January 2024

Cybernomics 101

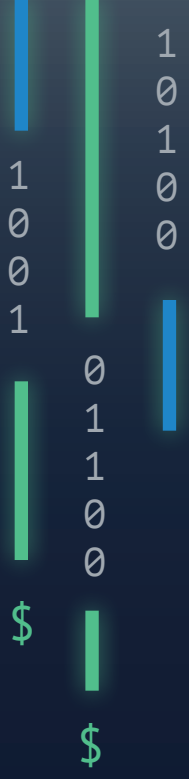
Uncovering the financial forces driving cyberattacks

Dissecting hackers' profit motives

Ponemon INSTITUTE

Barracuda
Your journey, secured.

Contents



Executive summary

It's understandable if IT security professionals feel overwhelmed, even helpless, in the face of the cyberattacks that strike organizations around the world every day. Their anxiety is not unfounded.

The Identity Theft Resource Center tracked 2,116 data compromises in the first three quarters of 2023, breaking the all-time high of 1,862 compromises in 2021. One recent victim, Medicaid and Medicare plan provider CareSource, faces multiple class action lawsuits over a recent data breach that exposed the sensitive health information of more than three million people. Progress Software notified CareSource about the vulnerability on May 31, 2023, and CareSource patched the flaw on June 1, 2023. That timeline is what's so scary — CareSource addressed the vulnerability in one day, but they were too late.

While it can be difficult to pin down the average short- and long-term costs of a data breach due to the variables of each case (e.g., company size, industry, extent of the breach), there's no question the consequences can be financially devastating.

Consider that the average annual cost for small and medium-sized enterprises (100 to 5,000 employees) to recover from IT asset damage, theft, and operational disruptions could exceed $5 million. That's one of the key takeaways of an international survey we commissioned Ponemon Institute to conduct in order to uncover the 'cybernomics' of today's security threat landscape.

This report presents our analysis of the survey's findings into the security challenges organizations worldwide face and the financial consequences following security compromises like ransomware and phishing attacks. Our overarching goal was to determine the answers to one question: How can organizations respond to the complexities of cybercrime when cybercriminals only need to be successful once?

We also peek into the minds of individuals who profit from exposing vulnerabilities. A significant segment of our respondents have extensive ethical hacking experience. While different than the cybercriminals organizations encounter and combat every day, ethical hackers can provide fascinating and helpful insights into the most common and effective attack types. They also issue a warning about criminals using generative AI technology to increase the volume and effectiveness of their attacks.

Our report breaks down a number of common factors that contribute to organizations' exposable security postures. These include significant IT security budget shortfalls, a general lack of consistent enterprise-wide security policies and programs, ineffective (or no) incident response plans, and an inability to protect against automated security attacks criminals create using generative AI technology.

Fortunately, there are positive takeaways. Our survey identified a subset of 'High Performers' that stand out for their robust security measures. This report identifies what they have done to effectively harden their security postures and provides Barracuda's expert recommendations on the steps any organization can take to do the same.

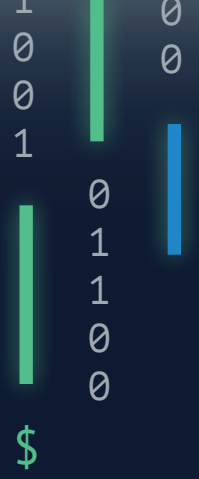
Methodology

Ponemon Institute surveyed a total of 1,917 IT security practitioners in the United States (522), the United Kingdom (372), France (329), Germany (425), and Australia (269) in September 2023. The final sample of respondents represented enterprises with a headcount between 100 and 5,000. All respondents are involved in the management of their organization's IT security functions or activities.

This report also references Barracuda-commissioned research published in 2023. Those two global surveys each included responses from 1,350 IT managers and technical IT professionals, senior IT security managers, and senior IT and IT security decision-makers from a broad range of industries.

Key findings

Here is a snapshot of the key findings and statistics outlined in greater detail throughout this report.



$5.34 mil

average annual cost to respond to compromises

$1.38 mil*

largest ransomware payment on average

**average total based on respondents sharing the amount of their largest ransomware payment*

6 vs. 427

hours for a technically proficient hacker to exploit a vulnerability vs. hours IT teams spent investigating, cleaning, fixing, and documenting successful phishing attacks over the last year

62%

stated cyberattacks are becoming more sophisticated

39%

believe their security infrastructure is adequately equipped to protect against GenAI-powered security attacks

Attack landscape

Cyberattacks are becoming more targeted, sophisticated, and severe

A majority (57%) of respondents reported their organizations suffered one or more cyberattacks in the past 12 months. Forty-eight percent said their organizations suffered a data breach in the past 12 months and lost, on average, 340,267 individual records. Viruses, other malware, and third-party mistakes were the primary root causes, underscoring the business imperative for investing in robust employee training programs that foster a culture of cybersecurity awareness and competence. Consider that phishing attacks generally require an employee to do something like click on a hyperlink or download an attachment. Well-trained, knowledgeable employees are much less likely to fall for an attacker's tricks.

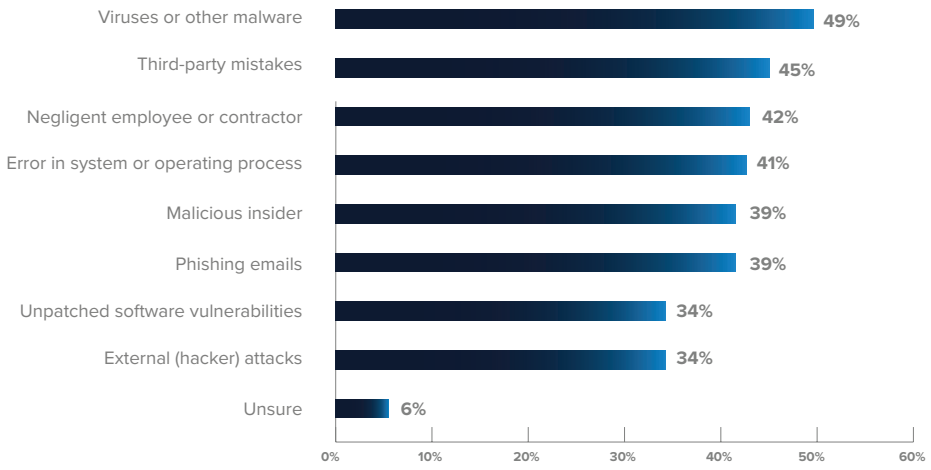


FIGURE 1

What were the root causes of the data breaches?

More than one response permitted

n=1,917

The majority of respondents said that attacks became increasingly targeted, sophisticated, and severe over the 12-month period between September 2022 to September 2023:

- 62% of respondents stated cyberattacks are becoming more sophisticated
- 55% said those attacks are becoming more severe in terms of an increase in the time it takes to investigate and attempt to mitigate the damage
- 53% of respondents agreed that cyberattacks are becoming more targeted

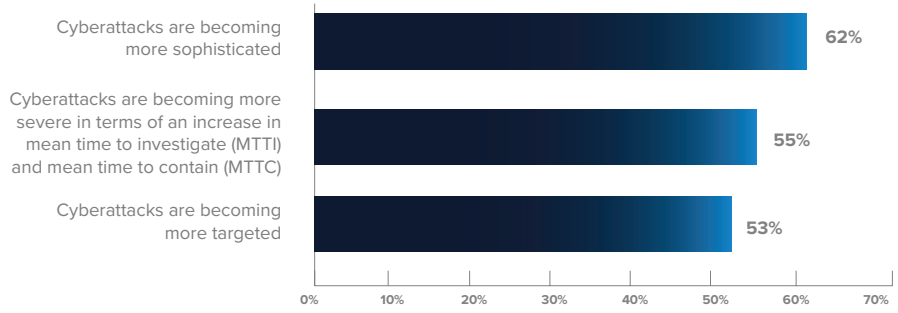


FIGURE 2

Cyberattacks are becoming more targeted, sophisticated, and more severe

Strongly agree and agree responses combined

n=1,917

Among the wide variety of attack types respondents say their organizations experienced, denial of service (52%), phishing/social engineering (48%), and credential theft (41%) ranked as the three most common. It's important to note that a malicious hacker can combine some or all of these types into one attack. For example, they may use phishing to access the credentials they need to breach the network and deploy malware within the system that enables them to steal data or lock users out of their systems and make a ransom demand.

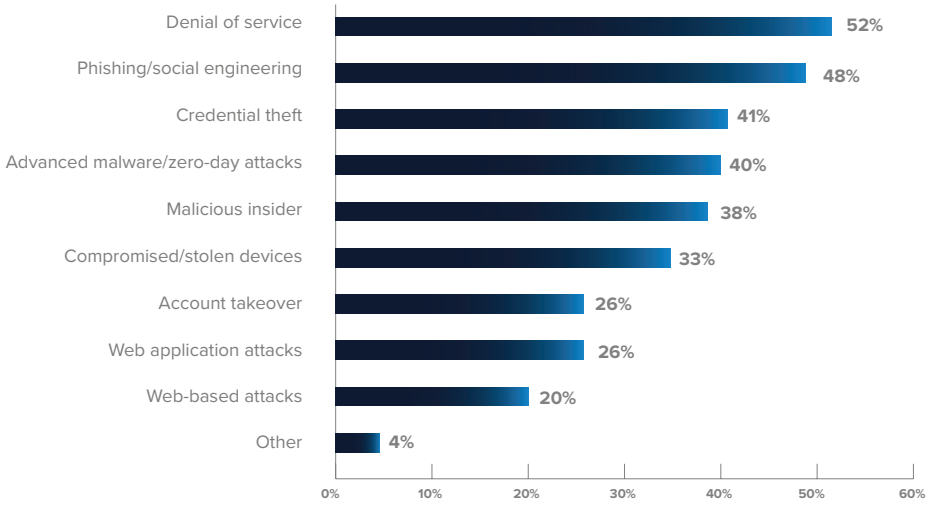


FIGURE 3

What best describes the type of attacks experienced by your enterprise?

More than one response permitted

n=1,917

Cybercriminals are winning the AI race

Cybercriminals run their operations like a business and are always striving to find ways to leverage technology to increase profitability. Increasingly, they're exploring how to use generative AI (GenAI) to increase the number and sophistication of their attacks, and their targets are woefully unprepared.

Forty-eight percent of respondents familiar with GenAI say its use will reduce the time it takes for a proficient hacker to exploit a vulnerability within an environment. Fifty percent of respondents expect the use of generative AI will increase the number of attacks a skilled hacker can launch in a single day.

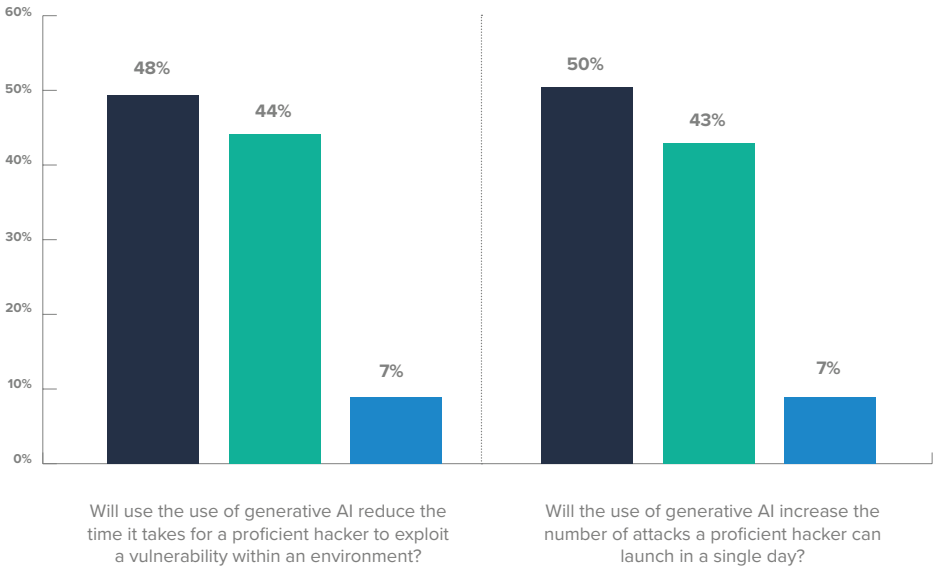


FIGURE 4

Generative AI benefits hackers

Yes
No
Unsure

n=1,917

Yet, alarmingly, while more than half (54%) of respondents say attackers' increased use of AI or GenAI will require new approaches to securing the organization, only 39% believe their security infrastructure is adequately equipped to protect against GenAI-powered security attacks.

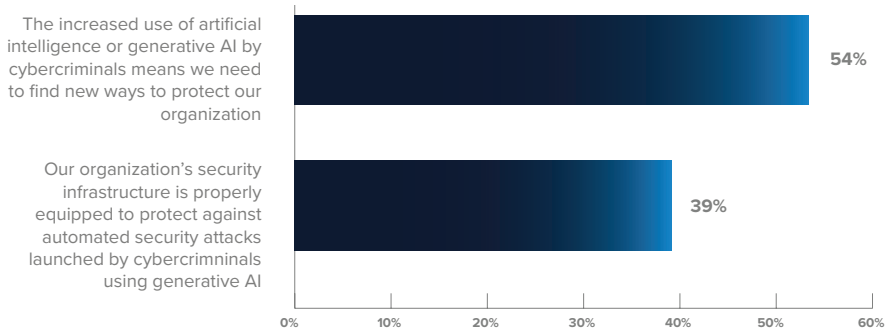


FIGURE 5

The impact of AI on security practices

Strongly agree and agree responses combined

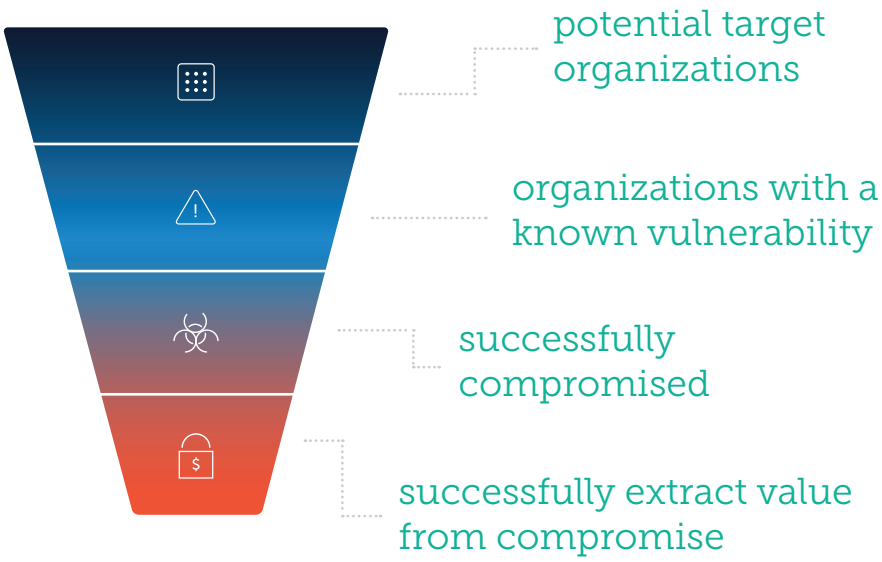
n=1,917

Cybernomics

The ‘cybernomic’ consequences

More than 20 years ago, hackers sought to achieve notoriety. They wanted to earn bragging rights about their successful attacks. Today, their operations more closely resemble legitimate enterprises driven by the universal business goal of maximizing profitability.

Understanding the “attack” funnel



Consider the traditional sales funnel model that maps the stages potential customers go through on their way to making a purchase. At the top of the funnel, the ‘Awareness’ stage captures potential customers’ attention through various marketing efforts. As these prospects move down the funnel, they enter the ‘Interest’ stage, where they start to show curiosity and seek more information. Following this is the ‘Desire’ stage, where interest

transforms into a consideration of purchase. The funnel narrows towards the 'Action' stage at the bottom, where the customer makes a purchase decision.

Hackers follow a similar path, but instead of beginning with researching products for potential purchase, they begin by discovering thousands of potential targets. Then they move down the funnel to identify those targets with vulnerabilities they can exploit, launch their attacks, and finally, reap their rewards. If they identify thousands of potential target organizations and only one cannot prevent their attack, they've achieved their "business goal."

Cyberattackers are businesspeople, and our survey reveals that business was good in 2023. We asked respondents, who represent a wide range of company sizes and industries from around the world, about the financial impact of security compromise, ransomware, and phishing attacks over the last year, including the costs from data, applications, and IT infrastructure compromises. We also asked them to consider associated costs like direct cash expenditures, labor costs, overheads, and lost business opportunities.

We learned the average cost associated with the damage or theft of IT assets and infrastructure and subsequent technical support, including forensic investigations, incident response activities, help desk and customer service operations, is $2.98 million.

The average cost of the disruption to normal operations, including revenue losses because of system downtime or other availability problems is $2.36 million. This accounts for the cost of users' idle time and lost productivity because of downtime or system performance delays.

Adding these costs together reveals the total average annual cost to respond to compromises is $5.34 million.

The cost of security compromises	Cost
The cost of damage or theft of IT assets and infrastructure over the past 12 months	$2,983,090
The cost of disruption to normal operations over the past 12 months	$2,357,795
Total	$5,340,885

Ransomware has become a global scourge. Seventy-one percent of respondents said their organizations experienced a ransomware attack over the last year, and 61% paid the ransom. The highest amount paid for a ransomware attack, on average, is $1.38 million.

Ninety-two percent said their organizations had an average of six credential compromises caused by phishing or other email-based threats over the past 12 months. The consequences of the phishing attacks were primarily the loss or theft of sensitive information or a lawsuit (17% of respondents).

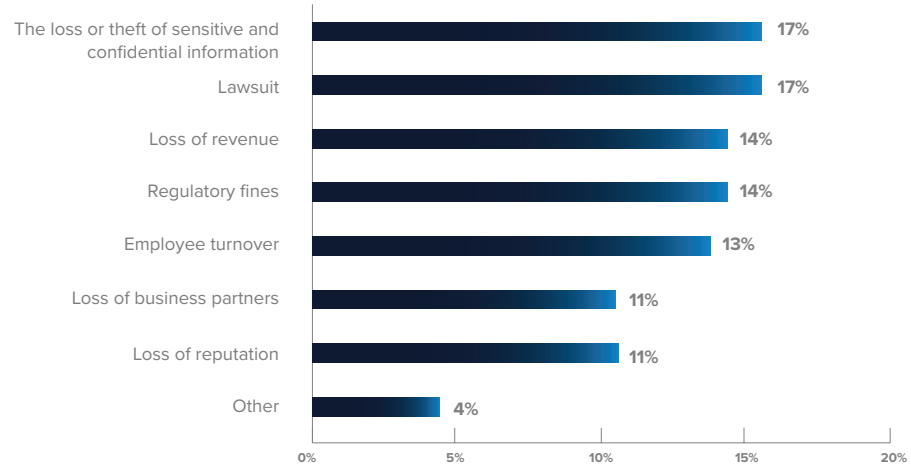


FIGURE 6

What were the consequences of the phishing attacks?

n=1,917

Just as damaging from a financial standpoint is the fact that each IT staff member assigned to remediation spent an average of 427 hours investigating, cleaning, fixing, and documenting the attacks. The cost of staff member time based on an hourly rate of $72.00 is an average of $30,744 per staff member, and an average total cost of $153,720 annually for the average team of five. If the organization outsourced the phishing response to a managed security service provider (MSSP), on average, the MSSP spent 504 hours to complete its work.

These findings are in line with other Barracuda research reports. According to our 2023 Email Security Trends report, 75% of the organizations we surveyed had fallen victim to at least one successful email attack in the previous 12 months at an average cost of about $1 million.

Our 2023 Spear-phishing Trends report reveals that organizations hit with a spear-phishing attack were more likely to say the costs associated with an email security breach had increased dramatically in the last year — 28% versus 15% of those who hadn't been victims of spear-phishing. These organizations are also more likely to have higher overall recovery and impact costs for the most expensive attack they suffer — an average of $1.1 million compared to $760,882 for those who were the victims of other types of email-based attacks.

Myriad technical and organizational challenges

Despite their realization of the dire nature of the threats they face every day, less than half (43%) of respondents described their ability to mitigate risks, vulnerabilities, and attacks across the enterprise as very or highly effective.

Among the reasons why the majority feel unprepared:

- Inadequate IT security budgets (55%)
- Inconsistent enterprise-wide security policies and programs (42%)
- Lack of inventory of third parties with access to sensitive and confidential data (38%)
- Poor or no visibility into the organization's networks and applications (37%)
- Difficulty securing the supply chain (32%)
- Lack of support from senior leadership:
  - » Management teams do not see cyberattacks as a significant risk (25%)
  - » Senior management does not receive regular updates about the many threats their organizations face (19%)

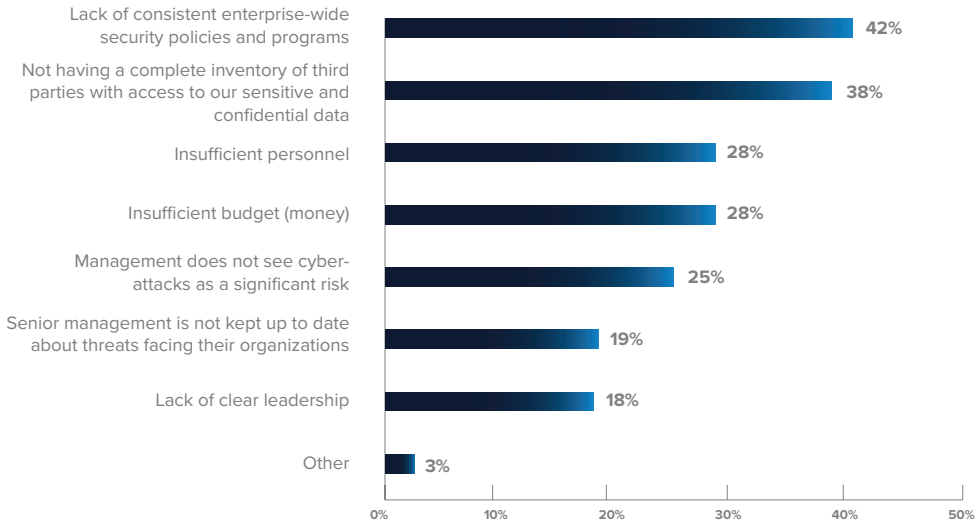


FIGURE 7

What governance challenges keep your organization's IT security posture from being fully effective?

Two responses permitted

n=1,917

Our survey also identified the lack of an incident response plan applied consistently across the entire enterprise as a common barrier to creating a strong security posture.

Incident response plans guide a security incident response team to manage the lifecycle of an incident from a tactical perspective to investigate and remediate incidents. While 90% of respondents said their organizations have a security incident response plan, only 50% say it is applied consistently across the enterprise. The other half said it is applied inconsistently, on an ad hoc basis, or not at all.

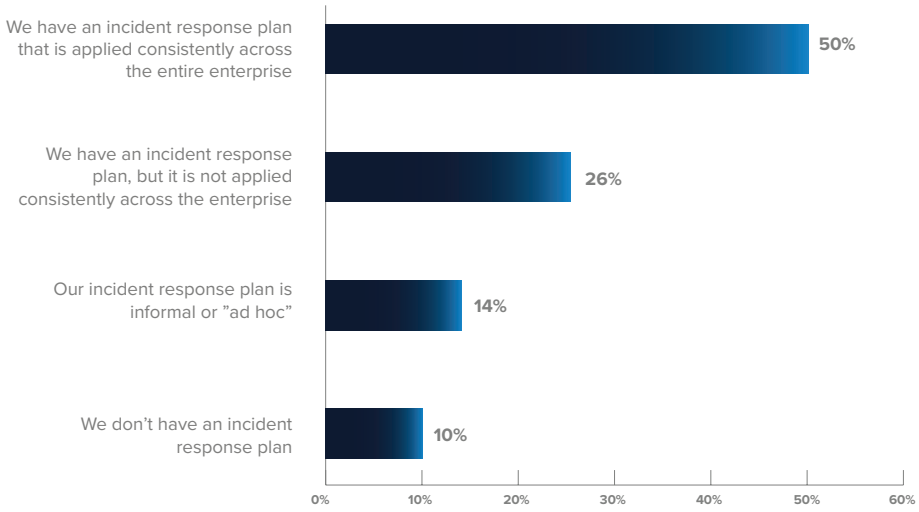


FIGURE 8

What best describes your organization's security incident response plan?

n=1,917

Additionally, among organizations with an incident response plan in place, the majority test it at most each quarter or twice a year, if at all.

Hackernomics

Survey respondents who identified as ethical hackers have an average of 10 years of experience helping their organizations assess where they are most vulnerable to a cyberattack. They use the same tactics, techniques, and strategies cybercriminals use to locate potential weaknesses and reinforce an organization's ability to recognize potential threat vectors. They identified weak authentication attacks (55%), phishing or spear phishing (48%), or exploitation of known vulnerabilities (45%) as key attack vectors.

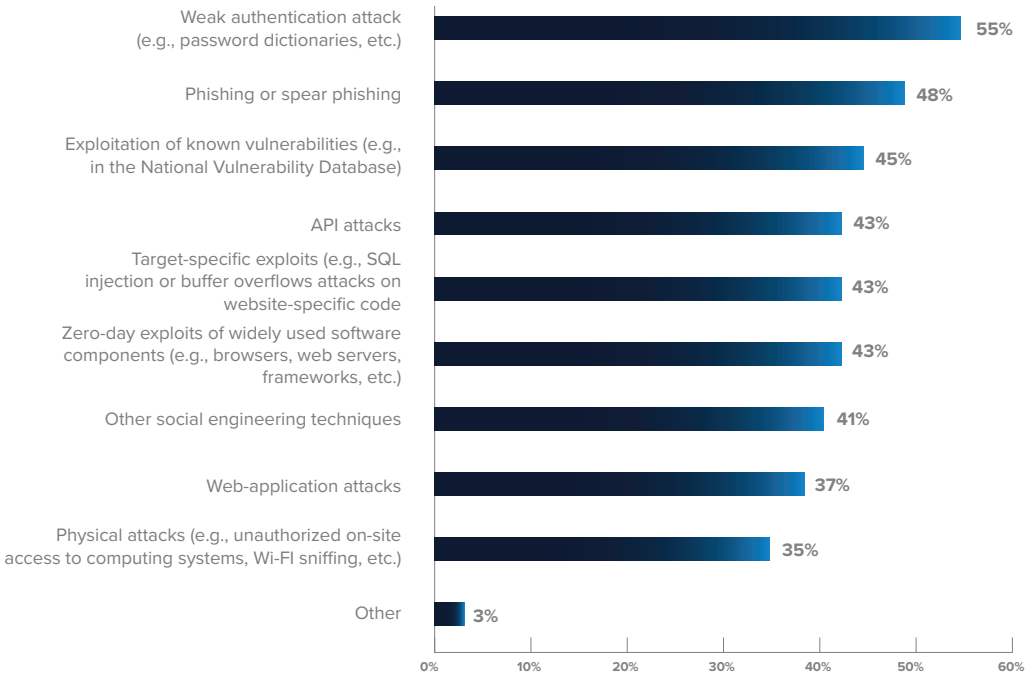


FIGURE 9

Which of the following attack vectors have you used as an ethical hacker?

More than one response permitted

n=1,917

Cybercriminals are not indiscriminate in their attacks. Before launching an attack, a malicious hacker will likely conduct research to identify vulnerabilities in organizations' IT environments they can exploit. After they discover those weak spots, they strike quickly.

On average, it takes a technically proficient hacker about six hours to exploit a vulnerability. In other words, it takes them less than a standard workday to launch an attack, slip past the target's security system, and expose or steal sensitive data.

Note that experience likely varies among our ethical hacker respondents. Some may have undertaken their work as part of their core job responsibilities and are working within technical environments they're familiar with — factors that may influence their determinations of a hacker's potential success rate.

Attackers are not limited to one target a day. On average, one hacker can launch 21 attacks a day.

The cybernomics of hacking	Hacker revenues
Average number of attacks in a day when the hacker decides to attack	21 attacks
Average success rate is 43 percent of the 21 attacks	9 successful attacks

Meanwhile, malicious hackers need to strike a balance between which types of attacks will be most successful and which attacks will be the best return on investment for their efforts. While weak authentication and phishing attacks are common vectors, they're not the most profitable. Our respondents identified target-specific exploits (58%), API attacks (55%), zero-day exploits of widely used software (52%), and weak authentication attacks (49%) as the most profitable attack vectors.

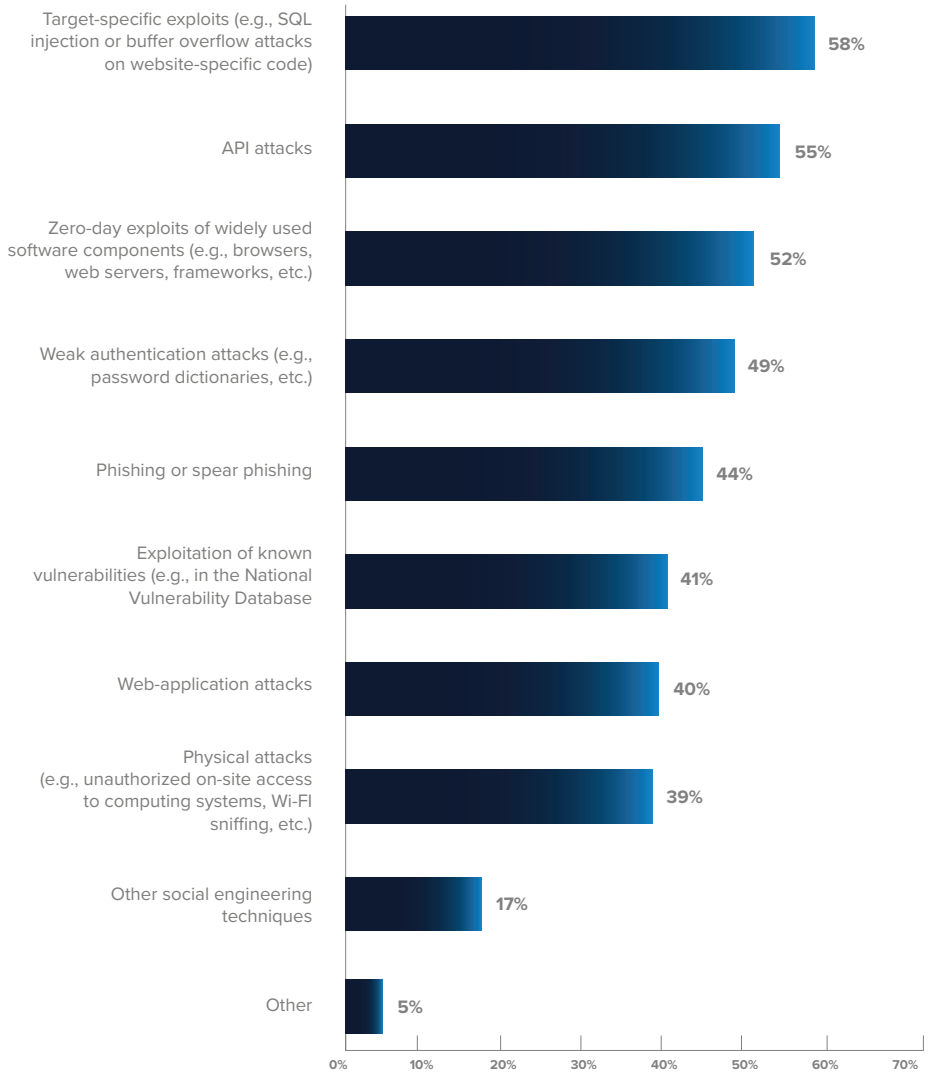


FIGURE 10

Where do hackers make the most money?

Four responses permitted

n=1,917

There are a number of other variables that factor into the profitability of an attack. Once a hacker breaches the network, did they exfiltrate valuable data or lock down the backup so recovery becomes impossible unless the victim pays a ransom? What industry is the victim in? Are they a small organization or a multinational enterprise? These are just a handful of the myriad factors that determine the damage an attacker can inflict after the initial exploit occurs.

Emulate the "high performers"

To this point, we've presented the reasons why the bad guys always seem to be several steps ahead of the security industry. Now, let's examine the segment of respondents with enterprises we classify as High Performers who the survey data reveals are best at mitigating risks, vulnerabilities, and attacks.

High Performer identification

Here's how we identified High Performers. Sixteen percent or 307 respondents from the international findings self-reported on a scale from 1 = not effective to 10 = highly effective that their enterprises are highly effective in creating a strong cybersecurity posture (9+ on the 10-point scale). We refer to the respondents who self-reported from 1 to 8 on the 10-point scale as "Other."

The High Performers' responses to the survey questions reveal they adhere to security practices and policies that all organizations should seek to emulate:

1) **Implement a security incident plan:** High Performers are far more likely to have a security incident plan that is applied consistently across the entire enterprise.

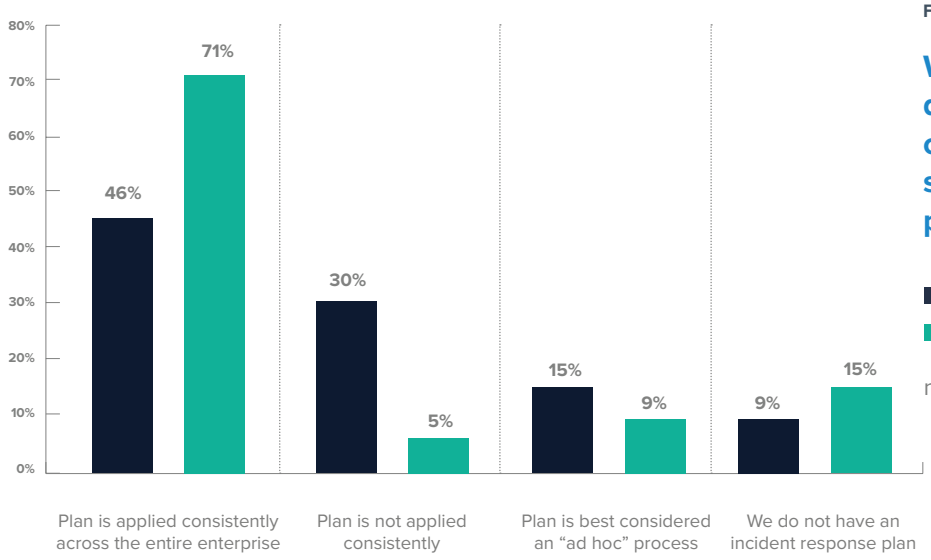


FIGURE 11

What best describes your organization's security incident plan?

Other
High Performers

n=1,917

2) Don't underestimate the threat: High Performers realize cyberattacks are more severe in terms of an increase in the mean time to investigate and contain. Sixty-five percent are more aware of the severity of cyberattacks in the past 12 months. Both groups see an increase in the sophistication of cybercriminals. More than half of the non-high performers (54%) are more likely to believe these attacks are more targeted.

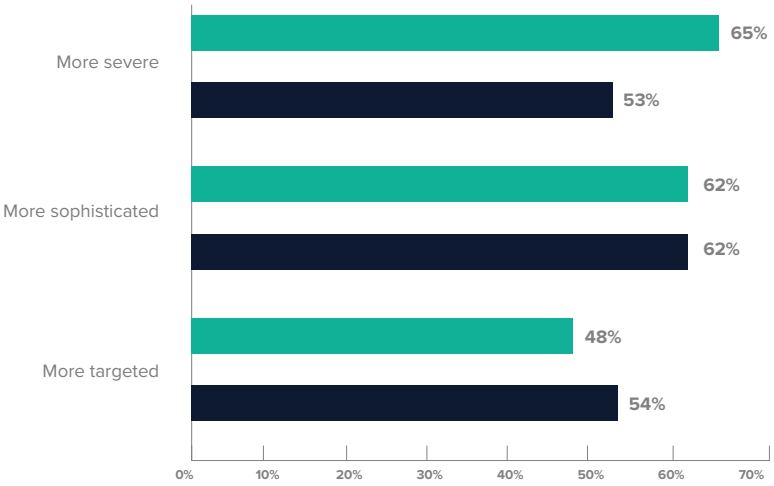


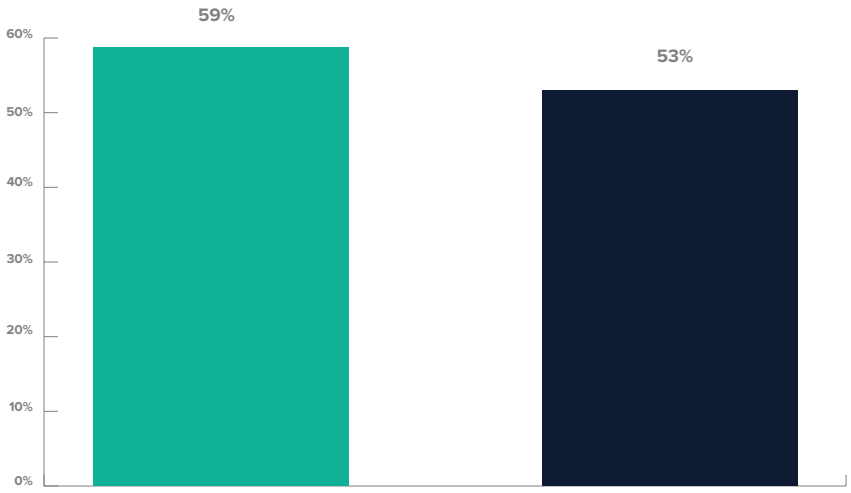
FIGURE 12

In the past 12 months, cyberattacks experienced by my enterprise are more targeted, sophisticated, and severe

Other
High Performers

n=1,917

3) Prepare for AI-generated attacks: Both High Performers and the non-high performer groups believe new ways are needed to minimize the risk from cybercriminals using AI or generative AI. Of those respondents who are familiar with generative AI, 59% of High Performers and 53% of other respondents agree that their enterprises need to be proactive in protecting their enterprises from cybercriminals' use of these technologies.



Strongly agree and agree responses combined

FIGURE 13

The increased use of artificial intelligence or generative AI by cybercriminals means we need to find new ways to protect our enterprise

Other
High Performers

n=1,917

High Performers are concerned that the use of generative AI will reduce the time it takes for a proficient hacker to exploit vulnerabilities. Fifty-nine percent of High Performers versus 46 percent of the non-high performers are concerned about how generative AI will make hackers more efficient. Additionally, more High Performers warn that the use of generative AI will increase the number of attacks that can be launched in a single day. Similar to the above, High Performers (71%) believe AI will enable hackers to launch more attacks.

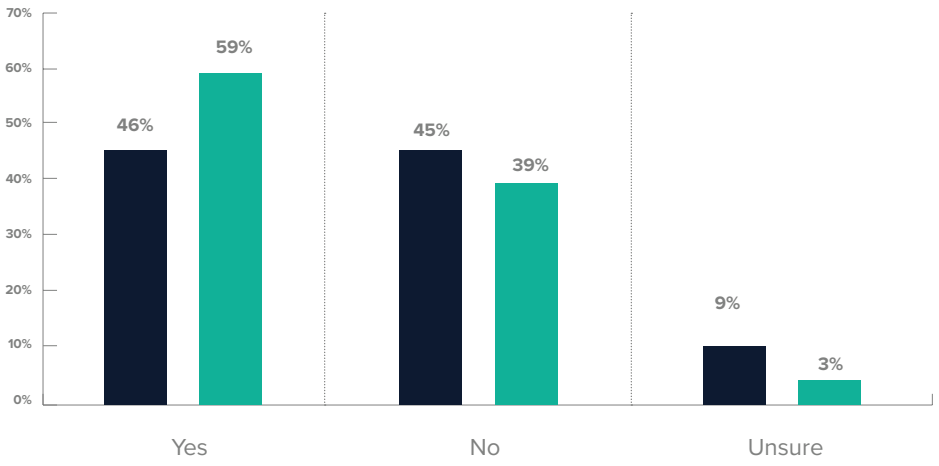


FIGURE 14

Will the use of generative AI reduce the time it takes for a proficient hacker to exploit a vulnerability within an environment?

Other
High Performers

n=1,917

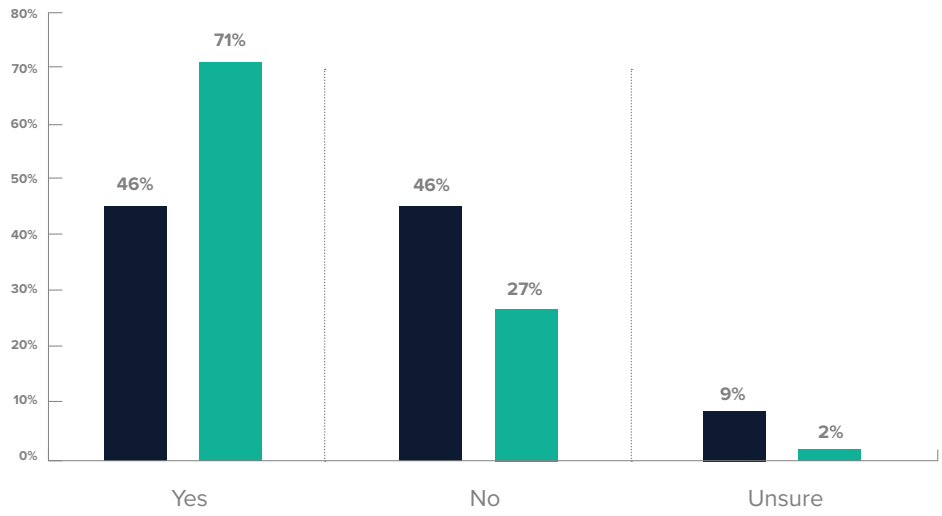


FIGURE 15

Will the use of generative AI increase the number of attacks a proficient hacker can launch in a single day?

Other
High Performers

n=1,917

4) Secure adequate budgets and resources: High Performers are more likely to believe they have the resources needed to achieve a strong IT security posture. Sixty-three percent of High Performers say they have an adequate budget to mitigate cyber risks and have a strong security posture compared to only 44% of their peers.

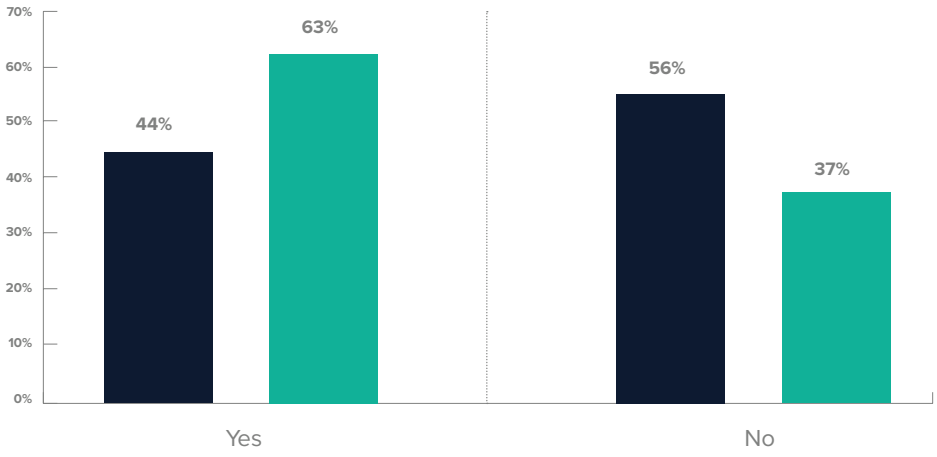


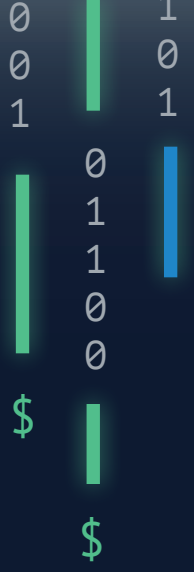
FIGURE 16

Is your enterprise's budget adequate for achieving a strong IT security posture?

Other
High Performers

n=1,917

Conclusion



Recommendations

The findings of our international cybernomics survey shed light on the escalating sophistication and economics of cyberattacks, the evolving tactics cybercriminals employ, and why so many organizations are unable to mitigate the risks. Several factors exacerbate this deficiency, including inadequate budgets, inconsistent security policies, and a lack of senior leadership support. As IT and security teams struggle with these technical, budgetary, and support challenges, cybercriminals are seizing the opportunity to generate enormous profits for themselves.

Turning the tide in this never-ending battle requires a paradigm shift in organizations and their security vendors' strategies to identify, contain, and recover from attacks

A need for a common language

A crucial aspect of this shift is establishing a common 'language' or protocol among vendors, enabling seamless communication and coordination in real time. Fostering a collaborative environment will enable vendors to significantly expedite the response to emerging threats and drastically reduce the window of opportunity for attackers.
The harmonization of threat intelligence and response protocols across vendors will facilitate a more robust defense mechanism, ensuring businesses are better poised to thwart the increasingly sophisticated and AI-augmented cyberthreats.

Take a platform approach

Because the ever-growing number of applications your organization uses may reside in the cloud, on premises, or in a hybrid environment (or all three), consider adopting a platform approach to security rather than relying on a collection of disparate individual security tools or solutions. This will ensure holistic security coverage across the organization's entire digital footprint, integrating various aspects like email, application, network, and endpoint security into a unified framework. Centralized management is a core feature, allowing for greater visibility and control over security operations from a single dashboard. This centralized system enhances the ability to swiftly detect and respond to threats, offering more proactive and intelligent threat management.

Moreover, the platform approach emphasizes seamless integration of different security components, ensuring that they work together efficiently and share information, which leads to stronger, more adaptive security responses. It enforces consistent application of security policies across all IT layers, minimizing the risk of gaps that could arise with disjointed tools. This approach is not only scalable (adapting to organizational growth and evolving threats), but also simplifies IT operations to potentially reduce costs and resource allocation complexities. By future-proofing against new technologies and threats, a platform approach offers a robust, dynamic solution to the challenges of modern cybersecurity.

Maintain a vigilant culture

Cultivating a well-informed and vigilant organizational culture is also paramount. The data in our report underscores why businesses must invest in comprehensive employee training programs that nurture a culture of cybersecurity awareness and competence. This requires a collaborative effort across the enterprise, including at the C-suite and board levels, to integrate advanced security technologies and foster a culture of continuous learning and adaptation to the evolving threat landscape. A well-informed workforce serves as the first line of defense against both external threats and internal vulnerabilities.

Get data access policies right

Furthermore, our findings highlight the need to establish stringent data access policies. Embracing a model of privileged access rights ensures that sensitive data remains accessible only to those individuals with the requisite authorization, significantly mitigating the risk of internal data breaches. Adherence to rigorous data compliance and storage standards is another crucial measure that safeguards against a spectrum of internal and external threats.

Have a plan and be ready

It's also important to emphasize the importance of implementing and regularly testing an enterprise-wide incident response plan that guides a security incident response team to manage the lifecycle of an incident from a tactical perspective to investigate and remediate incidents. While 90% of our respondents say their organizations have a security incident response plan, only 50% of that group say it is applied consistently across the enterprise. The other half admit it is applied inconsistently, on an ad hoc basis, or it doesn't exist.

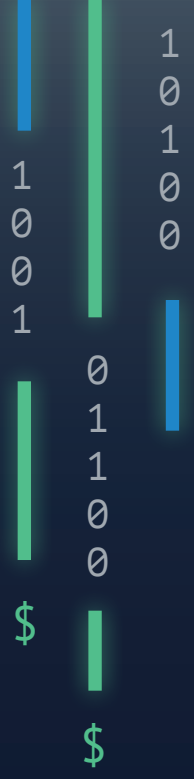
Keep it simple

Scaling back the number of security vendors an organization relies on is another step toward improving an organization's security posture and reducing cybersecurity costs.

Consider that, on average, the organizations we surveyed have 30 cybersecurity vendors. Thirty-nine percent of respondents plan to consolidate and reduce the number of vendors over the next two years.

This may be difficult to hear, but it's critical to understand and accept: It's inevitable your organization will be hit by an attack that results in a data breach. But that doesn't mean your hands are tied. Becoming more proactive in monitoring for and detecting attacks so they don't progress to the data exfiltration/ransomware stage will mitigate the damage, speed recovery, and avoid paying a ransom demand. Preparing for the inevitable will significantly reduce the short- and long-term costs of responding after the fact.

As cybercriminals refine their tactics, the onus is on organizations to bolster their security infrastructure and governance practices. Only through a holistic, well-funded, and well-supported cybersecurity strategy can they hope to mitigate the risks and shield themselves from the burgeoning financial and operational repercussions of cyberattacks.



About Barracuda

At Barracuda, we strive to make the world a safer place. We believe every business deserves access to cloud-first, enterprise grade security solutions that are easy to buy, deploy and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey. More than 200,000 organizations worldwide trust Barracuda to protect them — in ways they may not even know they are at risk — so they can focus on taking their business to the next level.

Get more information at barracuda.com.

Appendix

International Data Tables

Security posture

How would you describe your organization's IT security posture in terms of its effectiveness at mitigating risks, vulnerabilities and attacks across the enterprise on a scale from 1 = not effective to 10 = very effective?	US	UK	FR	DE	AU	Global
1 or 2	9%	12%	18%	15%	17%	14%
3 or 4	18%	20%	23%	19%	21%	20%
5 or 6	22%	26%	23%	21%	17%	22%
7 or 8	31%	24%	21%	34%	27%	27%
9 or 10	20%	18%	15%	11%	18%	16%
Total	100%	100%	100%	100%	100%	100%

What types of information if lost or stolen would have the greatest financial and operational impact on your organization? Please select the top two choices.	US	UK	FR	DE	AU	Global
Customer credit or debit card information	26%	25%	31%	26%	25%	27%
Financial information	45%	43%	50%	35%	46%	44%
Intellectual property	36%	23%	17%	19%	27%	24%
Customers' personally identifiable information	34%	43%	26%	46%	33%	36%
Employee records	31%	35%	42%	39%	38%	37%
E-mails, chat apps logs, text messages	23%	31%	34%	32%	29%	30%
Other (please specify)	5%	0%	0%	3%	2%	2%
Total	200%	200%	200%	200%	200%	200%

Security technologies

Which technologies has your organization implemented to mitigate cybersecurity risks?	US	UK	FR	DE	AU	Global
Anti-virus/anti-malware	56%	48%	44%	59%	45%	50%
Artificial intelligence/Machine learning	53%	39%	33%	62%	41%	46%
Cloud security posture management	51%	49%	42%	49%	53%	49%
Data loss prevention	65%	58%	46%	59%	50%	56%
Email security gateway	67%	69%	58%	69%	54%	63%
Encryption for data at rest	69%	64%	61%	75%	71%	68%
Encryption for data in transit	75%	67%	68%	76%	63%	70%
EDR	45%	43%	41%	35%	40%	41%
Identity & access management	69%	65%	49%	69%	51%	61%
Identity threat detection & response (ITDR)	55%	41%	56%	34%	50%	47%
Intrusion detection & prevention systems (IDPS)	73%	68%	62%	70%	60%	67%
Managed detection & response (MDR)	39%	44%	41%	36%	39%	40%
Mobile device management (MDM)	36%	35%	31%	28%	32%	32%
Multi-factor authentication	71%	67%	58%	67%	59%	64%
Network firewall	70%	64%	67%	69%	62%	66%
Network monitoring tools	34%	36%	40%	31%	23%	33%
Network traffic analysis	49%	45%	50%	39%	43%	45%
Patch & vulnerability management	60%	54%	48%	54%	52%	54%
Privileged access management	54%	46%	39%	48%	37%	45%
Secure Access Service Edge (SASE)	49%	39%	27%	34%	25%	35%
Secure web gateway	34%	37%	31%	29%	34%	33%
SIEM	64%	58%	37%	53%	39%	50%
Web application firewall (WAF)/ Web application & API protection (WAAP)	59%	43%	43%	41%	39%	45%
XDR	36%	39%	42%	45%	41%	41%
Zero Trust Network Access (ZTNA)	61%	52%	49%	53%	50%	53%

Does your organization have a data breach or cyber insurance policy?	US	UK	FR	DE	AU	Global
Yes	51%	44%	39%	52%	42%	45%
No, but we plan to purchase a policy in the next 12 months	22%	23%	33%	25%	26%	30%
No, we do not plan to purchase a policy	27%	33%	28%	23%	32%	25%
Total	100%	100%	100%	100%	100%	100%

Budget and costs

What is your organization's total IT budget in 2023?	US	UK	FR	DE	AU	Global
Less than $500,000	0%	2%	6%	1%	4%	3%
$500,000 to $1,000,000	5%	13%	15%	5%	8%	9%
$1,000,001 to $5,000,000	9%	17%	15%	13%	13%	13%
$5,000,001 to $10,000,000	16%	26%	24%	23%	33%	24%
$10,000,001 to $25,000,000	23%	21%	25%	29%	24%	24%
$25,000,001 to $50,000,000	29%	15%	12%	18%	15%	18%
More than $50,000,000	18%	6%	3%	11%	3%	8%
Total	100%	100%	100%	100%	100%	100%
Extrapolated average	$27,207,500	$15,467,500	$13,067,500	$20,582,500	$14,570,000	$18,179,000

What percentage of your organization's IT budget is dedicated to IT security activities?	US	UK	FR	DE	AU	Global
Less 5%	0%	4%	3%	2%	3%	2%
5 to 10%	6%	9%	6%	2%	5%	6%
11 to 15%	8%	9%	10%	6%	8%	8%
16 to 20%	11%	21%	9%	11%	12%	13%
21 to 25%	16%	13%	12%	21%	15%	15%
26 to 30%	18%	20%	17%	15%	18%	18%
31 to 40%	20%	10%	21%	22%	25%	20%
41 to 50%	14%	8%	14%	16%	11%	13%
More than 50%	7%	6%	8%	5%	3%	6%
Total	100%	100%	100%	100%	100%	100%
Extrapolated average	30%	25%	29%	30%	28%	28%