Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **September 2020**
Sponsored by **Mimecast**

How Small Businesses Overcome Email and Security Challenges

Executive Summary

Like larger firms and enterprises, smaller organizations face enormous problems in managing email and web security threats. However, smaller organizations are at a decided disadvantage when attempting to manage security using on-premises solutions because they lack the same economies of scale enjoyed by their larger counterparts while experiencing most of the same threats. Consequently, smaller firms must find a new model of providing email and web security that bypasses the inherent disadvantages that they face using traditional security delivery models. This has become particularly essential given that most information workers are now working from home or in other remote locations, not from their corporate offices.

KEY TAKEAWAYS

Here are the key takeaways presented in this white paper:

- Smaller organizations are at a decided disadvantage in the context of managing security in-house: they face roughly the same security issues as their enterprise counterparts, but they are limited in how they can address these problems: they have fewer users over which to spread the cost of a security infrastructure and technical staff, resulting in higher per-user costs compared to enterprises; and they often lack the technical expertise to address sophisticated security threats.

- Email and web security threats – which are typically managed as separate entities – are growing in number and sophistication, making the detection, identification and remediation of these threats more difficult, especially for smaller organizations that often lack the budget and technical expertise necessary to deal with these threats.

- The new paradigm of "work from home" that began during the first quarter of 2020 has made an already bad problem worse: cyber criminals have dramatically ramped up their efforts to exploit the vulnerabilities associated with employees working from home using infrastructure that is not nearly as secure as what is normally deployed in a typical office environment.

- Inadequate security makes it easier for bad actors to gain access to corporate networks and data sources, resulting in the theft of login credentials, the theft or destruction of sensitive or confidential data, and exfiltration of funds from financial accounts, among other problems.

- To address these security inadequacies, smaller organizations should integrate their email and web security capabilities using the cloud as the delivery model.

Like larger firms and enterprises, smaller organizations face enormous problems in managing email and web security threats.

ABOUT THIS WHITE PAPER

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

Email Threats are Bad and Getting Worse

The threats that organizations face vary widely, from simple and fairly innocuous spam to ransomware that can take down every endpoint in an organization. Here is an overview of the threats about which decision makers need to be concerned:

- **Mass-mailed, untargeted phishing**
  The vast majority of attacks start with simple phishing attempts sent to a mass audience. While it's the successful ransomware attacks that often receive the most attention in the press, it's actually relentless phishing campaigns that are

responsible for the vast majority of ransomware deliveries, as well as compromised account credentials that provide system access to cyber criminals. Normally, ransomware attacks start with a phishing campaign – either broad-based or highly targeted (spear-phishing). Given that phishing messages are sent in enormous volumes, it's almost inevitable that at least some of these messages will find their way to users' inboxes. Phishing – rather than malware – is increasingly the attack vector of choice because it is so lucrative and successful.

- **Targeted and highly targeted phishing**
  Spearphishing is a variant of phishing in which just a single company, a group of users within a company, or an affinity group (such as developers) are targeted by bad actors with a more focused message. Business email compromise (BEC) is an even more targeted type of phishing that often will go after just a single user within a company, such as the chief financial officer. When a bad actor is able to capture login credentials for business email accounts, it provides them with the opportunity to defraud organizations of enormous sums of money. The FBI reports that more than $5 billion has been lost to BEC scams around the world[i]. As just a couple of examples, a public school in Portland almost lost $3 million to a successful business email compromise attack[ii], and a county government in North Carolina was fooled into paying $2.5 million to the wrong account of a contractor working on a building project[iii].

- **Ransomware**
  Ransomware was quite common during 2016, dropped off a bit during 2017 and 2018, but came back with a vengeance in 2019, particularly in the government space. For example, successful ransomware attacks impacted four cities in Florida in April and June 2019[iv], and more than 20 local governments in Texas in one weekend during August 2019.[v] One security vendor reported that two-thirds of 70+ ransomware attacks in the United States during the first half of 2019[vi] targeted state and local governments. Ransomware can be particularly damaging not only because it can require replacement of desktop computers, laptops and other endpoints, but because of the enormous disruption it can cause within an organization, with the potential of putting some companies permanently out of business.

- **Data breaches**
  Data breaches are particularly egregious because they are responsible not only for the theft of sensitive information like customer data or valuable intellectual property, but they can cause a company to run afoul of regulations that require sensitive data to be kept secure. For example, the European Union's General Data Protection Regulation (GDPR) enables regulators to impose very large fines on offending organizations, in some cases reaching as high as €20 million or four percent of the previous year's revenues. In the United States, the California Consumer Privacy Act also carries with it enormous fines for data breaches, and it allows individual consumers whose data was breached to receive compensation when their data was lost or stolen. It's important to note that some ransomware authors are now posting to public sites the data they have stolen if their victims do not pay the ransom they demand, combining the damaging impacts of ransomware and data breaches into an even worse threat.

- **Account takeovers**
  Bad actors often attempt to steal account credentials in an attempt to find a more credible avenue for their criminal activity. For example, if a cybercriminal can trick someone into revealing their credentials for their Office 365 account, such as through a phishing attack, those credentials can be used to send spearphishing or BEC attempts to others within the same organization. These attempts will generally be more successful because they are coming from an actual account within the company.

- **Zero-day malware threats**
  Desktop and server operating systems that are widely used suffer from a variety

The FBI reports that more than $5 billion has been lost to BEC scams around the world.

of known vulnerabilities. Moreover, unpatched systems of various kinds increase the risk of being compromised by many types of malware. For example, the NotPetya ransomware attack in 2017 succeeded in establishing a destructive foothold worldwide because of exploits of known-but-unpatched vulnerabilities in Windows-based platforms. Other malware works stealthily in the background over time to scout the infected network and spread quietly to infiltrate an ever-expanding collection of devices before turning lethal.

WHY ARE CYBER THREATS SO SUCCESSFUL?

Cyber threats are incredibly successful for a variety of reasons:

- **Cyber criminals are very capable**
  A key reason that cybercrime is successful is that criminal organizations are well-funded, often because they part of organized crime organizations. Add to this the fact that they have the technical resources needed to create new and increasingly capable attack methods, and cyber gangs tend to collaborate with one another to share new techniques and processes.

- **Cybercrime is now a hobby for some**
  However, just about anyone with evil intent can become a bad actor with little knowledge of how cybercrime works. While malware kits have been available for many years, today ransomware-as-a-service kits and "how-to-hack" guides are available on the dark web for less than $200 and will enable amateur and hobbyist cyber criminals to generate sophisticated attacks. Some of these kits are quite good and offer robust feature sets.

- **Criminals earn lots of money**
  One study found that the most successful cybercriminals can make up to $2 million each year, and even entry-level hackers can earn $42,000 annually[vii]. Cyber criminals can generate individual earnings that are up to 15 percent higher than for more traditional crimes[viii]. Add to this the fact that laundered funds from cybercriminal activity are estimated at around $200 billion per year[ix]. In short, money is a key motivator for cybercrime.

- **Employees make simple errors**
  A large percentage of users employ the same password across multiple systems, they use simple passwords that are fairly easy to guess in brute force attacks, and they use the same password for years without changing them. Many users will employ non-secure systems – especially common with so many millions of employees newly working from home – such as personal webmail accounts or non-IT-approved mobile apps. Many users are not sufficiently skeptical of phishing emails that they receive and so will click on links that can download malware or reveal login credentials. Plus, some users visit web sites that have a high probability of infecting their endpoint with malware.

- **Organizations make simple errors**
  Bad actors are often successful because many organizations are not exercising due diligence in addressing various problems like ransomware, phishing, spearphishing, BEC, and other threats. For example:

  - Many organizations don't offer good security awareness training to help their users more easily recognize phishing attempts,
  - They don't properly backup their data and so cannot recover quickly or completely from a ransomware attack,
  - They don't have the right internal controls that will enable the recipient of a BEC attempt to verify the communication via text or mobile phone,

Bad actors are often successful because many organizations are not exercising due diligence in addressing various problems.

- They don't offer adequate detection for threats like phishing or spearphishing, and
- They don't have adequate data loss prevention capabilities that would detect when sensitive or confidential information is being sent unencrypted through unapproved channels.
- Plus, many have not adequately addressed the "Shadow IT" problem that would enable them to prevent many data breaches and other problems.

- **There are more points of ingress**
  The sudden, recent work-from-home phenomenon has dramatically increased the number and types of endpoint devices and applications that are accessing corporate network and data assets, creating an opportunity for cyber criminals to more easily exploit those resources. Because many employees are now using tools they never have used before while working remote, and because many of these have not been approved by IT, the chance for successful incursion by bad actors is now significantly higher.

Because many employees are now using tools they never have used before while working remote, and because many of these have not been approved by IT, the chance for successful incursion by bad actors is now significantly higher.

The Web is a Dangerous Place

The web is a critical tool for information workers and others it can make employees more productive by enabling them to access information, storage, social media, cloud services, and various other resources. This is particularly true during the work-from-home environment in which most companies find themselves today, since employees can access data and various capabilities via the web without IT being required to set up new infrastructure.

However, the web is an increasingly risky place and it can open organizations up to a number of threats, including ransomware and other types of malware, leaks of sensitive and confidential information, and catastrophic data breaches, among other things. While these problems can occur when employees visit web properties that are well outside the bounds of corporate policy, they can also happen when employees visit valid web sites or access webmail only for work purposes and in strict accordance with corporate policies. As a result, organizations need a cost-effective way to mitigate these risks that will balance employees' needs for productivity, while at the same time ensuring that the web does not create an avenue for threats to do damage on the corporate network.

Underscoring the seriousness of the problem is the rapidly growing use of cloud services and the web. One source[x] reports that in 2019, an average of 1,295 cloud services are in use per organization, an increase of 27 percent in just three years. Moreover, cloud services now represent 85 percent of enterprise web traffic, despite the fact that more than 96 percent of these services are not fit for enterprise use.

THERE IS LOTS OF POTENTIALLY DANGEROUS CONTENT

When a user accesses even a single web page, there is typically a large amount of potentially malicious content that is downloaded to their desktop/laptop or mobile device. For example, as discovered by the HTTP Archive as of June 1, 2020, each web page request results in a median of:

- 1.8 megabytes (mobile) to 1.9 megabytes (desktop) of content.
- Seventy resource requests.
- Fourteen to 15 TCP connections.
- Four vulnerable JavaScript libraries.

This means that every visit to a web page represents the potential for malicious content to find its way into the corporate network. The problem has been exacerbated dramatically by the work-from-home phenomenon that begin in the first

quarter of 2020, since tens of millions of workers are now working from their home PCs, using often-vulnerable routers, with significantly less security infrastructure available than they had while working in an office environment.

SOME USERS ARE CARELESS

Adding to the problem of users downloading such large quantities of content from the web during the course of their work are the risky behaviors that many users perform. For example, many are not adequately trained about potentially dangerous behavior, such as downloading non-IT approved content from the web or using consumer-focused web sites like Facebook or gambling sites. Many users will click on links on various web sites or on web advertisements, such as those that prompt them to download a software update, without thinking about the risks of doing so. Many users will log into non-secure Wi-Fi networks using their work computers, such as those in coffee shops, hotels or restaurants, potentially exposing the entire corporate network to damaging threats that can infiltrate through their web browser when they access corporate resources.

WHAT COULD GO WRONG?

A variety of problems can result from web browsing, even when employees access "good" sites:

- Users will sometimes visit non-business-oriented web sites and can accidentally or intentionally download dangerous content. For example, a scientist working for NASA has been accused of downloading child abuse images onto his computer in 2018[xi], and in October 2018 the US Office of Inspector General reported that a single employee of the US Geological Survey had visited 9,000 pages of pornography web sites. The images in the latter case were routed through Russian web sites that contained malware, thereby infecting the employee's computer and Android mobile phone[xii].

- It's relatively easy for users to be directed to malicious web sites or malicious pages on otherwise valid sites, which can result in a malware infection, client-side scripting and other serious problems. One firm estimates that at any given time there are roughly 18-19 million web sites infected with some type of malware – about one percent of the total[xiii]. A drive-by attack can occur in as little as half a second after a user visits a malicious page or site.

- The poisoning of search engine results is a common technique for distributing malicious content. Cybercriminals use search engine optimization (SEO) techniques to have malicious content appear prominently in search results. One example was the use of keywords that were used in the 2018 US mid-term elections. In this case, more than 10,000 web sites (mostly WordPress sites) were hacked to promote more than 15,000 different keywords[xiv].

- Browsers will store login credentials from the web sites that users visit. For example, some malware can be disguised as trusted software, such as those pretending to be updates to Adobe Flash. However, they are not from trusted sources and can serve up malware quite easily. One such fake Adobe Flash update installed a valid update of the Flash player – and cryptocurrency mining malware[xv].

- Malvertising is a huge issue. Many advertisements that appear on web sites can deliver malicious content. One such campaign had compromised more than 10,000 WordPress sites and was generating about 40,000 attempted infections per week[xvi].

- Most web browsers use autofill to improve the user experience, but this information can be captured by malicious actors to enable them to access login credentials, credit card information and other sensitive information.

Many users will log into non-secure Wi-Fi networks using their work computers.

- Shadow IT, as noted earlier, has been a problem for IT and security functions for many years, but has become a much more serious problem because of the new work-from-home paradigm. Users employing untested and unproven applications is a common problem for organizations of all sizes, and is generally caused by employees trying to be more efficient and productive. However, when Shadow IT applications are accessing corporate network and data resources, they can introduce malware, cause data breaches, create data residency problems, and create other problems that can have serious repercussions. For example, the overall security posture of an organization can be put a risk by employees who reuse corporate passwords in their Shadow IT accounts, particularly if the app is not secure or experiences some type of data breach.

- Other problems include the fact that geolocation data can be captured and analyzed, cookies can be captured and analyzed, and browser history can be captured and used to tailor phishing and/or spearphishing attacks.

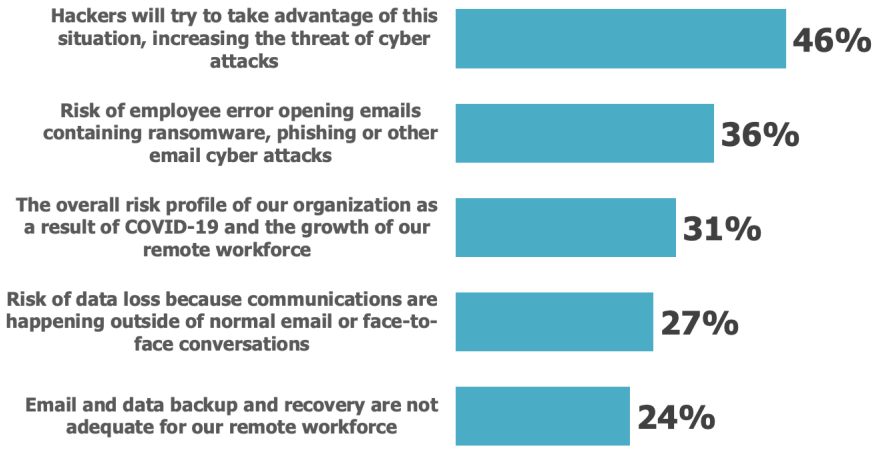
The New Normal of Remote Working Has Made the Problems Worse

An April 2020 Osterman Research survey found that before the COVID-19 crisis, 18 percent of employees in the organizations surveyed were working from home; as of April, that figure was 80 percent. What makes this a very difficult and risky proposition for many organizations is that only 19 percent of IT decision makers and influencers believe their organizations were "very well prepared" to deal with a crisis like this before it began.

There are a number of concerns that IT decision makers and influencers have about the current work-from-home phenomenon, as shown in Figure 1: 46 percent are concerned that hackers will try to take advantage of the current situation of employees suddenly working from home, thereby increasing the threat of cyber-attacks. Thirty-six percent are concerned about the risk of employees erroneously opening emails that contain ransomware, phishing or other email cyber-attacks.

Before the COVID-19 crisis, 18 percent of employees in the organ-izations surveyed were working from home; as of April, that figure was 80 percent.

Figure 1
Concerns About Various Issues
Percentage responding "concerned" or "extremely concerned"



Source: Osterman Research, Inc.

Important Considerations for Security Decision Makers

The growing problems associated with email and web security, coupled with the new work-from-home paradigm, increasingly necessitates a new approach to security, particularly for smaller organizations.

WHY MOVE SECURITY TO THE CLOUD?

Smaller organizations suffer from two critical problems in the content of cyber security:

- **Finding in-house security expertise**
  Lots of digital ink has been used in discussing the "cyber security skills shortage" – and for good reason: it's a real problem for organizations of all sizes, but particularly for smaller ones. Smaller firms generally have fewer resources available to devote to IT and security labor, and so have a more difficult time in finding experienced and capable security staffers. Consequently, smaller firms generally don't have the in-house skill sets necessary to deal with security threats, particularly more sophisticated and newer threats, and have more difficulty in justifying the hiring of these staff members.

- **Higher costs per user**
  In the context of cyber security, smaller firms have two disadvantages relative to their larger counterparts: a) they tend to pay more for security solutions because they don't enjoy the economies of scale that their larger counterparts enjoy, and b) they lack the number of users over which to distribute the cost of their security infrastructure and security-focused labor. Consequently, smaller firms generally pay much more per user than larger ones. This means that even though smaller firms more or less experience the same level of threats as larger firms, they are much less able to address them properly with on-premises security solutions. This is particularly true when organizations use multiple, disparate solutions with varying price points and degrees of efficacy – there is more to manage, costs are generally higher, and more internal resources are required to manage them.

Consequently, moving security to the cloud can get around these two problems by dramatically reducing the need for in-house personnel to deal with security issues, and by reducing the cost per seat to provide an equivalent level of service. That puts smaller firms on a par with larger firms in the context of providing robust security protection.

Another benefit of moving security to the cloud is the "community effect" that more or less is non-existent among smaller firms that operate on-premises security infrastructure. The community effect allows intelligence about an attack to be shared across the entire community of users, enabling a faster and more effective response than would be possible for individual organizations operating on their own. It's important to note that the community effect is not necessarily an inherent, automatic feature of cloud security, since not all cloud providers offer this capability.

The community effect allows intelligence about an attack to be shared across the entire community of users, enabling a faster and more effective response.

Yet another benefit of accessing security in the cloud is the ability to protect users well beyond the perimeter of a network when they're traveling or otherwise remote. This has become particularly important during 2020 as tens of millions of information workers have been forced to work from home or other locations outside of the office. As a result, having security that goes with users from wherever they might be working is essential. Cloud security can provide the anywhere, anytime protection that the current threat landscape requires.

USING A DEDICATED SECURITY PROVIDER

Microsoft offers native security through Exchange Online Protection (EOP) and Advanced Threat Protection (ATP), and many small- and mid-sized business decision

makers opt to use these tools (EOP is available in all Microsoft/Office 365 plans, and ATP is included with Plan E5 and separately). However, Osterman Research recommends the use of third-party providers that are dedicated to security because these third parties generally provide better performance and efficacy. As just one example, SE Labs published their analysis of security solutions from third parties and those that are included in Google G Suite and Microsoft Office 365. Of the eight solutions tested, the top four were dedicated, third-party solutions; the bottom four were included in Google's and Microsoft's suites[xvii].

WHY INTEGRATE EMAIL AND WEB SECURITY?

There are important advantages in integrating email and web security, including the following:

- A single console can be used to identify and manage threats, manage policies, make administrative changes and provide reports. That results in no need to have separate reporting mechanisms for email and web security. Moreover, a single interface and reporting mechanism provides greater simplicity and less time spent for administrators in creating policies, understanding security issues, and otherwise managing the security solution.

- Combined solutions can address combined attacks. For example, an attack may begin with a phishing email, but clicking on the link will direct the user to a web page that contains a malicious script. That web page could be genuine or bogus, and could result in the attacker's access to a session cookie that would enable the same access as the victimized user. By having an integrated email and web security capability, staffers are better able to deal with security issues in a holistic manner.

- Finally, other benefits associated with using a consolidated security solution include lower licensing costs, a single tech support path for any issues that may arise, a consistent user experience that can help to reduce user confusion and complexity, and overall improved efficacy as a result of sharing intelligence across the platform.

Osterman Research believes that organizations should integrate their email and web security and, particularly for smaller organizations, do so in the cloud. Doing so will enable more robust defenses against the growing array of threats

Organizations should integrate their email and web security and, particularly for smaller organizations, do so in the cloud.

Summary

Email and web security threats should be managed in a holistic, integrated way. However, smaller organizations are at a particular disadvantage in managing email and web security because they do not have the resources to properly manage security in-house, either in the current paradigm in which email and web security are managed separately, or in an integrated manner. To address these limitations, smaller organizations should seriously consider integrating their security services using the cloud as the delivery method.

About Mimecast

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

mimecast

www.mimecast.com

@mimecast

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

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

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

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

REFERENCES

[i] https://www.csoonline.com/article/3195010/bec-attacks-have-hit-thousands-top-5-billion-in-losses-globally.html

[ii] https://nakedsecurity.sophos.com/2019/08/22/quick-thinking-by-portland-public-schools-stops-29m-bec-scam/

[iii] https://www.journalnow.com/news/local/scammers-target-cabarrus-county-million-remains-missing/article_3daabb5b-3788-5a72-90c4-2c4fa0a5d078.html

[iv] https://www.naplesnews.com/story/news/crime/2019/08/20/7-florida-municipalities-have-fallen-prey-cyber-attacks-ryuk-ransomware-phishing/2065063001/

[v] https://arstechnica.com/information-technology/2019/08/ransomware-strike-takes-down-23-texas-local-government-agencies/

[vi] https://www.cbsnews.com/news/ransomware-attacks-on-the-rise-and-governments-are-in-the-crosshairs/

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

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

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

[x] Source: Netskope

[xi] https://www.click2houston.com/news/2019/07/30/hundreds-of-child-porn-images-found-on-nasa-employees-computer-court-documents-say/

[xii] https://www.oversight.gov/sites/default/files/oig-reports/ManagementAdvisory%20_USGSITSecurityVulnerabilities_101718_0.pdf

[xiii] https://www.securityweek.com/185-million-websites-infected-malware-any-time

[xiv] https://www.bleepingcomputer.com/news/security/seo-poisoning-campaign-targeting-us-midterm-election-keywords/

[xv] https://researchcenter.paloaltonetworks.com/2018/10/unit42-fake-flash-updaters-push-cryptocurrency-miners/

[xvi] https://www.bleepingcomputer.com/news/security/massive-malvertising-campaign-discovered-attempting-40-000-infections-per-week/

[xvii] SE Labs, *Email Security Services Protection, January-March 2020*