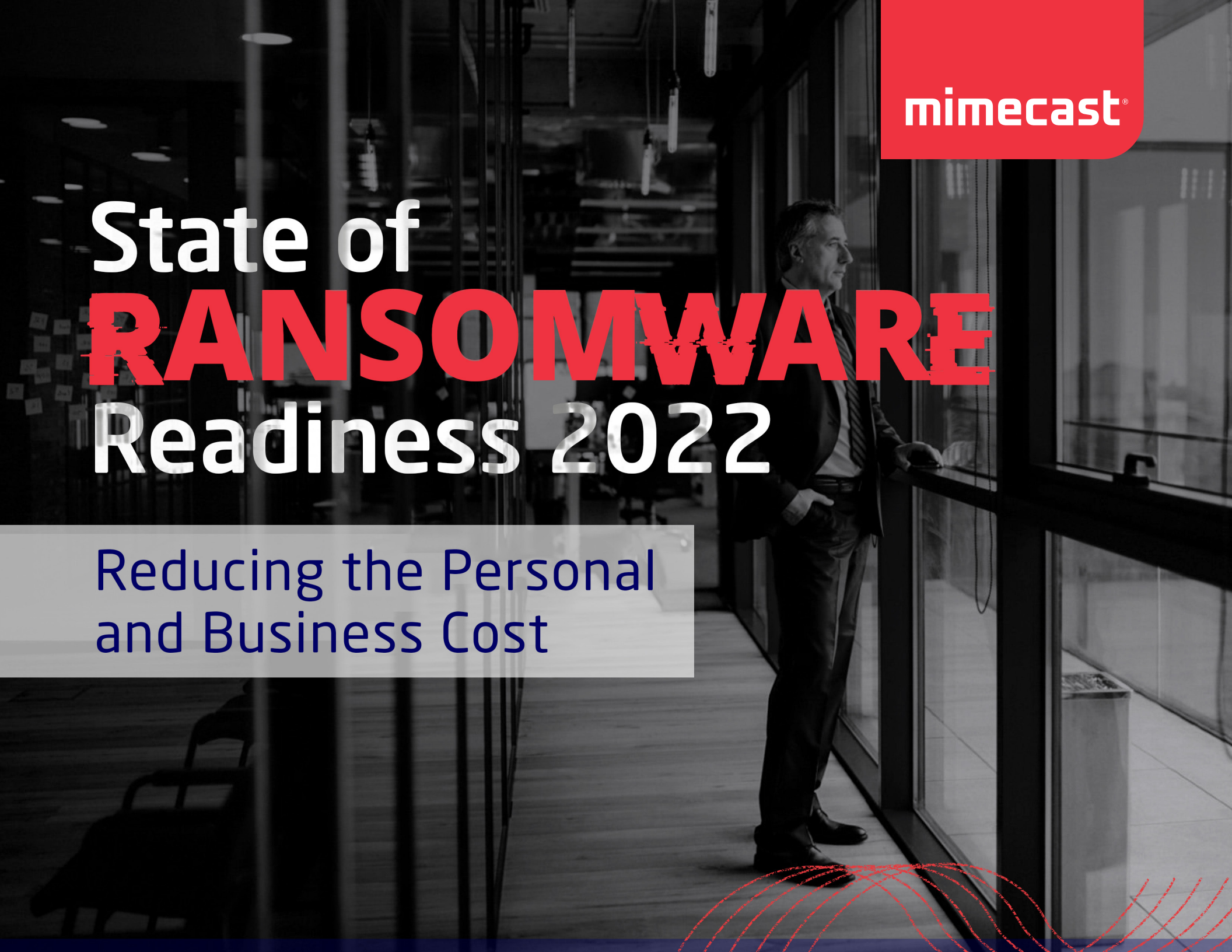
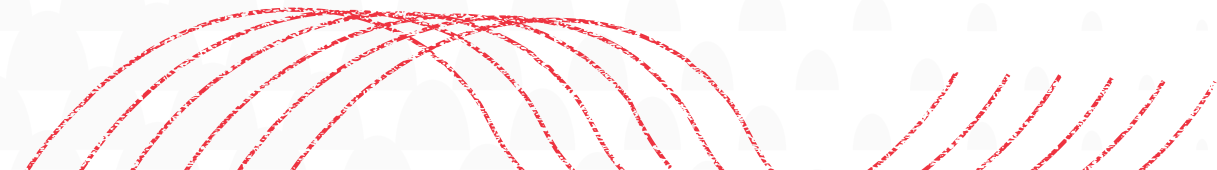


mimecast®

State of RANSOMWARE Readiness 2022

Reducing the Personal and Business Cost

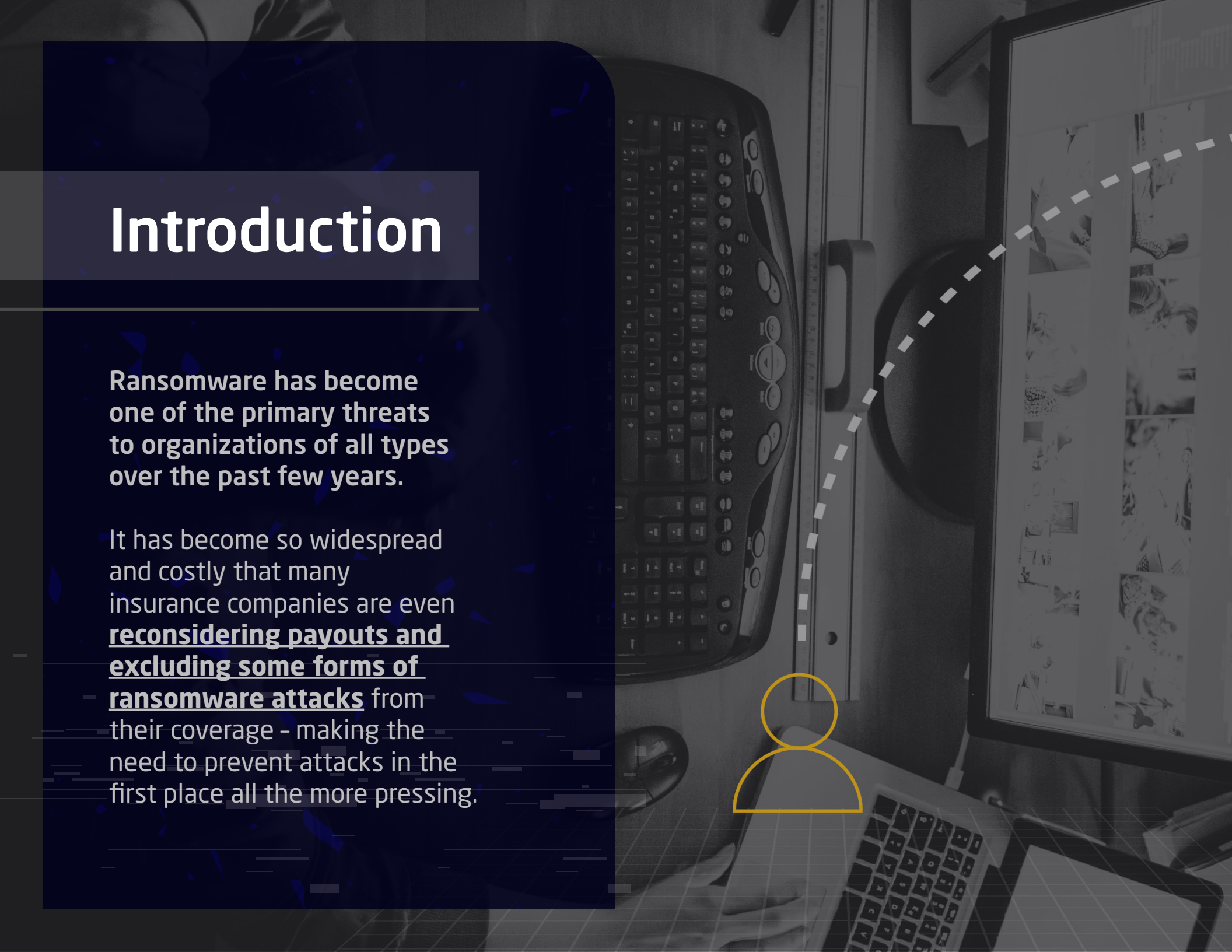
Table of Contents



Introduction

Ransomware has become one of the primary threats to organizations of all types over the past few years.

It has become so widespread and costly that many insurance companies are even **reconsidering payouts and excluding some forms of ransomware attacks** from their coverage – making the need to prevent attacks in the first place all the more pressing.



Since the notorious **WannaCry** attack brought ransomware to the headlines in 2017, numerous incidents targeting companies and infrastructure have gained international attention.

The **Colonial Pipeline attack** resulted in the shutdown of a U.S. oil pipeline in 2021, together with the loss of a $4.4 million ransom. Even more recently, criminals targeted **an N.H.S. IT supplier in the U.K.**, blocking access to patient records and compromising an urgent healthcare service.

Moreover, global chaos such as the pandemic, natural disasters, or political instability means the frequency of ransomware attacks – and cybercrime more broadly – is increasing, as well as **the total cost to victims**.

This all comes at a critical time for businesses and their IT and cybersecurity organizations.

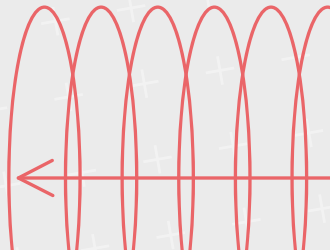
The pandemic provided novel opportunities for savvy cyberattackers who used **remote work and hybrid work**, as well as shadow IT, to find new entry points into organizations.

After a damaging few years, professionals are also facing personal challenges. Many cybersecurity teams are contending with stress and even burnout, while the industry experiences a **talent shortage** that is far from abating.

On a positive note, although the threat is growing, there are opportunities for businesses to evolve their cybersecurity strategies, and address the challenges of complex enterprise networks, limited resources, stretched teams, and complex threats. This means businesses must focus not only on mitigation, but proactive prevention, to improve their threat detection capabilities and attack responses – and ultimately, lower the personal and business cost of ransomware.

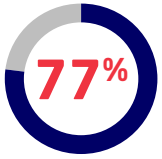
To dig deeper into the ransomware threat and to assess its impact on cybersecurity teams and businesses, we spoke with 1,100 cybersecurity decision-makers across Australia, Canada, France, Germany, the Netherlands, the Nordics, Singapore, South Africa, the U.A.E., the U.K. and the U.S.

This report explores the business implications and personal impacts of ransomware, as well as how organizations are defending against attacks today.



Key Findings

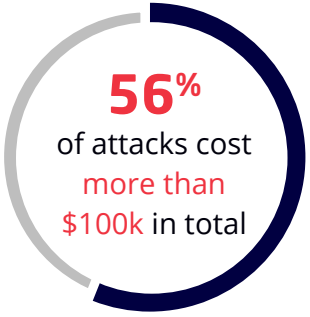
Cybersecurity professionals face mounting pressure from ransomware attacks



of cybersecurity leaders say the number of cyberattacks against their company has increased since last year or stayed the same

Two-fifths of organizations have experienced significant downtime because of ransomware attacks

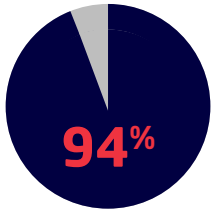
Many professionals are reaching their breaking point, as **one-third** are considering leaving their role in the next two years due to stress or burnout



of attacks cost more than $100k in total

Attacks are becoming more harmful each year, but defenses remain static

One-third of teams experience an increased number of absences due to burnout following an attack

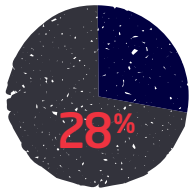


of cybersecurity leaders believe more budget is required to combat ransomware, identifying an incremental budget boost of 28% on average

of organizations have experienced a loss in revenue due to a ransomware attack in the last twelve months

Key Findings *cont.*

Leaders see ransomware attacks as virtually inevitable, driving a focus on mitigation rather than prevention



Integration is overlooked, as only 28% integrate their security controls into an SIEM or SOAR platform to orchestrate their ransomware response

File backup and recovery is the most critical technology for reducing the risk and damage of ransomware attacks

Fewer cybersecurity leaders feel personal accountability when an attack succeeds: **57%** would feel very personally responsible in the event of a ransomware attack, **falling from 71%** last year

Cybersecurity leaders must focus on proactively reducing the chances of a ransomware attack causing disruption by:

01. Integrating security tools to improve threat detection capabilities and responses, alleviating pressures on busy teams
02. Ensuring the business has good security fundamental practices in place to reduce vulnerabilities
03. Evaluating crisis planning to understand the real consequences of an attack
04. Ensuring leaders consider it a larger business prerogative and do not leave the financial and personnel resource burden to IT teams

Methodology

This survey comprises 1,100 cybersecurity decision-makers across Australia, Canada, France, Germany, the Netherlands, the Nordics, Singapore, South Africa, the U.A.E., the U.K., and the U.S. The survey was conducted online during July 2022 by Vitreous World and commissioned by Mimecast.

01.

The Ransomware Landscape: Mounting Pressure

The COVID-19 pandemic prompted a **spike in ransomware attacks** – and it's clear that the pressure on cybersecurity professionals is far from relenting. Three-quarters of cybersecurity leaders say the number of cyberattacks against their company has increased since last year or stayed the same (**77%**).

Most of these cybersecurity leaders have experienced a ransomware incident recently. In fact, **nearly two-thirds** (64%) have experienced at least one ransomware attack in the past year, rising to **75%** for businesses in the U.A.E. Many of these ransomware attacks impede the day-to-day operations of the business. **Two-fifths** (40%) of organizations have experienced significant downtime because of ransomware attacks – although this figure varies widely from 27% in the Nordics to 49% in the U.K.

There is also the potential for enduring long-term consequences. As the result of a ransomware attack, **22%** of businesses have experienced C-suite changes, while 20% have been subject to legal action against the company.

These consequences have driven a rise in journalists' interest in cybercrime; more than half of leaders (**53%**) say that growing media coverage of ransomware attacks is causing increased pressure to prepare.

In addition to the toll ransomware can take on brand reputation, the total cost of a ransomware attack, including ransom payments, systems recovery, additional security, and additional staff, can be high – and consume a substantial proportion of the **cybersecurity budget**.

When looking deeper into cybersecurity budgets and the cost of attacks across the businesses surveyed, **56% of attacks cost more than $100k in total**. Given that half of the decision-makers allocate less than $550k to their cybersecurity budget annually, a single attack could cost 20% of the total budget.

In South Africa, the proportion of businesses allocating less than $550k to their cybersecurity budget annually rises to 82%, potentially exacerbating the issue further.

This has personal consequences for the **wellbeing** of cybersecurity leaders. More than half (54%) report that ransomware attacks have a negative impact on their mental health, while 56% say their role gets more stressful every year.

With pressure mounting, many professionals are reaching their breaking point: **one-third** (33%) of cybersecurity decision-makers are thinking of leaving their role in the next two years due to stress or burnout, rising to 46% of those in the U.A.E. and 42% in the U.K.

77% of cybersecurity leaders say the number of cyberattacks against their company has increased since last year or stayed the same

Nearly two-thirds (**64%**) of these cybersecurity leaders have experienced at least one ransomware attack in the past year

The Bottom Line

The consequences of a cyberattack can be devastating, both for businesses and individual cybersecurity professionals. The level and intensity of attacks has not diminished for many years, and ransomware is a key contributor to the challenges faced by cybersecurity leaders and their teams.

Organizations are experiencing firsthand that cybercrime can take a hefty financial toll, from the operational impacts through to long-term damage to the company's reputation and legal standing.

Equally, cybersecurity teams often pay with their wellbeing, as they battle to protect the business against the growing frequency of ransomware – and counter the damage of attacks when they succeed.

With the profession facing a pressure cooker of ongoing attacks, disruption, and burnout, it's critical that organizations support security teams by giving cyberattacks the focus and resources needed – or face losing critical employees.

Allocating a level of resource to cybersecurity that aligns with the severity of the threat will help teams manage threats in a way that's sustainable, for them and for the business.

> According to **Mimecast Senior Product Manager, Kiri Addison**, "Ransomware attacks can be particularly devastating, and they aren't going away. They are associated with a variety of high impact outcomes and rising levels of uncertainty, making them particularly stressful and hard for organizations to deal with. For example, the decision to pay or not pay and not knowing if data will even be recoverable if you do. Then the move to double extortion tactics, where the threat actor threatens to sell or release exfiltrated data if demands are not met, added further pressure. Moreover, as part of the attack response and recovery, restoring services from backups and/or ransom negotiation can be lengthy processes and security teams will be pushed to limit business downtime."

02.

Attack Mitigation: Evolving Threat, Static Defenses

The ransomware threat is constantly evolving, and there are indications that attacks are becoming more harmful each year. **Two-fifths** of cybersecurity leaders (40%) have encountered ransomware attacks that use compromised credentials tactics this year, compared to 33% last year. While ransomware attacks tend to originate via endpoints, this rise in ransomware via compromised credentials is alarming and should drive cybersecurity leaders to double down on email security to prevent **credential harvesting**.

Over one-third of organizations (36%) have experienced a loss in revenue due to a ransomware attack in the last twelve months, compared to 28% last year. This rises to 44% of businesses in Germany and the U.A.E.

Cybersecurity leaders are also becoming less confident in their ability to mitigate the damage when an incident takes place. Although last year 82% of professionals were confident they could maintain **email continuity** with no disruption following a ransomware attack, this year that has fallen to 73%. And this waning confidence should be of concern to all enterprises.

Organizations are increasingly turning to **cybersecurity insurance** to cover losses when attacks succeed, but again professionals are becoming less trusting of this safety net. While last year four in five (79%) believed their cyber insurance provider would cover any ransom payment demanded by attackers, this year only 64% think so – falling to 50% in Canada. Given that **insurers are limiting the coverage provided** against certain types of attacks, leaders are right that relying on cyber insurance may be a risky strategy.

Additionally, there are signs that often cybersecurity teams lack the basics when it comes to attack prevention. When leaders consider the additional resources needed to prevent and prepare for attacks, **nearly half say they need up-to-date security systems** (46%).

Likewise, 46% pinpoint higher-quality **security awareness training** for end-users as a necessary extra resource – in Singapore, this figure rises to 61%.

Almost every cybersecurity leader (**94%**) believes more budget is required to address this threat, from both the preventive and the impact mitigation perspective.

Decision-makers would need, on average, an incremental budget boost of **28%** to combat ransomware alone.

Mentally prepared teams are also critical for preventing and mitigating cybercrime – but once an attack takes place, employees often struggle with their wellbeing. One-third of teams (33%) experience an increased number of absences due to burnout following an attack.

In addition, **34%** of cybersecurity leaders have trouble recruiting essential IT staff once an attack has taken place, further eroding their ability to combat incidents in the future.

The Bottom Line

Ransomware is constantly evolving, and cybersecurity leaders are seeing firsthand the damage that attacks can do. And with the safety net of cyber insurance becoming less dependable in the event of an attack, ensuring an attack is never successful is becoming the only safe path left.

But concerningly, businesses' ransomware defenses appear to have remained static, with many firms lacking the basics like up-to-date security and employee awareness, potentially increasing vulnerability and exposure in the event of an attack.

Businesses can become more vulnerable to attacks after one has taken place, not least due to the stress, burnout, and recruitment issues experienced by teams in the wake of an incident.

To avoid this cycle, it's critical to have fundamental measures in place, like robust email security and employee training, supported by a large enough budget.

Integration between security systems is another powerful way of increasing visibility and alleviating some of the pressures busy teams experience.

> "Organizations that have cyber insurance are still highly vulnerable. It's not a stand-alone solution. The loss of intellectual property and future profits are not typically covered. Significant losses to brand and reputation are also not covered. Even worse, coverage can be capped if the attack involves ransomware or not applicable at all if it's a state-sponsored attack. Organizations need to maintain their modernized email security even if they have cyber insurance."
>
> - **Andrew Williams,**
> **Principal Product Marketing Manager**

03.

Business Preparedness: Inevitability Limits Proactivity

Despite the lack of resources and mental strain they identify, generally, cybersecurity leaders feel prepared and backed by the business. Three-quarters of cybersecurity decision-makers (**77%**) feel supported by their senior leadership team or board.

After a cyberattack, on average, leaders believe it would take 3.5 days to return to normal operations – with 46% believing it would take two days at most. Overall, seven in ten (**70%**) say their company is very well prepared to prevent ransomware attacks.

This optimistic response may be because there's a sense of inevitability around ransomware; as attacks increase in frequency and sophistication, leaders feel it is more likely one will eventually succeed.

As a result, cybersecurity leaders feel less personal accountability when an attack succeeds: **57%** would feel very personally responsible in the event of a ransomware attack, falling from 71% last year. In the Netherlands, this drops to 36%.

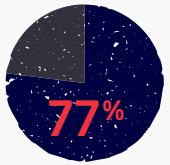
Given the perception that attacks are inevitable, many leaders are placing greater emphasis on mitigation than prevention.

While last year, 46% of leaders said they felt prepared because they were proactive in preventing attacks, this year that has fallen to **43%**.

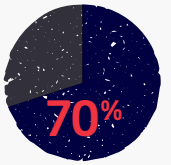
Instead, cybersecurity decision-makers consider **file backup and recovery** the most critical technology for reducing the risk and damage of ransomware attacks – selected by **49%** of leaders, compared to 39% last year.

There seems to be space for many businesses to take a more proactive stance when it comes to attack prevention, particularly the deployment of more sophisticated tools and integrations.

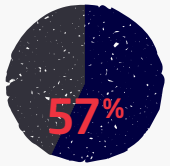
For instance, email is a key vector for cyberattacks. Over half of the cybersecurity leaders (53%) have encountered a **phishing email** with ransomware attachments, rising to 72% in Germany, while **43% have faced phishing emails leading to a drive-by download**.



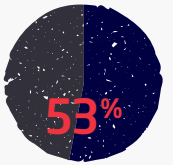
of cybersecurity decision-makers feel supported by their senior leadership team or board



say their company is very well prepared to prevent ransomware attacks



of cybersecurity leaders would feel very personally responsible in the event of a ransomware attack



of cybersecurity leaders have encountered a phishing email with ransomware attachments

As a result, two-fifths (39%) consider flagging suspicious email messages with **warning banners** one of the most effective measures their company takes to protect against ransomware.

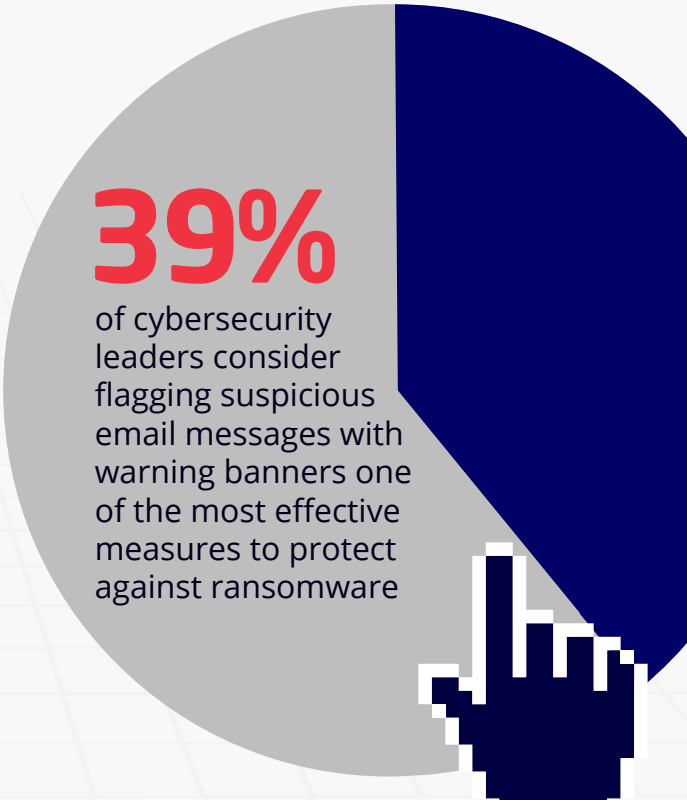
Nonetheless, just 35% are investing additional budget in AI/ML such as warning banners embedded in suspicious emails over the next year, while only 35% are introducing dedicated **secure email gateways**.

Importantly, cybersecurity leaders aren't currently tapping into the power of integration to drive a more proactive approach to their posture. Despite the growing complexity of enterprise networks and the range of **security solutions** in place, under three in ten leaders (29%) feel their preparedness for ransomware attacks is based in **sharing threat intelligence** across different security controls using **API integrations**.

Likewise, only 28% integrate their security controls into a **SIEM** or **SOAR** platform so they can orchestrate their ransomware response.

Conversely, when considering the additional resources they need, **31%** of leaders say their company needs integration of security controls into a SIEM or SOAR platform to prevent and prepare for ransomware attacks, and **30%** name sharing of threat data across security controls.

Many organizations appear to be missing the opportunity to use integration to gain better visibility and earlier threat detection: ultimately, not only identifying attacks earlier when they do occur, but reducing likelihood of success.



The Bottom Line

The frequency of attacks seems to be breeding a sense of inevitability that attacks will happen. Cybersecurity leaders seemed almost resigned to a breach – in turn, they feel less personally responsible if criminals succeed, as long as mitigation strategies are in place.

However, this is a dangerous strategy, which depends on organizations having the best practices in place. Not all data backup and recovery strategies are created equal; it would be one thing to lose a week of data, but what about six months? Is there a robust plan for coping as an attack takes places, and dealing with the aftermath? Would employees be able to access vital information and continue to operate?

In the face of the growing ransomware threat, security must go beyond checking the boxes on compliance and mitigation. Proactive prevention will not only reduce the likelihood of attacks but lower their impact when they do succeed.

Given the complexity of most enterprise networks, organizations will often benefit from an integrated approach – adopting a cybersecurity mesh architecture that adapts security protections to each asset in the network. This increases visibility, minimizing **dwell time** and helping busy teams to identify and address attacks more readily.

Mimecast's VP of Sales Engineering Brian Pinnock, the often-repeated phrase, "It's not a question of if but rather when a cyber incident occurs," may well be true, but is not a very useful guide to proactive cyber risk management.

Brian states, "The phrase provides limited actionable insight with which to direct investment in people, processes, or controls. The phrase suggests inevitability on an infinite time horizon which steers our attention away from making actionable risk-based decisions today based on a quantitative assessment of the organization's risk of future ransomware incidents."

"When examining metrics like the loss event frequency, which is increasing in most geographies, and the loss magnitude, which is also increasing, it is important to ask, 'by how much?' and 'What preventative measures can reduce these statistics?'" Brian continues.

"Proactive measures such as the use of AI/ML, threat sharing and integrating security tools appear underutilized, which suggests there is greater scope to reduce vulnerability and bring down the frequency of successful ransomware attacks. Mitigation is important too but the implicit assumption by 56% of the respondents is that it is the only lever available to pull."

The Mimecast State of Ransomware report allows organizations to update to their risk assessments based on quantitative changes being seen in different geographies in metrics like the threat event frequency, levels of vulnerability, the potential loss magnitude both in terms of primary loss (usually monetary loss based on ransom payments, loss of data, and productivity) as well as secondary losses such as reputational losses and fines. These assessments can then help to direct an organization's investment decisions in more appropriate ways.

Recommendations

Cybersecurity teams are suffering from significant personal strain today, including those in leadership positions. Cybercriminals have only intensified their efforts since the pandemic, leaving teams battling to defend complex networks against sophisticated attacks. There are clearly personal consequences, from stress and burnout for individuals, through to talent shortages across the profession as a whole.

Ransomware is a large part of the problem, as the threat evolves and proves increasingly harmful – whether that's on an operational level, or from businesses' wider financial or reputational perspective.

Yet, amongst cybersecurity decision-makers, there's an ambiguity around their readiness to combat it. While only 6% feel somewhat prepared to mitigate the effects of a ransomware attack, at the same time, they're still hungry for more resources to get ahead of the threat for proactive prevention.

There's a sense of inevitability that can even border on fatalism around ransomware attacks, leaving many organizations overly reliant on mitigation like file backup and recovery – which isn't a failsafe strategy.

Once an attack takes place, another is much more likely, not least because cybersecurity teams can struggle to retain and recruit staff. It's critical that businesses look ahead to avoid getting caught in a cycle of incident after incident.

Cybersecurity leaders should focus on improving their defensibility: making their posture more proactive to reduce the chances of a ransomware attack causing disruption.

01.

Integrate security tools to improve threat detection capabilities and responses, alleviating pressures on busy teams

With threat actors launching sophisticated attacks that move across networks, fragmented security systems offer limited protection. Implementing a **cybersecurity mesh architecture** (CSMA) can connect separate security tools to adapt protections to each asset in the network, creating a zero-trust environment. In turn, using an **extended detection and response** (XDR) architecture can unify detection, investigation, and response by leveraging real-time data from multiple security systems – and then automatically instructing the security systems to respond. Doing this turns email systems into the eyes and ears of an organization, enabling greater threat detection capabilities.

02.

Ensure the business has good security fundamental practices in place, to reduce vulnerabilities

Simple steps can make attacks much less likely. It's crucial that cyber risk is considered a priority at the board level and leaders take a more involved approach. As employees are often targeted directly by attackers, **security awareness training** will improve your posture across the business. Email is a particularly threatening vector of attack, so robust, up-to-date **email security solutions** are also a valuable investment.

03.

Evaluate your business continuity planning to understand the real consequences of an attack

Given the increasing number of ransomware incidents, it is important for teams to have the best **disaster recovery** strategies in place in case an attack takes place – but that depends on the detail. Ensure that best practices are followed throughout your organization; for instance, ensuring that **data backups** are completed as regularly as possible. Modeling your attack response can help highlight any gaps in your **business continuity planning**.

Ransomware, along with all forms of cybercrime, won't stand still. It's critical that cybersecurity teams can make the best use of their resources – and that organizations ensure they have the support they need.

This way, we can lower the total cost of ransomware to businesses and individuals, as well as ensuring that cybersecurity is a sustainable, fulfilling career.

Work Protected.

Advanced Email & Collaboration Security

mimecast

Mimecast is a cybersecurity provider that helps thousands of organizations worldwide make email safer, restore trust and bolster cyber resilience. Mimecast's expanded cloud suite enables organizations to implement a comprehensive cyber resilience strategy. From email and web security, archive and data protection, to awareness training, uptime assurance and more, Mimecast helps organizations stand strong in the face of cyberattacks, human error and technical failure.