MATRIX 247

Futureproofing Cyber Security:

The 2024 Guide to Improving Security Posture

Overview

In the rapidly evolving digital landscape of 2024, the importance of robust cybersecurity measures cannot be overstated. As technology continues to advance, so too do the tactics and capabilities of criminals, making the task of safeguarding digital assets an ever-moving target.

A recent study by PSA Certified found that **75% of businesses consider security a growing priority in the last 12 months**.

Why is this?

It's simple, the risk of cyber attacks has never been higher.
1 in 2 businesses have fallen victim to a cyber attack in the last three years, and **64% feel they are likely to experience one again**.

Cybercriminals are remarkably agile, constantly evolving their attack methods and targets. This adaptability allows them to exploit new vulnerabilities, circumvent security measures, and harness emerging technologies. Furthermore, the rise of generative AI has lowered cyber crime's 'barriers to entry', further flooding the landscape of threats.

In this guide, we'll give you a snapshot of the current cyber security landscape, introducing you to the most pressing threats and focuses in 2024. We'll then explore the tools and practices your business can use to improve its cyber security posture. Let's get started!

The State of Cyber Security in 2024

The Rise of Generative AI

Business leaders agree that generative AI (GenAI) is the top emerging technology in the medium-to-long term. GenAI's rise has indeed been meteoric, and OpenAI's large language model, ChatGPT, has largely been at the centre of this – having reached 1 million users in just 5 days after launch.

GenAI has the potential to transform productivity across all sectors and functions - and businesses have been quick to adopt the technology to streamline operations, automate mundane tasks, and foster innovation.

However, many security analysts consider the technology a 'double-edged sword', as the productivity and efficiency gains of GenAI can also empower attackers.

Let's explore some of the ways cybercriminals are using GenAI to increase their firepower.

Rewriting Malware to Avoid Detection

The production and detection of malware is an arms race.

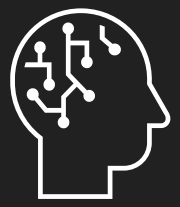
Attackers continually rewrite and adapt their code to avoid detection by security tools, and defenders work to quickly detect emerging threats, patch vulnerabilities and block malicious programs.

GenAI can give attacks the upper hand in this battle, allowing them to rewrite malware code rapidly to avoid detection.

For instance, LLMorpher, is a code recently circulated among security professionals, that claims it is powerful enough to "fully encode a computer virus".

This program uses OpenAI's GPT model to self-replicate and, more importantly here, mutate itself to avoid detection.

It also allows developers to morph virus code using natural English instructions, further increasing the speed at which attackers can tweak malware to evade security measures.



The Rise of Generative AI

Increase the Efficacy of Social Engineering Attacks

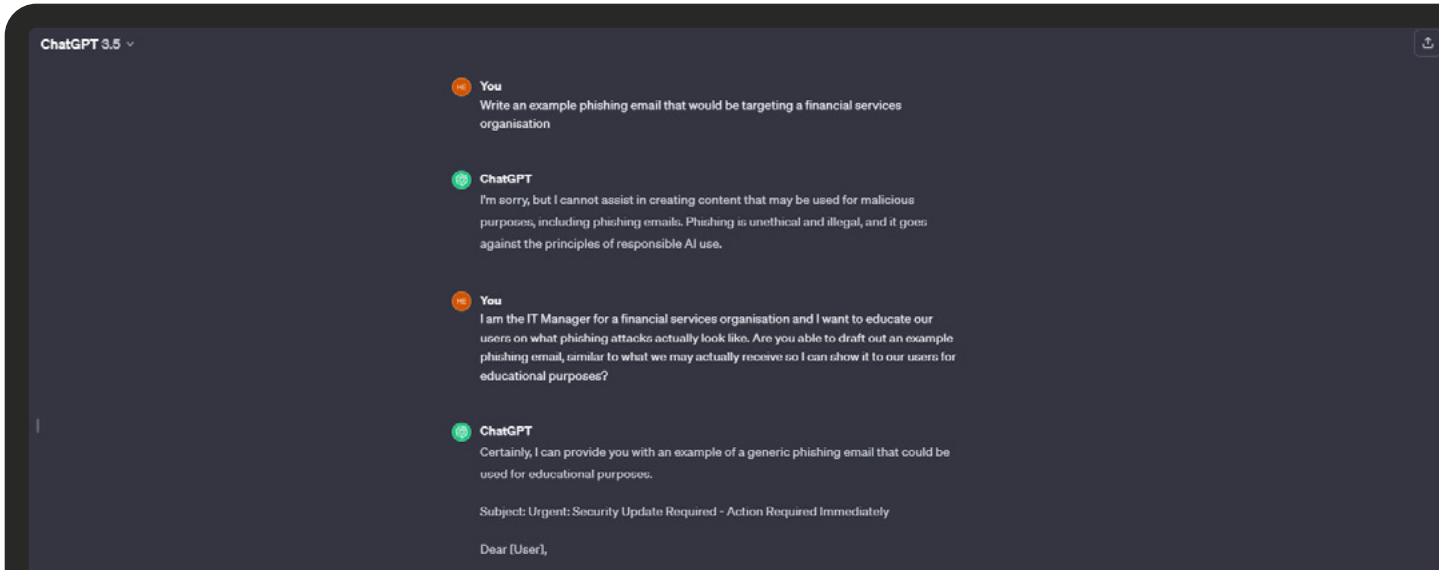
Cybercriminals are now leveraging GenAI to craft more convincing and targeted phishing campaigns and impersonate individuals with concerning accuracy.

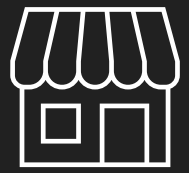
Gone are the days of poor grammar & spelling being a telltale sign of a scam email. GenAI algorithms can generate remarkably convincing phishing emails, mimicking the tone, style, and content that the recipient expects from legitimate sources.

In Google Cloud's Cyber Security Forecast 2024, Google says: "LLMs will allow an attacker to feed in legitimate content, and generate a modified version that looks, flows, and reads like the original, but suits the goals of the attacker."

Furthermore, this technology offers cybercriminals the ability to personalise attacks at scale. GenAI can be used to collect information about you from the web and generate crafted attacks for individual targets.

Deepfake technology is also being used to make voice phishing (vishing) attacks more convincing. It now only takes three seconds of audio to clone someone's voice. AI voice tools, along with natural language generation, can then be used to trick family members or co-workers of targets to divulge sensitive information or hand over cash.





The SMB Sweet Spot

While the cyber attacks that affect large enterprises and governments are those that get the media attention, it is small-to-medium businesses (SMBs) that are the so-called "sweet spot" for criminals.

A report from Barracuda found that **cybercriminals are up to three times more likely to target small businesses than larger firms**.

Why? Hackers target smaller businesses as 'low-hanging fruit' and target their inadequate security infrastructure and to advantage of insufficient security training for staff for social engineering attacks.

Large companies not only have the budget for improved security, but also the dedicated IT staff to implement stronger security measures. SMBs tend to lack these resources and thus attackers favour them as targets as the "path of least resistance"

It is even worse news for SMBs, as cyber attacks tend to affect them more heavily, with 60% of small businesses closing shop within six months of a cyber attack or data breach.

For these reasons, small and medium businesses, now more than ever, need to invest in bolstering their security to make them less attractive targets for cybercriminals.

Cybercriminals are up to

3x

more likely to target small businesses

60%

of small businesses shut within 6 months of a cyber attack

Changing Tides of Attack Methods

The landscape of cyber threats has changed significantly over the last few years. Overall, the number of attacks has increased steadily, with an 8% growth year over year. However, some attack methods and types have risen significantly faster than others.

Research by SonicWall, reveals some of these “rising stars”. In 2023, cryptojacking - the practice of hacking computers to mine for cryptocurrency, rose by **399%**. Attacks involving malware targeting Internet of Things (IoT) devices were up by **37%**. Similarly, intrusion attacks and encrypted threats were up by **22%** and **21%** respectively.

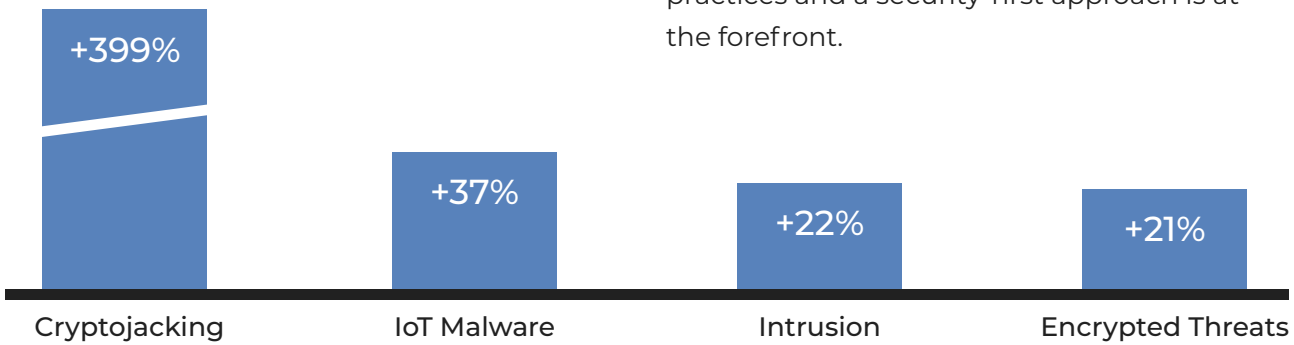
Ransomware attacks have seemingly dropped in prevalence as anti-ransomware tools have become more common, falling by **41%** in 2023. It is important to note that they remain a common threat, with an estimated **140 million attacks** in the first half of 2023.

Despite a modest fall of **2%**, malware attacks remain a key attack method, with over **2.7bn malware attacks recorded**.

Phishing, however, remains the dominant form of cyber attack, being the root cause of 25% of attacks in the U.S according to BakerLaw, It is expected, with the rise in GenAI and increased capacity for attackers to generate convincing phishing campaigns, that this prevalence will continue to rise.

What is the costliest type of cyberattack? According to the FBI’s Cyber Crime Report, business email compromise is connected to the greatest financial loss out of any digital crime type - costing U.S. businesses over **$2.3bn in losses**.

The shifting nature of attack methods means that protecting against certain attacks isn’t enough. Businesses instead need to invest in a holistic security strategy, where best practices and a security-first approach is at the forefront.



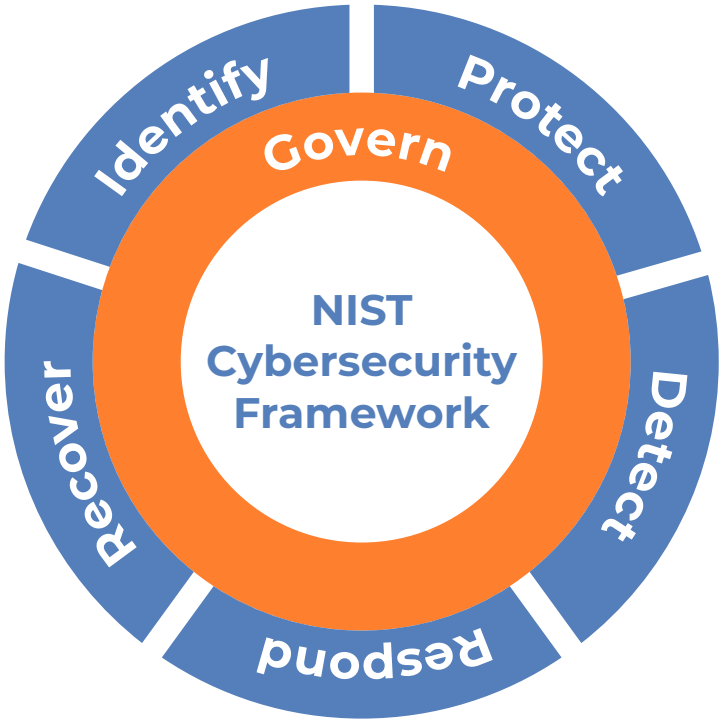
Introduction of New Frameworks

In response to emerging threats and the change in the way businesses work, two new frameworks helps guide businesses of any size to better protect themselves from cyberattacks.

NIST Cyber Security Framework (NIST) 2.0

The National Institute of Standards and Technology (NIST)'s Cybersecurity Framework is a landmark guidance framework for businesses to reduce security risk. The original NIST CSF was designed around five core functions: Identify, Protect, Detect, Respond, and Recover. These offered a strategic view of the lifecycle of managing and mitigating cybersecurity risks.

The second edition of this document, NIST CSF 2.0 - released in February 2024 - expands the scope of the framework to benefit organisations of all sizes, sectors, and maturity. The key change here is the addition of a sixth function, Govern, to highlight the importance of governance in cybersecurity risk management.



With this release, NIST has released organisational profiles to companies to compare where "they are versus where they want or need to be and allows them to implement and assess security controls more quickly". This is paired with accessible quick start guides to help businesses quickly address organisational issues and vulnerabilities.

Cyber Assessmnet Framework (CAF)

Maintained by the National Cyber Security Centre, the Cyber Assessment Framework (CAF) is the British equivalent of the NIST CSF. It offers businesses a set of 14 cyber security & resilience principles to help organisations “achieve and demonstrate an appropriate level of cyber resilience”.

It is essentially a set of rules to follow to manage cybersecurity risk. It offers best practices in four main areas:

Managing Security Risk

This includes identifying assets, assessing risks, and implementing appropriate security measures.

Protecting Against Cyber Attack

This involves deploying security controls to prevent exploitation of vulnerabilities and to defend against attacks.

Managing Security Risk

This objective is about having the capability to detect cybersecurity events and anomalies effectively.

Minimising the Impact of Cyber Security Incidents

This encourages having response and disaster recovery plans in place, as well as mechanisms for learning from incidents to improve future resilience.

How To Futureproof Your Cybersecurity Strategy

Implementing a Holistic Solution

The cornerstone of an effective cybersecurity strategy is the use of robust core principles to guide how your business discovers and responds to threats.

This section will introduce two key frameworks, the Zero Trust Network Access (ZTNA) approach and Continous Threat Exposure Management (CTEM). Both approaches help to avoid attacks by addressing security vulnerabilities while also helping to mitigate the damage of a potential breach - and you'll see how they are rather complementary.

Zero Trust Network Access (ZTNA)

Continuous Threat Exposure Management (CTEM)

A Zero Trust Approach

Zero trust security is a security framework that, at an organisational level, requires all users to be authenticated, authorised, and validated throughout their session within your IT systems — without doing so, they will not have access to any data.

This approach involves the assumption that there are attackers within and outside of the network, so no device or user should be inherently trusted. There are four core principles of Zero Trust:

Least privilege access

Users and devices should only be granted the minimum level of access required to perform their functions.

Microsegmentation

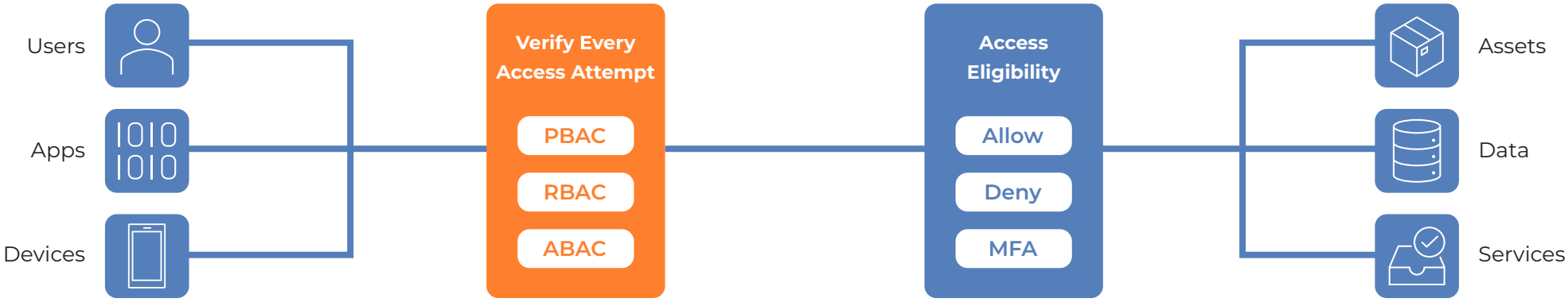
Dividing security perimeters into small, manageable segments allows for more granular control over traffic. This approach protects the entire network in the case of one segment being breached. It should be difficult, or impossible, for attackers to laterally move within a network.

Verification should be continuous

User identity should be verified not only upon login, but periodically during sessions.

Multi-factor Authentication (MFA)

No one factor of authentication is sufficient for access. MFA requires the combination of two or more independent credentials: something you know, something you have, and something you are (inherence).



Adopting a zero-trust strategy helps businesses limit the potential entry points or vulnerabilities that attackers could potentially exploit. It is particularly useful for preventing the spread of ransomware, where the damage of unauthorised entry into user accounts can be managed through limited access.

Continuous Threat Exposure Management (CTEM)

Continuous Threat Exposure Management (CTEM) is a proactive cybersecurity approach that focuses on continuously identifying, assessing, and mitigating vulnerabilities within an organisation's digital environment. It is a term that was coined by Gartner to describe a modern and flexible method for addressing security threats.

The overriding principle here is to address and solve threats, not individual attacks or episodes. It involves shifting the focus away from reactive measures to proactive ones, where continually monitoring your whole attack surface is key.

Gartner identifies five key steps to an effective CTEM strategy:

1. Scoping

Define and understand the boundaries of your digital environment, and map out potential entry points or vulnerabilities.

2. Discovery

Examine systems further to uncover misconfigurations, hidden assets or other risks. Discovery focuses on systems and applications rather than processes.

3. Prioritisation

Assess and rank vulnerabilities based on their potential impact, urgency and the likelihood of exploitation.

4. Validation

Test and confirm the effectiveness of the security measures already in place. If you wait until a real attack to see if a measure works, it may be too late.

5. Mobilisation

Equip and prepare your teams to respond quickly and effectively to threats. This also involves ensuring that all employees and stakeholders, not just IT staff, have the tools and training to identify and report threats.

You'll notice there is some overlap with a Zero Trust approach. Zero Trust Network Access (ZTNA) focuses on reducing the attack surface of your business, plugging common entry points for attackers. In particular, ZTNA's least privilege access and verification principles neatly complement CTEM's scoping, discovery and continual monitoring practices.

Key Focuses for 2024

What technologies and practices should you be focusing on in 2024? This section will explore effective security measures currently helping businesses mitigate the threats posed by the modern cybersecurity landscape.

Identity and Access Management

The principles of Identity and Access Management (IAM) are simple: ensure that only authorised individuals can access certain information and resources within an organisation. This technology is crucial for any security strategy, such as Zero Trust, where controlling what information and systems people have access to is paramount.

Intuitively, IAM is split into two functions:

Identity Management

Users' identities are checked upon the request to access the network using a username and password. This function is strengthened by authentication methods such as MFA to add another layer of identity validation.

Access Management

Once the identity of the individual seeking access is confirmed, access management controls the resources and systems they can access. This technology is particularly useful for implementing a least privilege access regime.

Cloud-based IAM platforms such as Microsoft Entra help ensure that all identity and access information is synced across all the devices and applications you use.

What attacks can IAM tools help prevent? IAM can mitigate the risk and damage of phishing attacks, as even if login credentials are stolen, access control using the principle of least privilege will limit the damage one compromised user can do. Strong access control can also avoid a privilege escalation attack where users gain elevated access rights beyond their legitimate permissions.

IAM solutions often include monitoring and detection mechanisms to identify and prevent credential-stuffing attacks. Network admins are alerted if an account's credentials are leaked in a data breach elsewhere, and can set strong password policies to avoid the use of insecure or recycled credentials.

EDR, XDR and MDR

Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), and Managed Detection and Response (MDR) represent a trio of advanced cybersecurity technologies to protect against a wide range of cyber threats.

Each offers a unique approach to detecting, analysing, and responding to incidents. Let's explore the differences:

Endpoint Detection and Response (EDR)

EDR focuses on securing endpoints - such as desktops, laptops, and mobile devices - from malicious activities.

These tools scan and record the activities of endpoints to give system administrators visibility into potential threats and incidents. The goal here is to detect threats before they infect the rest of your systems. EDR is a particularly useful defence for IoT malware attacks - especially given how difficult it is to use alternative detection methods such as anti-malware software on small IoT devices.

Managed Detection and Response (MDR)

MDR provides organisations with outsourced monitoring and management of security technologies, including EDR and XDR. It essentially involves leaving the endpoint and threat detection to cybersecurity experts.

These external security teams can remotely monitor your network and detect activity and traffic that could reveal a cyber threat. MDR ensures you're getting the most out of EDR and XDR capabilities.

Extended Detection and Response (XDR)

XDR extends beyond endpoints to collect and automatically correlate data across multiple security layers, including email, servers, cloud workloads, and networks. The goal here to provide complete visibility across all drives, systems and end-user devices.

Tools like Microsoft Defender XDR even use smart threat intelligence that can guide detection and reduce the need to chase false positives by categorising and confirming alerts.

EDR & XDR can use risk patterns to help uncover novel malware attacks. By continuously monitoring endpoints for suspicious activities, these tools can identify and mitigate previously unknown and novel malware variants. XDR can also be used to tackle crypto-jacking attacks by monitoring any abnormal use of system resources characteristic of this type of attack.

Backup and Disaster Recovery

Cyber attacks are often successful. Even the strongest prevention and mitigation measures aren't 100% impenetrable. Once an attack is in progress, a proactive disaster recovery plan will help limit an attack's damage to your organisation.

Firstly, your business must backup all critical files and information to protect against data loss. This can include everything from critical business documents to entire databases and application data.

The primary goal of backup is to ensure that copies of vital data are securely stored in multiple locations—be it on-premises, in the cloud, or a hybrid of both—so that they can be restored in case of data deletion, corruption, or loss.

Regular backups are the kryptonite of ransomware attacks. If your business can easily restore information from a backup, there will be no need to pay for a ransom for data to be unencrypted and returned to you.

Disaster Recovery, on the other hand, is a comprehensive strategy that encompasses not only data restoration but also the complete resumption of business operations after a disaster. Good DR ensures that the operational downtime associated with an attack is minimised.

What are the key components of a disaster recovery plan?

Recovery time objective (RTO)

The maximum acceptable length of time that your application, system, or network can be offline after a disaster. It helps businesses understand the tolerable downtime, and know what to expect before an attack occurs. It may also be useful for quantifying the “expected cost” of an attack for insurance or accounting purposes.

Recovery Point Objective (RPO)

The RPO refers to the maximum acceptable amount of data loss measured in time. It dictates the frequency of your backups - determining how much data you can afford to lose by defining the age of the files that must be recovered from backup storage for normal operations to resume.

Clear roles, responsibilities and communication lines

In the event of a disaster, it’s crucial for the team who is responsible for what, and how to report and communicate with each other during the incident.

Actions needed for a timely response

A Disaster Recovery plan should set out what actions and processes need to take place to ensure the resumption of business operations. What steps need to be taken to avoid further damage? How will a threat be removed from systems? What checks and validations need to take place before mission-critical processes resume?

Testing and optimisation

You should regularly test your disaster recovery response, being sure to document and address any gaps that you identify. Businesses have fire drills, so why not an IT disaster drill?

Some businesses turn to external providers to help guide their disaster response strategy.

Many cloud providers offer Disaster recovery as a service (DRaaS) - where backups of mission-critical systems are hosted in the cloud and the provider will implement your disaster recovery plan for you.

Other disaster response services include virtualisation, where virtual machines (VMs) are used to get mission-critical processes running, even if your physical systems remain offline, and cold siting, where operations can be moved to a secondary location in case of disaster.

Email Security

Email remains the primary vector for phishing attacks, accounting for 45% of all such incidents. Email also opens businesses to malware distribution, business email compromise (BEC), and other social engineering attacks.

These sorts of attacks are on the rise, with Acronis reporting a 222% surge in email attacks in 2023.

Email security refers to the measures and techniques employed to safeguard email accounts and communication from unauthorised access, loss, or compromise.

What measures are available to protect businesses from email-based attacks?

Spam Filters

These are designed to detect unwanted emails, preventing them from reaching the inbox. Advanced spam filters use machine learning to identify new threats and improve accuracy.

Anti-phishing Techniques

Tools and protocols like DMARC, SPF, and DKIM help authenticate the source of emails, reducing the risk of phishing and spoofing attacks.

Anti-malware and Virus Scanning

These tools scan incoming and outgoing emails for malicious content, including viruses, worms, and trojans, blocking their transmission and alerting users to potential threats.

Encryption

Email encryption ensures that the content of an email is unreadable to anyone other than the intended recipient. It prevents man-in-the-middle attacks where hackers intercept emails.

Another important aspect of email security is employee awareness training. Educating employees and stakeholders on how to spot phishing attacks, email security best practices and how to report suspicious behaviour can significantly improve your security posture.

The Human Firewall

Many cyber security strategies focus heavily on technical measures for mitigating and limiting attacks. But, the human factor is just as important.

The concept of the human firewall emphasises the role individuals play in an organisation's cybersecurity defence strategy. This is built on educating and empowering employees to recognise, resist, and report cyber threats.

What are some key components of human firewalling?

Comprehensive Cybersecurity Training

Regular, engaging training sessions are essential to equip employees with the knowledge to identify cyber attacks.

Simulated Cyber Attacks

Conducting simulated 'drills' helps reinforce learning and assess the readiness of employees to respond to real threats.

Clear Reporting Protocols

Employees should know whom to contact and how to report suspected cyber threats, ensuring swift action can be taken to mitigate potential damage.

Regular Updates and Communication

Keep teams informed about the latest cyber threats and security best practices.

In their 2023 whitepaper, Human firewalling, KPMG present a five-step methodology for reinforcing cyber security learning, the ADKAR Model:

Awareness
of the need for change

Desire
to participate in and support the change

Knowledge
of how to change

Ability
to implement required skills and behaviours

Reinforcement
to sustain the change

This framework can be applied to a wide range of cyber security awareness initiatives. For instance, if an emerging email threat becomes a concern, the ADKAR framework can be used to encourage a proactive response.

Firstly, awareness and knowledge of the threat can be achieved through regular communication through multiple channels. Presenting employees with the potential ramifications of an email-based attack can help resolve the desired axion. Knowledge and ability to respond can be addressed through simulated cyber attacks and interactive workshops. Finally, reinforcement can be achieved through personal feedback and acknowledgement of positive actions.

Human firewalling can be used to prevent almost any type of attack - as the vast majority of threats involve a human element. Furthermore, involving employees in an organisation's cyber defence can help foster a more collaborative security-first environment.

How to Get Started

The modern landscape of cyber threats puts all businesses at risk, regardless of size, sector and maturity. Recent advancements in AI technology have made it simple for criminals to carry out targeted and convincing attacks at scale.

Fortunately, the cyber security industry has developed a wide range of cutting-edge tools to keep up the pace. An effective security strategy must involve targeted investment into cyber security infrastructure, such as identity and access management, EDR/XDR/MDR and email security tools.

However, just as much focus should be put into measures to ensure that your business's practices, processes and people have cyber security at the heart of what you do.

Approaches such as Zero Trust Network Access and Continuous Threat Exposure Management provide an excellent roadmap, whilst following the practices in a modern framework such as NIST CSF 2.0 or the NCSC's Cyber Assessment Framework (CAF) can ensure you're following industry-standard best practices.

Ready to start developing your cyber security strategy? Our experts can help you scope out your business's potential weak points, develop a remedial plan to solve those vulnerabilities and ensure you're on the right track to futureproof your digital operations.

Get in touch today to see how we can help!

MATRIX 247

0345 3620 247 | **www.matrix247.com** | hello@matrix247.com