Deloitte. Insights

Cybersecurity threats and incidents differ by region

How 20 countries and three global regions compare across key cyber threat considerations

ARTICLE • 10-MIN READ • Deloitte Center for Integrated Research

Cyber threats are pervasive and increasingly sophisticated. When successful, they can compromise data, disrupt operations, and damage an organization's reputation. Today's security and business leaders face an exponential growth in threats in parallel with the challenges of evaluating the best solutions to counter these threats, all while compliance requirements continue to evolve. The complexities don't stop there.

As per the results of our 2023 Global Future of Cyber Survey, these challenges appear to differ by country and region (Americas, EMEA and APAC). Each region has a varying cyber maturity and risk profile, alongside disparate regulatory requirements. Given this variability, how can global organizations best assess their cybersecurity investments and the value gained from them? In addition, how can they assess and prioritize the top threat actors in a specific region and identify cyber incident patterns to help mitigate their impact?

This analysis, based on 1,110 anonymous respondents to a survey covering 20 countries (see, “Methodology”), assesses global cybersecurity threat trends that equip leaders with data to help them tailor cyber strategies based on regional and/or country benchmarks. The analysis highlights the regions and countries that are reporting the greatest cyber incidents, threats that are most prevalent, what impacts are experienced most by each region, and where organizations are seeing the most cyber investment value. We combined this information to help organizations better inform a global cyber strategy as well as provide recommended steps companies can take (by region) to help shore up cybersecurity weaknesses.

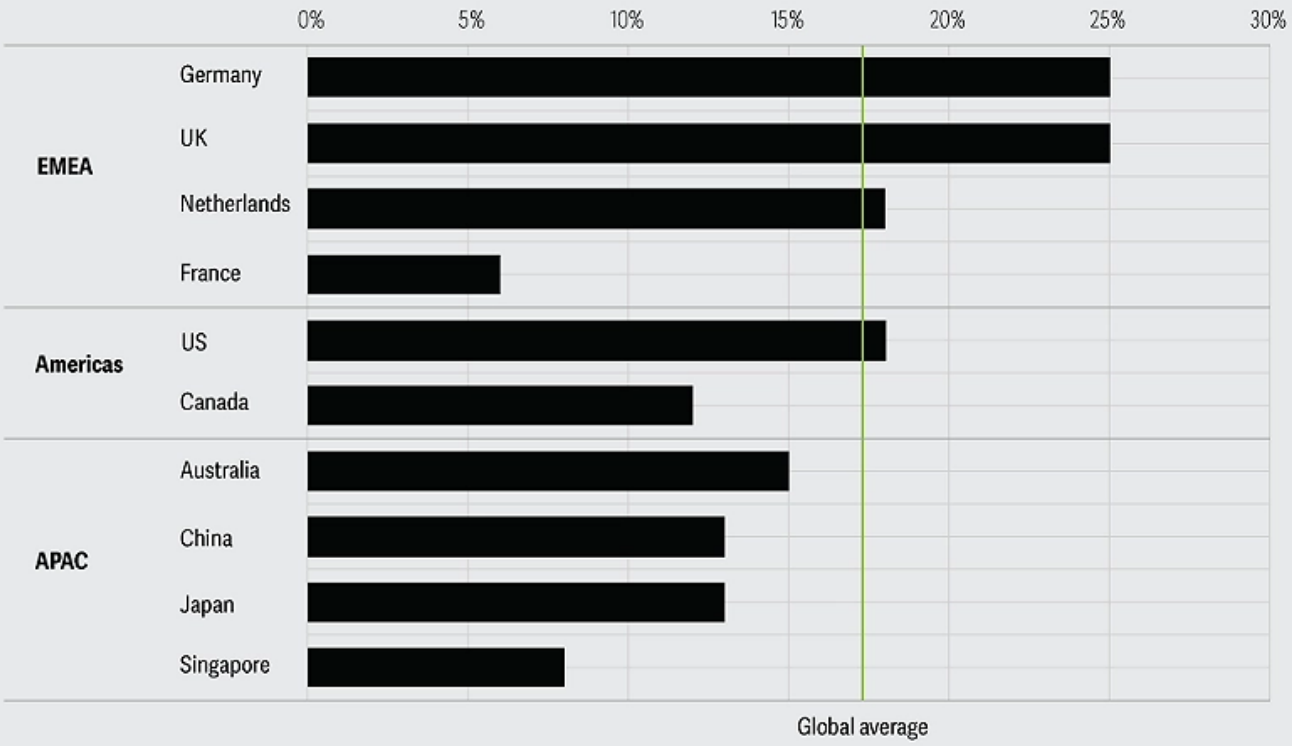
EMEA noted the most cyber incidents, while APAC saw the fewest

Despite some of the most stringent security and privacy requirements, our survey showed that organizations within EMEA experienced the highest number of cyber incidents.

Figure 1

Germany and the UK saw the highest number of cyber incidents on average

In the last year, how many significant cybersecurity incidents has your organization experienced?



Note: i) The total number of respondents is 1,110, surveyed across 20 countries, however, this figure depicts only 10 key countries that had a statistically significant sample size and a reasonably representative industry sample; ii) Percentages in the figure reflect only those respondents who selected the responses, "11-15 events" and "16 or above" in the survey; iii) Percentages are calculated based on the individual country totals and not the overall total. For country totals, refer to: Australia (n=81), Canada (n=100), China (n=40), France (n=51), Germany (n=61), Japan (n=40), Netherlands (n=50), Singapore (n=50), the UK (n=100), the US (n=202). For more details, see methodology.
Source: Deloitte Center for Integrated Research.

Deloitte. Insights | deloitte.com/insights

In the last year, our survey indicated that organizations in EMEA experienced the highest number of cyber incidents, with 20% of respondents experiencing 11 or more incidents in a year. Germany and the United Kingdom topped the list (both at 25%) with Germany reporting the highest number of malware incidents in 2021 – Germany's Federal Office for Information Security (BSI) detected 553,000 malware variants in a single day in February 2021. At the time, BSI[1] raised the threat level from "tense" to "tense-to-critical," indicating the need for organizations to be on high alert. An outlier within EMEA was France; they reported fewer significant incidents than the EMEA region *and* global overall respondents.

APAC trended better than the average, in part driven by Singapore, which had the least number of significant cyber incidents (8%) in the APAC region. Australia (15%), Japan (13%) and China (13%), had a higher number of significant cyber incidents. Importantly, fewer known incidents does not necessarily mean an organization experiences fewer incidents overall. Organizations may be experiencing cyber incidents that they are unaware of given the maturity of their threat detection capabilities.

Respondents from the Americas reported cyber incidents at par with the global average, with the US slightly more likely to report a high number of incidents than Canadian organizations by six percentage points.

Criminal threats are of deepest concern

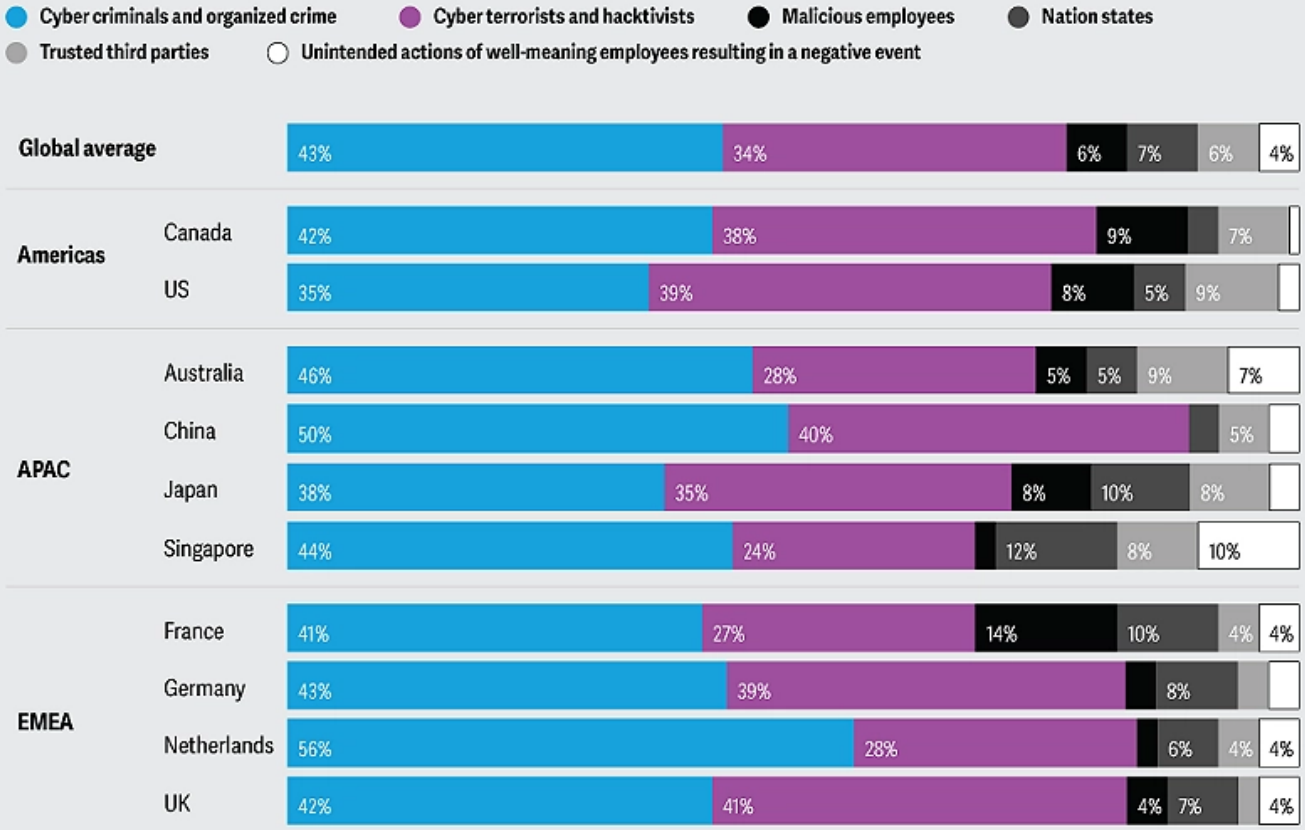
When given six potential threat actors to choose from, nearly 40% of respondents across all three regions reported that cybercrime (cyber criminals and organized crime) was the greatest concern. This data illustrates the all-pervasive nature of cybercrime, which was reported as having an especially high level of concern in the Netherlands (56%) and China (50%).

The second leading threat actor concerning organizations were cyber terrorists and hacktivists (34%), led by the UK (41%) and China (40%). China seems especially vulnerable potentially due to a proliferating digital and e-commerce ecosystem in the country.[2]

Figure 2

Cyber criminals, cyber terrorists, and hacktivists dominate global concerns

What bad actor or threat source is the single biggest cybersecurity threat facing your organization?



Note: i) The total number of respondents is 1,110, surveyed across 20 countries, however, this figure depicts only 10 key countries that had a statistically significant sample size and a reasonably representative industry sample; ii) Percentages are calculated based on the individual country totals and not the overall total. For country totals, refer to: Australia (n=81), Canada (n=100), China (n=40), France (n=51), Germany (n=61), Japan (n=40), Netherlands (n=50), Singapore (n=50), the UK (n=100), the US (n=202). For more details, see methodology.
Source: Deloitte Center for Integrated Research.

Deloitte. Insights | deloitte.com/insights

Overall, APAC organizations were most concerned with nation-state and trusted third-party threats, led by Singapore at 12% for nation states (5% above the global average) and Australia at 9% for trusted third parties (3% higher than the average). As organizations look to combat these threat actors, a multifaceted third-party risk program can help remediate security concerns before they develop into breaches.

With regard to France specifically, our data indicates an above-average concern with malicious employees (8% higher than the global average). This may be due to the study's high representation of respondents from the financial services industry in

France (24% in France vs. 17% globally), a sector recorded as susceptible to insider attacks.[3]

Conversely, the concerns related to malicious employees in the Americas, led by Canada at 9%, may have different causes. We see that disgruntled employees seeking to compromise sensitive company data is one of the key drivers of insider attacks. In 2020, Canada witnessed a high number of layoffs[4] that could have incited agitated employees to act out against their former employers.[5]

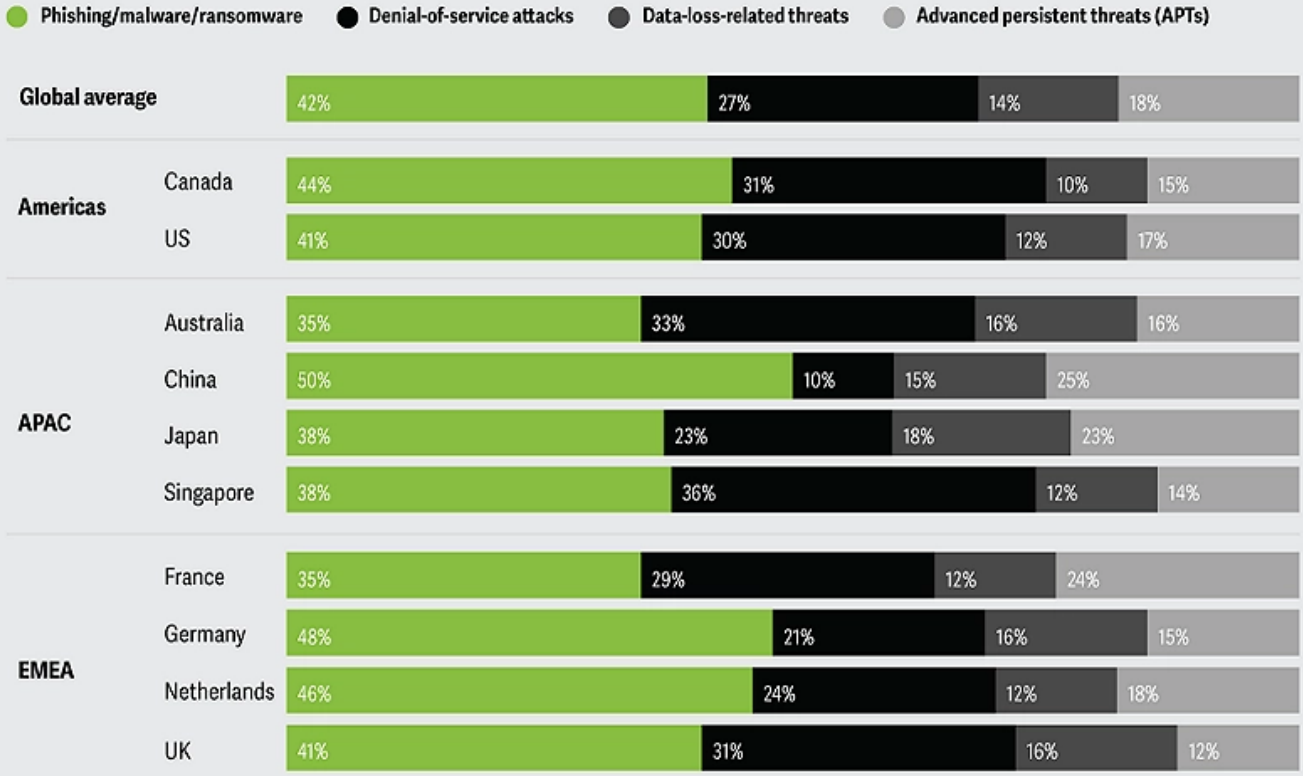
All three regions are concerned with 'phishing, malware, and ransomware'

'Phishing, malware, and ransomware' incidents were the most prevalent threats/tools/techniques (TTT) across every region, with China at 50%, leading by 8%, followed by Germany at 48%. These countries' high concern here relates directly to the high number of incidents mentioned earlier (figure 1) and a 60% spike in ransomware incidents reported as of March 2023.[6] Organizations in China and Germany, more than others, should focus on educational programs related to social engineering, as well as malware detection software and capabilities that would minimize the risk of ransomware attacks.

Figure 3

Concern for phishing, malware, and ransomware is the highest globally

What threats, tools, or techniques represent the single biggest cybersecurity threat to your organization?



Note: i) The total number of respondents is 1,110, surveyed across 20 countries, however, this figure depicts only 10 key countries that had a statistically significant sample size and a reasonably representative industry sample; ii) Percentages are calculated based on the individual country totals and not the overall total. For country totals, refer to: Australia (n=81), Canada (n=100), China (n=40), France (n=51), Germany (n=61), Japan (n=40), Netherlands (n=50), Singapore (n=50), the UK (n=100), the US (n=202). For more details, see methodology.
Source: Deloitte Center for Integrated Research.

Deloitte. Insights | deloitte.com/insights

Denial of Service (DDoS) attacks—which prevent users from accessing systems, networks, or platforms—were reported as the next most prevalent across all geographies. Singapore (36%) and Australia (33%) showed the most concern, reporting record-breaking incidents in 2023.[7] Organizations should minimize potential points of entry to reduce the attack surface area, plan for scaling up their network to handle large volumes of traffic, and deploy experienced support to differentiate between legitimate and illegitimate traffic patterns.[8]

Advanced persistent threats (APTs)—where a well-resourced adversary engages in sophisticated malicious cyber activity—were an above average concern in France at 24% (six percentage points higher than average).

Similarly, Japan saw APTs as a greater concern than other countries at 23% (five percentage points higher than other countries).

Operational impacts affected all regions.

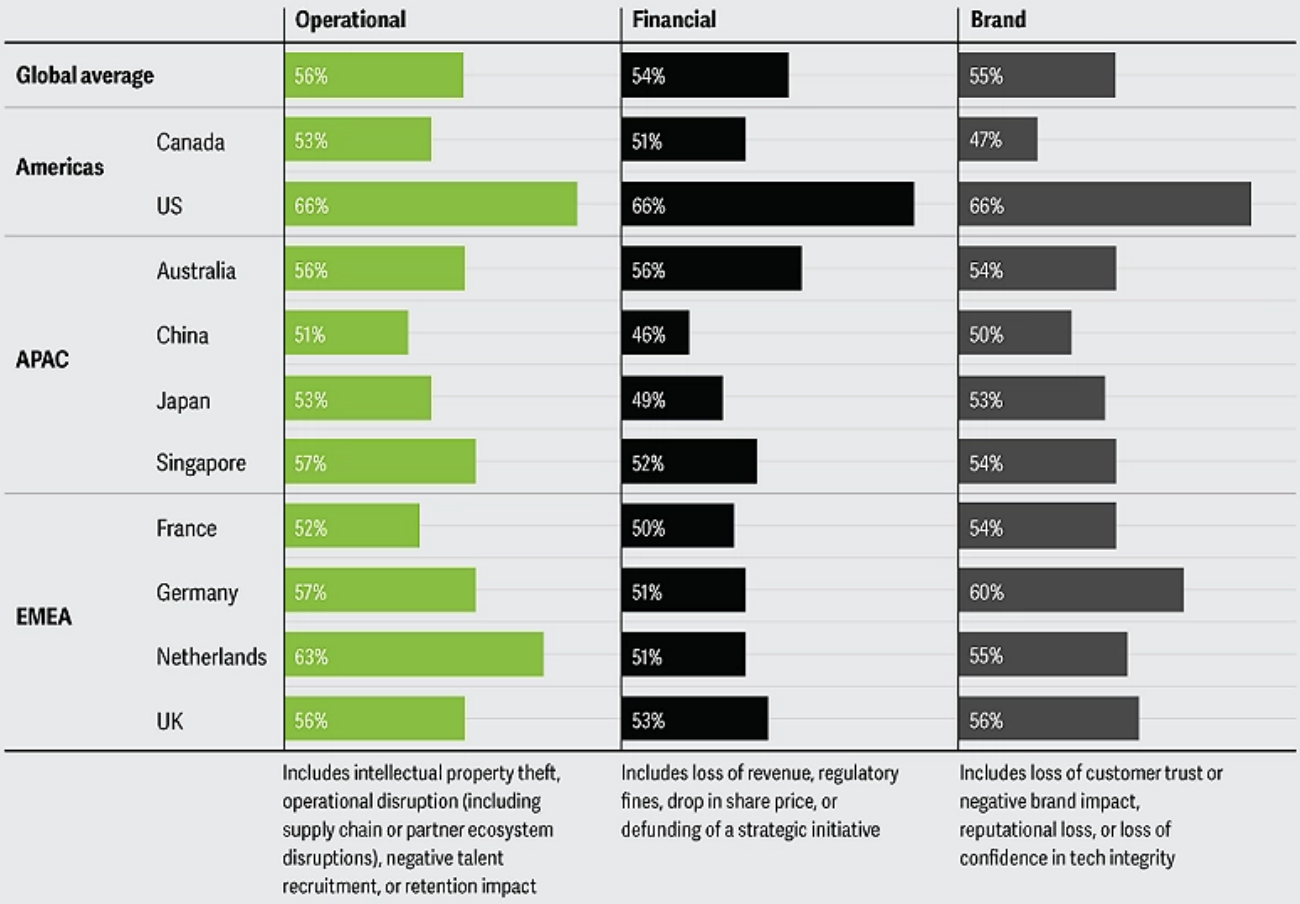
While cyber incidents can lead to a number of potential impacts, our data suggests that financial loss, operational disruption, and brand damage were most concerning for survey respondents (figure 4).

Of note, all three regions reported they are impacted most by operational disruption (56% overall). Brand damage ranked second, driven most by "loss of customer trust or negative brand impact." Financial impacts, while not insignificant, were reportedly suffered the least across all regions (54%), with the exception being the US, Australia, and the UK.

Figure 4

Operational consequences caused the most severe impact

How much has your organization suffered negative consequences to a "moderate" or "large" extent in each of these areas due to cybersecurity incidents?



Note: i) The total number of respondents is 1,110, surveyed across 20 countries, however, this figure depicts only 10 key countries that had a statistically significant sample size and a reasonably representative industry sample; ii) Percentages in the figure reflect only those respondents who selected the responses, 'to a moderate extent' and 'to a large extent' in the survey ; iii) Percentages are calculated based on the individual country totals and not the overall total. For country totals, refer to: Australia (n=81), Canada (n=100), China (n=40), France (n=51), Germany (n=61), Japan (n=40), Netherlands (n=50), Singapore (n=50), the UK (n=100), the US (n=202). For more details, see methodology.
Source: Deloitte Center for Integrated Research.

Deloitte. Insights | deloitte.com/insights

The Americas reported the highest negative impact across all three categories—operational disruption, brand damage, and financial impact—led by the US (66%). EMEA, on the other hand, suffered a lower-than-average impact from financial consequences, almost at par with the overall average for operational and brand consequences, led by the Netherlands (63%) and Germany (60%).

Given that our earlier analysis (figure 1) found that the US and EMEA had an average-to-high number of cyber incidents, it is possible that respondents are not fully accounting for all three categories of negative consequences. We conducted additional analysis to examine the negative consequences experienced by the organizations with the highest number of cyber incidents (16+) and found that these organizations (74%) ranked “loss of revenue” and “IP theft” equally as their top negative consequence.

Big incidents have multi-dimensional, negative impacts that can be bigger than organizations know

In October 2022, **a ransomware incident[9] in Anhalt-Bitterfeld, Germany,** forced the regional authority to declare a state of disaster, shut citizen-related services for 200+ days, and declare it the country's first “cyber catastrophe.”

Translating insights to action: Driving more value from cyber investments

The findings above can help organizations better target cybersecurity investments. Greater threat intelligence[10] is the cornerstone of a robust cybersecurity process. However, global organizations have difficulty assessing the right "spend vs. value" ratio. Keeping regional observations in mind, organizations can assess and recalibrate their cyber strategies, spend, and capabilities to drive greater resilience and trust, and protect and preserve long-term value.

Guide your threat response based on unique regional pain points

Organizations with a high number of cyber incidents and the pervasive threat of these incidents aren’t exactly ahead of the game, but heightened awareness is a solid

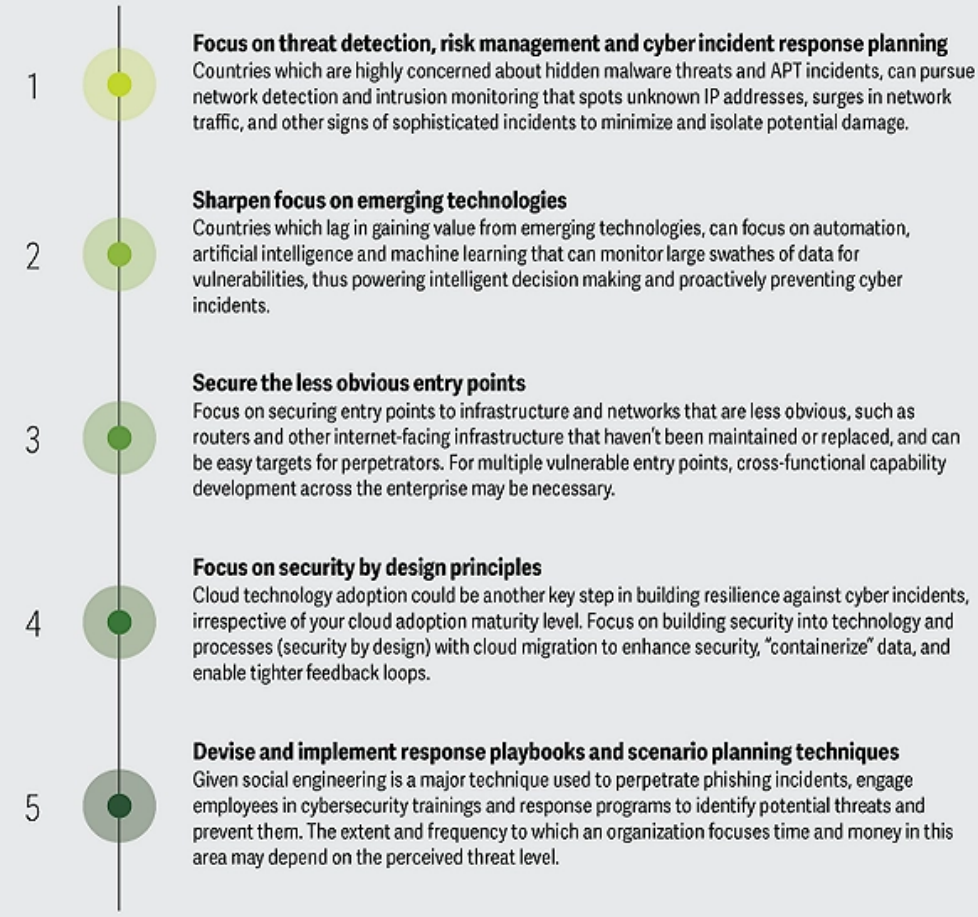
foundation on which to create strategic, innovative, and *targeted* cyber strategies that improve resilience and enable digital trust.

Below we discuss some tailored strategies that can help guide your cybersecurity efforts. While ideally a holistic cyber incident and response program would encompass all these strategies, given each region's most pervasive challenges, these actions line up with their incident profile, based on our data (figure 5).

Figure 5

Create targeted cyber strategies to guide threat response

Priority actions to guide your regional cyber strategy



Source: Deloitte Center for Integrated Research.

Deloitte. Insights | deloitte.com/insights

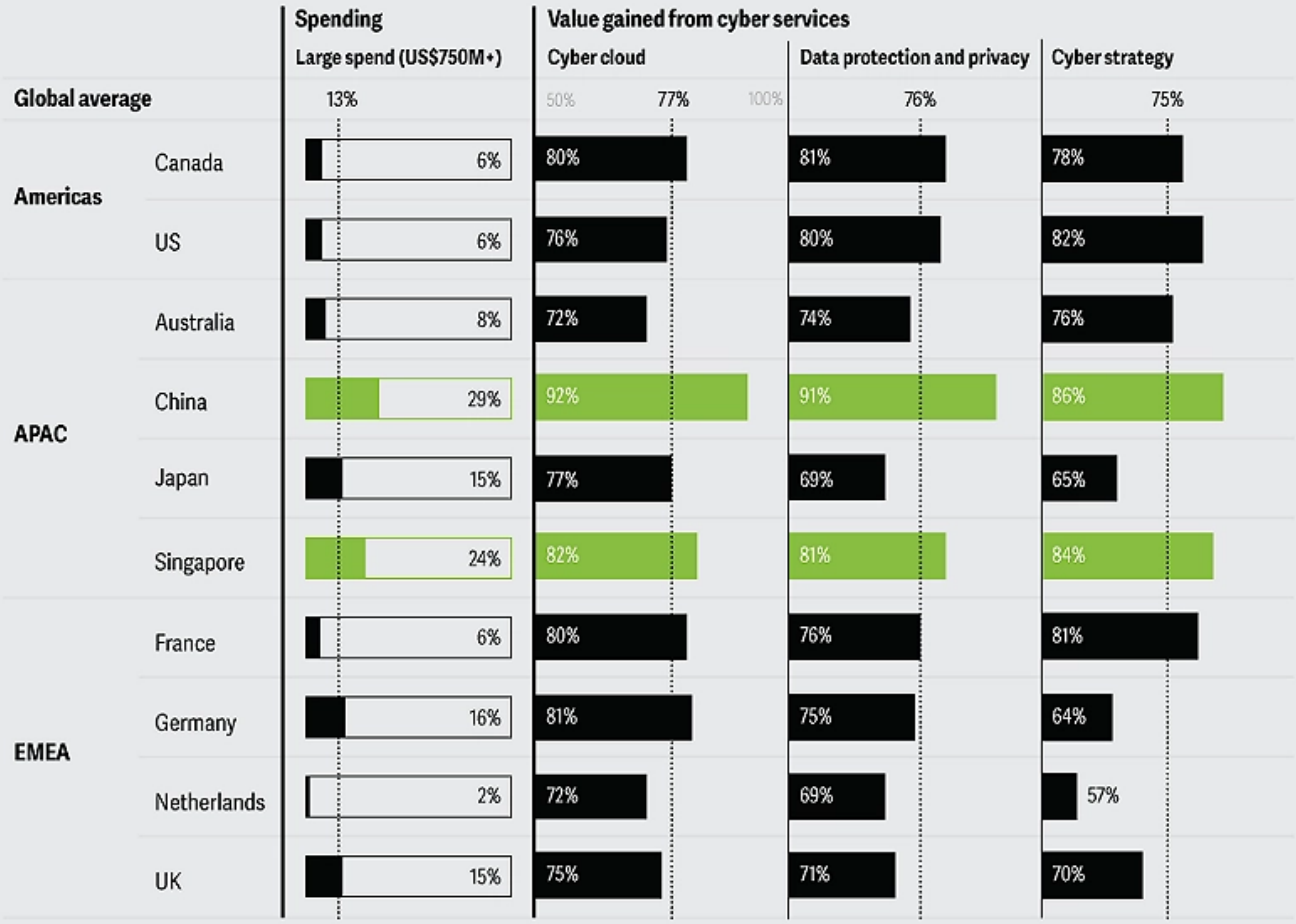
Organizations with more strategic cyber investments emerged as clear winners.

Our data tells us that when it comes to cybersecurity, you get what you pay for. Regional spend leaders, such as APAC, with "large spend" (US$750M+) saw more value from eight out of nine cyber services asked about in our analysis[6] (figure 6).

Figure 6

China and Singapore lead in cyber defense spending and attributed higher value gains from cyber cloud, data protection, and strategy investments than others

What was your company's annual cybersecurity spending for this fiscal year? (organizations spending US$750M+)
To what extent does your organization gain value from the following cyber services?



Note: i) The total number of respondents is 1,110, surveyed across 20 countries, however, this figure depicts only 10 key countries that had a statistically significant sample size and a reasonably representative industry sample; ii) The spending chart reflects a base size of only 1,038 respondents since we removed any anomalies in the spend to revenue data to make the analysis more accurate; iii) Percentages are calculated based on individual country totals and not the overall total. For country totals of the spending chart, refer to: Australia (n=74), Canada (n=90), China (n=38), France (n=48), Germany (n=57), Japan (n=40), Netherlands (n=44), Singapore (n=50), the UK (n=93), the US (n=186). For country totals of the value chart, refer to: Australia (n=81), Canada (n=100), China (n=40), France (n=51), Germany (n=61), Japan (n=40), Netherlands (n=50), Singapore (n=50), the UK (n=100), the US (n=202). For more details, see methodology.
Source: Deloitte Center for Integrated Research.

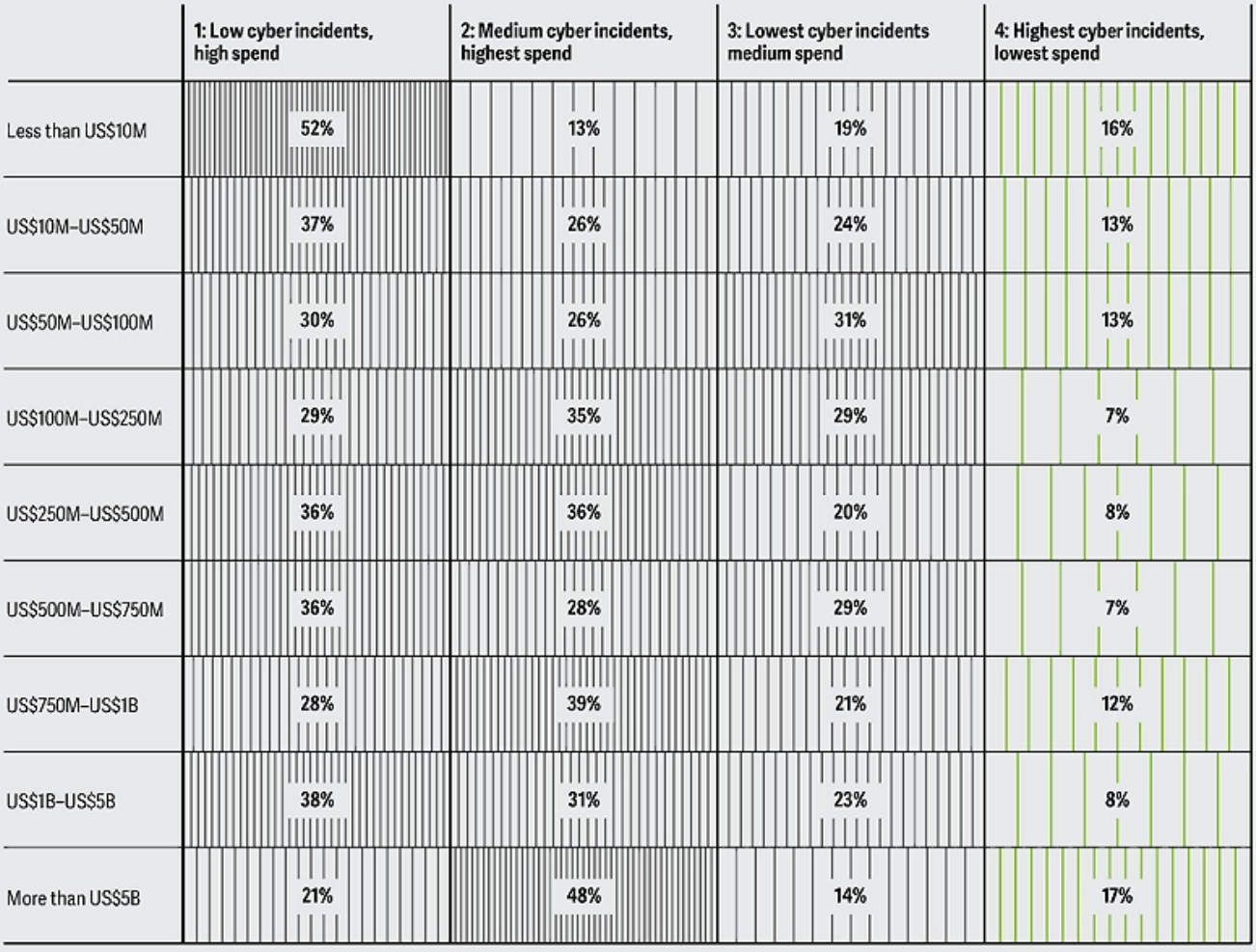
Deloitte. Insights | deloitte.com/insights

Conversely, our additional analysis (see, "Methodology") uncovered that based on the number of cyber incidents, a firm has different spending patterns.12 Organizations most impacted by cyber incidents (cluster 4) tended to spend less than other organizations in almost every budget range except the US$5B+ spend range where they were second to last (figure 7).

Figure 7

A high number of incidents does not guarantee a high spend in cyber defense

Cyber spend across four breach profile clusters (global average)



Note: i) The total number of respondents is 1,110, surveyed across 20 countries; ii) We conducted an additional cluster analysis for validating our spend analysis, thus generating four cyber incident profiles or clusters that are based on the same four survey questions on the number of threats, bad actors, tools and techniques, and negative consequences in the survey. For more details on the cluster analysis, see methodology.
Source: Deloitte Center for Integrated Research.

Deloitte. Insights | deloitte.com/insights

Your spending should be based on top threat trends and priorities where a particular country may be more at risk than others, creating better, more targeted strategies.

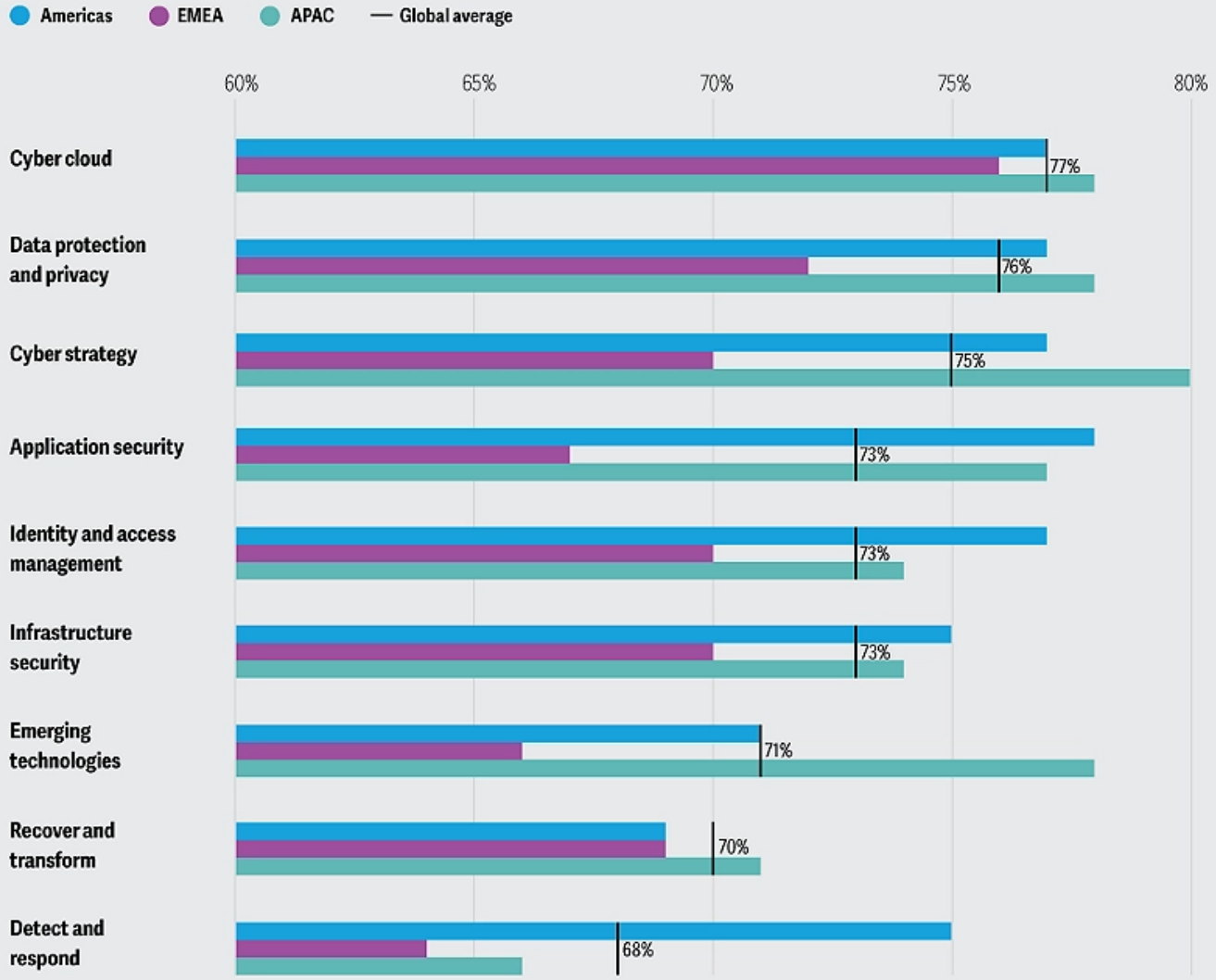
Prioritize strategy, cyber cloud, and data protection and privacy for the most impact

Globally, organizations are gaining high to very high value from all the cybersecurity services in which they're investing, but which capabilities drive the most value? Cybersecurity strategy, cyber cloud, and data protection and privacy seem to be the top value-driving capabilities across all three regions, according to nearly 75% of the respondents.

Figure 8

Cybersecurity strategy, cyber cloud, and data protection and privacy showed the most value globally

How much has your organization seen value to a "high" or "very high" extent from its cybersecurity services?



Note: i) The total number of respondents is 1,110, surveyed across 20 countries, however, this figure depicts only 10 key countries that had a statistically significant sample size and a reasonably representative industry sample; ii) Percentages in the figure reflect only those respondents who selected the responses, 'high value' and 'very high value' in the survey ; iii) Percentages are calculated basis individual region totals and not the overall total. For region totals, refer to: Americas (n=390), EMEA (n=440), APAC (n=280). For more details, see methodology.
Source: Deloitte Center for Integrated Research.

Deloitte. Insights | deloitte.com/insights

APAC and the Americas are value leaders (77-80% for the top three technologies), led by Singapore and China.

It's unclear why, but EMEA underperformed as value laggards in gaining value from these services, with major economies like Germany lagging by 11 percentage points

vs. the overall average. This could be because their implementation of these capabilities has not been able to keep pace with the breadth and scale of the incidents organizations have been experiencing as of late. Detect and respond capabilities are particularly low in EMEA (by four percentage points vs. the global average), and a foundational place to start.

Organizations are facing an increasingly challenging threat landscape. Regional intelligence can inform more focused cyber strategies and should minimize the potential operational and financial damage from cyber incidents. Strong programs look at where the threats are and adjust strategies accordingly. This takes the power out of their hands and keeps it in yours.

Survey methodology

Our research aims to provide an understanding of the cybersecurity threat trends and differences among the three regions—Americas, EMEA, and APAC—when it comes to today's global cyber threat landscape.

We analyzed 1,110 responses to the 2023 Global Future of Cyber Survey conducted from September to October in 2022 and grouped them into the three regions.

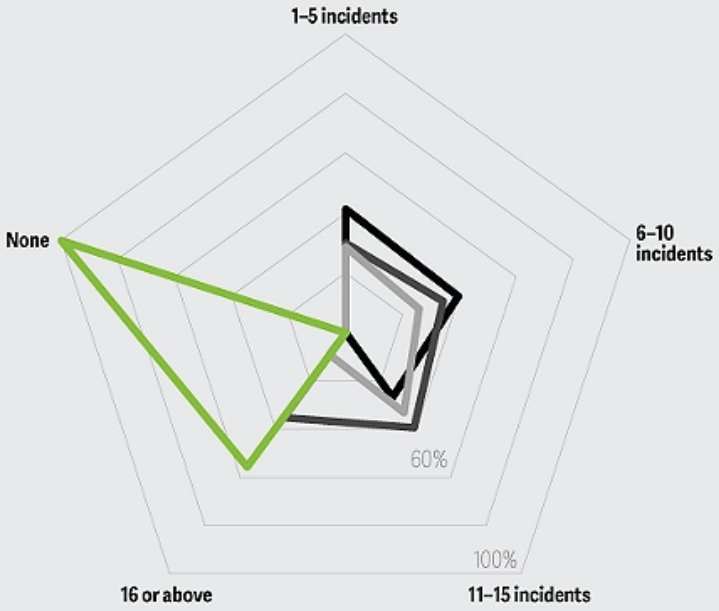
We also examined statistically significant differences across 10 selected countries including Australia, Canada, China, France, Germany, Japan, the Netherlands, Singapore, the UK, and the US, based on a total number of respondents in each country (40+) and an equitable distribution of responses across industries to be considered reasonably representative.

The four cyber incident profiles or clusters appearing in this analysis were based on the same four survey questions on the number of threats, actors, tools and techniques, and negative consequences in the survey. These questions were the input to a hierarchical cluster analysis with clusters validated via a factor analysis. The resulting clusters were then examined across the full survey to provide additional insights on cyber spend profiles in relation to incidents.

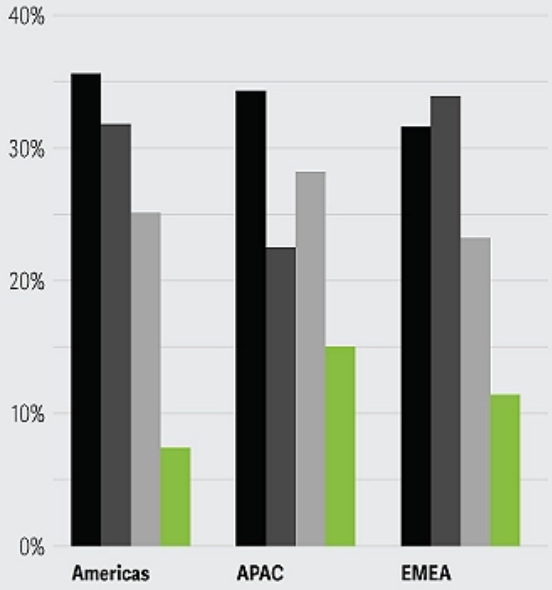
Methodology

1: Low cyber incidents, high spend
2: Medium cyber incidents, highest spend
3: Lowest cyber incidents, medium spend
4: Highest cyber incidents, lowest spend

Number of cyber incidents in the last year across four breach profile clusters



How the four breach groups break out by region



Source: Deloitte Center for Integrated Research

Deloitte. Insights | deloitte.com/insights

Kevvie Fowler
Canada

Kevin Urbanowicz
United States

William Burns
United States

Endnotes

1. *DW*, "German cybersecurity office issues dire threat warning", October 21, 2021.

   View in Article

2. Barry van Wyk, "China's cyber crime problem is growing", *The China Project*, August 23, 2022.

   View in Article

3. Doug Bonderud, "Why Financial Services Companies Are More Prone to Insider Threats, and What They Can do About It," *BizTech Magazine*, September 21, 2021.

   View in Article

4. Staff, "41% of Canadian businesses have laid off staff due to coronavirus: Stats Can," Benefits Canada, May 1, 2020.

   View in Article

5. Tim Keary, "How mass layoffs can create new risks for corporate security," *Venture Beat*, April 14, 2023.

   View in Article

6. Vikki Davies, "Cyber insurer reports 60% spike in ransomware in March 2023," *Cyber Magazine*, May 18, 2023.

   View in Article

7. George Hopkin, "Akamai shares details of Asia's record-breaking DDoS attack," *Cyber Magazine*, March 20, 2023.

   View in Article

8. Amazon Web Services, "What is a DDoS Attack? - Protection and mitigation techniques using managed Distributed Denial of Service (DDoS) protection

service, Web Access Firewall (WAF), and Content Delivery Network (CDN)" accessed August 4, 2023.

View in Article

9. Alexander Martin, "German cyber agency warns threat situation is 'higher than ever," *The Record*, October 25, 2022.

View in Article

10. Greater threat intelligence might include things like evolving cyber threats, dynamic incident notification, management expectations, regional inconsistency defining what constitutes a cyber incident, and more.

View in Article

11. The spend-to-value assessment is further validated by APAC being the least impacted by operational negative consequences from cyberattacks (three percentage points less than the overall global average) and witnessing the least number of 11 or more cyber incidents (four percentage points less than the overall global average).

View in Article

12. We recognize that spend patterns can be influenced by the number of cyber incidents, hence, we took two approaches in our spend analysis: a) First, we analyzed spend in relation to the value gained from cybersecurity investments; b) Second, we analyzed spend in relation to the number of cyber incidents. For the latter, we conducted a cluster analysis, which uncovered four profiles differentiated by their regional composition, cyber incidents, threat concerns, and spending patterns.

View in Article

Acknowledgments

The authors would like to thank everyone who contributed to the 2023 Future of Cyber Survey report and especially the team that supported the creation of this article including, **Ahmed Alibage**, **Andrew Ashenfelter**, **Andy Bayiates**, **Blythe Hurley**, **Deborah Elder**, **Heather Saxon**, **Jaya Gopalan**, **John Gelinne**, **Marco Manglaviti**, **Mike**

Nash, **Molly Piersol**, **Negina Rood**, **Prodyut Borah**, **Saurabh Bansode**, and **Saurabh Rijhwani**.

The team would also like to thank our advisors **Emily Mossburg**, **Kelly Nelson**, **Matt Holt**, and **Nicola Esposito** from the Deloitte Cyber Practice for their leadership and guidance.

Cover image by: **Sofia Sergi**
