Nonprofit Risk Management Center
Find the answer here | nonprofitrisk.org

READY TO RESPOND

Building Resilience for a Cybersecurity Incident

Cybersecurity breaches can be scary and overwhelming for any nonprofit. Here are six **MUST-DO TASKS** for any organization to ensure you'll be ready if and when a breach happens.

1. **Identify experts who could help your organization conduct a full breach response. If you have legal counsel, they should be on your team and any cybersecurity law or forensic experts your counsel recommends. Your team could also include your information technology and/or information security vendors,** as well as operations, human resources, communications, and management.

2. **Know how you will stop additional data loss and preserve evidence. In the event of a breach, you will need to ensure your organization has multiple people who could bring any affected equipment offline right away.** Get protocols in writing that instruct staff not to turn off the machines until forensic experts arrive or delete or destroy anything that provides evidence of the breach. Your organization will also need to monitor entry and exit points in your systems; put clean machines online in place of breached ones, if possible; update credentials and passwords of authorized system users; and document your steps to preserve evidence for forensic investigations.

3. **Ensure team members and/or vendors know how to remove improperly posted information from the web.** If personal information gets posted on your website in a breach, remove it immediately. Note that Internet search engines cache information for a period of time. You'll need to contact search engines to ensure they don't archive personal information posted in a breach. You'll also need to search for your organization's exposed data to ensure other websites have not saved or published it. If they have, ask the company to remove it.

4. **Have a communication plan.** Create a comprehensive plan that will reach everyone who needs to know about a breach: employees, constituents, donors, vendors, and other stakeholders. Ensure your team knows not to say anything misleading about the breach or publicly share information that might put people's personal information at further risk.

5. **Gather contact information and plan how you will notify affected parties of a breach.** Determine your legal requirements. Every state has laws that require notification of security breaches that involve personal information. Other laws or regulations may apply as well.

A. **Notify law enforcement.** Call your local police department right away. Report the situation and the risk of possible identity theft.

B. **Evaluate health data reporting requirements.** If the breach involved electronic personal health records, you might have to notify the federal trade commission and/or the Secretary of the U.S. Department of Health and Human Services, as well as the media.

C. **Notify affected businesses.** If the breach involved account access information, notify the institution that maintains the accounts so it can monitor them for fraudulent activity.

D. **Notify individuals.** If you quickly let people know their personal information has been compromised, they can take action to reduce the chance that someone will misuse the information.

- **Consult with your law enforcement contact** about the timing of the notification, so it doesn't impede the investigation.
- **Designate a point person in your organization to release information.**
- **Consider using letters, websites, and toll-free numbers** to communicate with the public, especially if you don't have contact information for all the people whose information has been compromised.
- **Consider offering at least a year of free credit monitoring or other support.**

6. **Bring your systems back online safely.** Make sure your team knows that you'll need to wait for your forensic experts to give you the all-clear before you bring the affected systems back online. Take any additional steps your experts advise to ensure systems are secure against future attacks.

Helpful Resources.

Data Breach Response: A Guide for Businesses - FTC

How to Manage A Data Breach: 5 Steps To Keep Your Business Safe - SecurityMetrics

How A Company Should Respond To A Security Breach - Chron Small Businesses