Fighting crime with tech: Protecting your information from cybersecurity threats

As businesses increasingly adopt new technologies that help them store and share data more efficiently, such as open-source software and the cloud, they become more vulnerable to cyberthreats.

Temps de lecture : minute

21 September 2023

Of course, there are always promises that these new technologies are safe and come with protections, but cybercriminals often learn to adapt to these upgrades quickly, finding new and more clever ways to breach systems.

Furthermore, human error and uneducated staff also contribute to higher cyber incident rates. As such, it's crucial for you, as a business owner, to find better ways to protect your data. This can include implementing more secure protocols, offering cybersecurity training to staff, and adopting the right technologies.

The biggest cybersecurity threats today

In 2019, the UK government accounted for *1 million instances of cybercrime in England and Wales*. Unfortunately, such a loss can devastate a business, especially smaller ones that don't have the support and resources to bounce back.

Cybercriminals attack organisations across all industries, big and small,

meaning no business is safe. As such, you must understand the potential *cyberthreats your business might face* so you know what to do to protect your company going forward.

- Ransomware: This is the most common cyberthreat that businesses face. It breaches software and encrypts company data so it cannot be accessed, and then holds it for ransom. This can be particularly brutal for small businesses that don't have the money to pay the ransom demand.
- Phishing attacks: These are another common threat to businesses. Phishing attacks typically occur through email, with someone pretending to be a trusted contact and enticing you to click on a malicious link, which then downloads a virus or gives them access to sensitive data.
- Malware attacks: These attacks occur when hackers breach networks and systems and steal or destroy data. They typically come from spam emails, malicious website downloads, or through a connection to another device that is infected.
- Insider threats: Of course, it is also possible for your own employees to steal data. It's not uncommon for employees to have access to accounts and files they shouldn't, which can lead to purposeful malicious intent or even accidental data breaches due to ignorance.

Identifying and assessing what types of threats your company is most vulnerable to should be part of your business' *risk intelligence strategy*. Once you have this information, you can then tailor your cybersecurity approach to be more effective and monitor threats as they arise. Using technology is one way to reduce the cybersecurity threats your business faces.

The right tech can keep your business safe

The *key to reducing cyber incidents at work* is to adopt the right

technology. This might seem backwards because the reason most businesses are at risk is because of digitalization and the integration of new technologies.

One such technology is *blockchain*. Blockchain uses decentralization and cryptography principles. Data is stored in blocks, and each of those blocks is linked to a previous one, which reduces the likelihood of the data being altered. By using reliable blockchain software, you can minimise potential risks.

Cloud Service Providers (CSPs) are another tool that can help keep your company data more secure. Using the cloud can put you at risk, but if you use a CSP, it can help limit what a person can do within the cloud, which can help mitigate data leaks and breaches. CSPs also provide several tools to help with security, such as identity and Access Management, Guardrails, and Web Application Firewalls.

Artificial Intelligence can also be used for security purposes. AI-powered systems can detect the behavioural patterns of users, such as when things are accessed, how frequently they are accessed, and what location they are accessed from. This then enables the AI to learn and predict patterns that might be a sign of fraudulent activity.

Additional ways to prioritise cybersecurity

In addition to using the right technology, there are other steps you can take to *improve cybersecurity protocols* and increase awareness to mitigate threats. For instance, you can offer training courses for your staff. As mentioned previously, human error is also a reason why cyber incidents occur. So to ensure your staff is more aware of cyberthreats and what behaviours to use to avoid them, you can provide them with access to training courses so they can learn more about cybersecurity.

You can also adopt a zero-trust security model. This approach relies on continuous verification to ensure that only authorised users can access sensitive data. Essentially, you limit who can access what data and ensure there are strict verification processes in place. Using these techniques in tandem with effective risk management and cybersecurity technology can go a long way to effectively protecting your business.

In summary

It’s likely that cyber incidents will only continue to increase as organisations adopt more data-sharing technologies that put them at risk. However, as long as you have solid cybersecurity protocols in place, are using advanced tech to keep data secure, and are training your staff to be more aware, then this will help mitigate the risk of data being stolen and systems being breached.

Article écrit par Indiana Lee