HORNETSECURITY

CYBERSECURITY REPORT 2025

An In-Depth Analysis of the Microsoft 365 Threat Landscape Based on Insights from

55.6 Billion Emails

hornetsecurity.com

HORNETSECURITY
CSR2025

ABOUT HORNETSECURITY

Hornetsecurity empowers companies and organizations of all sizes to focus on their core business by protecting M365 workloads, email communications, securing data, and ensuring business continuity and compliance with next-generation cloud-based solutions.

Our flagship product, 365 Total Protection, is the most comprehensive cloud security solution for Microsoft 365 on the market, including email security, compliance, governance, and backup.

WHAT IS THE CYBERSECURITY REPORT?

The Cybersecurity Report by Hornetsecurity is an annual analysis of the Microsoft 365 threat landscape based on real-world data collected and studied by Hornetsecurity's dedicated Security Lab team. Hornetsecurity's cybersecurity solutions process more than **4 and a half billion emails every month.** By analyzing the threats identified in these communications, combined with a detailed knowledge of the wider threat landscape, the Security Lab reveals major security trends, threat actor actions and can make informed projections for the future of Microsoft 365 security threats, enabling businesses to act accordingly. Those findings and data are contained within this report.

WHAT IS THE SECURITY LAB?

The Security Lab is a division of Hornetsecurity that conducts forensic analysis of current and critical security threats, specializing in email security in the Microsoft 365 ecosystem. Our multinational team of security specialists has extensive experience in security research, software engineering, and data science.

An in-depth understanding of the threat landscape established through hands-on examination of real-world phishing attacks, malware, ransomware gangs and more, is critical to developing effective countermeasures. The detailed insights uncovered by the Security Lab serve as the foundation for Hornetsecurity's next-gen cybersecurity solutions.

TABLE OF CONTENTS

CYBERSECURITY REPORT 2025

CHAPTER 1
EXECUTIVE SUMMARY

CHAPTER 1 – EXECUTIVE SUMMARY

By leveraging its huge user dataset, Hornetsecurity is uniquely positioned to conduct a detailed examination of email-based threats as well as those threats targeting the greater Microsoft 365 ecosystem. This allows the security researchers at Hornetsecurity to distill this data into important insights for IT teams and security professionals. Email continues to be a major communication channel, particularly for companies and professional organizations. In our analysis of more than 55.6 billion emails in 2024, 36.9% are categorized as "unwanted." 97.8% of unwanted emails are spam or rejected outright due to external indicators and 2.3% of unwanted emails were flagged as malicious.

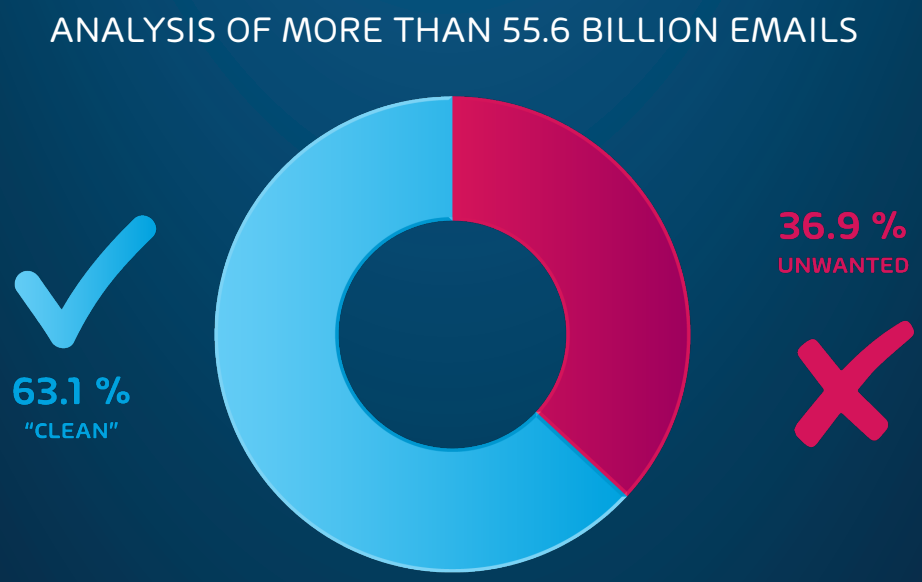


FIG 1. CLASSIFICATION OF EMAILS SCANNED BY HORNETSECURITY

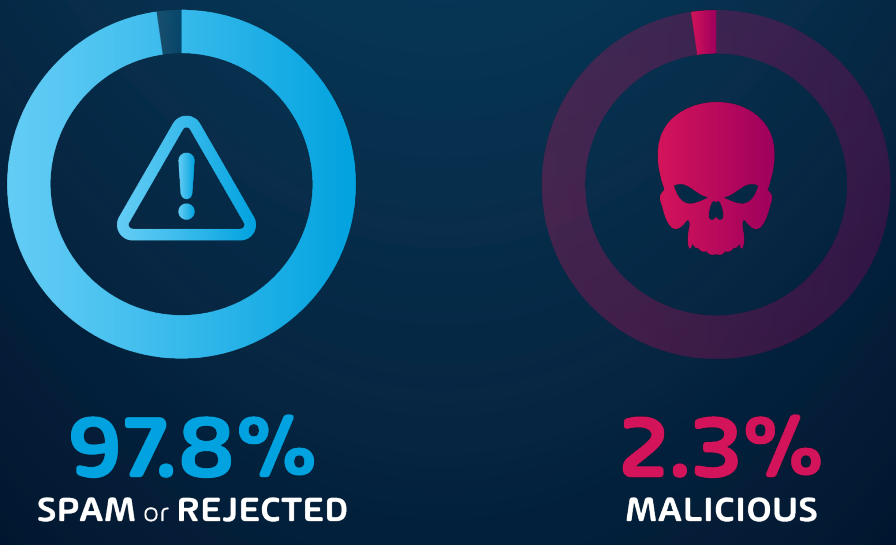


FIG 2. CLASSIFICATION OF UNWANTED EMAILS

"PHISHING: 33.3% OF ATTACKS"

When we look at the attack types used in email attacks, phishing retains its top place as the most prevalent attack method, accounting for 33.3% of attacks. This is followed closely by malicious URLs accounting for 22.7% of cases. These numbers align with the types of attacks that have gained popularity amongst threat actors over the past year - mainly in reverse-proxy style credential theft attacks that heavily leverage social engineering and malicious links.

A renewed focus on social engineering and security token / credential theft is noticeable in our data regarding malicious file types as well. We track the types of files used for the delivery of malicious payloads in email attacks and found that there are noted decreases in the use of malicious attachments period. Nearly every malicious file type saw a decrease when compared with last year. That said, HTML files, PDFs, and Archive files remain in the top three spots in a continuation from the previous year.

Threat actors have been leveraging a slightly higher volume of easier to detect (and ultimately "rejected") email attacks over the data period. This is indicated by the slight decrease in the number of malicious emails that were classified as "Threats" and "AdvThreats". As a result, we saw the threat index for nearly every industry drop during the data period. This is because our industry threat index compares the number of clean emails vs. the volume of "Threats" and "AdvThreats". Also notable is the fact that there is little variation from industry to industry. Yes, there are some that are higher than others, but the data continues to show, year after year, that EVERY industry is under attack.

In terms of brand impersonations over the last year, we found that despite remaining in the position of number 1 most impersonated brand there was a large decrease in the amount of DHL impersonation attempts.

That said, the amount of FedEx impersonation attempts tripled, Docusign and Facebook both had more than double the amount of impersonation attempts, while Mastercard and Netflix both saw notable increases as well.

Finally, when we continue our annual discussion regarding the safety of data in the cloud, a key theme that we've seen from attackers this year is, again, the increasing use of credential / token theft toolkits via an Adversary-in-the-Middle attack. When compared with previous years, these attacks have become popular with threat actors. This is because of the ease with which they can target a large number of victims with VERY convincing landing pages with minimal effort.

These toolkits are designed to account for MFA (Multi-Factor) authentication as well, which many organizations assume (wrongly) keeps them 100% safe from said attacks. The cybersecurity industry continues to address this concern with better scanning mechanisms, security awareness training, and phishing-resistant login technologies like passkeys. However, these mitigations take time of course, and as a result, some organizations have fallen victim leading to a loss or leakage of sensitive data.

As this style of attack still makes heavy use of email communications as well as increasing use of chat communications like Microsoft Teams, a robust email and Microsoft 365 security strategy is essential for operating safely in today's digital ecosystem.

CYBERSECURITY
REPORT 2025

CHAPTER 2

THE CURRENT MICROSOFT 365 THREAT LANDSCAPE

CHAPTER 2 – THE CURRENT MICROSOFT 365 THREAT LANDSCAPE

On an annual basis, Hornetsecurity's dedicated Security Lab reviews the company's extensive data set and analyzes the state of global email threats and communication statistics. Additionally, the team regularly conducts forward-thinking exercises and provides insight into potential future threats. This chapter focuses on reviewing the data from November 1st, 2023, to October 31st, 2024, which forms the basis for projections of the changing threat landscape laid out in Chapter 4.

EMAIL SECURITY TRENDS

Despite increasing usage of collaboration and instant messaging software, such as Microsoft Teams, email continues to be a top area of concern in terms of cyberattacks. We've observed a continued decrease in the number of emails categorized as Threats/AdvThreats - 2.3% this year, compared to 3.7% from last year, and 5.5% the year before that (When looking at "Unwanted" emails). That said, the risk to businesses around the globe remains high. This is primarily due to increased use in social engineering techniques via low-effort spray-style email attacks that seek to get the target user to engage somehow.

By reviewing more than 55.6 billion emails collected over the current reporting period (November 1st, 2023 - October 31st, 2024), the Security Lab has made the following determinations:

SPAM, MALWARE, ADVANCED THREAT METRICS

As we've seen over the last decade, email continues to be one of the primary methods that threat actors use to launch attacks. Our data from this report's data period classifies 36.9% of all emails as "Unwanted" - a 0.6 percentage point increase from 2023. The definition of "unwanted" refers to emails that are not genuine communications desired by the recipient. The chart below shows our breakdown of unwanted emails along with clean emails.

This contrasts with last year's reported number of 36.3% of all emails being categorized as "unwanted", showing a slight increase in unwanted emails year over year.

When you consider that we processed 55.6 billion emails in 2024, the number of unwanted emails accounts for roughly 20.5 billion "unwanted" emails sent to businesses over the reporting period.

FIG 3. 2024. UNWANTED EMAILS BY CATEGORY INCLUDING CLEAN

For a concise breakdown of percentages that make up "unwanted" emails, we classified them as follows:

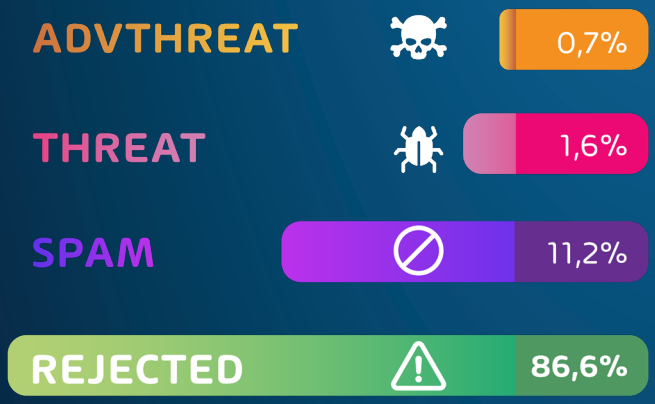


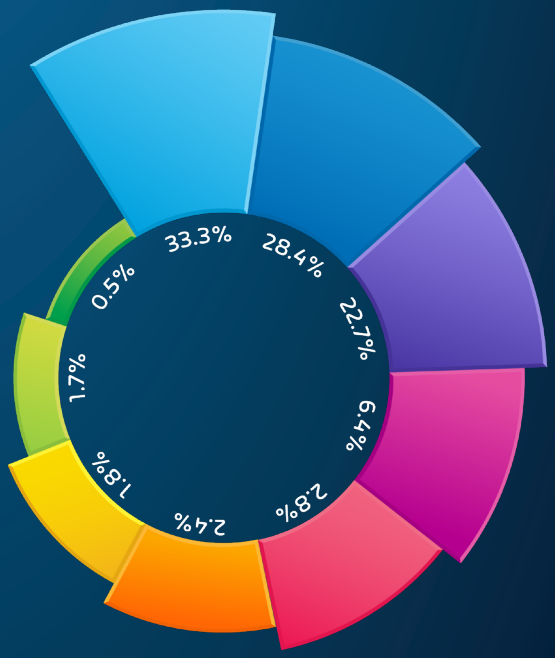
FIG 4. 2024. UNWANTED EMAILS BY CATEGORY

CATEGORY	DESCRIPTION
Spam	These emails are unwanted and are often promotional or fraudulent. The emails are sent simultaneously to a large number of recipients.
Threat	These emails contain harmful content, such as malicious attachments or links, or they are sent to commit crimes like phishing.
AdvThreat	Advanced Threat Protection has detected a threat in these emails. The emails are used for illegal purposes and involve sophisticated technical means that can only be fended off using advanced dynamic procedures.
Rejected	Our email server rejects these emails directly during the initial connection from the sending email server because of external characteristics, such as the sender's identity, and the emails are not analyzed further.

NOTE: To provide a little more detail, the "Rejected" category refers to mail that Hornetsecurity services rejected during the SMTP dialog because of external characteristics, such as the sender's identity or IP address. If a sender is already identified as compromised, the system does not proceed with further analysis. The SMTP server denies the email transfer right at the initial point of connection based on the negative reputation of the IP and the sender's identity.

ATTACK TECHNIQUES USED IN EMAIL ATTACKS IN 2024

In our data analysis of emails from the data period we observed the below breakdown of attack types used in email attacks:



ATTACK TECHNIQUE	
PHISHING	33.3%
"OTHER"	28.4%
URL	22.7%
ADVANCED-FEE SCAM	6.4%
EXTORTION	2.8%
.EXE IN DISK IMAGE / ARCHIVE	2.4%
IMPERSONATION	1.8%
HTML	1.7%
MALDOC	0.5%

FIG 5. ATTACK TECHNIQUES USED IN EMAIL ATTACKS 2024

NOTE: In previous years we've been able to track the change in occurrence of attack types from year to year. However, due to changes in how we identify malicious items and unwanted emails, there is a subset of occurrences that are marked as "Other". This category includes various attack methods that do not neatly fit into one of the main categories we've displayed in previous years. While we can provide a breakdown of attack types for this data period, comparing this data directly to last year would not yield an accurate representation.

What our data does show us for this data period is that phishing remains the number one attack type used in email-based attacks, followed by malicious URLs. The growing popularity of malicious URLs among attackers is largely driven by their use in reverse-proxy credential harvesting attacks, leveraging tools like Evilginx.

Outside of that, Advanced-Fee scams are still quite popular amongst threat-actors followed by extortion in 4th place. Extortion is notable as we continue to see cases where threat-actors will first exfiltrate data prior to putting ransomware in place within a given environment. Should the target refuse to pay (due to recovering from backup) the threat actor will threaten to release the data to the public.

ATTACHMENT USE AND TYPES IN ATTACKS

Email attachments continue to be used by threat actors for the delivery of malicious payloads in 2024. Threat actors use attachments to hide malware as well as add an air of authenticity to their malicious communications, depending on the attached file type in use. Additionally, some rudimentary spam/malware filters may be unable to scan certain file types leading to infection by more complex attacks such as **HTML smuggling**. In fact, the use of malicious HTML files remains in the number one spot for most used file types used in malicious emails, as shown below.

The breakdown of the file-types used for delivery of malicious payloads over the data period is shown below:

FILE TYPE	2023	2024
HTML	37.5%	20.4%
PDF	22.8%	19.2%
ARCHIVE	19.4%	17.6%
EXECUTABLE	3.5%	3.2%
EXCEL	3.2%	3.0%
WORD	3.0%	2.5%
DISK IMAGE FILES	2.2%	2.2%

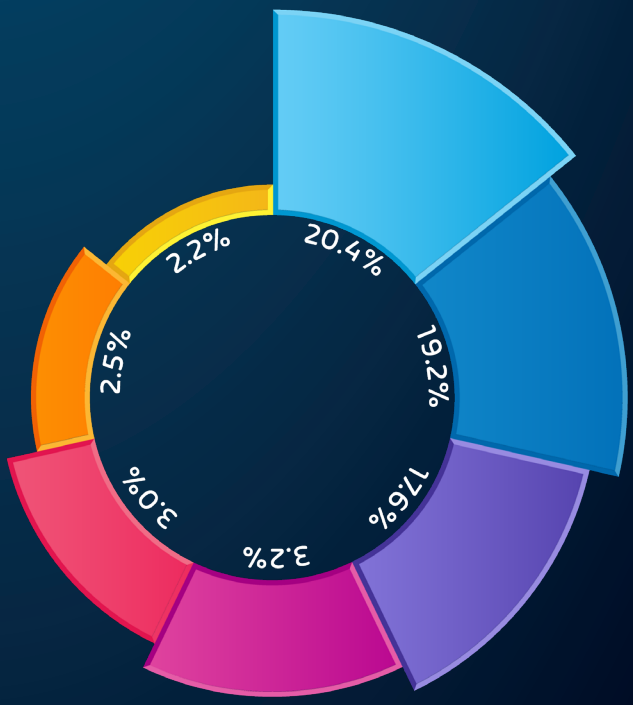


FIG 6. FILE-TYPES FOR MALICIOUS PAYLOADS IN 2024

> 17.1% DROP IN THE USE OF **HTML FILES** IN 2024 COMPARED TO 2023

- **PDF file** usage saw a 3.6% point decrease in 2024
- **Archive files** saw a similar trend in a percentage point decrease of 1.8 in 2024
- We observed a near universal decrease in **all malicious file types** as attackers pivot to other attack styles

Over the past year, the use of malicious attachments has not been as useful for threat actors as it has in the past. As such we've seen a trend where attackers are pivoting to more social engineering with the goal of getting the target to take an action other than open an attachment. For example, the use of reverse-proxy adversary-in-the-middle toolkits has seen much use during the data period. This is due to the fact that with increasing adoption of Multi-Factor Authentication (MFA), attackers are leveraging token theft more frequently via tools like Evilginx and PyPhisher. It's easier to procure the authentication token as opposed to dealing with the headache of gaining access to the target's MFA method.

EMAIL THREAT INDEX FOR BUSINESS VERTICALS

One of the key areas we review on an annual (and monthly) basis, is the number of threats being levied at different industry verticals. This allows us to determine if there are dedicated campaigns or targeted attacks on specific industries. It also provides some insights that business leaders can use to help determine if they're at increased risk of attack or not.

Most notable in this year's data is the fact that EVERY industry vertical saw a decrease of the associated email threat index. This correlates with our data above showing the number of emails classified as "Threats" and "AdvThreats" decreasing when compared with last year.

That all said, there were some industries that were targeted slightly more than others.

- **Mining Industry** - Most mining organizations have the same types of problems and challenges as a manufacturing organization. They also commonly deal in precious metals, and this tends to make them a prime target for threat actors looking to use ransomware to extract money from the organization.
- **Entertainment Industry** - Organizations of this type typically fall into gambling, or tickets sales etc. These organizations have become a target due to the large amount of money involved. Look at the 2023 attack on MGM and Caesars Entertainment that we discuss in more detail below.
- **Manufacturing** - The manufacturing space has a history of being targeted frequently by threat actors. This typically comes down to threat actors going after intellectual property for profit and / or ransom and many see this sector as an easy target for **double-extortion** and production disruption due to the nature of their network security and also the fact that they often utilize a large number of insecure Internet of Things (IoT) devices and programmable logic controllers (PLCs).

The table below shows the threat index rating for major industry verticals.

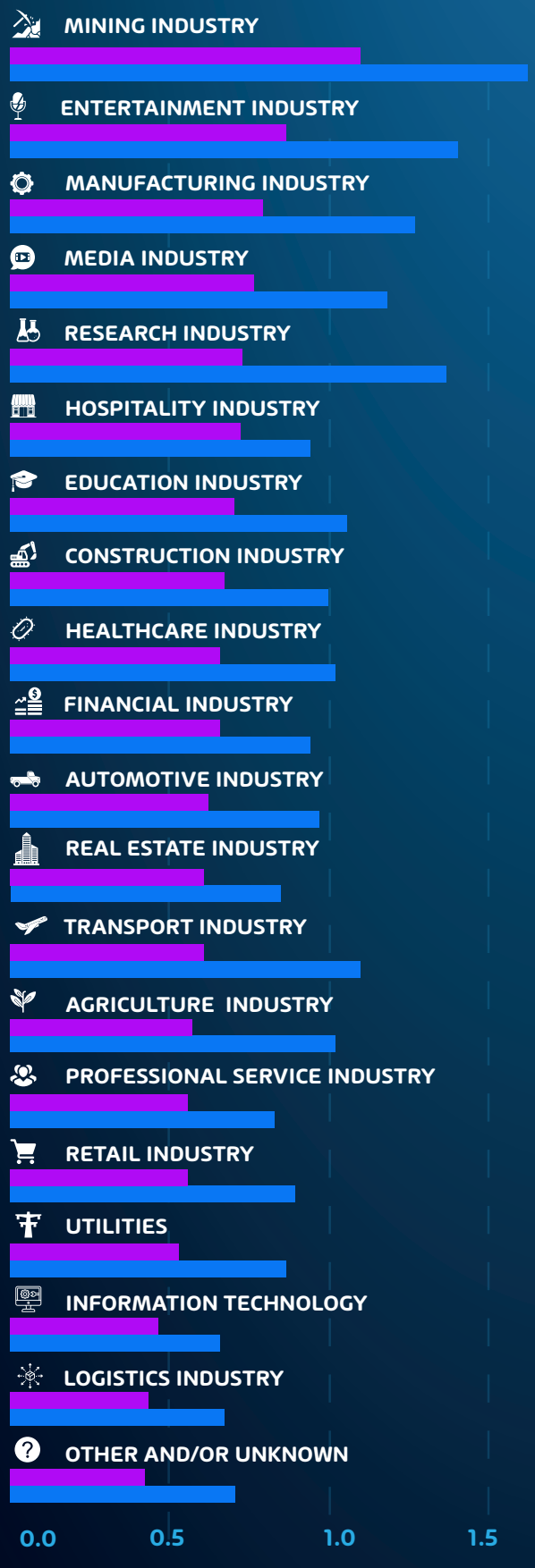


FIG 7. MEDIAN THREAT VS CLEAN EMAIL RADIO PER INDUSTRY

NOTE: The threat index value is determined by the following calculation:

Threat Index Percentage = number of malicious emails (Threat+AdvThreat) / (the number of malicious emails (Threat+AdvThreat) + the number of clean emails) multiplied by 100 – This excludes spam and info mail.

Note on methodology

Different (sized) organizations receive a different absolute number of emails. Thus, we calculate the percent share of threat emails from each organization's threat and clean emails to compare organizations. We then calculate the median of these percentage values for all organizations within the same industry to form the industry's final threat score.

BRAND IMPERSONATION

Brand impersonation continues to be a major email attack technique targeting end users and businesses in 2024.

The shipping company DHL has seen perhaps the most dramatic shift in brand impersonation attempts. The brand saw a mere fraction of impersonation attempts in 2024 vs. 2023. That said, it still remains in the number one spot on our most impersonated brands list, followed closely by FedEx.

Shipping brands continue to be popular due to the fact that they can be easily incorporated in social engineering style attacks via phishing and **smishing.** Both attack styles boast a high degree of similarity to real communications from these organizations and easily trick less trained users into giving away personal details and / or payment information.

Other notable data in this area:

- The amount of FedEx and Facebook brand impersonations has tripled in the past year
- The amount of Docusign brand impersonations has doubled over the data period
- Mastercard and Netflix are two other notable brands that have seen noted increases as well

Our full data over the reporting period has revealed most impersonated brands, as follows:

FIG 8. TOP 10 IMPERSONATED BRANDS

NOTE: Brand impersonation data is heavily affected by regional variation. Several German brands are listed here due to our large customer base in Germany.

Our analysis of 10,743,561 active mail-sending domains in 2024 reveals gaps in email authentication implementation, leaving many organizations vulnerable to brand impersonation attacks and email spoofing.

> **ONLY 35.4%**
> HAVE IMPLEMENTED DMARC

Only 35.4% of analyzed domains have implemented **DMARC** (Domain-based Message Authentication, Reporting, and Conformance) protocols, indicating that nearly two-thirds of domains lack this critical security measure. Just 16.6% of all domains utilize RUA (Aggregate Reporting URI) capabilities, which provides essential visibility into email authentication results.

RUA (Aggregate Reporting URI) records are a vital component of DMARC that enables domain owners to receive detailed reports about emails sent using their domain. These reports include:

- Volume of messages received
- IP addresses sending mail on behalf of the domain
- Authentication pass/fail rates
- Sending sources and their compliance with domain policies

Of the domains that have implemented **DMARC**, 47% are leveraging RUA capabilities, demonstrating that many organizations who adopt DMARC understand the value of monitoring and visibility.

Through RUA monitoring, organizations are able to observe surges in spoofed emails originating from previously unknown IPs, enabling them to alert their customers about the specific phishing campaign. Financial institutions often utilize RUA monitoring to initiate takedown procedures within hours of a phishing campaign's launch.

SAFETY OF DATA IN THE CLOUD

The "cloud" has been here for more than a decade now, but we've just started to see businesses either mass-migrating to cloud services or being established as 100% cloud-hosted businesses. Take the storage of business data for example. 10 years ago, most businesses still held some sort of on-premises file server that hosted the organization's critical data. Now it's becoming more common to leverage cloud storage for this. SharePoint Online and OneDrive for Business are increasingly becoming the place where data lives and is secured with services like Microsoft Entra. As such the safety of data in the cloud becomes an important discussion, not just in the M365 cloud, but for cloud services in general. While we'll focus on Microsoft 365 and the Microsoft cloud ecosystem throughout this report, much of what is discussed here applies to other cloud providers as well.

Baseline defenses in the Microsoft Cloud have improved over the years, but they are far from perfect. More organizations are making use of newer security features like Multi-Factor Authentication (MFA) and basic email security through services like Exchange Online Protection, but this is often still not enough. Attackers are always evolving and that can be seen clearly in the case of Adversary-in-the-Middle attacks.

Passkeys and Adversary in the Middle (AitM) Attacks

Where defenders go, attackers follow. For several years, we here at Hornetsecurity, as well as every other security minded person and company, has advocated for MFA as a more secure replacement for the traditional username + password dance for signing in to systems. There has been a slow and steady increase in the adoption of various forms of MFA, from SMS text messages to hardware security keys. However, it's not like the criminals are going to throw up their hands and give up their lucrative "business" and they have adapted instead.

Their main approach has been to use reverse-proxy-style phishing kits, either open source or "commercial" packages that both help with crafting convincing email lures to trick users into clicking a link, and also sets up proxy services with legitimate looking sign in pages.

When a user clicks the link and is taken to a fake login page to enter their username and password, these credentials are then passed onto the real site (as well as captured by the attacker). When the MFA prompt is then raised, these reverse-proxy toolkits enable the end user to enter their MFA code or approve the prompt as usual and it too is passed onto the real sign in page behind the scenes. Meanwhile the attacker steals the token that the target identity service generated (Entra ID for example) and now the attacker can use it to sign in as the user, thus this method is called Attacker in the Middle (AitM).

To defeat these more sophisticated attacks, you need a phishing resistant MFA method. These methods are newer and not seeing huge adoption (yet) in the industry. Some examples include **Windows Hello for Business**, FIDO2 hardware USB keys and most recently **Passkeys**. These MFA methods lock the authentication to the legitimate site URL only, so even if the user is tricked into visiting a sign in page that looks legitimate, the technology itself refuses to work because it sees that the site address isn't matching.

The problem is that Windows Hello for Business requires specialized hardware (and only works for Windows), while FIDO2 hardware keys are costly which has limited their adoption. That said, a Passkey uses the same technologies as a FIDO2 key but relies on the security chip in your iPhone or Android phone instead, removing the need for extra hardware.

Here, again, adoption has been slow, but more and more services now support it, and if you're responsible for security at your organization, you should definitely start piloting it today. We predict that now that Microsoft's Entra ID, Google Workspace and AWS along with Facebook and many others support Passkeys, adoption will increase dramatically over the next 12 months.

Vendor Overdependence Concerns Deepen with Regards to Cloud Data Safety

Vendor Overdependence is the practice of placing many or nearly all core business processes and procedures into the hand of a vendor partner. The problem with the arrangement is if the vendor has issues of some sort (security related or otherwise), then the business suffers as a result.

We've talked at length about the potential vendor overdependence issue that some businesses could face with Microsoft extensively via our **Monthly Threat Reports** and **The Security Swarm Podcast.** Needless to say, it's an issue that persists and is likely to worsen as Microsoft continues to build market share in various areas.

That all said, there are some new concerns that have come to light over the past year to shine an even brighter light on this issue. In the ongoing series of successful breaches at Microsoft an **interesting article** surfaced in June 2024.

In summary, Andrew Harris, who was working at Microsoft at the time, identified a serious flaw in Active Directory Federation Services (AD FS) and tried desperately to get it fixed. His fears were downplayed and as the US federal government was about to sign a multi-billion-dollar deal with Microsoft for their cloud services, the issue was essentially swept under the rug. After he left Microsoft in 2020, the SolarWinds attack, probably the largest supply chain attack ever, was revealed - and while the focus was on SolarWinds and their compromised Orion product, Russian attackers spread through networks using the ADFS flaw after their initial foothold. This of course happened long before the **Cyber Safety Review Board (CSRB)** report mentioned further below, and long before the **Secure Future Initiative (SFI)** at Microsoft got started in earnest but time will tell if the "new" Microsoft will indeed put security above new features, something that's a challenge for every commercial company.

Again, organizations each need to make their own decision when it comes to the matter of vendor overdependence, but taking into account years of varying security concerns at multiple levels, and the fact of where Microsoft's responsibility ends with regards to your data, the choice becomes clear.

What is Microsoft Responsible for?

Many ask: "If Microsoft isn't taking care of my data and security, what are they really responsible for?" The current stance from Microsoft on this question has not altered in 2024. To fully understand, you must be familiar with Microsoft's Shared Responsibility Model.

The important bit is that the shared responsibility model states,

> "THE RESPONSIBILITY IS ALWAYS RETAINED BY THE CUSTOMER FOR:"

- Information and Data
- Devices (Mobiles and PC)
- Accounts and Identities

Essentially, the customer is responsible for securing and protecting their information and data. Microsoft is not. As organizations move to the cloud, they must keep this in mind when protection strategies are implemented.

Another point worth mentioning is something that we included in this report last year. It's still coming as a surprise to many existing M365 customers so it's worth mentioning in this annual report as well. Microsoft changed its long-time stance in 2023 on the use of backup applications with M365. At a Microsoft conference last year, **Microsoft announced Microsoft 365 Backup**. A service was shown to provide basic backup capabilities for M365. The important part of this announcement is not the service itself, but the change of Microsoft's long-time stance of "you don't need to backup data in M365". Many in the industry see this as being driven by one of two things:

1. **Microsoft has finally capitulated and now agrees that a focus on data retention alone is NOT enough in M365**
2. **Microsoft simply wants a piece of the M365 backup market now that they've seen there is a large market for such a service.**

Both options seem likely, with option 2 being bolstered by the fact that they have also released a backup API that vendors can use as well, for a fee. Regardless, the message is clearer than ever. Businesses **ARE** responsible for the protection of any data that they place within Microsoft Cloud services.

The Difficulties Posed by Multiple Tenants in the Microsoft Cloud

As Microsoft's core cloud services have been out for a decade or more many organizations are finding themselves in a place where they need to manage and maintain multiple Microsoft 365 environments. This could be a business that has conducted several mergers and acquisitions, or maybe you're a managed services provider (MSP) providing IT services across multiple customers. In both cases many of these organizations are realizing the difficulties around managing multiple M365 tenants.

When we talk about the man-power overhead associated with this increased management burden there can be direct ramification on the safety of data in the cloud. As an organization there have most likely been standards defined for security best practices and feature enablement within the M365 environments under management. Many administrators are finding that enforcing standards and limiting configuration drift / mistakes within multiple disparate M365 tenants is highly difficult. With the nature of cloud services, one misconfiguration can be the difference between a safe organization and a serious data breach.

Tenant Management is increasingly becoming more important for organizations looking to keep their M365 data safe. While Microsoft does provide a utility called Lighthouse, it has some limitations and many MSPs find it lacking in features and scale. Some software vendors have built solutions to address this management need for MSPs like **365 Multi-Tenant Manager for MSPs by Hornetsecurity**. Proper management and governance is becoming critically important in today's cloud-first world and leadership teams must be aware of the dangers these challenges pose on the safety of data in the cloud.

CYBERSECURITY
REPORT 2025

CHAPTER 3
AN ANALYSIS OF THE MAJOR SECURITY INCIDENTS AND CYBERSECURITY NEWS OF 2024

CHAPTER 3 – AN ANALYSIS OF THE MAJOR SECURITY INCIDENTS AND CYBERSECURITY NEWS OF 2024

The last 12 months have been a rollercoaster when it comes to cyber events worldwide. If we covered all of the (big) ones this report would be twice as long, so we'll focus on the most important ones, either based on their impact on society, or where they give us a good insight that we can all use to improve the cybersecurity posture of our organizations.

THE CROWDSTRIKE INCIDENT

On 19 July 2024 arguably the largest IT outage ever occured. Within a few minutes approximately 8.5 million Windows systems that were running the Crowdstrike Falcon agent globally crashed / bluescreened and continued to restart and then crash, until manually repaired. This Endpoint Detection and Response (EDR) tool relies (like all of them do on Windows) on a kernel driver and a particular signature update had a logical flaw in it which crashed the system after writing data to a portion of the memory it wasn't supposed to. The estimated cost for the Fortune 500 companies affected is over 5.4 billion USD.

In September, Microsoft held a summit for all the cybersecurity vendors that produce agents for Windows to discuss the way forward and ensure that an outage like this never happens again. Many have suggested that Microsoft should adopt the macOS approach, allow no EDR agents Kernel access and only provide API access. Many experts, including us here at Hornetsecurity think this is too drastic, plus it also stifles innovation, and Microsoft seems to agree. It looks like future versions of Windows will have more guardrails in place against these types of risks, while not blocking kernel access altogether.

CHANGE HEALTHCARE

In February 2024, Change Healthcare, a subsidiary of UnitedHealth, experienced a massive **ransomware attack** that compromised the personal, financial, and healthcare records of ~100 million Americans. This breach, has been attributed to the **Russia-based BlackCat ransomware gang** and is considered the largest ever known data breach of protected health information in the US. The attackers exploited vulnerabilities in the company's network, gaining access to sensitive data, including patient medical histories, insurance details, and payment information. The breach not only exposed the inadequacies in Change Healthcare's cybersecurity defenses but also underscored the broader vulnerabilities within the US healthcare sector.

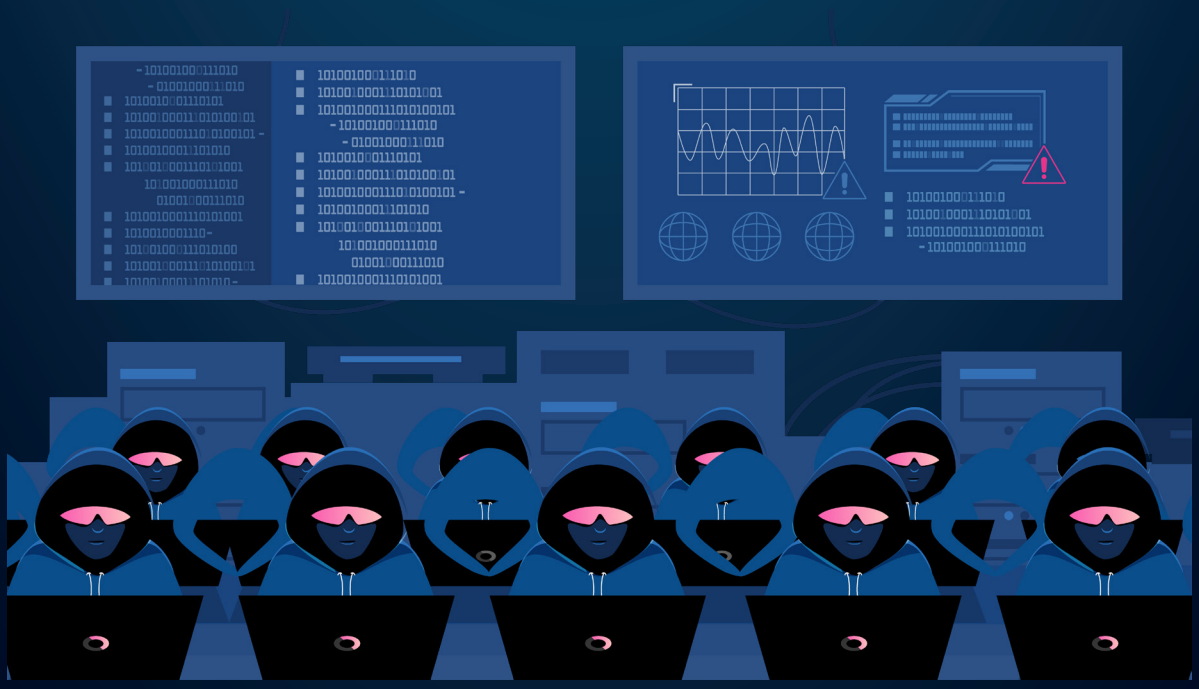
The aftermath of the breach saw Change Healthcare scrambling to mitigate the damage and working closely with federal authorities to investigate the incident. The company faced significant backlash from both the public and regulatory bodies, leading to calls for stricter data protection regulations in the healthcare industry.

The other notable fact about this attack is that it's one of a growing number of cases where there is a very **REAL** human toll as a result of a cyber-attack. In this case there were patients in the US that were unable to get critical medications in a timely manner. Another example of an attack with a very real human cost is a similar breach of the **UK's NHS (National Health Service.)** These attacks show that attackers are increasingly callus in who they target and as a matter of fact may even pick healthcare targets to increase the likelihood of a big payout.

NATIONAL PUBLIC DATA

The **National Public Data (NPD) breach**, which occurred in early 2024, is one of the largest data breaches in history, exposing up to 2.9 billion records. This breach affected approximately 170 million people across the US, UK, and Canada. The compromised data included highly sensitive personal information such as full names, Social Security numbers, mailing addresses, email addresses, and phone numbers. The breach was discovered when a malicious actor gained access to the company's systems in December 2023 and leaked the data onto the dark web from April to the summer of 2024.

The risks associated with this breach are significant, as the exposed data can be exploited for various cybercrimes and fraudulent activities. Individuals affected by the breach face the usual increased risks of identity theft, unauthorized financial activities, and targeted phishing attacks. What is so notable about this trove of data is that threat actors are able to use it for cross-linking of individuals. This allows them to craft increasingly convincing social engineering attacks targeting future victims.



MGM AND CAESAR'S CASINO BREACH

This attack occurred late in October 2023 just as we were starting to put the finishing touches on last year's report. As such it was worth a mention here as the aftereffects DID fall into the data period for this report. What's more is the fact that this was one of the more impactful attacks of the last 12 months primarily due to the size of the organizations impacted.

In October 2023, MGM and Caesar's casinos and resorts were both hit by ransomware. MGM didn't pay the ransom, and they expect their recovery to cost 100 million USD, whereas Caesar's did pay, about 15 million USD. The lesson here isn't pay the ransom, it's about **how they got in in the first place**, with relentless social engineering against help desk staff, including offering bribes.

23ANDME DNA TESTING SERVICE BREACH

The large **breach at the 23andMe DNA testing service** was downplayed by the company for several months until in December 2023 it became clear that 6.9 million customers had their data stolen (but not leaked publicly), whereas 1 million customers with Jewish heritage had their data leaked on BreachForums, a now defunct popular hacking forum. MFA wasn't enforced but is now mandatory for all users and 23andMe is currently facing serious financial issues, partly due to the breach.

LOCKBIT'S LEADER UNMASKED

In February 2024, the leaders behind LockBit, once one of the largest ransomware criminal gangs **were themselves hacked, led by the British National Crime Agency**, and their leader identified as Dmitry Yuryevich Khorosev. This is part of an interesting trend where law enforcement can't extradite or arrest identified criminals because they're in Russia, or other countries where the authorities have no problem with harboring criminals (as long as they don't attack domestic targets) so doxing or revealing the identity of someone is a way to indirectly make their life difficult. After all, if other criminals know who you are, and where you live, they might come visit to get a share of your stash of crypto currency.

XZ UTILS BACKDOOR

The **XZ Utils backdoor** was an interesting saga, revealed in March 2024. Here fake personas built up a relationship with the maintainer of the XZ Utils Open-Source Software (OSS) package over several years. They assisted in code updates and writing documentation with the eventual goal of taking over as maintainers, and then injected a malicious payload where any Secure SHell (SSH) connection could be unlocked if you had the special key.

The poisoned package only made it into alpha / testing builds of various Linux distros and was found by Andres Freund (Microsoft) who noticed some weird CPU spikes when testing an open-source database package. Had it made it into mainstream Linux (and other systems relying on SSH) it could have had a huge impact. This attack hasn't been formally attributed, but most experts agree it was Russian spies.

The takeaway here is realizing that if you create in-house software which relies on OSS components (they nearly always do), you must take their security posture (and that of their building blocks too) into consideration as a risk.

A YEAR OF MICROSOFT SECURITY DRAMA

Microsoft hasn't had a good last few years when it comes to security, back in June 2023 the Chinese group (Storm-0558) compromised email inboxes in 22 organizations worldwide, including the US State Department (60,000 emails stolen). In January 2024 Midnight Blizzard (Russia) broke into corporate mailboxes at Microsoft themselves, using password guessing to access a test tenant, which had an OAuth application with access to the production environment. This was a follow up of the Midnight Blizzard attack in 2020 (SolarWinds), and the July 2021 hack where they stole information on a limited number of customers. Then in March 2024 they followed up with another attack, accessing some internal systems and source code repositories using authentication materials stolen in the January attack.

In April 2024, the Cyber Safety Review Board (CSRB) released its **third report**, this time focusing on the Chinese hack in 2023 mentioned above. The report was scathing in its assessment of why Microsoft was compromised, outlining a series of failures that led to the breach, and following up with 25 recommendations on improvements.

This report and the attacks have led Microsoft to adopt the Secure Future Initiative (SFI), originally looking more like a marketing flyer, but now Microsoft employees will all have their security impact measured yearly, and the new mantra from Satya Nadella is "put security first". We'll see how this pans out over the next year or two.

CYBERSECURITY
REPORT 2025

CHAPTER 4
FORECASTING THE THREAT LANDSCAPE IN 2025

CHAPTER 4 – FORECASTING THE THREAT LANDSCAPE IN 2025

DID WE GET LAST YEAR'S PREDICTIONS RIGHT?

Looking back on our various predictions in the 2024 previous edition of the Cybersecurity Report is an interesting exercise, foretelling the future is always challenging, but we definitely got some things right, and a few things didn't pan out as we expected.

$459 MILLION USD
RANSOMS PAID IN THE FIRST HALF OF 2024

There are more ransomware groups in 2024 than in 2023, and more posts on leak sites, indicating that ransomware is still going strong with more businesses being compromised than last year. The approximate amount of ransoms paid in 2023 was $1.1 billion USD, whereas the **statistics for the first half of 2024 is $459 million USD,** although the prediction was that 2024 will be a more "fruitful" year than 2023. This is in part due to larger payments for more severe breaches, with the largest known ransom ever being $75 million USD (by an unknown Fortune 50 company).

We expected MFA fatigue attacks and MFA bypass attacks to increase, and this has certainly been the case. The number and proliferation of both open source and "commercial" kits for both crafting the email lures and setting up the proxy services that pretend to be a real login site has exploded, in response to more widespread adoption of push notification MFA options. To combat this in your organization look for phishing resistant MFA, such as Windows Hello for Business, FIDO2 hardware keys or Passkeys, which uses a smartphone as a FIDO2 key, obviating the need for additional hardware purchases. These technologies are "locked" to the legitimate sign in page, thus even if the user is tricked into visiting a fake site, the sign in tech won't work, hence they're called phishing resistant. Our recommendations for password-less security in the 2024 Cybersecurity Report still stand today, with the one addition of Passkeys, which are also password-less, as well as being phishing resistant.

We saw some risks with the old Microsoft Teams client being built on the electron platform, fortunately it's now been replaced with the new Teams client which seems not to have as many vulnerabilities. Teams is still an attack vector for phishing lures, although since Microsoft changed the default options for accepting communications from external parties and displaying warnings when a new contact is trying to reach you, this hasn't exploded in popularity.

Spyware and malware on smartphones are ongoing issues with both **the EU** and **US taking steps** to contain the proliferation of vendors and their use in democratic societies as we predicted.

As we mentioned, attacks against Application Programming Interfaces (APIs) increased in 2024, compared to 2023 (various sources estimate between 20 – 29%). This is often a "hidden" attack vector, and thus popular with criminals, as the monitoring and alerting on APIs aren't as robust as for other systems. If your organization publishes APIs for your web applications publicly, make sure you have a robust security model for access, and monitor for malicious use, including DDOS attacks.

The task of managing Microsoft 365 tenants cybersecurity posture continues to be a challenge, as we predicted, although we do want to point to a new tool, currently in public preview which is available to all M365 tenants – **Exposure Management**. This gives you insight into your tenant's security configuration and posture, plus initiatives to focus on to improve in particular areas such as defending against BEC or ransomware.

Time-to-Exploit (the time between a vulnerability becoming publicly known and a working exploit for it being available) went from 63 days in 2018/2010, 32 days in 2021/2022, down to five days in 2023. While we haven't seen the statistics for 2024 yet, we have seen several successful attacks within days of a vulnerability disclosure. This is putting further strain on defenders as patching is a never-ending job, and you can't patch everything, everywhere all at once, and so will need prioritization, trying to make sure internet exposed devices are kept up to date.

We looked at IoT devices as a vector for attacks in enterprise networks and in the **first five months of 2024** they surged 107% compared to the same period in 2023.

While we have certainly seen some convincing deep fakes in 2024, even with the support of AI tools for generating images, audio and video, we haven't yet seen major breaches caused by them. We still expect that as these tools become easier to use and more capable, we'll see more attacks, and general disinformation campaigns relying on them.

THE SECURITY LAB'S PREDICTIONS

Every year, as part of this report, the **Security Lab** team at Hornetsecurity looks at the state of the industry, our data, attack trends, and more to make a series of predictions for the coming year. This serves to inform businesses what potential threats they may face in the coming year, along with how the industry may change. The following are the Security Lab predictions for 2025.

It should come as no surprise that many of our predictions in this report involve AI. While some of these predictions can easily be grouped together, others are more specific. We've broken out these predictions as needed throughout this section.

LLMs in Attacker's Hands

Last year we looked at the rise of ChatGPT and other Large Language Models (LLMs) and their impact on cybersecurity, both for attackers and defenders. The original fears of LLMs writing flawless malware code haven't materialized and arguably, the inclusion of AI chat interfaces and other automation into security solutions has been more successful in helping defenders.

We have seen some actual data on LLM usage by attackers from **Microsoft**, where Forest Blizzard, a Russian state sponsored threat actor used them for researching satellite and radar technologies, probably to support the Ukraine war, as well as assistance with scripting tasks, including file manipulation.

Emerald Sleet from North Korea on the other hand extensively uses phishing to lure their targets and used LLMs to understand known vulnerabilities as well as improve the language and tone in phishing messages. Finally Crimson Sandstorm (Iran, connected to the Islamic Revolutionary Guard Corps) used LLMs for social engineering assistance, troubleshooting errors and .NET development assistance. Notably nearly all these use cases could have been fulfilled using ordinary search engine queries which would not have enabled Microsoft to gather these insights, so arguably as an attacker you've failed in your operational security (OpSec) if you're using a public LLM to do your research.

Attacks on LLMs themselves continue to proliferate and MITRE has created **ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems)** to track the different types, in a similar way to the Enterprise **ATT&CK matrix**.

With all this in mind, we're likely to see AI / LLMs in the Cybersecurity discussions in the coming year for a number of reasons:

1. **AI will be increasingly used for reconnaissance and information gathering**
2. **AI will be used to help attackers understand the best time to launch attacks based on data provided**
3. **AI will continue to be used to improve nearly every attack vector for threat actors, including email, voice, social engineering...etc.**
4. **AI will increasingly be used to quickly identify easily exploited objects in weak infrastructure**
5. **AI-enabled tools will continue to evolve to assist defenders**

AI-Enabled Deepfakes Used for Spear-Phishing and to Influence the Public

The use of deepfake technology in spear-phishing attacks is a growing concern and we're likely to see this combination in 2025. Deepfakes can create highly realistic videos and audio recordings that mimic the appearance and voice of real individuals. This technology can be used to create convincing phishing messages that trick recipients into revealing sensitive information or performing actions that compromise security.

The rise of advanced deepfake technology will also pose a potential threat to public opinion and trust. Deepfakes can create highly realistic videos and audio recordings that are difficult to distinguish from genuine content. This technology has already been used to spread misinformation and will continue to see increased use by threat actors. This will ultimately lead to an erosion of trust in digital media.
We'll Start to See Noteworthy Attacks on LLM-Products

Large language models (LLMs) are becoming increasingly popular, but they're also vulnerable to various types of attacks themselves. These include injection attacks, data exfiltration, and jailbreaks, where malicious actors manipulate the input data to deceive the model or extract sensitive information. These vulnerabilities can compromise the integrity, security, and ultimately the trust of LLM-based systems.

With increased reliance on these systems, threat-actors (especially nation states) would love nothing more than to use a popular LLM to their advantage. Whether that's disinformation, the dissemination of malicious links or something else remains to be seen.

Legal Cases Will Arise Due to AI Use and Will Lead to Regulation

This has been discussed at length since ChatGPT first made waves in the market. The question of legalities, copyright, and ownership have underpinned AI generated content at nearly every stage of evolution. That said, we're likely reaching a point where we're going to see more frequent and impactful litigation as a result of the use of LLMs.

We're also likely to see some form of government regulation on the use of AI by major nation states as a result. This is likely to be centered around data privacy, especially in places like the EU, who is already leading the way with their AI **Act** . These new regulations will not only require attention on the side of LLM creators themselves, but also by organizations that are looking to use generative AI in their own organizations.

New Regulatory Frameworks and Challenges

Speaking of regulation, the introduction of new regulatory frameworks such as NIS2, DORA, CRA, and KRITIS (Germany only) will present significant challenges for organizations. These new frameworks aim to enhance cybersecurity and data protection and are sorely needed, but complying with them will be difficult and resource-intensive for many organizations. In addition to this, the place of compliance officer within many organizations will continue to evolve and become increasingly important.

On a side note, the number of organizations requiring a certain type of compliance adherence in order to conduct business with them will increase as well. Supply chain attacks are becoming more prevalent and damaging, and rather than explicitly trust partner organizations like the old days, many organizations are requiring that their customer and / or suppliers conform with some of the same regulatory frameworks that they themselves must as well.

Corruption of the Open Source Community

For many years free and open-source software (FOSS) was seen as something of an oasis in a perceived security poor software ecosystem. With the XZ Utils incident we discussed earlier in this report, along with several other high-profile security vulnerabilities, this sentiment is no longer the case. The XZ Utils situation saw a very determined threat actor try to take a very popular open-source package and attempt to use it to create a widespread supply chain attack. With that (near) level of success, attackers are likely to attempt something similar with other industry critical open-source packages. There has already been a **noted increase in the amount of malicious open source packages, and what has been recently been happening with the PyPi software repository** is likely only a taste of the things to come.

Continued Predictions for Quantum Computing

In past reports we've spoken about a threat that's not imminent but on the horizon; Quantum Computing. While we're still some years away from a cryptographically relevant quantum computer (CRQC), some experts estimate 2037, minus 5 to plus 20 years, and development is progressing rapidly. The day these computers arrive is known as Q-Day. And if your business is storing sensitive data in encrypted form today that you expect to still need access to in 10 years' time, you need to look at this now. That's because the NSA, and presumably their counterparts in other countries are capturing vast amounts of data that they can't decrypt today but may be able to in the future.

NIST in the US agrees and has **standardized three post-quantum encryption algorithms:**

- ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism)
- ML-DSA (Module-Lattice-Based Digital Signature Algorithm)
- SLH-DSA (Stateless Hash-Based Digital Signature Algorithm)

There's a fourth standard coming as well. The old kyber crystal inspired names were definitely nerdier. The new names indicate which area of cryptography they should be used in.

Microsoft is also taking this upcoming threat seriously through the **Quantum Safe Program** and recently **announced** that their open-source core cryptographic library **SymCrypt** which is used in Windows 10 & 11, Windows Server, Azure and Microsoft 365 now support ML-KEM with ML-DSA and SLH-DSA support coming soon.

The challenge with quantum computers is scaling them up, both the number of physical qubits (a CRQC will need many thousands) and the error correction required to produce a reliable logical qubit to program against. We still recommend that if your organization holds sensitive data, that you expect / have a regulatory requirement to keep for 10+ years, figure out how to re-encrypt it with a quantum safe algorithm, particularly now that the standards have beenratified.

Increased Adoption of "Memory Safe" Languages

Software has long been plagued by security issues that are the result of memory management issues. This includes things like buffer overflows and **use-after-free** errors. As a result, the industry has started to move towards "memory safe" languages like Rust and / or Swift. These languages have built-in protections against many common memory-related vulnerabilities, and it eases the burden on software developers when it comes to writing secure code.

With the increasing outlook of **pending regulation** on the software industry, developers are likely to increase adoption of these languages to not only make their software more secure but also prepare for the aforementioned regulations ahead of time.

HOW MUCH AT RISK WILL MY ORGANIZATION BE IN 2025?

Our answer to this question remains much the same as it was in previous years, if your organization is capable of paying a ransom or you hold some information of intellectual property that can be sold for a profit - you **ARE** a target. This is demonstrated by our data regarding the industry email threat index showing continued targeting by cyber criminals across all industry sectors. That said, if your organization handles sensitive data, is involved in the defense space or critical infrastructure, or holds highly valuable intellectual property, you are an even higher priority target.

WHAT ORGANIZATIONS SHOULD DO TO DEFEND THEMSELVES

Start with the Basics

There's a tendency for organizations to react to specific threats and acquire point security solutions for each area, and thus focus on technology solutions, rather than covering the basics of security hygiene first. The vast majority of businesses that are breached don't fall victim to an obscure zero-day exploit or an advanced hacking technique. Their defenses fail because they didn't implement strong authentication (MFA, preferably phish resistant hardware), allowed simple passwords, set up users as local administrators on their devices or didn't train users to be cautious when clicking links in emails. Not validating backups by testing restore procedures can lead to a very bad day when ransomware strikes, as can having a lax patching policy.

In other words, take care of basic security hygiene first, which includes technology and processes and people. Start with a Zero Trust mindset:

- **Verify each connection** – just because a device is managed, doesn't automatically make it safe, and just because a user is connecting from a known network doesn't mean it's not an attacker, utilizing stolen credentials.

- **Use least privilege** – only give users and workload identities the **permissions** they need to fulfil their role and perform regular reviews to make sure given permissions don't accumulate.

- **Assume breach** – build your defenses as strong as your budget allows, but also work through the possible scenarios when they fail. If an attacker compromises a user, how will you detect that? How can you limit the ability of an attacker to move laterally in your environment?

A fuller list is available in the Open Groups **ZT commandments**.

Culture Eats Strategy for Breakfast

To transform your organization into a cyber resilient business will take time, effort, and persistence. You cannot turn your business into a well defended cyber fortress without involving everyone and helping them see how it affects them, and why they must be part of the solution.

When it comes time to roll out MFA, make sure the C-suite leads by example, and that they (and the board) understand the reason for adding the extra friction for authentication. Part of this culture shift is understanding that cyber resiliency isn't the IT departments, or the security department's job. IT can't secure workloads they don't know about, and if the marketing department is rolling out a website and a SaaS lead tracking solution without involving IT and security, the risk that this introduces belongs with the marketing department. Every technology choice or process decision that defines how a business will run caries risk, and how that risk will be managed needs to be transparent to the business so that they can make good decisions.

And an important lesson for IT and security departments is speaking the right language – risk management. If you start talking about technical details, and how it works, you'll lose anyone else in the business, but if you translate technology and process changes into business risk (or business opportunity) language, everyone should be onboard.

And this cyber resilient business isn't static, just like other risks to business (geopolitical, economic, competitors), it's ever changing and the business needs to continuously learn and adapt. Recent examples include the way attackers are bypassing or defeating "weaker" forms of MFA, with Attacker in the Middle toolkits or MFA fatigue attacks. And social engineering is an ever-present risk – would your helpdesk have been more successful in defending your business than those of Caesar's or MGM's?

A Balanced Security Strategy

To navigate the challenges of today's security ecosystem, businesses must think about implementing a balanced approach to security – one that addresses advanced threats specific to their industry while ensuring foundational security measures are firmly in place.

Relying on a single security tool or solution is no longer sufficient. Organizations should implement a multi-layered strategy that protects against common attack vectors while addressing threats unique to their business sector. This strategy should include:

- **Next-Gen Spam/Malware detection with ATP** for behavioural analysis to protect against the continued barrage of email-based threats we see in this industry
- **End-User Security Awareness Training** to train end-users to spot social engineering attacks and spear-phishing attacks
- **Backup and recovery capabilities** for BOTH on-premises data and data that lives in cloud services such as M365 for recovery purposes should a ransomware attack get through
- **Compliance and governance** features that help protect against accidental data leakage and ensure that compliance controls are met.

Learning More

The methods mentioned here regarding how to keep your business safe are just the beginning. Amongst the risk management, the vendor assessments, and the training are ever changing regulations and security requirements. Not every organization can be an expert when it comes to security. Make sure that you're leveraging trusted vendors that enable you to not only keep your business safe but allow you to take advantage of their deep knowledge in cybersecurity. For example, maybe your security staff has deep knowledge regarding data loss prevention, but knowledge of advanced email attacks is lacking. By partnering with a trusted security vendor like Hornetsecurity you will be able to leverage the vendor's knowledge as well as your own. Collectively we can all work together to enhance security, so be sure to reach out to your security vendors to learn more and see how you can more closely work together.

HORNETSECURITY

CSR2025

365 TOTAL PROTECTION

NEXT-GEN MICROSOFT 365 SECURITY

BUSINESS

PLAN 1

- SPAM & MALWARE PROTECTION
- EMAIL ENCRYPTION
- EMAIL SIGNATURES & DISCLAIMERS

ENTERPRISE

PLAN 2

INCLUDES ALL BENEFITS OF PLAN 1

- ADVANCED THREAT PROTECTION
- EMAIL ARCHIVING
- EMAIL CONTINUITY

ENTERPRISE BACKUP

PLAN 3

INCLUDES ALL BENEFITS OF PLAN 1 + 2

- AUTOMATIC BACKUP OF M365 DATA
- GRANULAR RECOVERY WITH END USER SELF SERVICE
- UNLIMITED STORAGE IN ONE ALL-INCLUSIVE FEE

COMPLIANCE & AWARENESS

PLAN 4

INCLUDES ALL BENEFITS OF PLAN 1 + 2 + 3

- SECURITY AWARENESS
- PHISHING & ATTACK SIMULATION
- ESI® REPORTING
- PERMISSION MANAGEMENT
- PERMISSION ALERTS
- PERMISSION AUDIT
- DMARC REPORTING & MANAGEMENT
- ENHANCED EMAIL REPUTATION & DELIVERY
- EASY DNS MANAGEMENT & OPTIMISATION
- AI RECIPIENT VALIDATION
- COMMUNICATION PATTERN ANALYSIS
- SENSITIVE DATA CHECK

START YOUR FREE TRIAL

HORNETSECURITY
CSR2025

ABOUT THE AUTHORS

WRITTEN BY

Andy Syrewicze

Andy has over 20 years' experience in providing technology solutions across several industry verticals. He specializes in Infrastructure, Cloud, and the Microsoft 365 Suite.

Andy holds the Microsoft MVP award in Cloud and Datacenter Management and is one of few who is also a VMware Expert.

Paul Schnackenburg

Paul Schnackenburg started in IT when DOS and 286 processors were the cutting edge. He runs Expert IT Solutions, a small business IT consultancy on the Sunshine Coast, Australia. He also works as an IT teacher at a Microsoft IT Academy.

Paul is a well-respected technology author and active in the community, writing in-depth technical articles, focused on Hyper-V, System Center, private and hybrid cloud and Office 365 and Azure public cloud technologies.

He holds MCSE, MCSA, MCT certifications.

HORNETSECURITY
CSR2025

CHAPTER 5
RESOURCES

- https://attack.mitre.org/techniques/T1027/006/
- https://github.com/kgretzky/evilginx2
- https://www.techtarget.com/searchSecurity/definition/double-extortion-ransomware
- https://www.csoonline.com/article/569273/what-is-smishing-how-phishing-via-text-message-works.html
- https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/
- https://youtu.be/SScaV2PjFcg?si=Ivjyfnk7YmwUUnVh
- https://www.hornetsecurity.com/en/blog/category/threat-reports/
- https://www.youtube.com/watch?v=o3JFNaNES0Q&list=PLyKOQIbp_zWzsfkSUQ0F-Ved_0bZXts70W&index=13
- https://www.propublica.org/article/microsoft-solarwinds-golden-saml-data-breach-russian-hackers
- https://www.cisa.gov/resources-tools/groups/cyber-safety-review-board-csrb
- https://www.microsoft.com/en-us/trust-center/security/secure-future-initiative?msocki d=35a127b0490c698b23e234bd4819680d
- https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
- https://techcommunity.microsoft.com/t5/microsoft-syntex-blog/welcome-to-microsoft-inspire-2023-introducing-microsoft-365/ba-p/3874887
- https://www.hornetsecurity.com/us/services/365-multi-tenant-manager/
- https://techcrunch.com/2024/02/29/unitedhealth-change-healthcare-ransomware-alphv-black-cat-pharmacy-outages/
- https://en.wikipedia.org/wiki/2024_National_Public_Data_breach
- https://cybernews.com/security/mgm-caesars-ransomware-attack-timeline/
- https://www.theverge.com/2024/9/13/24243986/23andme-settlement-dna-data-breach-lawsuit
- https://www.nationalcrimeagency.gov.uk/news/lockbit-leader-unmasked-and-sanctioned
- https://en.wikipedia.org/wiki/XZ_Utils_backdoor
- https://www.cisa.gov/resources-tools/resources/CSRB-Review-Summer-2023-MEO-Intrusion
- https://www.bleepingcomputer.com/news/security/ransomware-rakes-in-record-breaking-450-million-in-first-half-of-2024/
- https://www.politico.eu/article/eu-commission-national-security-does-not-justify-spying-document/

- https://home.treasury.gov/news/press-releases/jy2581
- https://virtualizationreview.com/Articles/2024/03/25/exposure-management.aspx
- https://wca.org/security-attacks-on-iot-devices-surge-by-107-in-early-2024/
- https://atlas.mitre.org/matrices/ATLAS
- https://attack.mitre.org/matrices/enterprise/
- https://www.infosecurity-magazine.com/news/156-increase-in-oss-malicious/
- https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
- https://www.microsoft.com/en-us/security/blog/2023/11/01/starting-your-journey-to-become-quantum-safe
- https://techcommunity.microsoft.com/t5/security-compliance-and-identity/microsoft-s-quantum-resistant-cryptography-is-here/ba-p/4238780
- https://github.com/microsoft/SymCrypt
- https://en.wikipedia.org/wiki/Buffer_overflow
- https://en.wikipedia.org/wiki/Dangling_pointer
- https://securityboulevard.com/2024/10/eu-cra-good-intentions-impossible-requirements/
- https://pubs.opengroup.org/security/zero-trust-commandments/