What to do after a data breach?

Posted At : April 27, 2021 3:40 PM | Posted By : Admin
Related Categories: Security

A data breach is just about the scariest thing that can happen to your business's or organization's technology. It's an assault and it can feel very personal. Depending on what you do next can actually make the situation worse or quite a bit better. Here is an article from the Federal Trade Commission with general advice on how to proceed. It can be useful in developing an internal plan of protecting your information and how best to proceed in the event of a breach.

*And **please call The Computing Center immediately**. We can be of help even if you know how to proceed. We can be the 2nd opinion and also can use our resources to confirm the plan.*

You just learned that your business experienced a data breach. Whether hackers took personal information

from your corporate server, an insider stole customer information, or information was inadvertently exposed on your company's website, you are probably wondering what to do next.

What steps should you take and whom should you contact if personal information may have been exposed? Although the answers vary from case to case, the following guidance from the Federal Trade Commission (FTC) can help you make smart, sound decisions.

SECURE YOUR OPERATIONS

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

> **Secure physical areas potentially related to the breach.** Lock them and change access codes, if needed. Ask your forensics experts and law enforcement when it is reasonable to resume regular operations.

Mobilize your breach response team right away to prevent additional data loss. The exact steps to take depend on the nature of the breach and the structure of your business.

Assemble a team of experts to conduct a comprehensive breach response. Depending on the size and nature
of your company, they may include forensics, legal, information security, information technology, operations, human resources, 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 legal counsel. Then, 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.

Stop additional data loss. Take all affected equipment offline immediately — but don't turn any machines off until the forensic experts arrive. Closely monitor all entry and exit points, especially those involved in the breach. If possible, put clean machines online in place of affected ones. In addition, update credentials and passwords of authorized users. If a hacker stole credentials, your system will remain vulnerable until you change those credentials, even if you've removed the hacker's tools.

Remove improperly posted information from the web.

> **Your website:** If the data breach involved personal information improperly posted on your website, immediately remove it. Be aware that internet search engines store, or "cache," information for a period of time. You can contact the search engines to ensure that they don't archive personal information posted in error.
>
> **Other websites:** Search for your company's exposed data to make sure that no other websites have saved a copy. If you find any, contact those sites and ask them to remove it.

Interview people who discovered the breach. Also, talk with anyone else who may know about it. If you have a customer service center, make sure the staff knows where to forward information that may aid your investigation of the breach. Document your investigation.

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

FIX VULNERABILITIES

Think about service providers. If service providers were involved, examine what personal information they can access and decide if you need to change their access privileges. Also, ensure your service providers 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.

Check your network segmentation. When you set up your network, you likely segmented it so that a breach on one server or in one 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.

Work with your forensics experts. Find out if measures such as encryption were enabled when the breach happened. Analyze backup or preserved data. Review logs to determine who had access to the data at the time of the breach. Also, analyze who currently has access, determine whether that access is needed, and restrict access if it is not. Verify the types of information compromised, the number of people affected, and whether you have contact information for those people. When you get the forensic reports, take the recommended remedial measures as soon as possible.

Have a communications plan. Create a comprehensive 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. Also, don't publicly share information that might put consumers at further risk.

Anticipate questions that people will ask. Then, put top-tier questions and clear, plain-language answers on your website where they are easy to find. Good communication up front can limit customers' concerns and frustration, saving your company time and money later.

NOTIFY APPROPRIATE PARTIES

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

Determine your legal requirements. Most states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information. In addition, 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.

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

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. In addition, 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.

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.

Did the breach involve electronic personal health records? Then check if you're covered by the Health Breach Notification Rule. If so, you must notify the FTC and, in some cases, the media. *Complying with the FTC's Health Breach Notification Rule* explains who you must notify, and when. Also, check if you're covered by the HIPAA Breach
Notification Rule. If so, you must notify the Secretary of the U.S. Department of Health and Human Services (HHS) and, in some cases, the media. HHS's Breach Notification Rule explains who you must notify, and when.