2016

Mimecast Business Email Threat Report

Email Security Uncovered

mimecast® | making email safer for business

Mimecast Business Email Threat Report

Executive Summary

While information systems may use increasingly complex security measures, these updates continue to leave one significant vulnerability unaddressed: employees themselves. Email, in particular, represents one of the largest threats that employees can unintentionally pose to their network's integrity. To explore the email security threat landscape and identify best practices for countering the threat, Mimecast surveyed 600 IT security decision makers in four countries about their email security attitudes and behaviors.

In general, most IT security managers recognize the threat that email attacks pose to their organizations, but aren't confident about their ability to prevent those attacks:

- 83% think email is one of the most common sources of attack.
- 64% believe email attacks pose a high – or extremely high – threat to their organization.
- 65% don't feel fully equipped and up-to-date to cope with the risks posed by email threats.

Two variables emerged during the research analysis to guide the report: **confidence** and **experience**. Mimecast sought to answer two questions:

1. How can IT security managers achieve the high confidence of some of their peers?
2. What can they learn from those with recent, direct experience with email hacks and breaches?

Helping IT security managers understand where they are – so they can focus on the specific insights that will help improve their security position – was one of the key goals that drove Mimecast to conduct this research. To help do just that, Mimecast employed statistical analysis to translate the survey data into five distinct personas that IT security managers can relate to.

Categorized broadly, based on **confidence** and **experience**, the five personas comprise the **Cyber-Security Shiver Grid**. They are:

- The **Apprehensive** (31%)
  - No experience with an email hack or breach; not equipped to prevent or deal with one.
- The **Nervous** (6%)
  - Has some experience with an email hack or breach, but feels unequipped to deal with one.
- The **Battle-Scarred** (28%)
  - Has direct, recent experience with an email hack or breach; doesn't feel confident in ability to prevent or cope with the next one.
- The **Vigilant** (16%)
  - Has never experienced an email hack or breach; feels equipped regardless.
- The **Equipped Veteran** (19%)
  - Has personally experienced a hack or breach; feels equipped and ready for the next one.

Based on these personas, Mimecast has created a Confidence Checklist for IT teams designed to boost – or maintain – confidence in their security measures.

The Mimecast Confidence Checklist:

- ✔ **Don't overlook new threats**
- ✔ **Engage with the C-suite**
- ✔ **Hit the security spend sweet spot**
- ✔ **Upgrade on-premises software or go to the cloud**
- ✔ **Learn from experienced pros: use advanced tactics**
- ✔ **Protect against internal threats, not just external ones**

Full Report

Introduction

IT security is a game of cat-and-mouse. Security managers and threat actors – be they cyber-criminals, state-sponsored hackers, malicious insiders, hacktivists, corporate spies, or others – constantly jockey for primary position and the ability to outmaneuver the other. While information systems may use increasingly complex security measures, these updates continue to leave one significant vulnerability unaddressed: employees themselves. Email, in particular, represents one of the largest threats that employees can unintentionally pose to their network's integrity.

New terms arise daily to describe emerging techniques in email threats: spoofing, phishing, clone-phishing, spear-phishing, whaling, link manipulation, social engineering. Email breaches run from the mundane and undetected to the provocative and public, and many cost thousands or millions of dollars to address.

To gather insight into the threat inherent to email, and collect best practices for preventing and deterring email breaches, Mimecast commissioned a survey of 600 IT security decision makers in four countries. The study, designed by Mimecast and March Communications and fielded by Vanson Bourne, surveyed 200 IT security decision makers in the U.S. and UK each, as well as 100 in Australia and South Africa each.

The State of Email Security

Overall, Mimecast found that, most managers recognize the threat that email attacks pose to their organizations. 83% think email is one of the most common sources of attack, and 64% believe email attacks pose a high – or extremely high – threat to their organization.

It is altogether troubling, then, that so many managers lack strong confidence in their ability to cope with the email security risks they face. Mimecast found that two-thirds of IT security decision makers don't feel fully equipped to cope with the risks of email security. Overall, most managers feel *somewhat* secure, but the lack of confidence is disconcerting given the level of threat.

The impact of email hacks should not be understated. Though a plurality of respondents with direct experience indicate that the cost of the most recent breach at their organization was under $100 thousand, a full 37% of respondents reported experiencing email hacks that cost over $1 million in total.

So, How Secure Is Your Infrastructure?

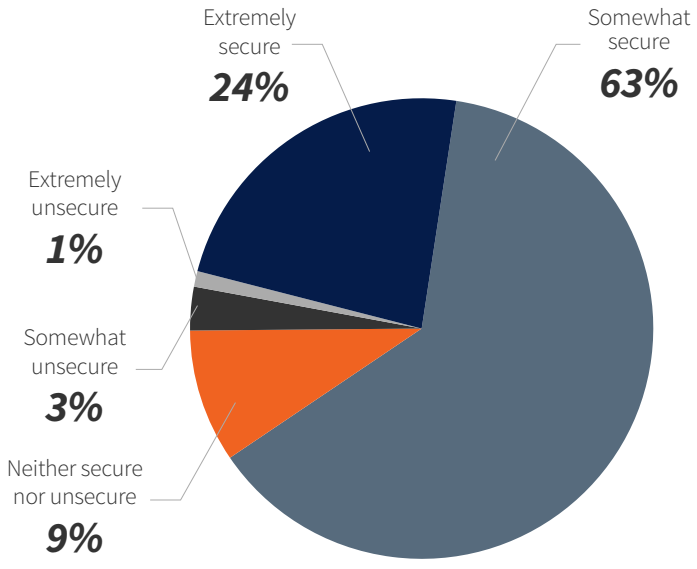


Fig. 1

Overall Cost of Most Recent Hack/Breach to Organization

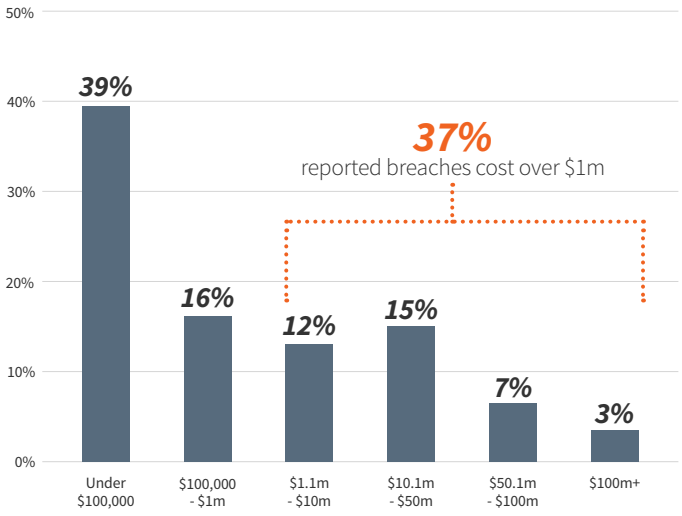


Fig. 2

Past experience can be a key tool to inform strategies to combat future threats, so special attention should be paid to IT security managers who have direct experience of an attack. Mimecast was able to gather insights from 123 experienced managers whose organizations had suffered an email hack or breach during their tenure as decision makers.

There are three major impacts hacks or breaches can have on the confidence of IT security managers. They can either:

1. **Learn a lesson.** By gaining valuable knowledge about their systems' weaknesses after an attack, managers can emerge feeling less vulnerable.

2. **Remain unchanged.** Even after an attack, some managers can emerge with a roughly unchanged perspective on their level of vulnerability.

3. **Feel more vulnerable.** Experiencing an attack, and learning first-hand the reality that the threat poses, can leave managers feeling more vulnerable to cyber-threats than before.

Unfortunately, as Mimecast found, most surveyed experienced the third reaction. Fully half of IT security managers with recent, direct experience think their organizations' email infrastructures are somewhat or much more vulnerable than they were just twelve months ago. Those experienced respondents are more than four times as likely to feel much more vulnerable than one year ago compared to those without that experience (18% with experience vs. 4% without), and nearly two times as likely to feel somewhat more vulnerable (32% with experience vs. 18% without). What's more, Mimecast found that IT security managers with email hack or breach experience are two times as likely to think that email poses the number one entry point of attack for their organization (19% with experience, 8% without).

With all of this in mind – the overall lack of confidence in email security, the high cost of email breaches, and the respect that experienced decision makers have for email breaches – what can IT security professionals do to increase their confidence and ability to prevent or combat an email attack?

Perceived Vulnerability vs. 12 Months Ago

Respondents with recent, direct experience of an email breach

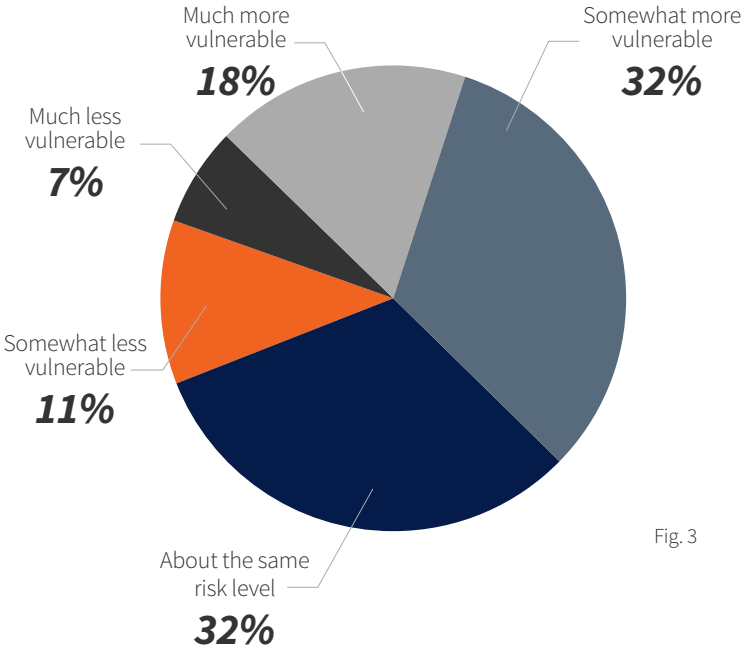


Fig. 3

The Cyber-Security Shiver Grid

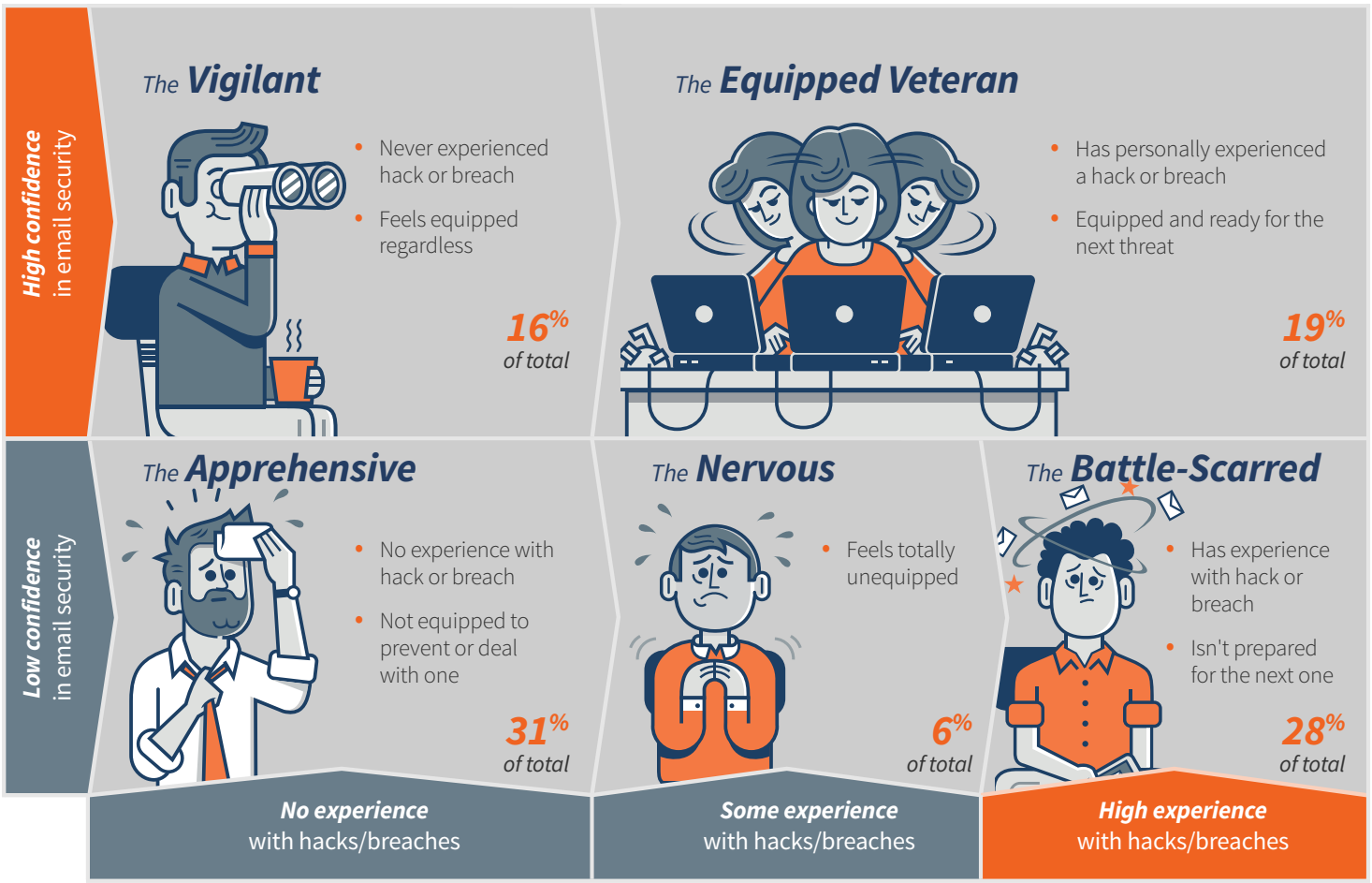
Introduction

Helping IT security managers understand where they are – so they can focus on the specific insights that will help improve their security position – was one of the key goals that drove Mimecast to conduct this research. To help do just that, Mimecast employed statistical analysis to translate the survey data into five distinct personas that IT security managers can relate to.

Each persona is defined by a set of attitudinal and behavioral data that describe where they are today. Factors like C-suite involvement, email security spend, top vulnerabilities, security tactics, and company size all impact confidence in email security. Using the data included in the personas, IT security professionals help learn where they are, where they want to go, and how to maintain their confidence once they get there.

By plotting based on two defining factors – experience with email hacks/breaches, and confidence in one's email security infrastructure – Mimecast aligned the five personas in an easy-to-understand grid.

Enter: The Cyber-Security Shiver Grid.



Regardless of where IT security managers currently fit on the grid, the desired positions are clear – the Vigilant or the Equipped Veteran, both of whom have high confidence in their systems' abilities to prevent or combat an email hack. Unfortunately, they are in the minority – 75% of IT managers are Apprehensive, Nervous or Battle-Scarred.

Where do you fit on the Shiver Grid? And what can you learn from those in your position – or those in the positions you want to be in?

Meet the Personas:

*The **Apprehensive***

31% of all ***IT security pros***

Not equipped for:

1. Malicious insiders
2. Mobile device threats
3. Spear-phishing

- No direct experience with an email hack or breach; doesn't feel equipped to prevent one in the future.
- Tends to work at midsized companies (~400 employees).
- C-suite involvement is varied; security spend is a comparatively low proportion of overall IT spend (averaging 6.9 percent).
- More likely to have multiple security technologies in place, but this doesn't translate into increased confidence.

*The **Nervous***

6% of all ***IT security pros***

Not equipped for:

1. Denial of Service attack
2. Mobile device threats
3. Spear-phishing

- Has some experience with an email hack or breach, but feels completely ill-equipped to prevent a future one.
- Tends to work at midsized companies (~450 employees).
- C-suite involvement is more likely to be low; security spend as proportion of IT spend is similarly low at (7.3 percent).

The Battle-Scarred

28% of all ***IT security pros***

Not equipped for:

1. Malicious insiders
2. Mobile device threats
3. Network-based attacks

- Has direct experience with an email hack or breach, but unable to translate that experience into confidence.
- Tends to work at a large company (~1,400 employees).
- More likely to see cyber-criminals as a major threat.
- Only 50% enjoy C-suite engagement.
- Organizations exhibit lower than average IT security spend (9.7 percent), but still more than the Apprehensive or Nervous.

The Vigilant

16% of all ***IT security pros***

Not equipped for:

1. Malicious insiders
2. PC-based malware
3. Mobile device threats

- Doesn't have direct experience with an email hack or breach, but feels equipped to prevent or deal with one.
- Tends to work at large companies (~800 employees).
- On average, C-suite engagement in their department is high; security spend as a percentage of overall IT spend is higher than average at 11.5 percent.

The Equipped Veteran

19% of all ***IT security pros***

Not equipped for:

1. Malicious insiders
2. Compromised partners
3. PC-based malware

- Had direct experience with an email hack or breach, and has come out of it with the confidence to handle future incidents.
- Tends to work at large organizations (~1,200 employees) that have high C-suite involvement and high security spend to match.
- Respects the threat; having experienced an email incident before, is more likely to see email as the number one point of vulnerability for their organization.

Implications – So What?

Mimecast has created a Confidence Checklist designed to boost or maintain confidence in their security measures. Follow these best practices to become the IT security pro you want and need to be.

1. Don't overlook new threats

Viruses and malware; these are the main threats that come to mind when discussing email security. They are also the top threats cited by respondents as areas of concern. It is notable, then, that Mimecast found that IT security managers who have direct, recent experience with an email hack are more open-minded in the threats that give them pause.

2. Engage with the C-suite

As part of the survey, Mimecast explored two related topics among IT security professionals: the amount to which their C-suite is currently involved in matters of email security, and how appropriate respondents think it is for their C-suite to be involved in email security. Based on the responses given, it is clear that C-suite executives are less involved in email security than their IT security decision makers would prefer.

Concerns Posed by different Email Threats - % Who Ranked them in their Top 3 Concerns

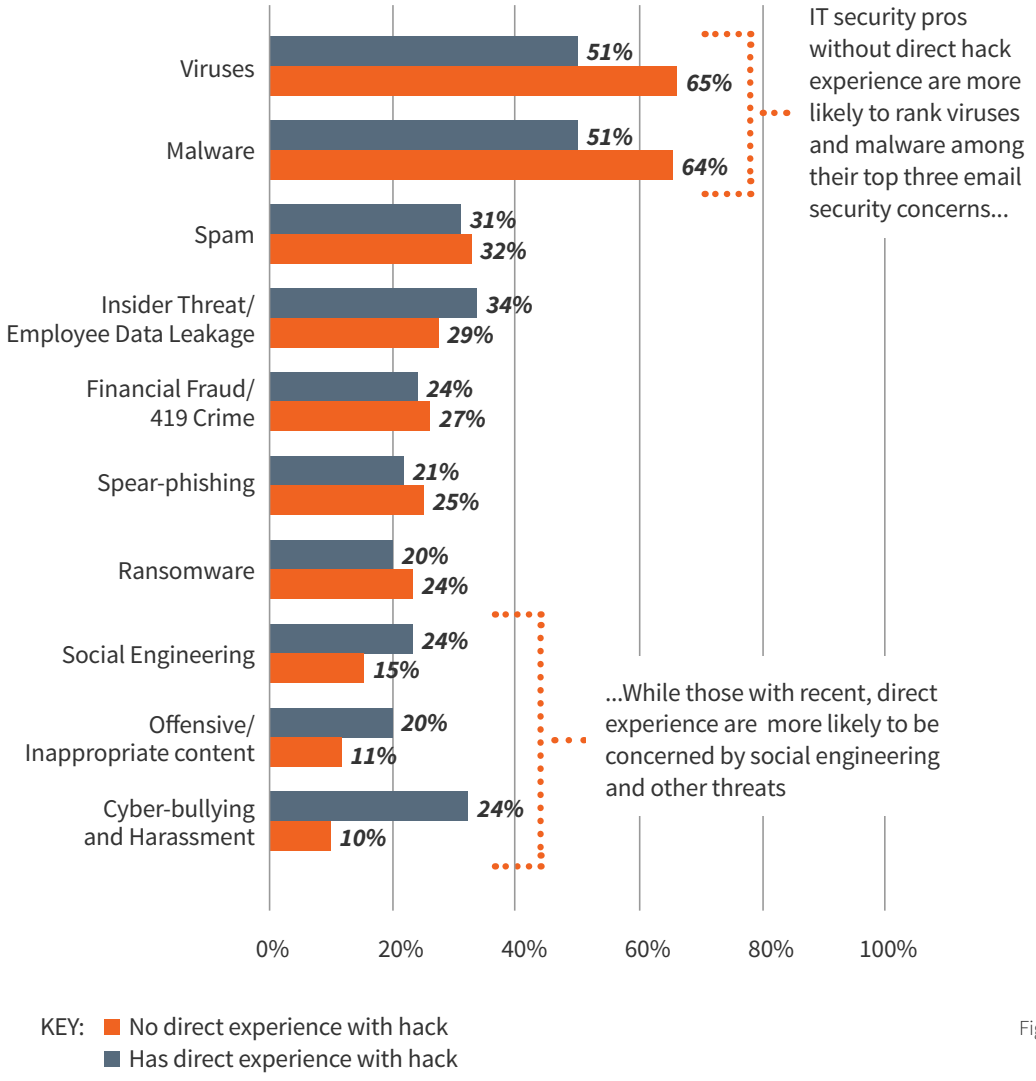


Fig. 4

Mimecast looked specifically at the responses of IT pros who are confident in their email security infrastructure and found an even clearer connection. Confident IT security managers are 2.7 times more likely to have a C-suite that is extremely or very engaged in email security; they are also 1.6 times more likely to see C-suite involvement in email security as extremely or very appropriate.

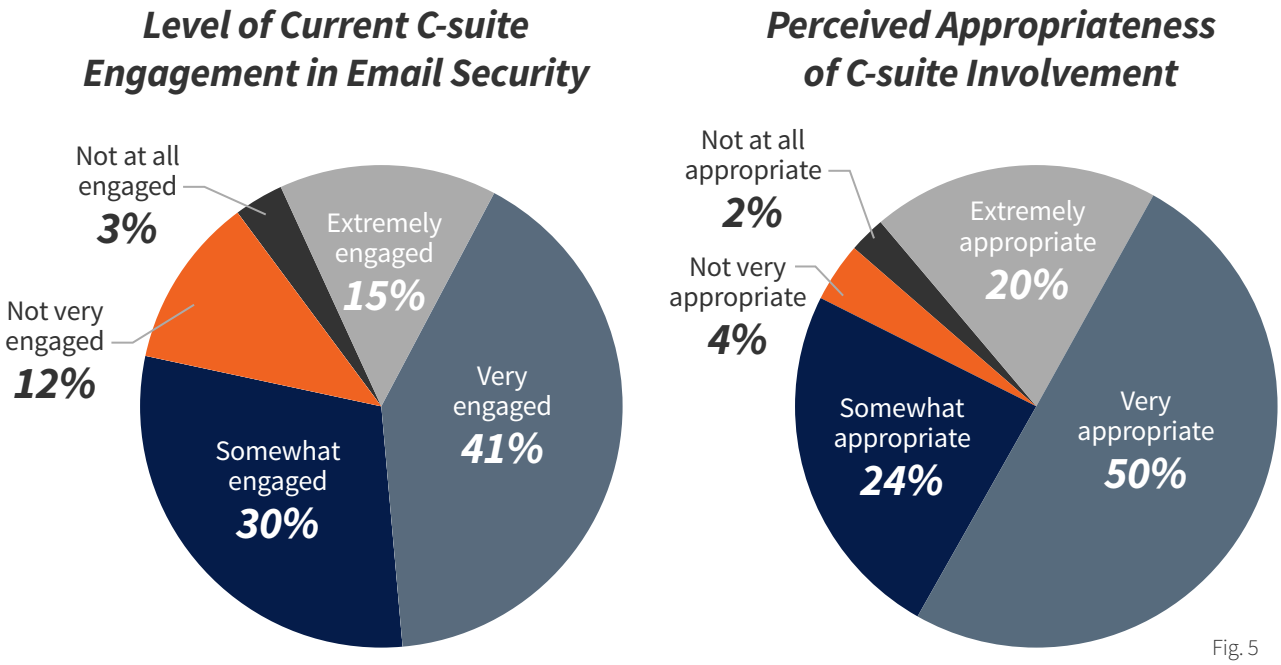


Fig. 5

3. Hit the security spend sweet spot

Bigger budgets bring increased confidence. This perceived truism is supported by our data:

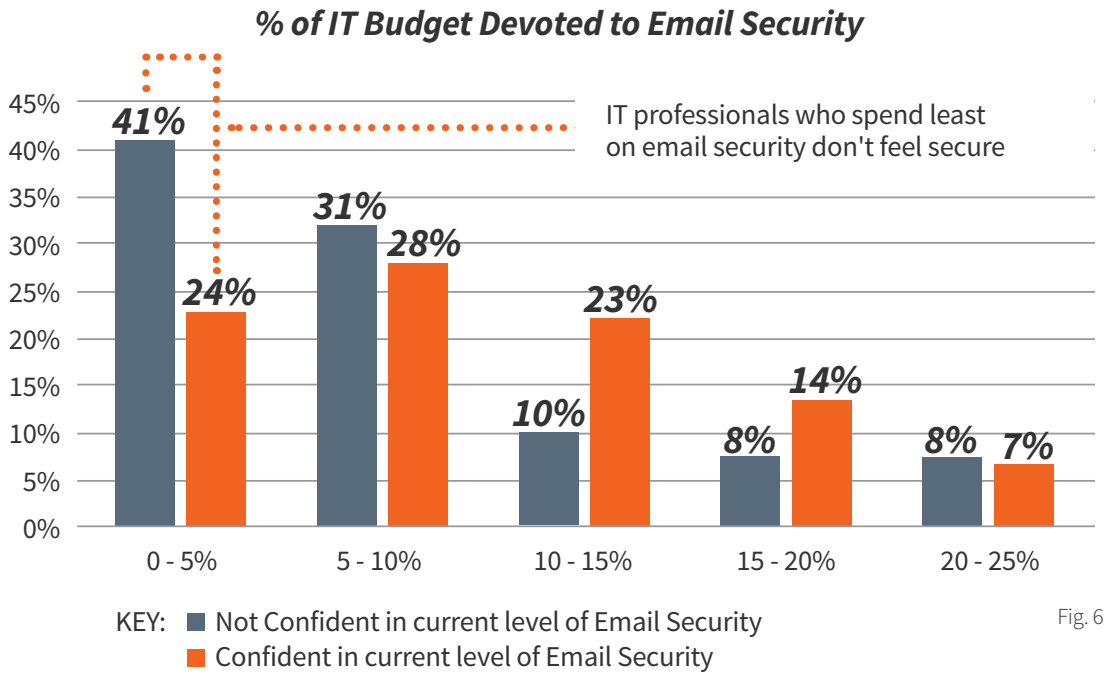


Fig. 6

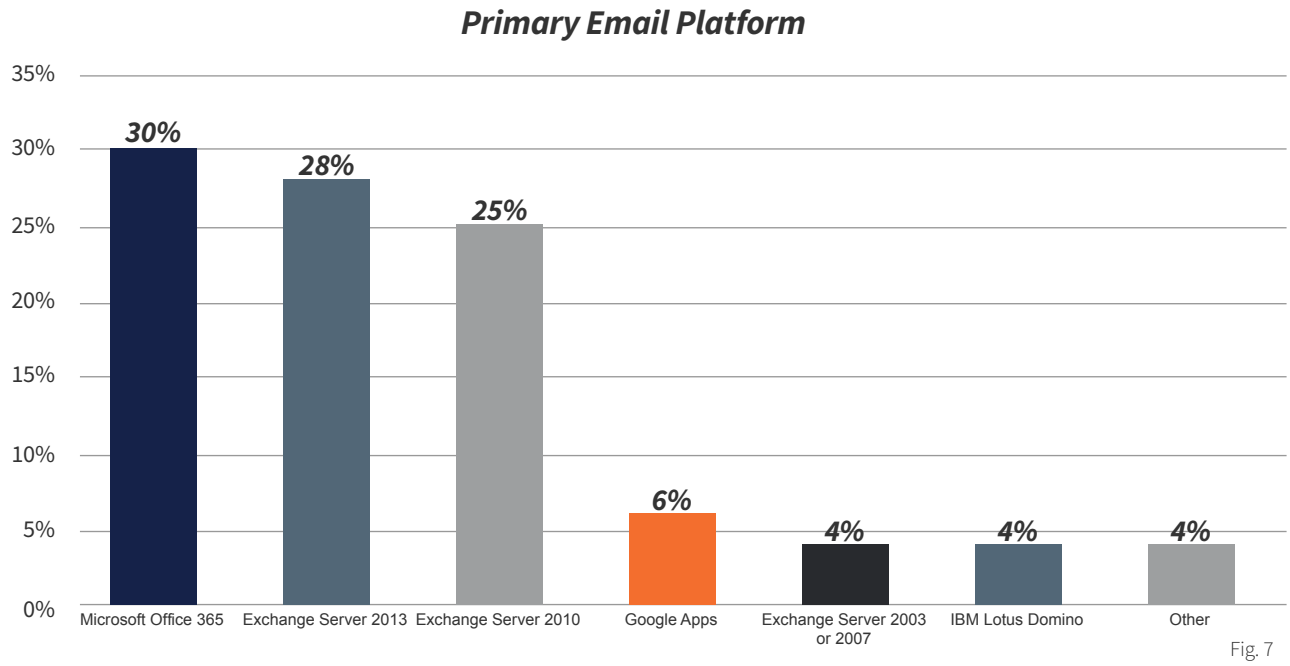


Fig. 7

Of course, email security is only one part of the overall IT security toolkit, and managers need to have flexibility in how they allot their resources. Based on the relationship between email security spend and manager confidence, Mimecast found that IT managers should strive to devote 10.4% of the overall IT budget to email security to hit the email security spend sweet spot.

4. Upgrade on-premises software or go to the cloud

One quarter of respondents are still using Exchange 2010, which ended mainstream support from Microsoft in January 2015. Exchange 2010 is also more likely to be the platform used by two unconfident personas – the Apprehensive and the Battle-Scarred. Alternately, managers with the most confidence are more likely to be using Exchange Server 2013.

While Office 365 usage isn't a predictor of where IT security managers fall in the Shiver Grid, that might not be the case in the future – Mimecast discovered that managers with recent, direct experience with an email hack or breach are more likely to have plans to migrate to Microsoft's cloud option in the next two years.

5. Learn from experienced pros: use advanced tactics

IT security managers who experience an email hack or breach may emerge *feeling* more vulnerable than before, but their tendency to employ additional safeguards may make them better prepared. Mimecast found that experienced IT security professionals are more likely to utilize a variety of additional email safeguards over and above traditional anti-virus, anti-malware, and spam filter measures. These measures are listed in order of proliferation:

- Intrusion prevention (HIPS, NIDS, IPS, IDS) within the email infrastructure (78%)
- Email encryption gateway (push encryption) (75%)
- Email attachment sandboxing (70%)
- Data leak prevention (69%)
- Anti-spear-phishing or targeted attack gateway (69%)
- URL rewriting (61%)
- Separate content control gateway (60%)
- DLP gateway (56%)

6. Protect against internal threats, not just external ones

For most IT security professionals, the first priority is securing the perimeter. This makes sense; as shown earlier in this report, the threats that IT security professionals are most concerned about are external. Perimeter security is a well-established practice, as indicated by the proliferation of anti-virus, anti-malware, and anti-spam products on the market today.

IT security professionals should take care, however, to ensure that the pendulum does not swing too far towards a focus on external threats. When asking about the vulnerabilities that organizations are least-equipped to deal with, Mimecast found that the top source of worry for IT security professionals is internal.

Mimecast also found that direct, recent experience with an email hack or breach also brings increased concern for internal threats. IT security professionals who have that experience are twice as likely to categorize malicious insiders as high threats compared to their less experienced colleagues. Malicious insiders are also the top worries for both Vigilant and Equipped Veterans, the two most confident Shiver Grid personas.

It is clear that while external threats may be most prominent, internal threats cannot be ignored. There is a reason why 69% of IT security professionals that have experience with an email hack have data leak prevention and other internal threat mitigation protocols in place; they know that email threats don't just come from the perimeter.

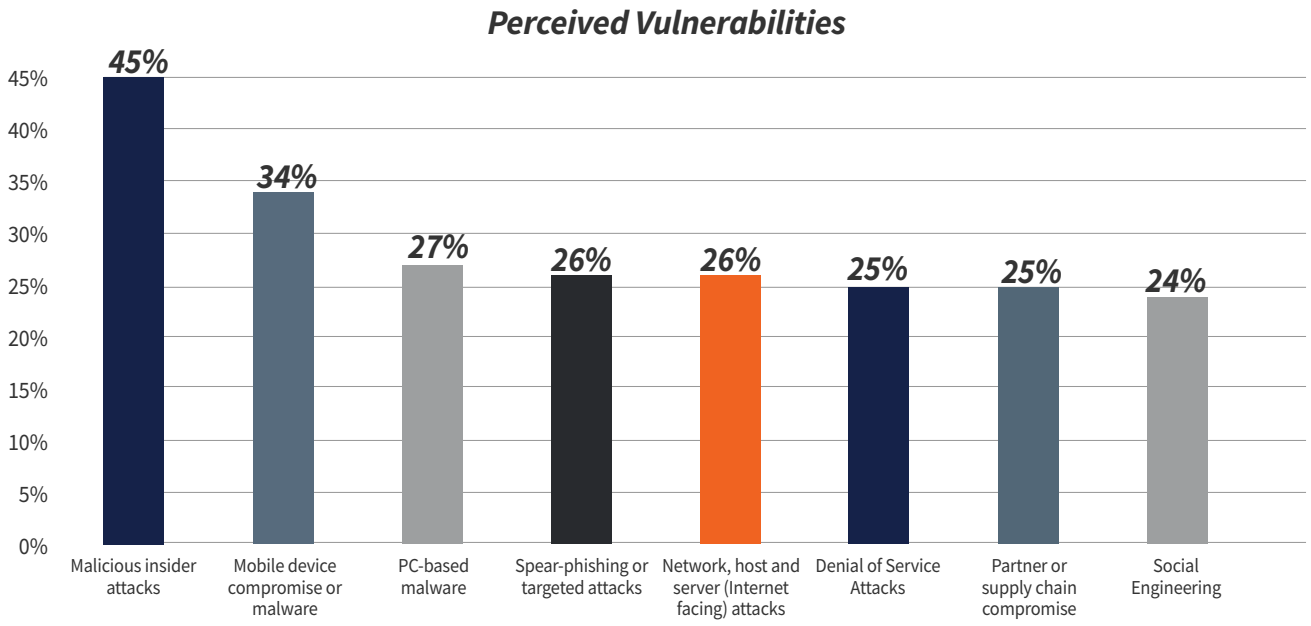


Fig. 8

Email doesn't have to be scary. And, regardless of how confident, experienced or prepared you truly are to navigate the world of cyber-crime, you don't have to do it alone. Learn more about the state of email security and ways to cope with impending threats.

LEARN MORE

Appendix: Methodology

Survey methodology

Mimecast and March Communications designed a 15-minute, online survey that went into field in October 2015. The survey, facilitated by Vanson Bourne, was completed by IT security decision makers in the following countries:

- n=200 in the United States
- n=200 in the United Kingdom
- n=100 in South Africa
- n=100 in Australia

The overall margin of error is ± 4% at the 95% confidence level.

Charted data

- **Fig. 1**: Q10. Which of the following best describes how you feel about the level of security your current email technology infrastructure offers?
- **Fig. 2:** Q23a. Please estimate the overall cost of the email hack or breach for your organization? (Base: n=123)
- **Fig. 3:** Q18. Do you feel your email security is more or less vulnerable to risk today than it was 12 months ago? (Base: n=123)
- **Fig. 4:** Q4a. How much of a concern are the following email security threats?(SHOWN: % OF RESPONDENTS WHO RANKED ITEM AMONG TOP THREE CONCERNS) (Base: No recent, direct experience n=477; With recent, direct experience n=123)
- **Fig. 5:** Q17. How engaged is your organization's C-suite with your email security and risk management practices? Q17a. How appropriate do you think it is for your organization's C-suite to be involved with your email security and risk management practices?
- **Fig. 6**: Q5. What percentage of your annual IT budget is spent on email security safeguards/technology? (BASE: CONFIDENT n=522; NOT CONFIDENT n=78)
- **Fig. 7:** D4. What is your organization's primary email platform?
- **Fig. 8**: Q13. What email security risks do you believe your organization is ill-prepared to cope with?

Mimecast (NASDAQ: MIME) makes business email and data safer for 16,200 customers and millions of employees worldwide. Founded in 2003, the Company's cloud-based security, archiving and continuity services protect email, and deliver comprehensive email risk management in a single, fully-integrated subscription service. Mimecast reduces email risk and the complexity and cost of managing the array of point solutions traditionally used to protect email and its data. For customers that have migrated to cloud services like Microsoft Office 365, Mimecast mitigates single vendor exposure by strengthening security coverage, combating downtime and improving archiving.

Mimecast Email Security protects against malware, spam, advanced phishing and other emerging attacks, while preventing data leaks. Mimecast Mailbox Continuity enables employees to continue using email during planned and unplanned outages. Mimecast Information Archiving unifies email, file and Instant Messaging data to support e-discovery and give employees fast access to their personal archive via PC, Mac and mobile apps.

Mimecast (NASDAQ:MIME) makes business email and data safer for thousands of customers and millions of employees worldwide. Founded in 2003, the Company's next-generation cloud-based security, archiving and continuity services protect email and deliver comprehensive email risk management.