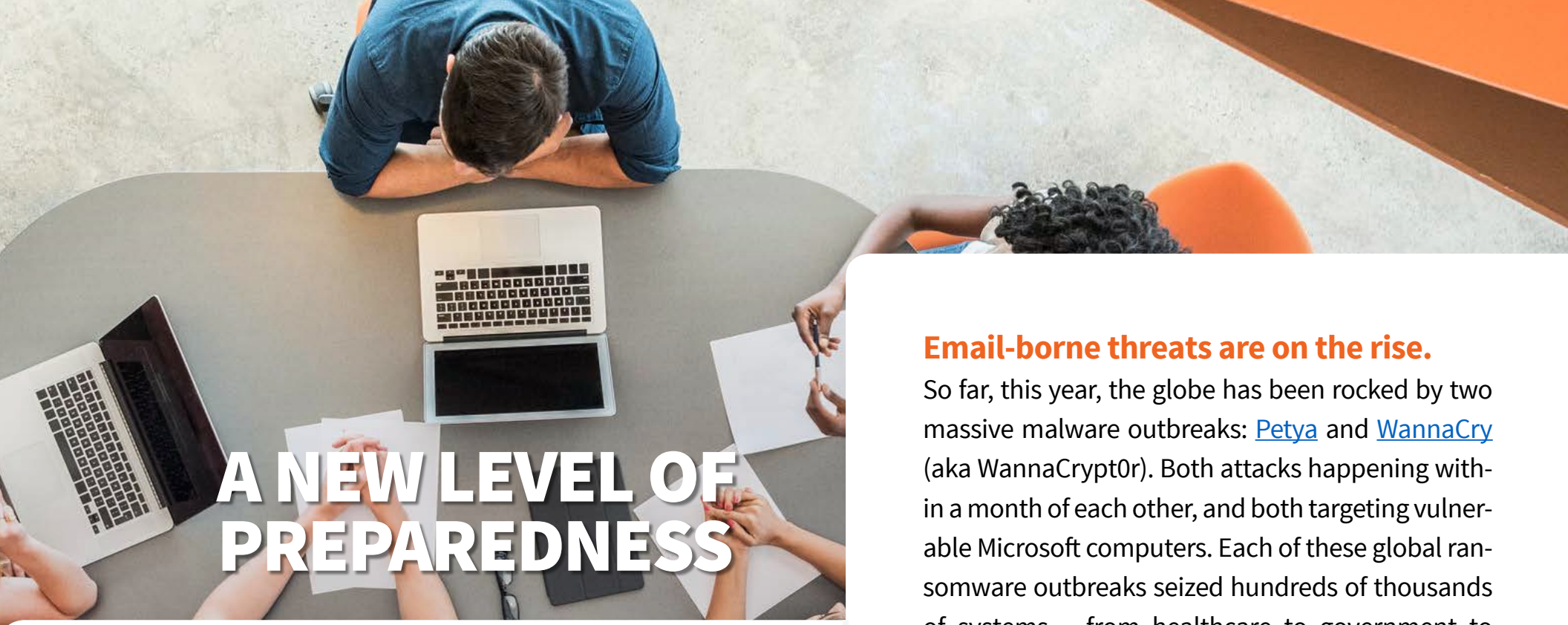
Strengthen Your Defenses Against Cybercrime

Cyber Resilience Planning for Email

CYBER RESILIENCE THINK TANK

mimecast®

CONTENTS



A NEW LEVEL OF PREPAREDNESS

Operating and securing a business in the cloud can be hard. The rapid evolution of cyber-threats, inevitability of technical failure, and potential for human error are risk factors that organizations simply can't ignore. These risk factors can cause irreparable damage like business disruption, lengthy downtime and data loss. Plus, the complexity and cost involved with addressing these issues continues to increase.

As organizations learn to navigate life in the cloud, they need a new level of preparedness.

Email-borne threats are on the rise.

So far, this year, the globe has been rocked by two massive malware outbreaks: Petya and WannaCry (aka WannaCrypt0r). Both attacks happening within a month of each other, and both targeting vulnerable Microsoft computers. Each of these global ransomware outbreaks seized hundreds of thousands of systems – from healthcare to government to transportation – across 150 countries.

More than half of organizations surveyed have SEEN THE VOLUME OF CYBERATTACKS INCREASE THIS YEAR – including ransomware, phishing and impersonation fraud.

The data presented in this e-book is from a 2017 Vanson Bourne global survey, commissioned by Mimecast.

Despite this worsening security climate, IT decision makers are struggling to keep pace. **In fact, less than 20 percent feel completely confident in their ability to spot and defend against cyberattacks.** With confidence among these decision makers low, there is a lot at stake. After all, attackers are after more than just your money. Many want to get their hands on corporate data, credentials and other valuable intellectual property; some want to take your business offline or put your system into lockdown; and others want to destroy your good reputation.

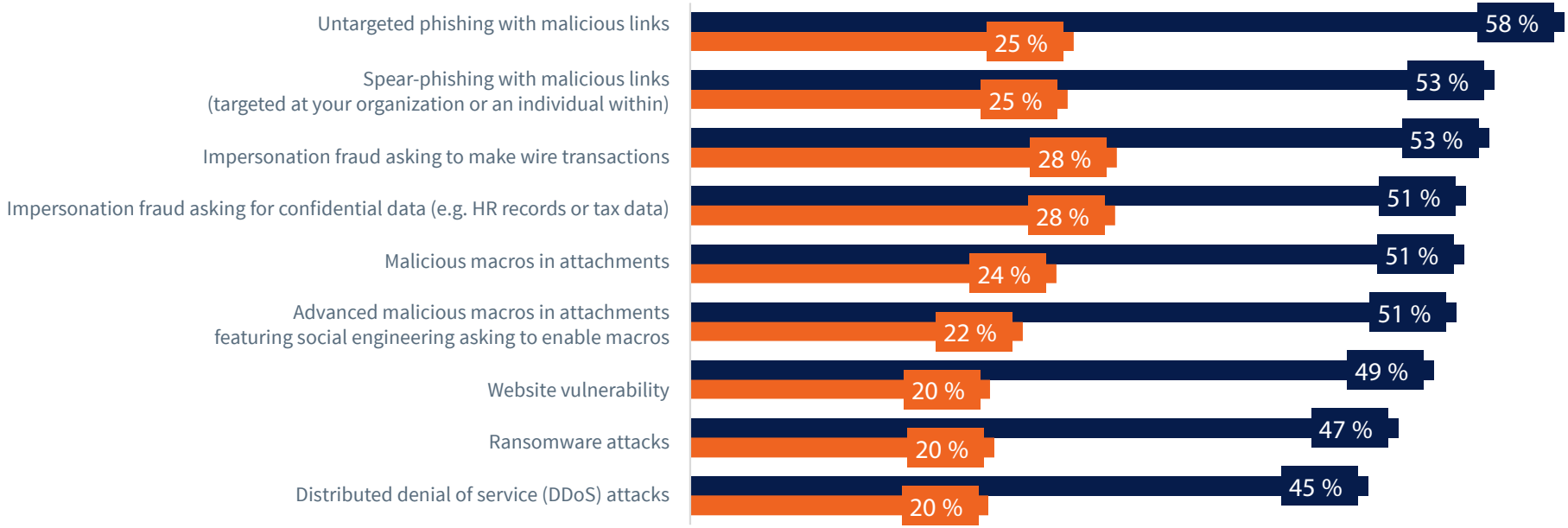
Are you willing to put all of this at risk?

Attacks like Petya and WannaCry are preventable – if you have the right strategy in place to protect your organization. You can no longer stand in front of your C-suite or Board and claim a prevention-focused security plan alone is enough. What worked for email security just six or twelve months ago is no longer sufficient, and the days of relying exclusively on basic anti-spam and anti-virus protection are gone.

It's time to start thinking holistically about protecting your business operation – it's time to implement a cyber resilience strategy to safeguard against email-borne threats and mitigate risk. ■

A CLOSER LOOK ...

THE CHANGING THREAT LANDSCAPE



Despite the fact that email-borne attacks are a real threat, many organizations aren't confident in their ability to spot or stop one.

CYBER RESILIENCE: AN INDUSTRY OUTLOOK

Mimecast hosted a first-of-its-kind CYBER RESILIENCE THINK TANK AT RSA CONFERENCE 2017 IN SAN FRANCISCO. This event brought together industry experts to discuss the issue and help define the meaning of cyber resilience.

The definition of 'cyber resilience' varies across industries. But in the world of cybersecurity, one thing is clear: The only way to protect every facet of your organization from email-borne threats is to have a holistic plan that embodies security, business continuity, data protection and end-user empowerment; and to ensure the entire organization is educated, engaged and involved in planning and response, from the Board to IT and beyond.

The concept of cyber resilience is more important than ever, and it's critical that organizations across the globe understand its meaning and business impact.

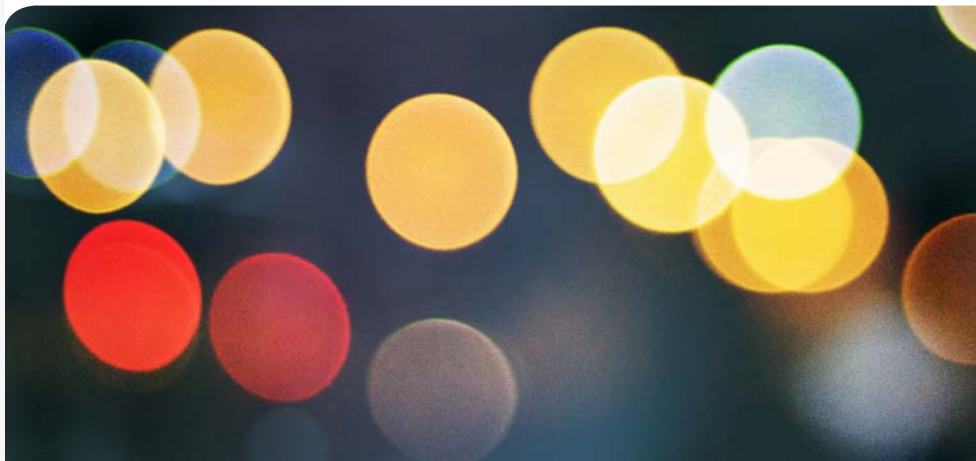
But the discussion didn't stop at the event. Cybersecurity impacts every part of a business, and cyber resilience must be at the forefront of planning. No one vendor can do this alone, so the Cyber Resilience Think Tank strives to solidify the definition, shed light on common challenges, and provide guidance on possible solutions.

Ari Schwartz, Managing Director of Cybersecurity Services at Venable, said: "The days when organizations could hide behind a shield of ignorance are numbered. We are fast reaching a tipping point where not preparing and not looking for vulnerabilities will be more damaging than having known vulnerabilities that have not been addressed."

Unfortunately, too many organizations are still playing catch up.

The Think Tank defines 'cyber resilience' as:

"An organization's capacity to adapt and respond to adverse cyber events – whether the events are external or internal, malicious or unintentional – in ways that maintain the confidentiality, integrity and availability of whatever data and service are important to the organization."

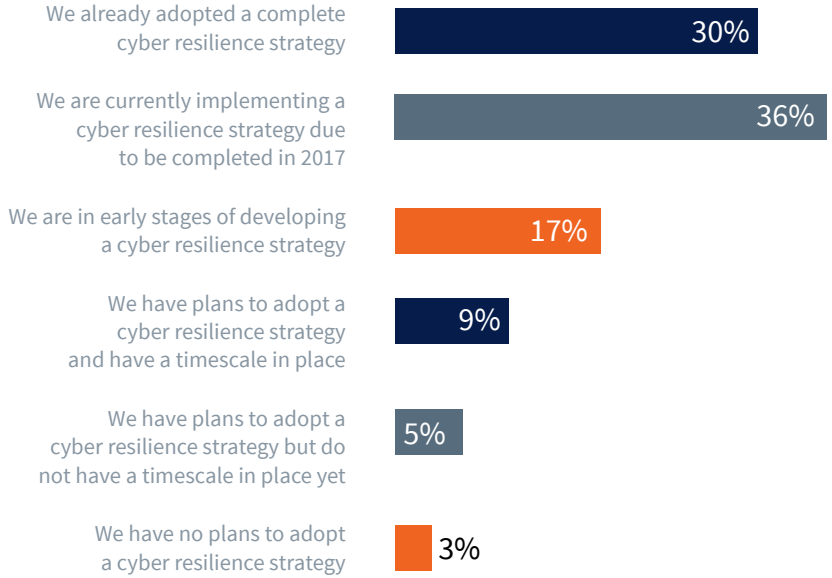


> Only **30 percent have adopted a complete cyber resilience strategy, with about one-third still in the early stages of development or planning.** This low rate of adoption – and ultimately, preparedness – has consequences: **64 percent think they will suffer a negative business impact from cybercriminal activity this year.**

Helen Rabe, Head of Information Security – Strategy, Risk and Compliance at Costa Coffee said: "Cyber resilience is not taken seriously enough, despite the published evidence identifying the growing impact of cyber risk. There is a notable gap between perception and reality when it comes to the impacts of poor cyber resilience planning."

"We are currently outmatched and don't have the capabilities to fight back. I have accepted the fact that cyberattacks will get in, despite my layered defenses. However, I work closely with my business

CYBER RESILIENCE ADOPTION TRENDS



> **Too many organizations aren't making cyber resilience planning a priority.**

on how to mitigate so they are prepared to act and aware of the implications," said Rabe.

Thinking Holistically Can Be Hard

According to Schwartz, organizations face common roadblocks when it comes to cyber resilience planning. "First, there is often an inability of IT professionals to communicate with leadership about the problems facing the organization. And there is usually concern over what they might find, such as liability risks they don't have the resources to fix, or past breaches they need to respond to immediately. Finally, there is often a lack of understanding of what needs to be done to plan for cyber resilience."

John Sapp, Director, IT Security and Controls, and Information Security Officer at Orthofix Inc. said many organizations don't consider cyber-type threats when it comes to planning for business risks.

"Organizations have a lot of difficulty putting

"The lack of thought that goes into the different types of risks causes a major gap in planning, and ultimately, a domino effect throughout the organization."

JOHN SAPP JR.
DIRECTOR, IT SECURITY & CONTROLS |
CISO, ORTHOFIX INC.

things in a business risk context. For example, they aren't thinking about cyber-type threats needing continuity planning or preparation. The lack of thought that goes into the different types of risks causes a major gap in planning, and ultimately, a domino effect throughout the organization."

According to Rabe, lack of investment in cyber resilience planning is another major problem. "We are not keeping up with the evolving nature of cyberthreats. It's overwhelming to organizations, and we aren't spending on cyber resilience," she said. "There needs to be a mindset shift; organizations need to invest on an ongoing basis. Crisis planning should be evolutionary in nature – it's not a static one-off investment or activity. This decision can make or break them."

"It's Not My Problem."

Cyber resilience planning can be overwhelming and time consuming. There is often lack of ownership, investment and understanding of what needs to happen. There are a lot of moving

"IT'S NOT MY PROBLEM."

parts, and organizations often struggle to identify a single owner.

"There is an ostrich mentality happening within organizations. Cyber resilience is often considered to be a security-only problem. As a result, the attitude of 'it's not my problem' takes over, and cyber resilience planning gets passed off," said Rabe. "It's overwhelming and IT are terrified of it. Not to mention, they are busy with daily operational tasks. All of this contributes to a lack of proactive, integrated planning."

But designating the sole burden on IT is a huge problem. Cyber resilience is a business issue, not only an IT issue. There should be one owner at the top, but a lot of players involved throughout the business; holistic engagement is the only way effective cyber resilience will work.

"IT need to engage other stakeholders in the business. Right now, they are taking on too much, and it's leading to a lack of confidence, preparedness and ownership," said Rabe. "We aren't going to stop cybercriminals. We need to accept that effective crisis management

> *"We aren't going to stop cybercriminals. We need to accept that effective crisis management should be part of a holistic plan that supports recovery time objectives and a controlled, confident response."*

Helen Rabe
HEAD OF INFORMATION SECURITY STRATEGY RISK AND COMPLICANCE, COSTA COFFEE

should be part of a holistic plan that supports recovery time objectives and a controlled, confident response."

Don't Make "Planning" a Dirty Word

One-off, scenario-based plans are simply not enough when it comes to executing an effective cyber resilience strategy. Instead, planning and education should be a regular, ongoing forum for every employee, and part of the core business process.

"Cyber resilience planning needs to be part of the muscle memory of the business," said Rabe. "Make planning ubiquitous, and do it more than once a year. Most importantly, make planning accessible to the entire business so they know what you're doing behind the scenes. After all, they will be impacted as end users."

Planning and education should be a regular, ongoing forum for every employee, and PART OF THE CORE BUSINESS PROCESS.

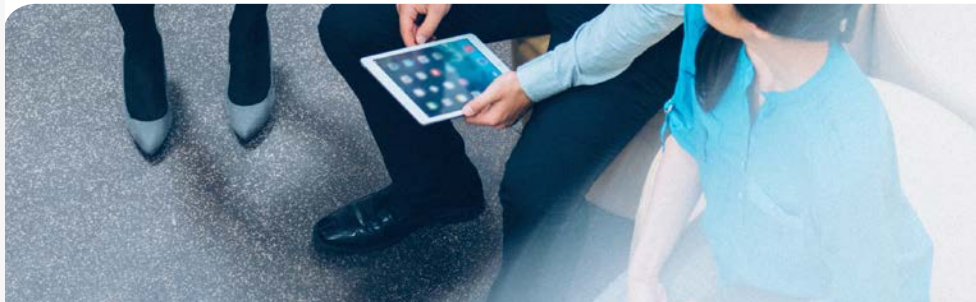
Lack of Board Buy-in is a Killer

According to Phillip Owen, CISO at IHS Markit, often, the Board do not fully recognize the risk that comes from cyberthreats, and worse, the prevalence of modern attacks. “They grasp the concept, and read the stories about victims, but this doesn’t manifest itself in a clear, well-funded plan to establish effective cyber resilience.”

Owen continued: “It’s critical that the CISO ensures cyber resilience is identified as a priority by the Board. A CISO must create the permissive financial and business environment that is needed to deliver cyber resilience. They must educate decision makers, produce the roadmap, plan a major infrastructure project, secure resources from the wider business – and above all else, deliver on expectations.”

Sapp agrees that cyber resilience planning needs to start at the Board level. “When you educate the Board on the value and ROI that comes from a cyber resilience plan, you gain trust, confidence and buy-in.” ■

> *“It’s critical that the CISO ensures cyber resilience is identified as a priority by the Board.”*
>
> **PHIL OWEN**
> GLOBAL HEAD OF INFORMATION SECURITY, IHS MARKIT



EXPERT ADVICE: AVOID A PLANNING HEADACHE

1. **DEVELOP A STRATEGIC PLAN** for cyber resilience that considers broad business objectives.
2. Don't put the onus on IT: **ENGAGE LEADERS ACROSS THE BUSINESS**.
3. Communicate planning to all staff, and **EDUCATE AND ENGAGE** them on a regular basis.
4. **DON'T OVER-ENGINEER** your plan.
5. **CLEARLY DEFINE THE RISK AND THE SCOPE OF THE PROBLEM TO THE BOARD** to secure their buy-in and funding.
6. **INVEST!** Threats can be costly to your brand, revenue and IP.
7. Hire a **CISO/LEADER WITH STRONG COMMUNICATIONS SKILLS**.
8. Share a **CLEAR AND LOGICAL CYBER RESILIENCE ROADMAP** with the business.

BUILD A CYBER RESILIENCE PLAN FOR EMAIL

Going from vulnerable to cyber resilient against email-borne threats doesn't have to be time-consuming, expensive or painful. Step one is making cyber resilience planning a priority; it should be part of your organization's foundation and business strategy. Next, have a firm understanding of your needs, strengths and weaknesses. Finally, consider every aspect of your business in your planning, and spread out the responsibility – even if it means layering in a third-party solution.

You're ready to get started. Here are the four pillars of cyber resilience planning.

PILLAR #1: SECURITY

Security is your front-line defense, and a layered approach is key. Remember: Cybercriminals use email in a lot of different ways to execute attacks – even from within your organization. This means you want an email security scanning layer that not only blocks spam and viruses, but also protects users from phishing, ransomware and impersonation fraud. And technology capabilities such as URL filtering, attachment sandboxing, instant preview and safe-file conversion of all incoming attachments are must-haves.

QUICK TIP:

It's important to always stay one step ahead of attackers. One way to do this is through centralized monitoring, analysis and intelligence sharing to help better anticipate and defend against emerging tools, tactics and techniques. Plan to integrate your email security system with third-party SIEM systems such as Splunk or LogRhythm.

PILLAR #2: DATA PROTECTION

As threats like ransomware evolve, it's more important than ever to have a separate and safe copy of your data. Once launched, email-borne threats can traverse a network quickly. If your archive is accessible to an attacker, it can be rendered useless, and your business can suffer. Your archive should be immediate – with data captured in transit – as well as tamper-proof and perpetual. And users need the ability to sync files, folders, data and calendars - and recover them if an attack occurs. The bottom line: your business needs to function; end-users need the ability to find what they need when they need it; and you need fast search and e-discovery capabilities to meet regulatory compliance and governance requirements – no matter what. The only way to guarantee all of this is to create a central repository of corporate data which is stored for 99 years in a fully encrypted, immutable and redundant system.

QUICK TIP:

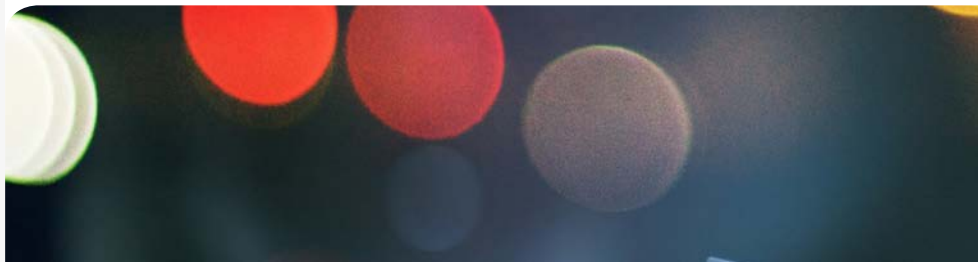
Survey your employees to understand how they would like to access their data and historical emails. In many cases, accessibility can be improved and the speed of archive retrieval can be increased.

PILLAR #3: BUSINESS CONTINUITY

Email systems, whether hosted on-premises or in the cloud, can go down. Should downtime occur – whether due to a breach, human error or technical failure – you need to be prepared to quickly and seamlessly switch to an available service. Doing so should allow your employees to continue to work and access everyday tools, like Microsoft Outlook or G-Suite by Google Cloud, without disruption. But business continuity is about more than just email communication flow. Access to data is equally important. For example, new external regulations, like the General Data Protection Regulation (GDPR), make having anytime access to your email archive critical for organizations – even during an outage. Why? You are legally required to respond to GDPR subject requests quickly.

QUICK TIP:

To bolster your business continuity planning, implement a separate, always-on solution that provides multiple access systems through the web and mobile apps.



PILLAR #4: END-USER EMPOWERMENT

Employees are your most valuable customer. Technology features can create a powerful human defense against email-borne threats – but employees need to understand how to use them, what to look for, and how to respond. Regular end-user training can help maximize your organization's agility to respond to cyber threats. This helps make for a stronger, more productive workforce while investing everyone more broadly with cyber resilience responsibility.

QUICK TIP:

Intuitive interfaces, mobility, and integration with established apps also help to delegate responsibility more effectively, removing bottlenecks and freeing individuals to focus on value-added work.

Four Tips to Up Human Defenses

1. Conduct ongoing security training and awareness activities for all employees.
2. Don't overcomplicate things: educate users, track responses, test users – repeat.
3. Talk to your employees! They are the pulse of your business. Find out what they are experiencing, and what types of training and programs they would benefit from the most.
4. Make security training a business requirement with measurable goals and results.

THE BOTTOM LINE

The way businesses operate continues to evolve, and the sophistication of cyber-threats does, too. At the same time, knowledge workers need to be free to communicate and collaborate without disruption or constant fear of threats. You can't stop disruptions from happening. Technology failure, human error and cyberattacks are simply part of business operation. But you can control how quickly and effectively your organization adapts, responds and recovers from disruption.

The solution doesn't have to be overwhelming, costly or complicated. Don't wait. Here are four quick tips to help you get started on a cyber resilience plan for email:

1. **DEPLOY** a cloud-based email security solution.
2. **ENGAGE** fellow stakeholders across your business.
3. **PREPARE** your organization through consistent review of your response process and simulation exercises.
4. **EDUCATE** employees on the value, use-case and plan for cyber resilience.

The data presented in this e-book is from a 2017 Vanson Bourne global survey, commissioned by Mimecast.

Cyber Resilience ThinkTank

INDUSTRY THOUGHT LEADERS

ARI SCHWARTZ
CEO & FOUNDER, VENABLES LLC,
MODERATOR

Helen Rabe
HEAD OF INFORMATION SECURITY,
COSTA COFFEE

JOHN SAPP JR.
DIRECTOR, IT SECURITY & CONTROLS |
CISO, ORTHOFIX INC.

PHIL OWEN
GLOBAL HEAD OF INFORMATION
SECURITY, IHS MARKIT

CHRIS WYSOPAL
CTO & CO-FOUNDER
VERACODE

MARC VARNER
CORP. VP AND GLOBAL CISO,
MCDONALD'S CORP

GARY HAYSLIP
CISO
CITY OF SAN DIEGO

MATT CROUSE
DIRECTOR, INFORMATION SECURITY AND
COMPLIANCE, LUCKY BRAND, LLC

NEIL MURRAY
CTO & CO-FOUNDER
MIMECAST

BRIAN REED
CHIEF PRODUCT OFFICER
ZEROFOX

JOEL LOWE
HEAD OF INFORMATION SECURITY
SONIC AUTOMOTIVE

Allan Carey
VICE PRESIDENT, BUSINESS
DEVELOPMENT, PHISHME

JIM HANSEN
COO
PHISHME

MALCOM HARKINS
CHIEF SECURITY & TRUST OFFICER
CYLANCE

PHIL HUGGINS
HEAD OF INFORMATION RISK &
SECURITY, PRUDENTIAL ASSURANCE

STEWART CAWTHRAY
GM, ENTERPRISE SECURITY
ROGERS COMMUNICATIONS

NIGEL HEDGES
DEPUTY HEAD OF SECURITY
REECE

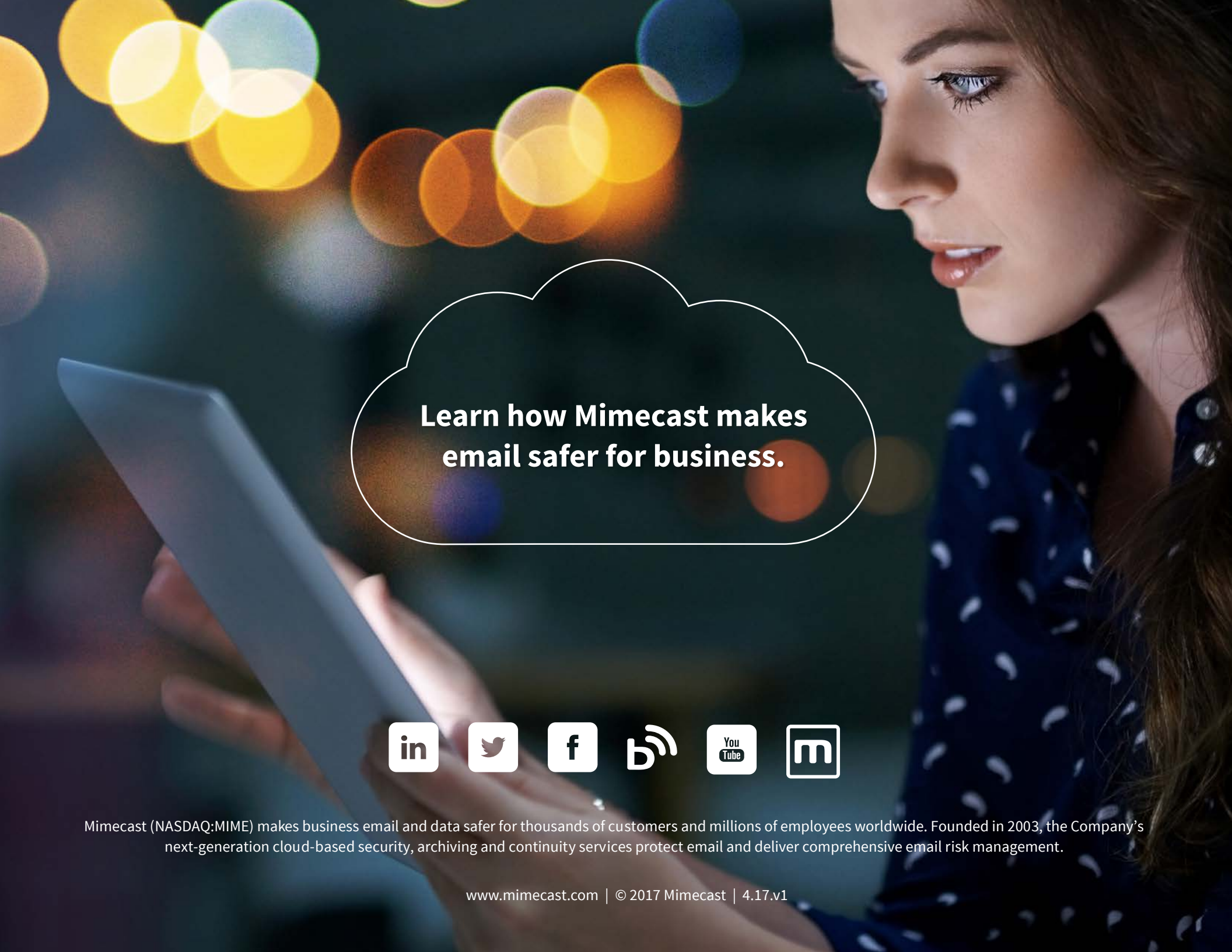
MAURICE STEBILA
COMPLIANCE AND PRIVACY OFFICE
HARMAN INTERNATIONAL INDUSTRIES, INC.

JASON GUNNOE
CISO
BRIDGESTONE TIRES

CATHY HAMMOND
CHIEF SECURITY ARCHITECT
TELEFLEX

JOE GAJDOSIK
DIRECTOR OF IT SECURITY
CURTISS-WRIGHT CORPORATION

ED JENNINGS
COO
MIMECAST



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.