Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **August 2019**
Sponsored by **Zix**

New Methods for Solving Phishing, Business Email Compromise, Account Takeovers and Other Security Threats

Executive Summary

The "network perimeter" today is almost non-existent. Almost all organizations operate a large and growing number of cloud services for mission-critical and non-mission-critical purposes, sometimes just at a departmental level (one source estimates that there are nearly 1,200 cloud services in use in the typical large enterprise and that the vast majority of these are not "enterprise-ready"[i].) Mobile devices – many employee-owned – are regularly used to access corporate data resources and sensitive data assets. These devices typically contain a large number of apps, many of which can be exploited to steal login credentials and other sensitive information. IoT devices are now commonplace and the number of these devices in the workplace is skyrocketing, employees continue to use conventional endpoint devices like desktop and laptop computers, and the "Bring Your Own" trend has expanded from personally-owned and managed devices (BYOD) to personally-owned and managed cloud, mobile and desktop/laptop applications of many types.

In short, the network in most organizations has a dramatically expanded attack surface. There is no longer a defensible perimeter that can fully protect corporate data, and so new approaches, technologies and practices are needed to protect corporate data and finances.

KEY TAKEAWAYS

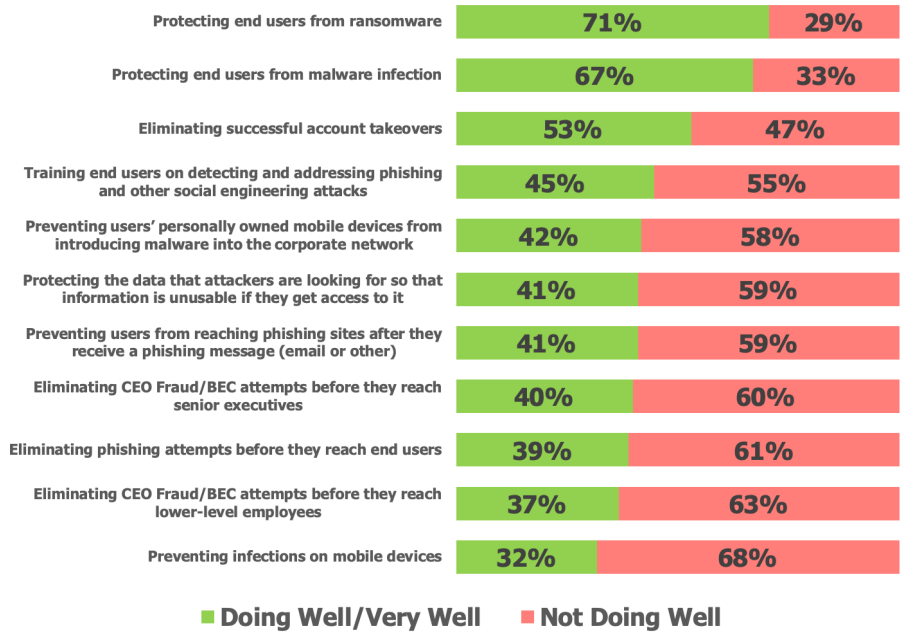
Osterman Research conducted an in-depth survey of security-focused professionals specifically for this white paper. Here are the key takeaways from the research:

- Eighty-one percent of organizations have reported being the victim of some type of data breach, targeted email attack, successful phishing attack or other security incident during the previous 12 months – and the actual number may be a bit higher than that.
- Security decision makers and influencers are concerned about a wide range of issues, but successful phishing attempts, employees unable to recognize phishing and social engineering attacks, and zero-day exploits top the list of concerns.
- The security skills gap is a top-of-mind concern for most security decision makers and influencers: 38 percent believe that the security skills shortage is a "definite" problem for their organization, and another 30 percent consider to be a "very serious" problem.
- There is a significant disconnect between the security tools that are currently in place and what security staffers would like to have in place. Most notably, security teams would like to have more cloud-based tools available, and they would like much greater use of artificial intelligence (AI) and machine learning (ML) capabilities.
- Many of those who influence and make decisions about security issues for their organizations are not confident in their organization's ability to thwart a wide range of security problems. As shown in Figure 1, 29 percent do not believe they are "doing well" at protecting end users from ransomware, 33 percent do not believe they are "doing well" at protecting end users from malware infection, and the problems get worse from there.
- For many organizations, their ability to deal with various threats over the past three years is either not improving or is getting worse. Across five key threat vectors, the average improvement rate is a rather modest 42 percent, while the combined rate of things getting worse or not improving is 58 percent.
- Many organizations lack the ability to deal properly with internal threats. For example, 28 percent of the organizations surveyed do not have the ability to

Eighty-one percent of organizations have reported being the victim of some type of data breach…during the previous 12 months.

identify which email account has been compromised once a threat has been discovered.

Figure 1
Organizational Effectiveness Against Various Security Issues



Source: Osterman Research, Inc.

- Security awareness training is an essential element to bolster the security infrastructure, something with which the vast majority of security decision makers agree. Osterman Research cost modeling has demonstrated that good security awareness training can result in a positive return-on-investment (ROI).

ABOUT THIS WHITE PAPER

This white paper was sponsored by Zix; information about the company is provided at the end of this paper.

Our research found that the vast majority of organizations have experienced some type of security incident.

The Threats That Organizations Face

INCIDENTS THAT HAVE OCCURRED IN THE RECENT PAST

Our research found that the vast majority of organizations have experienced some type of security incident and/or successful infiltration of their corporate security defenses during the past 12 months. As shown in Figure 2, nearly one-third of organizations have experienced an accidental leak of sensitive or confidential information, while nearly as many have experienced a successful Business Email Compromise (BEC) attack or an external phishing attack that installed malware on the corporate network. In fact, only 19 percent of organizations have not reported an occurrence of the problems listed in Figure 2.

Figure 2
Security Incidents That Have Occurred During the Previous 12 Months

Incident	%
Sensitive / confidential info was accidentally leaked through email	30%
An email as part of a CEO Fraud/Business Email Compromise (BEC) attack successfully tricked one or more lower level employees in our organization	29%
An external phishing attack successfully stole user credentials	28%
A phishing attack was successful in infecting systems on our network with malware	24%
A targeted email attack launched from a compromised account successfully stole a user's account credentials	20%
A fileless/malwareless attack reached an endpoint	20%
A targeted email attack launched from a compromised account successfully infected an endpoint with malware	18%
Sensitive / confidential info was accidentally or intentionally leaked through a channel other than email	14%
An email as part of a CEO Fraud/BEC attack successfully tricked one or more senior executives in our organization	13%
A targeted email attack launched from an internal account successfully infected an endpoint or software system	12%
One or more of our systems were successfully infiltrated through a drive-by malware attack from employee web surfing	12%
Malware has infiltrated our internal systems, but we are uncertain through which channel	10%
One or more of our endpoints had files encrypted because of a successful ransomware attack	10%
A targeted email attack launched from an internal account successfully stole a user's account credentials	9%
A targeted email attack was successful in infecting one or more of our senior executives' systems with malware	9%
An unauthorized user successfully accessed a secure database	7%
An account takeover-based email attack was successful	7%
Sensitive / confidential info was intentionally leaked through email	7%
Sensitive / confidential info was accidentally or intentionally leaked through a social media / cloud application	7%
Sensitive / confidential info was accidentally or intentionally leaked, but how it happened is uncertain	4%
None of these things happened	19%

Source: Osterman Research, Inc.

The biggest concerns are phishing attempts that reach end users and employees who fail to recognize phishing and social engineering attacks.

It's important to note that not everyone in an IT security department will be completely forthcoming about every bit of dirty laundry that occurs in their organization. That's not to say that survey respondents aren't telling the truth, but security breaches are often embarrassing incidents that can reveal mistakes that security staffers might have made. Consequently, we believe that the 19 percent figure noted above might be slightly high, and that problems might be a bit worse than they seem.

ISSUES THAT CONCERN DECISION MAKERS THE MOST

The issues that concern security decision makers are varied, but the biggest concerns are phishing attempts that reach end users and employees who fail to recognize phishing and social engineering attacks, as shown in Figure 3. There are a number of other issues about which decision makers are concerned or extremely concerned,

such as zero-day exploits, ransomware attacks, targeted attacks, and compromised login credentials.

Figure 3
Issues About Which Security Teams are Concerned
Percentage Responding "Concerned" or "Extremely Concerned"

Concern	%
Phishing attempts making their way to end users	74%
Employees failing to spot phishing and social engineering attacks	72%
Zero-day exploits	54%
Ransomware attacks successfully infecting endpoints	53%
Targeted attacks	53%
Login credentials being compromised	51%
CEO Fraud/Business Email Compromise attempts making their way to end users	51%
Fileless malware, e.g., rogue browser extensions	49%
Accidental breaches of sensitive or confidential data by employees	49%
Malware getting into your network from employees using the web	49%
Malware other than ransomware successfully infecting endpoints	46%
Malicious breaches of sensitive or confidential data by employees	38%
Command-and-control (C2) callbacks	36%
"Shadow IT" – employees using unauthorized cloud apps and services	32%
Internal threats (threats originating from within your organization)	24%
Spam reaching end users	21%
Cryptocurrency mining malware being installed on your internal PCs or servers	20%
Employees surfing web sites that violate corporate policies (e.g., porn sites, gambling sites, etc.)	18%

Source: Osterman Research, Inc.

It's important to note that the figure above includes both root causes of exploits and the outcomes of those exploits. For example, a phishing attempt that reaches an end user can be the delivery mechanism for the attack that will successfully infect an endpoint with ransomware or some other type of malware.

CREDENTIAL PHISHING IS INCREASINGLY COMMON

Credential phishing is an increasingly common attack vector; if an attacker can secure valid credentials, further concealed attacks can be executed and hidden from sight. Capabilities are necessary to detect near-match spoofing of domain names, because attackers will craft domain options that look similar to a distracted human eye, or even worse, that are hidden completely from display on mobile devices. When internal accounts have been compromised and the message header settings are perfectly valid technically, other non-message header signals must be assessed and correlated in order to identify the attempted fraud. People have higher trust for internal messages from known accounts and known people, and carefully planned internal attacks via compromised accounts are often almost impossible for a recipient to identify.

INTERNAL THREATS ARE A CONCERN

Decision makers are also concerned about various issues related to internal threats. As shown in Figure 4, most are concerned or extremely concerned about negligent or careless employees putting the company at risk. Moreover, nearly one-half of decision makers are concerned about threats delivered because of credential theft, and more than one-third are concerned about malicious or disgruntled employees.

Decision makers are also concerned about various issues related to internal threats.

Figure 4
Concerns About Various Types of Internal Threats
Percentage Responding "Concerned" or "Extremely Concerned"

Type of Internal Threat	%
Negligent/Careless: Employee does not intend to put the company at risk but does so unknowingly.	53%
Imposter: Through credential theft gains access to a corporate account and poses as the identity of the compromised user.	47%
Malicious/Disgruntled: Intentionally exfiltrates data or commits malicious acts, e.g., sending other users infected files.	36%
Collusive: Current employee that knowingly works with an external threat actor to compromise the organization.	22%

Source: Osterman Research, Inc.

THE SKILLS SHORTAGE IS MAKING THE PROBLEM WORSE

The cybersecurity skills shortage is compounding security problems. Because many organizations cannot find or afford a sufficient number of highly skilled security analysts and other security staff members, they often will not have the resources necessary to investigate, analyze and remediate security alerts and the various threats they encounter.

The survey we conducted for this paper found that 38 percent of security-focused decision makers and influencers believe that the security skills shortage is a "definite" problem for their organization, and another 30 percent consider to be a "very serious" problem. Only four percent consider the security skills shortage to be "no problem at all".

The cybersecurity skills shortage is compounding security problems.

SECURITY HAS NOW BECOME A REGULATORY ISSUE

Security breaches have always entailed serious financial, reputational and other consequences, but regulations like the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), are among a growing number of privacy regulations that have made the consequences of security problems much more severe. For example, if a bad actor is able to penetrate the defenses of a company that has not properly protected its sensitive corporate data, such as Personally Identifiable Information (PII) or Protected Health Information (PHI), the company can face enormous financial penalties. Moreover, new privacy regulations and individual requirements within them (such as Article 33 of the GDPR) require reporting of a data breach within 72 hours. Organizations that do not have the ability to detect that they have been breached – let alone understand the cause of the breach and how to remediate it – can run afoul of regulations that require rapid response to breaches and other security issues.

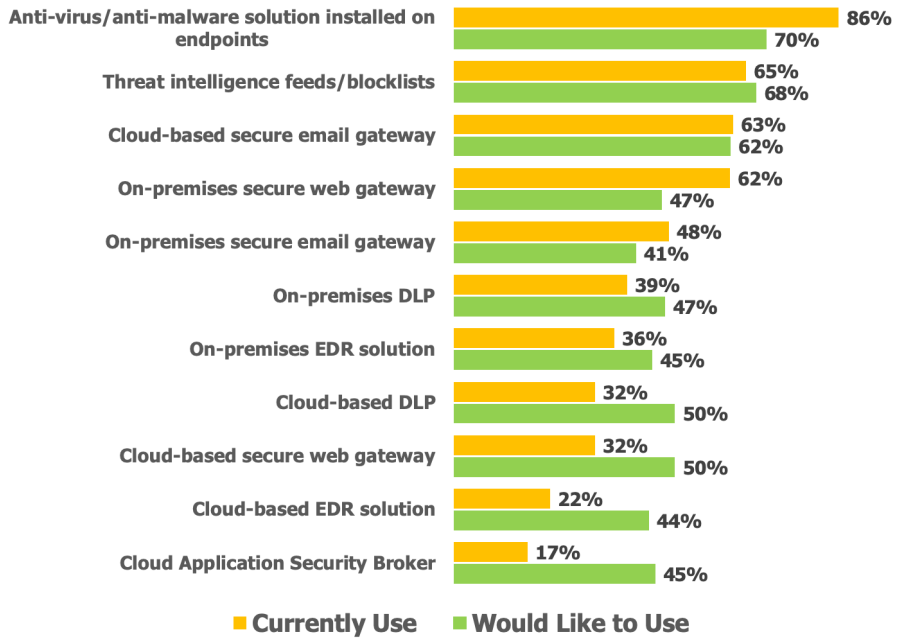
WHAT DOES – AND SHOULD – THE SECURITY INFRASTRUCTURE LOOK LIKE?

Our research found that the vast majority of organizations have deployed endpoint-based anti-virus/anti-malware tools; threat intelligence feeds or blocklists; cloud-based, secure email gateways; and on-premises secure web gateways; among many other solutions, as shown in Figure 5.

However, we also wanted to discover what security decision makers and influencers would like their security infrastructure to look like. What we found, also as shown in Figure 5, is that security staffers would like to deploy many more capabilities than they operate currently. Most notably, these solutions include cloud application security brokers, cloud-based end point detection and response (EDR) solutions, cloud-based secure web gateways, and cloud-based Data Loss Prevention (DLP).

DLP is an essential element of any security infrastructure because of its ability to monitor, detect and block potential exfiltrations of data or violations of corporate policy. For example, a DLP solution can detect and block when malware is attempting to steal sensitive or confidential information, and it can detect when this type of information is being sent outside of an organization in violation of corporate policy (e.g., when someone attempts to send this data without encryption or to a jurisdiction in violation of a privacy policy).

Figure 5
Security Tools That are Currently Used and that Organizations Would Like to Use



Source: Osterman Research, Inc.

Security departments want to move security to the cloud.

The data in the figure above strongly suggest that security departments want to move security to the cloud, they want less emphasis on on-premises secure web and email gateways, and reduced use of endpoint-based anti-virus and anti-malware solutions. Interestingly, the one notable exception is that security decision makers and influencers want more on-premises DLP than they have deployed today.

WILL THE CLOUD INCREASE SECURITY THREATS?

Moving applications and critical data assets to the cloud raises an important question for corporate decision makers: will moving to the cloud improve security or will it actually make things worse? There are two schools of thought on this:

- Security will improve as applications and security capabilities move to the cloud, since specialist security providers are sometimes more adept at managing sophisticated and emerging threats. This is particularly true when comparing cloud security providers to in-house security teams in smaller organizations.

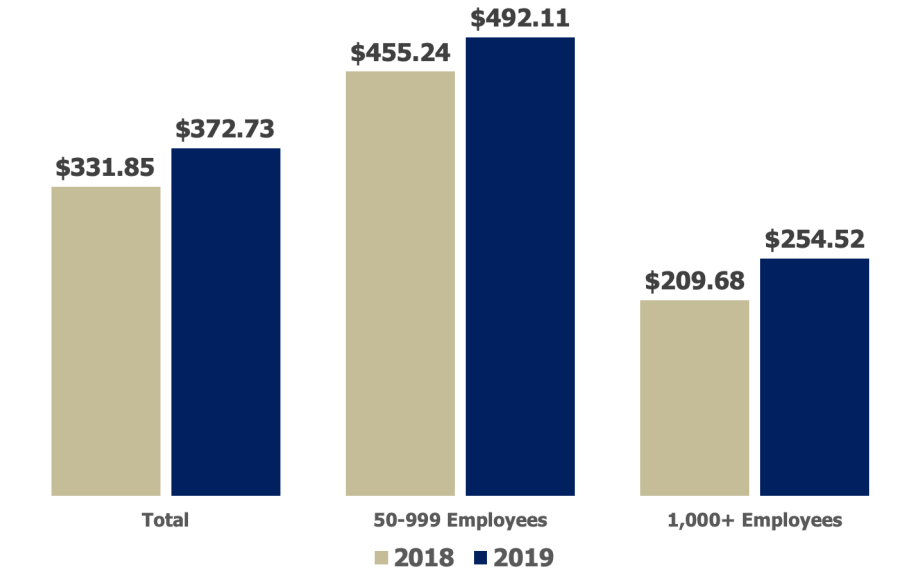
- Security will get worse as more applications move to the cloud. Because each application provider uses a different security model, and because credential theft can be more likely in cloud environments, organizations may become more vulnerable to phishing, BEC, social engineering and other threats.

SECURITY SPENDING IN 2019 VS. 2018

Security budgets vary widely based on a number of factors, including the industry in which an organization participates, the number of employees it has, the geographical distribution of its employees and offices, the risk tolerance of its senior management, and so forth.

We found that for 2018, the mean security budget at the organizations we surveyed was $332 per employee, increasing to $373 per employee in 2019, an increase of 12 percent. However, the per-employee budget at smaller organizations was much higher in 2018 at $455, growing to $492 in 2019, representing an increase of eight percent year-on-year. Larger organizations, owing to the economies of scale that they enjoy, had a mean security budget of $210 per employee in 2018, growing to $255 in 2019, representing an increase of 21 percent, as shown in Figure 6.

Figure 6
Security Budgets per Employee



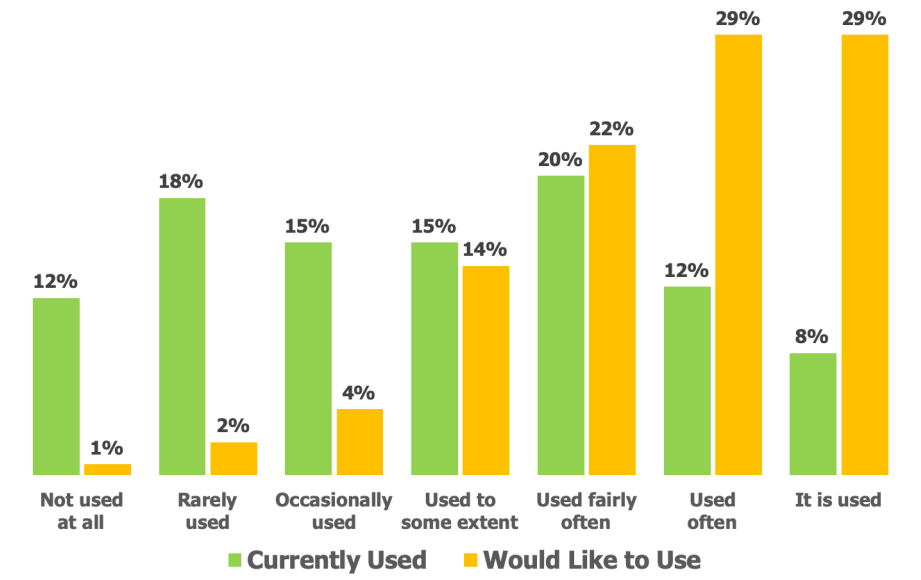
Source: Osterman Research, Inc.

Nearly three in five organ-izations would like to incorporate AI/ML much more than they do today.

SECURITY TEAMS WANT MORE AI, ML

Our research found that security decision makers and influencers do not have security solutions that incorporate AI and ML to any great extent. As shown in Figure 7, one in eight organizations have no AI/ML-enabled security solutions and most of the rest use it only moderately. However, we found that nearly three in five organizations would like to incorporate AI/ML much more than they do today.

Figure 7
Extent to Which AI/ML is Currently Used and Extent to Which Security Teams Would Like to Use It



Source: Osterman Research, Inc.

Why Are Bad Actors So Successful?

CRIMINAL ORGANIZATIONS ARE CAPABLE

Criminals and criminal organizations are typically well funded, they have the technical resources they need to create new and ever more capable attack methods, and they tend to collaborate with one another to share new techniques and processes. Cybercrime is an industry that operates like any other, and its success is due in large part to the fact cybercriminals operate like business professionals[ii].

THREATS ARE DESIGNED TO EVADE MULTI-LAYER DEFENSES

Cybercriminals are successful in large part because many organizations are not carrying out due diligence in addressing the problems of BEC, phishing, spear phishing, ransomware and other threats. For example, many organizations provide no or inadequate security awareness training, so their users are not trained to recognize some of the more common threats. Many don't back up their data so that they can recover from a ransomware attack. Many don't have good security against threats like phishing or spear phishing. Many don't have the internal control processes necessary to enable the recipient of a BEC attempt to verify requests for wire transfers or information. Many have not adequately addressed the problem with Shadow IT, allowing threats to enter through unprotected channels. In short, there are things that organizations can do to protect themselves, but often are not doing.

THERE ARE MORE ACCESS POINTS

Shadow IT, the growing number of approved applications, and the growth of the Internet of Things (IoT) is creating many more entry points that cybercriminals can exploit for activities like malware distribution, phishing, and distributed denial-of-service (DDoS) attacks.

THREATS ARE BECOMING MORE SOPHISTICATED

Bad actors are developing increasingly sophisticated methods to gain access to corporate data, financial assets, networks, etc. Here are some of the methods used by cybercriminals:

Cybercrime is an industry that operates like any other, and its success is due in large part to the fact cybercriminals operate like business professionals.

- Magecart is a data skimming technique in which cybercriminals will use a browser to steal sensitive data from online forms, such as those found on e-commerce sites, travel reservations sites, and other consumer-facing sites. Web-skimming threats, led by Magecart, were a significant threat in 2018 and the threat shows no signs of abating in 2019.

- Cybercriminals attacked mostly Russian Asus laptop users in early 2019 by hijacking a legitimate software update tool to distribute malware that created a backdoor on infected computers. About one million users were targeted and 57,000 users were infected[iii].

- Credential-stuffing is a technique used by cybercriminals in which usernames and passwords gathered from previous breaches are used in automated attacks on other sites. The technique is effective because a large number of users will employ the same login information across multiple sites. One source has found that credential-stuffing tools are effective five percent of the time[iv], and that there were 115 million credential stuffing attacks every day during 2018[v].

- There has been substantial growth in rogue browser extensions serving as malware. Many serve legitimate purposes, but can also serve as "man-in-the-browser" as silent keyloggers, screen scrapers, two-factor authentication interceptors, and data exfiltration. These are very hard to detect because they are part of a trusted browser application, are simple JavaScript and HTML rather than executable, and execute entirely in memory. All of these factors enable them to avoid detection by antivirus and sandboxing technologies.

- As a corollary to the point above, cloud-to-cloud brute force attacks are becoming more common as more organizations migrate key applications to the cloud. These attacks also assume that users commonly employ the same usernames and passwords across multiple accounts, allowing bad actors to focus on high-value accounts[vi].

- There has been a significant increase in PDF-based attacks in 2019. A leading security vendor discovered more than 47,000 new attack variants within PDF files in all of 2018, but discovered 73,000 such attacks in March 2019 alone[vii].

- Given that Microsoft Office is the leading desktop productivity suite, macros continue to be used by bad actors for their exploits[viii]. Some macro-based attacks can launch simply by a user opening a document without giving approval for macros to run. For example, there are vulnerabilities in Excel's equation editor that enable an attack to execute simply by opening a spreadsheet[ix].

- Similarly, hackers often use local Windows tools to infect endpoints, such as PowerShell, Windows Scripting Host and the Windows Management Instrumentation command line once they gain administrator privileges[x].

USERS ARE THE WEAK LINK IN THE CHAIN

Despite enormous investments in technology solutions to stop phishing, ransomware, infiltration of other types of malware, etc., users continue to be the weak link that can often subvert even the most robust of security defenses. They will use personal webmail or insecure mobile apps to access corporate data stores. They will use insecure passwords and not change them regularly. They will click on links in phishing emails or open email attachments without checking the validity of the sender. They can be phished through other digital channels, such as text messages, browser pop-ups, advertisements, etc. Even trained users who are in a rush or distracted can make mistakes. In short, users are often the most insecure part of any security infrastructure.

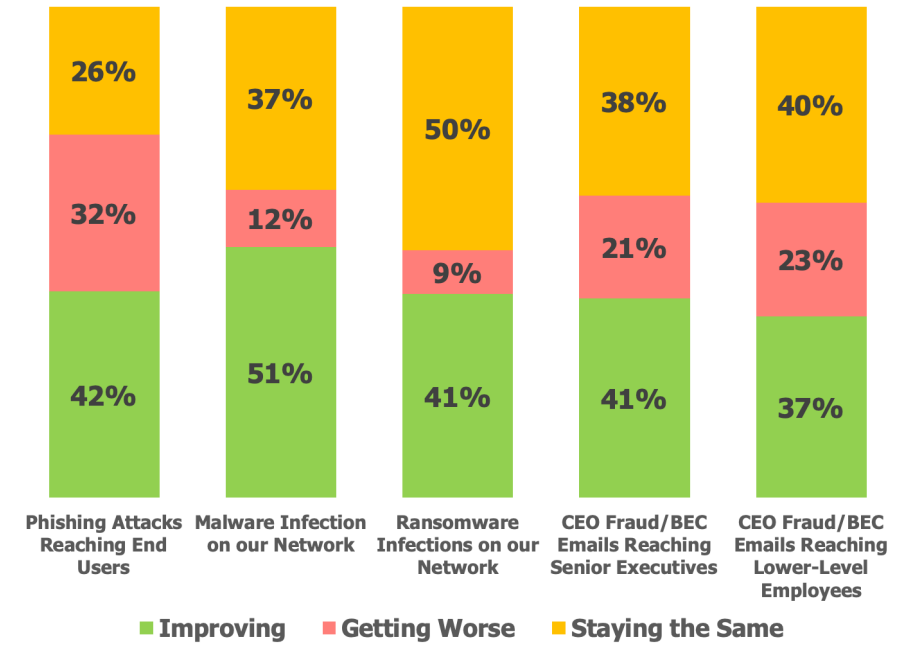
Users continue to be the weak link that can often subvert even the most robust of security defenses.

Security Must Improve

SECURITY IS NOT GETTING BETTER FOR MANY

Obviously, one of the goals of any security investment is improving the catch rate, detection rate, prevention rate, etc. for various types of threats. Our research found both good and bad news: for major threats like phishing emails reaching end users, malware infections, ransomware and the other threats shown in Figure 8, things have been improving for a large proportion of the organizations surveyed over the past three years. In fact, slightly more than one-half of organizations reported that the prevention of malware infections is improving. However, a significant proportion of organizations reported that the problems they're experiencing are actually getting worse over time, and for many things have just not improved. Across the five threats shown in Figure 8, the average improvement rate is a rather modest 42 percent, while the combined rate of things getting worse or not improving is 58 percent. It's important to note that the problems shown in the four rightmost columns of Figure 8 are not mutually exclusive: they are all the result of some type of phishing activity.

Figure 8
Change in the Ability to Deal With Various Threats Over the Past Three Years



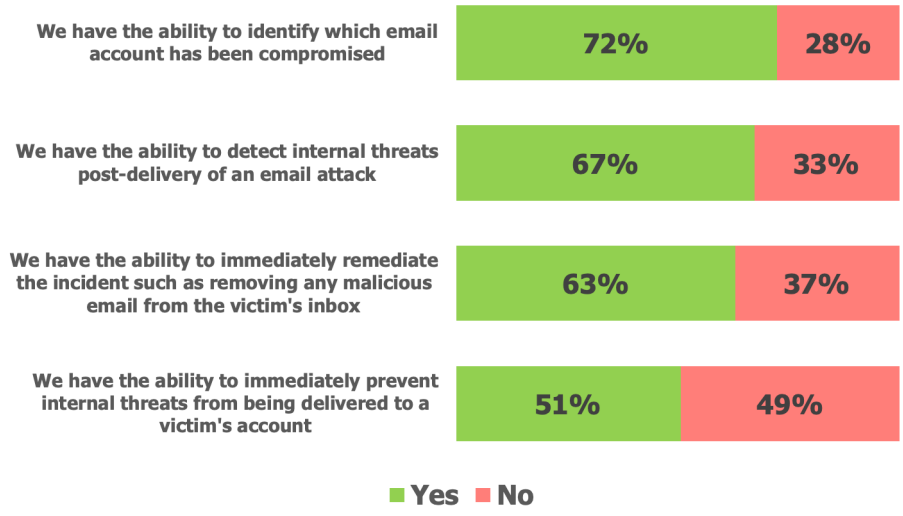
Source: Osterman Research, Inc.

Many organizations are not adequately prepared to address internal threats.

DETECTION OF INTERNAL THREATS IS LACKING

Internal threats are a serious issue and typically account for most of the threats with which security teams must contend. These threats range from successful phishing attempts to social engineering attacks to malicious employee behavior. As shown in Figure 9, many organizations are not adequately prepared to address internal threats because they do not have the necessary tools in place to do so. For example, 28 percent of the organizations surveyed do not have the ability to identify which email account in their organization has been compromised. One-third cannot detect internal threats after the delivery of an email attack. Nearly one-half do not have the ability to prevent internal threats from being delivered to a victim's account. In short, cybercriminals are increasingly successful in carrying out these types of attacks because they are focused on doing so, and because the defenses to prevent them often are not in place.

Figure 9
"For internal threats that use compromised email accounts to launch attacks, do you have a capability for each of the following?"



Source: Osterman Research, Inc.

TRAINING VS. TECHNOLOGY

One of the key issues that many security decision makers deal with is determining the role of technology versus training in the context of preventing various types of threats. Striking the right balance is essential, particularly for threats that do not contain any malware or links to malicious sites, such as BEC attempts. As shown in Figure 10, we found that the vast majority of security decision makers believe that there is a role to play for security awareness training *and* technology-based solutions, although this varies substantially based on the type of threat. For example, while 40-plus percent view phishing and BEC prevention as mostly or completely about good training, only 17 percent consider that account takeover prevention is primarily about good training. Conversely, while only 11 percent consider spear phishing prevention to be primarily a technology-focused issue, 36 percent consider ransomware a problem to be addressed primarily or completely using technology solutions.

The vast majority of security decision makers believe that there is a role to play for security awareness training and technology-based solutions.

Figure 10
The Role of Security Awareness Training vs. Technology-Based Solutions

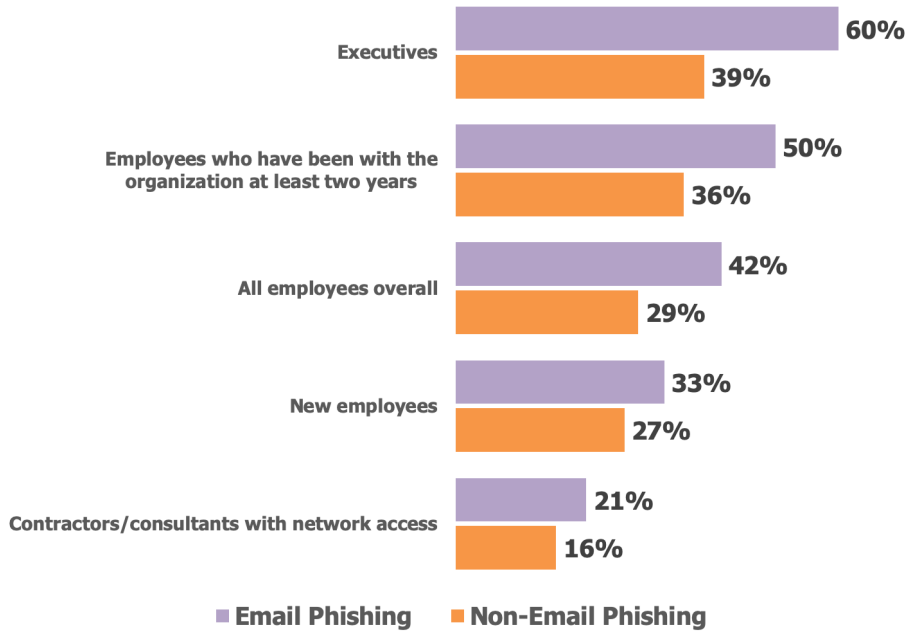
	Phishing	Spear phishing	Ransom ware	BEC	Account Takeovers
Good training can solve the problem completely	6%	8%	2%	9%	1%
It's primarily about training, but process/tech can help	38%	37%	16%	31%	16%
Training and process/tech are equally important	43%	44%	46%	47%	44%
It's most about process/ tech, but training can help	10%	9%	28%	9%	31%
Problems can be solved only through process/tech	2%	2%	8%	4%	7%

Source: Osterman Research, Inc.

EMAIL VERSUS NON-EMAIL THREATS

Our research found that security awareness training is becoming more common, and that it is having a positive impact on user behavior. For example, as shown in Figure 11, security decision makers have significant confidence in both executives and more tenured employees in the context of their ability to detect email-based phishing attempts. However, for non-email phishing attempts, such as might be encountered in social media feeds, pop-ups, ads, search, instant messaging, rogue apps, and more, confidence is significantly lower. This is due in large part to the fact that much of today's security awareness training focuses on email, since email continues to be the primary avenue for phishers to attempt to create new victims. It's important to note, however, that tools other than email are often and increasingly used to create phishing victims.

Figure 11
Confidence That Various Groups are Well Trained to Recognize Email- and Non-Email Based Phishing Attempts
Percentage Indicating "Strong" or "High" Confidence



Source: Osterman Research, Inc.

Our research found that security awareness training is becoming more common, and that it is having a positive impact on user behavior.

PREVENTING ADVANCED ATTACKS IS ESSENTIAL

Advanced attacks can create serious consequences, including loss of intellectual property, direct financial losses, major data breaches, or worse, including loss of human life; and so preventing them is essential. Here are some examples:

- American Medical Collection Agency (AMCA), a medical billing firm, suffered a major, months-long data breach of its customers' data that may have exposed upwards of 20 million patient records[xi] from major labs like LabCorp and Quest Diagnostics. The breach caused AMCA to pay more than $3.8 million to mail information about the breach to victims, and roughly $400,000 in consulting costs to help correct the problem. The company cut its staff from 113 people to just 25, and in June 2019 the firm filed for bankruptcy.

- A type of anesthesia machine produced by GE Healthcare can be hacked to change the amount of anesthesia delivered to patients, and alarms that would warn of a problem can also be disabled. GE's Aespire and Aestiva 7100 and

7900, if connected to a hospital network, are vulnerable to infiltration by hackers[xii].

- In July 2019, Monroe College in New York was infected with ransomware and the perpetrators demanded 170 Bitcoin (approximately $2 million). Many of the school's systems were shut down[xiii].

- The TrickBot malware has been around since 2016 but continues to evolve. Among the most recent additions to TrickBot's arsenal is a malicious email-based infection and distribution module that is used to harvest email credentials and contacts. Deep Instinct reported in July 2019 that it had recovered a database containing 250 million email accounts that had been harvested by cybercriminals using TrickBot[xiv].

BUT POST-DELIVERY PROTECTION IS ALSO ESSENTIAL

Although preventing security incidents is the ideal, it's almost certain that a ransomware or other malware infection will occur, or someone will click on a phishing link and install a data-stealing Trojan, or login credentials will be compromised, and so forth. Consequently, proper security measures must include a strong emphasis on what happens after something bad happens. Among these should be:

- Detonated ransomware should be prevented from encrypting backups.

- Frequent backups and snapshots should be used so that endpoints that become infected with various types of malware or ransomware can be recovered to a known good state as quickly as possible.

- Firewalls should be configured to prevent malware from connecting to command-and-control servers.

- Access control solutions should prevent the execution of malware.

- Sandboxing should be used to evaluate any and all suspicious file types and links.

NATIVE SECURITY IN MANY APPS IS NOT ADEQUATE

Many organizations will rely on the native security capabilities that come with their applications, particularly cloud applications like Office 365. While native security provides some level of protection against various types of threats, third-party solutions provided by specialist providers often will yield higher catch rates, more thorough protection against sophisticated threats, and coverage across a wider range of applications than is possible with native security tools. For example:

Third-party solutions provided by specialist providers often will yield higher catch rates.

- Exchange Online Protection (EOP), the default security solution in Office® 365®, allows users easily to access their Office 365 junk folder and release any message back into their inbox. Once a message has been released, the user can then click on any dangerous link or open any dangerous attachment it might contain.

- Some customers of Office 365 have reported poor recognition of phishing attempts using EOP. This includes attacks that impersonate Microsoft products like Office 365, Outlook and SharePoint that contain links leading to malicious payloads.

- Mimecast has discovered a 16 percent false negative rate in spam and phishing detection within Office 365's native security over testing which included more than 100 million emails.

- Native security solutions do not analyze and detect malicious north-south traffic to inform blocking defenses on a real-time basis, even though doing so would provide robust protection against a wide range of phishing attacks.

Please note that this is not a criticism of Microsoft's security-related shortcomings (we believe Office 365 to be a good offering and we recommend its use), but merely to illustrate that native security capabilities sometimes will not be adequate and should be supplemented or replaced with third party solutions.

INCIDENT RESPONSE IS ESSENTIAL

Osterman Research has found that security teams spend the largest single share of time on identifying potential security threats, but less time gathering information about incidents and resolving them. As a result, many IT and security decision makers would prefer to adopt automated capabilities into the incident response process to shorten the resolution and escalation time necessary to manage security incidents, and to handle automatically the more mundane and routine alarms they encounter – the data in Figure 7 illustrates just how much decision makers would like to incorporate AI/ML to address this problem.

DETAILED POLICIES NEED TO BE ESTABLISHED

All organizations should establish detailed and thorough policies and procedures for protecting sensitive corporate data, financial assets, intellectual property and other valuable content. For example, these policies should include things like:

- Acceptable use policies for every platform that is or will be used in the organization, including personally managed/owned devices, applications and services. This includes non-business tools, as well, such as personal social media accounts.
- The frequency with which every endpoint is backed up, where it is backed up, and the procedures for testing these backups.
- The manner in which employees should handle and share sensitive and confidential data, including classifying and encrypting this data, as well as the tools that can be used to send and store this information.
- Consideration of passphrases instead of passwords. For example, "SallyMobius56" can be brute forced using a typical home computer in about seven months, whereas "Sally has a fish named Mobius" would take 10,000 or more centuries to crack[xv].
- Best practices for password-management, such as minimum password requirements (length, use of upper- and lower-case characters, use of punctuation, etc.), how frequently passwords must be changed, how passwords are stored, etc.
- Which systems and data assets should require dual-control procedures so that a single employee cannot steal or delete highly sensitive data assets?
- Determination of which sensitive data assets are made available via the internal corporate network or the public network, and which should be air gapped.
- Detailed requirements for the use of at-rest and in-use encryption for every platform and device, particularly mobile devices and laptops, and the ability to wipe them remotely if they are lost or stolen – including personally owned devices that are allowed to touch corporate data or financial assets.

All organizations should establish detailed and thorough policies and procedures for protecting sensitive corporate data.

HOW WILL THINGS CHANGE IN THE FUTURE?

It goes almost without saying that security threats will become more difficult to address in the future as well-funded cybercriminals become more adept at penetrating corporate defenses. We anticipate that:

- While non-email channels will become a greater target, email will continue to be the primary threat vector for attacks on the enterprise for at least the next several years.

- While phishing emails that contain links or attachments intended to distribute malware will continue to increase – particularly as more users are served by cloud-based email and collaboration solutions – we also will see significant growth in the use of malware-less threats such as email fraud.

- Spam will remain an effective tool for cybercriminals to distribute malware and social engineering attacks and will continue to represent the bulk of email traffic. For example, Cisco/Talos Intelligence reported that total email volume for the month ended June 1, 2019 was 539.2 billion emails and that 85.1 percent of this volume was spam – this represented the highest volume for both email and spam since the month ended February 1, 2018[xvi].

- Public sector entities, such as city and county governments, are now a focus of ransomware attacks and we anticipate this will continue for some time. In just 2019, the governments of Baltimore, MD; Albany, NY; Fisher County, TX; Genesee County, MI; Cartersville, GA; Lynn, MA; Augusta, ME; Akron; OH; Sammamish, WA; Jackson County, GA; Stuart, FL; Greenville, NC and many others have been infected by ransomware[xvii]. Even many federal government agencies are at serious risk of cyber attack according to a United States Government Accountability Office report published in July 2019[xviii].

New Approaches to Improving Security

The title of this paper – *New Methods for Solving Phishing, BEC and Other Security Threats* – is really the crux of what we've been discussing. What is needed is the use of much of what is working now, but with the addition of new approaches and practices to enhance the security posture of the typical organization. Here are some ideas to consider:

- **Focus first on the board**
  Getting the board of directors and senior management in a company to understand the critical nature of security risks – and just how devastating they can be – is essential. A board that is well-versed on security risks and aware of the financial and other consequences of a major data breach, a ransomware attack or some other security incident is more likely to loosen the purse strings and fund security appropriately.

- **Understand the risks**
  While many corporate decision makers believe they fully understand the risks that their organizations face, many do not. As just one example, a Symantec survey[xix] found that while seven percent of those surveyed believe that account takeovers are a key risk for their organization, the reality is that account takeover activity is implicated in 42 percent of security risks. In the survey conducted for this white paper, we found that 33 percent of organizations have been impacted by account takeover threats during the past 12 months.

We found that 33 percent of organizations have been impacted by account takeover threats during the past 12 months.

- **Take a risk-based approach**
  Gain visibility into the people who are the greatest risk for phishing and BEC attacks. Then apply adaptive controls for those very targeted people. For example, an organization could isolate users' browsing experience to prevent potential malware from downloading onto the device.

- **Analyze what's in use**
  As a corollary to the point above, there are many applications, cloud solutions, mobile apps, employee-owned personal devices, etc. accessing corporate applications and data, much of which is unbeknownst to security teams. This lack of knowing which app touches what data creates enormous security risks, since security teams are at a serious disadvantage trying to protect sensitive corporate data and financial assets from tools they know nothing about. To address this shortcoming, a thorough and ongoing audit should be performed so that security can understand every device, application, mobile app, etc. that is being used across the enterprise.

- **Train users properly**
  A growing number of organizations are understanding the importance of providing robust security awareness training to their users. While there are still some skeptics who believe that technology-based solutions alone can address their security needs, the truth is that there must be a balance between training and technology to achieve an optimal security posture. And, a recent Osterman Research analysis[xx] found that the return-on-investment (ROI) for security awareness training can be substantial, particularly for larger organizations.

- **Focus on the endpoint**
  Keeping endpoints safe, secure, and sound is a job that crosses the disciplines of IT security and IT operations. The endpoint is one of the most challenging and serious threat vectors facing security decision makers. Conventional malware is ongoing, but now has been joined by advanced threats that can hide in plain sight until triggered, cover their tracks, or attempt to slip in undetected through social engineering tricks or rogue and/or vulnerable applications. That said, the endpoint is an additional layer to counter the attacks. It must be managed in a coordinated fashion together with secure email gateway solutions to ensure that threat information is shared between solutions.

  It's also worth noting that as more network traffic becomes encrypted with SSL and TLS 1.3, network-based security solutions will lose visibility and effectiveness. Endpoint security will become more important, not less. And, as endpoints are increasingly mobile and use outside-of-network-perimeter protections, endpoint security solutions become a primary defense. Moreover, it's not just about protecting the endpoints from malware with antivirus solutions. It's also about protecting endpoint users from phishing, both inside and outside perimeter defenses, with stronger anti-phishing protections on the endpoint.

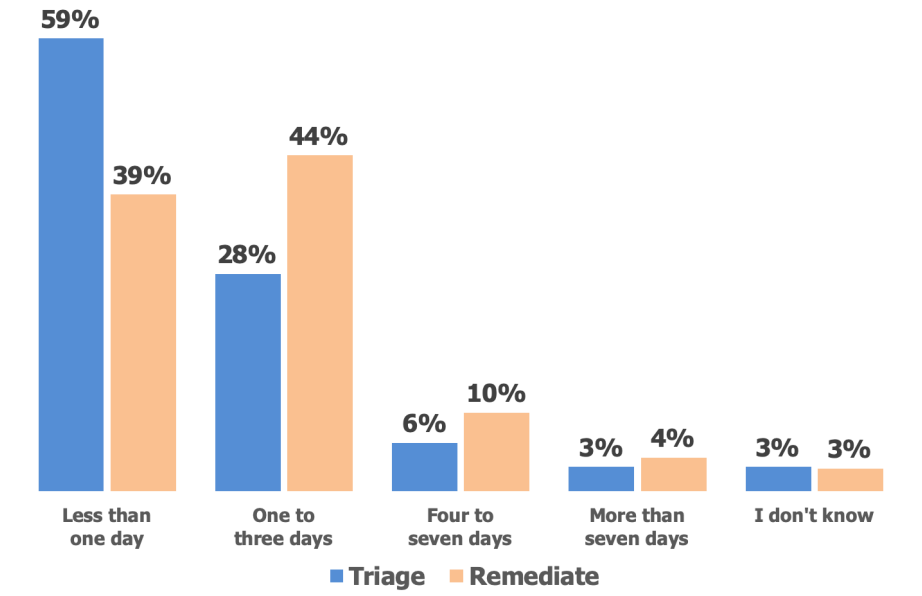
  Many organizations are implementing endpoint detection and response (EDR) solutions to address some of the shortcomings in their current security infrastructure. EDR provides continuous monitoring of the wide range of endpoints on or off corporate networks, which enables security staffers to monitor not only malicious attacks from external sources, such as advanced persistent threats (APTs) that might result in data breaches; but also to keep tabs on anomalous activity from inside the organization, such as crypto mining or data theft from departing employees. Moreover, EDR solutions record enormous volumes of activity that take place on the network in a way that other tools, such as security information and event management (SIEMs) and endpoint protection platforms (EPP), typically don't or don't do quite as well. Plus, EDR solutions offer analysis tools that can enable security analysts, threat hunters and others to more quickly evaluate and block follow-on attacks. These include sweeping for indicators of compromise to see if others in an organization were infected,

Triage and remediation of security incidents is often not adequate.

proactively hunting for indicators of attack, and determining the root cause of an incident and enabling protections against it.

- **Focus on faster triage and remediation**
  Our research found that the triage and remediation of security incidents is often not adequate. As shown in Figure 12, only 59 percent of internal threats are triaged in less than a day, while 12 percent take four or more days. Worse, only 39 percent remediate threats in less than a day, while 17 percent of remediation activities take four or more days.

Figure 12
Time Required to Triage and Remediate Internal Threats



Source: Osterman Research, Inc.

It's critical, then, to significantly shorten both the time required for triage and remediation in order to deal with security threats more effectively and to minimize the damage from them. Key in this regard are the use of automation and AI/ML – as discussed earlier, the latter technologies are not used to nearly the extent that decision makers and influencers report they would like.

Also key is the use of good threat intelligence that can enable threat hunters and security analysts to better understand the significance of alerts and anomalous behavior, to provide more context around these events, to understand how alerts and suspicious behavior fits into previously identified patterns, and so forth.

Good threat intelligence that can enable threat hunters and security analysts to better understand the significance of alerts and anomalous behavior.

- **Create communication backchannels**
  One of the best ways to thwart a BEC attack is by enabling out-of-band communications between the supposed sender and the recipient of the request. For example, if a CFO receives an email request from the CEO for a quick wire transfer, or a low-level staffer receives an email request from the VP of Human Resources to send all of the company's W-2 information, all that's usually needed to verify the validity of the request is a phone call or text message. There have been numerous examples in which something simple like this wasn't done, and some companies have lost millions of dollars as a result.

  Of course, enabling these communication backchannels requires the support of a corporate culture in which managers are open to the idea of their requests being

challenged. A VP of Human Resources that would be offended by an intern challenging his or her request for sensitive information increases the risk that a BEC attempt will be successful.

- **Take a Security Orchestration, Automation and Response (SOAR) approach to security**
  Many organizations have a variety of disparate security solutions but have not integrated them adequately to take a more holistic view of security. The use of SOAR can provide this needed integration by a) integrating the various security processes and tools necessary to address a security incident, b) automating the management of various tasks inside of and between different security solutions that otherwise would be managed using manual processes, and c) enabling more rapid response to security threats than would otherwise be possible using traditional, manual processes.

  An example of the efficacy of the SOAR approach in the context of phishing: detecting and stopping phishing attempts before they reach end users is essential, as is the speed with which this is accomplished. According to Verizon's *2018 Data Breach Investigations Report*, testing has found that the length of time from when a phishing campaign is launched to the first report from a user is 28 minutes. Verizon also found that the length of time from the launch of most phishing campaigns to the first person clicking through it is 16 minutes. That gap of 12 minutes is critical, since a lot of bad things can happen during the interval between the click and report phase of a phishing campaign. Taking a SOAR approach can provide faster response time and result in potentially less damage.

- **Secure your cloud accounts**
  With the growth of cloud apps, cyber criminals are compromising cloud accounts to launch phishing, BEC and malware-based attacks. Once they compromise a corporate-approved cloud app, they use legitimate accounts to send phishing emails and BEC emails inside and outside an organization. For example, if an attacker compromises a CFO's Office 365 account, he can now use a trusted account to email to employees and business partners to wire money or send sensitive data. The attacker could also upload a malicious file and email employees a link to the file – again using a trusted account that has been compromised.

  To address this problem, organizations must secure their cloud accounts. They'll need granular visibility into cloud usage and detection capabilities that can identify risky files in their cloud apps, and spot suspicious logins or activity. Analytics will be important to establish a baseline of user behavior and detect anomalies for investigation.

With the growth of cloud apps, cyber criminals are compromising cloud accounts to launch phishing, BEC and malware-based attacks.

Summary

Security represents the worst of both worlds: cybercriminals are well-funded, smart, collaborative and innovative, and they need to exploit only a single vulnerability to wreak havoc on an organization. Cybercriminals' victims, on the other hand, are often not as well-funded, their users not as well-trained, they often are not as prepared as they need to be, and they must face an increasingly rigorous legal and regulatory environment that will punish their security mistakes. And they have to protect every single point on a large and growing attack surface.

To address the growing set of threats that organizations face, they need a new way of approaching the problem of security: new technologies, better and more frequent training, and new processes.

Sponsor of This White Paper

To better meet your company's security, data protection and compliance needs, Zix can enhance your Office 365 environment with advanced threat protection, archiving and email encryption. Zix delivers a superior experience and easy-to-use solutions that have earned the trust of more than 19,000 organizations including the nation's most influential institutions in healthcare, finance and government.

To defend your company from malware, ransomware, phishing and other email threats, ZixProtect combines a multi-layer email security approach with automated traffic analysis, machine learning and real-time threat analysts. In addition, ZixProtect's business continuity feature ensures that your organization can continue to communicate if your email experiences a disruption.

ZixArchive eases email archiving and eDiscovery with automatic email collection and storage in a secure cloud. Its automatic indexing and multiple search criteria gives you and your employees convenient and rapid access to archived emails. ZixArchive also enables you to share an email hold with outside legal counsel and auditors and revoke privileges when access is no longer needed, keeping your data within your control.

To ease email encryption for you, your employees and your recipients, leverage the industry's leading solution ZixEncrypt. Automatic transparent delivery between customers and robust delivery methods for other recipients enables easy access to encrypted email for anyone, anywhere and on any device, making the user experience exceptional and compliance simpler. Proven policies and advanced reporting provide peace of mind, while customizable branding and security capabilities make email encryption fit your unique company needs.

Leveraging our more than 15 years of hosted experience, you can have confidence that Zix email security solutions integrate seamlessly with Office 365. You also benefit from the support of the ZixData Center, a state-of-the-art facility with PCI DSS 3.2 certification, SOC2 accreditation and SOC3 certification. Staffed 24/7/365, ZixData Center has a track record of consistent 99.999% availability. In addition, Zix delivers exceptional customer support 24/7/365 no matter your questions or concerns. With reliability, experience and superior support, Zix improves email security for your Office 365 environment. To learn more about our solutions for Office 365, visit www.zixcorp.com/office365.

www.zixcorp.com

@ZixCorp

+1 866 257 4949

sales@zixcorp.com

REFERENCES

[i] Source: Netskope Cloud Report, Winter 2018

[ii] https://www.ameinfo.com/industry/media/cybercriminal

[iii] https://www.consumerreports.org/hacking/shadowhammer-hackers-attack-asus-computers-through-routine-software-update/

[iv] https://biztechmagazine.com/article/2019/03/rsa-2019-cybercriminals-overlooked-tactics-and-favorite-industries-target

[v] https://secureteam.co.uk/news/credential-stuffing-on-the-rise/

[vi] https://www.navisite.com/blog/beware-five-innovative-cyberattacks-office-365

[vii] https://www.sonicwall.com/news/sonicwall-detects-reports-dramatic-rise-in-fraudulent-pdf-files-in-q1-2019/

[viii] https://www.howtogeek.com/171993/macros-explained-why-microsoft-office-files-can-be-dangerous/

[ix] https://www.tsg.com/blog/security/3-top-cybercriminal-tactics-you-need-know-2019-and-how-prevent-them

[x] https://www.tsg.com/blog/security/3-top-cybercriminal-tactics-you-need-know-2019-and-how-prevent-them

[xi] https://krebsonsecurity.com/2019/06/collections-firm-behind-labcorp-quest-breaches-files-for-bankruptcy/

[xii] https://www.bbc.com/news/technology-48935111

[xiii] https://nypost.com/2019/07/11/hackers-target-monroe-college-demand-2-million-in-bitcoin-as-ransom/

[xiv] https://www.deepinstinct.com/2019/07/12/trickbooster-trickbots-email-based-infection-module/

[xv] Source: Kaspersky Secure Password Check (https://password.kaspersky.com)

[xvi] https://www.talosintelligence.com/reputation_center/email_rep

[xvii] https://go.recordedfuture.com/hubfs/reports/cta-2019-0510.pdf

[xviii] https://www.gao.gov/assets/710/700503.pdf

[xix] https://www.bleepingcomputer.com/news/security/business-decision-makers-focus-on-the-wrong-security-issues/

[xx] Source: *The ROI and Other Benefits of Security Awareness Training*, Osterman Research, Inc.