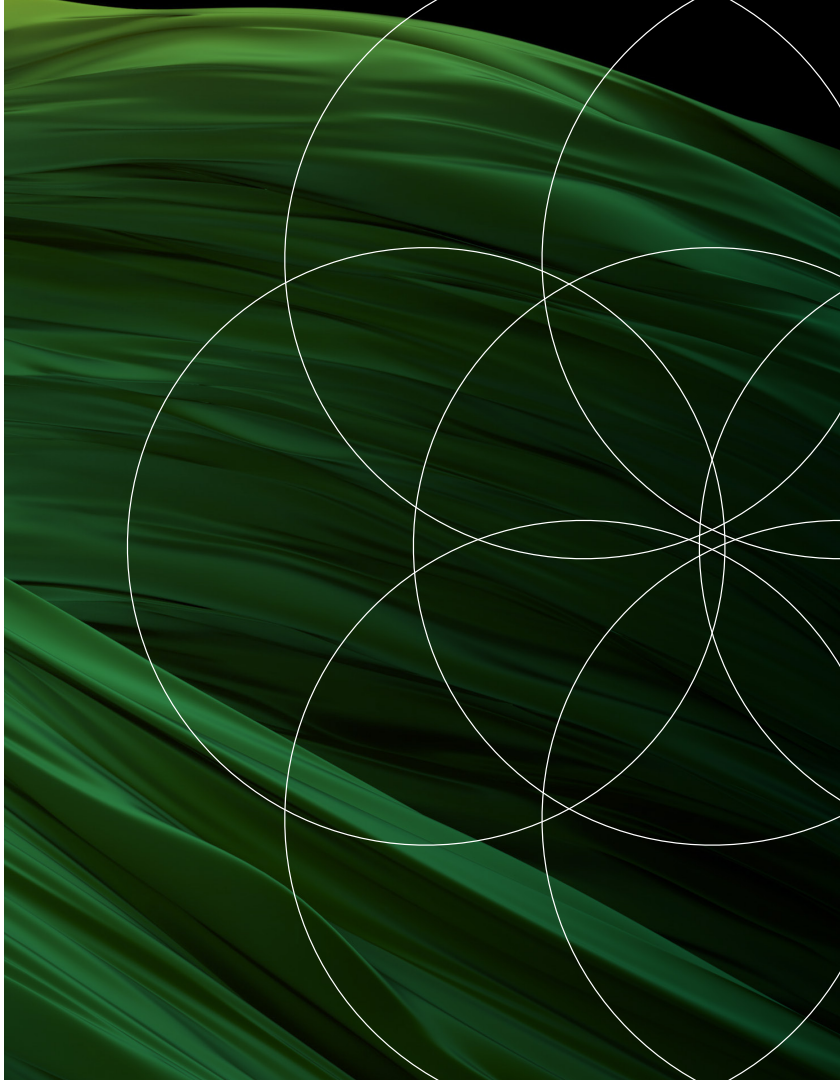
FORRESTER®

Automate Cloud Data Security And Risk Insight For Modern Business Resiliency

Data Security Automation Offers Information Security Leaders A Solution To Modern Security Challenges That Impede Many Businesses

Get started →

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY CYERA | SEPTEMBER 2023



Overview

As the volume and business value of data continue to grow, so does the use of cloud services to manage it. However, an astonishing 74% of security decision-makers estimated that their organization's sensitive data was breached at least once in 2022.[1]

In a study commissioned by Cyera, Forrester Consulting surveyed 253 information security decision-makers at organizations based in North America. The study shows that companies are struggling to meet their security goals while also enabling the business. Cumbersome, manual security controls are the biggest challenge security leaders face, and the lack of automation is hurting business. Automating data security is a critical step. It not only unlocks business value, but also helps companies strengthen and maintain a robust security posture, and 70% of respondents expect significant or transformational benefits from investing in it.

Key Findings

Security leaders expect the most transformational benefits to come from automating data security, specifically risk assessments, data discovery, and classification.

Inefficient security controls are draining resources and hurting business. Seventy-one percent of security leaders said legacy technologies and manual processes inhibit business success.

Security leaders are investing in automation to improve Zero Trust maturity, avoid regulatory fines, improve operational efficiency, and maintain customer trust.

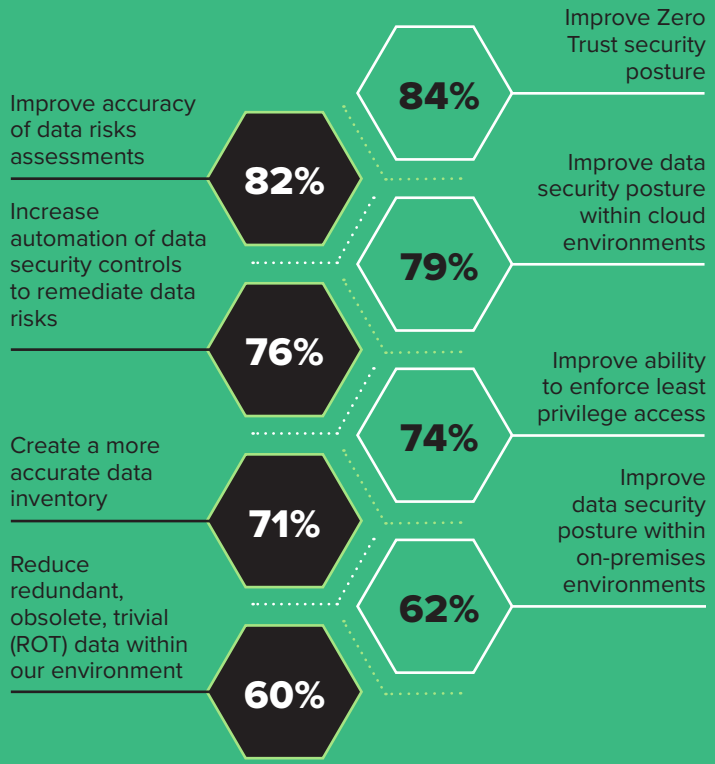
Zero Trust Is Top Priority For Security Leaders

Information security decision-makers have many important goals for the coming year, with 60% of respondents rating all eight highlighted in this study as critical or high priorities. But the top goal for security leaders is strengthening their organizations' Zero Trust security posture (84%).

This aligns with Forrester's Security Survey, 2022, which found that firms allocated on average 14% of its security budget to cloud security, with boosting cloud security strategy a top priority in 2023.[2]

Without adequate cloud data protection, organizations cannot migrate on-premises data to the cloud. Improving Zero Trust security posture and data security ensure that sensitive data does not fall into the wrong hands. Improving data risk assessment accuracy (82%), data security posture in the cloud (79%), and increasing automation of security controls (76%) are critical or high priorities for security leaders.

Importance Of The Following Data Security Goals To Organizations In The Next 12 Months



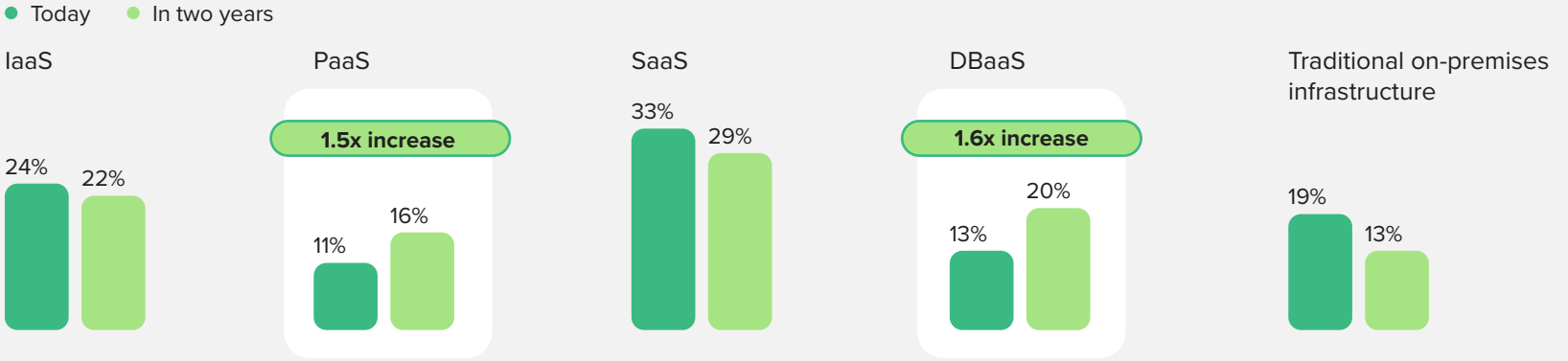
Base: 253 information security decision-makers of at least director level at North American companies
Note: Showing sum of responses for "Critical" and "High" priority
Source: A commissioned study conducted by Forrester Consulting on behalf of Cyera, June 2023

Businesses Continue To Move More Data To Cloud Platforms and Databases

As on-premises infrastructure becomes less relevant, the use of platforms as a service (PaaS) and databases as a service (DBaaS) at organizations will grow in the coming two years. While the planned use of infrastructure as a service (IaaS) and software as a service (SaaS) is expected to dip slightly, they remain the most frequently used cloud environments.

Many security leaders will need to maintain and secure data across a hybrid environment, with a heavy emphasis on cloud environments and some on-premises infrastructure. They must rethink how to manage and secure these environments. As various cloud environments also offer built-in security functionality, security leaders must assess the tradeoffs of using built-in capabilities (e.g., manual processes, fragmented deployments, and protracted implementations) versus best-of-breed third-party solutions.

Approximate Current And Planned Percentage Of Organizational Data Stores In The Following Categories



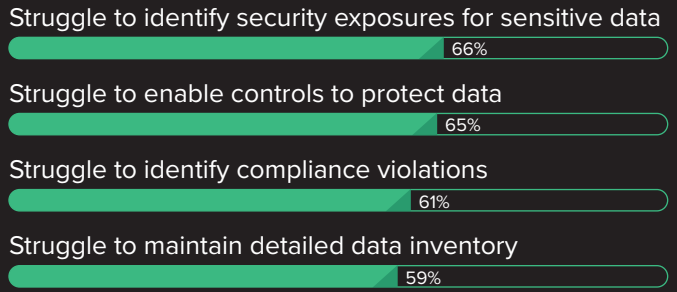
Base: 253 information security decision-makers of at least director level at North American companies
Note: Showing mean values
Source: A commissioned study conducted by Forrester Consulting on behalf of Cyera, June 2023

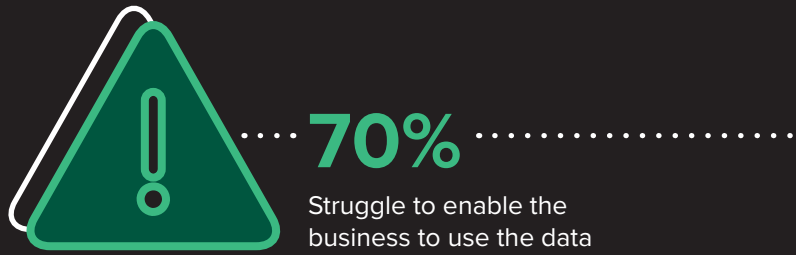
Most Companies Struggle To Meet Security Goals While Enabling The Business

Advanced insights-driven business capabilities are essential to unlock and sustain competitive advantage.[3] Maturity goes beyond data quality for generating data value. Ensuring security, privacy, and compliance are critical to turn data into insights. This includes adhering to regulatory requirements, business partner, and contractual requirements. Unless leaders design organizations to align groups to the goal of enabling data-driven decision-making through the appropriate use of proprietary or sensitive information, no amount of data, regardless of its quality, can make a difference.

Using data to enable the business is the biggest challenge information security leaders face, as 70% reported it is challenging or very challenging for their organizations. This struggle to use data is largely caused in part by the inability to identify security exposures for sensitive data (66%) and compliance violations (61%).

Challenges Faced By North American Companies In Achieving Security Goals





Base: 253 information security decision-makers of at least director level at North American companies
Note: Showing sum of responses for "Challenging" and "Very challenging"
Source: A commissioned study conducted by Forrester Consulting on behalf of Cyera, June 2023

A New Approach To Data Security Is Needed Today

Conventional approaches using traditional tooling for cybersecurity do not enable robust data security controls.[4] Ninety-eight percent of respondents said the data security status quo at their company is a problem. As organizations continue to modernize their operations and depend more on cloud environments, they must overcome new challenges securing data. This is not an easy task, as companies also contend with existing data security challenges.

The common challenges of legacy technologies, fragmented deployments, and protracted implementations collectively indicate systemic problems that would benefit from a new approach to data security. These manual and cumbersome processes directly conflict with the dynamic security controls that enable a true Zero Trust architecture, ultimately designed to safeguard sensitive data across networks, workloads, identities, and devices.

Challenges Faced By Organizations With Their Current Approach To Data Security

Base: 253 information security decision-makers of at least director level at North American companies
Note: Respondents were asked to select all challenges that were applicable to their organization
Source: A commissioned study conducted by Forrester Consulting on behalf of Cyera, June 2023

Lack Of Automation Hurts The Business

Only data that has been identified and prioritized according to its risk can be effectively protected. Cloud-native security capabilities and dedicated data security platforms that can cover cloud and on-premises environments but lack automation cannot maintain current asset inventories. Sixty-nine percent continue to manually maintain asset inventories today. Companies treat cloud environments like a massive expandable garage for growing volumes of data assets. It is no surprise that 59% admit they struggle to maintain a detailed data inventory.

Seventy-one percent of respondents reported that manual data security processes inhibit their business's success. Security leaders who find new ways to automate data security processes and controls will not only improve security, but also empower their business colleagues to unlock value in new ways. Identifying your data and gaining visibility into its risks are essential before you can protect and use it.

"How much do you agree or disagree with the following statements?"

69%
Maintain asset inventories manually

71%
Say manual data security processes and controls inhibits business success

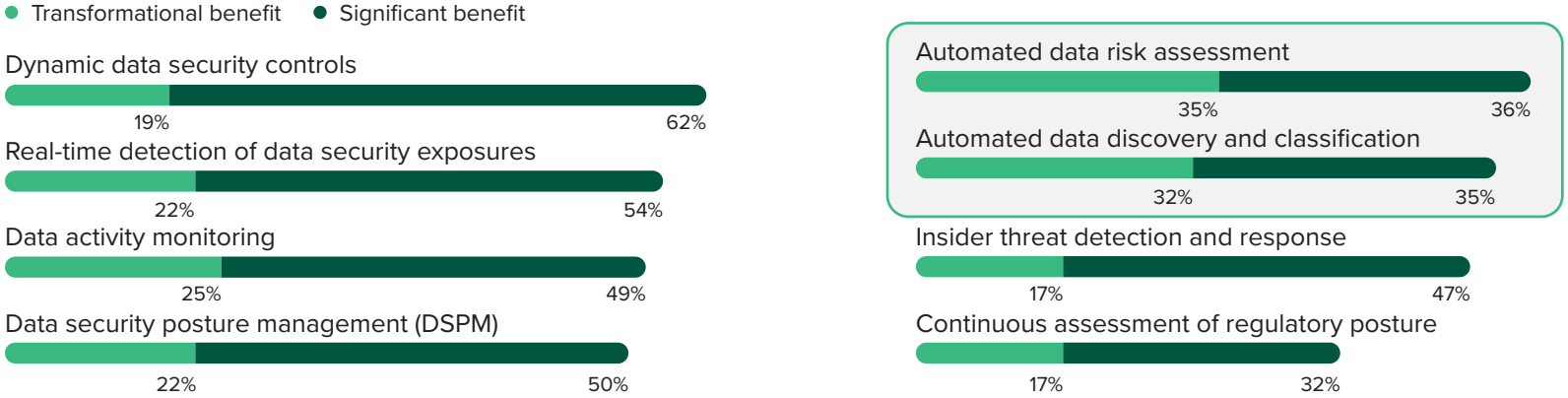
Base: 253 information security decision-makers of at least director level at North American companies
Note: Showing sum of responses for "Agree" and "Strongly agree"
Source: A commissioned study conducted by Forrester Consulting on behalf of Cyera, June 2023

Cloud-Native Data Security Tools With Automation Would Have A Large Impact

Information security leaders reported their organizations stand to gain important benefits from investing in modern data security technology. Capabilities that will drive meaningful change are dynamic security controls (81%), real-time exposure detection (76%), and data security posture management (72%).

A key insight is that respondents expect to get the most transformational benefits from improving data security automation. Data security platform vendors are extending artificial intelligence and machine learning (AI/ML) functionalities to enable dynamic controls through automation. This shift promises to improve security policy automation and orchestration. Overcoming the manual nature of legacy security technology will reduce the complexity and necessary steps for managing and maintaining security controls that are as dynamic as the modern organizations they protect.

Extent Of Expected Benefit From Investing In Each Of These Capabilities



Base: 253 information security decision-makers of at least director level at North American companies
Source: A commissioned study conducted by Forrester Consulting on behalf of Cyera, June 2023

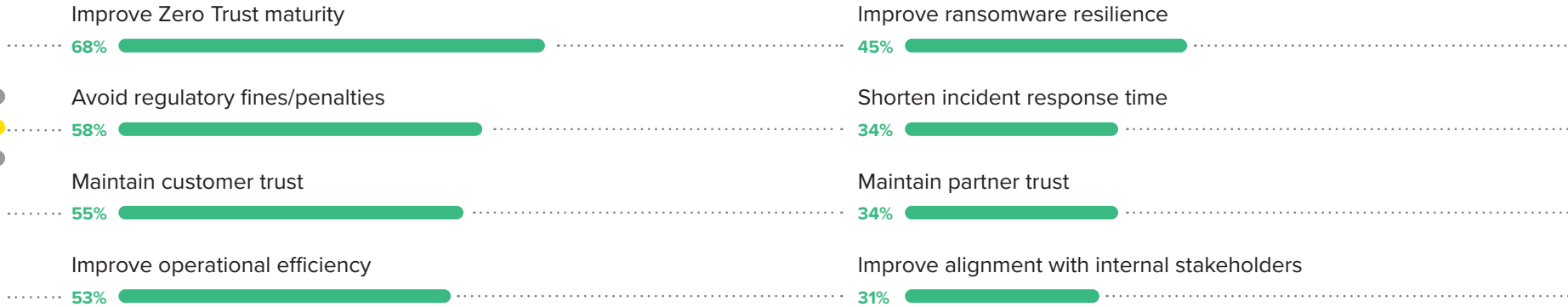
Automation Accelerates Efforts That Go Beyond Maintaining A Good Security Posture

As more IT work is done in the cloud and data volume grows, information security leaders need more automation to maintain a strong security posture.

Among the benefits from investing in automated data discovery, classification, and risk assessment were improving their Zero Trust maturity (68%), avoiding regulatory fines (58%), improving operational efficiency (53%), increasing their resilience to ransomware threats, and maintaining customer trust (45%).

Investing in automation would also help to better align security efforts with business imperatives. Expected business benefits include maintaining customer trust (55%) and improving operational efficiency (53%).

Expected Benefits From Investing In A Data Security Platform That Automates Data Discovery, Classification, And Risk Assessment



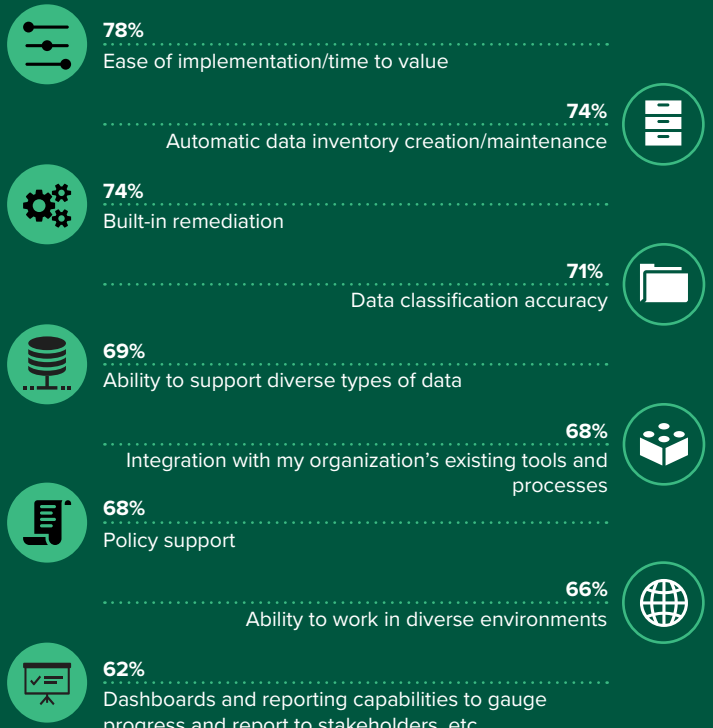
Base: 253 information security decision-makers of at least director level at North American companies
Source: A commissioned study conducted by Forrester Consulting on behalf of Cyera, June 2023

Time To Value Is The Most Critical Consideration

Information security leaders need solutions that provide many important capabilities, given improving their data security posture is such a high priority and they stand to gain so much from investing in automating data security. However, the most important purchasing consideration is the ease of implementation to shorten time to value, with 78% of respondents rating it as critical or very important.

Security leaders also need automatic data inventory creation and maintenance (74%), built-in remediation (74%), and the ability to work in diverse environments (66%). Prior experiences with deploying data security technologies, current gaps in existing tools, and staffing pressures are likely factors that contribute to the importance that security leaders place on these capabilities.

Importance Of These Capabilities In Investing In A Data Security Platform



Base: 253 information security decision-makers of at least director level at North American companies
Note: Respondents were asked to rate the importance of each capability shown above. Showing sum of responses for "Critical" and "Very important"
Source: A commissioned study conducted by Forrester Consulting on behalf of Cyera, June 2023

Conclusion

Automating important processes is key to addressing modern data security challenges. This study found that:

- **Many companies struggle to meet security goals while enabling the business.** These often-interconnected challenges, including identifying sensitive data, visibility into security exposures and compliance risks, and enabling data controls, necessitate a new approach to data security.
- **A piecemeal approach to securing multicloud and hybrid deployments won't work.** To achieve rapid time-to-value, replace fragmented approaches and long implementation cycles with architecture and capabilities appropriate to the unbounded nature of cloud workloads and data.
- **Automation would improve security and unlock business value.** The greatest uplift would come from automating data discovery and classification and data risk assessments.

Endnotes

[1] Source: Forrester's Security Survey, 2022.

[2] Source: Forrester's Security Survey, 2022.

[3] Source: "Build An Insights-Driven Business," Forrester Research, Inc., March 9, 2023, January 27, 2022.

[4] Source: "Gauge Your Zero Trust Maturity," Forrester Research, Inc., March 10, 2023.

Resources

Related Forrester Research:

Gauge Your Zero Trust Maturity, Forrester Research, Inc., March 10, 2023.

Build An Insights-Driven Business, Forrester Research, Inc., January 27, 2022.

Related Resources

Heidi Shey, Redefining Data Security For The Modern Age, Forrester Blogs.

Project Team:

Lane Abernathy, Market Impact Consultant

Lillie Sinprasong, Associate Market Impact Consultant

Contributing Research:

Forrester's Security & Risk research group

Methodology

This Opportunity Snapshot was commissioned by Cyera. To create this profile, Forrester Consulting supplemented this research with custom survey questions asked of 253 decision-makers of at least director level who are responsible for information security at North American companies. The custom survey began and was completed in June 2023.

Demographics

COUNTRY	
United States	51%
Canada	49%

INDUSTRY	
Financial services	26%
Healthcare	24%
Technology and/or technology services	25%
Travel and hospitality	25%

CURRENT DEPARTMENT	
IT	58%
Operations	42%

Note: Percentages may not total 100 due to rounding.

NUMBER OF EMPLOYEES	
20,000 or more	24%
5,000 to 19,999	36%
1,000 to 4,999	40%

CURRENT POSITION	
C-level	15%
Vice president	38%
Director	46%

LEVEL OF RESPONSIBILITY	
Final decision-maker	19%
Part of a team making decisions	39%
Influences decisions	42%

Demographics (Continued)

PRIMARY RESPONSIBILITIES IN IT AND OPERATIONS ROLE	
Cybersecurity	**57%**
Information security	**53%**
Security operations	**43%**
IT operations	**52%**

Note: Respondents were asked to select all the primary responsibilities they were involved in.

FORRESTER®