could still give them the ability to steal more. These are important questions to ask after a data breach.

Identify What Data was Stolen

Determine what information was stolen. This helps you identify what types of identity theft you are at risk of and how you can mitigate the damage that hackers can do. For example, a cybercriminal can do much more damage with a Social Security number than an unused user account name. The most common data targets that attackers go after include:



Email — Thieves can use your email to send spam and attempt to log into other accounts that share the same email. For example, thieves may log into your bank using your Facebook email.



Encrypted Passwords — Most sites encrypt passwords. But attackers use software to crack weak ones within minutes or hours. Once they have access to your passwords, they'll try them on as many accounts as possible.



Full Name — Hackers use your name to find other publicly available information about you in your online footprint. With enough information, they can commit identity theft.



Phone Number — Cybercriminals can use your phone number for spam calls, identity theft, and SIM-jacking. This is where a thief claims your number for their own and receives all your texts and incoming calls.



Home Address — An exposed address can put you at risk of change-of-address scams, tax fraud, and other forms of identity theft.



Credit Card Numbers — Thieves can use stolen credit card details to pay for goods online or buy gift cards that can't be traced (a scam called "carding"). This is even if they don't have your physical card.



Social Security Number (SSN) — Your Social Security number is perhaps the most vulnerable piece of information a thief can steal. With your SSN, they can commit identity theft, tax fraud, unemployment scams, loan fraud, and much more.



Credentials & Keys — Attacks leverage stolen API keys and credentials to access different technology services used by the organization such as Cloud providers (AWS, GCP, Azure) and payment processors (Stripe, Braintree, etc.)

Mobilize Your Breach / Incident Response Team

Once you know what sensitive information is vulnerable, it's time to protect yourself. Prevent additional data loss by mobilizing your breach/incident response team. The exact steps depend on the nature of the breach and the structure of your business.

Assembling your team in advance of an incident allows all those involved to thoughtfully and thoroughly vet through team members to find the best qualified candidates for your needs. Once the team is assembled, preparing and practicing your response plan will ensure each member understands their role and can work together as an effective team.

Vet and have a data forensics team to have on retainer. Thorough preparation for a breach incident can lead to faster reaction and lower costs should a breach occur. Plus, you'll have peace of mind knowing you're covered.



Assemble a team of experts to conduct a comprehensive breach response

Depending on the size and nature of your organization, they may include forensics, legal, information security, information technology, operations, communications, investor relations, and management.

Identify a data forensics team

Consider hiring independent forensic investigators to help you determine the source and scope of the breach. They will capture forensic images of affected systems, collect and analyze evidence, and outline remediation steps.

Consult with legal counsel

Talk to your internal legal counsel. Additionally, you may consider hiring outside legal counsel with privacy and data security expertise. They can advise you on federal and state laws that may be implicated by a breach.

If you have cyber insurance, notify your carrier

Your insurance policy documents detail how to report a claim. There are a range of policies that may cover aspects of cyber-related claims. Your cyber carrier will be able to provide

Fix Vulnerabilities

After the cause of a breach has been identified and remediated, you need to ensure all systems have been hardened, replaced, and tested before you consider re-introducing previously compromised systems back into your production environment.

During this process, ask yourself these questions:

- Have you properly implemented all of the recommended changes?
- Have all systems been patched, hardened, and tested?
- What tools/remediations will ensure you're secure from a similar attack?
- How will you prevent this from happening again?

Once your company has addressed what happened in your data breach, it's time to make sure any cybersecurity patches or procedures you put in place really work. It is important to do a test and make sure the method used by the attacker to gain access to your data can't happen the same way all over again.



Update and Harden Your Infrastructure

- Make sure operating systems are up to date
- Apply security and software patches
- Use only the latest versions of your antivirus software
- Ensure your systems are protected by conducting regular vulnerability assessments and penetration tests. This will help identify any vulnerabilities before attackers do, thereby enabling you to identify and remediate any issues

Check Your Network Segmentation

When you set up your network, you likely segmented it so that a breach on one server or site could not lead to a breach on another server or site. Work with your forensics experts to analyze whether your segmentation plan was effective in containing the breach. If you need to make any changes, do so now.

Think About Service Providers

If service providers or other third parties were involved, examine what personal information they can access and decide if you need to change their access privileges. Also, ensure they are taking the necessary steps to make sure another breach does not occur. If your service providers say they have remedied vulnerabilities, verify that they really fixed things.



Notify Appropriate Parties

When your business experiences a data breach, notify law enforcement as well as other affected businesses and individuals.

Create a plan that reaches all affected audiences — employees, customers, investors, business partners, and other stakeholders. Don't make misleading statements about the breach. And don't withhold key details that might help consumers protect themselves and their information.

Determine Your Legal Requirements

All states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information. Depending on the types of information involved in the breach, there may be other laws or regulations that apply to your situation. Check state and federal laws or regulations for any specific requirements for your business. Read more about what [each state requires for security breach notification](#).

Notify Law Enforcement

Call your local police department immediately. Report your situation and the potential risk for identity theft. The sooner law enforcement learns about the theft, the more effective they can be. If your local police aren't familiar with investigating information compromises, contact the local office of the FBI or the U.S.

Secret Service. For incidents involving mail theft, contact the U.S. Postal Inspection Service.

Notify Managers and Internal Employees

Never keep the information about a data breach secret. After all, your business is about serving customers and clients. Poorly informed employees can often circulate misinformation. Designate a company spokesperson whose role is to speak to the media and ensure employees understand that they are not authorized to speak about the breach. Disclosures of the breach, both internally and externally, should be in accordance with advice from your legal team.

Notify Affected Businesses

If account information — like credit card or bank account numbers — has been stolen from you, but you don't maintain the accounts, notify the institution that does so it can monitor the accounts for fraudulent activity. If you collect or store personal information on behalf of other businesses, notify them of the data breach.

If Social Security numbers have been stolen, contact the major credit bureaus for additional information or advice. If the compromise may involve a large group of people, advise the credit bureaus if you are recommending that people request fraud alerts and credit freezes for their files.



[Equifax Website](#)
or 1-800-525-6285



[Experian Website](#)
or 1-888-397-3742



[TransUnion Website](#)
or 1-888-909-8872

Notify Individuals

If you quickly notify people that their personal information has been compromised, they can take steps to reduce the chance that their information will be misused. In deciding who to notify, and how, consider:

- State laws
- Nature of the compromise
- Type of information taken
- Likelihood of misuse
- Potential damage if the information is misused

For example, thieves who have stolen names and Social Security numbers can use that information not only to sign up for new accounts in the victim's name, but also to commit tax identity theft. People who are notified early can take steps to limit the damage.



Consider offering at least a year of free credit monitoring or other support such as identity theft protection or identity restoration services, particularly if financial information or Social Security numbers were exposed.

Clearly describe what you know about the compromise. Include:

- How it happened
- What information was taken
- How the thieves have used the information (if you know)
- What actions you have taken to remedy the situation
- What actions you are taking to protect individuals, such as offering free credit monitoring services
- How to reach the relevant contacts in your organization
- Include current information about how to recover from identity theft

Conduct a Security Post-Mortem

A post-mortem is held after an incident has taken place. The security team meets with the rest of the organization (or the affected team) and talks through what happened, identifies causes, lessons learned and how to move forward.

The key to an effective post-mortem is doing it in a way that does not place blame on employees. This encourages communication and collaboration between security and members of other teams.

The key steps in conducting a post-mortem include:

1. Do your homework

Take your time to understand exactly what happened and figure out how to explain it to your team in appropriate terms. If there was a phishing attack that occurred when an employee clicked on a bad link, talk about what phishing attacks look like and signs to look out for. If there was a larger systemic or organizational failure that ultimately led to a specific incident, make sure you have a clear picture of the problem (not just one person's role in it) before you sit the team down to talk about it.

2. Discuss How to Prevent Problems in the Future

The most important part of a security post-mortem is making sure the problem doesn't happen again. In some cases, this may be a matter of increasing employee education and training to make sure that everyone understands what they need to look out for in the future. In other cases, there is a larger organizational issue — a broken process, a missing or misunderstood tool or technology, or misunderstood directives. The post-mortem is a good time to begin the correction process. For example, if a flawed process was ultimately to blame, have an open discussion about how that process needs to be amended and solicit input from everyone on next steps. This way, after the post-mortem, you can form a plan of attack. Keeping everyone focused on prevention (or improvement) will go a long way toward reducing blame.

3. Encourage an open discussion

Make it clear that team members can always come and talk to the security team if they aren't sure whether something is safe, or if they think they've already done something that will compromise security. Keeping an open line of communications will help identify and remediate potential issues later as well as foster trust and transparency. Consider creating a channel where people are encouraged to post about anything that strikes them as suspicious and have a security team member follow up with them.





Conclusion




Since data breaches are becoming more common, how you respond to one can go a long way in maintaining your business reputation and keeping you from losing the trust of your customers. Taking a proactive stance against vulnerabilities through continuous scanning of your environments can go a long way in preventing breaches. They allow your security team to identify, prioritize, and remediate issues before attackers have the opportunity to exploit them.

If your business does not have an incident response plan, making one should be a top priority. Then practice and review your plan. This helps members of your response team to remain calm

About VULNERA

Security assessments should empower companies to achieve compliance while also improving the security of the organization. The industry is riddled with variances in quality, fragmented offerings, logistical constraints, and resource limitations. That's why VULNERA built solutions that help organizations with the heavy-lifting so stakeholders can focus on what matters – remediating security issues.

Solutions

-  **One-Time Assessment**
Satisfy an audit, third-party request, internal initiative, or other requirement to perform a security assessment. [Learn More](#)
-  **Remediation Validation**
Conduct an assessment and work through remediation so you can validate vulnerabilities are resolved. [Learn More](#)
-  **Continuous Assessment**
Continuously tackle vulnerability management with visibility into assets, vulnerabilities, and remediation progress. [Learn More](#)

Appendix A: Additional Resources

References below provide best practice recommendations regarding data breach response process and tips on general information systems security.

Congressional Research Service	<ul style="list-style-type: none">• Federal Information Security and Data Breach Notification Laws (2010)
National Institute of Standards and Technology (NIST)	<ul style="list-style-type: none">• NIS SP 800-61, Computer Security Incident Handling Guide (2012)• FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems (2004)
Cybersecurity Infrastructure Security Agency (CISA)	<ul style="list-style-type: none">• Cybersecurity Incident & Vulnerability Response Playbooks• Cyber Incident Response
U.S. Department of Health & Human Services (HHS)	<ul style="list-style-type: none">• Breach Reporting• Breach Notification Rule• Breach Reporting Guidance
Federal Privacy Council (FPC)	<ul style="list-style-type: none">• Breach Response
Federal Trade Commission (FTC)	<ul style="list-style-type: none">• Data Breach Response: A Guide for Business
National Institutes of Health (NIH)	<ul style="list-style-type: none">• Privacy Incidents and Breach Response
National Conference of State Legislatures (NCSL)	<ul style="list-style-type: none">• Security Breach Notification Laws



+1 626.515.5523
www.vulnera.com



SB1021 REVA 11/2022