TitanHQ™

Ransomware Guide for MSPs:

How to Protect Your Data,
Your Business, and Your Clients.

Ransomware Guide for MSPs:

Ransomware has, unfortunately, become a household name. The reasons for the infamy of ransomware are the insidious nature of the threat and the extensive damage it has done to brands like the Royal Mail in the UK and the Costa Rican government. Ransomware is an acute problem for businesses worldwide. This problem is unlikely to disappear as hackers reap the rewards from increased ransom amounts. Phishing remains the top vector for ransomware delivery, bolstered by increasingly evasive email tactics and as-a-service delivery. New technologies like Generative AI allow cybercriminals to de-skill, opening the playing field for entry into the murky world of ransomware attacks.

The number of ransomware victims in 2023 has already surpassed what was observed for 2021 and 2022. (DarkReading). In 2023, three-quarters of organizations were victims of a ransomware attack, and around one-quarter of data breaches were related to ransomware[1]. CyberSecurityVentures estimates the global cost of ransomware will spiral 30% year over year to $265 billion (USD) annually by 2031. The report also predicts attacks will happen every two seconds[2]. As the costs of ransomware infection spiral, companies must find ways to protect their people and assets.

This is where an MSP can help. An MSP model can deliver many measures to protect an organization from ransomware infection. In this short eBook, TitanHQ will show you the breadth, depth, and complex nature of modern ransomware threats. Importantly, this eBook will describe the top seven measures to protect your clients from the impact of a ransomware infection.

Key Takeaways on Ransomware

- Ransomware is a big money business.
- New methods like GenAI and as-a-service automation will allow ransomware attackers to de-skill, increasing ransomware further.
- Phishing remains a core initiator of a ransomware infection.
- Ransomware gangs may not just be after money; they may also want to change your business decisions.
- An MSP is uniquely positioned to mitigate ransomware threats using the proper measures.

Source 1

Source 2

Section One: The Deepening Threat of Ransomware Across the World

Ransomware is not a new type of threat. While attempts to use digital means to extort money can be traced back to 1989, the modern phenomenon only appeared after the invention of cryptocurrency. Bitcoin changed the ransomware stakes because it allowed money collection to be anonymized. Cryptolocker appeared in 2013 and made full use of Bitcoin. Crypolocker encrypted data and demanded a payment in Bitcoin for a decryption key. The scene was set to develop the type of ransomware we see today.

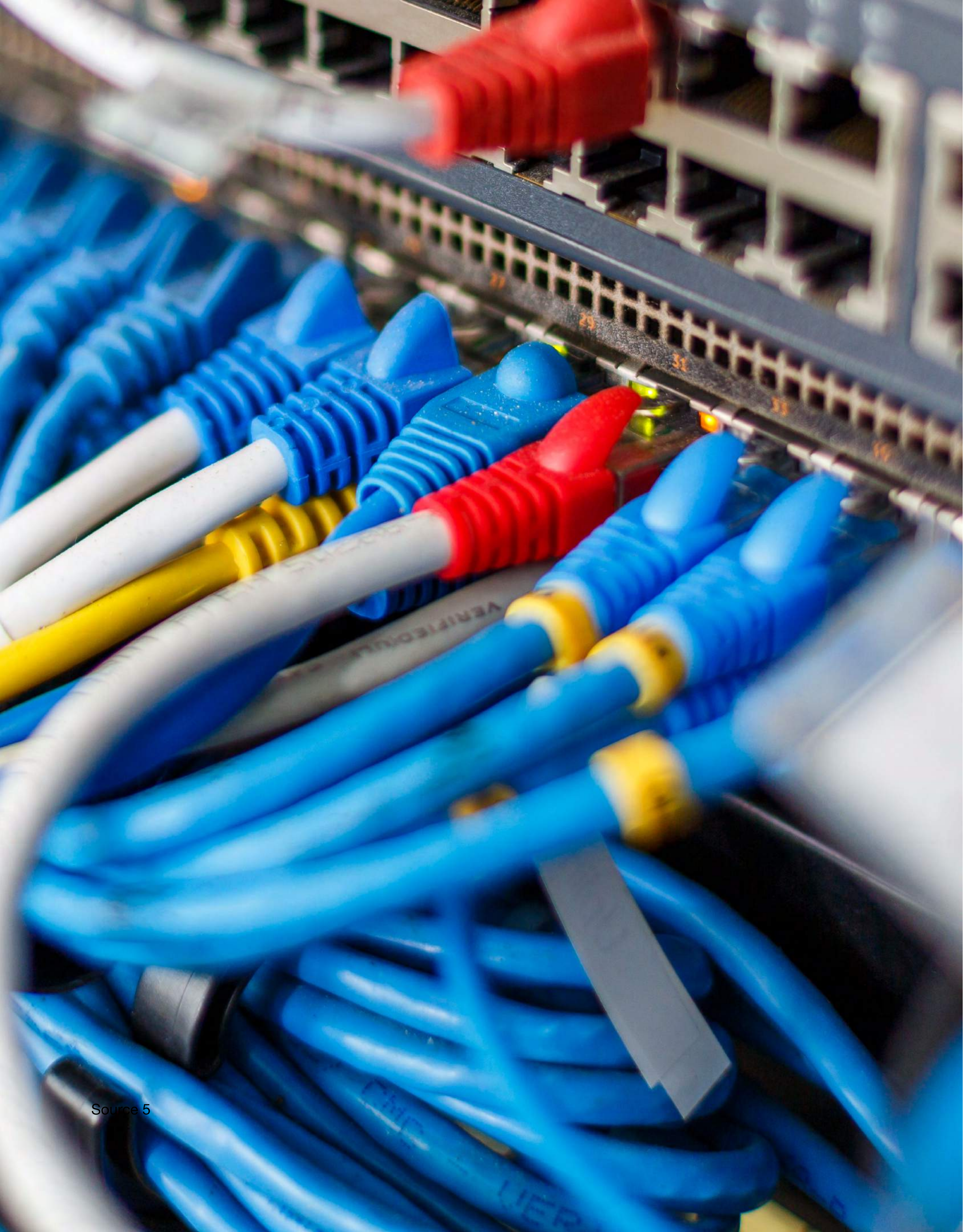
The WannaCry ransomware of 2017 has become synonymous with the type of ransomware we see today. Modern ransomware attacks have honed their craft. The cybercriminals behind these attacks are adept at manipulating human behavior. To fuel the fire, ransomware attacks are more likely to encrypt and exfiltrate the data beforehand. The stolen data is then used as leverage to obtain larger and larger ransoms. In late 2023, infotech company CDW reported that the LockBit ransomware infection came with a demand of $80 million. LockBit threatened to leak stolen CDW data unless the ransom was paid[3].

Ransomware hacking gangs are adept at complex chains of attacks. Hacking groups like the Lapsus$ Group and TA505 often use double or triple-whammy attacks[4]. The cyberattacks, usually initiated via phishing, will encrypt files, steal data, and perform account takeover. Some ransomware attacks result in stolen data being used to send out phishing emails to steal credentials and data and carry out further ransomware attacks.

The complex, multi-stage nature of modern ransomware threats has made ransomware such a successful tool for extortion. Some recent attacks that made the headlines show the damage done to companies and the connection with phishing.

Source 3

Source 4



Source 5

Recent Ransomware Attacks

Reddit: In February 2023, Reddit experienced a ransomware attack by the BlackCat ransomware gang. The attackers used spear phishing campaigns targeted at Reddit employees. The gang stole around 80GB of data and demanded a $4.5 million ransom. However, this was not enough for the attackers, who also demanded that Reddit roll back its latest API changes. This additional demand for control over a company's policies may become integral to a ransomware gang's demands.

Harvard Pilgrim Health Care (HPHC): was affected by a ransomware incident in April 2023 that compromised data servers. The attackers stole the sensitive data of over 2.5 million people. The company alerted customers to the potential of identity theft and phishing scams using the stolen data. HPHC is now being sued in several class actions under HIPAA violations.

Royal Mail: the UK's incumbent delivery service, The Royal Mail, was attacked by LockBit ransomware in January 2023. The attack impacted the company's international services. The hacking gang behind the attack demanded $80 million (£67 million) not to leak data stolen in the attack. While Royal Mail refused to pay the ransom, the costs of remediation and security measures after the attack are expected to be upwards of £10 million (approx. $13 million). The attack was likely initiated by spear-phishing emails from Royal Mail employees[5].

DragonForce: A recently emerged ransomware group disclosed 21 victims on its leak site last month, with a notable incident involving a major attack on the Ohio Lottery on Christmas Eve. During this assault, the group asserted to have encrypted devices and pilfered sensitive data exceeding 600GB, encompassing personal information of Ohio Lottery customers and staff.

Section Two: The Scope and Impact of Ransomware

The popularity of ransomware continues to challenge organizations with the specter of ransom and stolen data. However, it is essential to note that ransomware strategies change and evolve. One thing is sure: cybercriminals play a war of attrition with security vendors and security teams to ensure their tactics succeed.

Recently, ransomware attacks have focused on human-centered attack methods.

Social engineering and phishing are valued tactics, and if the stakes are high enough, i.e., a high ransom, leveraging payment using stolen data, or reselling sensitive or financial data, then additional work, such as intelligence gathering, is worth doing.

The cybercriminals behind ransomware attacks are also benefiting from pre-configured Ransomware-as-a-Service options. These rent-as-you-go ransomware kits allow even novice cybercriminals to get in on the ransomware act.

GenAI is also changing the metrics of ransomware activity. The UK’s National Cyber Security Centre (NCSC) has warned that the global ransomware threat will soar because of AI. The NCSC said in the warning: **“Most ransomware incidents typically result from cyber criminals exploiting poor cyber hygiene, rather than sophisticated attack techniques”**

> “Most ransomware incidents typically result from cyber criminals exploiting poor cyber hygiene, rather than sophisticated attack techniques”

Costs of a Ransomware Incident

According to research from Unit 42’s “2023 Ransomware and Extortion Threat Report,” the median ransomware demand was $650,000, but the median ransomware payment was $350,000[6].

The most considerable ransomware demand to date was $240 million in an attack against German electronics retailer MediaMarkt. The attack shut down IT systems and prevented store operations in the Netherlands and Germany. The ransom was negotiated down to $50m[7].

In 2022, the average downtime after a ransomware attack was 24 days, a 60% increase over the 15 days in 2020[8].

Ransomware Tactics

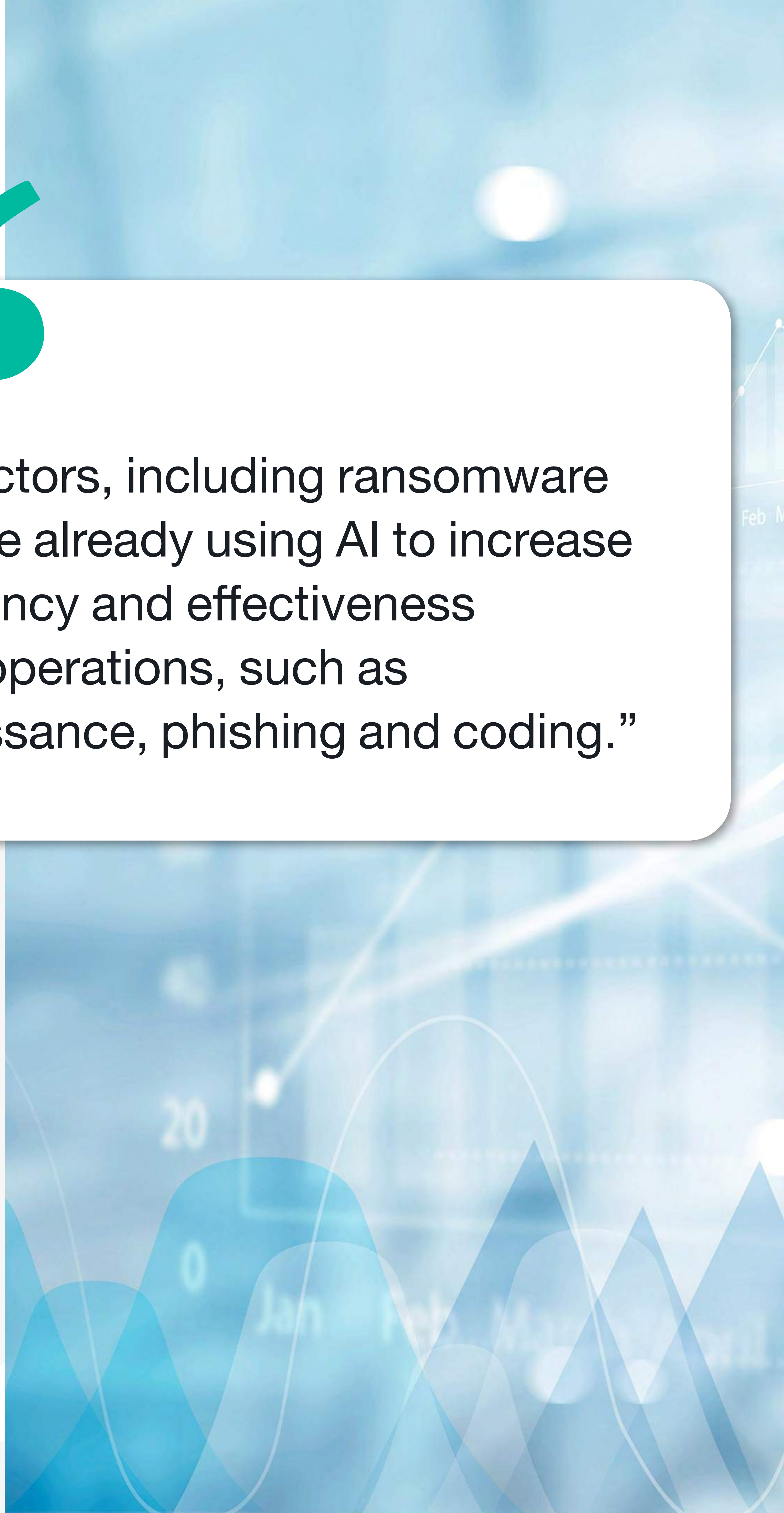
Tactics used by ransomware threat actors change as conditions in the landscape change. For example, ransomware actors will likely use GenAI to create even more believable phishing attacks. Also, the ransomware-as-service model may see increased attempts at ransomware attacks over the next few years as the bar to entry of a cybercriminal is lowered.

However, the following trends are being noted in the field of ransomware attacks:

AI-enabled ransomware attacks: An NCSC analysis of the use of AI in cyber-attacks shows that all aspects of a ransomware attack chain, such as Social engineering, phishing, passwords, and data exfiltration, will be uplifted by using AI[9]. The NCSC states that

“Threat actors, including ransomware actors, are already using AI to increase the efficiency and effectiveness of cyber operations, such as reconnaissance, phishing and coding.”

Zero-day exploits: unpatched computer systems are an ideal exploit for ransomware attacks that exploit flaws in software. Zero-days are, as such, unidentified defects and even patched systems cannot defend against ransomware that exploits zero-day threats.



“Threat actors, including ransomware actors, are already using AI to increase the efficiency and effectiveness of cyber operations, such as reconnaissance, phishing and coding.”

Source 5

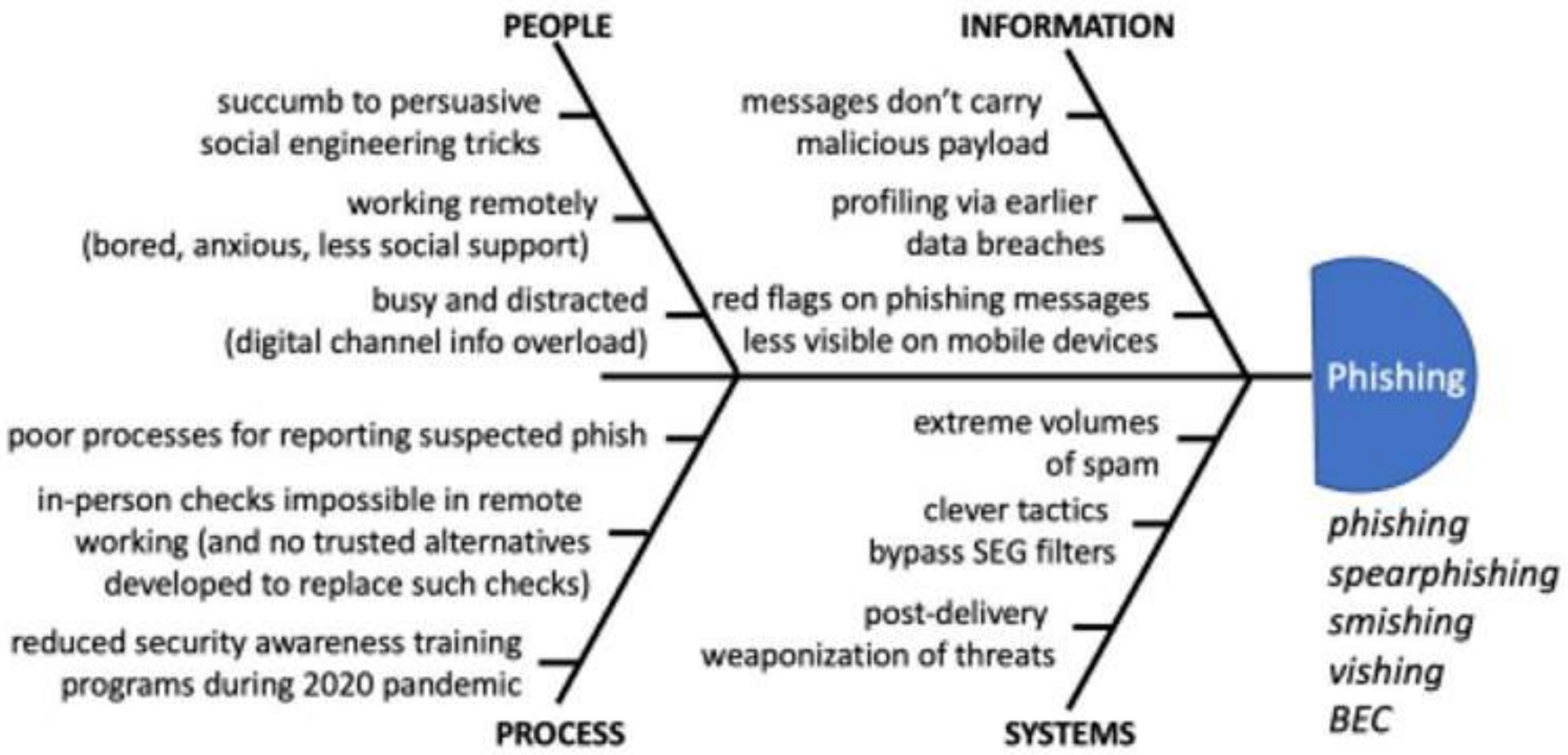
Source 6

Source 7

Source 8

Source 9

Sophisticated levels of phishing for ransomware: phishing continues to be the vector of choice in initiating a ransomware attack. Email phishing and the targeted version, spear phishing, are the most common methods of starting a ransomware attack. Often, the phishing exercise steals privileged login credentials and allows the attacker access to the network. Alternatively, ransomware can be delivered in an infected attachment in an email. Recent research from Osterman pinpoints the causes and contributors to phishing attacks. The most noticeable element of phishing and ransomware is that cybercriminals manipulate human behavior, work environment, and events to increase their chances of success. The phishing emails are also being adjusted to evade conventional secure email gateway filters.



PEOPLE

succumb to persuasive social engineering tricks

working remotely (bored, anxious, less social support)

busy and distracted (digital channel info overload)

INFORMATION

messages don't carry malicious payload

profiling via earlier data breaches

red flags on phishing messages less visible on mobile devices

PROCESS

poor processes for reporting suspected phish

in-person checks impossible in remote working (and no trusted alternatives developed to replace such checks)

reduced security awareness training programs during 2020 pandemic

SYSTEMS

extreme volumes of spam

clever tactics bypass SEG filters

post-delivery weaponization of threats

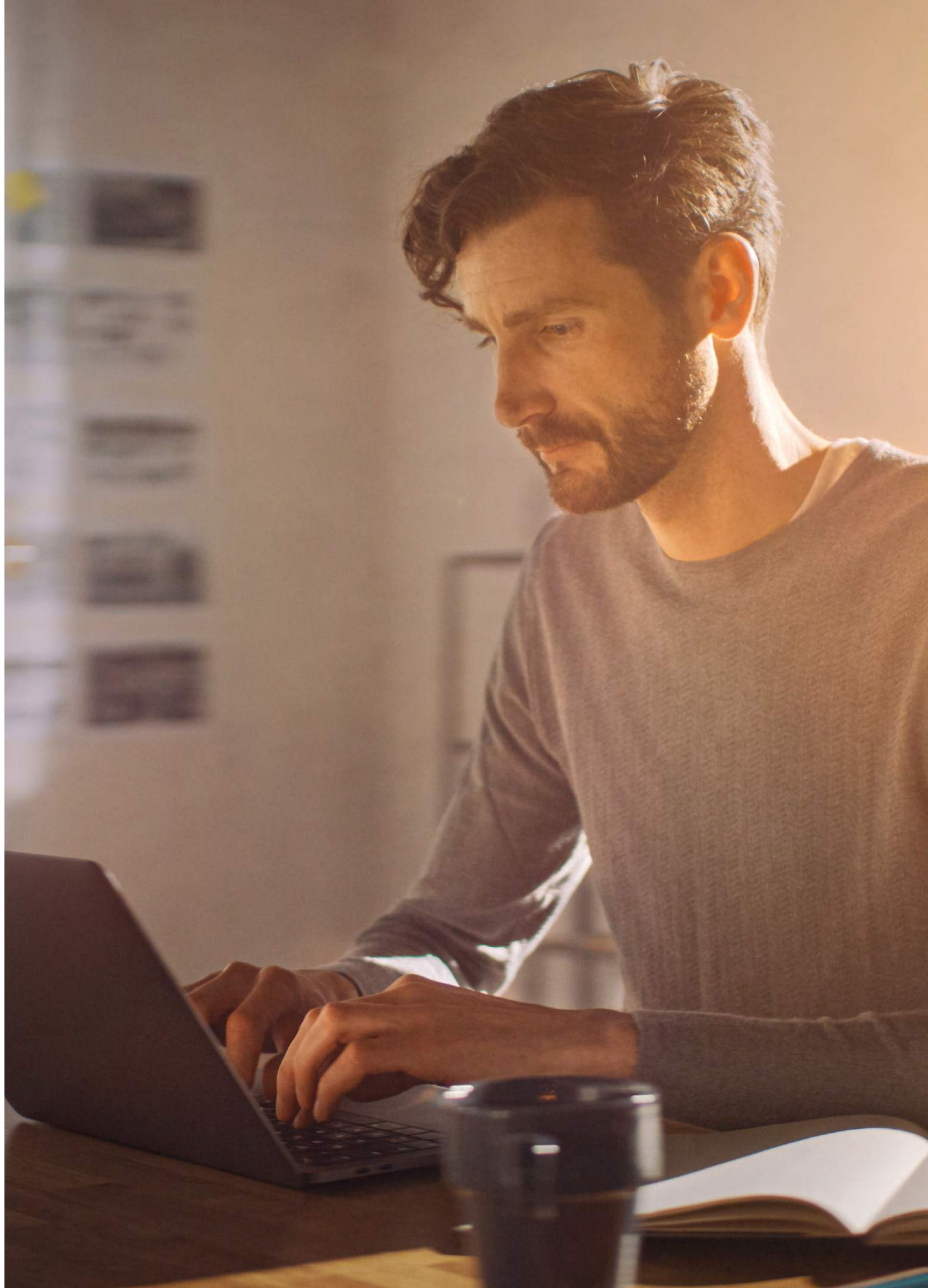
Phishing

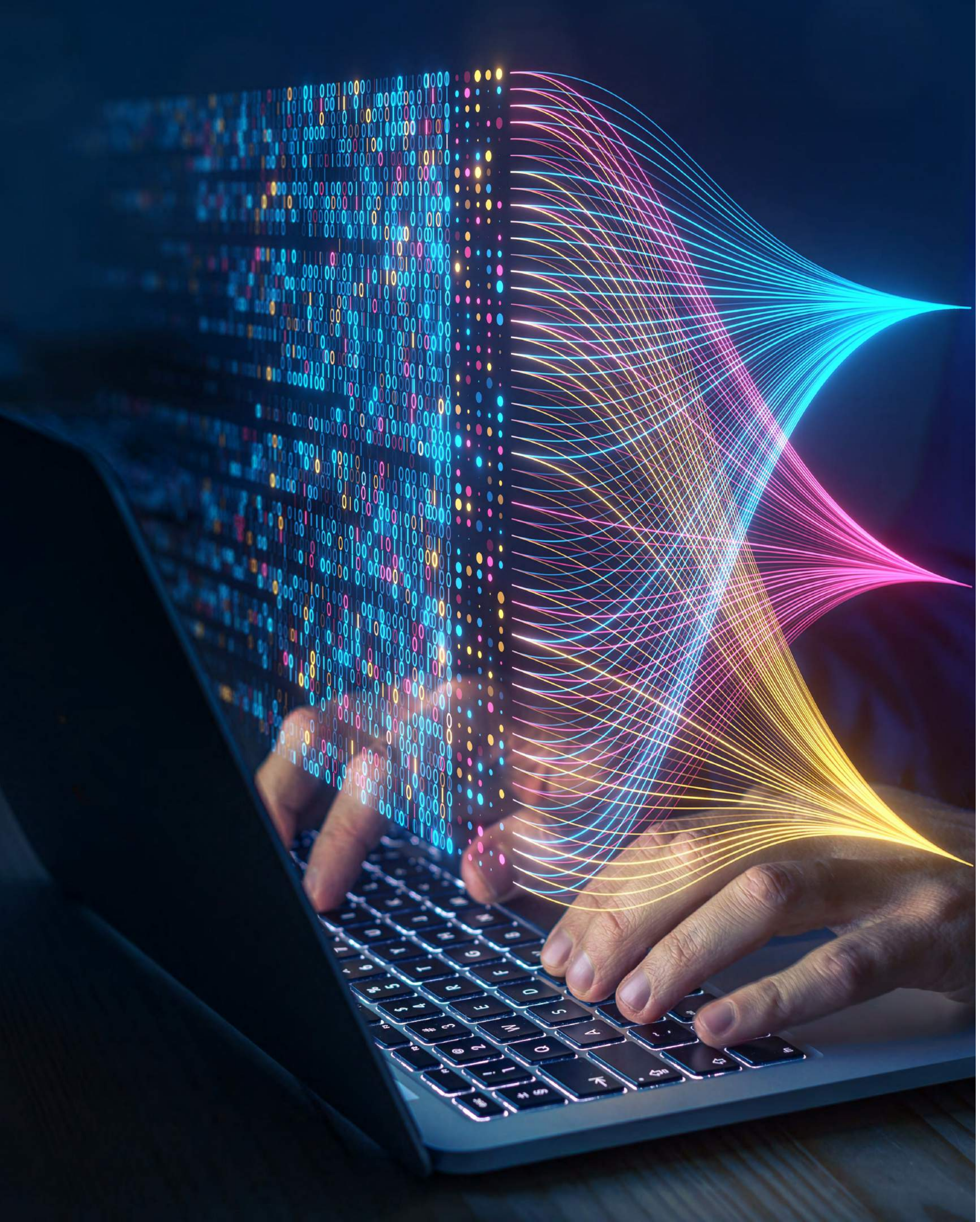
phishing
spearphishing
smishing
vishing
BEC

Source: Osterman Research

With phishing being a rich source of ransomware, this type of cyberattack must be classified as a form of human-centric attack. The term zero-minute phishing attacks has also been coined to describe the speed at which some phishing attacks occur[10].

Source10





Social Engineering: phishing is now a sophisticated exercise. Social engineering has created highly successful phishing variants. For example, Clone Phishing duplicates legitimate emails that the target recognizes and trusts. This lulls the target into downloading ransomware payloads or clicking malicious links that lead to ransomware infection. The mix of behavior manipulation, driven by social engineering, and evasive phishing has created a perfect storm, delivering damaging ransomware straight into the heart of the enterprise.

Phishing for Targets

Cybercriminals use intelligence and surveillance to determine their target. However, more conventional phishing methods are still a potential source of vulnerable victims. Two noted tactics used by ransomware attackers are:

Spray and Pay: the tactic known as ‘spray and pay’ is based on the mass mailout of spam emails. Depending on the campaign metrics gathered by the attackers, the phishers choose which network to target. Target choice can be taken from results associated with “sector, geolocation or perceived security posture.”

Big Game Hunting: a trend towards targeting large enterprises has been identified; the reason for choosing larger targets is to maximize the payout. Chain analysis expects a rise in ransomware due to Big Game Hunting, finding $449.1 million collected in ransoms in the first half of 2023.

Section Three: The Impact of Ransomware

Cybercriminals are ruthless and will stop at nothing to ensure a payout. Ransomware attacks have moved from the damaging impact of encrypted files and data to the additional theft of data by exfiltrating data before the ransomware event; don’t or won’t pay - expect your sensitive data to be up for sale on the dark web. And, of course, these are cyber criminals, so even if a company pays the ransom, the chances of the stolen data being deleted are slim to zero.

The recent Reddit ransomware attack demonstrates that some cyber-criminal gangs may want more than a financial payout. The Reddit case is one to watch, as ransomware attackers may attempt to influence geopolitical strife and business policies.

To this end, cybercriminals use guerrilla warfare tactics to create massively disruptive encryption events at the worst time possible for an organization—such as late in the evening or just before a primary holiday season. The choice of time can help to leverage ransom demands further.

In an Osterman survey, respondents were asked to indicate a deep concern with several threats related to ransomware. The results show that more respondents are concerned about the fact of a ransomware attack than about their ability to clean up after a ransomware attack. On average, being unable to prevent an attack is of high concern to 55% of respondents. The post-attack problems, such as brand reputation impacts and the ability to recover corporate data, are, on average, of high concern to 48% of respondents.

Security Issue	Prevent	Recover
Breaching of corporate data by a ransomware attack	61%	
Ransomware attacks successfully infecting endpoints	59%	
Our ability to prevent zero-day threats from infecting our systems and applications	56%	
Negative effects on our brand reputation after a security incident		54%
Our ability to keep all systems and applications patched against current threats	52%	
Our ability to recover corporate data and system integrity after a ransomware attack		50%
Our ability to prevent a data exfiltration as part of a ransomware attack	47%	
Our ability to restore normal business operations after a a ransomware attack		46%
Our ability to learn from phishing and ransomware attacks to mitigate future attempts		42%
AVERAGE	55%	48%

Source11

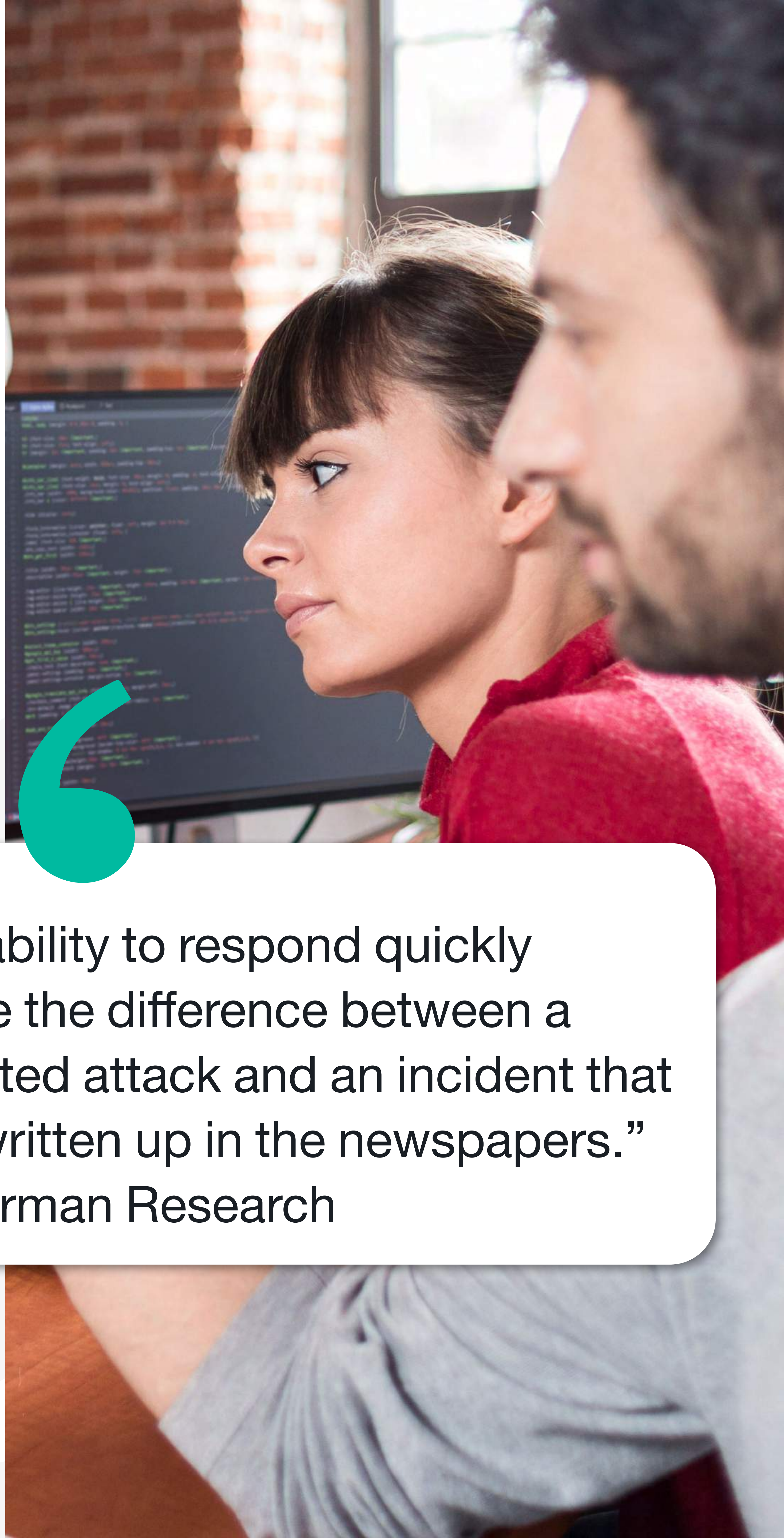
Fast Response = Fast Mitigation

As mentioned previously, the average time to mitigate the impact of a ransomware attack is 24 days. Pingdom has estimated the cost of downtime to be roughly $25,620 for SMBs and $540,000 for enterprises per hour[12]. Fast response to a ransomware attack can save a company money. In terms of ransomware response tactics, key takeaways from a 2021 Osterman report show that:

- 88% of respondents always or mostly have the ability for employees to report suspicious messages. This can be done by an employee forwarding an email to a particular help desk address for review by a security analyst or clicking a button in their email client.
- Roughly half of respondents had a group of capabilities available for post-compromise mitigation, including remediating user-reported incidents, identifying which email account was compromised, |and detecting threats after the delivery of an email attack. On average, another third said these capabilities were mainly available.
- Respondents had the lowest ability to identify internal threats that originated within their systems (e.g., internal phishing from a compromised account) and external threats that did not touch their systems (e.g., spoofing against others using their domain name). Internal phishing emails can be challenging to identify because the message and content come from within the system rather than outside. External threats that use spoofing, domain impersonation, or lookalike domains often do not touch the organization's email infrastructure. DMARC and additional brand protection solutions, like Passive DNS, are necessary to discover these external-only threats.

Osterman recommends the following remediation methods to help reduce downtime caused by ransomware:

- Employees reporting suspicious messages
- Post-delivery threat detection
- Removal of suspicious messages from mailboxes



"The ability to respond quickly can be the difference between a mitigated attack and an incident that gets written up in the newspapers."
- Osterman Research

Source12

Section Four: How to Stop Ransomware

If you've read to this point, you'll have realized that ransomware is here to stay and likely to become even more challenging to detect. This most insidious cyberattack is expanding in scope, too; the attackers are alleged to expect more demands, not necessarily financial. An MSP can help its clients deal with ransomware by offering seven measures that make it much harder for ransomware to enter and embed in the corporate network when used as integrated layers. These seven layers are part of a defense-in-depth approach to ransomware detection and prevention. In fact, by offering multiple layers of defensive measures as a managed service, an MSP can protect clients against any cyber-attack initiated via phishing. Considering that phishing negatively impacts 96% of businesses, offering this level of service is a significant value-add above and beyond ransomware protection.[13]

Seven Integrated Ways to Stop Ransomware

The following seven measures combine policy types, human-centered learning, and technology to provide a defense-in-depth approach to ransomware mitigation.

Security Policies that Include Ransomware Threats

Ransomware is a must include-in any security policy. Adding ransomware threats to a security policy begins by assessing the risk to your organization. This risk should include the critical assets, data, and systems that ransomware could impact and how to protect them. Processes such as backup and recovery should be assessed considering ransomware risks. In parallel, an incident response plan must include communication protocols in case of a ransomware attack. Measures that the security policy will cover will include the following:

Source13

Security Awareness Training

Educating employees about the risks of ransomware and other security threats is so well established that standards such as ISO27001 mandate its use. Security awareness training has advanced in recent years to become a behavior-driven series of educational programs. Often, this includes interactive videos, comprehensive training across all aspects of the business, quizzes, and fun events. Security awareness training generates metrics so program administrators can adjust the training to improve results.

Security awareness training offers a structured method to augment an organization’s technological security defenses. Through education and training, an organization’s people become experienced and knowledgeable about malicious activity and how accidents can lead to security incidents. All staff take part in the exercises. Employees, managers, and executives are educated in phishing and ransomware tactics. The education teaches people how to react to security incidents to align with a company’s security policies. Executives and others, such as administrators and accounts payable staff, are given targeted training to reflect the elevated risks of those roles.

The “training” element of security awareness training includes regular events—posters in the elevator, an email update, a video episode to watch, a discussion to participate in—but should not be limited to events only. Coaching embedded in the flow of daily interactions reinforces the concepts of security awareness training within the context and content facing employees. Like their IT security counterparts, front-line employees need solutions that augment their skills to help prevent security attacks. This help comes in many forms, but interactive and in-line training is one of the most effective. For example, an employee is shown alerts that a given message from a named individual is now coming from a different email address, that the email headers in the background do not line up, or that the message itself includes a link to a destination that has never been used.

Much of the security awareness training efforts are focused on creating a security culture. Culture is associated with behavior, so behavior-driven awareness training is essential in developing a cohesive and robust security culture.

Practical security awareness training comes from training metrics. Using feedback from a training session allows modification based on the way an employee behaves when confronted with a phishing attack. Individuals and groups who consistently fail to recognize the warning signs in simulated attacks can be targeted for further tailored training, process and policy changes, and added security precautions (e.g., various types of multi-factor authentication).

Having behavioral metrics closes the loop on training as an input with positive behavior change as an outcome.

Phishing Simulations

Phishing simulation exercises train employees and other people to spot tell-tale signs that an email is a phishing email. A simulated phishing attack mocks up a real phishing campaign. In a simulated phishing attack, employees receive a phishing email; this phishing email is delivered under the organization's control. Unlike real phishing emails, the phishing simulation email does not contain malware; any links used in the simulation go to spoof sites under the organization's control.

Advanced phishing simulation platforms are cloud-based and usually used alongside other security awareness training. The administrator of the phishing simulations can be an in-house team or an MSP (managed service provider). Phishing simulation exercises are designed using templates that create realistic-looking phishing emails. Being cloud-based, the phishing simulation platform can be configured, updated, and delivered centrally. The same central console captures training metrics and generates reports.

Phishing simulation emails may also link to a fake malicious website to test employees' reactions. Employees who click a fake phishing link will visit the fake website. Interactive training ensures the employee understands what would happen if this was a phishing email.

Simulated phishing emails can also be designed to carry fake malicious attachments. Suppose the employee attempts to open or download the attachment. In that case, the simulator will open an online screen explaining why doing this is risky behavior and what would happen if this was a real cyber-attack. The interactive learning sessions will also explain how to prevent this behavior in the future.

During the simulation exercises, data is collected on how each employee responds to the phishing email. These data provide insights to help modify, tailor, and improve phishing exercises.

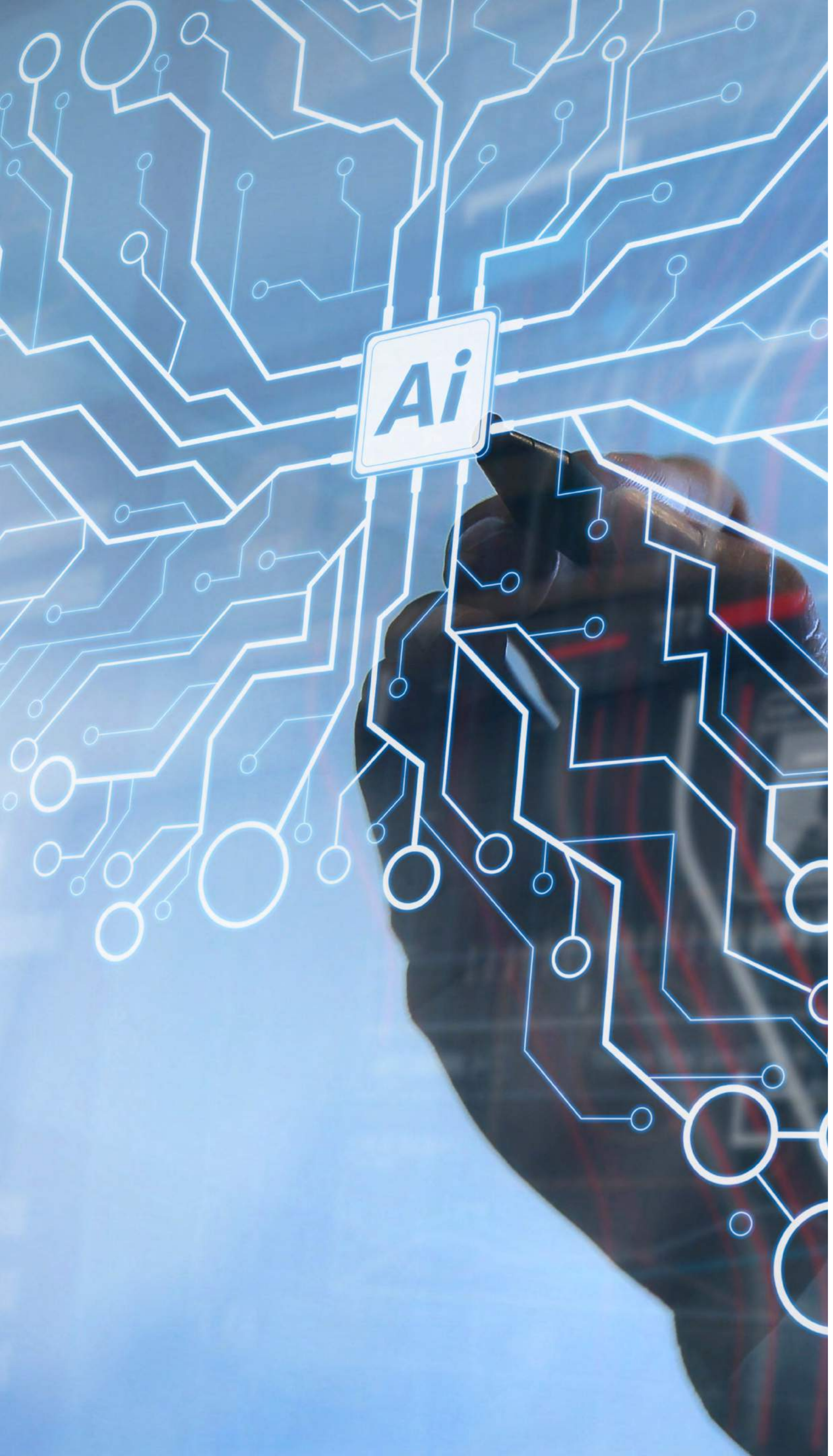
Phishing simulation exercises are usually combined with other security awareness training in a concerted effort to increase security awareness, prevent cyber-attacks, and help develop a security culture.

Advanced AI-enabled Email Security

Security awareness training is essential; however, the goalposts are changing rapidly, and the NCSC gives this stark warning:

"To 2025, GenAI and large language models (LLMs) will make it difficult for everyone, regardless of their level of cyber security understanding, to assess whether an email or password reset request is genuine, or to identify phishing, spoofing or social engineering attempts."

The changing phishing and ransomware landscape leads to the next and most vital tool in an organization's armory, AI-enabled email security with advanced anti-phishing capability.



We are familiar with the conventional secure email gateway (SEG), which will identify and quarantine suspicious emails based on known malware and phishing signatures and signals. However, a recent study demonstrates that conventional methods are falling short. The study found that almost 20% of phishing emails went undetected by Microsoft 365 Exchange Defender and Microsoft Exchange Online Protection (EOP).[14] This finding demonstrates that while an SEG is a good foundation stone, it does not protect completely. The limitations of an SEG have been overcome with a new breed of phishing prevention known as Integrated Cloud Email Security (ICES).

An Integrated Cloud Email Security (ICES) is based on AI and uses a dynamic phishing detection and prevention approach. ICES solutions are cloud-based, protecting emails in a modern cloud environment that includes remote and hybrid working. ICES does not use the static database approach to phishing detection an SEG uses. Instead, ICES applies AI, machine learning, and natural language processing (NLP) to identify multi-part, sophisticated, and even zero-minute phishing threats. Technologies like AI and NLP also allow the detection of complex phishing threats such as Business Email Compromise (BEC). These multi-part, targeted threats may use compromised email accounts that can abuse employee trust. ICES solutions, such as PhishTitan, can use AI to train using a vast corpus of data reflecting phishing threats to identify emerging threats and zero-minute phishing attacks.

MFA

Multi-factor authentication is where additional layers of authentication checks are used with a username and password. However, it must be cautioned that cybercriminals have been able to compromise even a second factor during a phishing attack in some circumstances[15].

However, in most cases, using an additional authentic layer, i.e., MFA, increases the difficulty in successfully leveraging compromised credentials. This tactic can be thought of as having an alarm system just inside the door, a guard dog patrolling the premises, or a security guard performing additional checks on whoever walks in the door.

Source 14

Source 15

Options for MFA include the following:

Phone or Email Based

MFA via SMS or an email address is a comparatively weak form of MFA. For email-based MFA, for example, if a threat actor already has the username and password for the email account due to a phishing attack, they can also access the MFA code for any systems that use that email address. SMS-based messaging is more challenging to compromise, but SIM-card cloning, SIM-card re-issuance following an impersonated request to the mobile carrier's call center, and even fake-destination login websites with scripts to capture and immediately act on an MFA entry have already been used to circumvent such controls.[12] Reliance on SMS codes also fails when cell coverage is lacking.

Authenticator App-Based

Authenticator apps, such as those from Google and Microsoft, can be installed on a mobile phone. After an account for MFA is registered and linked to the authenticator app, the unique code generated by the app is needed to log into a service (along with the username and password). Authenticator apps do not share the same weaknesses as SMS or email-based codes, but attackers have been able to compromise the login activity using fake-destination login sites.

Hardware Security Keys and Biometrics

The strongest forms of MFA currently available are FIDO2-based security tokens that rely on public key encryption and biometric authentication approaches. Hardware keys provide a portable root of trust. Biometric authentication provides the most robust identity assurance for the person seeking access to a system. Anyone with access to financial systems, employee records, patient data, and other systems containing commercially and personally sensitive data should be using as strong a form of MFA as possible.

Secure Backups

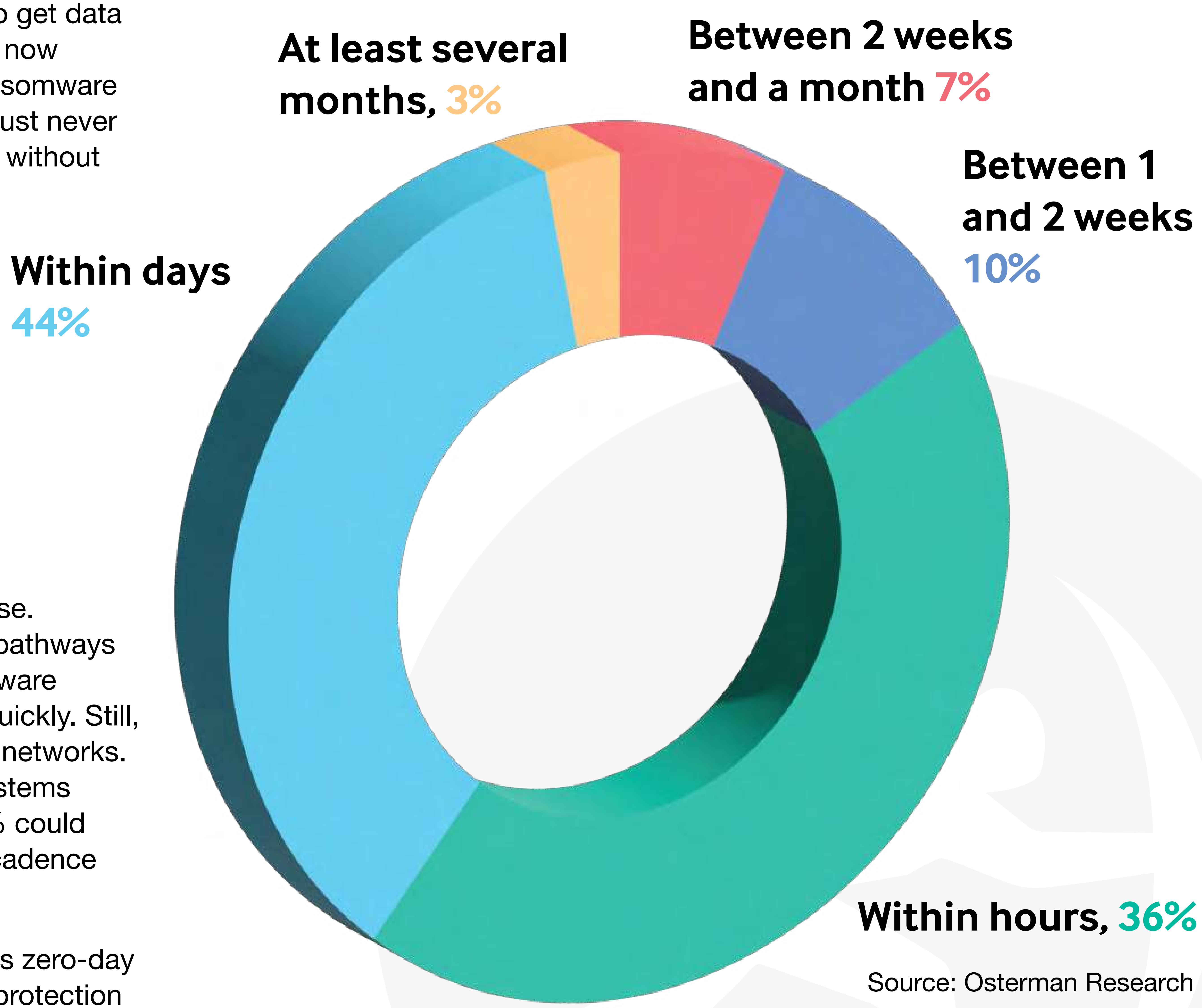
A secure backup system from a ransomware attack is an excellent way to get data back without paying a ransom. However, as many ransomware attackers now also steal data, having a backup only solves some of the problems of ransomware infection. When choosing a ransomware-resistant backup system, you must never forget the end goal: to restore business operations swiftly and accurately without significant data loss. Backup services must be able to:

- Backup to multiple locations
- Have at least one backup location offsite
- Perform regular and frequent backup intervals
- Educate employees on your backup policies
- Limit and control access to backup locations

Patch

Patching software and hardware is a cybersecurity prevention 101 exercise. Cybercriminals use vulnerabilities in systems and applications to exploit pathways into sensitive parts of a network. Patching policies should reflect ransomware threats and patching cadence should Threat actors go on the offensive quickly. Still, it can take organizations days, weeks, or months to counter-defend their networks. Research from Osterman found that 36% of respondents could patch systems and applications within hours of discovering new vulnerabilities, and 44% could do so within days. The remainder took one week and several months, a cadence representing a significant threat.

However, caution comes with the latest batch of ransomware that exploits zero-day vulnerabilities for which no patch is available. This is why multi-layers of protection are vital in the fight against ransomware.



Source: Osterman Research

AI in Ransomware Prevention

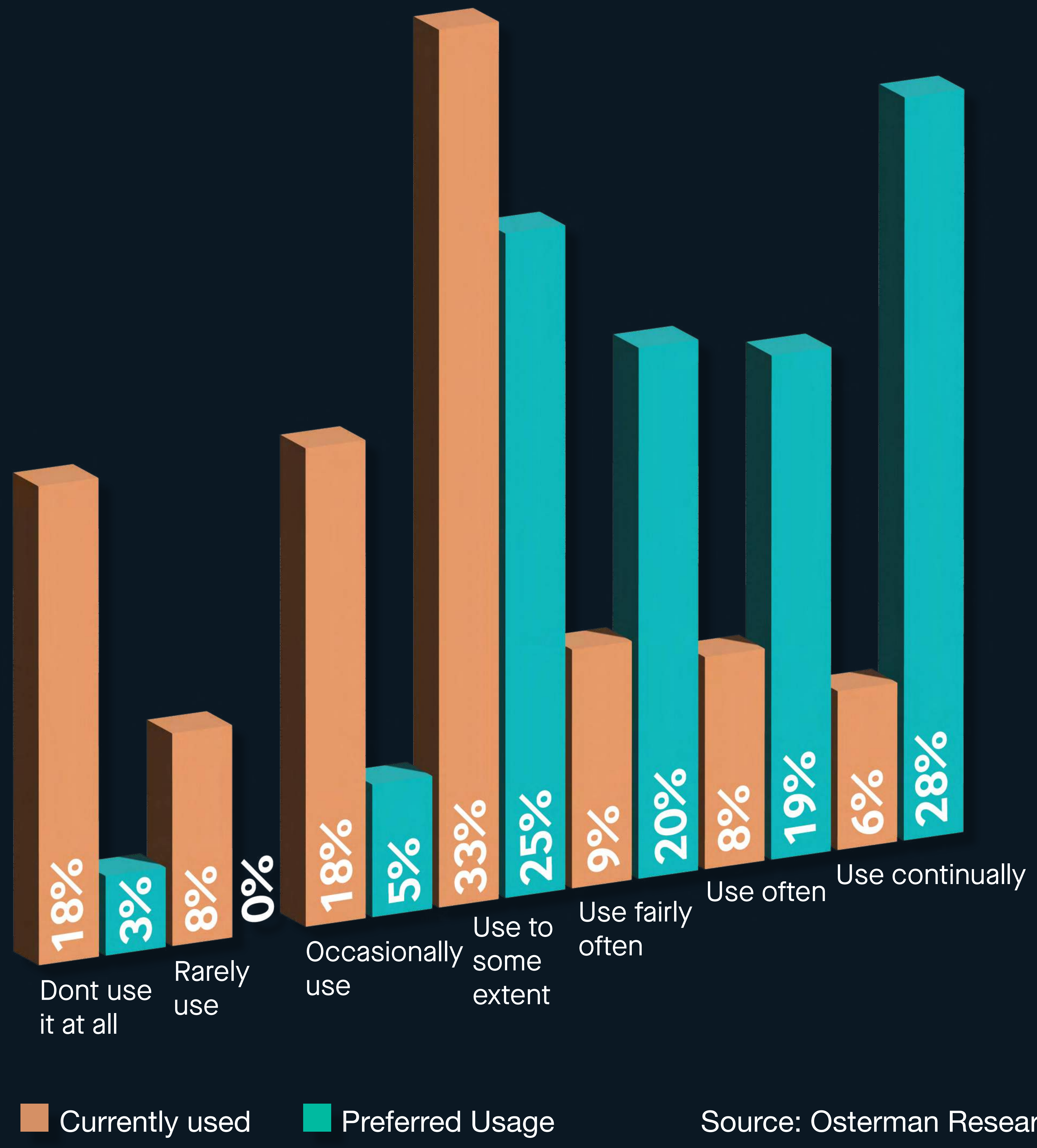
AI is becoming a must-have in preventing modern complex ransomware attacks. AI-enabled email security, such as Integrated Cloud Email Security (ICES), offers a substantial benefit over the conventional secure email gateways built into productivity suites such as Microsoft 365. In terms of organizational views on the use of AI in tackling phishing and ransomware, research from Osterman shows that companies want much more use of AI/ML than currently deployed:

Current Usage

77% of respondents said AI/ML is currently used to some extent or less, with the “to some extent” almost half of this value.

Preferred Usage

92% of respondents would prefer that AI/ML was used to some extent or more. Of the total, 47% wanted AI/ML used often or continually, up from 14% of respondents who say that is currently the situation.



Source: Osterman Research

Section Five: The MSP and Ransomware Prevention

An MSP is perfectly positioned to deliver the multiple layers of protection needed to stop ransomware. The latest generation of AI-enabled anti-phishing solutions is driven by the need to deploy and manage these capabilities centrally and remotely. Advanced, behavior-driven, security awareness training and phishing simulation platforms are similarly designed with an MSP delivery model in mind.

This places an MSP uniquely positioned to deliver exceptional anti-ransomware solutions to their clients. However, integrated security awareness training, phishing simulation, and AI-enabled ICES solutions designed for an MSP must have additional criteria, such as:

- API and RMM integration.
- Full lifecycle backing from billing to onboarding to continued support.
- Cloud-based with a comprehensive and centralized management console
- Multi-tenant dashboard for client isolation.
- Real-time data monitoring to locate anomalies and potential threats.
- Dynamically expandable for MSPs as they
- grow their business.
- Fully automated security awareness training.
- MSP Dashboard: allows manual or automated simulated phishing campaigns to be set up.

How TitanHQ Prevents Ransomware

TitanHQ offers an integrated solution suite with the tools to prevent modern, complex phishing threats that lead to ransomware. Our solutions are all designed to meet the needs of an MSP. TitanHQ anti-ransomware solutions include the following:

PhishTitan

PhishTitan is an integrated multi-layered anti-phishing solution designed for MSP delivery. PhishTitan comes with an MSP dashboard for ease of deployment and management. PhishTitan is based on Defense-in-Depth principles, applying multiple layers of integrated security technologies to detect and prevent evasive and evolving threats such as ransomware. Phish-Titan is cloud-based, which is ideal for deployment and management by an MSP. The phishing prevention and remediation offered by PhishTitan is AI-driven and powered by LLM intelligence.

The layers of protection offered by PhishTitan include the following:

AI-driven threat intelligence: detection models predict and detect malicious content that conventional email security misses. AI-driven phishing prevention used by PhishTitan can see zero-minute URLs.

Real-time threat analysis: PhishTitan performs real-time detection and prevention to stop even emerging threats.

URL rewrite detection: PhishTitan applies URL analysis to detect malicious links in phishing emails and uses this intelligence to protect against these links using a unique ‘Link Lock’ service.

Post-delivery remediation: even if a phishing message gets through, PhishTitan initiates a post-delivery remediation process. This process monitors emails and removes malicious mail from an inbox.

Time of click protection: Post-delivery remediation applies a secondary protection mechanism called ‘time of click’ protection.

Integration with M365: PhishTitan seamlessly integrates into M365, augmenting and enhancing Microsoft native security. PhishTitan scans inbound and outbound emails to prevent phishing and the loss of sensitive data.

A report from TitanHQ identified a **92% drop in phishing susceptibility** when employees were trained using PhishTitan’s automated security awareness training solution[16].

Source 16

PhishTitan is an integrated multi-layered anti-phishing solution designed for MSP delivery.

SafeTitan

SafeTitan for MSPs is a Security Awareness Training and Phishing Simulation platform allowing an MSP to deliver enterprise-grade training to SMB clients. As a purpose-built MSP solution, SafeTitan can have precisely what clients need to train employees to deal with phishing threats. Some of the MSP-focused features include the following:

Auto Campaigns: SafeTitan Auto Campaigns provides an automation tool. This tool allows an MSP to dramatically improve customer security awareness while reducing the time spent planning and managing cybersecurity initiatives.

MSP Dashboard: view all quick actions and live analytics in one place with our MSP dashboard.

A vast array of templates: over 1.8K phishing templates, 80+ Videos, training sessions, and webinars.

Reactive Training: exclusive to the MSP layer, Reactive Training enables real-time identification of insecure behavior, allowing for tailored follow-up training.

Direct Email Injection (Graph API): Phishing simulation emails delivered directly into the user`s mailboxes. There is no need to spend resources and time configuring allowed lists or firewalls.

Rounding up Ransomware

As an MSP, you know your clients' needs intimately. As ransomware attacks increase, you can protect your clients' businesses and employees against this insidious threat. The seven integrated ways to stop ransomware offer a blueprint to fight against ransomware infection. You will give your client peace of mind by choosing an integrated AI-driven approach to anti-phishing and backing this up with an automated security awareness training program.

GET IN TOUCH