

The Deloitte logo is positioned in the top left corner of the page. It consists of the word "Deloitte" in a white, sans-serif font, followed by a small yellow dot. The background of the entire page is a futuristic cityscape at night, with glowing blue and green digital lines and light effects overlaid on the scene. A silhouette of a person is visible in the lower right, looking out over the city.

Deloitte.

Cybersecurity
insights 2023:
Budgets and
benchmarks for
financial services
institutions

Cybersecurity insights 2023: Budgets and benchmarks for financial services institutions

Cybersecurity's importance is reflected in Deloitte's 2023 Cybersecurity for financial services survey, conducted in June 2023. Among the 61 organizations that participated, three key trends emerged:

- Cybersecurity budgets are constrained compared to previous years, but fundamental concerns still dominate priorities.
- Digital transformation is the top business driver for cybersecurity in organizations, but regulatory pressure is increasing and gaining in importance.
- Cybersecurity functions are increasingly focusing on business impact and risks, and not just technology challenges. This shift reflects cybersecurity's growing strategic role for the business.

The task of managing cyber risk has never been more challenging. Deloitte's 2023 survey provides chief information security officers (CISOs), chief information officers, CEOs, and boards the insights to help align their cybersecurity operations with industry standards.

Cybersecurity priorities remain consistent as budgets are challenged

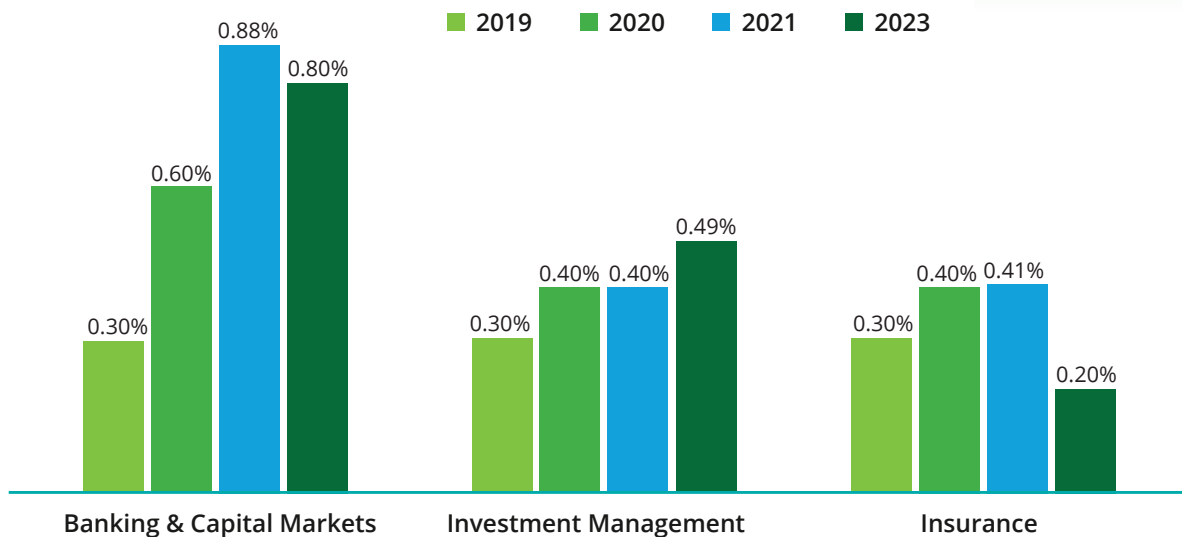
Even as cybersecurity programs mature under the pressure of business requirements and regulatory interest, CISOs are facing budgetary pressure. Spending cuts across financial institutions have reduced cybersecurity budgets as a share of total revenue in banking and capital markets and insurance. Spending grew slightly relative to total revenues in investment management.

Annual cybersecurity spend / revenue

.72%
2021

.54%
2023

Figure 1: What is your organization's cybersecurity budget as a percentage of your organization's total revenue?

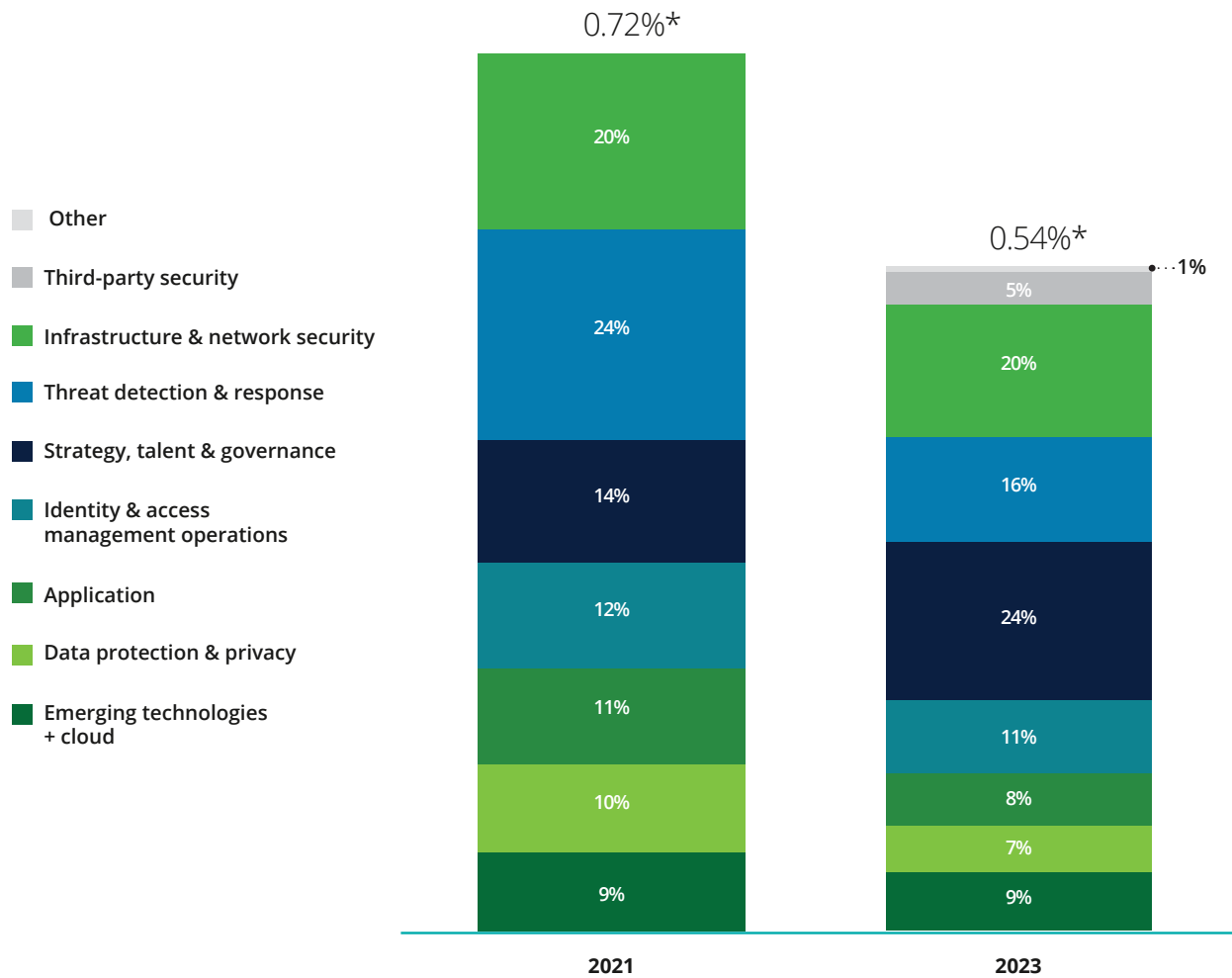


Source: Deloitte & Touche LLP, 2023 Cybersecurity for financial services survey; Deloitte Global, 2021 Future of Cyber Survey; (FSI cut of data) Deloitte FS-ISAC Cyber Benchmarking Surveys, 2019, 2020
Real estate: .54% in 21, .10% in 23, but as only one institution responded in 23, the comparison is not valid.



Within those budgets, spending priorities revealed by the survey were largely consistent with those seen in Deloitte’s 2020 and 2021 cybersecurity reports for financial institutions. Infrastructure and network security, threat detection and response, strategy and governance, and identity and access management operations continue to command the largest shares of spending.

Figure 2: What percentage of your organization’s overall cybersecurity budget for this fiscal year is allocated to the following areas?

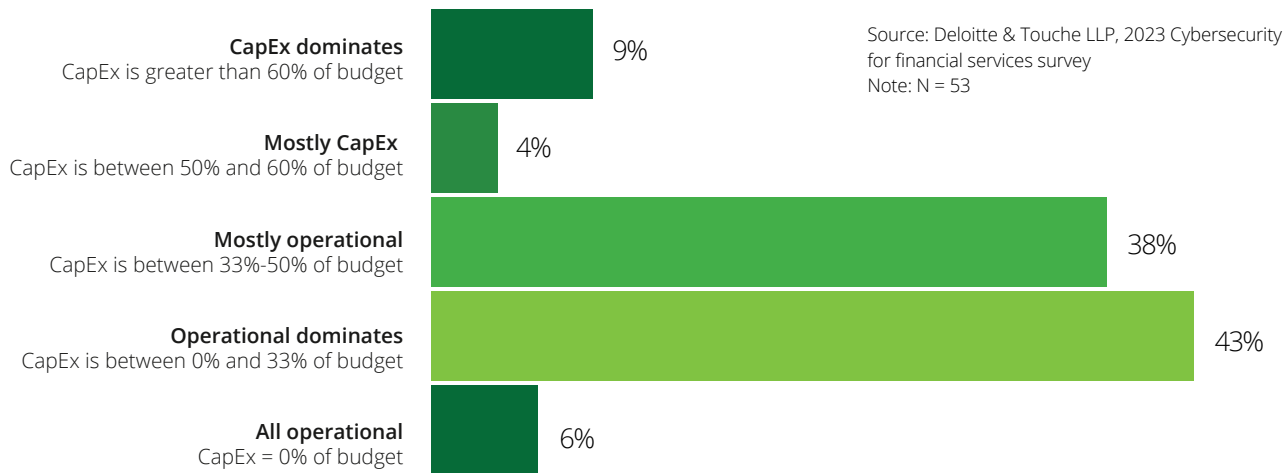


*Represents the annual cybersecurity spend as a percentage of revenue

Note: Cloud migration, integration, & DevSecOps were combined into Emerging technologies + cloud. Cyber transformation was combined into strategy & governance + talent & training. Infrastructure security + IoT, ICS, OT were combined into Infrastructure and network security. These were combined from the 2021 survey to 2023.

The same emphasis on fundamentals emerges when comparing operational and capital expenditures. For the vast majority of financial services institutions, most cybersecurity spending is devoted to operations—not capital investment. Operational expenditures exceeded capital expenditures at 87% of respondent institutions, including 6% of respondents that were fully focused on operations, with no allocation to transformative investments.

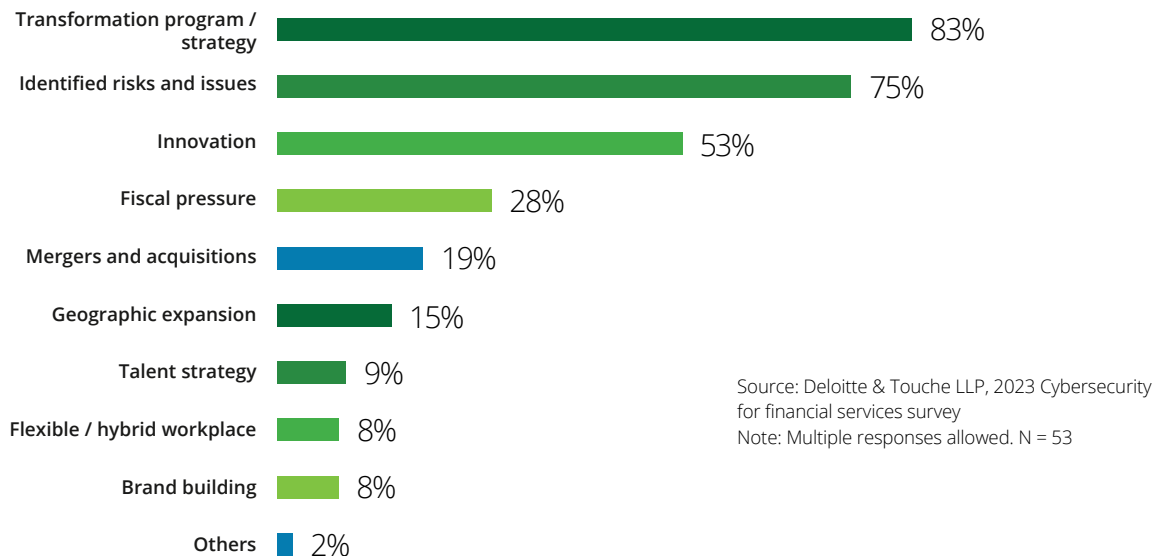
Figure 3: What percentage of your organization’s cybersecurity budget is devoted to capital expenditures (CapEx) vs. operational expenditures (OpEx)?



Digital transformation and regulatory pressure are top business drivers for cybersecurity

As cybersecurity assumes a more central role in business risk management, CISOs’ strategies are increasingly driven by their firms’ broader needs. Two business imperatives emerge in the 2023 survey as critical drivers of cybersecurity enablement.





















Figure 4: What are your organization’s top three business considerations which require security enablement?



Digital transformation: For financial services institutions, adopting emerging technologies is vital for developing business and controlling costs. As the aftershocks of the COVID-19 pandemic fade, firms are refining their strategies for digital transformation. Cybersecurity is being integrated into the new processes and systems as they are built.

Cloud computing remains the top transformation priority for financial services institutions in the 2023 survey, followed by increased use of intensive data analytics. But interest in artificial intelligence is surging as well, creating new concerns that CISOs should address.

Figure 5: What are your organization's top five digital transformation priorities?

	2018	2019	2020	2023
1	 Cloud	 Cloud	 Cloud	 Cloud
2	 Data/analytics	 Data/analytics	 Data/analytics	 Data/analytics
3	 Mobile	 Mobile	 Artificial intelligence / cognitive computing	 Artificial intelligence / cognitive computing
4	 Artificial intelligence / cognitive computing	 Robotic process automation (RPA)	 Robotic process automation (RPA)	 New or upgrade for Enterprise Resource Planning (ERP) Program & operational technology
5	 Social Media	 Artificial intelligence / cognitive computing	 Mobile	 Blockchain / cryptocurrency

Source: Deloitte & Touche LLP, 2023 Cybersecurity for financial services survey; Deloitte Touche Tohmatsu Limited, 2021 Future of Cyber Survey (FSI cut of data); Deloitte FS-ISAC Cyber Benchmarking Surveys, 2019, 2020
Note: N = 53

Risk reduction: Regulators are increasingly focused on cybersecurity risks, forcing financial services institutions to pay increased attention to managing identified risks. Financial services institutions identify coping with identified risks (e.g., audit findings) and regulatory issues as the main drivers for cybersecurity spending, almost on par with new digital investments.

Regulatory pressure is expected to increase: on July 26, 2023, the US Securities and Exchange Commission issued a final ruling to adopt new regulations requiring faster and more comprehensive reporting on cyber breaches and other issues from all public companies. Financial firms—including brokers, dealers, investment companies, and registered investment advisers—could face additional new requirements for safeguards to protect customer records and information, and to create or update incident response programs for data breaches.

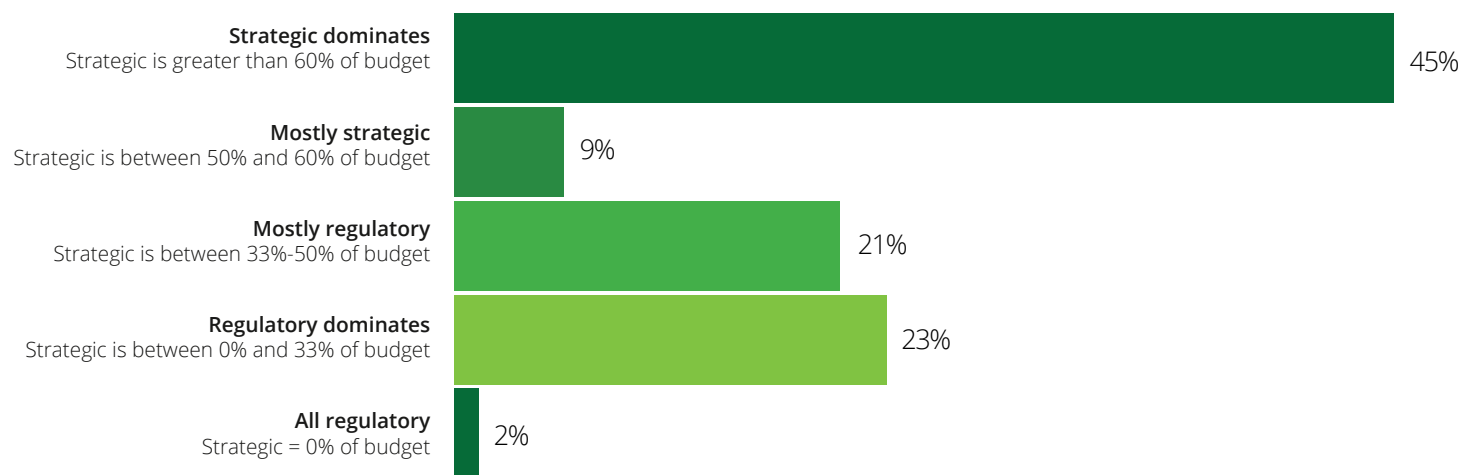
Source: SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, 2023 <https://www.sec.gov/news/press-release/2023-139>

These two drivers, increased risk and regulatory pressures, feed one another: each new technology introduced into business processes invites increased regulatory scrutiny. While regulators have been focused on risks associated with cloud data and services, cyber concerns raised by artificial intelligence and cognitive computing are soon likely to attract more attention.

The growing importance of risk reduction is reflected in financial services institutions' spending: regulatory drivers account for more than half of the cybersecurity budget at 46% of the firms surveyed in 2023, not far short of the 54% who report that strategic priorities are dominant.

Figure 6: What percentage of your organization's cybersecurity budget is driven by strategic priorities, rather than regulatory priorities?

(Percentage of responding firms)



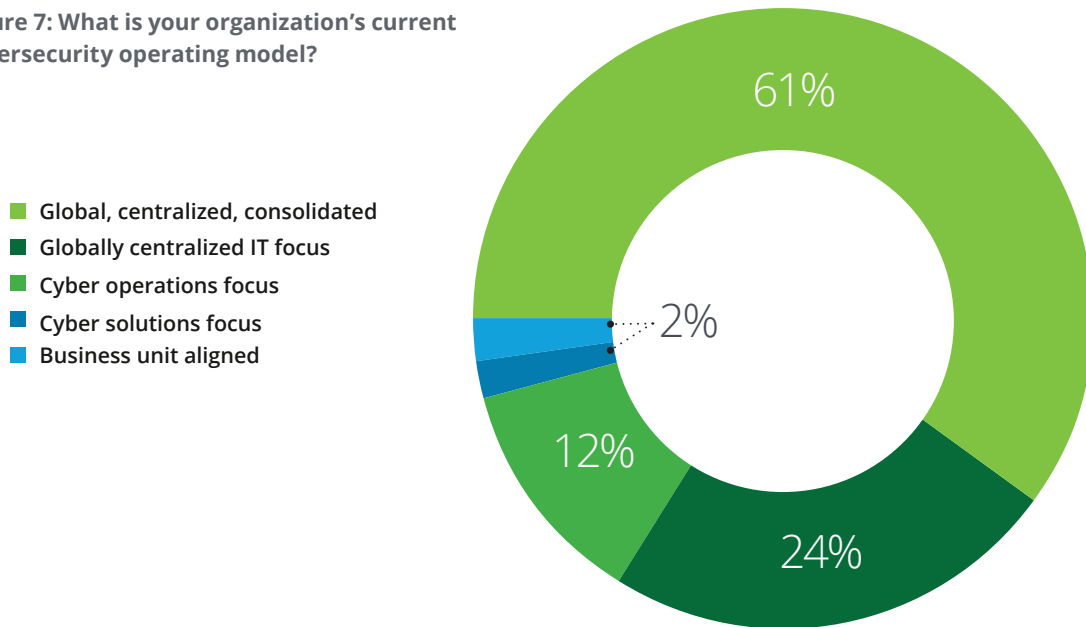
Source: Deloitte & Touche LLP, 2023 Cybersecurity for financial services survey
Note: N = 53

Cybersecurity organizations are more independent, centralized

In 2020, Deloitte's *Reshaping the Cybersecurity Landscape* report pointed out that realizing cybersecurity's strategic importance would require looking beyond information technology, including how it impacts the businesses strategy.. The 2023 survey demonstrates that many businesses have taken that message to heart. The majority of responding financial institutions report that their cybersecurity organization follows a global, centralized, and consolidated operating model.

- Global: the cybersecurity organization spans the institution's geographic locations
- Centralized: one cybersecurity organization provides service to all lines of business and/or defines central policies and standards that should be implemented by all lines of the business
- Consolidated: the organization focuses on all aspects of cybersecurity beyond technology/IT including impact on business, risk, and talent

Figure 7: What is your organization's current cybersecurity operating model?



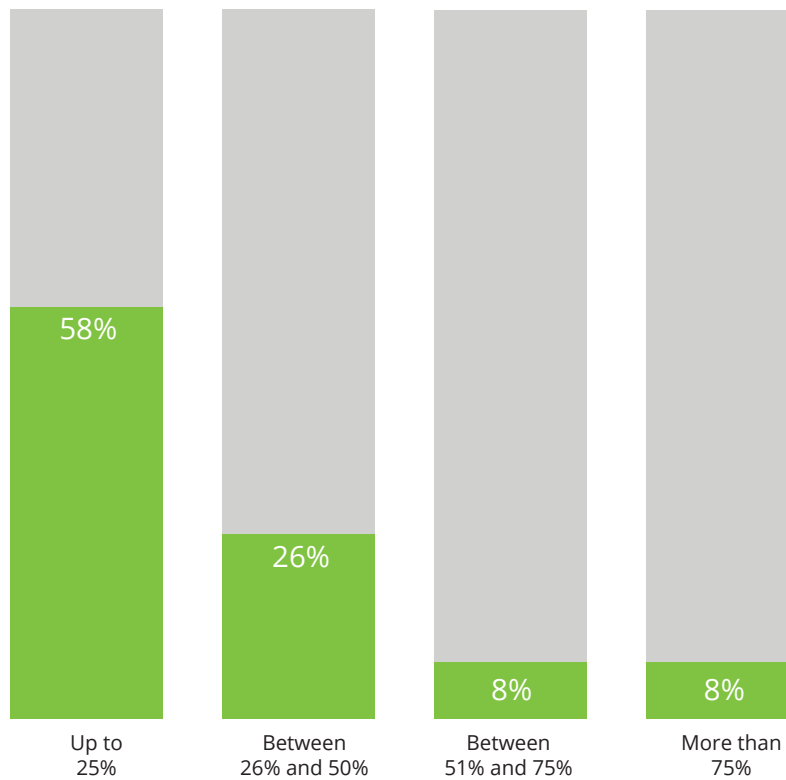
Source: Deloitte & Touche LLP, 2023 Cybersecurity for financial services survey
Note: N = 51



The second most common operating model is globally centralized, with an IT focus—leaving some aspects of cybersecurity to the broader business organization. Only 2% of institutions reported that their operating model distributed cybersecurity functions to business units.

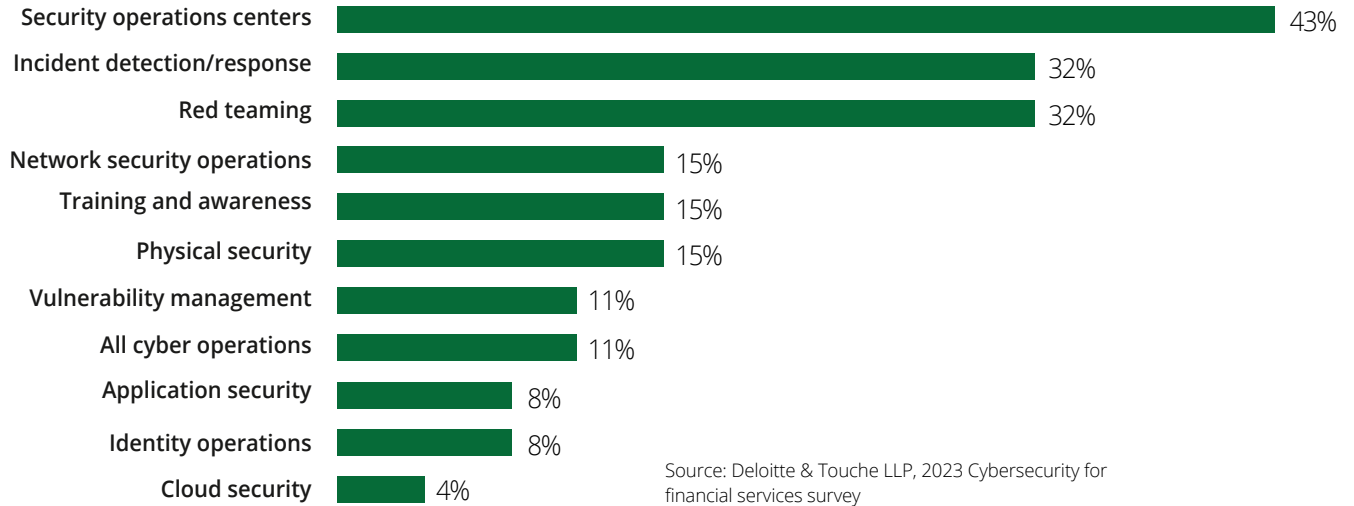
CISOs continue to depend on outsourcing for many of their operations: 42% of respondents report that they outsource more than 25% of their organization’s cybersecurity budget (Figure 8). However, 21% of respondents say that they have not outsourced any of their cybersecurity operations (Figure 9). Security operation centers are most commonly outsourced, followed by incident detection and response and “red teaming.” Virtually all financial services institutions prefer to keep cloud security in-house.

Figure 8: What percentage of your organization’s cybersecurity budget is outsourced?



Source: Deloitte & Touche LLP, 2023 Cybersecurity for financial services survey
Note: N = 53

Figure 9: Which of the following cybersecurity areas are outsourced (e.g., externally managed services) by your organization?

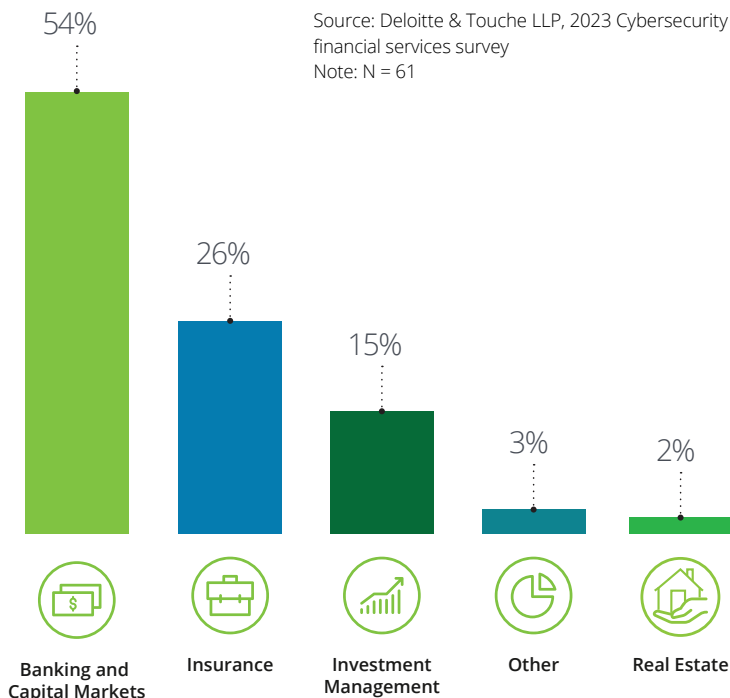


Source: Deloitte & Touche LLP, 2023 Cybersecurity for financial services survey
 Note: Multiple responses allowed. None=21%, N=53

About this survey

The 2023 Cybersecurity for financial services survey was conducted by Deloitte & Touche LLP in June 2023 to provide the financial service industry with benchmarks for the size, importance, and functioning of cybersecurity operations. A total of 61 financial institutions responded to the survey, with the majority in the banking and capital market sector.

Figure 10: What is the primary financial sector for your organization?



Source: Deloitte & Touche LLP, 2023 Cybersecurity for financial services survey
 Note: N = 61

The majority of respondents reported that they operated in the North America or Europe, the Middle East, and Africa (EMEA) markets (Figure 11). The respondents included institutions of all sizes, with the largest share reporting “midsize” revenues of between \$500 million and \$5 billion.

Figure 11: In what regions does your organization operate?

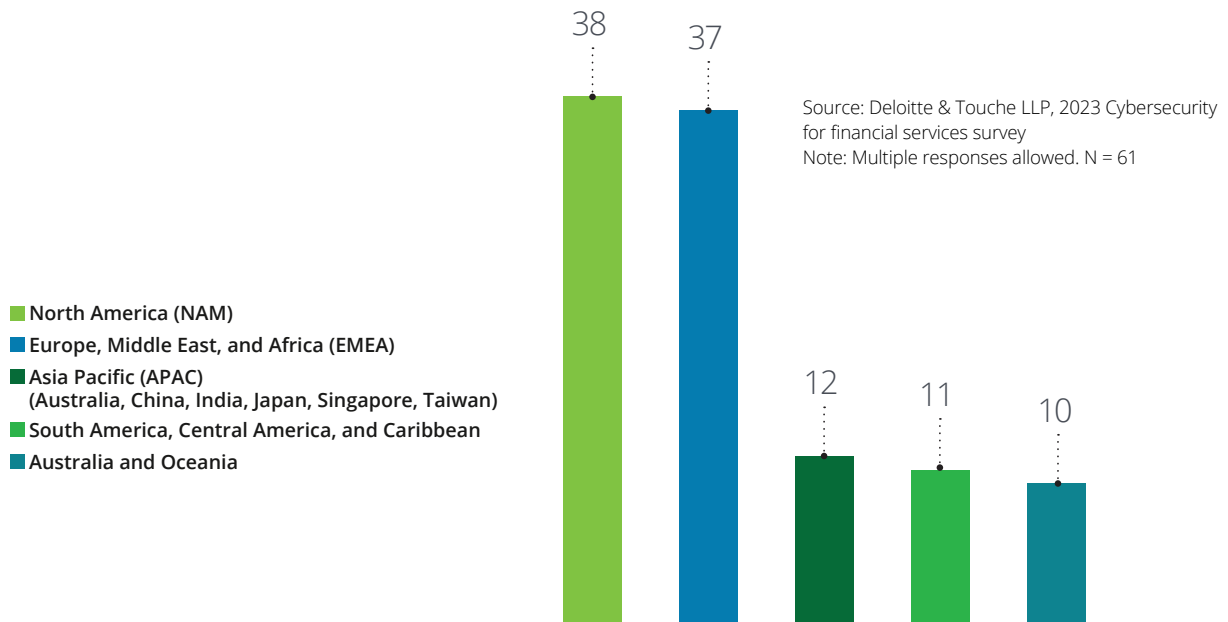
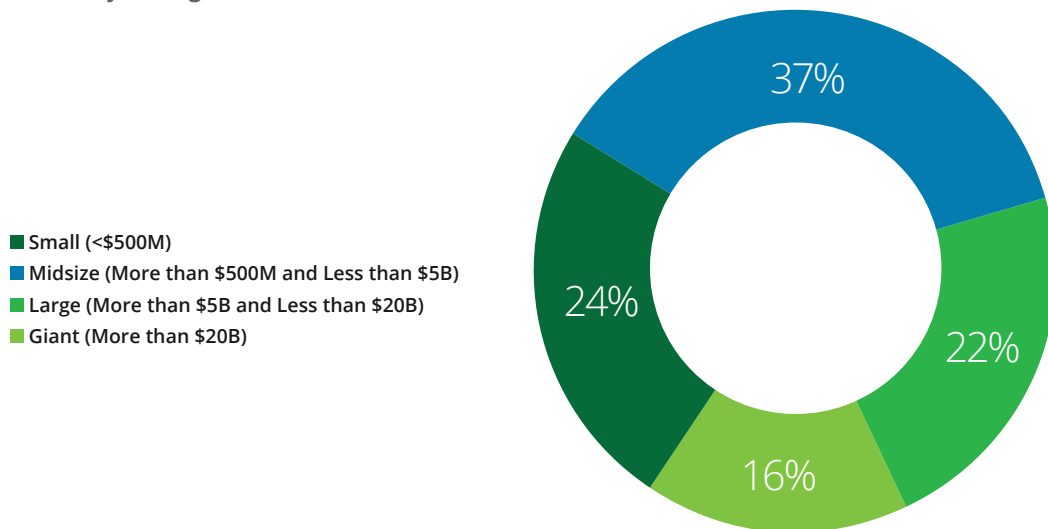


Figure 12: What is your organization’s total revenue?



Source: Deloitte & Touche LLP, 2023 Cybersecurity for financial services survey
 Note: N = 49. Responses may not add up to 100% due to rounding

Connect with us:



Julie Bernard
Principal

Deloitte & Touche LLP

juliebernard@deloitte.com



Meghana Kanitkar
Managing Director

Deloitte & Touche LLP

mkanitkar@deloitte.com



Steve Rampado
Partner – Cyber Leader

Deloitte Canada

srampado@deloitte.ca



Nick Seaver
Partner

Deloitte UK

nseaver@deloitte.co.uk

Deloitte.

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. In addition, this document contains the results of a survey conducted by Deloitte. The information obtained during the survey was taken "as is" and was not validated or confirmed by Deloitte.

Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.