# How to Spot Data Breach Warning Signs to Protect Your Business

Data breach. The phrase suggests compromised customer data, with resulting legal battles and hefty remediation costs. Most attacks take weeks, or even months, to detect. However, businesses that detect and address data breach warning signs can save millions of dollars while protecting sensitive data and business reputation.

Alarmingly, according to a recent Ponemon study, hackers spend an average of 197 days inside the targeted system before being discovered. That represents more than six months to pull sensitive information, introduce malware or encrypt files.

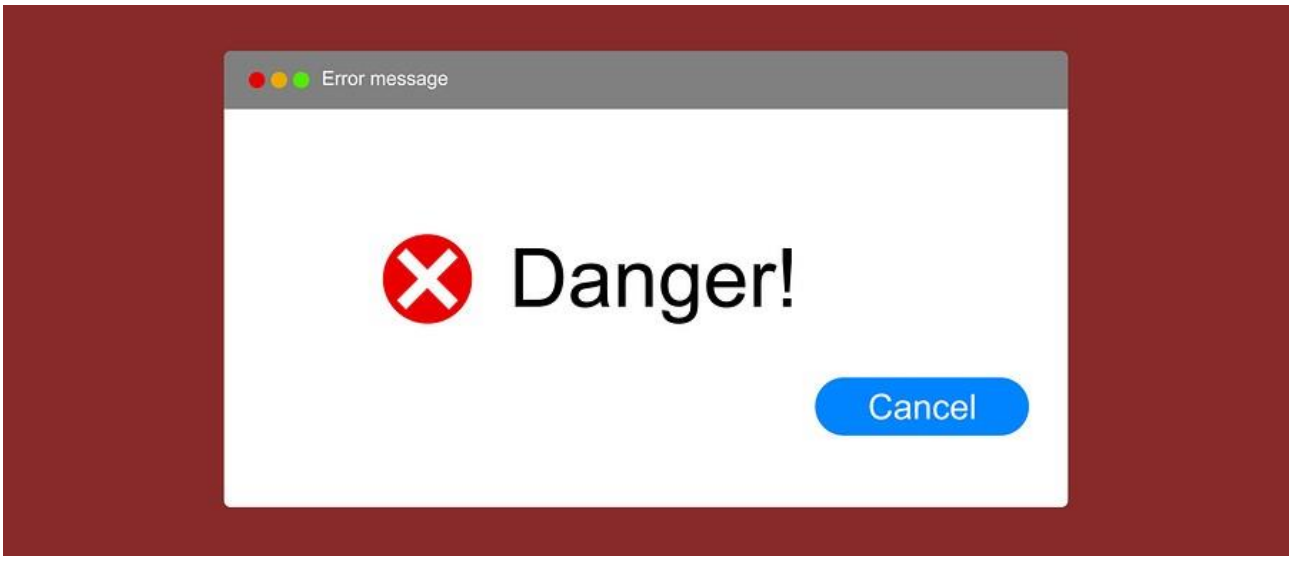
Adding to the problem, the mixture of public and private clouds, along with an increasingly mobile workforce and a growing IoT, creates an environment with hundreds of entry points. Hackers can enter the system, launch an attack and leave long before anyone notices any damage.

However, by following a few key steps, organizations can detect data breaches early enough to mitigate the consequences.

## 1. Pay Attention to the Little Things

The number one strategy to detect early data breach warning signs involves simply paying attention to the little things. If a user reports an unusual problem, no matter how small it seems, determine the source of the problem. This could include situations such as the following:

- Applications, such as email or word processing, that take longer than usual to load
- Abnormally slow internet or devices
- Frequent pop-up messages (including fake warnings) or unexpected toolbars in the internet browser




- Locked accounts, passwords that suddenly fail to work
- High volume of outbound traffic on the system
- Suspicious files
- Mouse cursor moving on its own
- Network access from an unusual location, or repeated access attempts in a short timespan
- New users with admin privileges
- Disabled antivirus or security software

Taking the time to discover the root cause of the problem can save significant headaches down the road. For example, a client recently reported a problem with a mailbox filling up quickly. After some detailed sleuthing, engineers discovered that hackers had added carefully hidden code that secretly forwarded copies of all outgoing messages to an unauthorized third party.

This client had implemented two layers of email filtering, but even that failed to stop the attack. The end user who reported the problem and the engineers who conducted detailed research saved the company from further damage that could have proved disastrous.

## 2. Tight Policies

Secondly, automate policies wherever possible to catch suspicious inbound and outbound traffic. This includes setting filters in the firewall and email systems. Additionally, automated monitoring can provide alerts to unauthorized access, suspicious files or unusual code.

In the example above, engineers added additional monitoring to alert administrators the next time anyone created a new forwarding rule. The situation had exposed an open door, which the organization then closed to prevent future breaches.

## 3. Educate Employees

Both end users and technicians need better training in best practices to promote system security and recognize data breach early warning signs. End users should know what early signs to look for, such as popups or slow system response times. And they need to know how to report any anomalies.

On the technical side, IT staff need sufficient training to learn how to conduct appropriate research and report back with a root cause analysis. All too often, a technician will fix a symptom without taking the time to identify the cause. They must develop the ability to differentiate between normal situations and potential red flags.

## 4. Expose Data Breach Warning Signs with Security Audits

In addition to setting automatic alerts for specific potential problems, system administrators should review system logs on a regular basis. They should also schedule regular security scans and penetration testing to highlight system vulnerabilities.

## 5. Constantly Improve Security

Hackers constantly study their targets and employ new tools and technology to up their game. You need to do the same. At the very least, implement basic cyber security best practices. Educate yourself about emerging technologies, including artificial intelligence, that can provide advanced security.

To increase your protection, partner with security professionals who can walk you through the steps to keep your system safe and ensure regulatory compliance. The experts at eMazzanti will help you implement a comprehensive cyber security strategy, including automated policies and compliance monitoring.

To learn more, call us today. You can also check us out at the upcoming National Retail Federation 2020 Vision conference, January 12-14 in New York City.