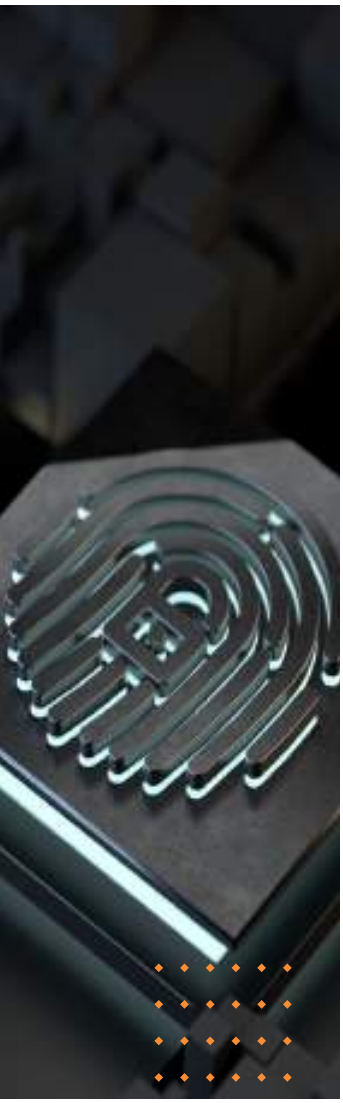
DATA BREACHES

A DEFINITIVE GUIDE FOR BUSINESS OWNERS

SUNDOG

YOUR STRATEGIC IT PARTNER

TABLE OF CONTENTS



What is a data breach?

Data is imperative to running a business effectively. It helps organizations make better decisions, analyze company performance, simplify processes, and understand consumer needs. Because data holds so much value, it's important that you take extra precautions to protect your business from data breaches.

A data breach is a security incident where unauthorized entities gain access to confidential data, which may include personally identifiable information, protected health information, intellectual property, trade secrets, and other sensitive company information.

No business is immune to breaches. Even enterprises like Microsoft and Facebook have had their share of data leaks, and alarmingly, 43% of data breaches involve small- and medium-sized businesses.

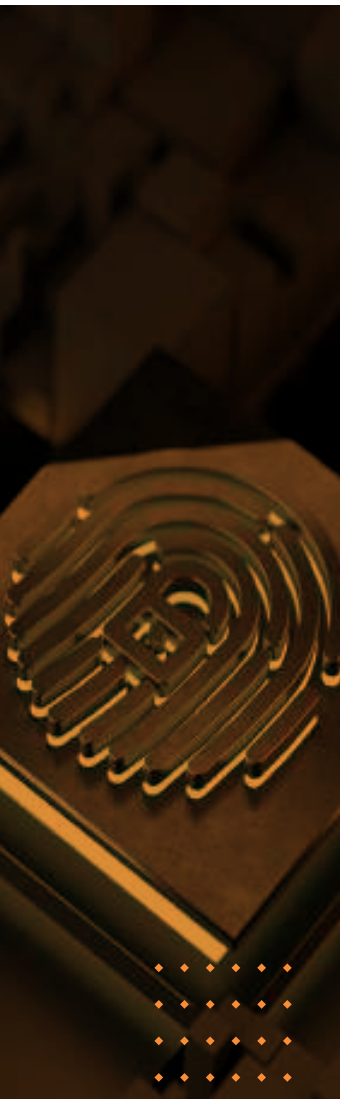
Who causes data breaches?

A data breach can be carried out by the following:

Malicious third parties – These are hackers who utilize various attack methods, such as malware or phishing, to steal company data. Some may also infiltrate lost or stolen company devices like laptops and smartphones that hold sensitive data.

Insiders – Employees can also cause data breaches, whether maliciously or accidentally.

- ***Malicious insiders*** intentionally access data to cause harm to the organization. They may have legitimate file access privileges or use attack methods to access sensitive information.
- ***Accidental insiders*** are employees, vendors, or partners who may accidentally click on a malicious link, forgo company policies, or use unapproved software. Accidental insiders are equally risky as their malicious counterparts.



What are the common data breach methods?

Malicious actors use the following attack methods to steal data from companies:

Phishing – This involves hackers sending emails or text messages to employees asking them to "verify" their account by clicking on a fraudulent link. If the employee submits their login credentials, the hacker will gain access to the company network.

Malware – Hackers can use keyloggers, spyware, backdoors, and bots to steal data from companies. They can launch malware via rogue email attachments, unpatched software, or malicious websites.

Mobile devices – Employees' personal devices can be used for data breaches. For instance, malware-laden apps can grant hackers access to company data stored on a smartphone or laptop.

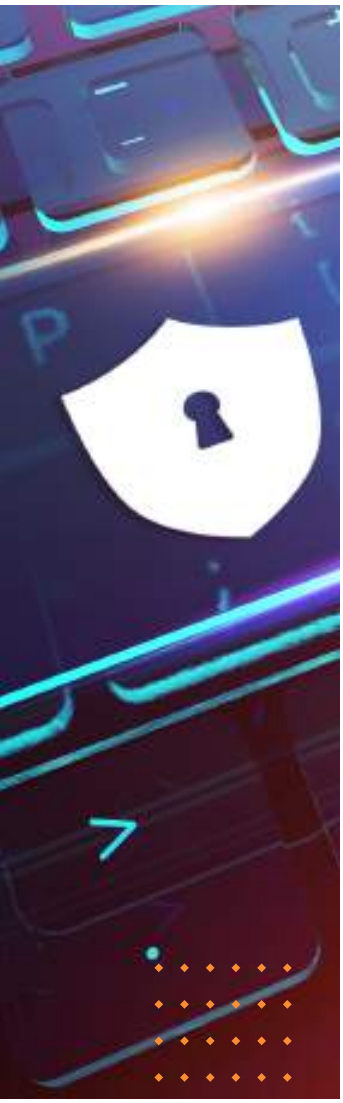
What do malicious actors do with stolen data?

After your data has been stolen, malicious actors may do any of the following:

Sell company information – After doing an inventory of the data, the hacker can sell the information in bulk on the dark web where they stay anonymous, making their activities impossible to trace.

Commit identity fraud – A hacker can steal the identity of a company employee and do unscrupulous activities such as accessing sensitive areas of the organization's IT infrastructure to steal more data.

Hold the data for ransom – If the breached data included trade secrets and other confidential information, the hacker can blackmail a business into paying them in exchange for the data's privacy. The information can be destroyed or sent to competitors if the organization fails to comply.



Signs your data has been compromised

Despite advancements in security software, data breaches can go undetected for months or even years. For instance, the Yahoo data breach that affected more than 500 million user accounts occurred in late 2014, but was only discovered and reported in the second half of 2016.

Hacking tools and data breach techniques are often covert and designed to evade detection from security systems, but not all hope is lost. Cybercriminals often leave subtle clues that indicate they've compromised your systems and data. While these clues can vary depending on the type of attack, there are common red flags to watch out for.

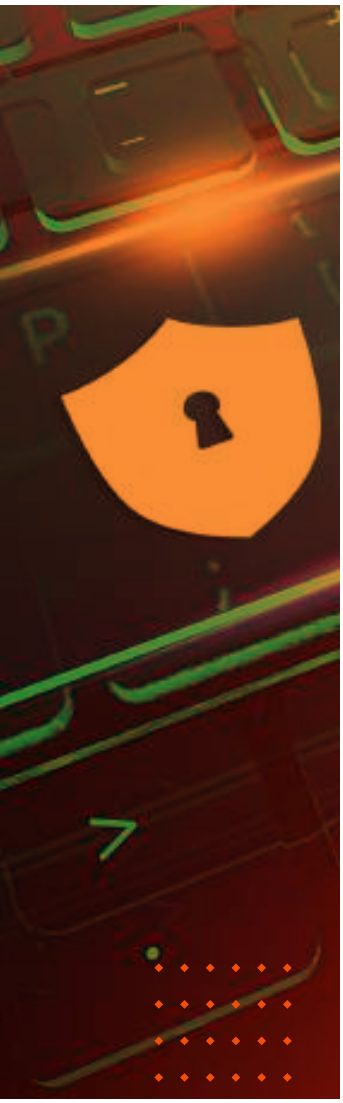
Abnormal account activity

Once cybercriminals establish a foothold in your system, their next priority is to elevate their system privileges so they can access sensitive information. Monitor your systems regularly for any unauthorized user accounts attempting to access and alter personal, financial, and proprietary records. If certain users appear to be transferring large amounts of data from company servers, your data may be compromised. Similarly, if certain users appear to be logging in at unusual times or from suspicious remote locations like a different country, your data could be in danger.

Another sign that your data has been compromised is that employees are receiving strange emails from one another. This suggests cybercriminals may have already hijacked one of your company accounts, and are trying to further compromise your business by sending authentic-looking phishing emails to other potential victims.

Locked user accounts

When users are unable to access their accounts despite using the correct password, a hacker may have already infiltrated the account and changed the password. In such cases, the system administrator must check account activity for password resets to confirm the breach. Then, have the IT team review access privileges and advise staff to change their passwords to minimize damage.



File changes

Files that have been modified, deleted, or replaced are a major sign of a breach. Unless you're regularly monitoring your systems, you may not notice these file changes for a long time. There can be dozens of critical documents being changed or even siphoned from your company database on a daily basis. Rogue employees and cybercriminals are often the culprits when it comes to sudden file changes, but unwitting employees may also modify or delete sensitive files by accident.

Having processes and security software in place to distinguish between normal changes and malicious ones is crucial. Fortunately, managed IT services providers (MSPs) offer round-the-clock monitoring services so you can detect malicious file changes as soon as these occur.

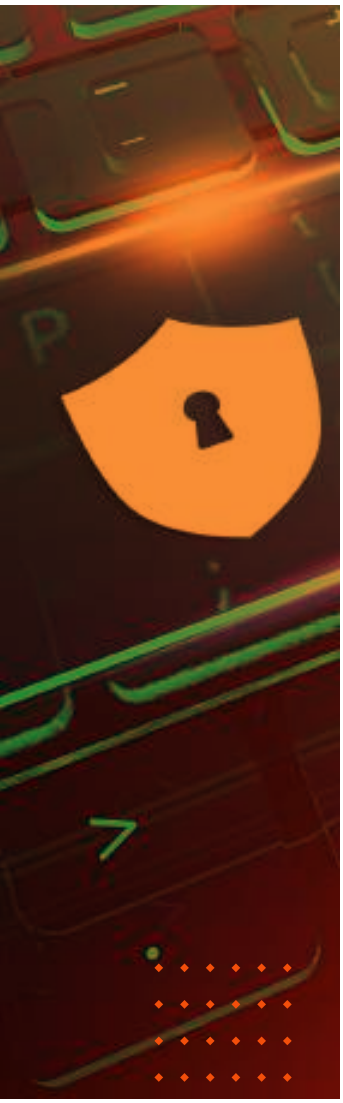
Unauthorized disclosure of information

While most data breaches are caused by cybercriminals, employees can also cause data breaches accidentally. They can share sensitive information with the wrong recipients via email, post classified information on the web, or even lose track of paperwork and storage devices. Make sure employees know to report these accidents so you can address the issue right away.

Device tampering

If an employee discovers that their device is still running after being turned off or a USB drive they don't recognize is plugged into the CPU, a data breach through device tampering may have occurred. Device tampering doesn't happen frequently because it requires a cybercriminal to physically break into work premises and access devices. Leaving devices unattended in public places like a cafe may also lead to tampering and eventually a data breach.

If employees have confirmed that their device has been tampered with, they should report it immediately to a system administrator and avoid logging in to business applications. For all they know, there may be keylogger malware or spyware designed to steal sensitive information installed on the device.



Slow internet connection

A slow internet connection may indicate that malware or other cyberthreats have successfully infiltrated your network. If employees report that their internet connection has slowed down to a crawl, monitor your network for unusual internet activity and high volumes of outbound traffic. Malicious programs and intrusions often consume your internet bandwidth so they can transfer data from infected devices to a cybercriminal's untraceable servers.

Strange computer behavior

Malware-induced data breaches can have different effects on your computer's performance. For one, they can use up your computer's processing power, causing it to run slowly. In most cases, they install dozens of third-party apps without your permission, litter your desktop with pop-up messages, redirect you to a different homepage, and add new toolbars to your web browser.

Sophisticated programs can even disable antivirus software to evade detection. Meanwhile, specialized malware like ransomware can encrypt all computers connected to your network.

The best way to spot these attacks early is to regularly update your security software and scan your systems for potential breaches. MSPs will proactively monitor your systems for harmful programs and help your business recover.

What to do in case of a breach

When you've been hit by a data breach — whether it was caused by cybercriminals or insiders — you need an incident response plan to bounce back. Not having one can result in massive financial losses and reputational harm for your organization and clients.

You can create an effective incident response plan by forming a response team composed of management, human resources, communications, legal, and IT personnel. The plan should clearly define what constitutes a data breach and establish clear guidelines on how to recover from it.

Below are five key steps you should include in your incident response plan.

Contain the breach

The first thing you need to do upon discovering a breach is to secure your systems and prevent further damage to your business.

- [ ] Immediately disconnect any affected equipment from the internet to stop additional data loss, and wait for forensic experts to arrive.
- [ ] Disable your network to limit the spread of self-propagating worms and ransomware.
- [ ] Secure physical areas that may be prone to breaches.
- [ ] Have staff reset their passwords to prevent account hijacking.
- [ ] Restrict access privileges of potentially malicious insiders while you are investigating the breach.
- [ ] Remove any sensitive data mistakenly posted to the web and ask recipients who have access to exposed information to delete them.

Analyze the attack

It's important to assess your IT environment to understand the severity of the data breach. Specifically, you'll need to interview those who reported the incident, root out the cause of the breach, identify the information that was compromised, and determine what systems should be fortified. Consulting with a cybersecurity and forensic specialist at this stage is highly recommended.

Fix your system and secure vulnerabilities

Once you've fully understood the nature of the data breach, your next priority should be repairing and fortifying your defenses. Make sure you:

- [ ] Update your firmware, operating systems, and security software.
- [ ] Run computers and servers in safe mode and remove any detected malware with a strong anti-malware program.
- [ ] Delete corrupted files and restore clean copies of your data with cloud backups.
- [ ] Utilize trusted decryption software to address ransomware.
- [ ] Encrypt your data and install advanced threat protection software.
- [ ] Reevaluate access privileges for each employee.
- [ ] Retrain any staff who may have accidentally caused a breach.

Report the incident

When your business suffers a data breach, you are legally obligated to notify authorities and affected parties. This means you need to:

- [ ] Call local or federal law enforcement for incidents involving data theft and cyberattacks.
- [ ] Check state and federal regulations for specific requirements regarding data breach notifications.
- [ ] Follow breach notification standards as outlined by industry-specific initiatives like the Health Insurance Portability and Accountability Act of 1996 (HIPAA) for healthcare and the General Data Protection Regulation (GDPR) for companies managing European Union- (EU) related data.
- [ ] Inform affected businesses or individuals and major credit bureaus about the breach.
- [ ] Create a communication strategy detailing what response staff are supposed to say to customers and stakeholders after a breach.

- [ ] Send emails that explain what data was compromised, how the breach occurred, what actions you've taken to fix the issue, and what clients should do.
- [ ] Set up an FAQ page so affected parties can learn more about the incident.
- [ ] Promptly draft a press statement about the mistakes that led to the breach.

Evaluate your data breach response

Finally, review how well your company managed the crisis and identify areas for improvement. Was your communication strategy standardized and reliable? Are your data recovery procedures and security software adequate? How can your company ensure the same breaches won't happen again? Asking these questions is crucial in mitigating the constant threat of data breaches.

How to prevent data breaches

No business is immune to data breaches. Cybercriminals will continue devising new methods to steal sensitive data from businesses for personal, financial, and professional gain. Fortunately, many data breaches are preventable if organizations follow the checklist below:

- [ ] **Know your legal obligations.** Your business must be compliant with applicable privacy laws. For instance, the EU's GDPR establishes rules on how organizations handle the data of EU citizens and other entities. Meanwhile, HIPAA provides patients access to their medical records and gives more control over how their personal health information (PHI) is used and disclosed.

- [ ] **Provide security training.** Train employees to recognize online scams by conducting simulated phishing exercises. Send out fake phishing emails to everyone in your company, and provide the necessary training for those who struggled with responding to the fake attack. Also, teach your staff to use strong passwords, file and store data properly, and avoid opening potentially malicious files.

- [ ] **Implement multifactor authentication (MFA).** MFA uses more than one method to verify a user's identity. For instance, in addition to a password, a user will be required to provide an SMS code, a smartphone prompt, a fingerprint scan, or a facial scan. This way, even if a hacker acquires an employee's login credentials, they won't be able to log in without access to the other authentication factors.

- [ ] **Keep business and personal email accounts separate.** By doing so, even if a cybercriminal infiltrates your personal email address, they cannot access any company data. Be wary of your email attachments too, as they may be used to attack your business accounts.

- [ ] **Implement strict data access privileges.** To prevent data breaches, your business's data must remain accessible only to authorized people. Access management platforms such as Microsoft Azure can help you secure your data better. Its role-based access control (RBAC) system allows you to set user access privileges to select areas of your system.

- [ ] **Keep your software updated.** Because of users' negligence when it comes to updating their programs, cybercriminals are able to exploit software vulnerabilities to attack a business's systems. Make it a habit to update your antivirus software so it can detect and block the latest malware making the rounds.

- [ ] **Create a data breach response plan.** This plan is crucial in case your business falls victim to a data breach. It should list out the steps you need to take, such as notifying authorities and customers, contacting IT consultants and insurance companies, and investigating the breach.

- [ ] **Limit corporate data access on mobile devices.** Set a time and place where employees can access company data on their mobile devices. For instance, you can allow them to access company and client information while on office premises. Their privileges should be revoked when they leave for the day.

- [ ] **Partner with a managed IT services provider (MSP) like Sundog.** MSPs can provide proactive system maintenance and threat monitoring so potential issues can be dealt with before they cause downtime and data breaches for your business.

MAKE CYBERSECURITY A TOP PRIORITY

SUNDOG OFFERS FIRST-CLASS SERVICES TO PROTECT YOUR DATA

Minimizing data breach risks and knowing how to respond when a security incident does occur can be an overwhelming task for any business, but you don't have to face these challenges alone. A dependable managed IT services provider like Sundog can establish a solid security strategy and framework to safeguard your data.

This means we will fully assess your security vulnerabilities and deploy robust preventive measures to defend against data breaches. We'll then proactively monitor your systems for any signs of a breach and help your business respond quickly. Best of all, our solutions and services can be customized to your needs and budget, so you can have peace of mind knowing your data is safe and sound.

Want to learn more about our cybersecurity services?

Contact our experts today!

Phone: **(815) 991-2400** Email: **yourteam@sundogit.com**

SUNDOG

YOUR STRATEGIC IT PARTNER

WWW.SUNDOGIT.COM