CyberProof®
A UST Company

12 Questions for Security Leaders in 2023

Based on Forrester's latest privacy report

DATA OVERVIEW REPORT

The State Of Privacy And Cybersecurity, 2022

September 8, 2022

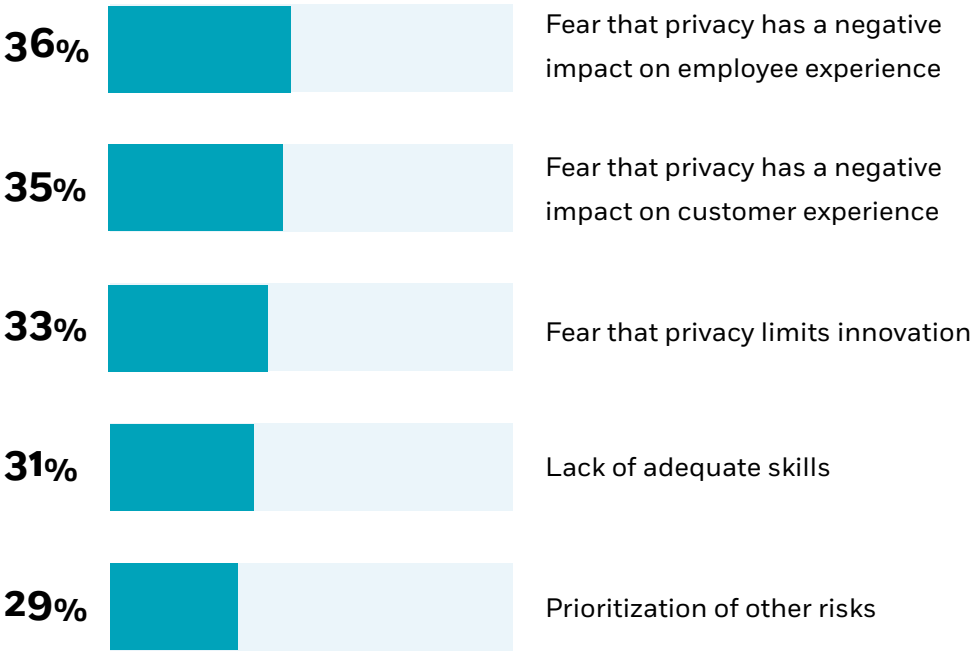
By Jeff Pollard, Heidi Shey, Paul McKay, Jinan Budge, Jess Burn with Amy DeMartine, Isabelle Raposo, Zachary Dallas, Peggy Dostie

FORRESTER®

Summary

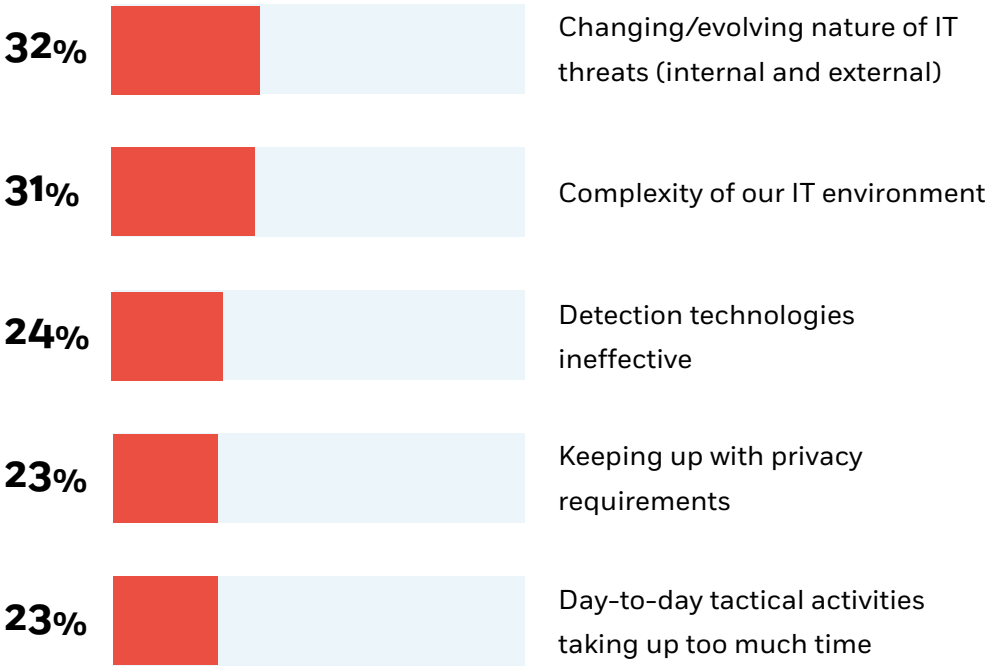
Tech execs face powerful headwinds as they shape privacy and cybersecurity programs to advance the organization's strategic objectives. A tumultuous backdrop of geopolitical upheaval, a frenzied rush to cloud, and a flood of regulatory requirements add to an already competing list of priorities. Tech execs should use the data in this report to track the challenges, concerns, and priorities of privacy and cybersecurity and modify their programs accordingly, rally support, influence stakeholders, and eliminate obstacles.

1 What are your organization's biggest challenges to protecting employees' and customers' privacy?



Fear challenges the progress of privacy programs.

2 What are your organization's biggest challenges to protecting employees' and customers' security?



Change and complexity of the IT environment challenge cybersecurity programs.

3 What initiatives are likely to be your top strategic and tactical privacy priorities over the next 12 months?

Strategic:

71%
Contribute to business operational excellence

71%
Increase business efficiency

71%
Increase customer trust in the brand

69%
Increase the influence of privacy in the organization

69%
Better support business decision-making

Tactical:

71%
Improve risk reporting

68%
Improve customer privacy communication

67%
Improve compliance

67%
Increase privacy assessments/ privacy protection of software

67%
Increase privacy assessments/ privacy protection in connection with data

Prioritizing privacy works in tandem with business growth and innovation.

What initiatives are likely to be your top strategic and tactical information/IT security priorities over the next 12 months?

Strategic:

29%

Improving security operations strategy

28%

Use built-in security capabilities instead of third-party security technologies for the same capability

27%

Establishing security strategies for public clouds

25%

Instilling a security culture by elevating communication and security training

23%

Improve our privacy and data ethics strategy

Tactical:

22%

Improving application security capabilities and services

20%

Improving security analytics capabilities (SIM, SIEM, NAV, SUBA)

20%

Implementing artificial intelligence (AI) technologies to improve security

19%

Securing internet of things (IoT) within the enterprise

19%

Improving threat hunting capabilities

Improving security means rethinking operational strategies to meet today's needs.

5 With which of the following teams/groups does your privacy team collaborate most often?

	Currently	12-month projection
IT	**62%**	**45%**
Security	**47%**	**31%**
Risk and compliance	**45%**	**42%**
Legal	**42%**	**30%**
Data management	**38%**	**31%**

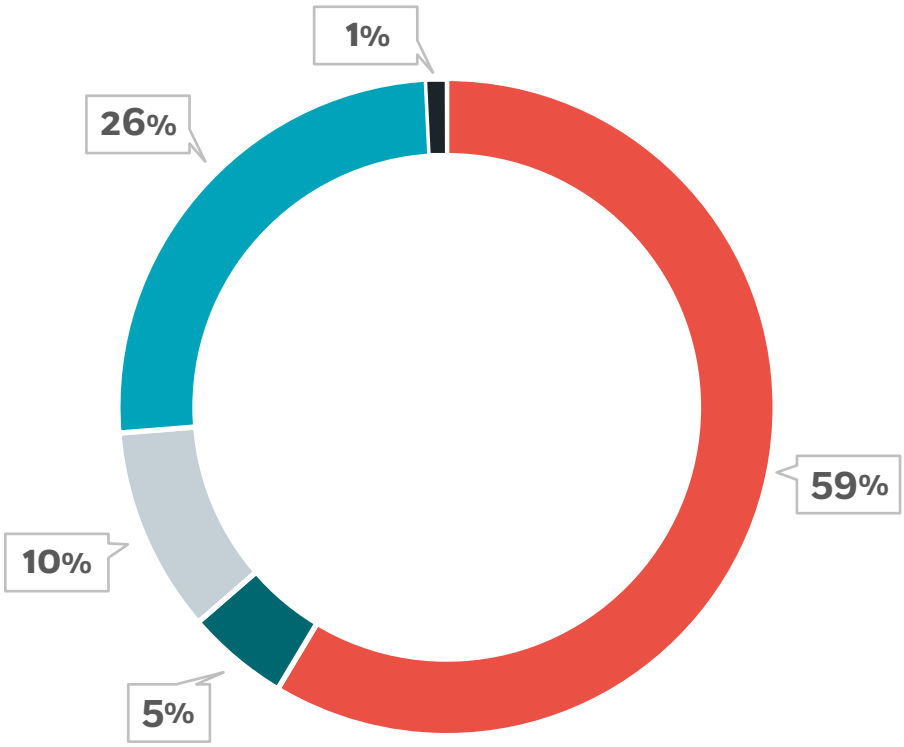
Privacy collaborates the most with IT but has branched out to other business functions.

6 Which of the following departments does your security team work most closely with?

	Currently	12-month projection
IT/technology	**59%**	**27%**
Information security	**28%**	**17%**
Digital business/ e-business/ e-commerce	**18%**	**14%**
Accounting/ finance/tax and revenue	**16%**	**6%**
Customer service, client service, or call center	**15%**	**11%**

Privacy and cybersecurity departments continue to collaborate primarily with IT.

7 Does your firm have a Chief Privacy Officer (CPO)?



- Yes
- No, but we have someone in an executive-level position who leads privacy efforts with a different job title
- No, but we have someone in a non-executive level position who leads privacy efforts
- No, we do not have someone in an executive level position who leads privacy efforts
- Don't know

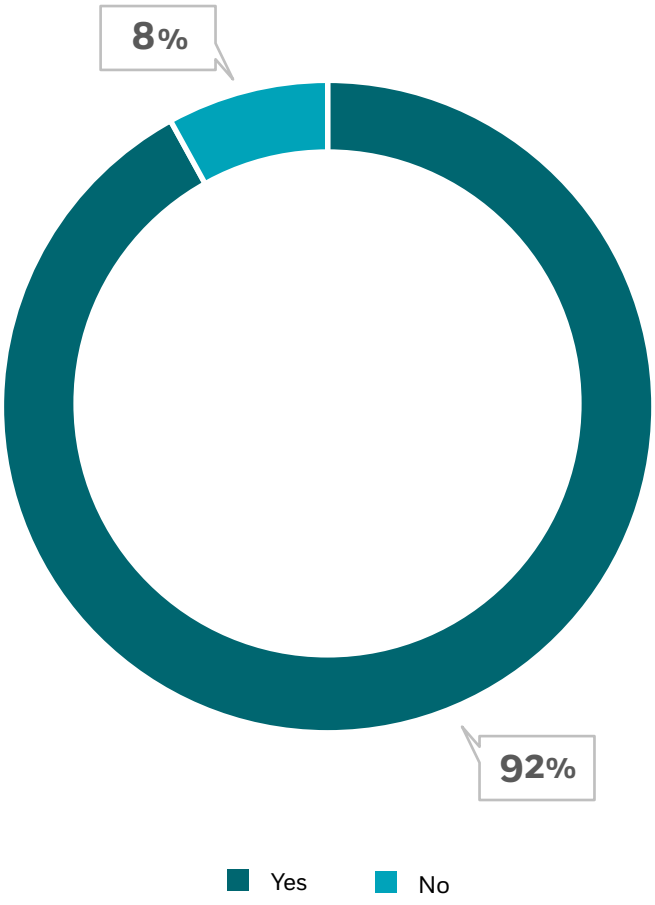
Appointing a CPO integrates privacy programs with business operations and innovation.

8 Into which of the following does the CPO or senior-most privacy decision-maker directly report?

Aligning privacy practices and cybersecurity is moving firms forward.

9

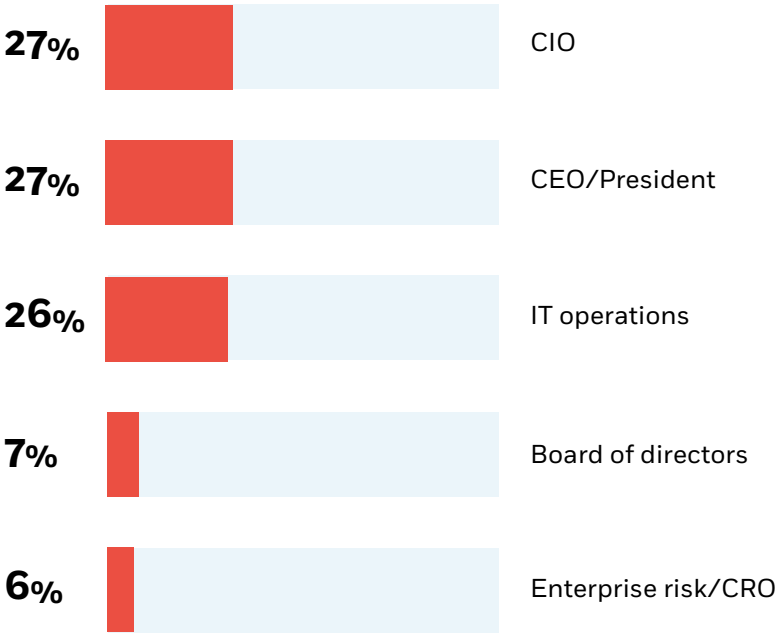
Does your firm have a Chief Information Security Officer (CISO) or Chief Security Officer (CSO)?



Integrating cybersecurity roles into the C-suite allows tech execs to build cybersecurity into a future-focused strategy.

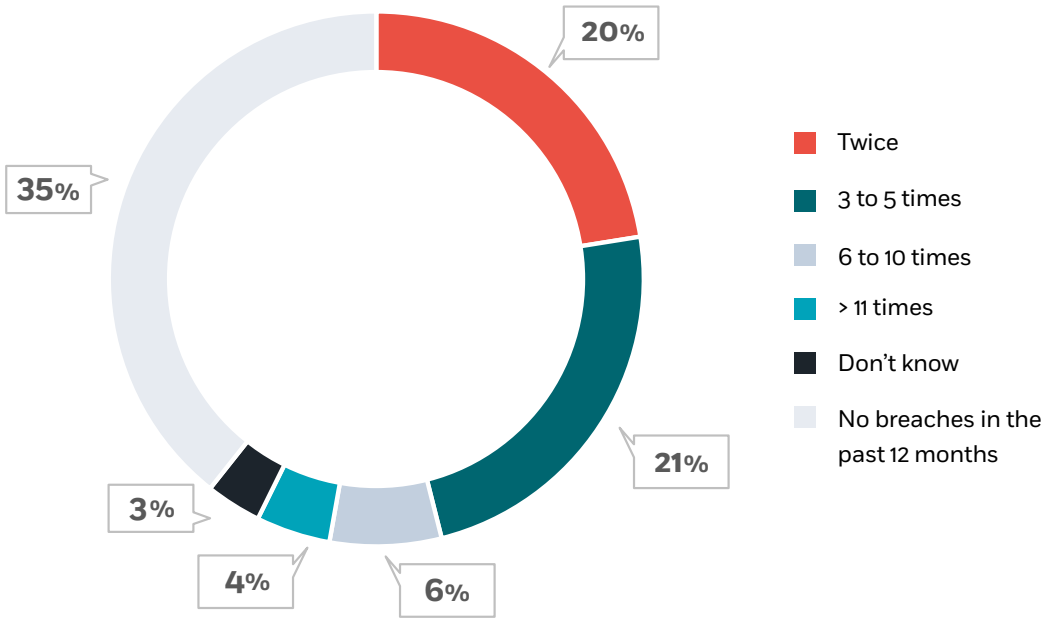
10

Who does the CISO, CSO, or senior-most security decision-maker directly report to?



CISOs or CSOs reporting to IT operations or CIOs have a tech-focused cybersecurity function.

11 How many times was your organization's sensitive data potentially compromised or breached in the past 12 months?

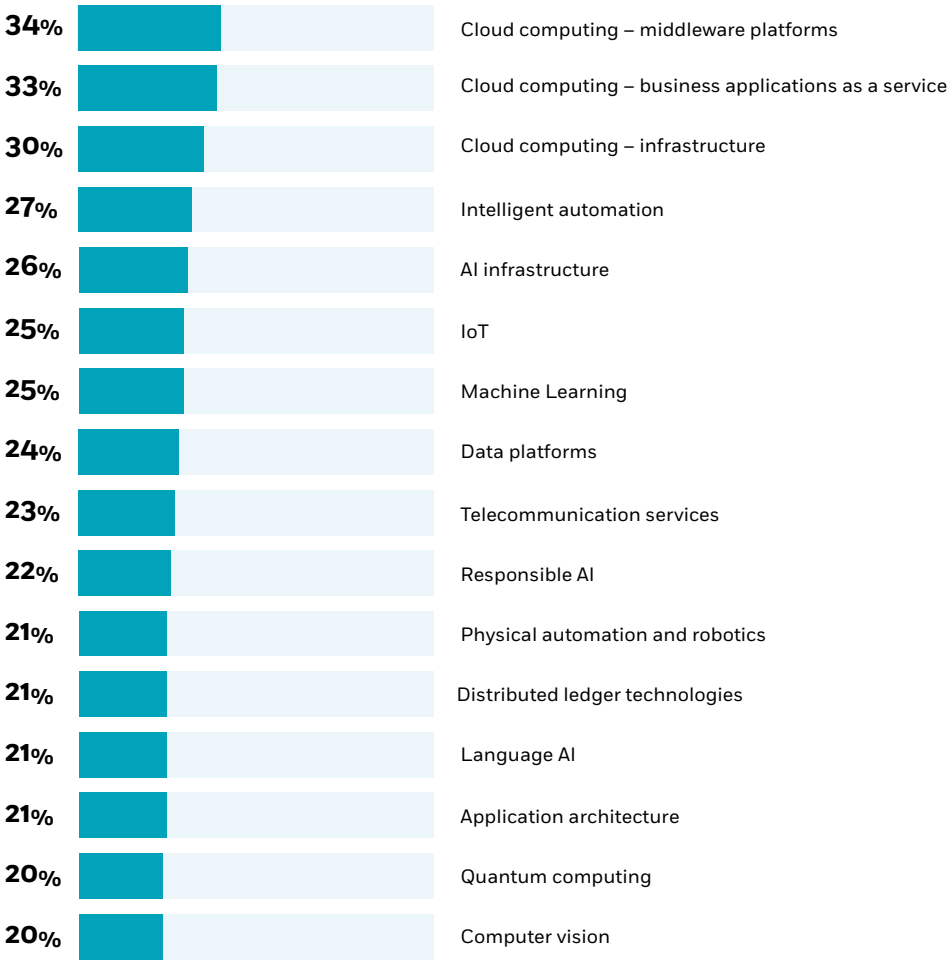


Respondents who had experienced a breach in the past 12 months attributed, on average, 29% of them to external attacks, 20% to internal incidents, 18% to a third-party incident, and 17% to lost or stolen assets.

35% of respondents who experienced an external attack attributed it to a software vulnerability exploit, 33% of a supply chain/third party breach, 32% to a web application exploit, 31% to phishing, and 30% to social engineering.

Diverse ranges of cyberattacks require creative response tactics.

Which technology categories are causing you the most concern because of the solutions that are emerging in them?



Emerging tech concerns for organizations are cloud adoption and data related.

The source for all data presented in this infographic is "The State Of Privacy And Cybersecurity, 2022", Forrester, September 8, 2022".