mailguard

Inside Email Security 2019

Trends, challenges & cyber-readiness

Executive Summary

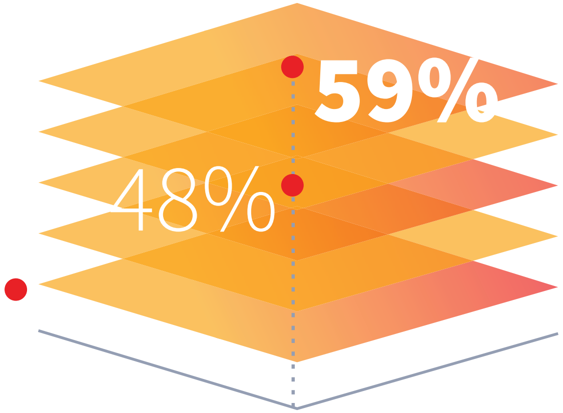
In his 2019 keynote speech, Microsoft CEO Satya Nadella warned that the cost of cybercrime is approaching US$1 trillion per year. Email-borne attacks like phishing and ransomware consistently contribute to a large percentage of this figure.

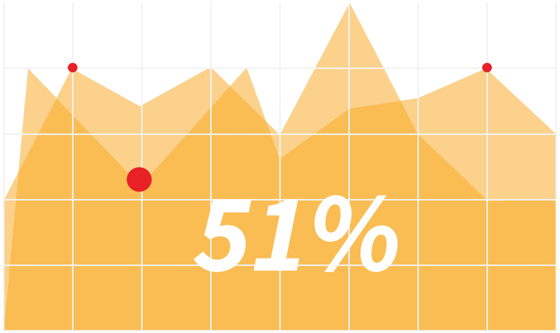
MailGuard surveyed participants from a range of over 10 industries to gain insights about their email security habits, challenges they face and the cyber-readiness of their businesses. The majority of those surveyed worked in enterprises of 50 or less people, with 80% of respondents belonging to organizations of less than 200.

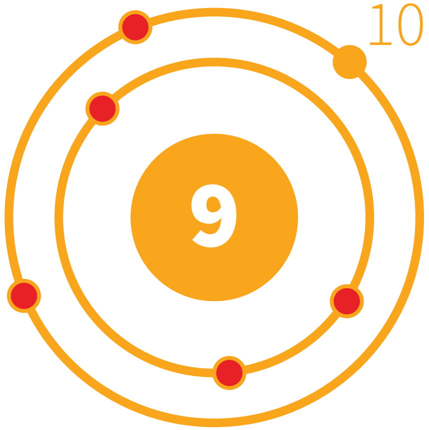
MailGuard's survey revealed

3 key findings

MailGuard's survey revealed 3 key findings:







1 **Cybercrime is significantly impacting those businesses surveyed:** 59% of respondents suffered either financial or customer loss, or a hit to their company's reputation. 48% identified financial loss as the biggest type of loss a company can suffer in the wake of a cyber-attack.

2 **There is a widespread lack of confidence in current cybersecurity methods:** Of those surveyed, 51% reported feeling concerned by or lacking confidence in their company's preparedness for handling the negative repercussions of a cyber-attack.

3 **Businesses desire capable, multi-layered protection:** Nine out of 10 businesses surveyed feel a need for multi-layered protection to defend against phishing and spear-phishing emails, citing filtering accuracy, speed of detection and the efficacy of stopping cyber-attacks.

Methodology

The survey was conducted in October 2019 with respondents spanning a sample of MailGuards customers, non-customers, partners and affiliates.

It sought to understand trends and challenges relating to email security, and the cyber-readiness of businesses, reflected in their ability to identify and detect email-borne attacks. The perceived importance of the role of education about cyber hygiene within organizations was also explored.

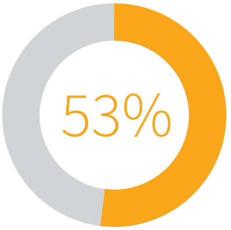
Respondents came from a variety of industry sectors including information technology, information media & telecommunications, manufacturing, banking & finance, education, health, retail and the not-for-profit sector.

Organizations of all sizes were surveyed, including small, medium, and enterprise businesses.

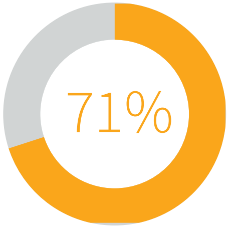
The roles and positions of the decision makers surveyed included:

- Business Owner
- Infosecurity Professional
- Technology Professional
- Finance/Accounting Professional

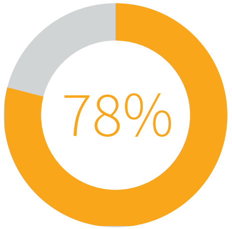
Key Statistics



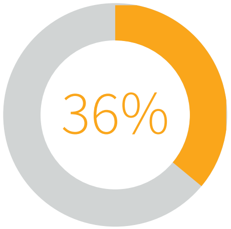
believe there is a chance their organization will suffer negative impacts from an email-borne attack in the next 12 months.



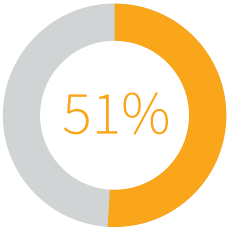
believe phishing/spear-phishing emails and ransomware are the biggest threat to their organization.



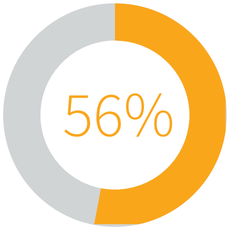
believe there is room for improvement in the training of employees when spotting an email scam.



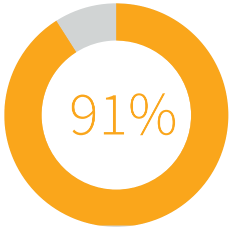
have experienced an email-borne cyber-attack in the last 12 months.



feel they're unprepared to handle the negative repercussions of a successful cyber-attack.



who experienced an email-borne cyber-attack incurred a financial loss or a reputational hit as a result of the attack.



stated they prefer an added layer of protection to protect their inboxes and not to rely on native email security alone.

Today's Cybersecurity Landscape

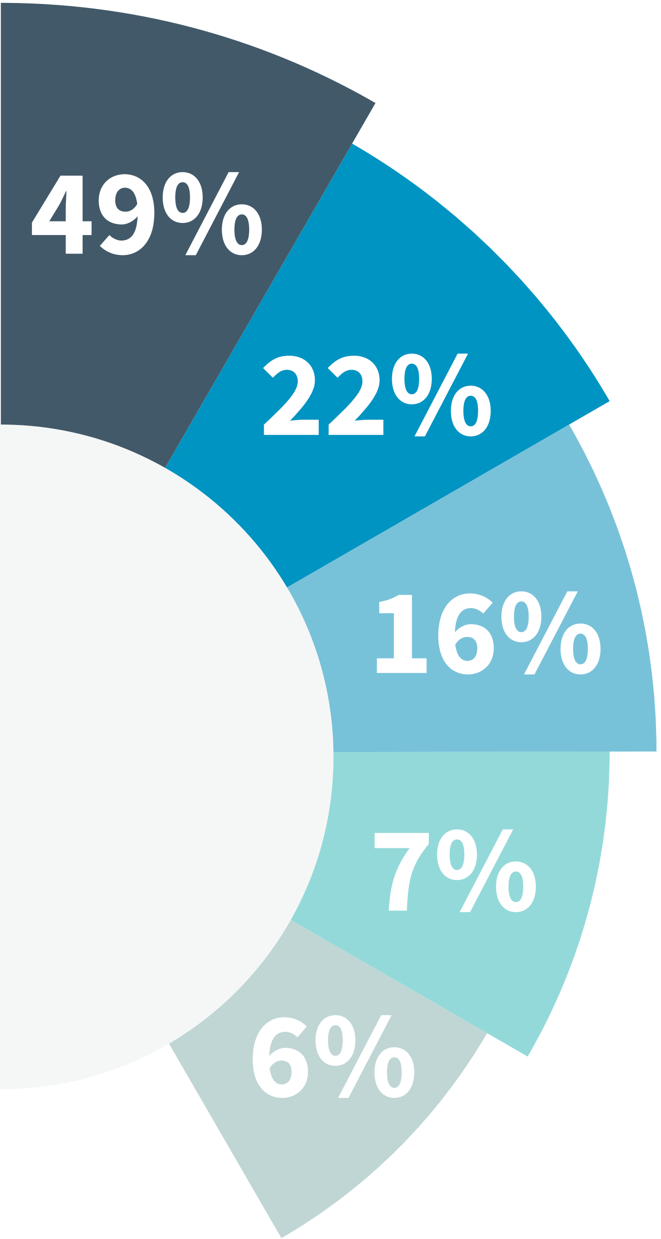
Email-borne cyber-attacks are a growing cause of concern for businesses. 49% of survey respondents identified phishing and spear-phishing scams as the biggest cybersecurity threat to their business, with 38% citing ransomware and malware. Since two-thirds of all emails circulating the world over contain unwanted content like viruses, malware, ransomware, phishing and spear-phishing scams, respondents are wise to be wary of these threats.

Although nine out of 10 enterprises report being impacted by spear-phishing scams, only 49% of those surveyed feel they're prepared to handle the negative repercussions of one.

In his 2019 keynote address in Sydney, Microsoft CEO Satya Nadella said "the impact of cybercrime is disproportionately felt by small businesses and ordinary citizens" who do not have the resources to adequately protect their organizations. Contrast this with the fact that 48% of those surveyed believe that financial loss will be the greatest impact on their business if impacted by a cyber-attack.

Monetary damage aside, a further 24% of survey respondents identified reputational damage, followed by 11% citing consumer confidence and another 10% customer loss, as the biggest types of loss a company can suffer as a result of a cyber-attack.

Today's Cybersecurity Landscape



THE BIGGEST CYBERSECURITY THREAT

to an organization

- ■ Phishing and spear-phishing emails
- ■ Ransomware
- ■ Malware
- ■ Third party and supply chain attacks
- ■ Other

Today’s Cybersecurity Landscape

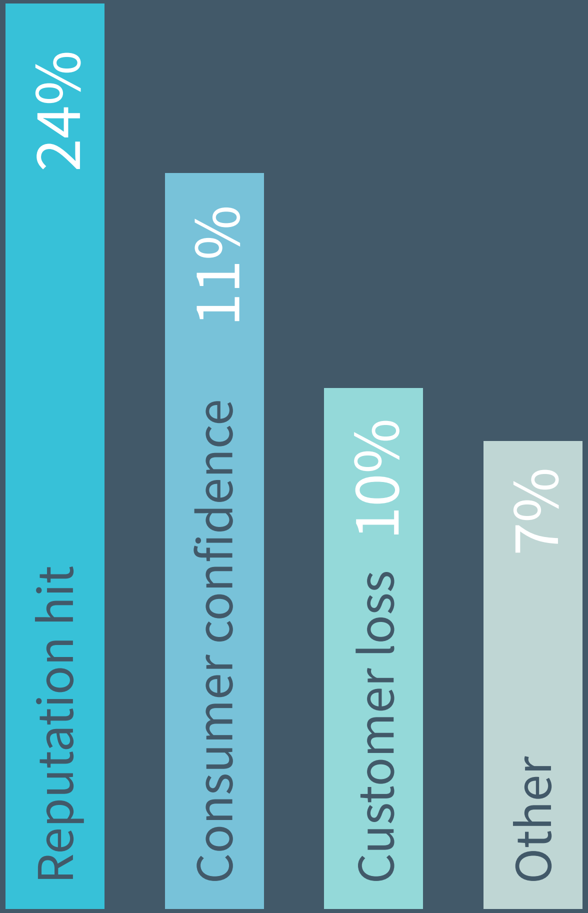
THE BIGGEST TYPE OF LOSS

a company can suffer if it falls victim to

an email scam

48%

identified **FINANCIAL LOSS** as the biggest type of loss



Attitudes & Behaviors

Towards Protection

Consider that more than half of those businesses surveyed anticipate having to deal with an email-borne cyber-attack in the future. 53% of those surveyed believe their organization will suffer the negative impact of an email-borne attack within the next 12 months. With 51% of respondents lacking confidence in their organizations' preparedness to handle the aftermath of a cyber-attack, the chief concern becomes changing the prevailing attitudes, behaviors and culture relating to cybersecurity within those businesses.

Attitudes & Behaviors

Towards Protection

78%

The survey found 78% of organizations acknowledge that their employees could benefit from more education and training about how to identify scams, and to understand the severity of them.

Changing behaviors towards protection mechanisms comes down to education about their value. With more than 293 billion emails sent & received daily, two-thirds of which contain malicious content, implementing a thorough cybersecurity plan has never been more important.

In his keynote, Satya Nadella acknowledged a shared responsibility to protect those most vulnerable to cyber threats by implementing end-to-end security, and taking a “defense in depth approach”.

Attitudes & Behaviors

Towards Protection

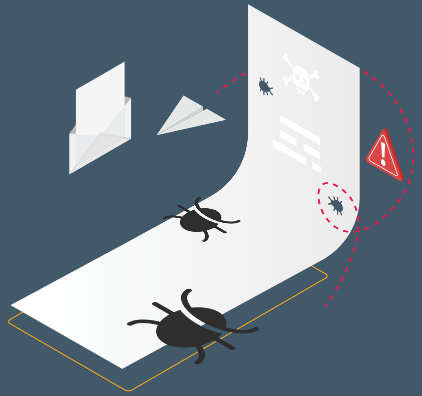
Along with better education, businesses identify the need for multi-layered security to defend their inboxes. Otherwise known as 'defense in depth', a multi-layered approach is regarded by experts as the best way to improve the resilience of an organization. Those that rely solely on the native security of their email provider are at an inherently higher risk of damage. Most enterprises surveyed are aware of the benefits of multi-layered security, with

91 percent

of respondents saying **the protection that comes with their native email platforms is NOT ENOUGH to defend their organization.**

Key Takeaways

The survey results reveal the following key insights into the state of cyber-readiness and the prevailing attitudes toward cybersecurity amongst businesses.



General awareness of the threat of cybercrime is high

Cybercrime, and particularly email threats are a clear and present danger for business. Over 50% of those surveyed expect that their business could come under attack within the next 12 months, and a further 36% of respondents say their organization has fallen victim in the last 12 months. Of chief importance is implementing a plan and preventative measures to ensure resilience, in the event of an attack, and that as little damage is incurred as possible.

Lack of confidence in business' capabilities in the wake of a cyber-attack

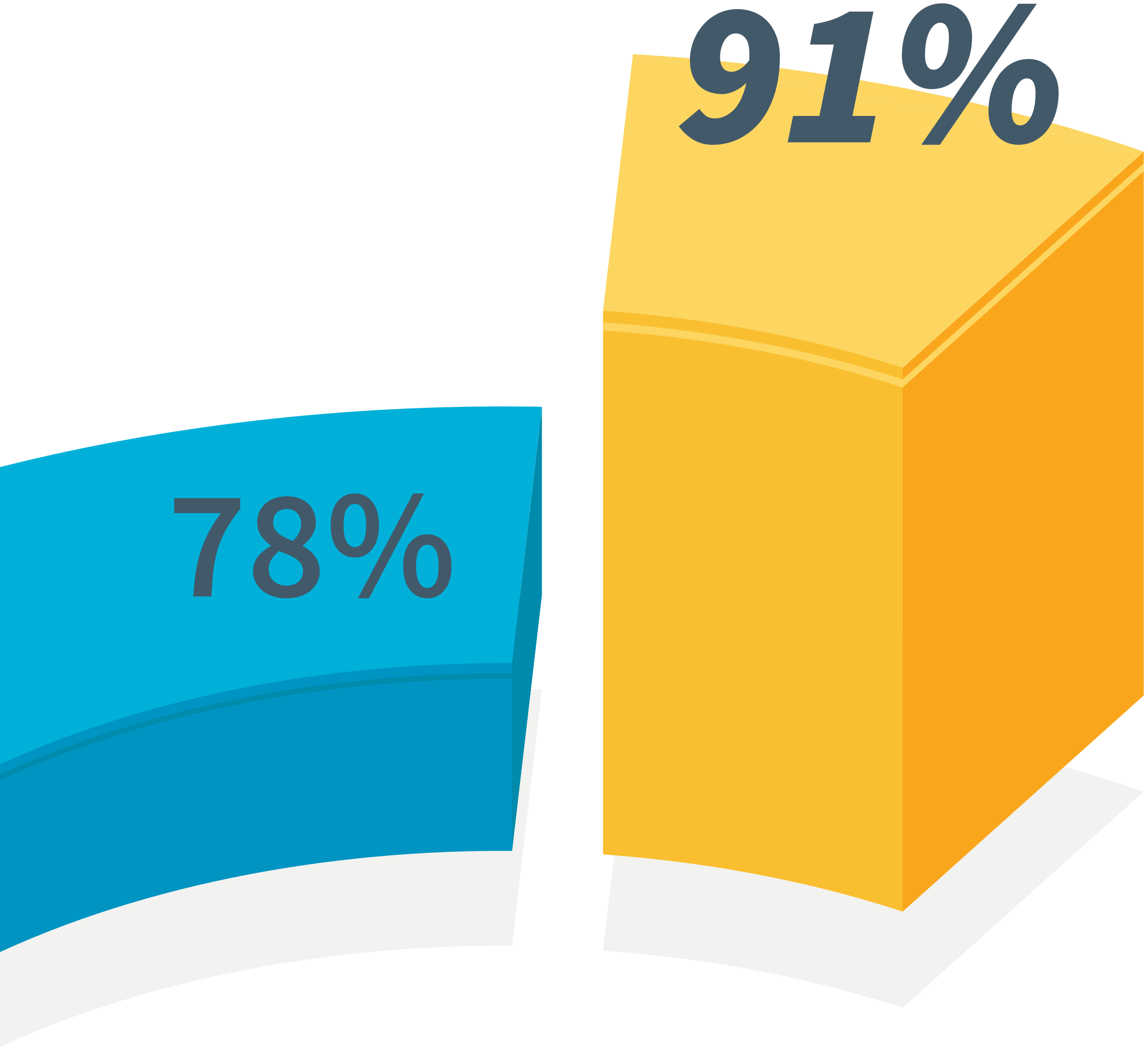
Around half of all those surveyed indicated that they are confident that their company could recover from a cyber-attack. This is in contrast to 51% of respondents who indicated they are concerned about the preparedness of their company to respond to a cyber-attack. 10% lack confidence because they have no formal cybersecurity strategy in place, and 3% have no confidence at all.

The impacts of cybercrime go beyond monetary loss

More than half of those surveyed identified a loss other than the mere financial cost of a cyber-attack. 24% cited reputational loss as the greatest loss a company can incur, while 11% cited a drop in consumer confidence, and a further 10% envisage a direct loss of customers as the greatest impact. With cyber-attacks in the news daily, and the incidence of new regulations like GDPR to protect customer data and privacy, businesses are recognizing that cyber-attacks are about more than money.

Conclusion

Conclusion



The most prominent statistic unearthed by the survey was that 91% of respondents feel safer if their business has a multi-layered security measure in place. A second key statistic was that 78% of those surveyed believe their staff could use better training about how to identify email threats endangering their organization’s security. With these two key statistics in mind, it is clear that the best next steps for businesses are the education of employees about the risks of cybercrime and email threats, and the implementation of a multi-layered approach to cybersecurity to create a more resilient organization, and a more secure workplace culture.

Are you confident about the preparedness of your business for a cyber-attack? Do you want to know more about improving your cyber resilience and your email threat protection?

Talk to a MailGuard expert by calling **1300 304 430**,
or email **expert@mailguard.com.au**

www.mailguard.com.au

mailguard

Gold
Microsoft Partner
Microsoft