WHITE PAPER

Best Practices for Dealing with Phishing and Next-Generation Malware

An Osterman Research White Paper

Published April 2015

KnowBe4
Human error. Conquered.

OSTERMANRESEARCH

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

EXECUTIVE SUMMARY

An attorney in the greater San Diego area opened an attachment in a phishing email that he thought was sent to him by the US Postal Service. The attachment installed malware on his computer, and shortly thereafter he found that $289,000 had been transferred from his firm's account to a bank in China[i].

An email attack on Fazio Mechanical, an HVAC contractor in Sharpsburg, PA, was able to penetrate the organization's email defenses and infected at least one computer with a variant of the ZeuS banking Trojan. About two months later, that infiltration was used in the attack on Target Corporation that resulted in the breach of information for approximately 110 million customers[ii].

A law firm in Charlotte, NC transferred $387,000 to a bank in Virginia Beach, VA after it closed a deal. Shortly thereafter, cybercriminals transferred most of this amount to the law firm's bank in Charlotte, which transferred the funds to a bank in New York and then to a bank in Moscow. The victim organization believes it had been infected with keystroke logging software from a phishing email that captured all of the critical information necessary to initiate the wire transfer[iii].

These are all examples of the types of the phishing and malware threats that are becoming more commonplace as cybercriminals become more adept, stealthier, and more able to penetrate corporate security defenses. The consequences of even a single such attack can be enormous, resulting in the potential loss of millions of dollars from corporate financial accounts, the loss of sensitive customer data, the loss of intellectual property like trade secrets or marketing plans, and possibly the dissolution of a business.

KEY TAKEAWAYS

To combat phishing attempts and next-generation malware, organizations of all sizes should consider a variety of issues related to security:

- Cybercriminals are getting better, users are sharing more information through social media, and some anti-phishing solutions' threat intelligence is not adequate. This makes organizations more vulnerable to phishing attacks and other threats.
- Moreover, malware is "improving" and is harder to detect and remediate. For example, malware is better able to detect when it has been placed into a sandbox, attackers can coordinate their attacks, threats can remain dormant for an extended period and are therefore less likely to be detected, one piece of malware can operate another, and some malware requires user interaction before going into action.
- Users should be considered the first line of defense in any security infrastructure, and so organizations should implement a robust training program that will heighten users' sensitivity to phishing attempts and other exploits.
- IT should implement robust and layered security solutions based on good threat intelligence, including how the cloud should be used as part of a robust security infrastructure.
- IT and business decision makers should implement best practices to help users more carefully screen their electronic communication and collaboration for phishing and other social engineering attacks.
- IT should deploy enterprise-grade alternatives to the consumer-focused file sync and share, file-transfer, real time communications, and other applications that are commonly used today.

- Decision makers should conduct a thorough analysis of the entire organization to understand where data is stored and who has access to it, as well as the tools that employees are using to access corporate data and network resources.

- IT should establish detailed and thorough acceptable use policies for the use of every type of communication or collaboration system that is in place now or might be used in the foreseeable future.

ABOUT THIS WHITE PAPER

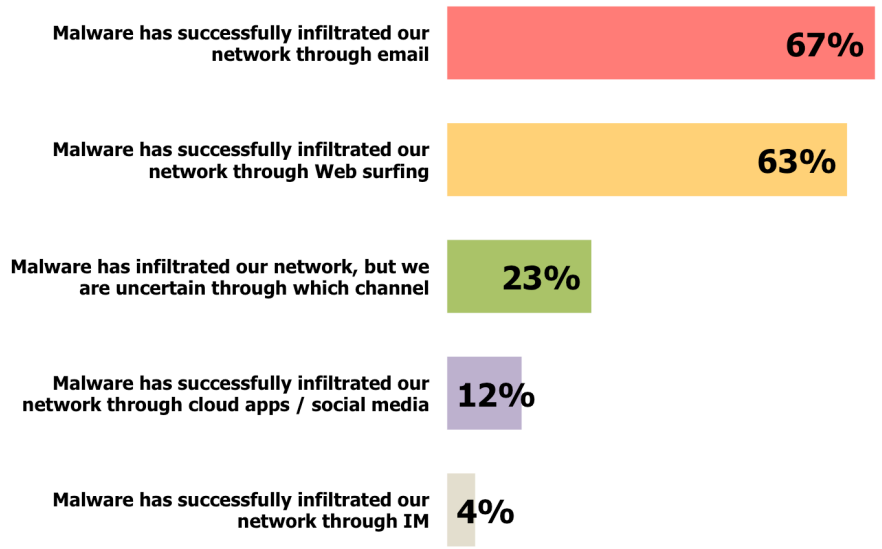
This white paper focuses on the current security problems with email and other systems, and it offers recommendations about how to improve security. This white paper was sponsored by Intel Security – information on the company is provided at the end of the white paper.

PRIMARY SECURITY CONCERNS

SECURITY PROBLEMS DURING THE PAST 12 MONTHS

Security decision makers are concerned – and rightly so – about the effectiveness of their security defenses to prevent infiltration of malware. As shown in Figure 1, email is the leading source of malware infiltration into an organization, followed closely by the Web in second place. More disturbing, however, is the significant proportion – nearly one in four – that have seen malware enter the corporate network through a source they have yet to discover.

Figure 1
Malware Infiltrations That Have Occurred During the Past 12 Months



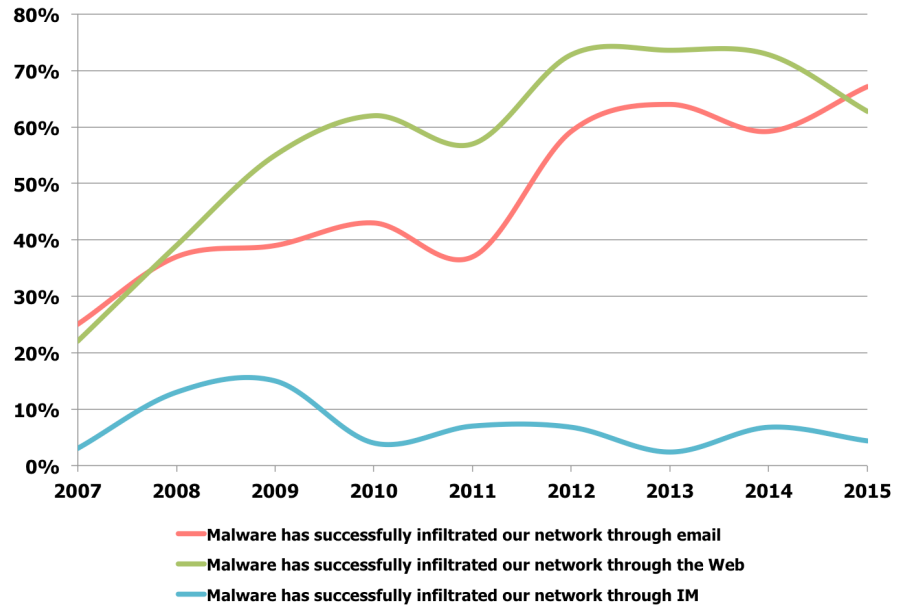
Source: Osterman Research, Inc.

If organizations cannot identify a successful security compromise, decision makers may never know that a particular event took place until it's too late. As a result, while decision makers have correctly acknowledged the security compromises of which they are aware, those about which they are not aware pose a more significant problem. It is likely that the actual rate of successful infiltrations or other leakage events is much higher than reported in the figure above because of poor organizational systems for tracking successful threats.

MALWARE INFILTRATIONS OVER TIME

Malware infiltration is generally getting worse over time, as shown in Figure 2. In 2015, however, we discovered that email has once again become the most serious incursion point for malware. Interestingly, while the Web was the primary threat vector for malware for several years, email reclaimed its place as the leading entry point for malware in 2015. The growing use of phishing as an attack vector leads us to believe that email will remain the most important entry point for malware for the next several years.

Figure 2
Malware Infiltrations for the Period 2007 to 2015



Source: Osterman Research, Inc.

FALSE POSITIVE REMAIN AN ISSUE

There is significant room for reducing the false positive ratio generated by anti-spam systems. Clearly, even a very small percentage of false positives can result in a large number of valid messages being misclassified and unavailable for their intended purpose. While false positives generated by anti-spam solutions are not considered a "sexy" problem to overcome by many decision makers, this is a problem that must be addressed for two reasons:

- Email users must spend time searching through their spam quarantine for mischaracterized valid emails in order to make sure that important business content, such as client inquiries or purchase orders, is not missed. This not only wastes employee time, but valid emails can still be missed because users do not recognize them as non-spam emails.

- An email user may identify a phishing attempt or other malicious email as valid and remove it from the quarantine, thereby potentially exposing the organization to the payload it contains or the malicious content to which it links.

ISSUES THAT CONCERN DECISION MAKERS MOST

Our research revealed that while malware incursions arising from employees' use of the Web was the single most serious concern of security-focused decision makers and influencers, the next five concerns all focused on phishing and phishing-related activities, and/or the consequences of a phishing attack, as shown in Figure 3. The

greater concern about Web-based malware as opposed to phishing may be due to the fact that while the Web was the primary threat vector for several years, some decision makers have not reacted quickly enough to the reemergence of email as an increasingly serious infiltration point for malware. This underscores the need to refocus as threats change, and to consider just how dangerous email is as a threat for malware entry.

Figure 3
Decision Makers' and Influencers Concerns About Key Security Issues
% Responding a Serious or Very Serious Concern

Concern	%
Malware being introduced from employees' Web surfing	49%
Phishing attacks	45%
Employees clicking on links within email which download malware	44%
Employees clicking email attachments which download malware	44%
Breaches of sensitive customer data	39%
Breaches of sensitive internal data	37%
Virus/worm/malware infections	37%
Malware being introduced from employees' personal Webmail	33%
Data loss from employees sending confidential info via cloud-based tools like Dropbox	29%
The lag between new virus outbreaks and when our AV vendor issues an update to deal with these outbreaks	27%
Data loss from employees sending confidential info via email	26%
Direct hacker attacks	24%
Spam - your IP address getting blacklisted due to outbound mail attack	23%
Mobile malware	23%
Spam – the amount of unsolicited email your organization receives	22%
Data loss from employees sending confidential info via social media	22%
Denial-of-service attacks	20%
Users off-network creating security problems	19%
Graymail – the amount of email users solicited (opted into) and now perceive as spam	18%
Time spent by email administrators dealing with malware	18%
Malware being introduced from employees' home computers	17%
Malware being introduced from employees' use of cloud apps	16%
Employees viewing inappropriate content on the Web	16%
Spam – the amount of false positives caused by your anti-spam system	16%
Time spent by email administrators dealing with spam	15%
Time spent by employees dealing with spam	11%

Source: Osterman Research, Inc.

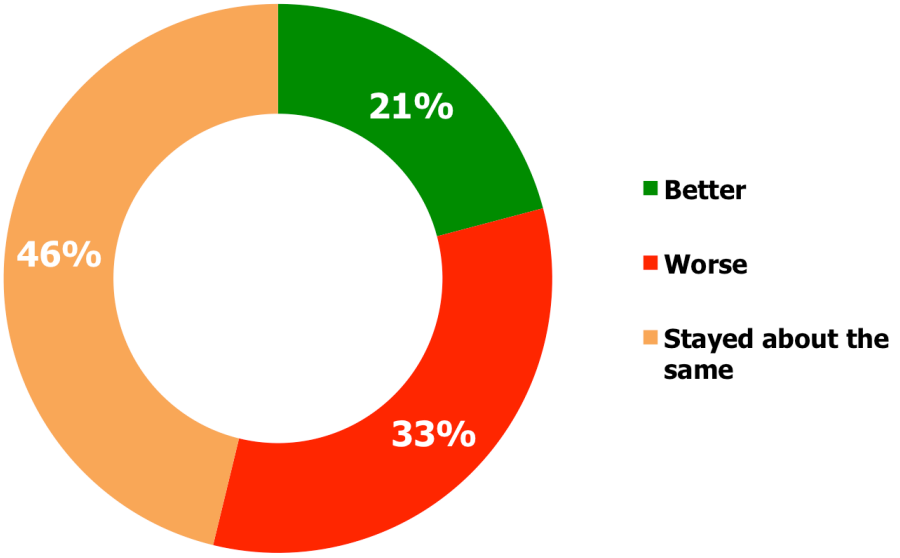
It is also important to note that while spam ranks fairly low on decision makers' list of concerns, the use of spam as a delivery vehicle for phishing attempts is rampant. Consequently, its accurate detection and remediation must be a top priority in any security infrastructure.

SECURITY NEEDS SIGNIFICANT IMPROVEMENT

PHISHING IS A CRITICAL ISSUE

As discussed in the previous section, five of the six most serious concerns of security-focused decision makers and influencers are directly related to phishing attacks or the aftermath of a successful such attack. Moreover, as shown in Figure 4, the phishing problem has remained more or less static over the past twelve months for nearly one-half of organizations, but has become decidedly worse for one-third of them. For only one-fifth of organizations has the phishing problem become a less significant security issue.

Figure 4
"Over the past year, has the phishing problem you experience gotten better, worse, or stayed about the same?"



Source: Osterman Research, Inc.

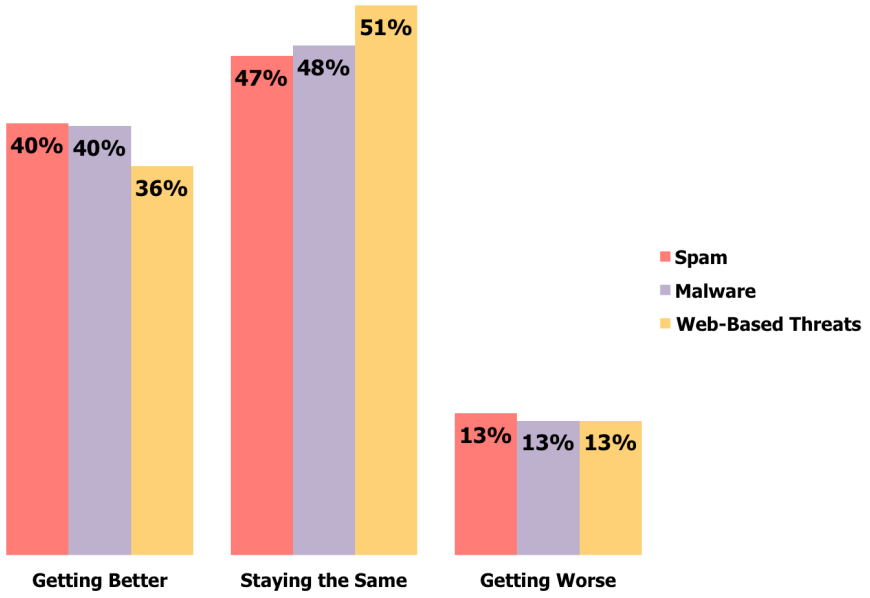
SECURITY SOLUTIONS ARE IMPROVING ONLY SLIGHTLY

The ability for organizations to block spam, malware and Web-based threats[iv] is improving for between 36% and 40% of organizations over time. However, as shown in Figure 5, the ability to block these threats is remaining relatively static over time for between 47% and 51% of organizations, and is actually getting worse for about one in eight organizations.

It is important to note that spam, malware and Web threats cannot be considered as distinctly separate threats. For example, many spam messages contain links to malicious Web sites that can infect an endpoint with malware or can be used to transmit a malicious attachment, while Web-based threats will also include the infection of endpoints with malware.

Moreover, it is also important to note that while the data in Figures 4 and 5 may seem to be somewhat at odds, there is a significant difference between them: the data shown in Figure 4 is focused on the overall phishing problem over the past 12 months – the amount of phishing attempts received, users' responses to them, and the security team's ability to prevent them from reaching end users – while the problems shown in Figure 5 deal only with the ability to *block* these threats over a longer period.

Figure 5
Improvement in Proportion of Threats Blocked Over Time



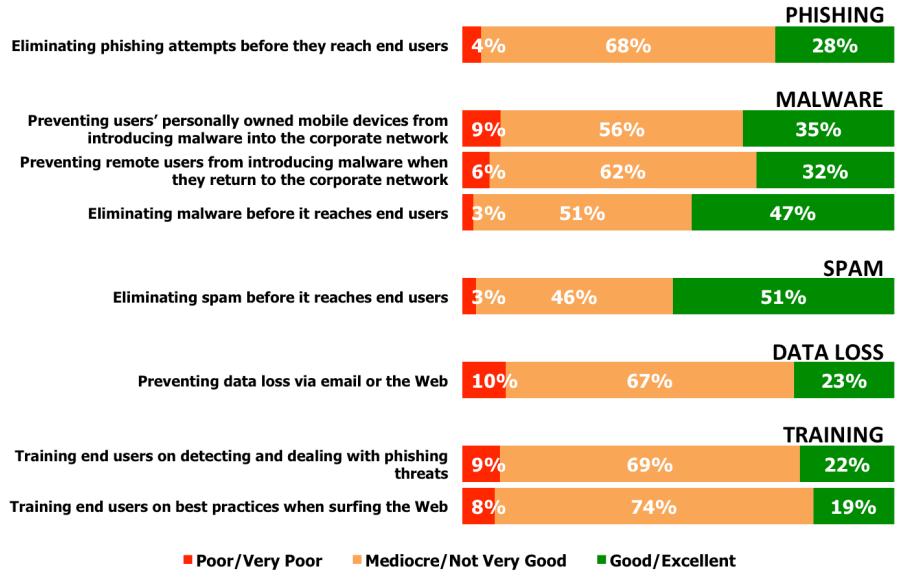
Source: Osterman Research, Inc.

SECURITY EFFECTIVENESS VARIES WIDELY

The effectiveness of organizations' security defenses varies widely, as shown in Figure 6. For example, for more "traditional" defenses like detecting and remediating spam and some forms of malware, security-focused decision makers and influencers believe their organizations do a reasonably good job: 51% rate themselves as "good" or "excellent" when it comes to eliminating spam, while 47% believe they are this effective at eliminating more traditional forms of malware.

However, as the threat vectors become more complicated and sophisticated – dealing with security on personally-owned devices, preventing malware incursions delivered via users who employ file sync and share tools, or dealing with phishing – confidence in the efficacy of existing security defenses declines substantially. Most notably, organizations believe that their training efforts for helping users to detect and avoid security threats are fairly ineffective.

Figure 6
Security Defense's Effectiveness Against Various Threats/Problems



Source: Osterman Research, Inc.

WHY IS PHISHING SO SUCCESSFUL?

Although the success of phishing attempts varies based on the victim's gullibility, their training, their organization's security defenses and other factors, there are three important reasons that phishing is so successful today:

- Cybercriminals are getting better at their craft. Their use of logos, professionally crafted messages, and personalization of content makes phishing attempts more believable, and so prospective victims are more likely to click on the links and attachments contained within them.

- Users are sharing an increasing amount of information through social media, thereby providing cybercriminals with the fodder they need to craft personalized and more believable messages.

- Some anti-phishing solutions are not supported with a sufficiently robust database of real-time messaging intelligence, and so can fall prey to the latest techniques used by phishers.

MALWARE IS IMPROVING

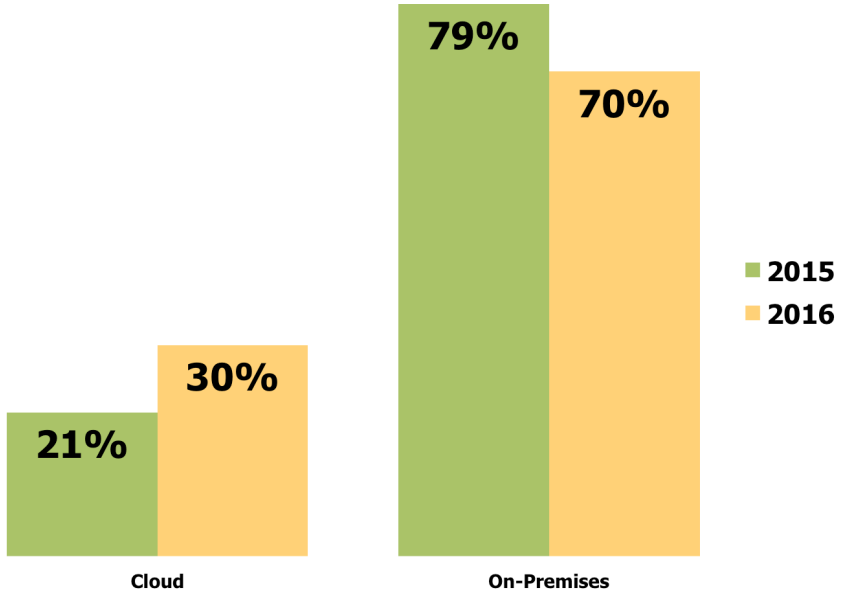
Cybercriminals are becoming more adept at accomplishing their goal of stealing financial or other data. For example, some malware variants can detect when it has been placed into a sandbox and so will not execute its code. Attackers can coordinate their attacks among various delivery venues, including email, the Web, social media, files, etc. Threats can remain dormant for an extended period and are therefore less likely to be detected by many traditional anti-phishing and anti-malware solutions. One piece of malware can operate another that appears to be innocuous. Some malware requires user interaction, such as clicking on a button in a dialog box, before going into action.

The bottom line is that malware, phishing and other threats are becoming more challenging and more difficult to address.

MANY VIEW THE CLOUD AS A BEST PRACTICE TO IMPROVE SECURITY

Our research revealed that spending for cloud-based security will increase significantly by early 2016, growing from 21% of all security spending in 2015 to 30% by early 2016, as shown in Figure 7. While on-premises security infrastructure and spending will continue to dominate for the foreseeable future, the trend is clearly moving away from on-premises systems as a proportion of total spending, although Osterman Research anticipates that both will grow substantially as organizations deploy hybrid cloud and on-premises solutions to create a more layered infrastructure.

Figure 7
Spending for Cloud and On-Premises Security, 2015 and 2016



Source: Osterman Research, Inc.

The use of cloud-based solutions to thwart phishing attempts and other malicious content from reaching endpoints can be an important best practice in either bolstering an existing, on-premises security infrastructure or adding another layer of defense to a cloud security solution. Many organizations have enough to deal with when it comes to phishing and malware, and so use of cloud-based solutions is viewed by many decision makers as an important supplement to existing defenses.

CURRENT AND PREFERRED SECURITY DELIVERY MODELS

A separate Osterman Research survey found that organizations have a much stronger preference for a small number of security systems that can be managed via a single interface, and that they have a lower preference for the use of best-of-breed solutions that are managed using different interfaces, as shown in Figure 8. This includes both cloud-based and on-premises solutions.

Figure 8
Current and Preferred Delivery Models for Security

Delivery Model	Current	Preferred
ON-PREMISES security solutions offered by one or only a small number of vendors and all of them managed through a single interface	22%	32%
ON-PREMISES, point, best-of-breed solutions from multiple vendors, each of which is managed through a different interface	60%	26%
CLOUD-BASED security solutions offered by one or only a small number of vendors and all of them managed through a single interface	15%	22%
CLOUD-BASED, point, best-of-breed solutions from multiple vendors, each of which is managed through a different interface	4%	8%
Not sure	--	12%

Source: Osterman Research, Inc.

There is a significant difference between the types of security solutions that many organizations use today and what they would like to use. Three out of five organizations presently use on-premises, best-of-breed point solutions from several vendors, each with a different management interface. However, only one-quarter of organizations would actually prefer to do so. In contrast, while just over one-fifth of organizations currently have on-premises solutions offered by a single or small number of vendors with a single management interface, one-third want to have such a solution. There is a similar difference between the current and preferred situation with cloud-based solutions from a single or small number of vendors – at 15% currently to 22% preferred.

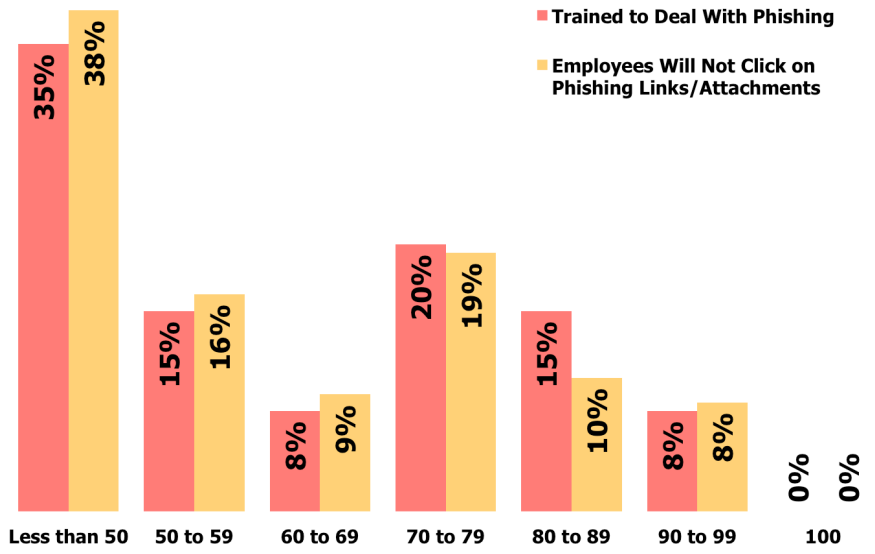
This is often an issue of market and product maturity. When products are not as mature as they should be and are being updated quickly, there is normally a significant difference in product effectiveness between established and new entrant vendors. Decision makers then have to choose between product effectiveness (and support multiple products from different vendors) or fewer vendors (generally with less product efficacy). As the market matures and vendor consolidation takes place, the dominant vendors work to integrate their various products and deliver improved integration. As this takes place, there is a transition period for organizations as they migrate from multiple systems to more integrated alternatives.

The results in the figure above with regard to the use of best-of-breed reflects, to some extent, the fundamental difference between on-premises solutions and cloud-based alternatives. When the infrastructure is maintained on-premises, different vendors' best-of-breed solutions can be employed because email is passed from one to the other efficiently and quickly. However, the same model cannot be efficiently applied to the cloud: sending email for filtering or other management functions from one cloud provider to another introduces significant latency into message processing and delivery, creates an additional number of potential failure points, and consumes significant bandwidth.

LOW CONFIDENCE FOR USER-FOCUSED PHISHING DEFENSES

As noted earlier, security-focused decision makers and influencers rated their security training as less effective than other aspects of their security defenses. The low rating for security training is further demonstrated in Figure 9, which shows that one-half of organizations have little confidence (scoring less than 60 on a scale of 0-100) in their organizations' training programs for phishing training, while an even larger proportion has this low level of confidence in their employees choosing not to click on links or attachments that appear in phishing emails.

Figure 9
Confidence in Employee Training and Behaviors Related to Phishing
Rated on a scale of 0 (no confidence) to 100 (very confident)



Source: Osterman Research, Inc.

VARIED APPROACHES TO SECURITY TRAINING

The approaches to security awareness training vary substantially, as shown in Figure 10. For example, 30% of the organizations surveyed for this white paper use the "Break Room Approach", an informal approach to security training that provides instruction on how to detect and avoid problems with phishing emails or basic Web surfing. A smaller proportion show short videos to their employees to make them more aware of security issues and best practices, while about one in five organizations provides no security awareness training whatsoever.

However, our research did find that slightly more than one in five organizations take a more proactive and formalized approach to security awareness training, conducting training on security awareness, following up with testing of various kinds to determine how well this training worked, and providing further follow-up, as necessary.

Figure 10
Approaches to Security Awareness Training
% of Organizations

Approach	%
The Break Room Approach: We gather employees for a lunch or special meeting and tell them what to avoid when surfing the Web, in emails from unknown sources, etc.	30%
The Monthly Security Video Approach: We have employees view short security awareness training videos to learn how to keep the network and organization safe and secure.	26%
The Do Nothing Approach: We don't really do security awareness training.	21%
The Phishing Test Approach: We pre-select certain employees, send them a simulated phishing attack, and then see if they fall prey to the phishing attack.	14%
The Human Firewall Approach: We test everyone in the organization find the percentage of employees who are prone to phishing attacks, and then train everyone on major attack vectors, sending simulated phishing attacks on a regular basis.	8%

Source: Osterman Research, Inc.

KEEPING UP IS INCREASINGLY DIFFICULT

One of the fundamental problems in managing security today is the speed with which malware variants are created and distributed. For example, on average there are 10,000+ new malware threats discovered every sixty minutes. This means that even if a malware engine is updated on an hourly basis, many new variants will not be detectable and so will have the potential to infect endpoints.

A key element in the success of phishing attempts using links is the rapidity with which domains can be created. For example, a phishing attempt containing a link is sent to victims, but the link points to a Web site that contains no malicious content. Consequently, many anti-phishing solutions will assume that the link is innocuous because the link points to a "safe" location. Only after the email has been sent and the link destination verified as safe will cybercriminals introduce malware to the site, thereby infecting visitors who click on the link in the email.

The stealthiness of a growing proportion of malware is increasing. For example, sandbox technology is increasingly used to evaluate suspicious files or untested code to determine if it contains malware or otherwise represents a threat. The goal of the sandbox, which is normally run on a virtual machine, is to allow malware to become manifest in a secluded environment where it can do no harm. However, malware authors can now detect if their content is running in a sandbox environment and so the suspect files will either stop working or wait to execute until after the content has been determined to be "safe".

Another very serious issue is the potential for malware to remain despite any attempts to eradicate it. For example, the Equation Group has developed malware that can infect hard drive firmware and that cannot be eradicated[v]. While this form of malware is extremely rare given the Equation Group's focus on only very high value targets, it represents a troubling development that could potentially impact a more mass-market victim base in the future.

KEY THREATS TO CONSIDER

Organizations of all sizes face a wide variety of threats, ranging from seemingly innocuous incursions like spam that create storage problems and general annoyance, to highly targeted email attacks that can create major breaches of sensitive or confidential information. Among the range of threats to consider are the following:

- **Phishing emails**
  Phishing emails are comparatively unfocused email messages that are designed to elicit sensitive information from users, such as login credentials, credit card information, Social Security numbers and other valuable data. Phishing emails purport to be from trustworthy sources like banks, credit card companies, shipping companies and other sources with which potential victims already have established relationships. More sophisticated phishing attempts will use corporate logos and other identifiers that are designed to fool potential victims into believing that the phishing emails are genuine.

  The impact of phishing emails should not be underestimated. An Osterman Research survey conducted in late 2014 found that there have been a variety of security incidents that were attributable to malicious emails, such as 41% of organizations that have lost sensitive data on an employee's computer and 24% that have lost sensitive data from the corporate network.

- **Spearphishing emails**
  A spearphishing email is a targeted phishing attack that is generally directed at a small group of potential victims, such as senior individuals within a company or other organization. Spearphishing emails are generally quite focused, reflecting the fact that a cybercriminal has studied his or her target and has crafted a message that is designed to have a high degree of believability and a potentially high open rate.

  One of the reasons that spearphishing is becoming more effective is that potential victims provide cybercriminals with the fodder they need to craft believable messages. For example, Facebook, Twitter, LinkedIn and other social media venues contain enormous amounts of valuable information about travel plans, personal preferences, family members, affiliations, and other personal and sensitive information that can be incorporated into spearphishing emails.

- **Remote users accessing corporate resources**
  Employees, contractors and others who access resources on the corporate network, such as those working from home or in another remote site, are a key source of threats. An unprotected user accessing a corporate asset, such as Outlook Web Access that is not accessed via a VPN, or a laptop computer that becomes infected and later is connected to the corporate network, can constitute a serious threat. This is becoming a serious problem for most organizations as users employ personally owned devices like their own smartphones, tablets and other traditionally consumer devices in a workplace setting.

- **Consumer file sync and share tools**
  Closely related to the point above is the widespread and growing use of consumer file sync and share tools like Dropbox, Microsoft OneDrive and Google Drive, among many others. These tools are commonly used by employees to make their files available on all of their desktop, laptop and mobile platforms for access when traveling, when they work from home, or when they are otherwise away from the office. While these tools are quite useful and generally work as they are intended, they represent an important incursion point for malware. For example, an employee who accesses his or her corporate files on a home computer, many of which do not have the latest anti-virus updates and whose use is not controlled by any sort of sophisticated security infrastructure, can inadvertently infect these files with malware. When the files are synced back to the employee's desktop computer, malware can readily infect the network

because it may have bypassed corporate email, Web gateway and other defenses. In an alternative infection scenario, an employee working from home can have files infected from their home computer and then send these files to a client or business partner without the files ever having passed through the corporate security infrastructure.

- **Watering holes**
  This is a type of social engineering attack in which cybercriminals will identify key Web sites that are frequented by individuals or groups they would like to infiltrate, such as mobile app developers. These targeted Web sites are then infected with malware, the goal of which is to infect members of the affinity group. An example of one such attack was an iOS mobile developers' forum that hosted malware and was targeted against Apple and Facebook[vi].

- **Employee errors**
  Employees will sometimes inadvertently install malware or compromised code on their computers. This can occur when they download a codec, install ActiveX controls, install various applications that are intended to address some perceived need (such as a capability that IT does not support or that a user feels they must have), or when they respond to scareware/fake anti-virus (rogue AV or fake AV) software. Scareware is a particularly dangerous form of malware because it preys on users who are attempting to do the right thing – to protect their platforms from viruses and other malware. Even users who are quite experienced can be fooled by a well-crafted scareware message.

- **Malvertising**
  Malicious Internet advertising is intended to distribute malware through advertising impressions on Web sites. An Online Trust Alliance brief discussed how a single malvertising campaign can generate 100,000 impressions, with approximately 10 billion malvertising impressions occurring in 2013 via more than 200,000 malvertising incidents[vii]. Underscoring just how serious the malvertising problem has become, a study by RiskIQ for the period January to September 2013 found that 42% of malvertising is carried out by drive-by exploits that did not require interaction by end users (58% of malvertising involves users clicking on malicious advertisements)[viii].

- **Mobile malware**
  The growing use of smartphones and tablets, particularly personally owned devices, is increasingly being exploited by cyber criminals. For example, Alcatel-Lucent found that 16 million mobile devices were infected with malware during 2014, an increase of 25% from 2013[ix]. This represents an infection rate of 0.68%, meaning that in an organization of 1,000 employees, each of whom has an average of 1.5 mobile devices, there will be a total of 102 infected mobile platforms at any given time. The vast majority of infections impact Android devices – the Alcatel-Lucent research suggests that under 1% of iPhone and BlackBerry devices are infected with malware.

- **Mobile copycat applications**
  Many developers distribute their mobile apps through vendor and third party stores that offer varying levels of security, much of it inadequate. Some app stores are highly secure operations and require that developers satisfy rigorous standards before their apps can be offered. Others' standards, however, are less stringent and create the opportunity for serious security risks. The result is that many third-party app stores are susceptible to a number of security and related problems like the distribution of copycat apps and malware distribution.

- **Compromised search engine queries**
  Valid search engine queries can be hijacked by cybercriminals to distribute malware. This form of attack relies on poisoning search queries, resulting in the display of malware-laden sites during Web searches. Search engine poisoning is

particularly effective for highly popular search terms, such as information on celebrities, airline crashes, natural disasters and other "newsy" items.

- **Botnets**
  Botnets are the cause of a large number of successful hacking and phishing attacks against many high-profile targets. For example, Sony, Citigroup, the US Senate, Lockheed Martin, the International Monetary Fund, Northrup Grumman, and RSA have all been victimized by botnet attacks. The result has been that millions of records have been exposed that will result not only in the disclosure of personal and sensitive information, but also lawsuits and other expensive remediation efforts.

- **Hacking**
  This is a form of specialized cyberattack in which cybercriminals use a number of techniques in an attempt to breach corporate defenses. An example of a successful hacking attack is the recent incursion against Sony Pictures that may have been carried out by an operation of the North Korean government.

- **Gullible users**
  Users can represent a major security threat because of a combination of their specific personality types and inadequate training. For example, 100 students from an undergraduate psychology at the Polytechnic Institute of New York were sampled[x]. These students a) completed a survey focused on their beliefs and habits with regard to online behavior; b) asked about how likely they thought they would be the victim of online crime, such as password theft; and c) completed a personality assessment survey. After completing these activities, these students were then sent obvious phishing emails.

  One out of six of those tested – most of whom were engineering or science majors – fell for the scam emails. Ignoring the gender differences of those who were most likely to fall for the phishing emails in this study, the researchers found that those with the most "open" personalities – i.e., those who are most extroverted – were more likely to fall for phishing scams. The findings strongly suggest that people who overshare on Facebook or Twitter, for example, are more likely to become victims of phishing scams and other online fraud than those who are more introverted, share less or who don't have social media accounts. Another study found that younger students (aged 18-25) were more likely to fall for phishing scams than their older counterparts[xi].

- **Ransomware**
  One of the more common recent examples of ransomware is the CryptoLocker malware that encrypts victims' files and then demands ransom to decrypt them. Victims who choose not to pay the ransom within a short period of time will have their files remain encrypted permanently. Cryptolocker typically extorts a few hundred dollars per incident and is normally delivered through email with a PDF or .zip file disguised as a shipping invoice or some other business document[xii].

RECOMMENDATIONS

To address the risks associated with phishing and next-generation malware, Osterman Research recommends a variety of actions that any organization should undertake:

- **Understand the risk that your organization faces**
  The critical first step in developing a best practices approach to security is to understand, at least at a high level, the risks that an organization faces. Many decision makers do not sufficiently appreciate these risks because they are too busy, they don't have enough budget, or they have not focused enough on the growing number of risks they face. Consequently, Osterman Research recommends that security decision makers study the growing variety of security

risks in detail and realize that they represent a serious threat to their organization. While this sounds simplistic, too many decision makers take a defensive approach, waiting until bad things happen until they take action, when they should be much more proactive in order to prevent them to the greatest extent possible.

As just one example, organizations must monitor the risk levels associated with their data assets, corporate systems and other tools that users may employ in response to regulatory requirements, advice from legal counsel, recent data breaches, cybercriminal activity and other factors. For example, a database might contain non-sensitive data that can safely be accessed using only a username and password. However, a change in an organization's offerings or a new industry regulation may mean that sensitive data will be added to the database, thereby increasing the risk of inappropriate access of that content store.

- **Understand the breadth of tools that might be used (and maybe shouldn't be)**
  There are a number of capabilities that employees use that can create significant risks. For example:
  - Personal Webmail accounts that users employ when the corporate email system is down or when they need to send files that are too large to be sent by the corporate email system.
  - Consumer-focused file sync and share tools that give users access to all of their files from any platform, but that typically do not scan content for malware or other threats.
  - File-transfer tools that are designed to send very large files independently of the corporate email system, and so do not get scanned for malware.
  - Personally owned smartphones or tablets that can be the target of mobile malware.
  - Social media tools that can be used to send corporate content or that can allow malicious content to enter an organization via short URLs or malvertising links.
  - Employees' home computers, which often are shared by family members who download non-secure content, and for which anti-virus defenses are often out-of-date.
  - The growing variety of mobile apps, cloud-based applications and other tools that can subject corporate data to infiltration by malware or expose sensitive data to exfiltration by cybercriminals.
- **Conduct a complete internal audit**
  Organizations need to conduct a thorough audit to understand where all of their data is located, who has access to this data, the specific legal and regulatory obligations to which this data is subject, the identity of the data stakeholders, and other relevant information. This is essential in order to build a map of sorts that will help decision makers to understand the security risks they face and how to prioritize their resources in closing the security gaps that exist.
- **Establish detailed and thorough policies**
  Most organizations have not yet established sufficiently detailed and thorough policies for the various types of email, Web and social media tools that their IT departments have deployed or that they allow to be used. Consequently, we recommend that an early step for any organization should be the development of detailed and thorough policies that are focused on all of the tools that are or

probably will be used in the foreseeable future. These policies should focus on legal, regulatory and other obligations to:

- Encrypt emails and other content if they contain sensitive or confidential data.
- Monitor all communication for malware that is sent to blogs, social media, and other venues.
- Control the use of personally owned devices that access corporate resources.

Creating detailed and thorough policies will help decision makers not only to determine how and why each tool is being and should be used, but it also will help decision makers determine which capabilities can or cannot be migrated to cloud-based security solutions and which should be retained in-house.

- **Implement best practices for user behavior**
  The next step is to implement a variety of best practices to address the security gaps that have been identified. For example:
  - Employees need to employ passwords that match the sensitivity and risk associated with their corporate data assets. These passwords should be changed on an enforced schedule, and should be managed by IT.
  - Employees should be strongly encouraged and continually reminded to keep software and operating systems up-to-date to minimize a known exploit from infecting a system with malware.
  - Employees should receive thorough training about phishing and other security risks in order to understand how to detect phishing attempts and to become more skeptical about suspicious emails and content. It is important to invest sufficiently in employee training so that the "human "firewall" can provide the best possible initial line of defense against increasingly sophisticated phishing and other social engineering attacks.
  - Employees should be tested periodically to determine if their anti-phishing training has been effective.
  - Employees should be given training about best practices when connecting remotely, including the dangers of connecting to public Wi-Fi hot spots or other unprotected access points.
  - Employees need to be trained on why not to extract potentially suspicious content from spam quarantines that might end up being phishing emails.
  - Employees need to be given a list of acceptable and unacceptable tools to employ for file sync and share, social media and other capabilities as part of the overall acceptable use policies in place.
  - Ensure that all employees maintain robust anti-virus defenses on their personally managed platforms if access to any corporate content will take place on them.
  - Employees should be reminded continually about the dangers of oversharing content on social media. The world will not be a better place if it knows that you had breakfast in Cancun this morning, but it could give cybercriminals a piece of information they need to craft a spearphishing email.
- **Deploy alternatives to solutions that employees use today**
  Decision makers should seriously consider implementing tools that will replace

many of the employee-managed solutions in place today, but that will provide users with the same convenience and ease of use. For example, IT may want to deploy an enterprise-grade grade file sync and share alternative for the consumer version of Dropbox that is so widely used today. They may want to implement a business continuity solution that will enable corporate email to be used during outages instead of users falling back on their personal Webmail accounts. They may want to consider deploying an enterprise-grade file-sharing system that accommodates very large files if the corporate email system does not allow these files to be sent.

- **Implement robust and layered security solutions based on good threat intelligence**
  It almost goes without saying that it is essential to implement a layered security infrastructure that is based on good threat intelligence. Doing so will minimize the likelihood that malware, hacking attempts, phishing attempts and the like will be able to penetrate corporate defenses.

  An essential element of good security is starting with the human component. As we discussed above, users are the initial line of defense in any security system because they can thwart some potential incursions like phishing attempts before technology-based solutions have detected them. Consequently, we cannot overemphasize the importance of good and frequent user training to bolster this initial line of defense, the goal of which is to heighten users' sensitivity to phishing and related threats, and to help users to be less gullible. By no means are we suggesting that users can be the *only* line of defense, but they should be incorporated into the overall security mix.

- **Determine if and how the cloud should be used**
  A critical issue for decision makers to address is whether or not internal management of security, as well as other part of the IT infrastructure, is a core competency that is central to the success of the organization. Key questions that decision makers must answer are these:

  - Will our security improve if solutions remain on-premises?
  - Will managing security on-premises and managed by in-house IT staff contribute more to the bottom line than using a cloud-based provider?
  - Should a hybrid security approach with both on-premises and cloud-based solutions be use? If so, for which systems?

  Many organizations are considering cloud delivery for the various types of security services they manage because of their lower and more predictable costs; the ability to free internal IT staff for other initiatives; and the advantage of blocking unwanted and dangerous content before it can reach the corporate network. Plus, the use of a hybrid security architecture enables most unwanted content to be eliminated in the cloud, while leaving deeper content inspection for on-premises systems.

  Cloud-based and on-premises security solutions are often viewed as complementary approaches, rather than as an either/or proposition. A double layer of protection – or a triple layer if both desktop and server/gateway approaches are used on-premises – decreases the likelihood of a successful attack being registered against the corporate network. This principle is particularly relevant for anti-virus and anti-malware solutions, but less so for other systems, such as data loss prevention systems, where a single approach can be effective when acting alone.

  An important requirement in accurately evaluating the use of cloud-based security solutions is for decision makers to understand the actual and complete total cost of ownership for managing the current, on-premises infrastructure.

Osterman Research has found consistently that many decision makers do not fully count all of these costs and are not confident in their estimates. If decision makers do not understand accurately what it costs their organization to provide a particular service to their users, this leads to poorly informed decision-making, as well as an inability to determine the potential cost savings and the return-on-investment from competing security solutions.

SUMMARY

Despite the billions of dollars spent each year on anti-phishing, anti-malware, anti-anti-spam and other security solutions, threats still find their way into most organizations despite the best efforts of security teams to stop them. In fact, for many organizations the problem is actually getting worse over time. The consequences of these incursions can be severe, and in some extreme cases cause a business to go bankrupt.

To combat phishing, next-generation malware and other threats, organizations should implement a variety of best practices, including effective training for users to detect phishing attempts, the creation of detailed and thorough corporate policies that will address acceptable user behavior, the deployment of enterprise-grade alternatives to the less secure consumer-focused tools widely used today, and the deployment of a layered security solution that will thwart malware, phishing attempts and other threats to the greatest extent possible.

REFERENCES

[i] http://www.privacyrisksadvisors.com/news/lawyer-who-clicked-on-attachment-loses-289k- in-hacker-scam-by-debra-cassens-weiss/#.VOa79t5nLoA.linkedin

[ii] http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/

[iii] http://krebsonsecurity.com/category/smallbizvictims/

[iv] We did not define "spam", "malware" or "Web-based threats" for the respondents in the survey conducted for this white paper, but instead relied on the generally understood definitions for these terms among the IT decision makers and influencers with whom we spoke.

[v] http://www.kaspersky.com/about/news/virus/2015/Equation-Group-The-Crown-Creator-of-Cyber-Espionage

[vi] http://threatpost.com/ios-developer-site-core-facebook-apple-watering-hole-attack-022013/77546

[vii] https://www.otalliance.org/resources/advertising-integrity-fraud

[viii] https://otalliance.org/system/files/files/best-practices/documents/advertising_risk_evaluation_framework.pdf

[ix] Source: Alcatel-Lucent Motive Security Labs division

[x] http://www.darkreading.com/vulnerabilities---threats/vulnerability-to-phishing-scams-may-be-linked-to-personality-nyu-poly-study-shows/d/d-id/1140578?

[xi] http://www.enigmasoftware.com/study-shows-young-internet-users-vulnerable-phishing-attacks/

[xii] http://www.today.com/money/nasty-new-malware-locks-your-files-forever-unless-you-pay-8C11511655