Data loss prevention: Securing your sensitive data

A group of large-scale German companies including BASF, Henkel, Siemens, and Roche has been hit by a cyber-attack as reported by Reuters UK on 24th July. The hack was carried out using a type of malware called Winnti having the potential to remotely access the computer network of the victims. The incident, while not an all-time-worst data breach is a frustrating reminder of the potential attacks that could compromise your most sensitive information!

Cybersecurity crimes are increasingly becoming a day-to-day struggle for organizations. Companies end up being targeted regardless of their size, line of business, or revenue.

Knowing the risks

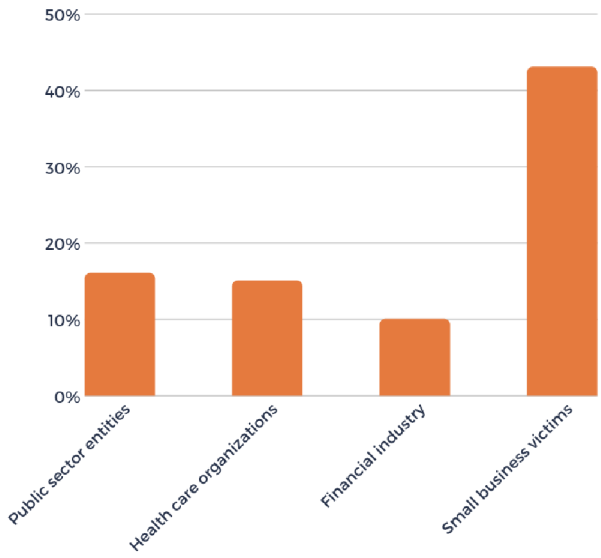


Fig.1. Data Breach Victims
Source : Verizon 2019 DBIR

Hackers of today are getting bolder and better at penetrating security barriers to enact more damaging attacks on organizations. Even if you have good insights on the ways of securing your sensitive data you can't be 100 percent sure that you're not going to be the next victim.

Data breaches can be a scary ordeal for the businesses involved. From fines to customer loss and legal ramifications – the consequences can be brutal and long-lasting. Sensitive corporate data falling into the wrong hands could have catastrophic effects that may even threaten the very existence of your organization.

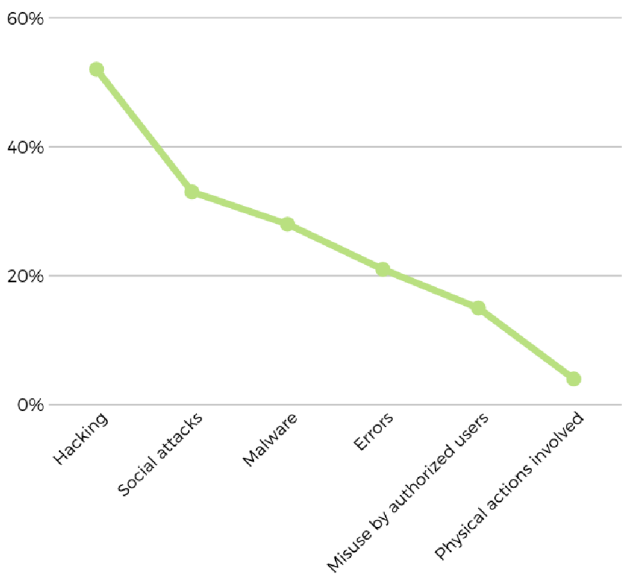
You'll have to deal with the financial repercussions and reputational damage caused by the data breach. Striving to rebuild the trust of customers and stakeholders is going to be the hardest part.

Cyber-attacks: How they happen?

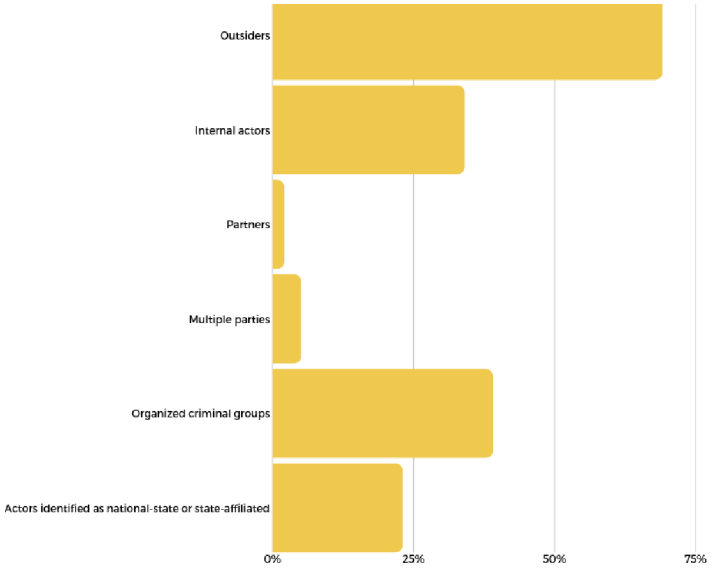
Although you can't predict how exactly the hackers are going to attack your sensitive data next time, understanding the threats can help you efficiently manage the risks. Knowing the cause is the primary step toward helping your organization tackle the threat of data breaches. Cyber-attacks by malicious outside actors top the list. Hackers use various attack vectors to gain access to sensitive information (there are always new methods proliferating).

Common causes of a data breach

- **Malware** or Malicious software is designed to render a computer, server, or system inoperable sometimes granting root access permission to the attackers so that they can control the system remotely.
- **Ransomware** is a technique by which cybercriminals hold the victim's data hostage by getting them to click on email attachments or links designed to make the system or data inaccessible. Perpetrators then demand a ransom to grant access back or by threatening the public release of confidential information.
- **Phishing** scheme too involves emails, but attackers may also use other techniques like text messages, social media quizzes, and even phone calls to trick the victims by disguising themselves as a trustworthy entity and getting hold of critical data.
- **Denial of Service** works by overwhelming a server or website with a flurry of bogus traffic until it is sent offline.



Now, attacks are not always perpetrated by an outside hacker, the carelessness of insiders can also put you in jeopardy. All it takes is a single click on a phishing email to get the entire organization exposed. How your employees behave can have a huge impact on the data security of your organization. They may accidentally send sensitive data to the wrong person or share it publicly. Data loss can also be from a lost or stolen device kept unencrypted.



Insider threat is another sort of data breach. In some cases, the insider might have deliberately accessed or shared protected data with the intent to cause harm to the company. While most attacks are financially motivated and involve outsiders, the contribution of internal actors is still a staggering 34% according to the 2019 Data Breach Investigations Report.

Mitigating the risk

Most companies have unprotected data and poor cybersecurity practices in place, which can make them vulnerable to attacks. Despite the fact that there is no silver bullet to protect your data from cyberattacks, there are things that you can do to clamp down the risk of a data breach. Putting in place adequate security measures can be a great starting point for data loss prevention. Implementing these basic safeguards can improve data security to a great extent.

Key steps to securing sensitive data

- Practice good password hygiene – The password for any purpose should be unpredictable and difficult to decipher.

1. Don't use personal information in the password.
2. Include complex characters in the password to make it hard to crack.
3. Avoid reusing the same password for multiple accounts.
4. Keep changing your credentials from time to time.
5. Never store passwords in your browsers.

- Encryption – Unencrypted devices are prone to attack when they are lost, stolen or misplaced. Encryption is the simplest, yet most often neglected technique to secure your sensitive data. Even if an encrypted device is stolen or breached, the data will be useless to malicious actors.
- Two-factor authentication – Enable two-factor/multi-factor authentication on externally reachable authentication endpoints wherever possible.
- Regularly update the software – Your network is vulnerable to attacks when application software and operating system aren't patched and updated.

- Monitor activities and events surrounding the corporate data – Tracking the movement of data within the corporate network will give a greater understanding of your organization's security postures and helps you prevent any unintentional access to sensitive information. A surge in network queries or slowdowns can be indications of an impending attack.

Taking security an extra step

Developing and deploying a data loss prevention strategy goes a long way in ensuring sensitive data is not lost, misused, or accessed by unauthorized users. There are tools to help you control what data end users can transfer. These tools classify confidential and business-critical data and identify policy violations so that unauthorized users can never access or share sensitive data.

Employing a UEM solution with fully-integrated support to enforce security and compliance will drive seamless security to your network. A single UEM solution could assist you with these baseline data security practices and keep your endpoints safe.

Additionally, educating your employees on how to spot and respond to an attack is key to securing your sensitive data. Most often, employees don't recognize that their actions can be a compliance risk. You need to increase cybersecurity awareness among your team and educate them on the best security practices to prevent socially engineered attacks. Especially, when dealing with unexpected emails, potentially phishing or fraud, your employees can be more skeptical and safer. So, train your employees to generate strong passwords, encrypt data and identify any malware.

Cyber-attacks are expected to become even more rampant in the coming years. It is almost impossible to prevent attackers from targeting your data. The goal is to prevent mere attempts from turning into a ruinously high data breach.