mimecast®

THE STATE OF EMAIL SECURITY

The latest threats, confidence killers and bad behaviors – and a cyber resilience strategy to fix them

2018 REPORT

CONTENTS

WE'RE FAILING **AT CYBERSECURITY**

Email. You use it constantly. And it's the number-one application to keep your organization functioning, lines of communication flowing, and productivity seamless. Organizations need email to stay up-and-running all the time. After all, it's supposed to just work, right?

This is where trouble often sets in. Cybercriminals use email constantly, too. It's the number-one vector used to initiate attacks like malware delivery (think ransomware), impersonations and phishing attacks. In fact, almost 90% of organizations* have seen the volume of phishing attacks either rise or stay the same over the past 12 months. Internal threats have also been on the rise: Most organizations have encountered internal threats driven by careless employees (88%), compromised accounts (80%) or malicious insiders (70%) over the last year.

ATTACKERS TAKE THE LEAD

Cyberattackers from all over the world are targeting organizations, like yours. Major changes like moving to the cloud – specifically, organizations migrating their email in droves to platforms like Microsoft Office 365™ – all while trying to drive down cost, minimize management complexity, and defend against evolving email-borne threats are leading organizations to implement an overly-simple, defense-only security strategy. This can have negative consequences that increase with time.

Attackers are leveraging these same changes, and are working in real-time to exploit gaps in your security program.

90%

of global organizations have seen the volume of phishing attacks increase or stay the same over the past 12 months.

*Global research from Vanson Bourne, commissioned by Mimecast.

59%

of organizations will suffer a negative business impact from an email-borne attack this year.

What would happen if you couldn't access email due to an adverse incident caused by malicious intent, human error or technical failure? Your organization could suffer from reputational damage, internal operational issues and financial loss. Are you willing to take this risk?

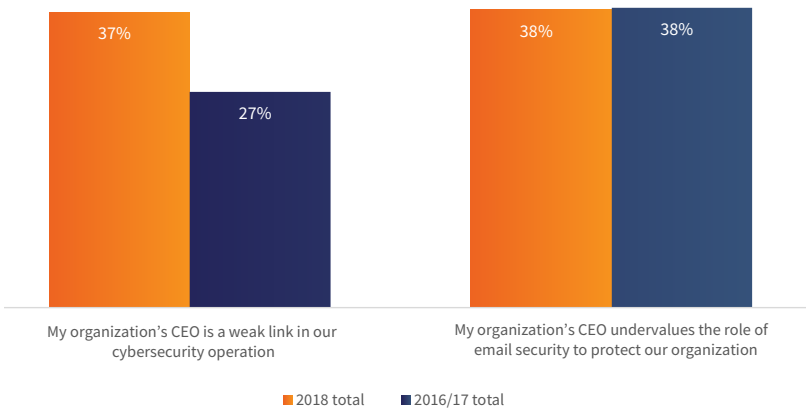
WE'RE FAILING **AT CYBERSECURITY**

AWARENESS MATTERS. AND IT STARTS AT THE TOP.

Email can be a powerful business tool. But if it isn't part of an organization's core security strategy, it can become a major vulnerability. Making cybersecurity a priority should start at the top. Unfortunately, in many cases, this isn't happening.

Nearly 40% agree that their organization's CEO is a "weak link" in their cybersecurity operation. This sentiment has increased by nearly 30% since last year. In fact, 31% of C-level employees are likely to have accidentally sent sensitive data to the wrong person in the last year compared to just 22% of general employees. And, 20% of organizations report that sensitive data was sent via email by a member of the C-suite in response to a phishing email in the past 12 months.

Could there be an awareness problem brimming at the top of many organizations? Perhaps. Nearly 40% think their CEO "undervalues the role of email security" as a key element of their security program.



Is the CEO a weak link in your cybersecurity operation?

WE'RE FAILING **AT CYBERSECURITY**

QUICK STEPS:

SIX WAYS TO CLOSE THE C-LEVEL GAP

1. Ensure there is security expertise on your leadership team.
2. Place cybersecurity into the function that manages overall risk mitigation for the organization.
3. Recognize that upper management sets the tone of the company's culture – this includes security culture.
4. Benchmark your security controls and risk management programs against peer organizations on a regular basis.
5. Constructively engage the appropriate regulators on your security program and their specific requirements.
6. Leverage internal marketing to communicate that security is not exclusively an IT problem.

WE'RE FAILING **AT CYBERSECURITY**

LACK OF TRAINING IS HURTING YOU

When was the last time you conducted security training for your employees? If the answer is "I don't remember," your organization is at risk. You're not alone. Only 11% of organizations continuously train employees on how to spot cyberattacks. 24% admit to monthly training, and 52% perform training only quarterly or once a year.

Why is security training frequency so low across the board, especially when nearly 40% feel that training their staff is the best way to protect their organization from email-based cyberattacks? Perhaps this is due to the 33% that want to address threats via increased investment in technology, or the 29% that opt to see improved business processes.

61%:

the number of organizations hit by an attack where malicious activity was spread from one infected user to other employees via email.

Malicious activity spread from employee-to-employee happens more than you think. Nearly 50% of organizations report malicious activity spread via infected email attachments, while malicious URLs via internal email was the cause for more than a quarter of these attacks.

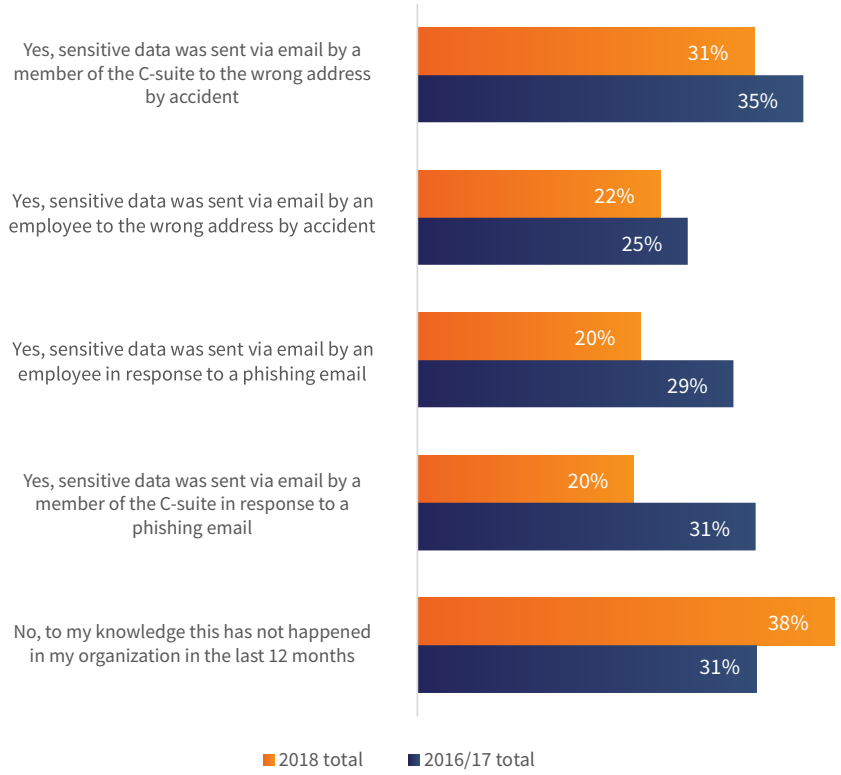
A CLOSER LOOK: **IMPERSONATION ATTACKS**

Email-based impersonation fraud has proven to be a major problem for both organizations and individual employees alike. **40% of organizations have seen the volume of impersonation fraud requesting a wire transaction increase in the past 12 months, while 39% have seen the volume of requests for confidential data increase.**

EVERYONE'S A TARGET

Armed with social engineering tactics, attackers have learned to hone-in on specific people in an organization – those with direct access to confidential and/or financial information. Nearly 40% of organizations have seen impersonations of "finance/accounts" over the last year; 28% state the C-suite as a common impersonation target; and 25% say they have encountered the impersonation of HR staff members.

While impersonation attacks normally target people from within the same company, the problem has extended to other scenarios: 31% have seen the impersonation of "trusted" third-party vendors or partners in the last year. In fact, 19% say that third-party vendors, versus their own organization, have been impersonated the most frequently over the same timeframe.



Have you emailed sensitive data to the wrong person?

A CLOSER LOOK: **IMPERSONATION ATTACKS**

CAN YOUR EMPLOYEES SPOT A FRAUD?

When it comes to preventing impersonation fraud, employee education is key. But organizations are failing at this critical step. **49% of organizations admit their management and finance teams are not knowledgeable enough to identify and stop an impersonation attempt.** And 40% are unsure if their CEO is dupe-proof. Less than one-quarter of organizations have complete confidence that their regular employees can spot an impersonation email asking for confidential data or wire transfers.

Without ongoing organization-wide security training, and investment in the right technology, impersonation attacks will become an increased reality – and the consequences will cost you.

20%

have suffered direct financial loss from an impersonation attack.

There's a lot at stake when it comes to the aftermath of an impersonation attack. 32% of organizations who have experienced email-based impersonation fraud in the past year have consequently suffered data loss. 25% experienced reputational damage and one-in-five lost customers. 61% report some loss due to supply chain impersonation fraud. What are you doing to improve employee training, careless email practices and technical controls against impersonations within your organization?

A CLOSER LOOK: **RANSOMWARE**

Ransomware attacks have fast gained popularity in recent years. Why? For one, easy-to-use ransomware crime kits are readily available on the black market – anyone can license and deploy them in the execution of a ransomware campaign. **Second, there is no single "ransomware security product" available on the market.** Perhaps the biggest reason for the rise in ransomware attacks: most organizations focus only on prevention. Traditional preventative systems, like anti-virus, can't detect and block the constantly-changing strains of ransomware. And the rise of anonymous cryptocurrencies has also played an important role.

A CLOSER LOOK: **RANSOMWARE**

RANSOMWARE IS WORSENING

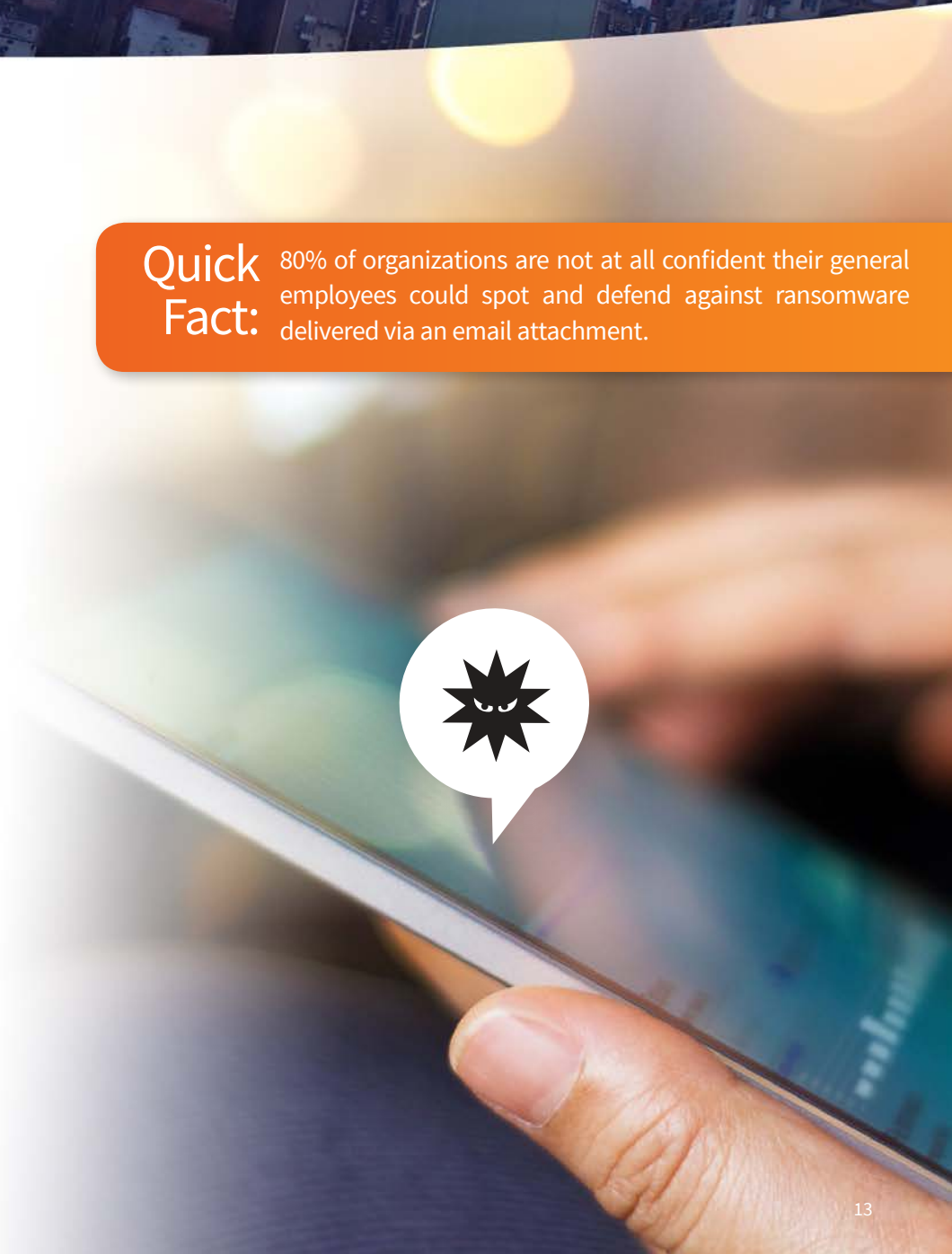
It's no secret that this dangerous strain of malware encrypts data and locks down servers and endpoints—holding the workday hostage and cutting off access to vital files, folders and productivity tools, including email. In fact, nearly 30% of organizations have seen business operations impacted by ransomware at some point over the last 12 months. Despite its known effects, why are ransomware incidents still on the rise?

92% report that their organization has seen ransomware delivered via email attachments in the past year. 49% experienced malicious activity spread from an infected user to other employees via infected email attachments. And 52% say the volume of these attacks has increased since last year.

WHAT'S YOUR DURABILITY PLAN?

The aftermath of a ransomware attack can be detrimental. Downtime can disrupt productivity, damage your brand and compromise your data. **It's no surprise that 46% of organizations think maintaining email uptime is critical for business continuity after a cyberattack.** But this is not achievable for most.

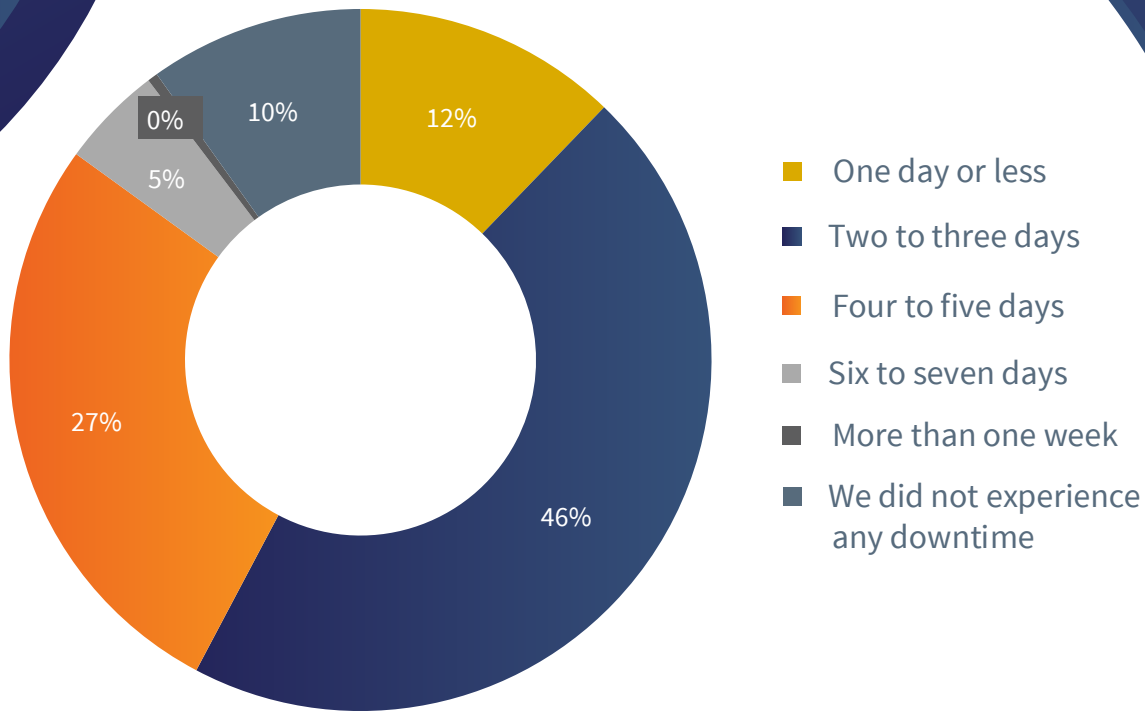
Quick Fact: 80% of organizations are not at all confident their general employees could spot and defend against ransomware delivered via an email attachment.



Three Days:

average downtime after a ransomware attack.

How much downtime can your business withstand? 78% of organizations that experienced a ransomware attack over the past year report that downtime lasted for more than one day, with three days of downtime being the average.



How long did you experience downtime as the result of a ransomware attack?

CYBER RESILIENCE FOR EMAIL

IT'S TIME FOR A NEW APPROACH

Email security in the cloud doesn't have to be complicated. Sure, there are a lot of variables: combating new and emerging email-borne threats; having a recovery plan in place when disaster strikes; ensuring constant uptime; and making sure data is protected and immediately recoverable. But trusting a single vendor, like Microsoft, or spending time and resources on security vendors offering disparate, acquired technologies is not the answer.

The only way to get ahead of attackers and holistically protect your business is to adopt a new approach to email security: one that brings together threat protection, adaptability, durability and recoverability.

It's time to embrace a cyber resilience strategy for email.

Quick Fact: 50% think implementing a cyber resilience strategy is "important," with 40% stating it's "crucial." Unfortunately, only 27% have adopted a complete cyber resilience strategy.

CYBER RESILIENCE FOR EMAIL

CYBER RESILIENCE IS EVERYONE'S RESPONSIBILITY

One of the biggest mistakes organizations make when it comes to cyber resilience planning is placing the onus on a single employee or team. **For example, 78% believe the IT department should take the lead when it comes to planning, implementing and managing the organization's cyber resilience strategy. This is a flawed approach.** Due to the critical nature of a cyber resilience strategy, this should be an organization-wide effort that includes many stakeholders with varied responsibilities and areas of focus.

80%

of organizations with a cyber resilience plan feel prepared to fight ransomware.

80% of organizations with a complete cyber resilience strategy in place are completely confident that important files or systems could be restored from backup if they were encrypted by ransomware. Conversely, only 35% of organizations in early stages of adoption have the same level of confidence.

Go Beyond **Defense-only Security**

If you're among the 44% of organizations who currently have no plans to adopt a cyber resilience strategy, your business is at risk. Threat protection should be part of your approach, but it's simply not enough. You need to consider every stage of an attack.
This means having:

1 The right security services in place **before** an attack happens.

2 A durability plan to keep email and business operations running **during** an attack or failure.

3 The ability to recover data and other corporate IP **after** an incident or attack occurs.

THE FOUR DIMENSIONS **OF CYBER RESILIENCE**

Cyberattackers are continually evolving and adapting, and the risks get worse by the day. You need a plan to keep email flowing, business operations running and the ability to recover lost or locked data quickly after an attack. You need these four core capabilities:

1 THREAT PROTECTION

The combination of internally-developed and third-party technologies paired with dozens of internal and external threat intelligence sources provides a multi-layered inspection system. This will protect against widely-used commodity attacks and customized, highly-targeted attacks.

2 ADAPTABILITY

You need to move and adapt quickly to stay ahead of the latest attacks. But technology should be only one part of a successful approach. Your employees must become more aware of the ongoing threats to help better protect your organization. This means delivering inline user education, continually assessing and deploying leading technologies, conducting ongoing threat analysis, and automating remediation services.

3 DURABILITY

Email may be forced offline by a cyberattack, or purposely by IT to contain a current threat. This can directly impact business operations by preventing or limiting the ability to communicate. Access to files held in the email system can be impacted, too. To prevent these types of outages, you need an email system that remains 100% available while ensuring the integrity of the data stored within.

4 RECOVERABILITY

You need to keep your data protected, but accessible for users. However, many organizations are unaware of the challenges involved when malicious attacks occur and point-in-time recovery is required. Leveraging an archiving service built for this can automate and simplify the process of recovering your email and other important Exchange data.

Quick Fact: Adapting can be hard. There will be 3.5 million unfilled security positions by 2022 globally.*

* Center for Cyber Safety and Education 2018

THE **BOTTOM LINE**

It's clear that you're up against an array of nasty email-based attacks – originating both externally and internally – and the climate is only getting worse. Email is at the intersection of a massive amount of risk. If addressing exposure doesn't become a priority, cyberattacks will continue – and data protection and personal privacy will all but crumble.

You know the consequences of relying on defense-only security, multiple vendors and point solutions. This approach isn't broad enough to protect against the fast-evolving threats that are putting organizations, like yours, at risk of data compromise, downtime, the inability to access or recover vital corporate information, reputational damage and financial loss.

It's time to transform your legacy security technology into a powerful, pure cloud platform that enables every dimension of cyber resilience.

THREE STEPS TO GET STARTED:

1. **ASSESS** (honestly) your organization against the four dimensions of cyber resilience.

2. **QUANTIFY** the soft- and hard-costs that your organization is experiencing due to gaps.

3. **SCOPE** three, six and 12 month plans and prioritize them to address gaps.

Ready to strengthen your defenses?

Learn More

Mimecast Limited (NASDAQ:MIME) makes business email and data safer for tens of thousands of customers with 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 in a single, fully-integrated subscription service.