Cyber security threats in 2024

ILUX®

The world has, without doubt, changed over the past few years. We are all more aware of cyber threats, and they are no longer an issue for just MNCs. No matter the size, every organisation needs robust security measures to protect its data from cyber criminals.

As we look to the start of 2024, things are completely different in our digital world.

We can no longer rely on installing anti-virus software and hoping for the best.

Cyber criminals relentlessly target businesses of all sizes, all the time, with increasing sophistication.

Companies are experiencing ransomware attacks that totally shut down their whole businesses, making them virtual hostages with no access to their own data.

We've also seen reports of organisations, including schools, having their data stolen and then sold on the dark web.

The consequences of a successful cyber attack can be utterly catastrophic in terms of financial losses and damage to your business's reputation.

Cyber threats are not just becoming more common; they are also evolving and quickly. Keeping on top of your business's cyber security has never been more crucial.

So, as we approach another new year, you may be left wondering what 2024 has in store for us on the cyber front.

This guide gives you our view on the major threats to be aware of next year.

We aren't trying to scare you; we simply inform you of the potential risks and share our experience with you. Once you understand how the criminals work, you can put in place the right security measures to stay safe.

We are, of course, happy to help you with this too.

Call us now for a free audit>>>

The ransomware renaissance

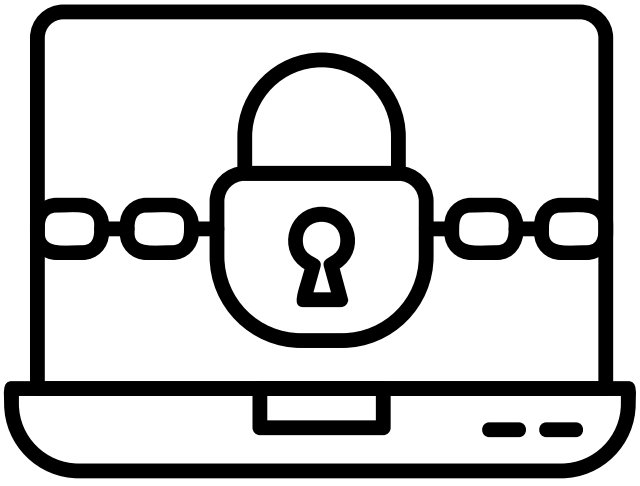
Ransomware is everywhere, and it's getting more and more sophisticated.

Cyber criminals gain access to your network, lock you out, prevent you from accessing your own data, and then try to charge a huge fee to let you back in. There's no guarantee they will, of course.

Without the right security measures and software in place, a full ransomware attack, implemented well, can be extremely hard to undo.

Of course, it is not only the ransom cost but also the days of lost time with no access to your systems, the lost revenue that comes with that, and the reputational damage.

In 2024, we predict that cyber criminals will be gearing up to unleash more sophisticated attacks, utilising machine learning and artificial intelligence. We expect them to fine-tune their approach, making it more efficient and more destructive.



The Internet of Targets

Have you heard of the IoT? It means the Internet of Things – devices other than our computers and phones that go online, such as your TV, your doorbell and even your fridge.

The security for these types of gadgets is often not nearly robust enough. Cyber criminals see this as a golden opportunity and are ready to pounce.

While many of these devices aren't regularly used in the office, many of us work from home and connect to our local Wi-Fi.

IoT devices can be used as a gateway to your network.

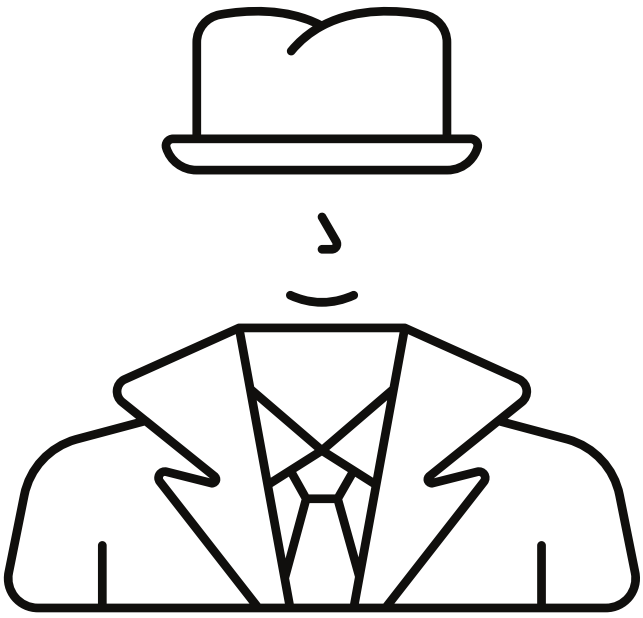
There is likely to be an onslaught of attacks on IoT devices because they can use them to gain access to your network, link devices together to form a botnet (where lots of computers are used to attack others), or, in the worst-case scenario, wreak havoc in critical sectors.

Invisible attacks that never end

Advanced Persistent Threats (APTs) are the sneakiest of attacks, where criminals take a long-term strategy with unauthorised access to your systems. They monitor what you and your business are doing and see what opportunities arise.

In 2024, they will not just be lurking in the shadows; they will be practically invisible.

APTs will use advanced evasion techniques, such as Living off the Land (LotL) attacks, which means using your legitimate software and tools to get past your security controls.



Mobile menace

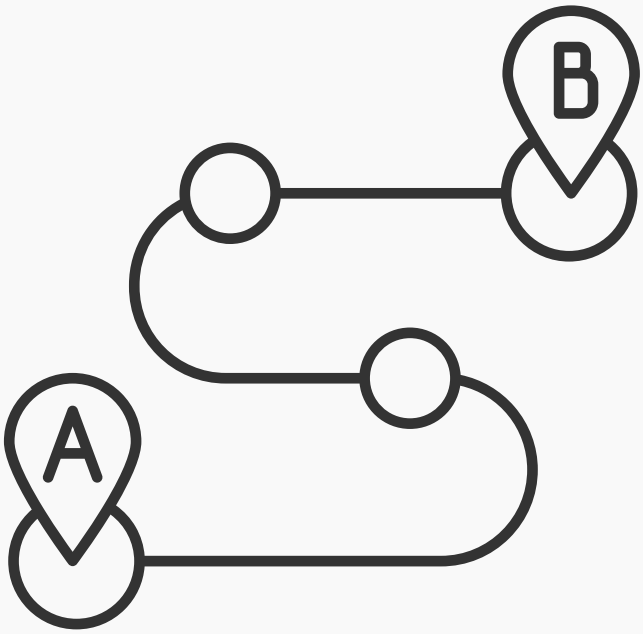
In 2024, cyber criminals will take the battle to your phones and tablets. Expect a significant rise in phone-specific threats like malware, banking trojans (that try to get your login details), and phishing attacks using your real login data on a fake site.

Mobile gadgets are treasure troves of personal and financial information. A breach could lead to identity theft, financial fraud, and unauthorised access to your most sensitive data.

Covert attacks through the tools you rely on

Supply chain attacks, where criminals compromise trusted vendors or third-party service providers, are expected to increase. They insert malicious code into legitimate software updates or gain privileged access to multiple organisations through these trusted entities.

Successful supply chain attacks can lead to unauthorised access, data theft, and long-term security risks.



What about the Cloud?

When it comes to cloud computing, the sky's not the limit; it's the gateway to innovation. As we become increasingly reliant on the cloud and the data we can access on any device, anywhere, at any time, we need to be mindful of its unique security challenges.

That's why it deserves a section of its own in this guide.

Data breaches
Data breaches can occur due to misconfigurations, weak access controls, or insider threats. Robust security measures are paramount.

Insider threats
Trust in cloud service providers is high, but your business still faces risks from your employees or stakeholders.

Insider threats can involve intentional data theft, unauthorised access, or accidental data exposure.

Shared infrastructure
Cloud services operate on shared infrastructure, introducing the risk of vulnerabilities that could lead to unauthorised access to other tenants' resources.

Lack of control and visibility
Relinquishing some control to cloud providers is part of the deal, but detecting and responding to security incidents can make it challenging.

Compliance and regulatory requirements
Regulated industries must ensure their cloud deployments comply with industry-specific regulations and standards. This includes addressing data residency, privacy, and data protection obligations. Careful evaluation of provider compliance capabilities is essential.

Data loss and recovery
Cloud outages or disruptions can lead to data loss or unavailability. Robust data backup and recovery strategies are vital, including regular backups, redundant systems, and disaster recovery plans. Understanding provider backup and recovery mechanisms and aligning SLAs with business needs is key.

10 steps that will strengthen your defences

There's a lot to think about, isn't there? The only way to protect your business next year is to take a fully proactive approach.

Here are 10 steps we recommend to give your business the highest levels of protection.

1. Audit

Before you make any changes, take stock of how well protected your business already is. Carry out a thorough audit to identify strengths and weaknesses. Understand your assets, from critical data to vulnerable entry points. This will act as a navigational chart, helping you make informed decisions about where to allocate resources.

2. Prevention

Strengthen your defences with robust security controls. Implement firewalls, intrusion detection and prevention systems, secure network architecture, and enforce strong access controls. By layering your defences, you create multiple barriers for would-be attackers, significantly reducing the risk of successful cyber assaults.

3. Detection

Despite your best efforts, some threats may still sneak past your defences. That's where detection mechanisms come into play. Invest in security monitoring tools, log analysis, and threat intelligence to identify and alert you to potential security incidents. Swift detection enables rapid response, mitigating the impact of cyber attacks.

4. Incident response

Breaches will happen. Having well-defined incident response procedures in place is crucial. These procedures should outline the steps to take when a security incident occurs, from containment and investigation to mitigation and recovery. Your incident response team should work together to minimise the damage and restore normal operations.

5. Vulnerability management

Regularly assess and test for vulnerabilities in your systems, applications, and network infrastructure. Vulnerability assessments and penetration testing are your allies in this battle (penetration testing is where good guys try to break into your network to see where there are opportunities). Identify and patch weaknesses quickly.

6. Awareness and training

Your people are both your greatest asset and biggest potential vulnerability. Invest in regular cyber security awareness training. Educate your employees about best practices, social engineering threats, phishing attacks, and the importance of strong passwords. If they feel they can recognise and respond effectively to potential threats, that will be a massive boost to your business's overall security posture.

7. Data protection and encryption

Protect your data with encryption. Even if an attacker gains unauthorised access, encrypted data remains unreadable without decryption keys. You should also establish data backup strategies and disaster recovery plans to protect against data loss.

8. Compliance and regulations

Make sure your business meets legal and regulatory requirements related to privacy, data handling, and security. This might involve implementing specific controls, conducting audits, and maintaining documentation to demonstrate your compliance.

9.Continuous monitoring and improvement

Effective cyber security is not a one-time event. Continuously monitor your systems, networks, and what people are doing to detect anomalies and potential breaches. Regularly assess and update your security measures based on emerging threats and changing best practices. By staying agile and adaptable, you will ensure that your cyber security measures remain effective and up to date.

10. Choose the right IT partner

Get this right, and everything else immediately gets easier and faster with less hassle for you. Find a partner who really understands cyber security and can design the most appropriate strategy to protect your specific business.

With every year that passes, cyber security becomes increasingly more complex. By understanding the evolving threats you are able to stay on top of your security measures with a multi-layered approach, you keep your data and staff better protected.

We help businesses like yours all the time. If we can help you, get in touch.

ILUX®