2018

Cybersecurity
RESEARCH

RANSOMWARE REPORT

INTRODUCTION

Ransomware attacks, in which hackers encrypt an organization's vital data until a ransom is paid, have become a billion dollar cybercrime industry according to the FBI. Ransomware is now widely seen as the single biggest cybersecurity threat to both business and government organizations.

In many respects, ransomware is a game changer. It is incredibly easy and inexpensive for criminals to execute global attacks. At the same time, ransomware is extremely profitable as many businesses will simply pay the ransom to get their mission-critical systems and data up and running again. And even if they don't pay out, the cost of downtime, cleaning up IT systems, and restoring backup data can significantly impact an organization's bottom line.

We hope you will enjoy the report.

Thank you,

Holger Schulze

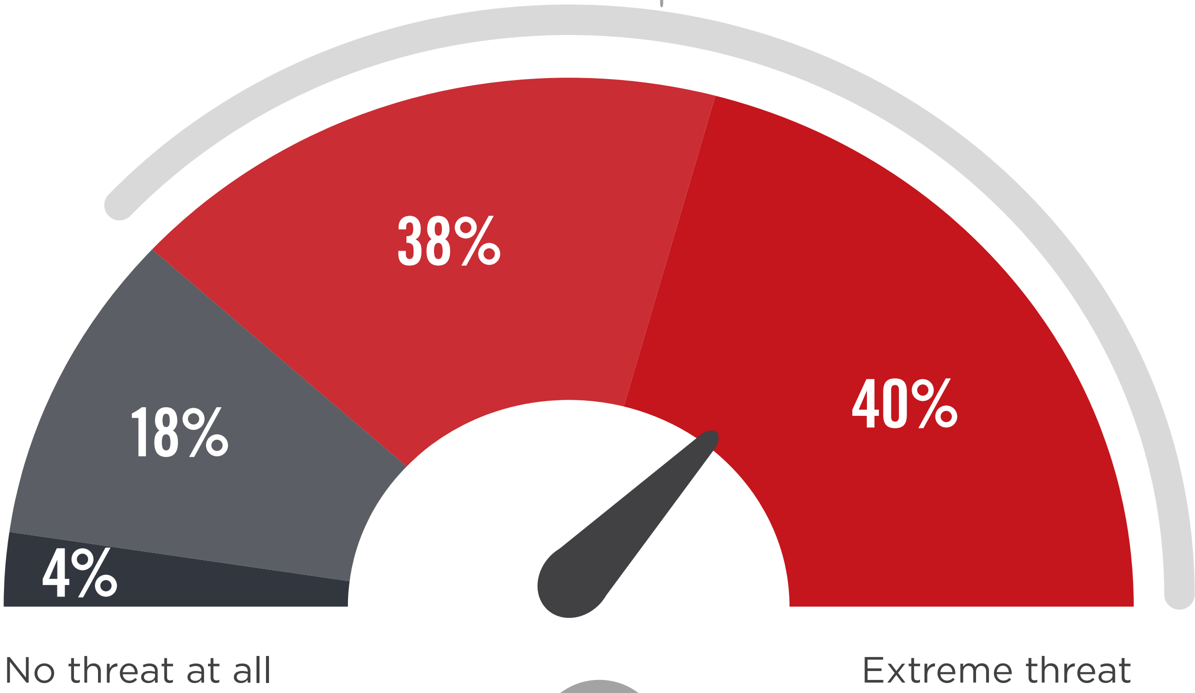
Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

RANSOMWARE THREAT

Ransomware is still one of the most destructive security threats affecting organizations of all sizes, from SMBs to large enterprises and government agencies. Seventy-eight percent of respondents perceive ransomware either as an extreme threat (40%) or moderate threat (38%). Very few respondents (4%) see ransomware as no threat at all.

▶ **How significant a business threat is ransomware to your business?**



78% of respondents see ransomware as an extreme or moderate threat.

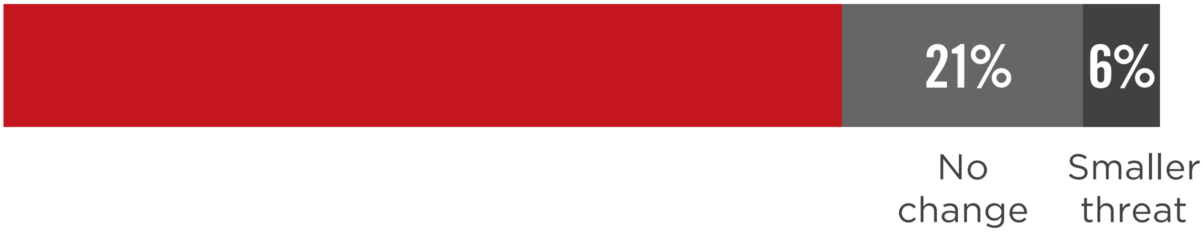
FUTURE ATTACKS

A significant majority (73%) of IT security professionals predict ransomware to become a larger threat in the future. 71% expect an increase in attack frequency over the next 12 months.

In the next 12 months, do you believe ransomware will be a larger or smaller business threat to organizations?

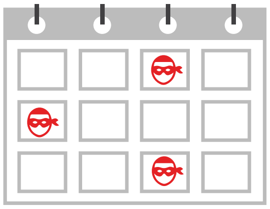
73%

believe ransomware will be a larger threat to organizations in the next 12 months

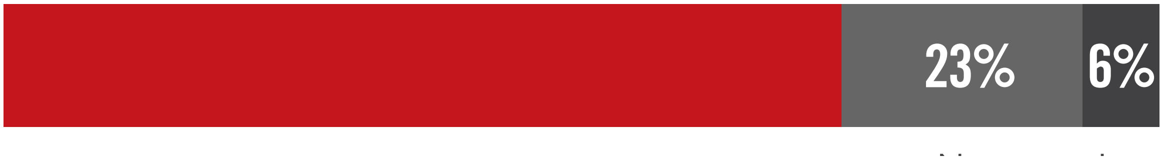


In the next 12 months, do you believe ransomware will be a larger or smaller business threat to organizations?

71%



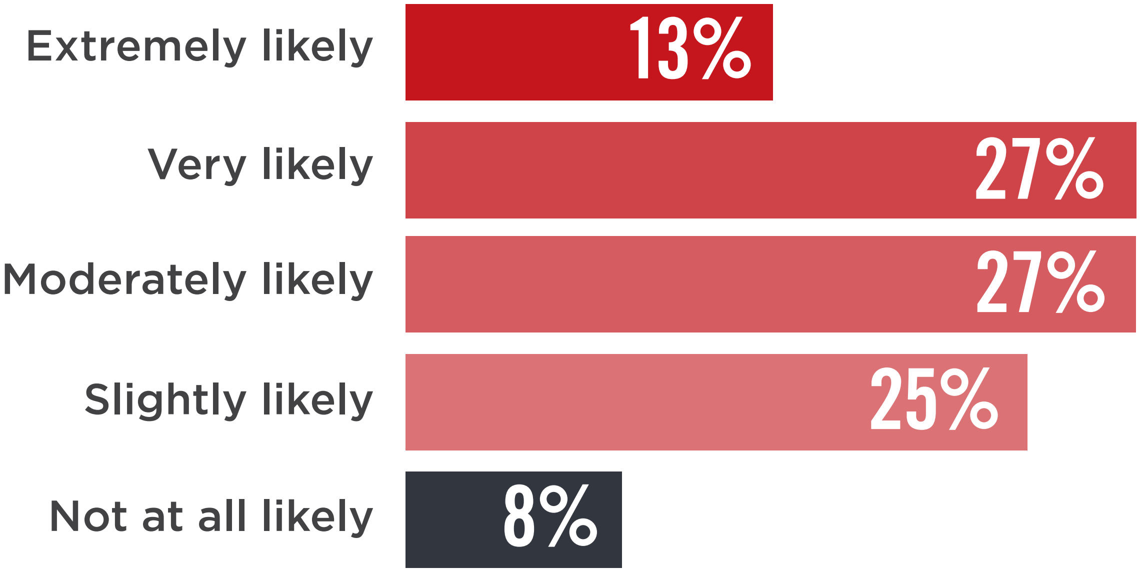
believe ransomware attacks will be more frequent



RANSOMWARE OUTLOOK

When asked about their outlook as a future target of ransomware, a majority of 67% estimate the probability to become a target of a ransomware attack as at least moderately likely.

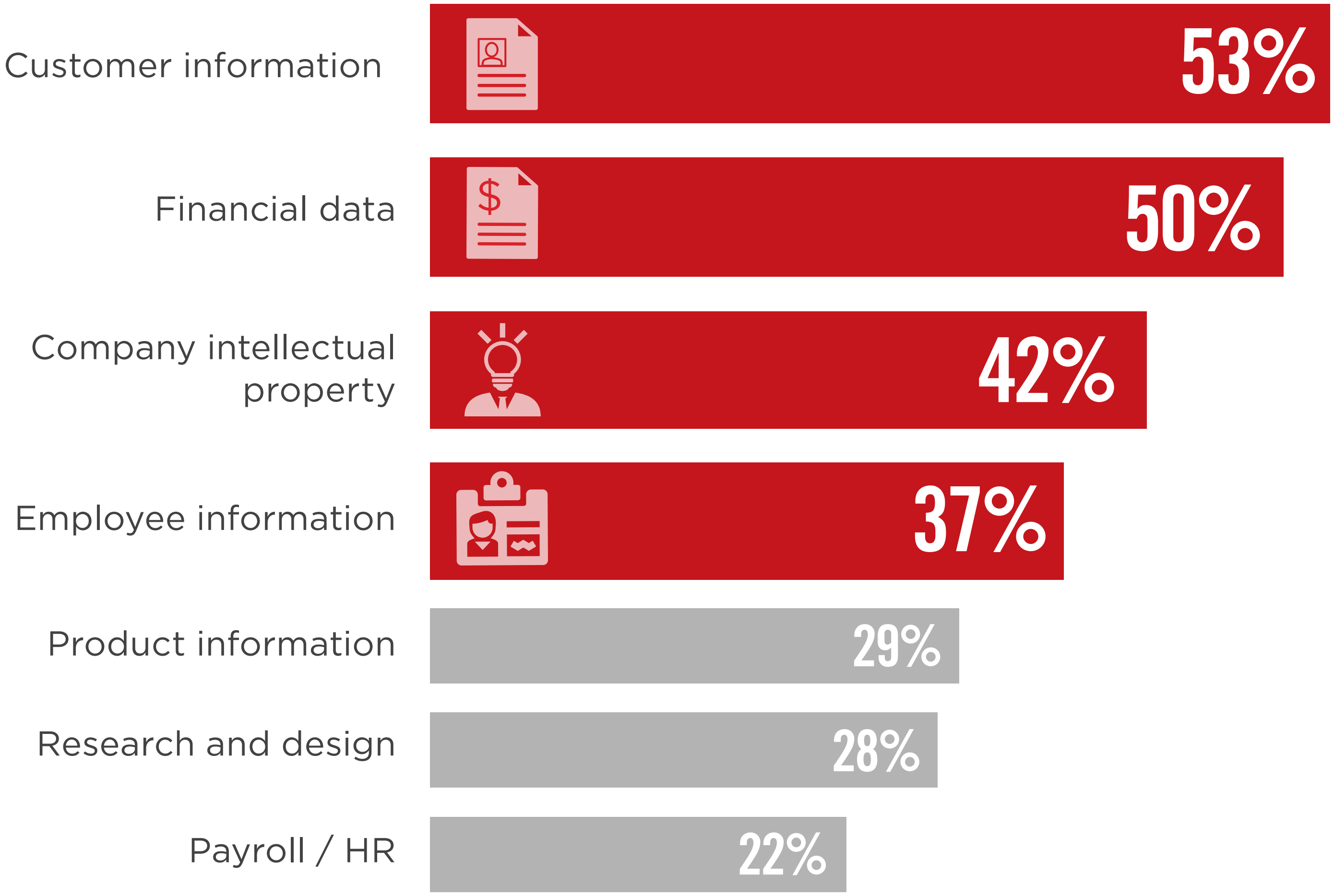
What is the likelihood that your organization will be a target of ransomware in the next 12 months?



DATA AT RISK

Data has become a strategic asset to virtually every organization and a high value target for cybercriminals. Our research reveals that the information most at risk from ransomware attacks is customer information (53%), closely followed by financial data (50%).

What type of data in your organization is most at risk from ransomware attacks?

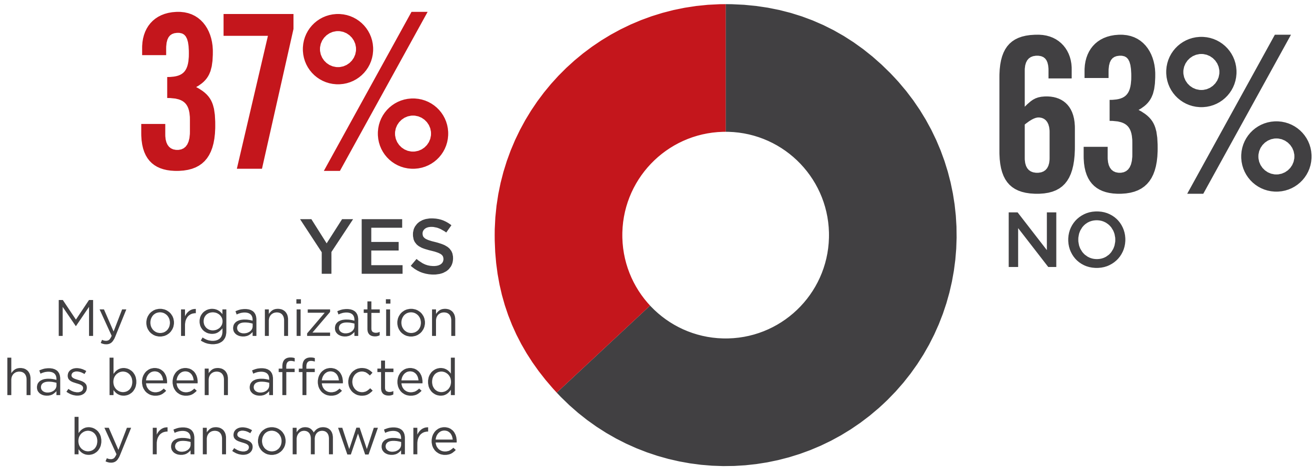


Other 6%

RANSOMWARE EXPERIENCE

Over a third of organizations surveyed (37%) said they experienced ransomware attacks, up from 33% in last year's survey. Sixty-three percent of respondents have not been affected by ransomware yet or aren't aware of a previous or ongoing attack.

Has your organization suffered from ransomware attacks in the past?

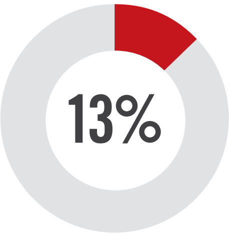


RANSOMWARE TYPE

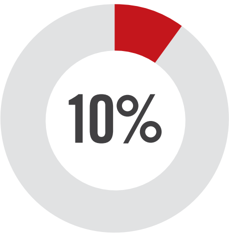
There is a wide and quickly evolving array of ransomware types, and new variants are created virtually every day. The organizations affected by ransomware overwhelmingly confirm that they encountered encrypting ransomware (or cryptoware that encrypts files and renders them inaccessible) as the top offender at 92%, up from 88% in last year's survey.

What type of ransomware infected your organization?

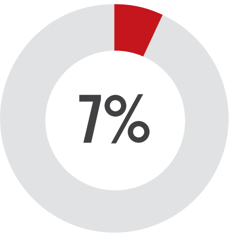
92% **Encrypting ransomware or cryptoware**
(encrypts files and makes them inaccessible)



Ransomware that encrypts MBR or NTFS
(prevents victims' computers from being booted up in a live OS environment)



Non-encrypting ransomware or lock screens
(restricts access to files and data, but does not encrypt them)



Mobile device ransomware
(infects cell phones through "drive-by downloads" or fake apps)

Leakware or extortionware (exfiltrates data that the attackers threaten to release if ransom is not paid) 6% | Not sure/other 6%

BUSINESS & IT SECURITY IMPACT

Ransomware is changing the threat landscape and how organizations are impacted at the business level as well as from an IT security policy and control perspective. On the business side, ransomware attacks mostly caused system downtime (41%) and productivity loss (36%), i.e. the effect intended by cybercriminals to cause maximum pain and extort money.

At the IT operations level, ransomware attacks caused cybersecurity professionals to update IT security strategy to focus on mitigation (51%) and increase spending on IT security (39%).

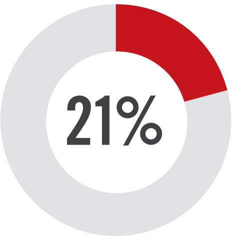
What has been the impact of ransomware attacks on your organization in the past 12 months?

51% Change of IT security strategy to focus on mitigation

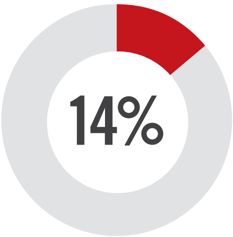
41% System downtime

39% Increased spending on IT security

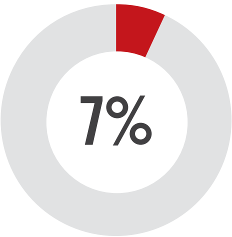
36% Productivity loss



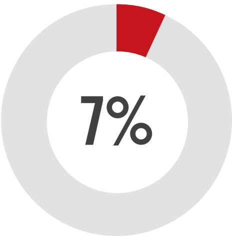
Data loss



Loss of confidence in existing cybersecurity solutions



Damage to company reputation



Revenue loss

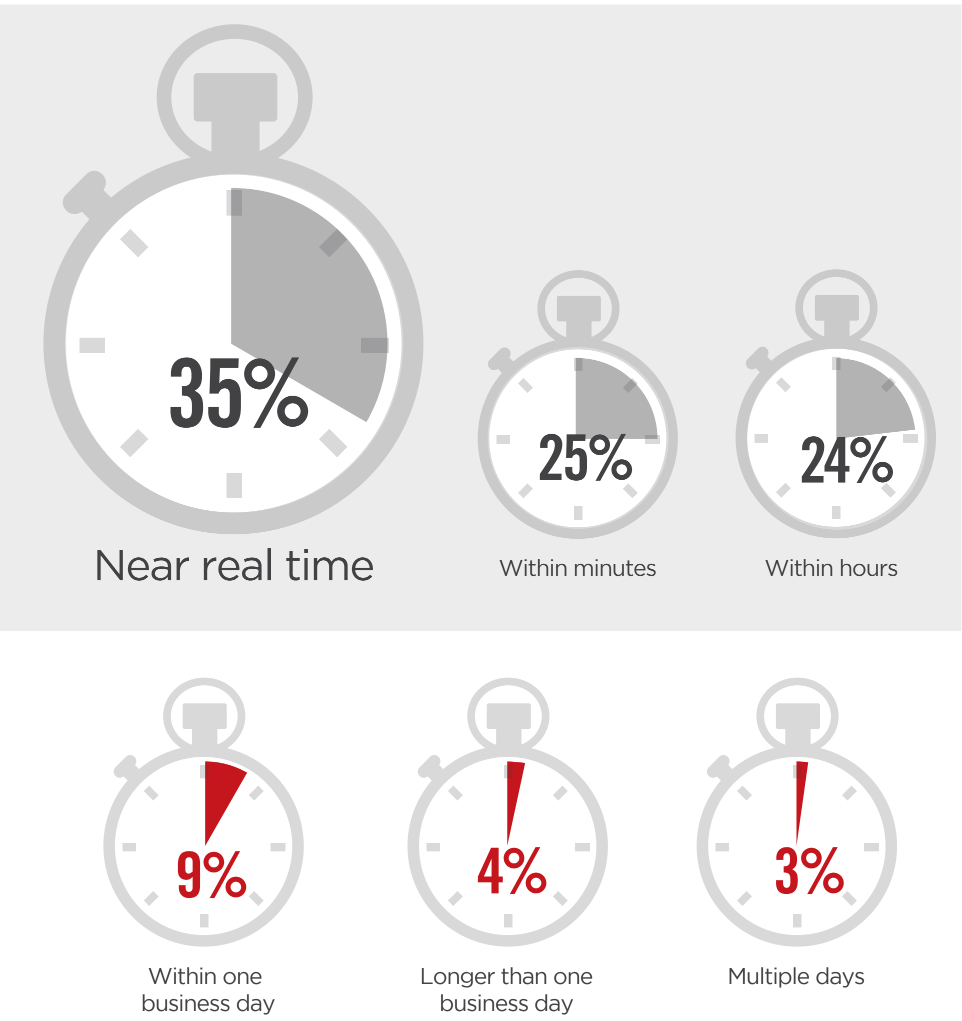
We did not experience any ransomware attacks 3% | Negative press/bad publicity 2% | Senior IT staff (CIO, CISO) lost their jobs 2% | Other 9%

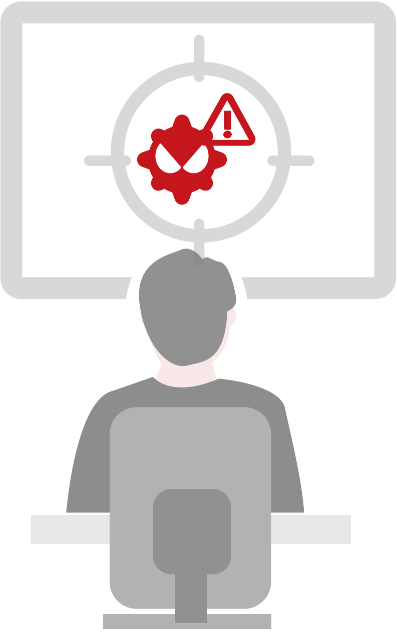
SPEED OF DETECTION

While the speed of ransomware detection varies based on the ransomware strain an an organizations detection capabilities, most attacks are typically detected within hours (84%), a marked improvement over last year's performance. Thirty-five percent of organizations claim detection is near real time, up from 24% in last year's survey. The rate and speed of ransomware detection is critical in combating fast moving attacks before they succeed in spreading across networks and encrypting vital data.

▶ **How quickly is ransomware typically detected by IT security when it attempts to enter your organization?**

84% Most attacks are typically detected within hours

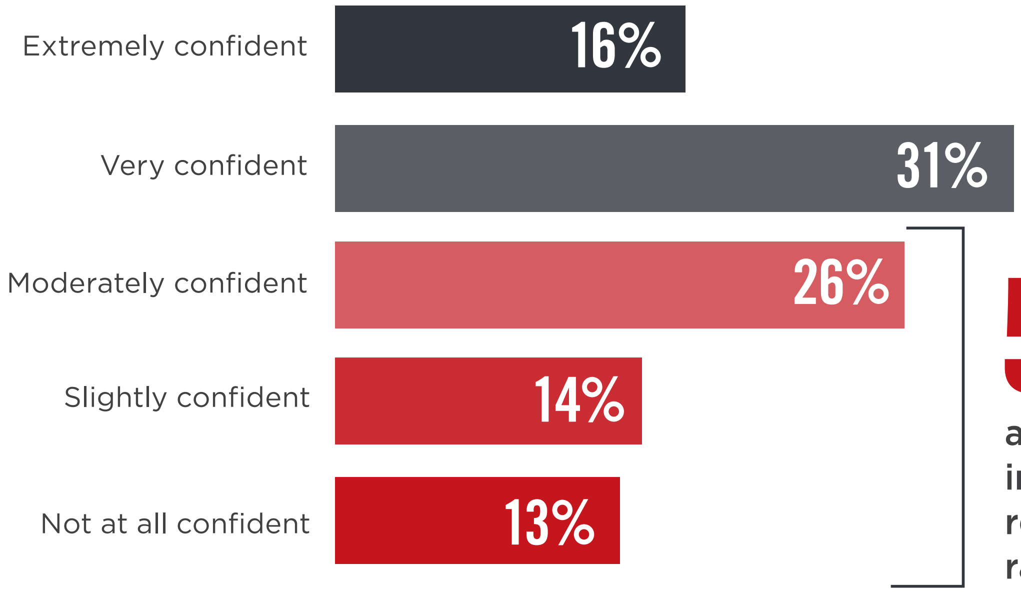




CONFIDENCE IN REMEDIATION

How confident are cybersecurity professionals in their organization's capacity to remediate a ransomware attack in progress that has already encrypted files and spread to critical IT systems across the organization? Only 16% are extremely confident in their organization's abilities to unlock or restore affected files and systems - unchanged from last year's survey. Thirty-one percent are very confident, up from 28% in last year's survey.

▶ **How confident are you in your organization's current ability to remediate ransomware AFTER it locks or encrypts data within your systems?**



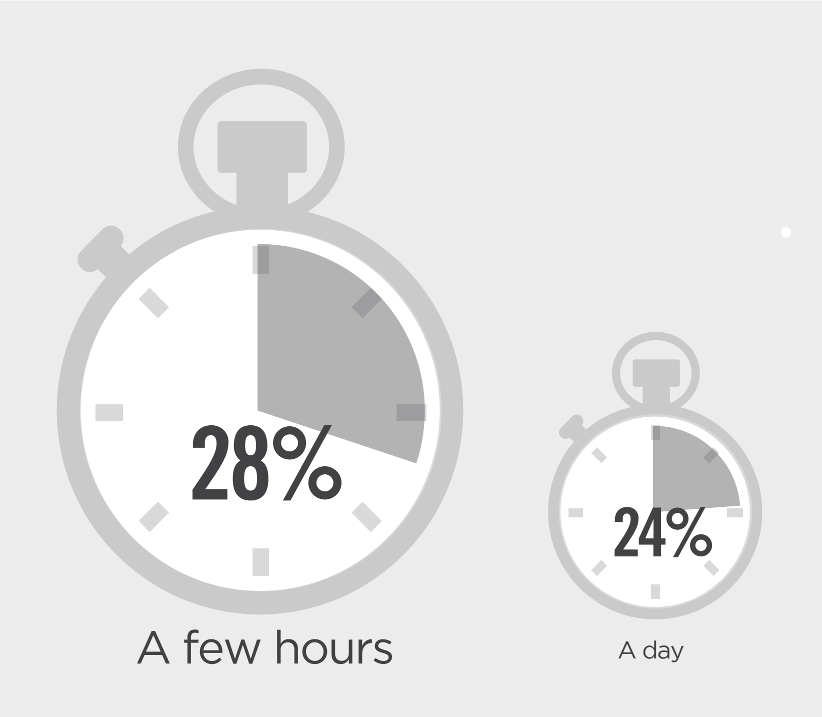
53%

are not fully confident in their ability to remediate after a ransomware attack

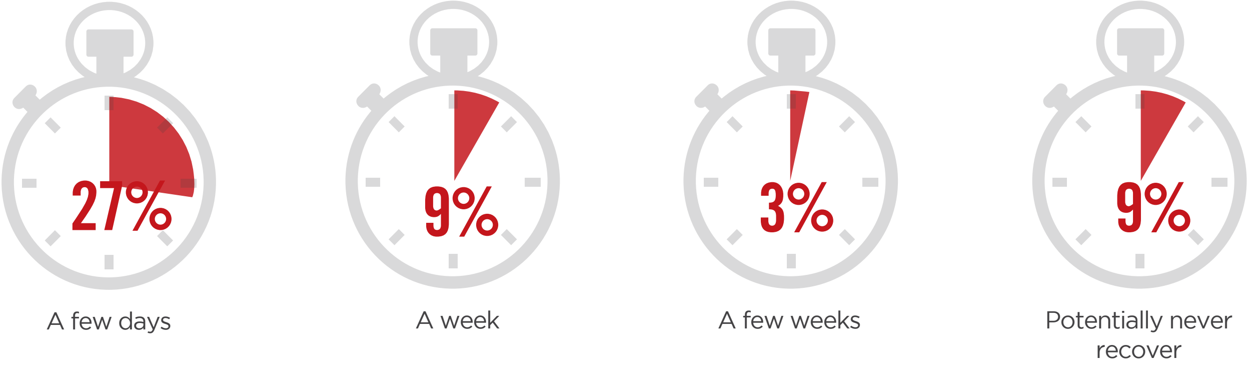
SPEED OF RECOVERY

A majority of 52% say they can recover from a ransomware attack within a day, while 39% estimate it will take more than one day to a few weeks to recover. Only 9% of the organizations believe they will never fully recover. Speed of recovery is absolutely critical as cost escalates with every hour the business cannot fully operate.

How fast do you believe you can recover from a ransomware attack?



52% could recover from a ransomware attack within a day

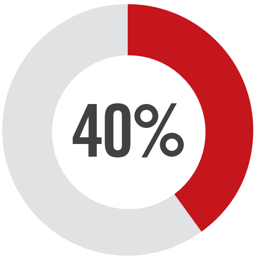


ATTACK RESPONSE TACTICS

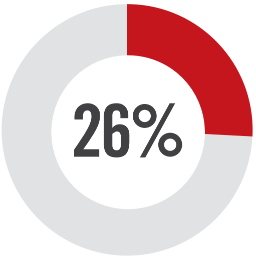
Following a ransomware attack, cybersecurity professionals can deploy a number of defensive responses. The single most common response motion (73%) is identifying the ransomware strain that is attacking the organization, containing the damage by isolating and shutting down all infected systems and accounts, eradicating the malware, followed by recovery from backup files. Only one percent of organizations admit to considering payment of the ransom.

▶ How would your organization respond when it has been detected that ransomware has attacked your systems?

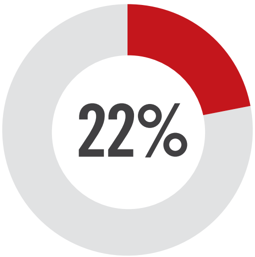
73% Isolate and shut down offending systems and accounts, recover encrypted files from backups, mitigate the initial attack vector if possible



Proactively shut down core systems to prevent spread



Immediately call law enforcement



Engage a third-party incident response service

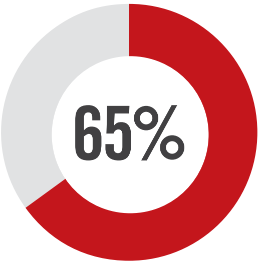
Attempt to decrypt files ourselves 20% | Notify customers 20% | Contact cyber insurance provider 16% | Attempt to negotiate with the attackers 10% | Pay the ransom 1% | Other 6%

RANSOMEWARE DEFENSE MOTIVATORS

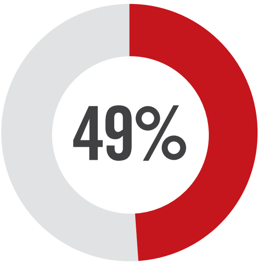
The biggest motivator for improving their organization’s ransomware defense is the protection of sensitive business data against attack, followed by preventing system downtime (65%).

What is your organization’s primary driver for improving ransomware defense?

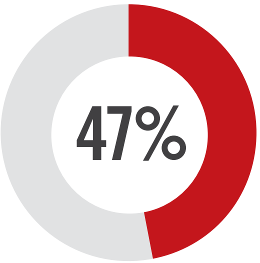
74% Protecting confidential data related to the business and clients



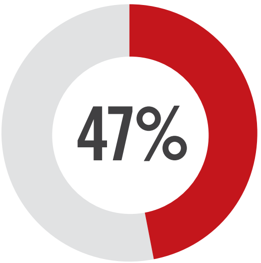
Saving the organization from potential downtime



Staying a step ahead of emerging threats



Protecting the reputation of the brand



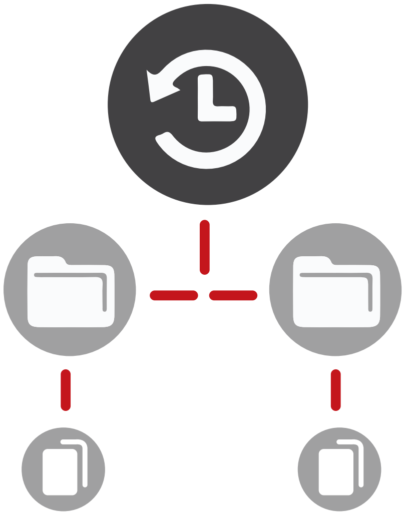
Mitigating the financial costs arising from ransomware attacks

Other 1%

RANSOMWARE RESPONSE

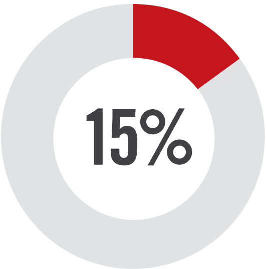
Cybersecurity professionals continue to view data backup and recovery (72%) by far as the most effective solution to respond to a successful ransomware attack. This way, organizations can often restore critical data without having to pay cybercriminals.

What security solutions would you say are the most effective to respond to ransomware?

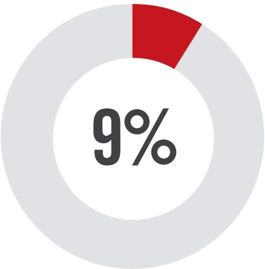


72%

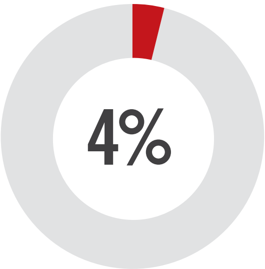
Data backup and recovery response



Threat intelligence



Behavioral analytics



Cyber insurance

ENDPOINT SECURITY

To stay ahead of evolving security threats, organizations employ a multi-layered security approach, including strong endpoint protection. When asked about the most effective endpoint security capabilities to protect against ransomware, most respondents agree that detecting and blocking traffic or executables at the first sign of malicious behavior (64%), and blocking ransomware attacks pre-execution (63%) rank as the most effective endpoint security capabilities.

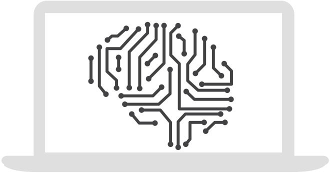
▶ What do you think is the most valuable endpoint security technology to have?

64%

Detect and block at the first sign of malicious behavior

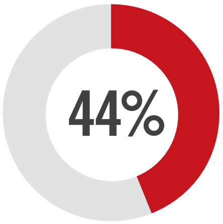
63%

Block ransomware and other at pre-execution to stem the spread

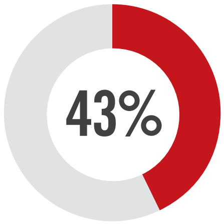


47%

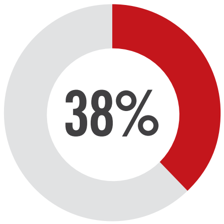
Non-signature based detection and prevention
(such as machine learning and behavior-based solutions)



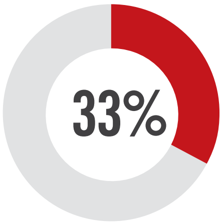
Advanced file analysis (i.e. nextgen antivirus tools)



Built-in web security preventing access to phishing, fraudulent or exploit-hosting sites



Fileless/exploit prevention through real-time behavior analysis



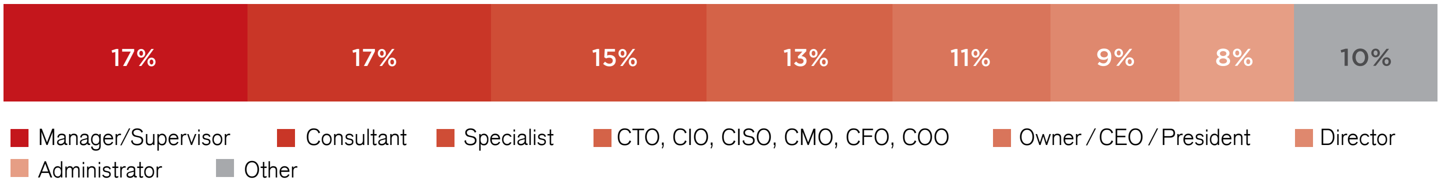
Endpoint integrated sandbox

Automatic mitigation including the ability to roll back changes 33% | File-based detection - signature-based traditional Antivirus 30% | Built-in anti-exploit 27% | Other 3%

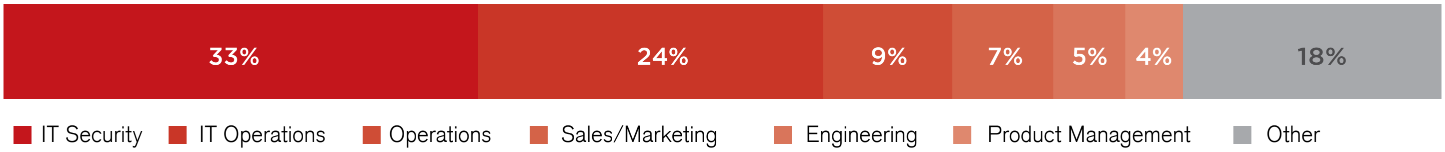
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of cybersecurity professionals to gain more insight into the latest trends, key challenges and solutions for Ransomware Security. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

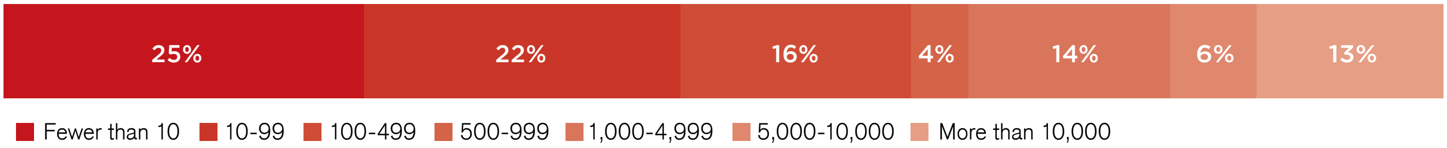
CAREER LEVEL



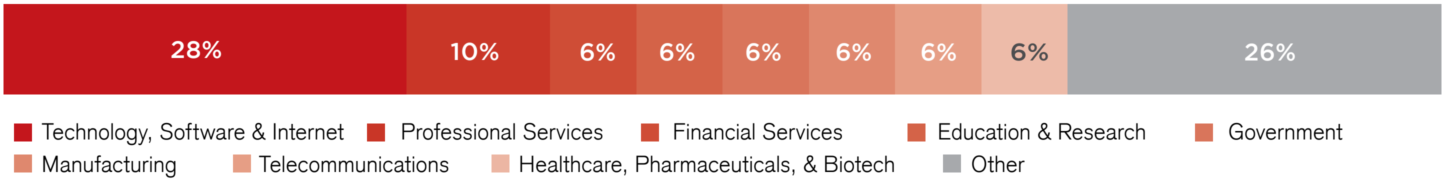
DEPARTMENT



COMPANY SIZE



INDUSTRY


Technology, Software & Internet
Professional Services
Financial Services
Education & Research
Government
Manufacturing
Telecommunications
Healthcare, Pharmaceuticals, & Biotech
Other