Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **January 2019**
Sponsored by **KnowBe4**

Addressing the Top 10 Security Issues Organizations Face

Executive Summary

Cybersecurity must be a top-level priority for any organization and for many it is. Security should be viewed holistically and should include a range of elements, including layered, technology-based solutions on-premises and in the cloud; security awareness training to help employees become a more integral part of security defenses; the establishment of common-sense policies and practices that will bolster security defenses; and security education for the board of directors and senior managers to help them understand the critical role they play in enabling a culture of security.

KEY TAKEAWAYS

Here are the key takeaways we discovered from the survey that was conducted for this white paper and in our analysis of the results:

- **Security incidents are common**
  Seventy-eight percent of the organizations we surveyed have experienced one or more serious security incidents during the 12 months ended October 2018. The most common of these incidents were infections resulting from phishing emails, the accidental leak of sensitive or confidential data through email, and targeted email attacks launched from compromised accounts.

- **Threats come from email and non-email sources**
  While email is a common vector for phishing and other threats, non-email threats are also quite common. Bad actors are frequently using web-based tactics, deploying diverse techniques to target human weakness. These sophisticated phishing attacks are delivered via targeted ads, social media, chat, browser extensions, and compromised sites. With as many as 46,000 new phishing sites going online each day, there is a misconception that existing security defenses are sufficient.

- **Decision makers and influencers are concerned about a range of issues**
  The issues of greatest concern to security-focused decision makers and influencers are users' credentials getting stolen through email-based phishing, computers getting infected with malware through email-based attacks, endpoints getting infected with ransomware, and senior executives' credentials getting stolen through spearphishing.

- **Security spending will increase in 2019**
  Our research revealed that the median security spending per employee will increase by 16 percent from 2018 to 2019.

- **Users are the weak link in the security chain**
  Our research found that three percent of users are never trained on security issues, 30 percent receive training only once per year, and another 21 percent are trained only twice per year. This means that more than one-half of users are trained too seldom to make them an effective barrier against security threats, especially against today's, more sophisticated and legitimate-looking attacks.

- **Security defenses are improving…sort of**
  We found that most organizations' security defenses are getting better over time at stopping malicious emails, but not at stopping at CEO Fraud/Business Email Compromise (BEC) and ransomware attempts.

- **Most want to use artificial intelligence and machine learning more**
  We found that while only one in 11 organizations is using artificial intelligence and machine learning extensively or nearly so for security management, nearly one-half would like to do so.

The median security spending per employee will increase by 16 percent from 2018 to 2019.

- **Ransomware will make a comeback**
  Among our predictions for 2019 is the view that ransomware will make a comeback in 2019 after calming down a bit in 2018, but that most of the ransomware demands will be for very small amounts.

ABOUT THIS WHITE PAPER

This white paper was sponsored by KnowBe4; information about the company is provided at the end of this paper.

The Key Concerns That Organizations Face

INCIDENTS THAT HAVE OCCURRED DURING THE PAST 12 MONTHS

Our research discovered that a wide range of security incidents have occurred over the 12 months ended October 2018. As shown in Figure 1, we found that the most common incident was an endpoint infection that occurred as a result of a phishing email (impacting more than one-third of organizations), followed by accidental leakage of sensitive or confidential information through email, a targeted attack launched through a compromised account, and employee web surfing that resulted in an infiltration of some type.

Among our predictions for 2019 is the view that ransomware will make a comeback in 2019.

Figure 1
Security Incidents That Have Occurred During the Past 12 Months

Incident	% of Orgs
One or more endpoints in our network were infected as a result of a phishing email	37%
Sensitive / confidential info was accidentally leaked through email	28%
A targeted email attack launched from a compromised account successfully stole a user's account credentials	24%
Employee web surfing resulted in one or more of our systems being successfully infiltrated	24%
A targeted email attack launched from a compromised account successfully infected an endpoint with malware	23%
A fileless/malwareless attack reached an endpoint	19%
A CEO Fraud/BEC attack successfully tricked one or more senior executives in our organizations	17%
Malware has infiltrated our internal systems, but we are uncertain through which channel	16%
One or more of our endpoints had files encrypted because of a successful ransomware attack	16%
An account takeover-based email attack was successful	16%
One or more of our senior executives' systems was infected with malware because of a phishing or spearphishing email	14%
Sensitive / confidential info was accidentally or maliciously leaked through a cloud-based tool like Dropbox	12%
Sensitive / confidential info was accidentally or maliciously leaked, but how it happened is uncertain	9%
Sensitive / confidential info was accidentally or maliciously leaked through a social media / cloud application	6%
None of the above	22%

Source: Osterman Research, Inc.

An examination of Figure 1 reveals that only 22 percent of organizations did not report any type of infiltration during the preceding 12 months. While we believe that number is reasonably accurate, we can draw a couple of conclusions from it:

- First, that number is probably a bit too high given that a few of the respondents in our survey may not have recalled every incident that occurred over the previous year, and some may have not revealed every security incident that they experienced. Discussing every security problem is likely embarrassing to some decision makers given that it reveals a weakness in their security defenses, and a few survey respondents may have been reluctant to share all of their "dirty laundry" to a research firm.

- Second, many decision makers likely are not aware of every security incursion that has occurred in their organization. A security threat can infiltrate an organization's security defenses and can remain undetected for long periods before it is discovered. The so-called "dwell time" – the period between the point of infiltration and the intrusion being detected – can vary, with estimates ranging from 49 days[i] to 150 days[ii]. The result is that an infection might have occurred of which security decision makers were not yet aware when the responded to the survey.

ISSUES THAT CONCERN DECISION MAKERS AND INFLUENCERS MOST

Our research also discovered a wide range of issues that concern decision makers. The most serious of these, as shown in Figure 2, is the successful theft of user credentials as the result of a successful email-based phishing attack. Following closely behind is the infection of endpoints with malware, a ransomware infection, and spearphishing resulting in one or more senior executives' credentials being stolen.

Only 22 percent of organizations did not report any type of infiltration during the preceding 12 months.

Figure 2
Concerns About Various Security-Related Issues
Percentage of Respondents Indicating a "Concern" or "Major Concern"

Source: Osterman Research, Inc.

Let's address each of these threats:

- **Phishing**
  Phishing, the primarily email-focused practice of cybercriminals sending deceptive emails that represent legitimate brands or inquiries for the purpose of stealing login credentials, personal information or infecting endpoints with malware, is typically the most common threat that organizations face. While some phishing attempts are quite easy to detect because of poor grammar or

spelling, phishers are becoming increasingly sophisticated and crafting messages that are difficult to distinguish from legitimate content. Even for employees who are skeptical about emails they receive, a well-timed phishing email might trick a preoccupied employee into clicking on a malicious link in a phishing email or opening a malicious attachment. These attempts might take the form of a shipping company requesting additional information, a fake email from an HR department during a benefits open-enrollment period, or a fake iTunes receipt.

A variant of phishing attempts lures victims into revealing their credentials for file-sharing and other services, such as Microsoft OneDrive, Dropbox or Google Docs. A potential victim will receive an email with a request to enter their credentials to download a large or encrypted file, after which the credentials will be stolen or malware will be installed on their endpoint.

It's important to note that while most phishing today is email-based, there are numerous other ways that phishing can occur. Hackers have a broader definition of phishing that includes other types of phishing schemes, delivered through targeted ads, social media, chat, browser extensions, and compromised sites. These channels deliver fake login, rogue software, fake media players, scareware, and gift and investment scams, among other threats.

- **Malware infiltration**
  Malware infiltration can occur in a number of ways, including malicious payloads in an email (e.g., a PDF file that contains malware); a malicious link in an email, a social media post or a poisoned search engine result; or via a drive-by attack while web surfing. The survey conducted for this white paper found that of all of the malicious emails that enter organizations, 45 percent contain malicious links, 28 percent contain a malicious payload (e.g., a file attachment), and 27 percent contain URLs with credential theft mechanisms that do not themselves contain malware.

  It's also important to note that new forms of malware that are fileless: to avoid detection by anti-virus tools, malicious sites will insert HTML and JavaScript into browser memory that function as spyware to steal credentials. Without any kind of .exe file to examine, these threats can avoid malware detection systems.

- **Ransomware**
  While generally not as common in 2018 as it was in 2017, ransomware, a more specialized form of malware, continues to be a very serious issue. A number of entities have been infected with ransomware during 2018, effectively encrypting and preventing access to corporate data on one or more endpoints. For example, major ransomware attacks during 2018 were launched against the City of Atlanta[iii], the East Ohio Regional Hospital and Ohio Valley Medical Center[iv], the Indiana National Guard[v], the Onslow Water and Sewer Authority[vi], and the Port of San Diego[vii], among many others. While the ransomware threat may not be as severe in 2018 as it was previously, a report by Datto found that 55 percent of managed service providers reported ransomware attacks against their clients during just the first half of 2018[viii].

- **Spearphishing, CEO Fraud/Business Email Compromise**
  Spearphishing is a more targeted form of phishing that is generally aimed at a group of individuals, such as those in a company or in some type of affinity group. CEO Fraud/Business Email Compromise (BEC), on the other hand, is even more targeted, generally aimed at just one or a very small group of individuals, such as a CFO or someone in HR with access to sensitive and valuable information.

  In a CEO Fraud/BEC attack, the normal attack vector is an email that purports to be from the CEO or some other highly placed individual within an organization. The attacker normally requests a specific action, such as wiring funds or sending confidential information, such as W-2 data. These types of attacks are difficult

While most phishing today is email-based, there are numerous other ways that phishing can occur.

for conventional security defenses to recognize, since they virtually never contain a malicious payload or link. These types of attacks are enabled by the stealthy nature of more sophisticated cybercriminal activity: an infiltration will occur and the criminal will search for things like wire transfer timing, amounts of these transfers and their recipients; executives' travel schedules; etc. and then craft a CEO Fraud/BEC attempt with the goal of tricking a victim into transferring money or data.

- **Accidental disclosures from insiders**
  Insider mistakes are common and can occur in a number of ways. As just one example, in June 2018 an employee of the Chicago Public Schools (CPS) system mistakenly sent a mass email that contained a link to a spreadsheet containing sensitive information on 3,700 students and families. The file to which the email linked was stored, without any protection, on the CPS Blackboard system[ix].

  Accidental disclosures can also occur when employees are careless in other ways, such as taking home an unencrypted laptop or losing a flash drive that contains unprotected data. Accidents can also occur when employees are not being careless. For example, if the corporate email system goes down or will not support the transfer of very large files, an employee may opt to use his or her personal webmail solution to continue working. This will bypass corporate security defenses and potentially increase an organization's exposure to malware, data breaches or other problems.

- **Threats introduced through web surfing**
  Web surfing is a potentially dangerous activity on a number of levels. Users can be directed to malicious web sites or malicious pages on valid sites, resulting in the installation of malware, client-side scripting and other dangerous content. Some users visit non-business-oriented web sites and can inadvertently download malicious content. A significant proportion of advertisements that appear on web sites can deliver malicious content – so-called "malvertising". Search engine poisoning is a common technique for distributing malicious content, wherein cybercriminals will use search engine optimization (SEO) techniques to get malicious content to appear prominently in search results.

  It's important to note that a significant proportion of malicious content and other threats are not delivered through "recreational" web surfing, but rather through valid, business-focused sites that have been compromised. Bad actors focus on phishing and social engineering through these compromised pages and sites for purposes of credential theft/fake logins and the like.

Web surfing is a potentially dangerous activity on a number of levels.

- **Social-media threats**
  There are a number of social media-related threats that can occur. For example, employees can (and often do) overshare personal information through Facebook, Twitter and other social media channels and this information can be used to create spearphishing or CEO Fraud/BEC attacks. Malicious actors can hijack valid social media accounts and use them to share malicious links, often via short URLs. Hijacked accounts can be used to solicit sensitive information from friends or followers.

- **Malicious insiders**
  Employees, contractors and other insiders who have malicious intent can cause significant harm to an organization. There have been numerous cases in which a terminated, laid-off or otherwise disgruntled employee has downloaded or deleted large volumes of sensitive content before leaving his or her employer, creating the potential for a data breach. Some employees may install cryptocurrency mining software, as discussed below, to mine digital currencies. One employee, upon learning of his termination, reset all of his employer's network servers to their default settings and then proceeded to disconnect remote backups[x].

- **Memory-based exploits**
  Many decision makers are concerned about memory-based exploits, such as Spectre and Meltdown, in part, because they can impact such a large number of endpoints. For example, Meltdown enables any application to access every part of a computer's system memory, while Spectre enables an application to access memory from other applications.

- **Account takeover-based email attacks**
  Account-takeovers are just what their name implies: a malicious actor will gain access to victims' online accounts and can then pose as that customer to commit a wide variety of cybercrime, including accessing confidential databases, sending CEO Fraud/BEC emails, accessing financial accounts, and the like. There have been several examples of account takeovers in the cloud, such as the May 2017 Google ATO that used a Gmail plug-in[xi] and a similar March 2016 attack against Dropbox users[xii].

- **Other issues**
  - The management of cryptocurrencies occurs using "blockchain" technology, a peer-to-peer system that serves as a distributed ledger of cryptocurrency transactions that will register and validate the creation of these currencies. The 1,000+ cryptocurrencies that exist are generated through "mining", a process of solving complex calculations that, if successful, will generate a "coin" of digital currency. The problem is that the mining process requires huge amounts of computing power, and so cybercriminals outside and inside of an organization can install cryptomining malware that will use corporate computing resources to mine for these coins. While this is not necessarily a security threat per se, it does consume computing capacity from email servers, web servers, endpoints and the like.

  - Password reuse is a well-publicized problem, but one that organizations continue to face in a significant way. For example, according to Troy Hunt, the founder of Haveibeenpwned, 86 percent of individuals continue to use passwords that are known to have been breached and are available in plain text[xiii]. A LogMein survey found that 91 percent of respondents understand the problems that can occur if they use the same passwords for multiple accounts, but 59 percent do it anyway[xiv].

TARGETED ATTACKS DIFFER FROM OTHER ATTACKS

Mass-mailed phishing and other, more conventional attacks are normally not personalized to their victims, but are typically sent to large numbers of people at the same time for the purpose of collecting sensitive user credentials like bank account logins. If even a tiny fraction of potential victims who receive these attempts are successfully exploited, the campaign will be a success.

A targeted email attack, on the other hand, may use spearphishing to steal information from identified victims, whether individual or corporate contacts. Note that spearphishing can also be accomplished via social media (e.g., LinkedIn InMails), instant messaging and SMS ("smishing").

A targeted attack will bypass an organization's security defenses using sophisticated malware to gain access to endpoints or other resources. The goal of the attack might include just poking around a corporate network, stealing intellectual property, or stealing login credentials for corporate financial accounts attack. The basic goal is to locate, exfiltrate and monetize stolen data and intellectual property without the victim finding out for as long as possible.

DOES THE CLOUD INCREASE SECURITY THREATS?

Leading cloud providers normally offer robust security defenses, but they can be vulnerable to attack because they hold such a large volume of their customers' valuable information, making them a prime target for sophisticated cybercrime.

A targeted attack will bypass an organization's security defenses using sophisticated malware to gain access to endpoints or other resources.

Although major cloud providers normally have better security capabilities than most of their customers and suffer fewer data breaches than the typical enterprise customer, even one successful breach of cloud-based data might expose a large number of their customers to regulatory fines, loss of customer confidence, and declining competitive market position, among a variety of other consequences.

Plus, it's important to consider that accounts in the cloud can be attacked just like they can be when managed using on-premises solutions, and so the cloud is not invulnerable to attack. As just one example, in 2017 48 Office 365 customers fell victim to a slow-moving, brute force login attack[xv].

SECURITY SPENDING IN 2019 vs. 2018

Osterman Research found that the median, per-employee security budget in 2018 was $78.05 at the large mid-sized and large firms that we surveyed for this white paper. Security decision makers and influencers anticipate that the median budget will increase by 16 percent in 2019 to $90.91 per employee.

Why are Cyberattacks So Successful?

Why is it that cybercriminals are so successful at stealing data, infiltrating corporate networks and otherwise penetrating corporate defenses? There are a number of reasons:

- **Criminals are smart and capable**
  An important reason for the success of cybercrime is that criminal organizations are normally quite well funded (often because they are enabled by organized crime), they have the technical resources needed to create new and ever more capable attack methods, and they tend to collaborate with one another to share new techniques and processes.

- **Criminals make lots of money from their efforts**
  A study by Bromium found that the most lucrative cybercriminals can make up to $2 million annually, and even entry-level hackers can generate an income of $42,000 annually[xvi]. Cybercriminals can generate individual earnings that are up to 15 percent greater than traditional crimes[xvii]. And laundered funds from cybercriminal activity are estimated at up to $200 billion per year[xviii]. In short, money is a key motivator for virtually any activity and cybercrime is no exception.

- **Organizations make mistakes**
  Another reason that cybercriminals are successful is that many organizations are not exercising proper due diligence in addressing the problems of phishing, spearphishing, CEO fraud/BEC, ransomware and other threats. For example, many organizations don't backup their data adequately and so cannot recover quickly or fully from a ransomware attack. Many do not provide good security awareness training to help users more easily recognize phishing attempts. Many don't have good internal control processes that will enable the recipient of a CEO Fraud/BEC attempt to verify the communication via text or mobile phone. Many don't have adequate detection for threats like phishing or spearphishing. Many don't have adequate data loss prevention capabilities that would detect when sensitive or confidential information is being sent unencrypted, through unapproved channels, or in anomalous ways. And, many have not adequately addressed the "Shadow IT" problem that would enable them to prevent some problems before they occur.

- **Users make mistakes**
  Many users will employ the same password for multiple systems, they won't change them on a regular basis, and they use simple passwords that are easy for brute force attacks to "guess". Some users will employ non-secure systems, such

Accounts in the cloud can be attacked just like they can be when managed using on-premises solutions.

as their personal webmail account or non-IT-approved mobile apps, to send sensitive or confidential work data. Some users will click on phishing links without first testing the veracity of the sender or the links contained within the message. Some users visit web sites that have a high probability of infecting their endpoint with malware.

- **Vendors make mistakes**
  It's almost a foregone conclusion that software will ship with vulnerabilities, some more serious than others. Vulnerabilities that can expose data or otherwise enable infiltration by cybercriminals are commonplace. For example, the NIST National Vulnerability Database analyzed 1,521 new common vulnerabilities and exposures during just November 2018[xix]. Moreover, while some organizations will fail to patch their software in a timely – as Equifax failed to do, contributing to a breach of 143 million records[xx] – sometimes vendors will fail to fix known vulnerabilities. For example, several years ago Microsoft had not fixed a known vulnerability in Internet Explorer 8 for at least seven months[xxi]; as of December 2018, a bug in Firefox appears not to have been addressed since it was first reported more than 11 years earlier[xxii].

- **There are more points of vulnerability**
  The growth of the Internet of Things (IoT) is creating orders of magnitude more entry points that cybercriminals can exploit for activities like phishing, malware distribution and distributed denial-of-service (DDoS) attacks. Gartner estimates that the 2020 installed base for IoT will reach 20.4 billion units, 7.6 billion of which will be in business settings.

- **Use of cryptocurrency**
  The availability of cryptocurrency has enabled some types of cybercrime to flourish, such as ransomware. Because cybercriminals that demand cryptocurrencies as payment are so difficult to trace, funds from ransoms can be "laundered" with relative ease. While threats like ransomware almost always use cryptocurrencies as payment because they're so difficult to trace, not all cybercriminals do so: as of December 2018, a Chinese ransomware strain that had impacted at least 100,000 endpoints manages ransom payments via the WeChat payment service[xxiii].

- **Cybercrime isn't just for professionals**
  Finally, just about anyone can become a cybercriminal with only a minimal knowledge of the mechanics involved in cybercrime. While malware kits have been available for more than 25 years, today ransomware-as-a-service kits are available on the dark web for as little as $175 and can allow "hobbyist" cybercriminals to generate sophisticated attacks. Some of these kits are quite sophisticated and offer robust feature sets.

The growth of the Internet of Things (IoT) is creating orders of magnitude more entry points that cybercriminals can exploit.

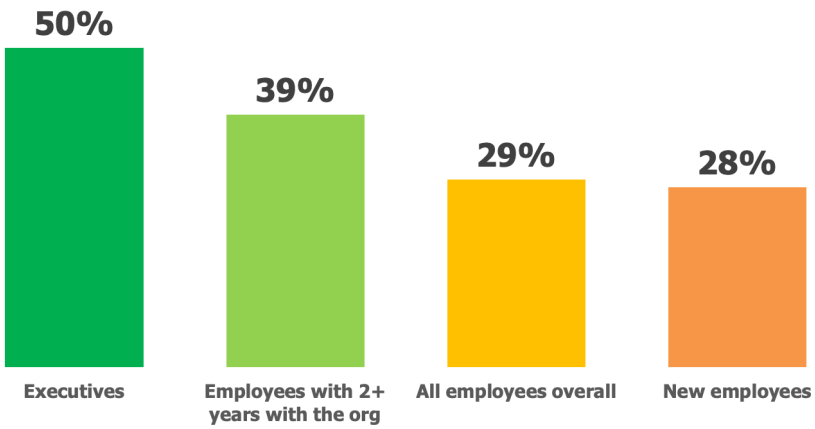
USERS ARE THE WEAK LINK IN THE SECURITY CHAIN

Another problem with many security defenses today is arguably the biggest vulnerability of them all – users who are inadequately trained about how to deal with issues like phishing, spearphishing, social media, web surfing and the like. Various Osterman Research surveys over the past couple of years have found that most corporate users are not adequately trained on security issues. The survey conducted for this white paper found that three percent of users are never trained on these issues, 30 percent receive training only once per year, and another 21 percent are trained only twice per year. That means that more than one-half of users receive minimal or no training on how to deal with the variety of security threats that they encounter on a regular basis.

What this translates to is a relatively low level of confidence in users' ability to deal with things like phishing and targeted email attacks, as shown in Figure 3 on the next page.

It's important to note that the fairly low effectiveness of current security awareness training – such as it is – should not be interpreted as a criticism of the concept of training itself, but rather the way that many organizations implement it. For example, our research found that many organizations use informal training processes that don't include phish testing to determine the effectiveness of the training regimen. In the absence of adequate training, many users will not be appropriately skeptical of the various threats they encounter, especially if these are delivered through social media channels, malvertising or text messaging that are implicitly assumed to be more trustworthy (or at least less suspect) than corporate email or the web.

Figure 3
Confidence That Various Groups are Well-Trained to Recognize Phishing and Targeted Email Attacks
Percentage Responding "Very Good" or "Excellent" Level of Confidence



Source: Osterman Research, Inc.

Fundamentally, the result of insufficient training is that IT and security lack confidence in their users' ability to recognize incoming threats or in their organizations' ability to stop phishing and related attacks. That said, security awareness training will not stop all attacks – some highly sophisticated attacks will use legitimate-looking web sites and evasive techniques that can trick even highly trained security staffers. Good security awareness training is essential, but it must be part of a robust security infrastructure.

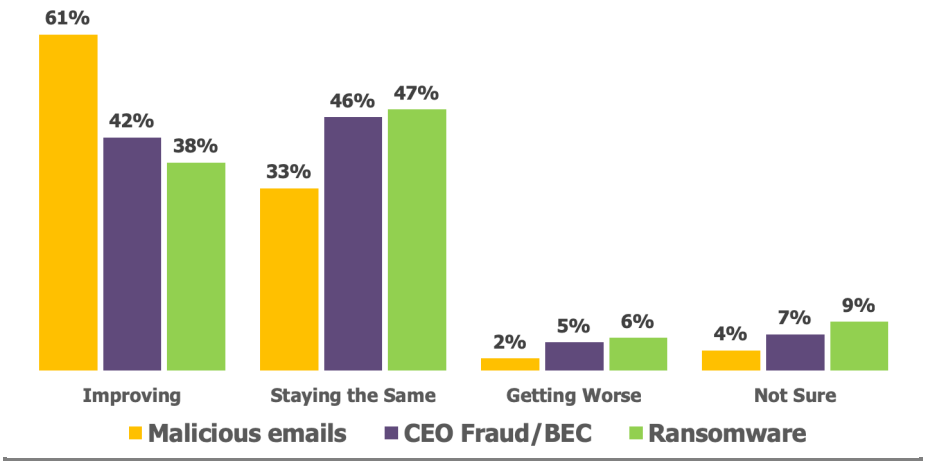
Good security awareness training is essential, but it must be part of a robust security infrastructure.

Security Must Improve

IS SECURITY REALLY IMPROVING?

The definitive answer is both yes and no. As shown in Figure 4, security defenses against malicious emails are improving for the majority of the organizations surveyed, but the level of improvement for threats like CEO Fraud/BEC and ransomware are significant lower. We also found that for a small proportion of organizations, these threats are actually getting worse over time, while for most of the rest the effectiveness of security defenses is remaining static.

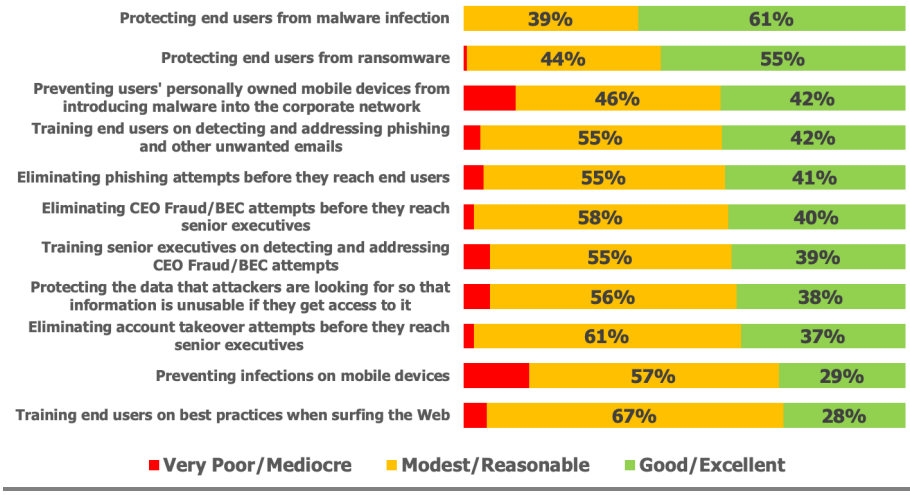
Figure 4
Changes in the Effectiveness of Security Defenses for Various Threats Over Time



Source: Osterman Research, Inc.

We also found, as shown in Figure 5, that most organizations consider their defenses against malware infection and protecting users from ransomware are either "good" or "excellent", but it falls off substantially from there.

Figure 5
Organizations' Views on Their Effectiveness Against Various Threats



Source: Osterman Research, Inc.

CYBERCRIME IS EXPENSIVE

Estimates of the actual cost of cybercrime vary widely based on the methodology used in calculating the estimates, but the costs are substantial no matter whose statistics are cited:

- Losses from various types of cybercriminal activity in the United States are increasing. For example, the FBI reported total losses of $1.42 billion in 2017, up from $525.4 million in 2012, an increase of 170 percent in just five years. In just 2017, for example, BEC fraud totaled $676.2 million and corporate data breaches totaled $60.9 million[xxiv].

Estimates of the actual cost of cybercrime vary widely based on the methodology used in calculating the estimates, but the costs are substantial no matter whose statistics are cited.

- McAfee and the Center for Strategic and International Studies (CSIS) estimated the worldwide cost of cybercrime in 2017 at between $445 billion and $608 billion[xxv].

- Cybersecurity Ventures estimates that global cybercrime will cost $6 trillion per year by 2021[xxvi].

POST-DELIVERY PROTECTION IS ESSENTIAL

The emphasis on security tends to focus on preventing threats – phishing attempts, spearphishing attempts, malware and others. However, security must also include an emphasis on post-delivery protection because of the high likelihood that malicious content will eventually get through even the best defenses. For example:

- Frequent backups and snapshots should be used to rapidly recover from endpoints that become infected with various types of malware or ransomware

- Solutions should be implemented that will prevent detonated ransomware from encrypting backups

- Firewalls should be used to limit the ability of malware to connect to command-and-control servers

- Access control solutions should be implemented that will prevent the execution of malware.

- Sandboxing should be used to evaluate suspicious file types.

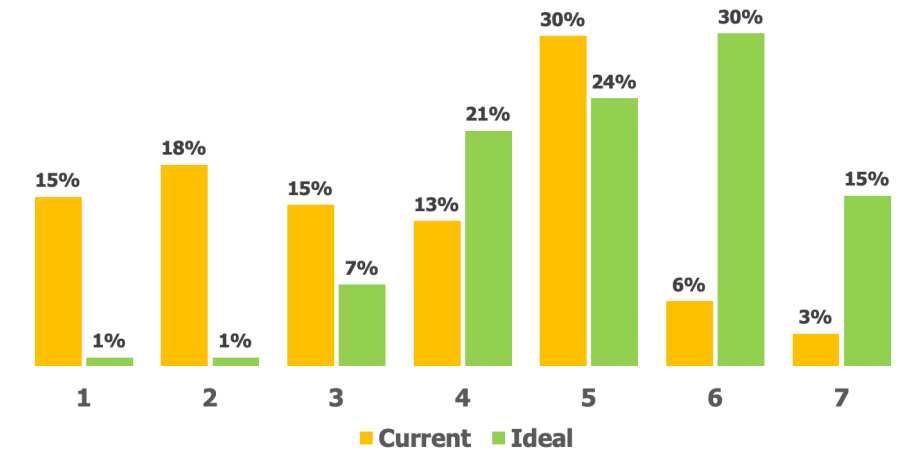
INCIDENT RESPONSE IS ESSENTIAL

A key component of any security capability is incident response, but it can be difficult and time-consuming. Osterman Research has discovered that security teams spend the largest single share of time on identifying potential security threats, followed by gathering information about incidents and then resolving the security threats they introduce. Consequently, 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.

To address incident response, alert management, etc., many organizations would like to use artificial intelligence/machine learning (AI/ML) to automate the incident management process. For example, as shown in Figure 5, only nine percent of organizations are currently using AI/ML widely or extensively, but 45 percent would like to do so.

A key component of any security capability is incident response, but it can be difficult and time-consuming.

Figure 5
Current vs. Ideal Use of Artificial Intelligence/Machine Learning
1 = No Use at All, 7 = Extensive Use



Source: Osterman Research, Inc.

NATIVE SECURITY IN MANY APPLICATIONS IS NOT ADEQUATE

A significant number of organizations rely just on the native security that is included with their email system or other applications – this is particularly true in Office 365 environments that include native security capabilities. However, many of these security capabilities do not provide the same level of protection as third party solutions that are offered by specialist providers. Office 365, for example, offers a set of good security capabilities, but it does have some limitations:

- The default Exchange Online Protection (EOP), the standard Office 365 security solution configuration, 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 Office 365 customers 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.
- Microsoft's more capable offering, Advanced Threat Protection (ATP), does not enable checking attachments and links for unknown and emerging threats by default – instead, an administrator must first set up these capabilities.
- ATP does not offer a whitelist or other integrated ability to mark particular domains as clear or safe.

This is not a criticism of Microsoft's security-related shortcomings (we believe Office 365 to be quite a good offering), but merely to illustrate that native security capabilities sometimes will not be adequate and should be supplemented or replaced with third party solutions. For example, many security solutions lack native phishing site detection capabilities. Many URL filtration, Secure Email Gateways, Firewalls, etc., have blacklists, but we are not aware of any that have the ability to detect if a user has browsed to a previously unknown malicious site. These blocking defenses need to be informed, on a real-time basis, about malicious sites and command-and-control server IPs to block.

A significant number of organizations rely just on the native security that is included with their email system or other applications.

Predictions About Security for 2019

Osterman Research anticipates the following security-related issues will occur during 2019:

- **Boards of directors will be a focus for security education**
  Boards of directors' knowledge about business issues is generally quite good, but knowledge about security issues is typically not their strong suit. As a result, CISOs, security managers and others charged with providing security for their organizations often feel overstressed and under supported. However, we believe that 2019 will be a turning point during which boards will get serious about security. This enlightenment will be driven by high profile data breaches (the Marriott data breach of 500 million records figuring prominently in this awakening) and will take the form of making more CISOs board members, discussing security issues at most or all board meetings, and accelerating funding for security in most organizations.

- **Ransomware will make a comeback, but with low ransom demands**
  The ransomware problem was terrible in 2016, got worse in 2017, softened a bit in 2018, but will make a comeback in 2019. However, we believe that the focus of ransomware authors in 2019 will be low level ransom demands, perhaps on the order of $20 to $40. The goal of cybercriminals will be to make ransom demands low enough to make paying the ransom an easy decision akin to an impulse buy at a supermarket check stand. Moreover, these ransom demands will come with full instructions about how to pay the ransom using Bitcoin or other cryptocurrencies.

- **Cryptocurrency mining will become a much more serious threat**
  Osterman Research believes that the price of Bitcoin will recover significantly from the significant drop it has experienced during 2018. This will motivate more external cybercriminals to infiltrate corporate systems for the purpose of installing cryptocurrency mining malware on various corporate servers, and it will motivate some insiders to do likewise.

- **Home routers will become a greater focus of corporate security managers**
  The large number of employees who work some or all of the time from home, coupled with the fact that 83 percent of routers in the US have unpatched vulnerabilities[xxvii], leads us to believe that a rapidly growing threat focus will be employees working from home. The relatively low use of VPNs, which ranges from 18 percent to 30 percent worldwide[xxviii], will contribute significantly to this threat and will motivate corporate security managers to address the security of their employees' home-based security infrastructure in a much more serious way.

- **Malware will be used to damage the reputations of celebrities and high level government officials**
  A tool commonly used to tarnish the reputations of celebrities, nominees to high level government positions and others is to reveal information they have posted to social media in the past, sometimes many years past. Osterman Research believes that in a few cases during 2019, some will go one step further and use malware to install compromising content on the computers, social media accounts or cloud accounts of celebrities and others. For example, while malware has been used in the past to install child abuse images on the computers of victims, such as in a 2009 case involving an employee for the Commonwealth of Massachusetts[xxix], we believe this approach will be used to discredit a few high-profile individuals in 2019.

- **The market for security awareness training will grow significantly**
  Employees are the last line of defense in any security infrastructure. Because technology-based solutions cannot block 100 percent of malicious content 100 percent of the time, employees need to be trained to deal with the phishing,

The ransom-ware problem was terrible in 2016, got worse in 2017, softened a bit in 2018, but will make a comeback in 2019.

spearphishing and other threats that will inevitably reach them. While the market for security awareness training has been growing at a healthy pace over the past several years, the fairly recent spate of acquisitions in this space by mainstream security solution providers will accelerate the trend at an even faster pace.

- **The market for web isolation technology will explode**
  A significant share of malware and other threats enters the corporate network through web browsing, webmail access and the like. To combat this, organizations of all sizes will increase their use of web isolation technology to prevent this avenue of attack from being effective. While these technologies have been available for several years, we believe that 2019 will be the breakout year for them.

  It's important to note that there are other options for protection of web-based phishing threats, including technologies for real-time detection of previously unknown phishing sites, as well as automated ingestion of real-time malicious site blacklists. This provides protection against fast-moving, zero-hour phishing threats that would normally evade more static, slow-moving threat feeds.

Steps to Improve Security

Osterman Research recommends a multi-step approach to improving security:

- **Start at the top**
  It's imperative that senior management and the board of directors in any organization get on board with cybersecurity and the need to make security a top priority. This includes increasing the cyberawareness of senior managers and board members, including CISOs or other technically savvy individuals on the board, and regularly putting cybersecurity on the agenda at senior management and board meetings.

- **Appreciate the risks**
  Decision makers need to understand the risks their organizations face from phishing, spearphishing, CEO Fraud/BEC, ransomware, traditional malware, cryptomining malware, other threats and user mistakes. They must address them as a high priority and provide the resources their security teams need to ensure they are managed adequately. While that seems obvious, many decision makers give intellectual assent to the risks they face without taking them to heart.

- **Conduct a thorough audit**
  A complete audit of the organization's current security infrastructure should be conducted, including the organization's security awareness training programs, the security capabilities they have in place, and the processes they have in place to remediate security incidents. This is essential to identify the gaps that may (and probably do) exist, and it can be used to prioritize spending to address the problems it finds.

- **View security in a holistic way**
  Instead of viewing security as a set of point solutions to address specific problems, focus on security holistically, from the cloud services that are deployed to detect and remediate threats all the way down to each endpoint solution. This does not mean that a single vendor must be used for all security solutions, but it does mean that solutions should be integrated and that security managers and analysts have a single view into everything that is happening in their organization from a security perspective.

- **Establish thorough and detailed policies**
  All organizations need thorough policies and procedures for protecting sensitive data and other assets. For example, they should include:

Decision makers need to understand the risks their organizations face.

- How passwords should be managed, including password requirements, frequency of password changes, rules against use of the same password on multiple systems, how passwords are stored, etc.
- Acceptable use policies for all communication, collaboration and related tools that will be used, including personally managed/owned devices, applications and services. This should include non-business tools, such as personal social media accounts.
- The frequency with which every system is backed up and the practices for doing so, including backup testing procedures.
- The methods for employees to handle and share sensitive and confidential data, including encrypting and classifying this data, as well as the tools they can use to send and store this information.
- Dual-control procedures should be established to ensure that one employee cannot steal or delete highly sensitive data assets.
- Creation of rules for how and why sensitive data assets are made available via the corporate network and which should be air-gapped.
- Establishment of requirements for the use of at-rest and in-use encryption for every platform, especially mobile devices and laptops. This should also include the ability to wipe these devices if they are lost or stolen – including personally owned devices.

- **Implement and revise corporate procedures**
  Every organization should update their company procedures on a regular basis. These procedures should focus on how sensitive and confidential data assets are managed, accessed and protected. For example, there needs to be an effective set of backup, restoration and testing procedures for all critical data assets so that the organization can recover quickly from ransomware or other malware infections. Moreover, dual-control procedures should be implemented for access to critical data assets, especially those that are focused on financial transactions, so that a single, disgruntled employee cannot cause a breach.

- **Work on improving user behavior**
  There are several best practices to address the cybersecurity gaps that might exist in the organization. For example:

  - Every employee in an organization – including senior executives who are the most likely to be the target of a CEO Fraud/BEC attack – should be reminded about the risks associated with oversharing information on social media, since this information can be used to craft CEO Fraud/BEC attacks.
  - Employees who deal with sensitive data or financial assets should have pre-established "backchannels", or out-of-band communication methods, provided to them for verifying sensitive requests. For example, if the CFO receives a request from the CEO to transfer money, he or she should have an alternate method of contacting the CEO to verify the request.
  - All staff members should use passwords that match the sensitivity and risk associated with the assets they are accessing. These passwords should be changed on a regular schedule enforced by IT. Multi-factor authentication should be used wherever necessary.
  - Patches should be applied to all software and operating systems as soon as they are available.

There are several best practices to address the cybersecurity gaps that might exist in the organization.

  - All endpoints should be configured with robust endpoint security if these devices will access any type of corporate resources like email or databases with sensitive information. This includes employees' personally owned computers and devices if they access corporate resources while traveling or at home.

- **Train everyone adequately and frequently**
  All users should participate in a good security awareness training program that will help them to make better judgments about the emails they receive, how they use social media, how they surf the web, and so forth. The goal is to increase user skepticism and awareness about what they receive in email, what they view on social media, and what they consider to be safe to access.

  To be fair, security awareness training by itself won't make an organization completely safe, but it will improve users' ability to be more aware of security issues and reduce the likelihood of security threats becoming successful. It's essential to invest enough in employee training so that the "human firewall" can provide a robust line of defense against increasingly sophisticated phishing and other social engineering attacks. In most cases, senior executives should have specialized or additional training to deal with the specific types of threats they will face, since they are higher value targets to cybercriminals and the consequences of their failure can be much greater.

- **Deploy good alternatives**
  A growing number of organizations allow employees to use their own smartphones, tablets, file-sharing accounts, mobile apps, cloud storage services and other resources. While this keeps IT from having to provide all of these tools to users, it can create huge security holes. Consequently, it's essential for IT to offer good alternatives to the solutions that employees have deployed, or might want to deploy. This includes solutions for file-sync-and-share, voice-over-IP, cloud storage, real-time communications and other capabilities that employees use because they don't have an equivalent capability from IT, or because IT-provided solutions are not as good as the free or freemium solution that employees use. Providing an IT-approved solution that is as good as the solutions that employees have deployed on their own can enhance cybersecurity and give IT more control over corporate content.

Sponsor of This White Paper

KnowBe4, the provider of the world's largest integrated new-school security awareness training and simulated phishing platform, is used by more than 17,000 organizations worldwide. KnowBe4 was created to help organizations manage the ongoing problem of social engineering through a comprehensive new-school awareness training approach. Organizations leverage KnowBe4 to enable their employees to make smarter security decisions and create a human firewall as an effective last line of defense when all security software fails. To learn more, please visit www.knowbe4.com.

KnowBe4
Human error. Conquered.

www.knowbe4.com
@KnowBe4
info@knowbe4.com
+1 855 566 9234

REFERENCES

[i] https://www.infosecurity-magazine.com/news/median-dwell-time-for-hackers/

[ii] https://www.helpnetsecurity.com/2017/03/06/frustrate-cio-ciso/

[iii] https://www.npr.org/2018/12/05/673958138/georgia-charges-iranians-in-ransomware-attack-on-atlanta

[iv] https://www.forbes.com/sites/leemathews/2018/11/28/ransomware-attack-disrupts-emergency-services-at-ohio-hospital/#8ddd87822548

[v] https://fox59.com/2018/10/18/ransomware-attack-hits-server-with-personal-information-on-indiana-national-guard-personnel/

[vi] https://siliconangle.com/2018/10/16/north-carolina-water-utility-crippled-ryuk-ransomware-attack/

[vii] https://siliconangle.com/2018/09/27/feds-called-port-san-diego-crippled-ransomware-attack/

[viii] https://www.datto.com/blog/dattos-global-state-of-the-channel-ransomware-report-2018

[ix] https://www.infosecurity-magazine.com/news/email-mistake-costs-chicago-school/

[x] https://www.cio.com/article/2379122/careers-staffing/ex-network-engineer-faces-prison-after-admitting-he-sabotaged-employer-s-system.html

[xi] http://www.businessinsider.com/google-doc-phishing-worm-affected-fewer-than-01-of-gmail-users-2017-5

[xii] http://www.mailguard.com.au/blog/dropbox-scam-new-phishing-attack

[xiii] https://www.troyhunt.com/86-of-passwords-are-terrible-and-other-statistics/

[xiv] https://www.darkreading.com/informationweek-home/password-reuse-abounds-new-survey-shows/d/d-id/1331689

[xv] https://www.tripwire.com/state-of-security/featured/new-type-brute-force-attack-office-365-accounts/

[xvi] https://www.infosecurity-magazine.com/news/cybercriminals-earn-millions/

[xvii] https://www.thesslstore.com/blog/2018-cybercrime-statistics/

[xviii] https://www.darkreading.com/attacks-breaches/cybercriminals-launder-up-to-$200b-in-profit-per-year/d/d-id/1331298

[xix] https://nvd.nist.gov/general/nvd-dashboard

[xx] https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/

[xxi] https://www.zdnet.com/article/after-seven-months-and-no-microsoft-patch-internet-explorer-8-vulnerability-is-revealed/

[xxii] https://www.zdnet.com/article/malicious-sites-abuse-11-year-old-firefox-bug-that-mozilla-failed-to-fix/

[xxiii] https://www.zdnet.com/article/over-100000-pcs-infected-with-new-ransomware-strain-in-china/

[xxiv] Source: *2017 Internet Crime Report*, FBI

[xxv] https://securityintelligence.com/news/global-cost-of-cybercrime-exceeded-600-billion-in-2017-report-estimates/

[xxvi] https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/

[xxvii] https://www.digitaltrends.com/computing/83-percent-routers-vulnerable/

[xxviii] https://www.statista.com/statistics/306955/vpn-proxy-server-use-worldwide-by-region/

[xxix] https://www.theregister.co.uk/2009/11/09/malware_child_abuse_images_frame_up/