Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **May 2021**
Sponsored by **Mimecast**

How to Reduce the Risk of Phishing and Ransomware

Executive Summary

Cybersecurity challenges abound for organizations across the world. The tsunami of phishing attacks that threaten account compromise, data breaches and malware infection remains a critical threat to neutralize. Ransomware is a second critical threat, with a well-played ransomware attack capable of bringing an organization to a complete halt, and in some cases putting it out of business permanently (e.g., Travelex[1] and Vastaamo[2]). Both phishing and ransomware were critical threats before the health pandemic of 2020 forced a sudden shift to remote working, and such a move has only served to intensify the threat levels. The Global Risks Report 2021, a recently released publication from the World Economic Forum, ranks information security as the top technology objective that has become a greater priority due to COVID, noting that it is complex, there is a skills shortage, and cybercriminals are difficult to track, among others.[3]

This white paper and the survey commissioned for this research looks specifically at the threats of phishing and ransomware, and how the risks of both can be reduced.

KEY TAKEAWAYS

Osterman Research conducted an in-depth survey of security-focused professionals specifically for this white paper. Here are the key takeaways from the research:

- Half of organizations believe they are effective at counteracting various phishing and ransomware threats. Of the 17 threat types we asked about in the survey, 37% of organizations believed they were highly effective at counteracting 11 or more of the threat types.
- Only 16% of organizations reported no security incident types related to phishing and ransomware in the past 12 months. In other words, it is a widespread problem for most organizations.
- Respondents indicated only mid-range confidence in the ability of various groups of employees to recognize phishing attempts through email and other channels. Confidence levels in the ability to recognize ransomware attacks were lower still.
- The most effective mitigations against phishing attacks, from our research, are multi-factor authentication, security awareness training, and the ability to remove phishing messages from employees' mailboxes. For ransomware, it is multi-factor authentication, rapid patching of vulnerabilities, and security awareness training.
- Best practices to reduce the risk of phishing and ransomware include focusing on significant root causes, not waiting to start, and making it harder for yourself.

Phishing and ransomware were already critical threats before the health pandemic forced a sudden shift to remote working.

ABOUT THIS WHITE PAPER

This white paper is sponsored by Mimecast. Information about Mimecast is provided at the end of the paper. This paper references data from an in-depth survey of 130 cybersecurity professionals in mid-sized and large organizations that was conducted specifically for this paper.

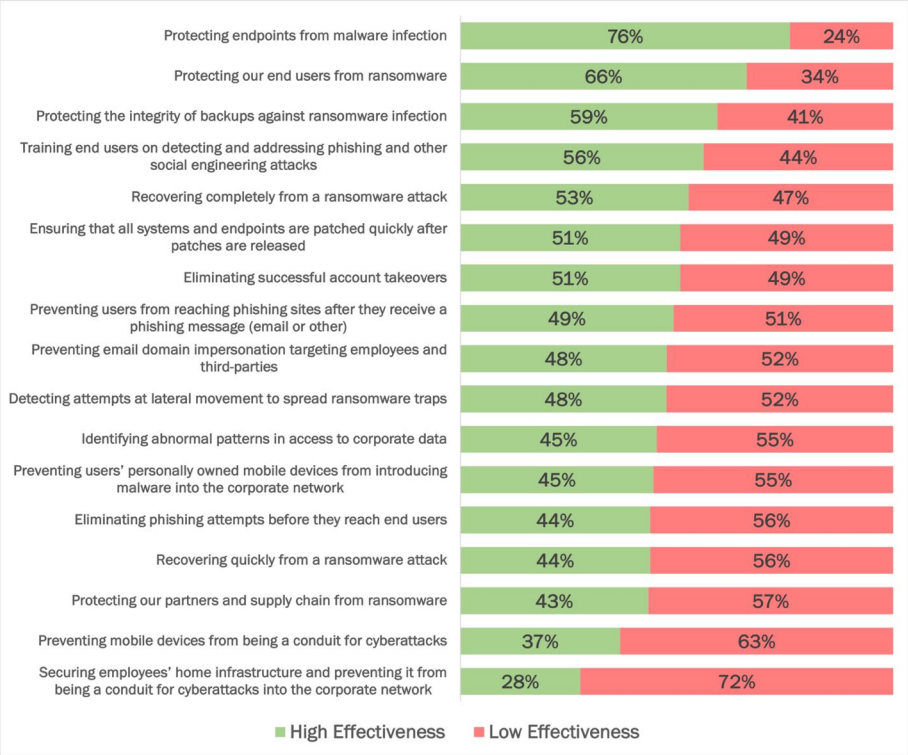
Current Threat Landscape

This section looks at the threats facing organizations today. It reports the data from the organizations surveyed for this report, along with the wider threat context.

HIGH AND LOW EFFECTIVENESS AGAINST THREATS

Whatever the threat type, low effectiveness at counteracting the potential effects makes an organization more susceptible to being hit hard. For the organizations we surveyed for this report, many believe they are highly effective at counteracting some threats related to phishing and ransomware, but not very effective at counteracting others. As a general conclusion, half of all organizations are not effective at counteracting phishing and ransomware threats. See Figure 1.

Figure 1
Organizational Effectiveness Against Various Phishing and Ransomware Threats
Percentage of Respondents



Source: Osterman Research (2021)

Only 37% of organizations believed they were highly effective at counteracting 11 or more of the phishing and ransomware threats.

Another way of looking at the data, however, is to look for a pattern of effectiveness against the 17 threat types at individual organizations. The question becomes whether an organization effective against one type of threat is more likely to be effective against the others as well. The survey data showed that:

- 37% of organizations believed they were highly effective at counteracting 11 or more of the phishing and ransomware threats.
- 63% of organizations believed they were highly effective at counteracting 10 or fewer of the threats.

INCIDENTS FROM THE PAST 12 MONTHS

Almost 85% of the organizations surveyed have experienced one or more of 17 types of security incidents in the past 12 months. Just over half of the organizations surveyed have experienced between one and three types of incidents. Just under a third have experienced four or more types. Only 16% of organizations have reported no security incident types related to phishing and ransomware in the past 12 months. The three most commonly occurring type of security incidents are business email compromise (BEC) attacks that successfully tricked lower-level employees (53%), phishing messages that result in a malware infection (49%), and phishing messages that result in an account compromise (47%). See Figure 2.

Figure 2
Types of Security Incidents That Have Occurred During the Previous 12 Months
Percentage of Respondents

Type of Security Incident	%
A business email compromise attack was successful in tricking at least one lower-level employee within our company	53%
A phishing message has resulted in a malware infection	49%
A phishing message has resulted in an account compromise	47%
Your domain has been "spoofed" to perpetrate phishing campaigns	38%
Ransomware was detected in our systems before it activated	34%
A business email compromise attack was successful in tricking at least one senior executive within our company	28%
A phishing message impersonating your domain compromised a third-party	16%
A phishing message has resulted in a ransomware infection	14%
A ransomware attack was successfully launched	10%
A ransomware attack resulted in internal IT systems becoming non-operational	10%
A ransomware attack resulted in unrecoverable data loss	6%
A department or business unit at our organization had to cease operations, at least temporarily, due to a ransomware attack resulting in unrecoverable system and data loss	6%
A ransomware attack resulted in operational technology systems becoming non-operational	4%
Our entire organization had to cease operations, at least temporarily, due to a ransomware attack resulting in unrecoverable systems and data loss	3%
Data was exfiltrated as part of a ransomware attack	2%
Data exfiltrated in a ransomware attack was offered for public sale or auction	1%
Our infrastructure was compromised to host malicious content that threat actors used against other companies and individuals	0%

Source: Osterman Research (2021)

Only 16% of organizations have reported no security incident types related to phishing and ransomware in the past 12 months.

While Figure 2 accurately reports the results from survey respondents, the results are likely to be understated. First, security incidents are embarrassing to an organization generally and IT security professionals personally, hence some incidents may remain unreported. Second, awareness of each type of security incident requires the capability to detect (and mitigate) such incidents, and not all

organizations have the optics to do so. On balance, we believe the rate of security incident types is higher than what is reported in Figure 2.

ISSUES OF HIGH CONCERN TO SECURITY TEAMS

Of the 14 security issues we asked respondents to rate, ten were rated of high concern by more than half of the respondents. Phishing attempts making their way to end users was the top-rated issue of concern (by 65% of respondents), followed closely by employees being unable to spot phishing or social engineering attacks before clicking a link or attachment (by 64% of respondents). The issues in third and fourth place were related to ransomware attacks.

Figure 3
Issues of High Concern to Security Teams
Percentage Responding "Concerned" or "Extremely Concerned"

Security Issue	%
Phishing attempts making their way to end users	65%
Employees failing to spot phishing and social engineering attacks before clicking on a link or attachment	64%
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 prevent lower-level employees from falling victim to a business email compromise attack	53%
Our ability to prevent senior executives from falling victim to a business email compromise attack	53%
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 data exfiltration as part of a ransomware attempt	47%
Domain impersonation to perpetrate phishing and BEC campaigns	46%
Our ability to restore normal business operations after a ransomware attack	46%
Our ability to learn from phishing and ransomware attacks to mitigate future attempts	42%

Source: Osterman Research (2021)

Phishing attempts making their way to end users was the top-rated issue of concern (by 65% of respondents).

In our 2019 report on phishing, business email compromise, account takeovers and other security threats, the same two issues above also rated at the top of the list but were of higher concern in 2019. The level of concern about ransomware, by contrast, has increased over the same time period, reflecting the growing occurrence and threat of ransomware incidents to organizations everywhere.[4]

THE THREAT OF PHISHING

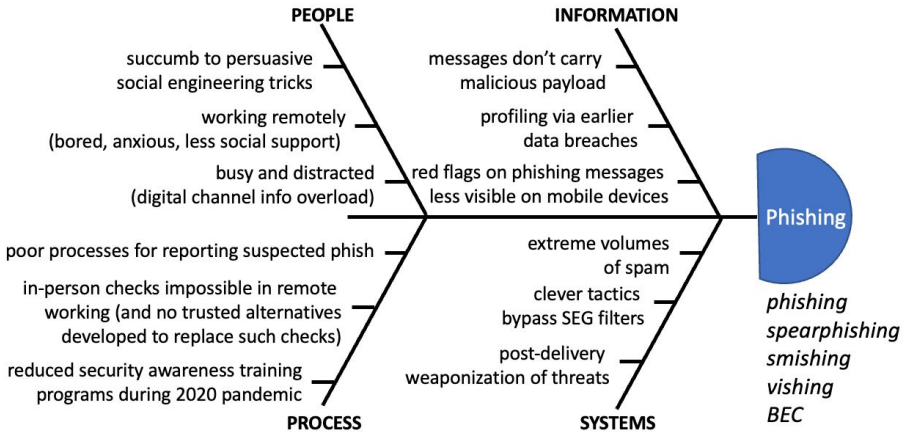
Phishing is an initial attack vector for cybercriminals, and by itself is but a nuisance. What phishing can lead to, however, makes it a critical threat for organizations to address. Successful phishing attacks—delivered as either broad-based phishing, targeted spearphishing or business email compromise—can result in one or more of the following outcomes (this is not an exhaustive list):

- Malware infection—for data theft and network reconnaissance.
- Ransomware infection—for data theft, ransom demands, and extortion.
- Credential theft—to support impersonation, data theft, lateral movement, compromise of other systems that share the same credentials (e.g., within Microsoft 365 from Exchange Online to SharePoint and Teams), and pre-attack reconnaissance for multi-stage threat campaigns.
- Financial sabotage—such as invoice and payment fraud. These are usually associated with the phishing-variant called business email compromise.

Phishing is undertaken through multiple channels, including email, SMS and mobile messaging services, social media apps such as LinkedIn, and voice phone calls. Most phishing attacks share common characteristics of an urgency to act or an impersonation of an individual or brand. Attacks will often leverage current topics to increase the likelihood of a victim taking the lure. Many phishing attacks over the past year have leveraged COVID-related themes, such as rates of spread and infection, accessing funding from government agencies, and in more recent months to getting early access to a vaccine program. The reasons phishing works so effectively are many and varied; see Figure 4.

What phishing can lead to makes it a critical threat for organizations to address.

Figure 4
ANTECEDENTS FOR PHISHING
Causal and Contributing Factors in Phishing Attacks



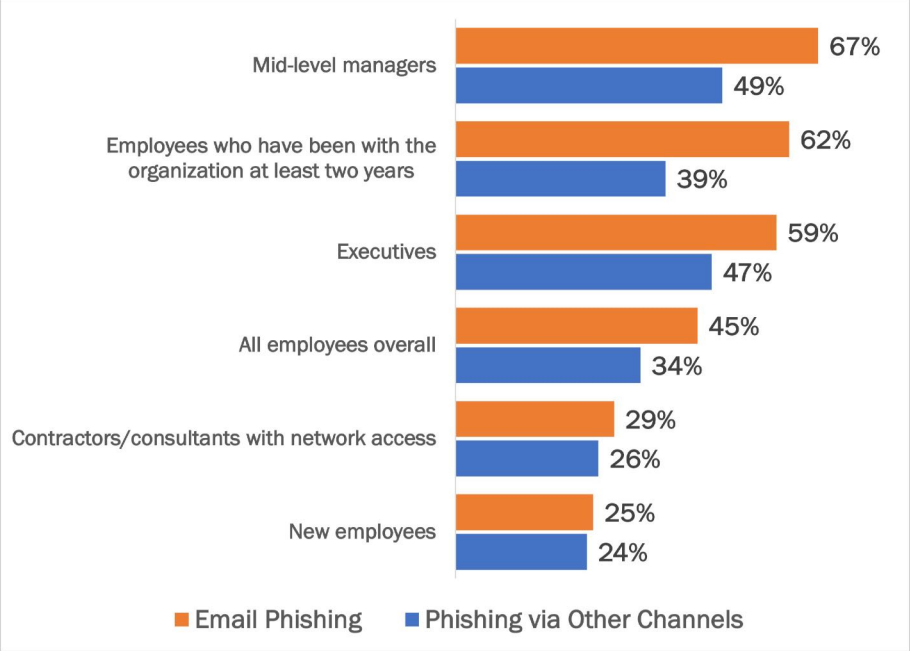
Source: Osterman Research (2021)

Phishing is a massive and growing problem. In 2020, Google detected 2.1 million domains tied to phishing attacks, up from 1.7 million detected domains the year before.[5] Phishing is implicated as the majority root cause for malicious breaches, and in the age of stringent data protection regulations (GDPR, CCPA, CPRA, etc.), the potential consequences of data breaches are significant. Added to the problem is the increased sophistication in phishing attacks by threat actors. Phishing-as-a-

service offerings combined with easily accessible phishing kits enable an attack scalability that even amateur threat actors can adopt. Post-delivery weaponization of URLs and other threats in an email message or attached document provides clear pathways through many secure email gateways, delivering messages with malicious intent and malicious content right to a user's inbox. Targeted spearphishing attacks can include unique identifiers that lead to victim-specific threats when activated. And finally, not all threat actors are out for an immediate payoff but evince a willingness to build a seemingly benign relationship with the victim for months in advance of unleashing the seedy reality.

Organizational preparedness to mitigate phishing attacks is a blend of technology, process and people factors. In our research, security awareness training—a people factor—was ranked by survey respondents as the second most effective mitigation against phishing attacks (behind using multi-factor authentication to reduce the ease of stealing usable credentials). However, respondents to the survey indicated only mid-range confidence in the ability of various groups of employees to recognize phishing attempts through email and other channels—see Figure 5.

Figure 5
Confidence That Various Groups are Well Trained to Recognize Phishing Attempts Through Email and Other Channels
Percentage Indicating "Fairly Confident" or "Completely Confident"



Source: Osterman Research (2021)

Respondents indicated only mid-range confidence in the ability of various groups of employees to recognize phishing attempts through email and other channels.

Other channels include messages and the news feed in social media, browser pop-ups, search results, and rogue apps. Respondents had lower confidence in the efficacy of training for detecting phishing through these other channels, highlighting an area for further attention as threat actors leverage tools beyond email. Interestingly, the spread of training confidence between email and other channels was the closest for people outside or new to the organization, indicating a reliance on training or experience gathered from other places. Trusting in the efficacy of this beyond-the-organization training is a dangerous planning assumption, however.

THE THREAT OF RANSOMWARE

Ransomware is a second-order effect of an initial successful attack, rather than an initial attack itself. It is an outcome, not a cause. Cybercriminals first need to capture a beachhead in the organization's network or supply chain, and then lay traps for a ransomware attack. Precursors to a ransomware infection include:

- Remote Desktop Compromise—gaining control of a computer through weaknesses in the configuration of the Remote Desktop Protocol (RDP). This is simple when RDP connections are not secured (e.g., there is no password set and thus it enables open access) or credentials are known (e.g., through an earlier credential compromise attack).
- Phishing—messages carrying malicious links or attachments that the targeted victim clicks or opens. This could result in credential theft or the installation of an initial malicious—but benign-looking—application that subsequently activates and downloads further code.
- Malvertising—after a user clicks on a fake advertisement that leads to a malicious site or downloads malicious code.
- Compromised Software Updates—where cybercriminals gain access to the software update mechanisms at a trusted vendor and add malicious code that creates a backdoor for further activity on infected devices. In 2018, for example, this happened to almost 1 million users of Asus laptops in Russia.[6]

Cybercriminals have become increasingly ruthless, giving up on the hope that an unexpected encryption event would be sufficient to guarantee a financial payout from the victim company. Ransomware attacks are now usually designed to include multiple pathways for financial gain, such as exfiltrating data before the ransomware event (to increase extortion leverage by threatening to publish the data if the ransom demand is not paid), or exfiltrating the data and selling it to the highest bidder at auction if the ransom demand is not forthcoming.

Cybercriminals have become increasingly ruthless in how ransomware attacks are executed.

Cybercriminals are also embracing underhanded guerrilla-warfare tactics to create massively disruptive encryption events at the worst time possible for an organization—such as late in the evening just before a major holiday weekend or vacation, or the day before school starts in the education sector. Such timing increases the social pressure on everyone who has a say in the resolution, making payment of the ransom seem like the easiest way out of the immediate problem.

Respondents to our survey indicated levels of high concern with several threats related to ransomware (see Figure 6, which is an extract of Figure 3). More respondents have a high level of concern about the fact of a ransomware attack happening than have a high level of concern about their ability to clean up after a ransomware attack. Not being able to prevent an attack is represented is, on average, of high concern to 55% of respondents. The post-attack concerns, such as brand reputation impacts and the ability to recover corporate data, are on average, of high concern to 48% of respondents.

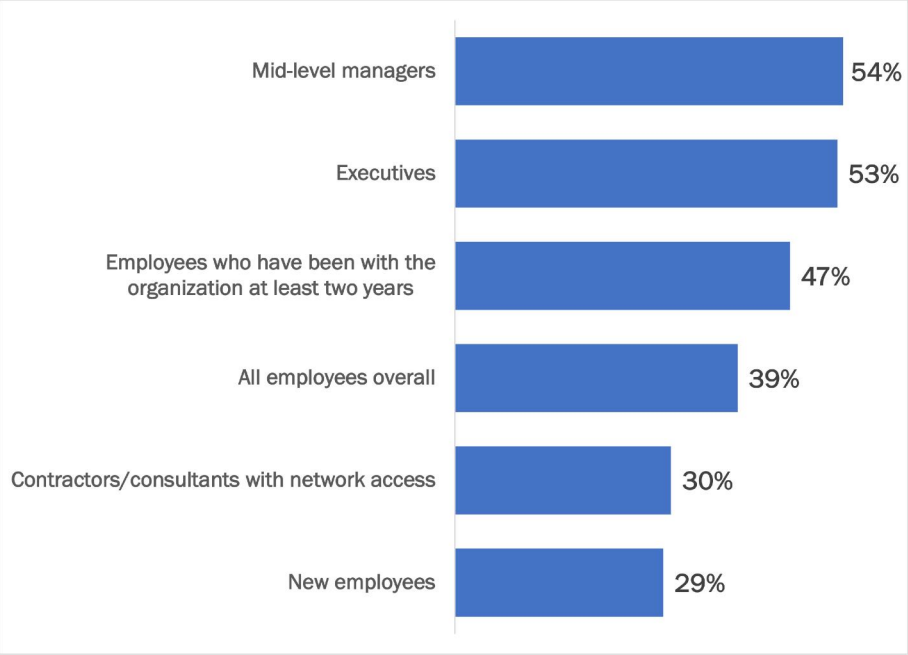
As with phishing attacks, organizational preparedness for ransomware attacks requires a blend of technology, process and people factors. In our research, respondents indicated a lower level of confidence in the ability of the internal employee groupings to recognize ransomware attacks compared to their ability to recognize phishing attacks through email and other channels. See Figure 7.

Figure 6
Ransomware-Related Issues of High Concern to Security Teams
Percentage Responding "Concerned" or "Extremely Concerned"

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 data exfiltration as part of a ransomware attempt	47%	
Our ability to restore normal business operations after a ransomware attack		46%
Our ability to learn from phishing and ransomware attacks to mitigate future attempts		42%
AVERAGE	**55%**	**48%**

Source: Osterman Research (2021)

Figure 7
Confidence That Various Groups are Well Trained to Recognize Malware or Ransomware Attempts
Percentage Indicating "Fairly Confident" or "Completely Confident"



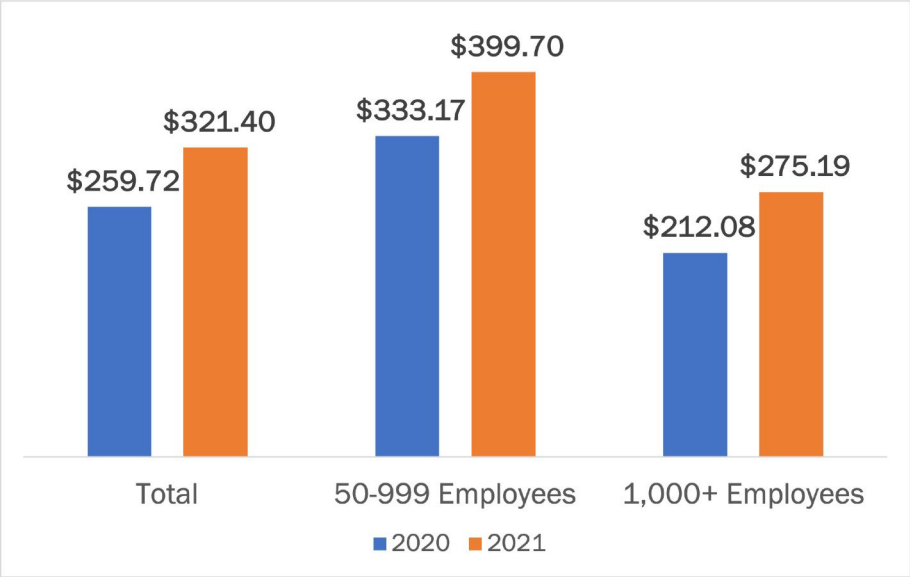
Source: Osterman Research (2021)

Respondents indicated a lower level of confidence in the ability of the internal employee groupings to recognize ransomware attacks.

SECURITY SPENDING IN 2020 VS. 2021

There is no perfect way to draw a comparison of security spending across a population of organizations because of differences in industry, business model, organization size, and even the data protection regulations in play in various geographies. However, despite the lack of perfection available, our research showed that security budgets are set to increase in 2021 compared to 2020 at both organizations with less than 1,000 employees and those with more than 1,000 employees. See Figure 8.

Figure 8
Security Budgets per Employee
Average of Respondents



Source: Osterman Research (2021)

Security budgets are increasing in 2021 compared to 2020.

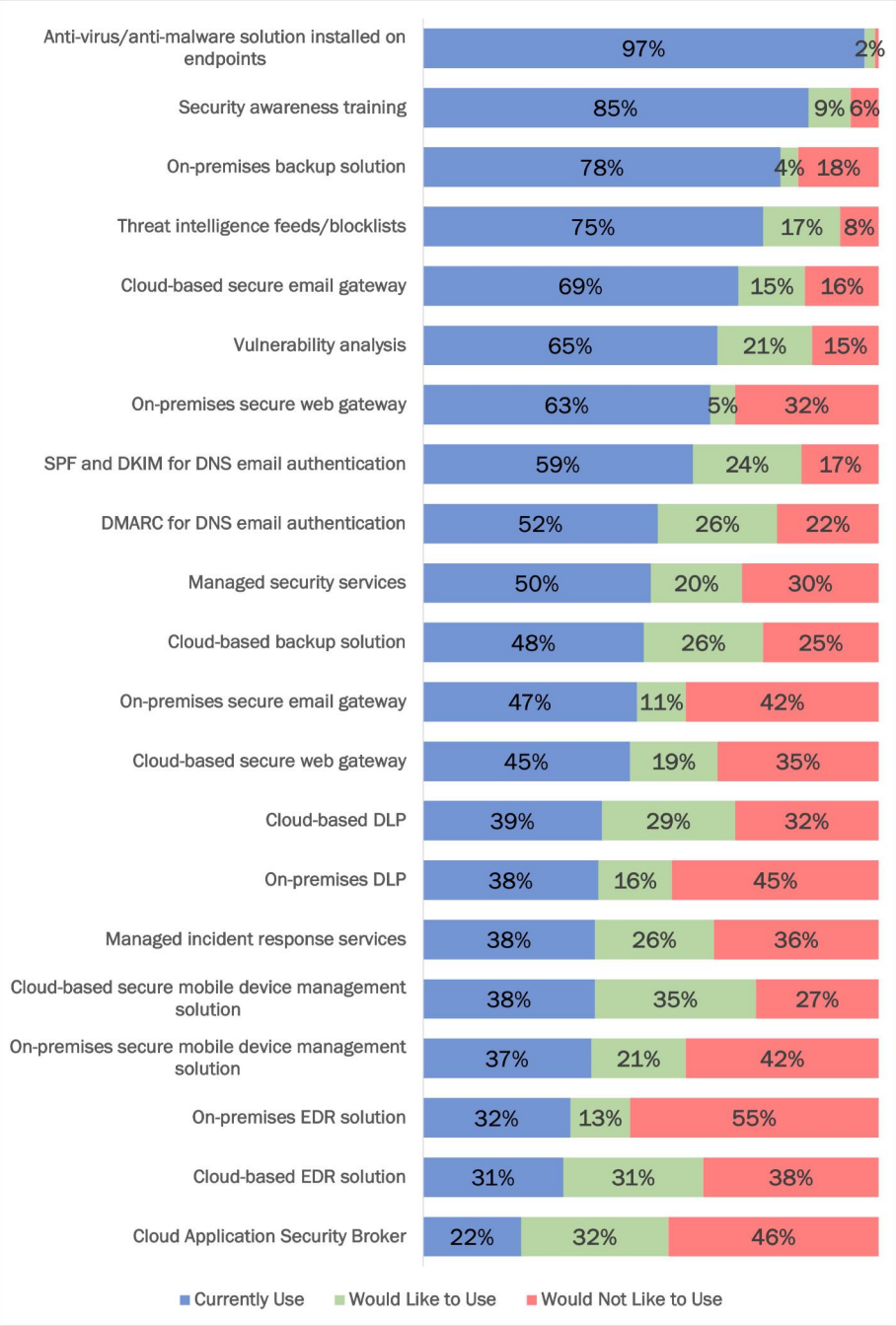
Increased spending is likely to—or should—focus on:

- **Greater Use of Cloud Security Services**
  Respondents indicated a preference for higher usage of cloud security services (see Figure 9). Cloud services offer a rapid pathway to elevated security, along with negating the need for many of the administration and maintenance tasks that go with on-premises infrastructure.
- **Improved Security Awareness Training**
  With respondents only indicating mid-range confidence in current security awareness training outcomes, elevating the competence of all employee groups to recognize and neutralize phishing and ransomware threats is essential. Refer to Figure 5 and Figure 7.
- **General Elevation of Security Solutions**
  Improved capabilities for rapidly patching vulnerabilities, and for faster detection of internal phishing threats and external spoofing attacks should be considered, as well as increased adoption of AI (artificial intelligence) and ML (machine learning) in the fight against phishing and ransomware. These are current areas where organizations show weaknesses.

CURRENT AND PREFERRED USAGE OF SECURITY TOOLS

Organizations make use of a variety of security tools to counteract, respond to, and mitigate security threats, and others would like to do so. See Figure 9. Please note that the third value in the chart—"would not like to use"—is a calculated value that attempts to map changing preferences for different types of security tools.

Figure 9
Current and Preferred Usage of Security Tools
Percentage of Respondents Currently Using or Wishing They Could



Source: Osterman Research (2021)

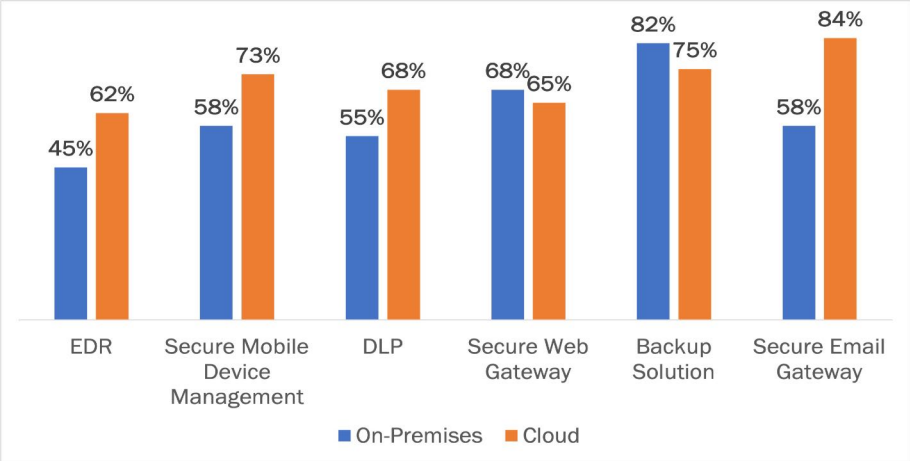
Organizations make use of a variety of security tools to counteract, respond to, and mitigate security threats, and others would like to do so.

In reviewing the current and preferred usage profiles, we note the following:

- **Endpoints Both Are and Are Not Protected**
  Endpoint protection through anti-virus and anti-malware solutions shows high usage (currently by 97% of respondents), but the use of Endpoint Detection and Response (EDR) is currently at the other end of the spectrum at slightly less than one third for both on-premises and cloud-based approaches. While one can stop and block active threats, the other can seek out threats and vulnerabilities across the entire endpoint estate, irrespective of whether a particular threat has broached a given endpoint.
- **Sender Policy Framework (SPF)/DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC) Are Almost Equivalent**
  The current and preferred usage of SPF/DKIM and DMARC for email authentication are almost the same, although DMARC trails slightly. Usage of the three is moving closer together, at it should, since the three work in lockstep. Clearly there is a difference between using DMARC with a policy of none and a policy of reject, a nuance we did not query in this research.
- **Growing Appetite for Managed Services**
  One half of respondents currently use managed security services, and two fifths use managed incident response services. Once the preference to use both is added to this base score, the variation between the two is negligible, at 70% for managed security and 63% for managed incident response services.
- **Growing Preference for Cloud Security Services**
  Respondents have a greater preference for using cloud security services than on-premises security tools for four of the six tools (see Figure 10). EDR, secure mobile device management, Data Loss Prevention (DLP) and secure email gateway all received a higher aggregate score for cloud-based usage for both current and preferred usage than on-premises versions of the same. Respondents currently have a higher preference for on-premises secure web gateway compared to cloud-based (although there is not much difference), and for on-premises backup.

Respondents have a greater preference for using cloud security services than on-premises security tools for four of the six tools.

Figure 10
On-Premises vs. Cloud-Based Security Tools
Percentage of Respondents Currently Using and Wishing They Could

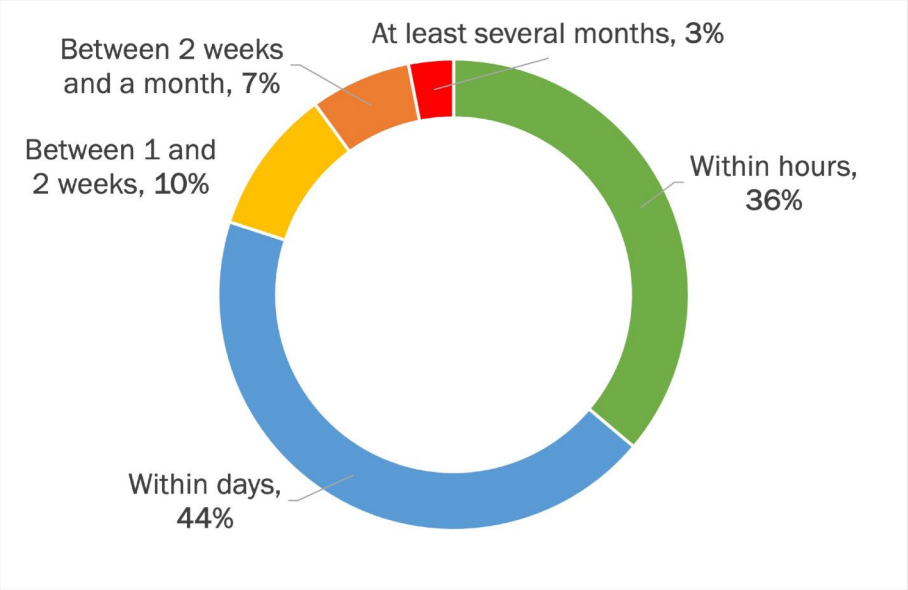


Source: Osterman Research (2021)

PATCHING CADENCE

A potential threat vector for any organization is leaving systems and applications exposed to exploitation and misuse after new vulnerabilities are discovered. When threat actors are able to go on the offensive within hours or days, organizations that take days, weeks or months to play defense will usually be outmaneuvered. In our research, 36% of respondents said they were able to patch systems and applications within hours of new vulnerabilities being discovered, and a further 44% were able to do so within days (e.g., less than one week). The remainder took between one week and several months, a cadence that represents a significant threat. See Figure 11.

Figure 11
Cadence for Patching Systems and Applications
Percentage of Respondents



Source: Osterman Research (2021)

Cybercriminals have exploited vulnerabilities at a faster cadence than organizations have protected against them in several recent incidents. For example, Accellion became aware of a vulnerability in its legacy File Transfer Application in mid-December 2020 and gave notice to its customers. Threat actors compromised many of those customers within 72 hours of the advisory being released, including SingTel (telecommunications), the Reserve Bank of New Zealand (government and regulatory), and Allens (legal services).[7]

Other research has concluded that cybercriminals have an advantage over the organizations they target. For example:

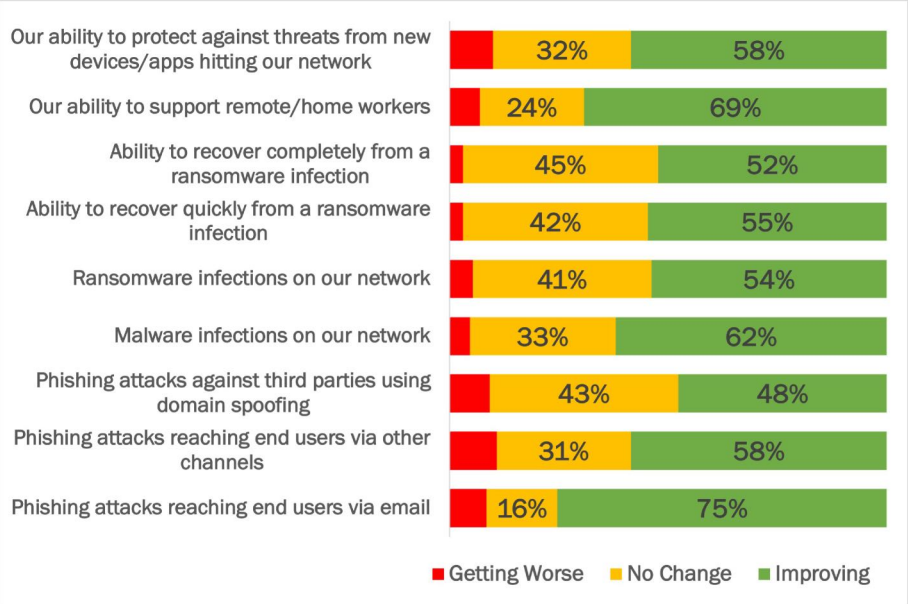
- 42% of respondents to the Cisco CISO Benchmark Report in 2020 said they were suffering from cybersecurity fatigue. Many had almost given up on proactively defending against malicious actors.[8]
- 44% of cybersecurity leaders in France, Germany, and the United Kingdom believed their teams were falling behind in the arms race against threat actors.[9]

Cybercriminals often exploit vulnerabilities at a faster cadence than organizations can protect against them.

IMPROVING ORGANIZATIONAL CAPABILITIES

Many respondents report seeing improvements over the past three years in the ability of their organization to deal with various threats. Across a collection of threats, roughly three out of five respondents say the situation has improved over the past three years, one third says it has remained unchanged, and the remainder say it has gotten worse. See Figure 12.

Figure 12
Three Year Change in Ability to Deal with Threats
Percentage of Respondents



Source: Osterman Research (2021)

In looking at these results, we make the following observations:

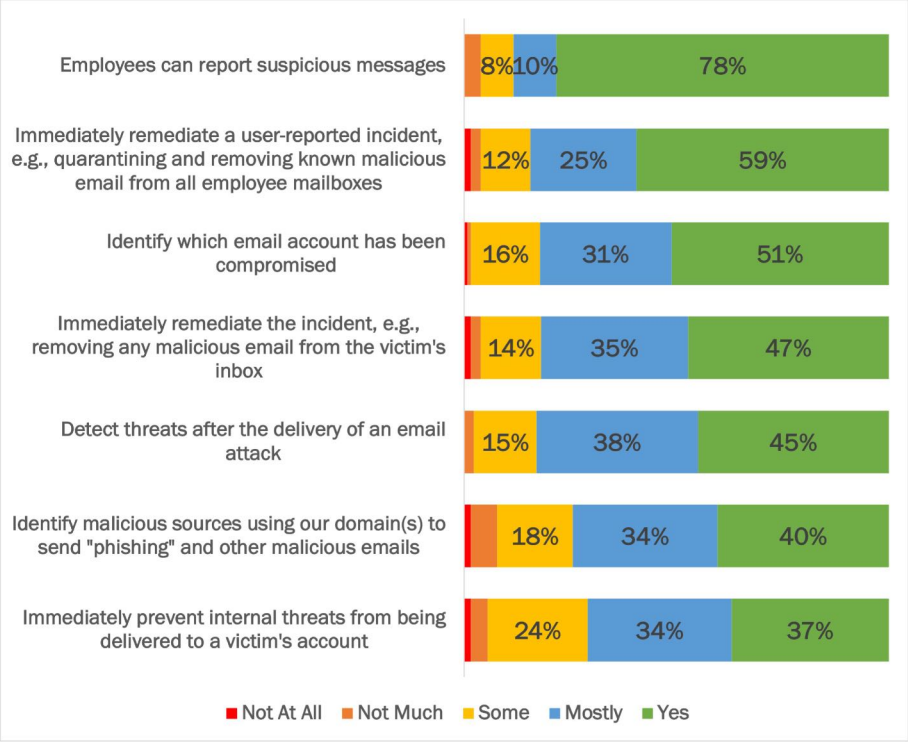
- **Phishing Attacks by Email vs. Two Other Types**
  Organizations have better capabilities to stop phishing attacks reaching end users via email than by other channels (e.g., social media) and against third parties using domain spoofing. The email channel is a common and well-established attack vector while the other two are newer and less well known as vectors. Organizations have a game of catchup to play with non-email phishing.
- **Getting Worse on Phishing vs. Ransomware**
  Respondents indicated the collection of threats about phishing had gotten worse by twice as much as the collection of ransomware threats. Phishing remains a significant challenge because it works for cybercriminals. As attack methods morph, being unable to mitigate new attack variants elevates risk of downstream impacts for organizations.
- **Unchanged Is Not a Good Result Either**
  An average of one third of respondents said the ability of their organization to deal with the nine threat types was unchanged. This is not a good result, because many organizations were unprepared three years ago and cybercriminals are better prepared and more equipped today than three years ago. Organizational capabilities may have stood still; cybercriminals have not.

Organizational capabilities may have stood still for one third of respondents over the past three years, but not so for cybercriminals.

CAPABILITIES TO HANDLE DIFFERENT TYPES OF THREATS

When an attack is underway, the ability to respond quickly can be the difference between a mitigated attack and an incident that gets written up in the newspapers. Organizations can make use of a variety of approaches to mitigate threats, including employees reporting suspicious messages, post-delivery threat detection, and removal of suspicious messages from mailboxes. See Figure 13.

Figure 13
Capabilities to Handle Threats
Percentage of Respondents



Source: Osterman Research (2021)

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

Key takeaways from the research are:

- **High Availability of the Simple Option**
  In our research, 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 by clicking a button in their email client.
- **Mid-Range Availability of Post-Compromise Options**
  Roughly half of respondents in our research 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 mostly available.

- **Lowest Availability of Capabilities for Internal and External Threat Discovery**
  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 difficult to identify, because the message and content come from within the system rather than from outside. External threats that use spoofing, domain impersonation, or lookalike domains often do not even touch the organization's email infrastructure. DMARC and additional brand protection solutions, like Passive DNS, are necessary for discovery of these external-only threats.

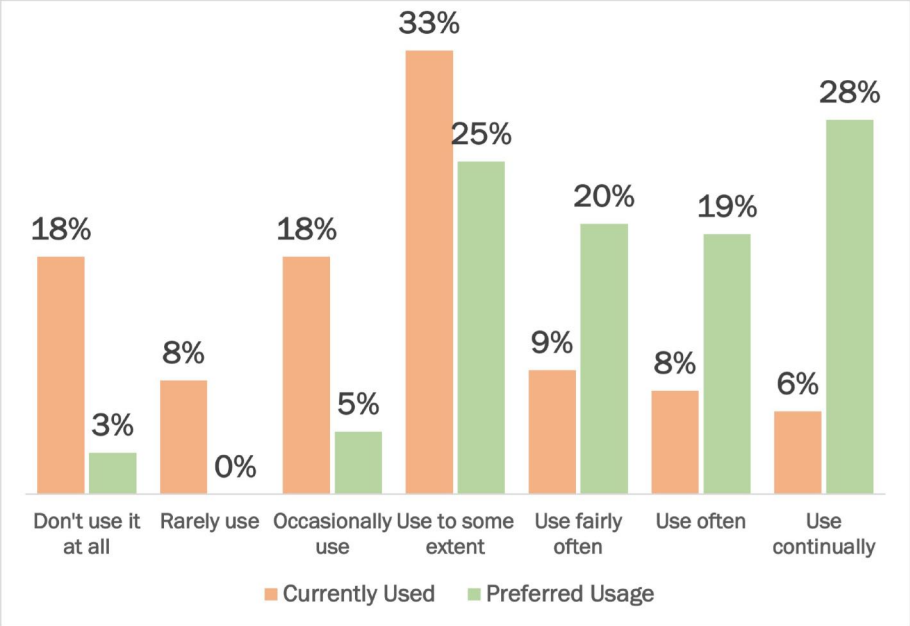
SCOPE TO USE MORE AI AND ML

Artificial intelligence (AI) and machine learning (ML) security technologies offer the prospect of greater capabilities to detect, triage, and mitigate security threats, and to prioritize high-impact incidents for investigation by an IT security analyst. In our research, respondents reported a mismatch between current and preferred patterns of AI/ML usage—respondents wanted much more use of AI/ML than currently deployed. See Figure 14. Specifically:

- **Current Usage**
  77% of respondents said AI/ML are 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.

Respondents reported a mismatch between current and preferred patterns of AI/ML usage.

Figure 14
Extent of AI and ML Usage Currently and Preferred
Percentage of Respondents



Source: Osterman Research (2021)

REASONS TO BE A THREAT ACTOR

Cybercriminals continue to leverage phishing and ransomware attacks because they work. Phishing attacks that result in compromised credentials provide high-reputation sending infrastructure, avenues for business email compromise, or footholds for ransomware attacks. Modern ransomware attacks that combine encryption and extortion are resulting in high payouts to cybercriminals—which one study pegged at $350 million in 2020.[10] But the context is ripe too, for example:

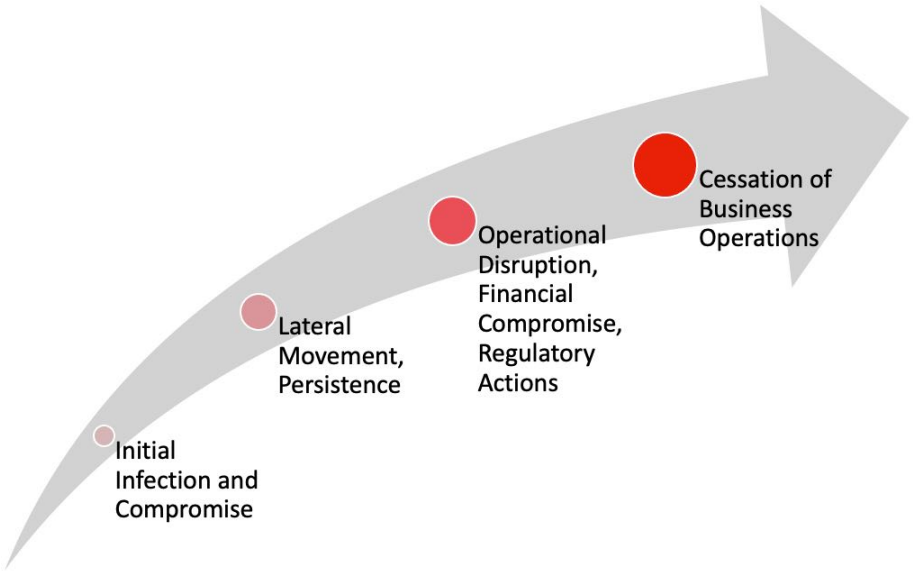
- **Organizations are Unprepared and Poorly Secured**
  Many organizations lack the technology, people, and process defenses to stop cyberattacks. While the situation is improving, many attack vectors remain unsecured and new attack vectors are regularly being developed.
- **People are Rushed, Busy and Distracted**
  Being rushed, busy and distracted creates a context ripe for making mistakes and misjudging intent. Working remotely from early 2020 pushed all interaction to digital channels, removing in-person options for confirming requests and judging veracity.

THE FLOW-ON RISKS OF PHISHING AND RANSOMWARE

The risk of phishing and ransomware begins with an initial infection and compromise, but it does not stop there. It is the subsequent and increasing risks—such as the risk of operational disruption and financial compromise, or the risk of cessation of business operations—that represent the more significant consequences from these two attack vectors. See Figure 15.

Cybercriminals continue to leverage phishing and ransomware attacks because they work.

Figure 15
Reducing the Risks of Phishing and Ransomware
The risks posed by phishing and ransomware increase in consequential impact the longer they are left unaddressed to fester



Source: Osterman Research (2021)

Threat Forecast

Our forecast for the threat context over the next several years is that:

- **Phishing Continues**
  The threat of phishing is not going to diminish. It is too easy, too successful, and too lucrative an attack pattern for cybercriminals to cease usage. It leads to many second-order effects that are highly valued by threat actors, such as credential compromise, avenues for BEC attacks, and espionage opportunities. Microsoft 365 customers will continue to be under attack, because the service aggregates access to email, document sharing, team collaboration, business intelligence and other data repositories behind a single credential.
- **Ransomware Intensifies**
  There is still a lot of scope for ransomware to become a larger problem. The growing reliance on cyber insurance to cover ransom demands encourages threat actors to attack again, and if organizations are ill-prepared the first time to defend against an attack, they may be ill-prepared the second and third times too (a serial infection attack pattern). Until the business model of ransomware and extortion is disrupted, ransomware is an enduring threat that organizations will have to defend against.
- **Targeted and Timed for Maximum (Devastating) Effect**
  Over the past year, ransomware gangs have focused on specific vulnerable targets and timed attacks in order to cause maximum disruption. By doing so, they hope to increase the odds of receiving a quick financial payoff. Attacks that hit outside of working hours, just before a major holiday weekend, or the day before the school year starts all greatly increase the social pressure for a quick resolution. We expect to see the use of these guerrilla-warfare tactics to continue, adding anticipatory stress to IT teams already under duress.

Cybercriminals are not resting on past wins.

Finally, as we said in one of our recent reports, cybercriminals are not resting on past wins. They are actively seeking new vulnerabilities, new attack vectors, and new ways of both compromising sensitive data and earning a financial payoff. Threat methods are getting more sophisticated and difficult to detect.[11]

Solutions for Phishing and Ransomware

This section outlines a range of solutions reducing the initial and subsequent risks posed by phishing and ransomware.

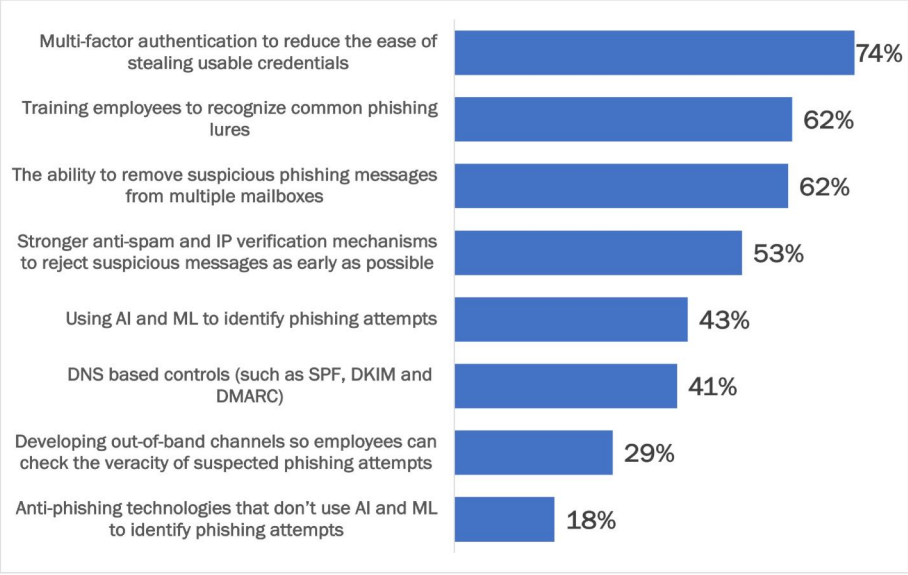
EFFECTIVE PHISHING MITIGATIONS

Respondents indicated the phishing mitigations they found most effective, with four mitigations ranked as mostly or highly effective by more than half of the respondents. See Figure 16. The three mitigations with the highest ratings were:

- **Multi-Factor Authentication (74%)**
  Multi-factor authentication (MFA) to reduce the ease of stealing usable credentials was ranked as the most effective mitigation by 74% of respondents in our research. When MFA is in use, even if a victim enters their credentials for the cybercriminal to harvest, the presence of the MFA demand renders usage of the compromised credentials much more difficult. While phishing may still result in compromised credentials, MFA reduces the consequential impact.
- **Security Awareness Training (62%)**
  Training employees to recognize common phishing lures was the mitigation with the second highest effectiveness rating, by just over 62% of respondents. When people have the ability to discern when something about a message doesn't seem quite right, or to recognize common phishing attack patterns, a successful phishing attack is harder to execute.
- **Removal of Phishing Messages from Mailboxes (62%)**
  The ability to remove suspicious phishing messages from multiple mailboxes was the third highest ranked mitigation, by just under 62% of respondents. When the first few instances of a phishing message are activated or questioned—which happens within minutes of the message being delivered—the ability to remove every other copy of the message decreases the available threat space.

Multi-factor authentication (MFA) to reduce the ease of stealing usable credentials was ranked as the most effective mitigation by 74% of respondents in our research.

Figure 16
Effectiveness of Phishing Mitigations
Percentage Responding "Mostly Effective" or "Highly Effective"



Source: Osterman Research (2021)

The ranking of the two options for AI and ML in identifying phishing attempts is interesting. Anti-phishing technologies that do use AI/ML were ranked as being almost two-and-a-half times more effective than technologies not using AI/ML.

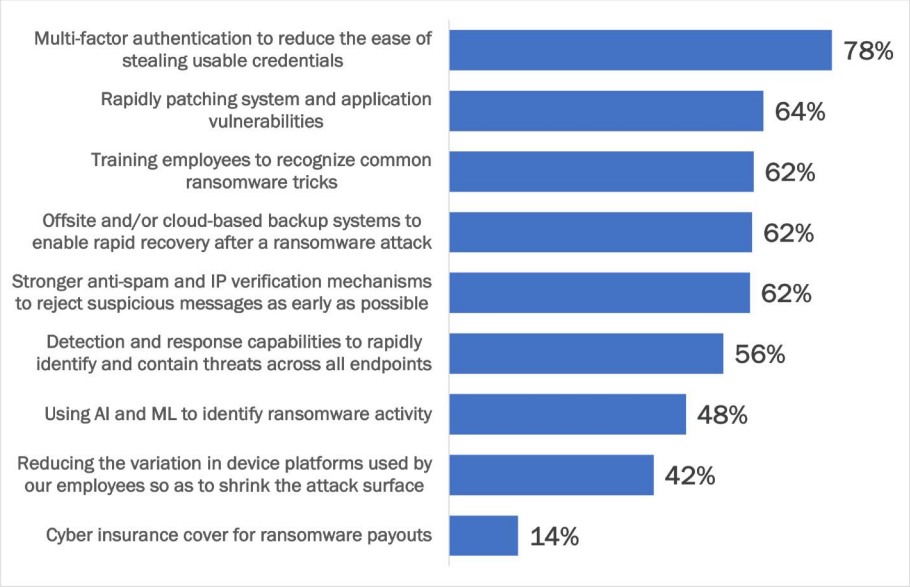
EFFECTIVE RANSOMWARE MITIGATIONS

Respondents found a range of mitigations to be more effective than others in addressing the risks of ransomware (Figure 17). The top-ranked mitigations were:

- **Multi-Factor Authentication (78%) and Security Awareness Training (62%)**
  MFA and security awareness training ranked in first and third place respectively. These were also ranked highly for phishing mitigations.
- **Rapid Patching of Vulnerabilities (64%)**
  Software and application vulnerabilities are often targeted by ransomware operators, as they offer a foothold into a device or network. Rapid patching reduces the undefended areas, decreasing the likelihood of attack susceptibility. Respondents ranked rapid patching as the second most effective mitigation in decreasing the risks of ransomware.
- **Offsite or Cloud Backup (62%)**
  Offsite or cloud backup services provide the ability to recover data encrypted by a ransomware attack and thus assure operational continuity. Backups must be protected from ransomware infection. While backups can restore data, they can do nothing about the extortion element of modern ransomware attacks.
- **Stronger Anti-Spam and IP Verification Mechanisms (62%)**
  Anti-spam and IP verification mechanisms aim to eliminate suspicious messages from reaching end users, by sanitizing the inbound message flow.

Rapid patching reduces the undefended areas of devices and networks, decreasing the likelihood of attack susceptibility.

Figure 17
Effectiveness of Ransomware Mitigations
Percentage Responding "Mostly Effective" or "Highly Effective"



Source: Osterman Research (2021)

Cyber insurance cover was ranked effective by the fewest number of respondents (14%). Such cover can provide an immediate resolution to an incident, but the money spent on cyber insurance doesn't directly elevate the security posture of an organization. Other mitigations in addressing ransomware present their own form of insurance (risk reduction), which can greatly reduce the likelihood of an impactful incident, and thus the extent of cyber insurance coverage required.

MULTI-FACTOR AUTHENTICATION

MFA was rated as the most effective mitigation against both phishing and ransomware in our research. Without MFA protections in place, phishing attacks that result in credential compromise hand a threat actor the key to the door. It is an open invitation to walk in, take whatever they want, and stay or leave at their whim. MFA increases the difficulty level in successfully leveraging compromised credentials, because a compromised username and password are no longer enough on their own. It is similar to having an alarm system just inside the door, a guard dog patrolling the premises, or a security guard performing additional checks on whomever walks in the door. In the same way that there are options for how physical premises are safeguarded beyond a lock, there are options for MFA too:

- **Phone or Email Based**
  MFA via SMS or an email address are comparatively weak forms 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 harder 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 (as well as 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 strongest identity assurance of the person seeking access to a system. Anyone having access to financial systems, employee records, patient data, and other systems that contain commercially and personally sensitive data should be using as strong a form of MFA as possible.

The strongest forms of MFA currently available are FIDO2-based security tokens that rely on public key encryption, and biometric authentication approaches.

SECURITY AWARENESS TRAINING

Security awareness training offers a structured method for increasing the non-technological security defenses of an organization by activating the people under attack to recognize suspicious, malicious and fictitious activity. Employees, managers and executives are informed of common phishing and ransomware tactics to be wary of, traps to avoid, and the support channels available when something doesn't feel right in a new message, such as escalation to the help desk. Executives receive targeted training given the elevated risks of being a known executive, and likewise for people holding roles that are commonly attacked, such as finance and HR professionals. Organizations hold an increasing responsibility for protecting data and processes from compromise and people play an essential role in this. In one recent case of business email compromise, the affected staff member was acquitted of wrongdoing in part because the organization had not provided sufficient staff training on detecting and dealing with BEC scams.[13]

The "training" sense 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 that is embedded in the flow of daily interactions reinforces the concepts of security awareness training within the context and content facing employees. Just as IT security professionals need solutions that multiply their capabilities (see below), so do regular employees on the front line of security attacks. Visual alerts in email messages to highlight the existence of red flags from a technology perspective multiplies and extends what employees are able to do. Examples include alerts that a given message from a named individual is now coming from a different email address, or 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 before. Such in-line coaching helps to create a culture of security.

The efficacy of security awareness training can be improved by analyzing and acting on actual behavioral data on people in an organization, for example, how individuals respond to simulated phishing, spearphishing or BEC attacks. Individuals—and groups, even—who consistently fail to recognize the warning signs in simulated attacks can be targeted for further training and coaching, process and policy changes, and added security precautions (e.g., stronger forms of multi-factor authentication). Actual behavioral data closes the loop on training as an input and behavior change as an outcome.

In our research, respondents acknowledged the joint roles of security awareness training and technology-based solutions in reducing the risks of phishing and ransomware. See Figure 18.

Organizations hold an increasing responsibility for protecting data and processes from compromise and people play an essential role in this.

Figure 18
The Role of Security Awareness Training vs. Technology-Based Solutions
Percentage of Respondents

Source: Osterman Research (2021)

Of particular note:

- **Little Trust in the Exclusive Options**
  Very few respondents chose the extremes of the continuum—that any of the security threats mentioned could be solved completely with either training alone or technology-based solutions alone. Only 1% or 2% of respondents selected either of these options for the six security threats listed, except for email domain impersonation, where 5% of respondents believed technology alone could solve the problem.
- **About Half for Equally Important**
  Across the six security threats listed, an average of 52% of respondents said that training and technology-based solutions were equally important.
- **Three More About Training**
  Respondents said phishing, BEC and spearphishing were more about training than technology-based solutions—at 35%, 27%, and 37% respectively. These attacks leverage social engineering tricks more than technology obfuscation, and thus activating human awareness and a healthy dose of skepticism is an effective mitigation. In counteracting social engineering attacks, humans have a contextual awareness that technology solutions often cannot see.
- **Three More About Technology**
  In contrast, respondents in our research said account takeovers (35%), ransomware infections (38%), and email domain impersonation (42%) had more to do with technology-based solutions than training. These attacks often use hidden code, obfuscated email headers, and other invisible attributes in execution, events that technology can detect and defend against faster and more effectively than people can.

Respondents said phishing, BEC and spearphishing were more about training than technology-based solutions. In contrast, the others were more about technology-based solutions.

ASSURE EMAIL AUTHENTICATION TECHNIQUES

Ensure your email infrastructure is properly configured to minimize impersonation, spoofing and usage for phishing attacks against other organizations. Three basic controls to increase the authenticity of email are SPF, DKIM and DMARC.

- SPF (Sender Policy Framework) uses DNS records to define which email hosts are trusted to send email for a given domain. Receiving email servers can reject incoming email if the traffic originates from non-trusted sources.
- DKIM (DomainKeys Identified Mail) uses public-private key cryptography to sign messages originating from a given email domain. Receiving email servers can check the validity of the key in order to rejected spoofed messages.
- DMARC (Domain-based Message Authentication, Reporting and Conformance) ties together and extends the protections offered by SPF and DKIM to specify what organizations should do when receiving email messages with suspicious authentication attributes. Once an organization has visibility into and control over which sending infrastructures are permitted to use the domains owned by the organization, a policy can be established that receiving organizations can reference when deciding whether to ignore, quarantine or entirely reject any message that does not line up. DMARC includes reporting options to highlight unrecognized traffic, which can be used to distinguish between fraudulent message flows and trusted third parties that need to be included in the email configuration (e.g., when a marketing firm is sending on your behalf).

Making changes to SPF, DKIM and DMARC normally requires updating DNS records, but there are newer and more dynamic approaches that simplify the configuration.

ENDPOINT SECURITY, VISIBILITY AND RESPONSE

Open, unsecured remote desktop ports have been implicated as a key root cause for ransomware attacks in many previous incidents. Having a standing policy that all such ports are either disabled or tightly controlled reduces the risk of initial device compromise, lateral movement, and subsequent ransomware activity. Solutions that provide detailed profiling of all endpoints, including the status of remote desktop ports, enable centralized oversight and control without having to physically touch any endpoint—which, clearly, has become ever more difficult in this age of remote working, and more complicated due to the growing variability in endpoint devices as distributed purchasing patterns replace corporate-wide policies that previously constrained vendor choice.

Endpoint Detection and Response (EDR) solutions enable detailed profiling of application versions, in-process incidents and endpoint estate-wide reporting on where similar weaknesses and vulnerabilities may exist. IT security professionals can mitigate incidents directly on compromised endpoints, and then scale out the mitigations across other endpoints to close newly identified vulnerabilities and reduce the attack surface.

BEYOND EDR TO EXTENDED DETECTION AND RESPONSE (XDR)

What EDR does solely for endpoints, XDR extends to other parts of the computing infrastructure—adding signals and analysis encapsulating the email sending and receiving infrastructure, servers, cloud services and applications, and network devices, among others. XDR aggregates threat signals and provides visibility into and prioritization of emerging threat vectors across the breadth of infrastructure and security services in use. The analysis capabilities of XDR incorporate threat intelligence to uncover connections between individual threat events so as to build insight into cross-infrastructure security threats that would be missed by using point solutions only.

What EDR does solely for endpoints, XDR extends to other parts of the computing infrastructure.

CLOUD-BASED BACKUP SERVICES

Cloud-based backup services that are sufficiently secured so as to avoid compromise by a ransomware attack reduce the risk that a ransomware attack will be successful by offering an unencrypted copy of data for restoration to operational systems. It reduces the risk of ransomware by enabling data recovery in two specific instances:

- When the ransom and/or extortion demand is paid but the threat actor does not supply the decryption key. In such a case, the payment would have been motivated by neutralizing the extortion aspect of publishing or selling the exfiltrated data more than the ransom one for encrypted data since the organization already had a secured copy for recovery; or
- When the ransom and/or extortion demand is not paid.

When ransomware gangs relied on encryption only for operational disruption, the value of cloud-based backup services in reducing the risk of ransomware was very clear. With ransomware gangs embracing modern criminal business models that combine encryption (for operational disruption), extortion (by threatening publication or sale of exfiltrated data), and exposure (to regulatory actions due to insufficient data protection mechanisms), cloud-based backup services continue to address the operational disruption aspect but not the newer ones.

SOLUTIONS THAT MULTIPLY CAPABILITY

The global shortage of trained cybersecurity professionals means that most organizations need to leverage solutions that multiply the capability of in-house IT security professionals. Such solutions automate, simplify, outsource or otherwise enhance the work done by internal IT staff. Examples include:

- **Managed Security Services for Incident Response**
  Few organizations can afford to have every security risk covered through in-house IT security professionals. While ransomware, in particular, is a critical threat to organizational operations and continuity, the occurrence of actual ransomware incidents is hopefully few and far between. Hence, employing dedicated ransomware incident response professionals for such low-frequency incidents is imprudent. Managed security services provide a strong alternative, offering access to IT security professionals who deal with and address the costs and fallout of a ransomware incident on a higher frequency across multiple client organizations.
- **Monitoring and Alerting on Abnormal Patterns**
  Monitoring systems that track access attempts by identity can alert people to abnormal authentication patterns to give early warning of credential compromise following a phishing attack, or of out-of-the-ordinary file download behaviors by individuals compared to an established baseline for the individual or a related group. For example, an alert can be raised automatically when the same credentials are used in two different countries at almost the same time, indicating a high likelihood of credential compromise due to the impossibility of travel required by one person to physically do so. Cloud Access Security Brokers (CASBs) usually include these types of alerting rules for an organization's cloud infrastructure, and User and Entity Behavioral Analytics (UEBA) solutions create behavioral baselines against which subsequent activity is compared. Such tools make commonplace what is impossible for an IT security professional to track any other way.
- **Vulnerability Analysis, Automated Patching, and Virtual Patching**
  In cases where a vulnerability is detected before a vendor is able to release a patch, some solutions use virtual patching to safeguard against malicious exploits. This is particularly valuable with legacy or older software that is patched infrequently or is out of support with no further patches coming from the vendor. While we recommend against retaining such legacy or older software, there are cases where it is impractical or impossible to do anything but stay with what is being used. But in such cases, network isolation and virtual patching through an application firewall are consequentially critical.
- **Threat Intelligence Services**
  Not all organizations are targeted simultaneously by new attacks or threats, but visibility into how threats are changing elsewhere provides early warnings of possible impending attacks, and an opportunity to proactively strengthen and safeguard defenses. Threat intelligence services aggregate and summarize threat signals across a wide collection of organizations, to both inform IT security analysts of new happenings and also to distribute protection updates to security solutions. Such services create leverage for in-house security teams because they do not have to endure every attack themselves. Threat intelligence data, including IP and domain reputation, provides automatic protection against the latest observed global threats. Reputation data can be applied to email and DNS infrastructure, with added protection against targeted threats through enhanced data sharing.

Leverage solutions that multiply the capability of in-house IT security professionals.

Best Practices

Solutions to reduce the risk of phishing and ransomware are best when they are complemented with good practice. Best practices to embrace are:

- **Focus on Significant Root Causes**
  Focus attention on the significant root causes of compromise, using a risk-based approach to deal with and address the most damaging threats. Phishing is a very common and disruptive initial threat vector and reducing the count and variety of phishing threats that reach end users is a good pathway to pursue. Ditto for resolving software and application vulnerabilities as promptly as possible.
- **Improve Authentication Hygiene**
  If usernames and passwords are still in use, ensure they are used with as many safeguards as possible. A password manager is better than writing passwords in a book. Having different passwords for each service or application is better than using duplicated but disconnected credentials across multiple services. Using a separate personal email address for personal services is better than using a corporate one. Tracking credential breaches as a consequence of third-party data breaches is better than being blindsided by a data breach of your own. Having recovery email addresses up to date is better than not having any set at all. Stronger authentication mechanisms that move away from passwords should be explored, including passwordless authentication that relies on public key cryptography and biometrics. Conditional access policies that look at additional attributes of an authentication attempt beyond the credentials themselves can prevent unauthorized access from unsanitary networks.
- **Think Together, Not Alone**
  Reducing the risk of phishing and ransomware requires a "together" approach combining people, process and technology factors. None of these factors alone will achieve what the factors working in sync can do. Training in security awareness and performing ongoing testing of training efficacy is important, but so are processes for escalating threats and responding to incidents, along with the technology solutions to reduce the attack surface, mitigate phishing attempts, and suppress ransomware activities as early as possible.
- **Do Not Wait to Start**
  Do not wait for a data breach, malware infection or ransomware incident to occur before developing an incident response plan. Do the work now to put the pieces in place and line up the support agreements you are likely to need. If your organization will need to work with the FBI, a data protection supervisory authority, or other national cybersecurity agency, get those relationships underway and established. If you will want support from a managed services provider, get the agreements signed and in place. Each of these external agencies and organizations is likely to have anti-phishing and anti-ransomware recommendations that will decrease the likelihood of an incident, and anything they have to offer to harden your defenses and decrease the attack surface is worth investigating.

Do not wait for a data breach, malware infection or ransomware incident to occur before developing an incident response plan.

- **Make It Harder for Yourself**
  Seek external verification for the cybersecurity readiness and security posture of your organization and put in place accountability measures to ensure an ongoing focus on security. Cyber insurance cover, for example, requires assessments of current security practices, and improving current practices reduces premium rates. Reporting regularly to the Board of Directors on cybersecurity readiness, rates of phishing and ransomware attacks within the organization, and roadblocks to effective mitigations will elevate the attention paid to the area, particularly if the CISO or equivalent for your organization is part of the board. Proactive testing of defenses and probing for weaknesses—either through an internal attack team or external white-hat hackers—gives an elevated confidence rating that appropriate controls are in place.
- **Create a Security-Minded Culture**
  Ensure there is a corporate culture that supports challenges to senior management. For example, an HR clerk who receives an email request from the CEO to send sensitive tax information should feel sufficiently comfortable in asking the CEO if the request is valid. If such questions cannot be asked, BEC scams and other data breaches will continue.

Summary

Phishing and ransomware are significant problems for all organizations, raising business risks that range from credential theft to business closure. Given the torrent of attacks unleashed on organizations, the riskiest approach is to do nothing. At minimum review and confirm the efficacy of your current security strategy, and strengthen defenses where weaknesses exist or where new threat vectors are emerging.

This research has highlighted the value of multi-factor authentication, security awareness training, rapid patching of vulnerabilities, and other solutions for reducing the business risks of phishing and ransomware. These solutions must be complemented with strong best practices, such as focusing on root causes.

Seek external verification for the cybersecurity readiness and security posture of your organization.

Sponsored by Mimecast

Mimecast: Relentless protection. Resilient world.™

Mimecast (NASDAQ: MIME) was born in 2003 with a focus on delivering relentless protection. Each day, we take on cyber disruption for our tens of thousands of customers around the globe; always putting them first, and never giving up on tackling their biggest security challenges together. We are the company that built an intentional and scalable design ideology that solves the number one cyberattack vector – email. We continuously invest to thoughtfully integrate brand protection, security awareness training, web security, compliance and other essential capabilities. Mimecast is here to help protect large and small organizations from malicious activity, human error and technology failure; and to lead the movement toward building a more resilient world.

Learn more about us at www.mimecast.com.

www.mimecast.com

@mimecast

UK/EUROPE
+44 (0) 207 847 8700
info@mimecast.com

NORTH AMERICA
+1 800 660 1194
+1 781 996 5340
info@mimecast.com

SOUTH AFRICA
+27 (0) 117 223 700
0861 114 063
info@mimecast.co.za

AUSTRALIA
+61 3 9017 5101
1300 307 318
info@mimecast.co.au

---

[1] Security Magazine, Ransomware Victim Travelex Forced into Bankruptcy, August 2020, at https://www.securitymagazine.com/articles/93062-ransomware-vicitim-travelex-forced-into-bankruptcy
[2] Caleb Boma, Ransomware Attack Forces Therapy Institution Into Bankruptcy, February 2021, at https://www.speartip.com/resources/attack-forces-institution-into-bankruptcy/
[3] World Economic Forum, The Global Risks Report 2021, January 2021, at https://www.weforum.org/reports/the-global-risks-report-2021
[4] Osterman Research, New Methods for Solving Phishing, Business Email Compromise, Account Takeovers and Other Security Threats, August 2019, at https://ostermanresearch.com/2019/08/20/orwp_0314/
[5] Simon Chandler, Google Registers Record Two Million Phishing Websites in 2020, November 2020, at https://www.forbes.com/sites/simonchandler/2020/11/25/google-registers-record-two-million-phishing-websites-in-2020/
[6] Lily Hay Newman, Hack Brief: How to Check Your Computer for Asus Update Malware, March 2019, at https://www.wired.com/story/asus-software-update-hack/
[7] Tara Seals, Singtel Suffers Zero-Day Cyberattack, Damage Unknown, February 2021, at https://threatpost.com/singtel-zero-day-cyberattack/163938/
[8] Help Net Security, Combat Complexity to Prevent Cybersecurity Fatigue, February 2020, at https://www.helpnetsecurity.com/2020/02/26/combat-cybersecurity-complexity/
[9] Help Net Security, Cybersecurity Professionals are Outgunned and Burned Out, June 2019, at https://www.helpnetsecurity.com/2019/06/28/cybersecurity-burnout/
[10] Robert Lemos, Ransomware Payoffs Surge by 311% to Nearly $350 Million, January 2021, at https://www.darkreading.com/vulnerabilities---threats/ransomware-payoffs-surge-by-311--to-nearly-$350-million/d/d-id/1340017
[11] Osterman Research, Better Ways to Deal with New Security Threats, October 2020, at https://ostermanresearch.com/2020/10/30/orwp_0333/
[12] Catalin Cimpanu, FBI Warns About Attacks That Bypass Multi-Factor Authentication (MFA), October 2019, at https://www.zdnet.com/article/fbi-warns-about-attacks-that-bypass-multi-factor-authentication-mfa/
[13] Fair Work Commission, Kylie Smith v Bank of Queensland Ltd [2021], January 2021, at http://www8.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/FWC/2021/4.html