The Cyber Security Guide for Business

Have you ever lived in a small community where crime rates are so low that people genuinely feel comfortable leaving their front doors unlocked?

In a way, that's how business computing was 25 odd years ago. You had locks on the doors of your digital network, but it didn't really matter if you didn't always use them. The worst that could happen was someone getting in and creating a little mischief, rather than doing real damage.

Now as we sit on the verge of 2024, things are completely different in our digital world. Today you don't just want a lock on your door, you want 3 heavy duty locks that are bolted shut all the time. And an alarm. And cameras. And a huge security guy standing guard, complete with a very big scary looking dog on a chain.

These days, cyber criminals relentlessly target businesses of all sizes, all the time. And the attacks take many different forms, all with increasing sophistication.

Have you heard of ransomware attacks that have totally shut down businesses, making them virtual hostages with no access to their own data?

Or the horror of businesses having their data stolen and then sold on the dark web?

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

And cyber threats are not just becoming more common, they're evolving fast. Keeping on top of your business's cyber security has never been more crucial.

So, as we hurtle towards another new year, you're probably left wondering what 2024 may have in store for us on the cyber front

Here's our view on the major threats to be aware of next year.

By the way, we've written this guide not to scare you, but to educate you. Only when you understand how the burglars can get in, can you make sure all the windows and doors are firmly shut and locked.

These are some of the specific cyber threats that will put your business at risk in 2024

The Ransomware Renaissance

Ransomware is everywhere, and it's about to get a makeover.

It's a very specific kind of attack where criminals get into your network, lock you out to prevent you from accessing your own data, and then charge a huge fee to let you back in. There's no guarantee they will, of course. And a full ransomware attack implemented well can be very, very hard to undo.

Cyber criminals are gearing up to unleash more sophisticated attacks, armed with the dark arts of machine learning and artificial intelligence. Expect them to fine-tune their extortion game, making it more efficient and more destructive

They're also setting their sights on bigger prizes. Brace yourselves for potential disruptions and big financial losses as they ransack their way through the digital realm.

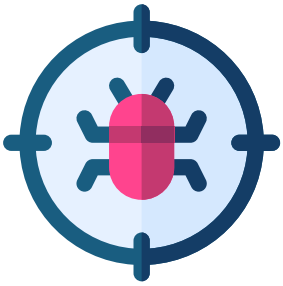
The Internet of Targets

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

Unfortunately, these gadgets often come with security that's as good as a cardboard fort. Cyber criminals see this as a golden opportunity, and they're ready to pounce.

Prepare for an onslaught of attacks on IoT devices. They might use them to get into 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.

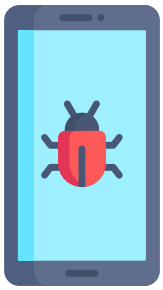
Invisible Attacks that Never End



Advanced Persistent Threats (APTs) are the sneakiest of attacks, where criminals aim for long-term unauthorised access to your systems. They do it to monitor what you're doing, and see what opportunities arise.

In 2024, they're not just going to be lurking in the shadows; they'll practically be invisible.

APTs will use advanced evasion techniques, such as Living off the Land (LotL) attacks. That means they'll use your own legitimate software and tools to waltz past your security controls.



Mobile Menace

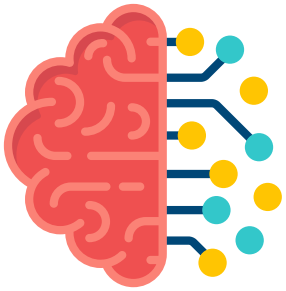
Your mobile devices – those loyal sidekicks you take everywhere – are no longer safe either. In 2024, cyber criminals will take the battle to your phones and tablets. Expect to see a rise in phone-specific threats like malware, banking trojans that try to get your login details, and phishing attacks where they get you to use your real login data on a fake site.

Why? Because your 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 are expected to increase too. This is where criminals compromise trusted vendors or third-party service providers. 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.



AI: The Game Changer

Artificial Intelligence (AI) is the ace up the sleeves of both attackers and defenders. Cyber criminals are using AI to automate attacks, improve evasion techniques, and craft clever social engineering tactics (where they gain access to systems by influencing people to take certain actions).

On the flip side, businesses are adopting AI-powered security solutions to spot threats in real-time.

AI is the new sheriff in town, playing a key role in threat intelligence, anomaly detection, and incident response. It's the future of cyber security operations, and it's here to stay.

What About the Cloud?

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

That's why it deserves its own section 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 businesses still face risks from their own employees or insiders. 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 it can make it challenging to detect and respond to security incidents.

Compliance and Regulatory Requirements
Regulated industries need to make sure 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, including regular backups, redundant systems, and disaster recovery plans, are vital. Understanding provider backup and recovery mechanisms and aligning SLAs with business needs is key.

10 Steps to 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. 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 your areas of strength and weakness. 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:** Remember, great 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'll ensure that your cyber security measures remain effective and up to date.

10 **Choose the Right IT Partner:** Get this one 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 way to protect your specific business. For example, locking everything down is rarely the right approach for any business, as it can encourage staff to cut corners. Imagine a physical security door that staff use several times a day but takes 2-3 mins to unlock each time. At some point, someone's going to prop it open for a few minutes to make their life easier. It's no different with cyber security.

With every year that passes, cyber security becomes increasingly more complex. But when you stay educated about evolving threats, what the dangers are, and stay on top of your security measures with a multi-layered approach, you keep your data and staff better protected.

This is something we help businesses like yours with all the time.
If we can help you,

Get in touch.

aag-it.com/contact

0114 303 0249

hello@aag-it.com