mimecast

FACING THE REALITY GAP

State of Ransomware Readiness

The Year of Ransomware

Awareness of ransomware and the risk it poses has accelerated dramatically in recent months. Thanks to a number of high-profile attacks, the involvement of nation-state actors, the response of governments around the world, and the downstream impact on everyday citizens, the conversation has been taken to a new level.

Who's at risk? Everyone.

Large enterprises represent a greater prize and therefore make for highly attractive targets. The lure of financial gain and increasingly, access to these organizations' customers and partners, is more than enough incentive for cybercriminals to apply the skills, time, and resources to launch sophisticated attacks. At the same time, small to medium-sized businesses may be considered softer targets that can be successfully breached at a higher volume.

Attacks can start in many different ways, though phishing and RDP attacks are common entry points. And complicating things further, attacks may not actually start as ransomware attacks.

Some threat actors exist to not launch the ransomware attack themselves but instead, to obtain something that they can sell to ransomware actors, such as credentials or access to a compromised device. This means that any cyber defense is a contributor to the fight against ransomware.

The bottom line is that all organizations must prepare for the reality of ransomware, doing everything possible to prevent attacks but also equipping themselves to contain, respond, and recover when an attack does get through.

WHO

Survey Results

For this report, Mimecast commissioned Hanover Research to conduct a global survey of 742 cybersecurity professionals from Australia, Canada, Denmark, Germany, the Netherlands, South Africa, Sweden, the United Kingdom, and the U.S.

> **The goal was to understand how executives are managing the rise in ransomware attacks, not only from a sense of confidence in their own preparation against these attacks, but also in how they are hardening their organizational defenses against ransomware.**

Participants were interviewed in September 2021. Sixty-eight percent of respondents worked in organizations with at least 1,000 employees; of that, 28% were from companies with 5,000 or more employees. All respondents held some or all responsibility for cybersecurity decision-making, and hold titles in security or cybersecurity operations including director, vice president, CIO, or CISO.

Key Findings

80%

of organizations have been attacked by ransomware

83%

Most executives (83%) say they regularly review disaster recovery protocols

1/3+

More than one-third of companies choose to pay the ransom in full when facing a ransomware attack

42%
Experience disruption

36%
Experience downtime

77%

of executives are confident in their company's preparedness for ransomware attacks

39%

More than one-third of executives (39%) feel they could lose their jobs over a successful ransomware attack

2/3

Two-thirds of executives would feel very or extremely responsible for a successful ransomware attack

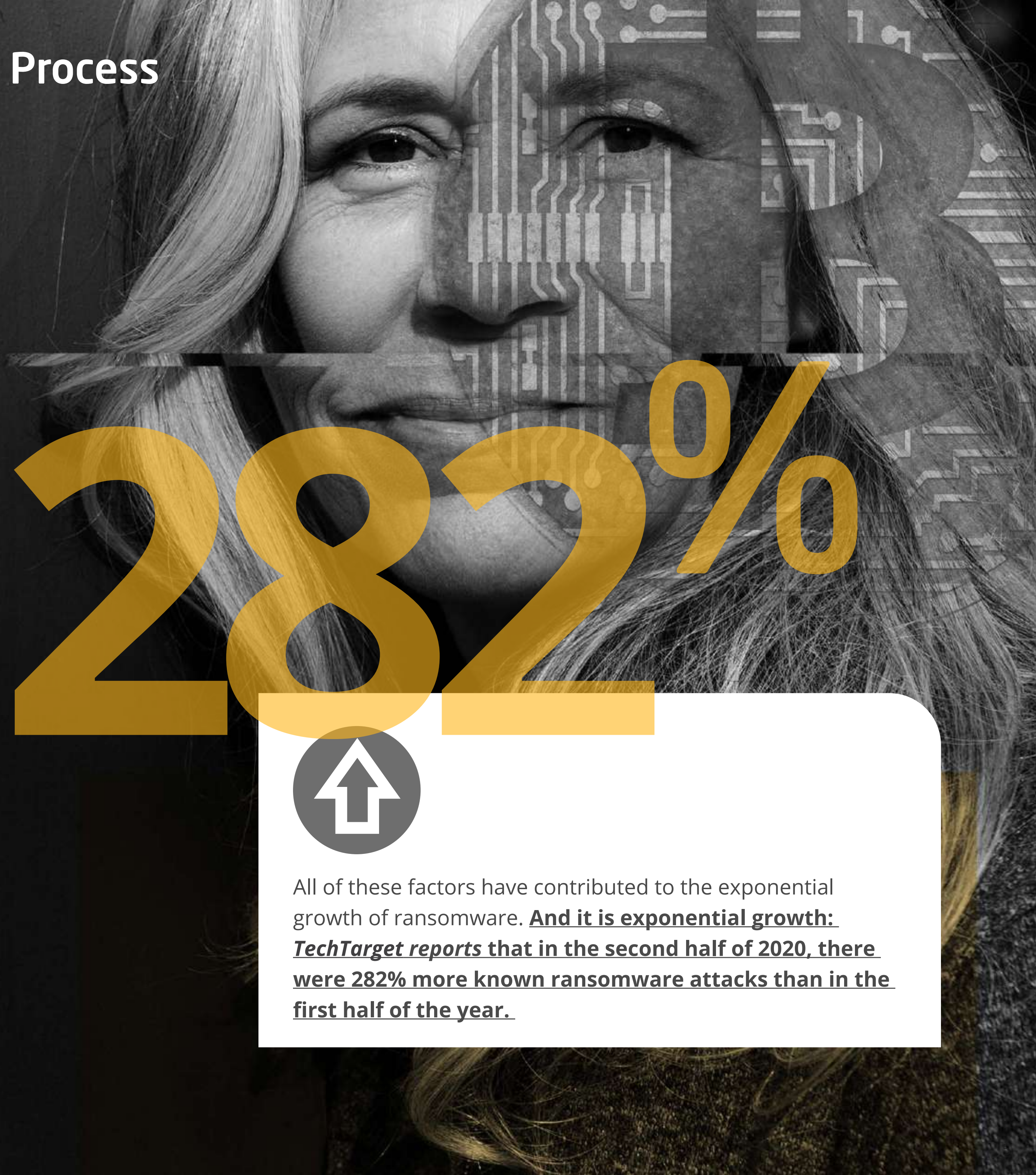
60%
because it is their job to protect the company

48%
because they underestimated the ransomware threat

Technology, People, Process

People, technology, and process are well known as the triangle critical for enterprise transformation and management. Together, these three areas can drive success for enterprises, but only if they are in lockstep to support each other.

Unfortunately, major global events like the COVID-19 pandemic have forced many employees to work remotely, and businesses – and their supply chains – have been thrown into well-documented chaos, creating imbalances among people, technology, and process.



All of these factors have contributed to the exponential growth of ransomware. **And it is exponential growth: *TechTarget reports* that in the second half of 2020, there were 282% more known ransomware attacks than in the first half of the year.**

BACK UP

IT security leaders are facing challenges related to **technology**, in particular. The shift to remote working has resulted in numerous new devices to protect and left organizations more vulnerable to attacks through unsecured networks. Shadow IT, or the use of unsanctioned applications by employees, is also a growing security problem that can open the door to ransomware attacks.

The survey results show that organizations are responding to this increased level of risk by investing in the technology they feel is most likely to reduce future ransomware attacks: Executives consider web security (47%) and end-point protection (45%) the most critical technologies for reducing ransomware risk.

47%

web security

45%

end-point protection

Yet, respondents cited phishing emails with ransomware attachments or a phishing email leading to a drive-by download as the primary source of ransomware attacks,

54%

phishing emails with ransomware attachments

45%

phishing email leading to a drive-by download

suggesting that they may be leaving the most critical attack vector – email – under-protected.

What's more, in the event of a ransomware attack, **data backups can help get companies back to normal more quickly** and can even help them avoid having to pay the ransom, but just 45% of respondents reported they have invested in file backups. Regardless of their investment priorities, a significant percentage (45%) would like budget to fund more up-to-date security systems.

46%

From a people perspective, most security experts agree that end-users remain the weakest link. **Nearly half of executives want additional resources for more frequent security awareness training of end-users (46%).**

42%

German executives were significantly more likely than other countries to want additional budget dedicated to security awareness training

58%

Companies with 5,000 or more employees were significantly more likely to invest in security training

On the process side, executives are interested in integrating their security controls, due to the complexity and rapidly evolving nature of ransomware. As every CISO is well aware, cybersecurity grows more complicated every year; adding tools to reduce ransomware risk sounds like a fix until it’s time for those tools and technologies to work together. This may be why 40% of respondents want greater *sharing of threat data* across their security controls.

This trend is even more pronounced in South Africa, where 50% of executives say they want integration of security controls into a SOAR platform to better prevent and prepare for ransomware attacks.

Preparedness vs. Confidence

In Mimecast's State of Email Security 2021, more than six in ten (61%) of respondents acknowledged that their business had been interrupted by ransomware; they reported six days on average of downtime; but for 37%, it was a week or more.

In this survey, respondents experienced an average of about 3,000 ransomware attacks over the last two years – or an average of four attacks per day. Large enterprises (companies with 5,000 employees or more) are bearing the brunt, experiencing nearly 10,000 attacks over two years. These companies have encountered encryption (52%), network-wide attacks (45%), and double extortion (41%).

on average

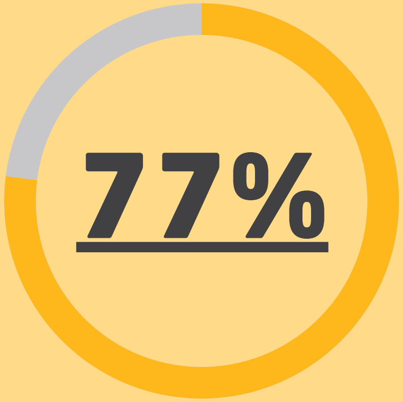
4 attacks per day

the average number of attacks for all respondents was 3,055 over two years which equate to 4 a day

on average

6 days downtime

but for 37%, it was a week or more



With these numbers in mind, it's somewhat surprising that so many executives – 77% - report feeling prepared for a ransomware attack. They indicated that their readiness was due to systems that are kept patched and up to date (47%), proactivity in preventing attacks (46%), a disaster recovery plan (46%), and file backups (45%). Respondents also stated they take additional measures to protect their organizations, such as training employees to recognize email threats that lead to attacks (60%), flagging suspicious email with warning banners (40%), and opening suspicious links in a browser isolation session (29%). Just one in five (18%) run red team exercises.

As for downtime, two thirds (67%) noted they can withstand just 1-5 days of downtime before incurring significant financial loss or reputational damage. This is perhaps why 59% believe they would be able to get business operations back up and running within five days of an attack.

An additional reason executives may feel prepared is that more than three-quarters have received incremental budget to help address the ransomware problem. Another 12% expect to receive incremental budget in the coming year, suggesting awareness of the gravity of the issue by the board and C-suite. *A recent Deloitte survey* supports the finding: Sixty-five percent of C-suite executives said ransomware is their primary cyber threat concerns, but only a third say their organizations have simulated ransomware attacks to prepare for such an incident.

58%

The US and Germany are most confident in their preparedness because they feel they have adequate IT and security staff

58%

Germany is most confident in their expertise (58%) and their budget to prepare for attacks (56%)

On the other side, very few executives (5%) believe they are not at all or only slightly prepared for a ransomware attack. Of these few executives who stated their company is not prepared, they highlight a lack of expertise (75%), cyber liability insurance (50%), and lack of file backups (50%) as the primary reasons.

43%

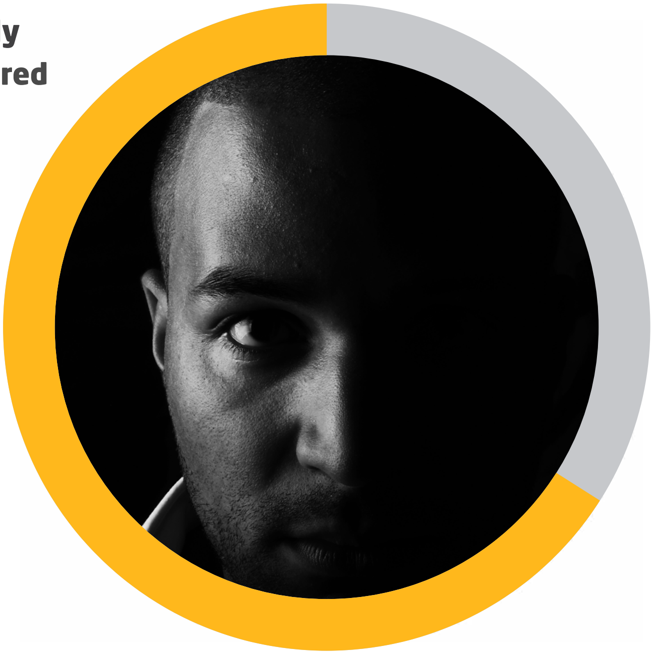
One positive takeaway? Companies are not relying on *cyber insurance.* In fact, **less than half of executives (43%) think it is extremely likely their insurance provider would cover the full ransom payment.**

Responsibility vs. Liability

It's a CISO's job to monitor the threat landscape and prevent cyber risks from taking root in the organization; preparing for ransomware attacks and maintaining disaster recovery plans are critical elements of cybersecurity leadership, and CISOs can be held to account by everyone from the C-suite and regulators, to customers and partners, when a ransomware attack threatens the business. Indeed, more than a third of executives (39%) stated they could lose their jobs as a result of a ransomware attack.

Two-thirds would feel very or extremely responsible if a successful attack occurred

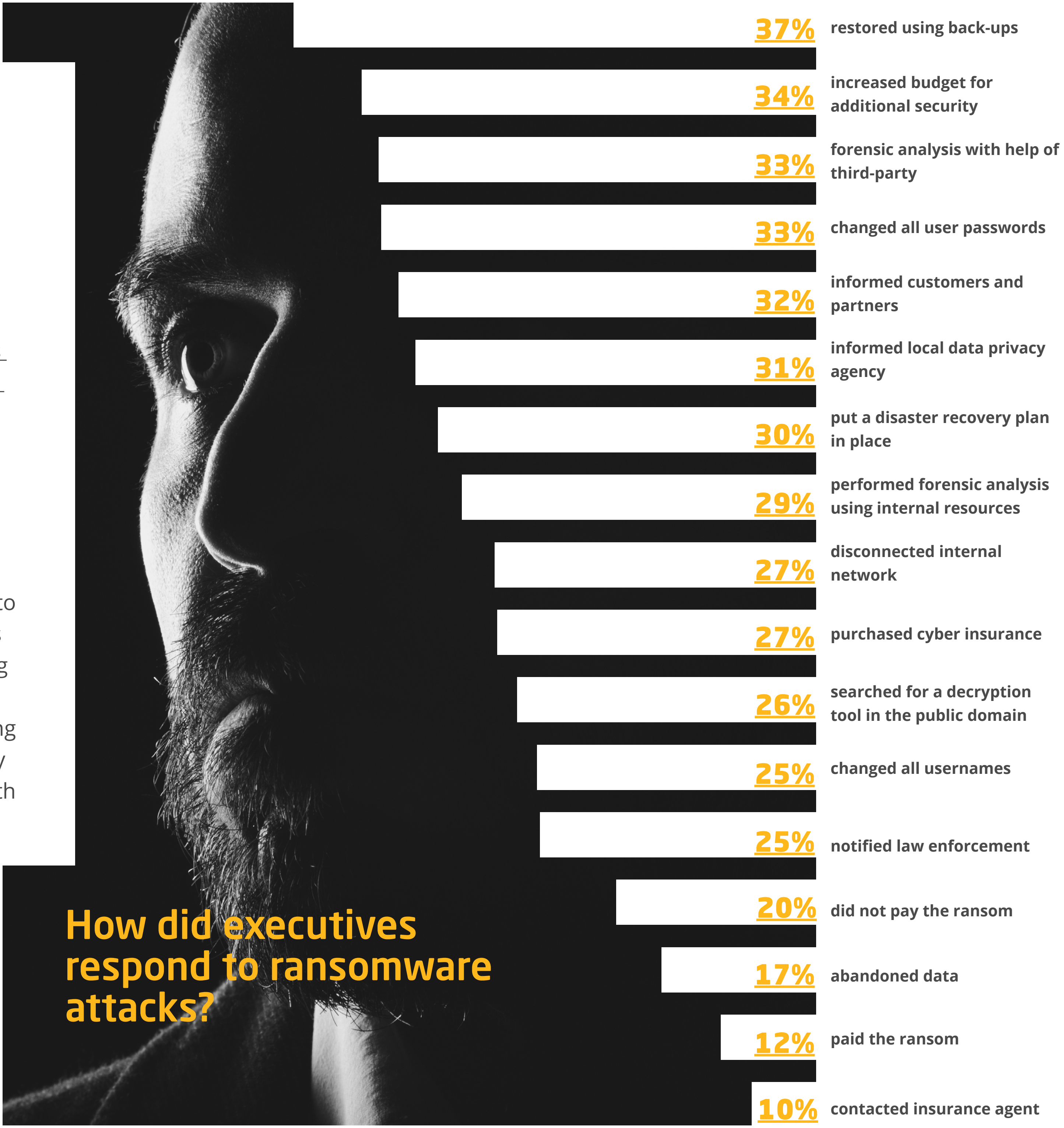
Why?
60% said it's their job to protect the company, and 48% said it would be because they underestimated the risk of a ransomware attack.



One-third would not feel personally responsible

Why?
Cybercriminals getting better at attacks (38%) and the fact that no one can prevent all attacks (35%). Others stated that they don't feel responsible because they are not adequately staffed to prevent attacks, and 11% state that their executive team doesn't support security awareness.

Regardless of whether executives feel a sense of responsibility to prevent ransomware, they do have an obligation to fight back against the tidal wave of ransomware businesses are experiencing. **Eight in ten respondents' organizations were successfully attacked via ransomware, which offers an important look into how to navigate post-attack waters.** For example, the figure showed that executives who experienced ransomware attacks tended to take a series of simultaneous actions immediately following the attack, such as restoring data using backups, increasing budget for additional security controls, forensic analysis with a third party, and more.

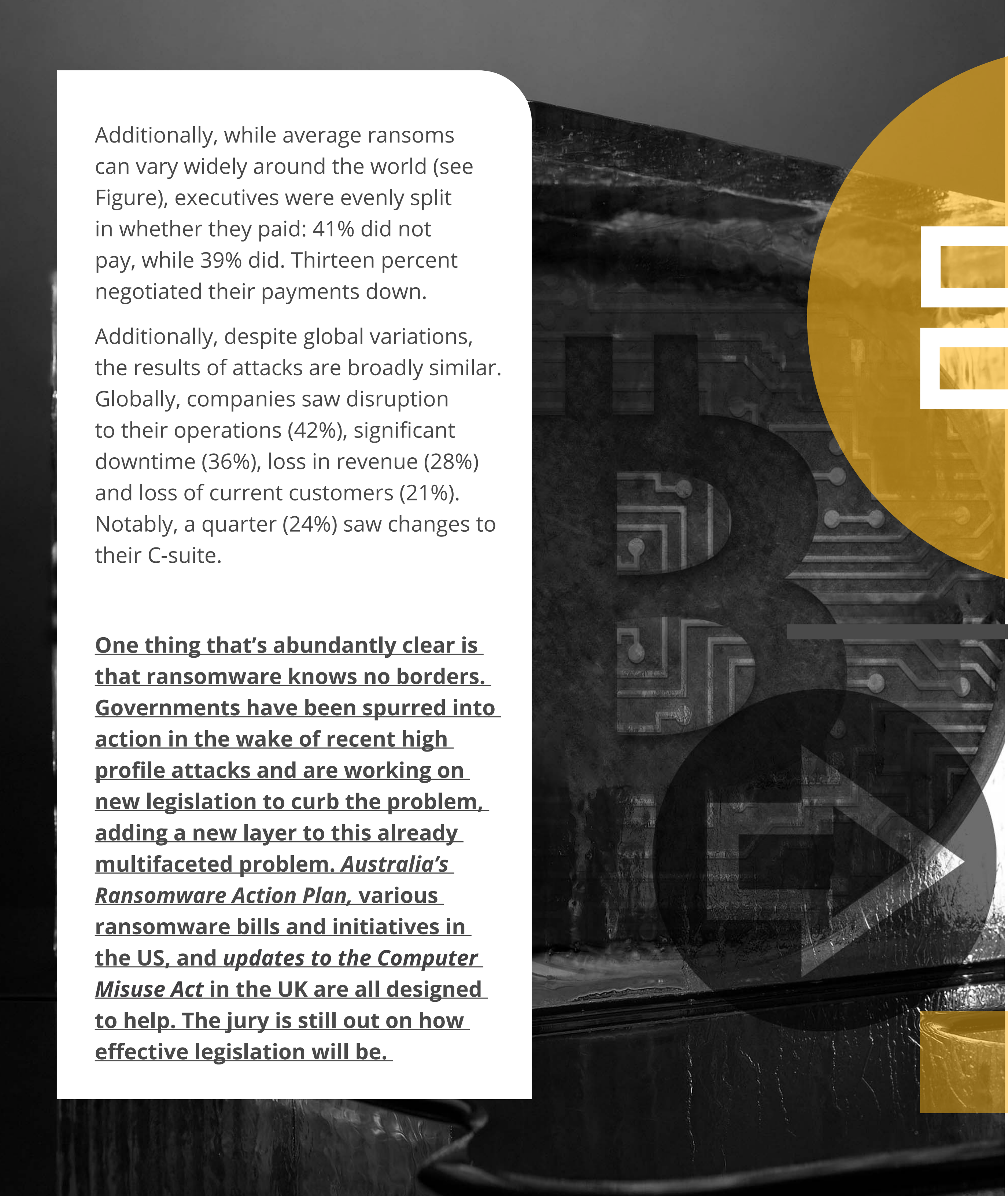


How did executives respond to ransomware attacks?

Additionally, while average ransoms can vary widely around the world (see Figure), executives were evenly split in whether they paid: 41% did not pay, while 39% did. Thirteen percent negotiated their payments down.

Additionally, despite global variations, the results of attacks are broadly similar. Globally, companies saw disruption to their operations (42%), significant downtime (36%), loss in revenue (28%) and loss of current customers (21%). Notably, a quarter (24%) saw changes to their C-suite.

One thing that's abundantly clear is that ransomware knows no borders. Governments have been spurred into action in the wake of recent high profile attacks and are working on new legislation to curb the problem, adding a new layer to this already multifaceted problem. *Australia's Ransomware Action Plan,* various ransomware bills and initiatives in the US, and *updates to the Computer Misuse Act* in the UK are all designed to help. The jury is still out on how effective legislation will be.



Average Ransom Payment by Country

Australia	$ 79,857
Canada	$ 6,666,220
Denmark	DKK 2,098,418
Germany	€ 171,203
Netherlands	€ 95,968
South Africa	R 3,261,352
Sweden	KR 11,917,905
United Kingdom	£ 628,606
United States	$ 6,312,190

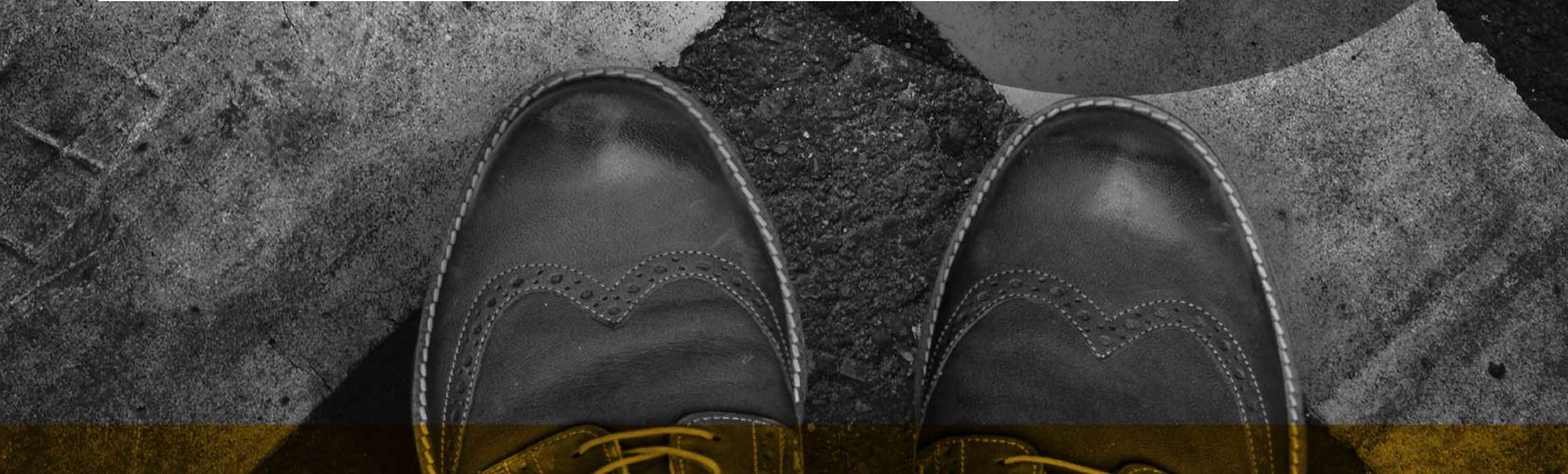
The Bottom Line

Ransomware has a devastating impact on businesses, governments, public services, and everyday lives. The problem is complex, and the risk is rising.

That means all organizations need the strongest possible protections in place. Email is the number one attack vector, making email security a priority for CISOs. But it's only one piece of the puzzle.

The reality is that the solution to ransomware does not lie with a single technology, entity, or idea. It lies with an integrated set of security controls that support a defense in depth approach. It lies with the collective power of organizations – both public and private – committed to regaining control. And it lies with fighting using every tool at the cybersecurity community's disposal, from technology and partnerships to intelligence sharing and policy, to stand strong against a determined set of adversaries. The time has come to fight back against ransomware together.

Visit Mimecast's Ransomware Hub to learn more and connect with a specialist.



mimecast®

Relentless protection. Resilient world.™