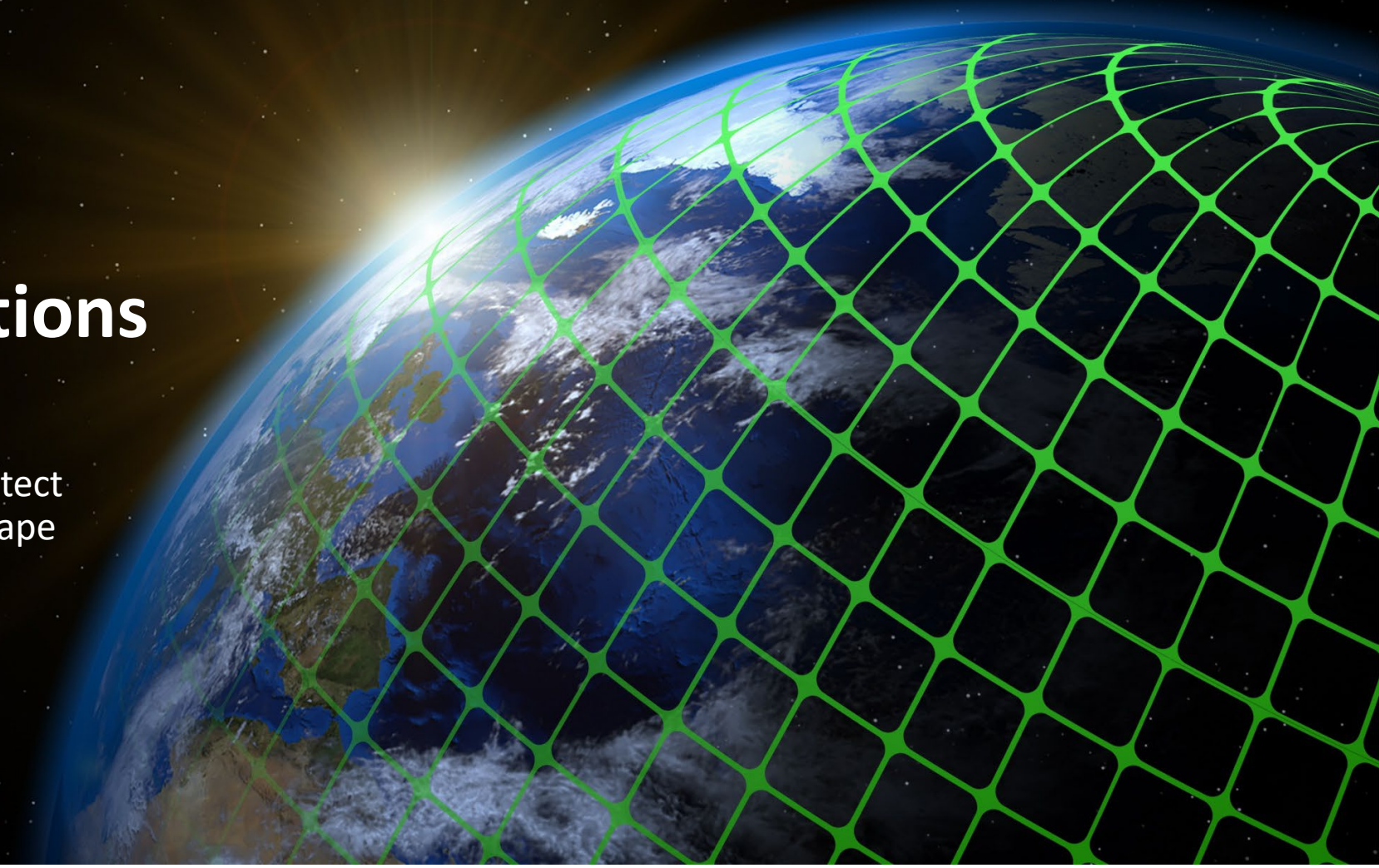
ThoughtLab

Cybersecurity Solutions for a Riskier World

How business and government can protect themselves in the emerging risk landscape

Executive Summary



Lead Sponsors

AXIS COMMUNICATIONS · Booz | Allen | Hamilton · CLAROTY · elastic · KnowBe4 Human error. Conquered. · securonix · SKYBOX SECURITY · VOTIRO · ZENKEY

Supporting Sponsors

CyberCube · servicenow

Introduction

Cybersecurity is at a critical inflection point. A confluence of events has brought the world to a watershed moment that will force businesses and governments to think differently about security in a risk landscape that has grown much more complex since ThoughtLab conducted its first cybersecurity study in 2018.

Cybersecurity is no longer just an IT issue: it is a strategic imperative for business and government. Yet many organizations are not prepared for what lies ahead. Their cybersecurity initiatives are not keeping pace with digital transformation, and their budgets are not growing as fast as the cyber risks they face.

Even worse, cybersecurity is still an imprecise science. Not all risk can be mitigated, transferred, or accepted; tradeoffs need to be made. Regulators, investors, and boards want to see progress. That requires evidence-based analysis that illuminates which approaches work best to mitigate risk. It also requires more rigorous benchmarking data to show how organizations are performing against cybersecurity frameworks like NIST and against their peers in their industry.

ThoughtLab has collaborated with a coalition of cybersecurity experts from leading companies, associations, and universities to fill this information gap. We worked together to answer a central question: How can organizations drive the best cybersecurity performance in a world of escalating digital risks?

To that end, we conducted a comprehensive benchmarking study from December 2021 to February 2022 covering the cybersecurity investments, practices, and performance results of 1,200 companies across 13 industries and the public sector in 16 countries. We also held peer group sessions and interviewed many cybersecurity experts from around the world.

Our research, released in May 2022, produced insights on how the most advanced entities in cybersecurity organize for success, where they invest, and which approaches around people, process, and technology deliver the best results. Crucially, the research draws on reported performance data and uses correlation analysis to show which efforts yield the best outcomes.

Lou Celi
Chief Executive Officer
ThoughtLab

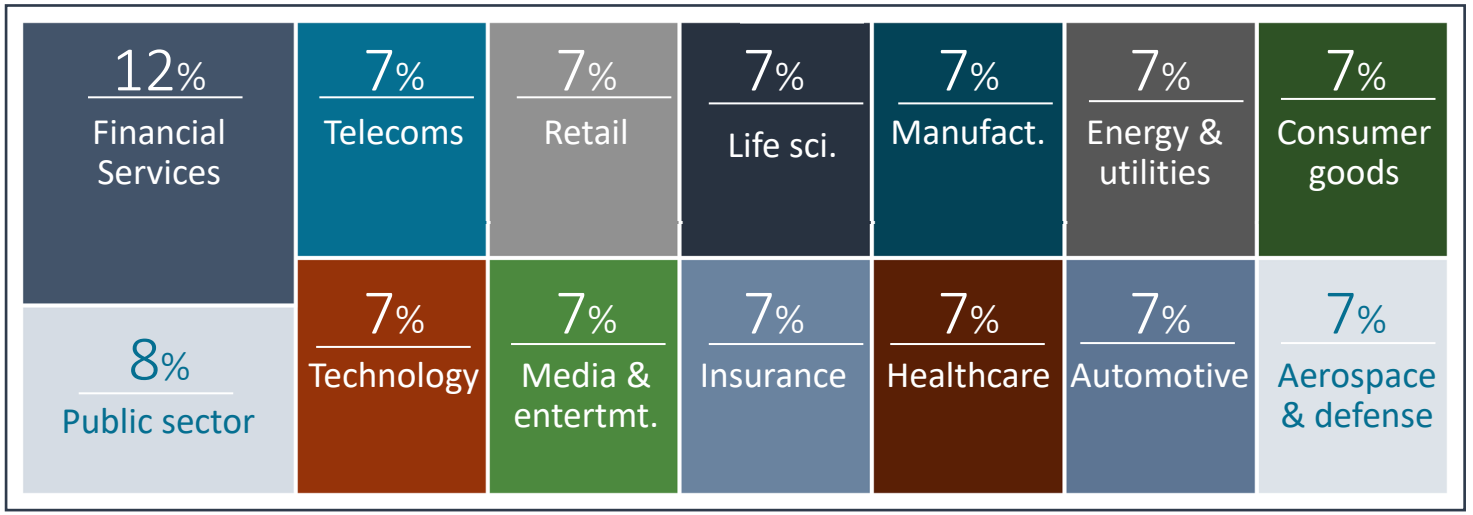
Anna Szterenfeld
Editorial Director and
Project Manager
ThoughtLab

Respondent profile

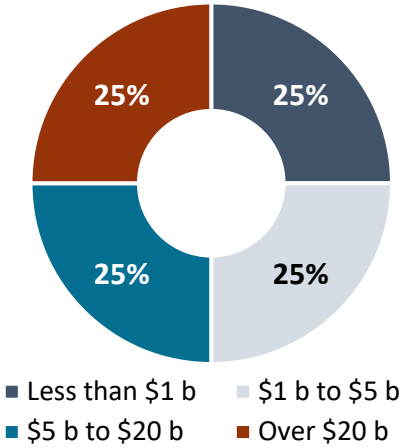
We surveyed 1,200 executives from four regions and 16 countries. We surveyed a range of C-Suite executives and some direct reports, all with some level of responsibility for cybersecurity. We conducted the survey using computer-assisted telephone interviews (CATI) to ensure accuracy and statistical rigor. Most of the organizations surveyed were large: three-quarters had revenue over $1 billion (average was $21.5 billion) and 55% had more than 10,000 employees (average 45,000). The executives hailed from 14 sectors, with the largest group from financial services firms.

Respondents by title	
Chief information security officer	10%
Report to one of C-level titles	9%
Chief executive officer/managing director	8%
Chief information officer	8%
Chief compliance/audit officer	8%
Chief operating officer	8%
Other C-level executive	8%
Chief risk officer	8%
Chief technology or digital officer	7%
Chief privacy or data protection officer	7%
Chief legal officer	7%
Chief security officer	7%
Chief security architect	7%

Respondents by industry



Respondents by revenue size



Countries surveyed	
Asia Pacific 33% Japan 8% | China/HK 8% | Australia 8% | India 4% | Singapore 4%	**Latin America 8%** Brazil 8%
Europe 33% France 10% | UK 8% | Germany 8% | Nordics 4% | Netherlands 4%	**North America 25%** US 17% | Canada 8%

The convergence of eight trends is ushering in a new era of risk

A confluence of eight megatrends has brought the world to a watershed moment that will require business and government leaders to think very differently about cybersecurity. As these developments converge, the cybersecurity landscape is becoming much riskier, more complex, and costlier to traverse.

1 Everything goes digital

The pandemic accelerated digital transformation of business, government, and social interaction.

2 Work becomes riskier

The rise of a remote or freelance workforce multiplies risks from the use of more devices outside corporate perimeters.

3 Organizations morph into ecosystems

Businesses and cities become elaborate networks of partners and suppliers as the platform economy takes shape.

4 Physical and digital worlds collide

Digitally connected physical assets expose strategic infrastructure to greater attack.

5 New technologies emerge

AI, IoT, multi-cloud, and 5G create cyber vulnerabilities for organizations and provide more advanced weapons for criminals.

6 Cyber adversaries up their game

Cybercrime becomes a bigger business through ransomware; threat actors become smarter, better organized, and more institutionalized.

7 Cyber warfare ushers in a new risk era

Russia's attack on Ukraine marks a new wave of geopolitical volatility, making cyber warfare a greater threat in the free world.

8 Regulations become more complex

Cybersecurity worries prompt a maze of new regulations around the world, from the US to the EU and to Asia.

Cybersecurity is at an inflection point for business and government

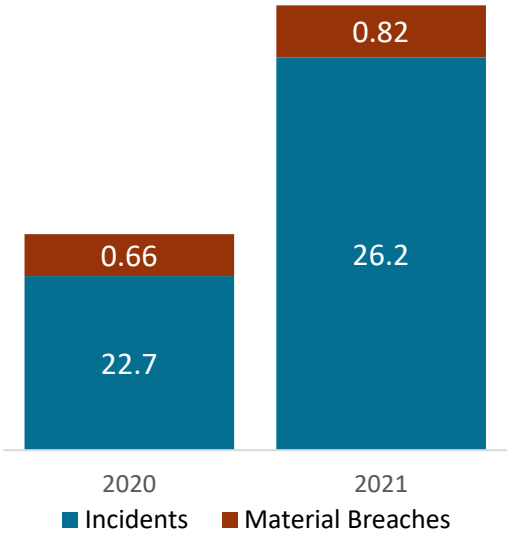
Cybersecurity is now at a turning point. Organizations are seeing an unprecedented rise in cyberattacks and making a step-change in cybersecurity investments and priorities.

The average number of attacks and breaches rose sharply in 2021—the number of incidents rose 15.1%, while the number of material breaches jumped 24.5%, according to our research. In fact, these figures may be underestimated because of the potential for organizations to fail to detect and to under-report attacks. Over the next two years, security executives expect an increase in attacks from social engineering and ransomware as nation-states and cybercriminals up their game. The root causes of these attacks will come primarily from four areas cited by executives: misconfigurations (49%), human error (40%), poor maintenance (40%), and unknown assets (30%).

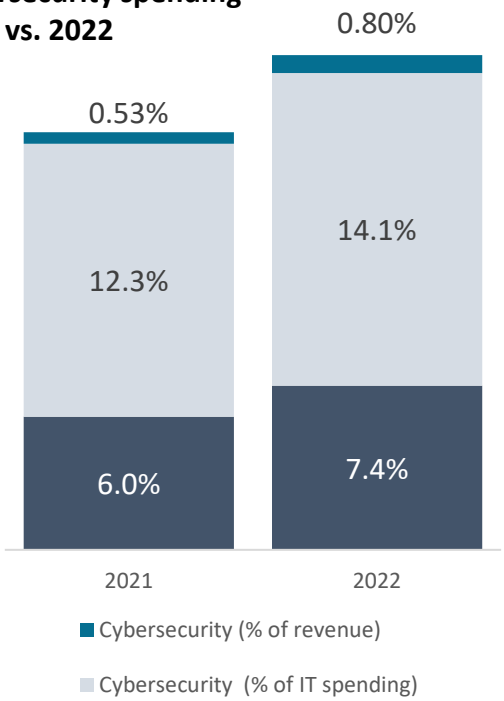
To keep up with digital transformation and attacks from adversaries, organizations are significantly boosting cybersecurity spending. From 2021 to 2022, cybersecurity budgets as a share of overall revenue are jumping 51%, from 0.53% to 0.80%—significantly higher than the average cybersecurity spending of 0.09% of revenue when we last conducted the study at the end of 2019. This cybersecurity budget will be 12-15% of overall enterprise IT spending in 2022—a doubling of the 5-7% that was considered the gold standard in the past. Cybersecurity spending on the cloud is also climbing as firms expand their use of cloud platforms and services.

Cybersecurity has moved from an IT issue to a core area of business risk and performance, requiring the vigilant attention of senior management and the board of directors. As organizations go digital, cybersecurity has become a strategic business imperative that requires the CEO, CIO, and other members of the C-Suite to work together to mitigate risks and meet the expectations of stakeholders. At the same time, the role of the chief information security officer (CISO) has expanded, with many taking on responsibility for data security (49%), customer and insider fraud (44%), supply chain management (34%), enterprise and geopolitical risk management (30%), and digital transformation and business strategy (29%).

Avg. incidents and breaches 2020 vs. 2021



Cybersecurity spending 2021 vs. 2022



> "Many organizations are what we often call target-rich, but resource-poor. They may be targeted by advanced adversaries, but can't always afford, at least in the needed timeframes, the controls and other mitigations needed."
>
> Security Magazine, March 10, 2022
>
> **Eric Goldstein, Executive Assistant Director**
> US Cybersecurity and Infrastructure Security Agency

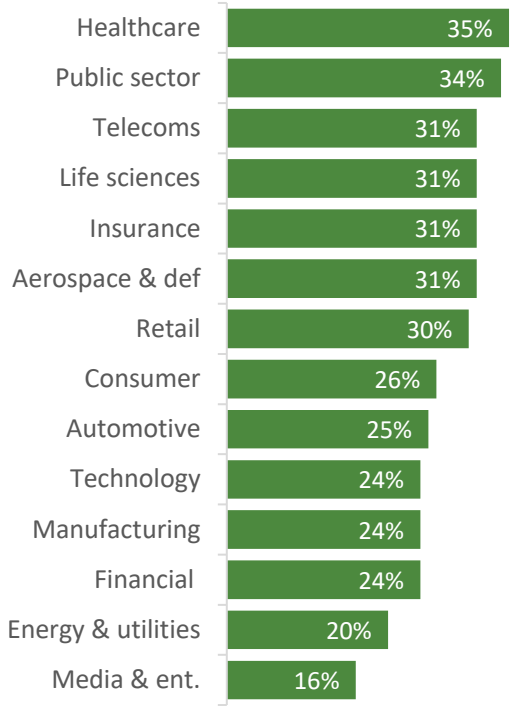
Yet many organizations are not well prepared for the risks ahead

More than a quarter of executives—and 4 in 10 chief security officers—say their organizations are not well prepared for the new threat landscape. Even more executives in critical industries, such as healthcare, aerospace and defense, public sector, and telecoms, say they are not ready for what lies ahead.

% saying their organizations are not well prepared for changing threat landscape, by title

All executives	27%
Chief Security Officers	40%
Chief Information Security Officers	29%
Chief Executive Officers	29%

% saying their organizations are not well prepared for changing threat landscape, by industry



44% of executives **> half** of CEOs, CIOs, COOs say their organization's growing use of partners and suppliers exposes them to a major cybersecurity risk.

41% of executives think that their cyber risk initiatives have not kept pace with digital transformation.

30% of executives **39%** of CEOs say they have inadequate budgets to ensure cybersecurity. **13%** say adversaries are better funded.

27% of executives say new technologies are their largest cybersecurity worry. In two years, the percentage will grow to **37%** of executives.

25% of respondents **34%** of CSOs believe that convergence of digital and physical systems, enabled by IoT, has increased the cyber risks that their organizations face.

24% of executives **36%** of CIOS see the shortage of skilled workers as their key cybersecurity challenge. **22%** cite ineffective training programs.

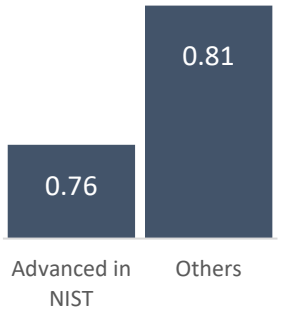
10 best practices to turbo-boost cybersecurity performance

Our evidence-based research revealed 10 best practices that can reduce the probability of incidents and material breaches or quicken the time to detect, respond to, and mitigate an attack.

1 Take cybersecurity maturity to the highest level

Organizations that are most advanced in applying the NIST cybersecurity framework outperform others on key metrics, such as number of material breaches, time to detect a breach, and time to mitigate.

Avg. # of material breaches in 2021



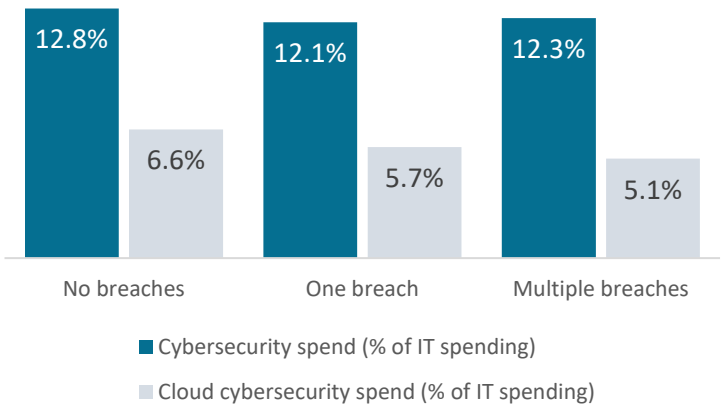
Metrics for organizations advanced in NIST vs. others

Metric	Advanced	Others	All
Time to detect a breach (days)	**118.9**	132.0	128.2
% of clients using multifactor authentication	**29%**	25%	26%
Time to get to 90% patched for external facing systems (days)	**48.8**	53.6	52.3
Time to respond to a breach (days)	**46.1**	47.7	47.1
Time to mitigate a breach (days)	**62.8**	64.6	63.9
# of times a year scan conducted on internet-facing infrastructure	**5.8**	4.7	5.0
Time after employee departs it takes to eliminate access (days)	**20**	22.7	21.8

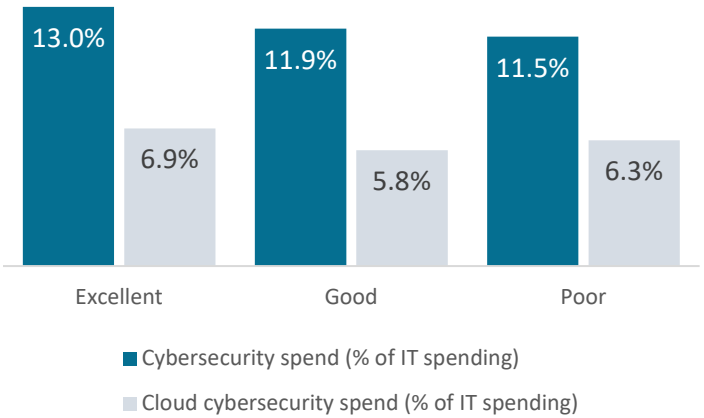
2 Ensure cybersecurity budgets are adequate

Our analysis found a clear correlation between investment and results. Respondents reporting no material breaches in 2021 spent an average of 12.8% of their IT budgets on cybersecurity, while those reporting multiple breaches spent 12.3% (a difference of $4.7 million given IT budgets averaged $946 million in 2021). Organizations that spent more also had better times to detect and mitigate.

Impact of cybersecurity spending on number of breaches in 2021



Impact of cybersecurity spending on time to detect in 2021

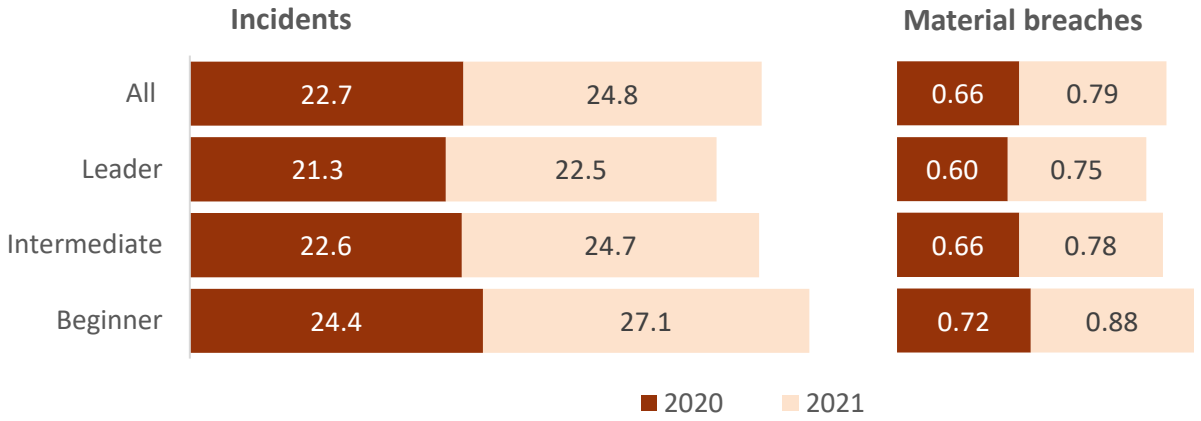


10 best practices to turbo-boost cybersecurity performance

3 Build a rigorous risk-based approach*

On average, leaders in risk-based management saw fewer incidents and material breaches than beginners in 2021 (22.5 incidents and 0.75 material breaches for leaders vs. 27.1 incidents and 0.88 material breaches). Over 4 out of 10 risk-based leaders embrace Zero Trust principles.

Performance by risk-based approach progress*



4 Make cybersecurity people-centric

Cybersecurity is as much about humans as it is about technology. Organizations see fewer breaches and faster times to respond when they build a human layer of security, create a culture sensitive to cybersecurity risks, provide more effective training, and develop clear processes for recruiting and retaining cyber staff.

Build human-layer security by assessing staff behaviors

39% with excellent times to detect invested in securing the human layer vs. **29%** with poor times.

48% with excellent times to respond invested in securing the human layer vs. **38%** with poor times.

Create a culture attuned to cybersecurity values and risks

22% of organizations that have invested in cybersecurity culture said it was one of their most effective initiatives.

37% of organizations with excellent times to respond have invested in culture vs. **35%** with poor times.

Build more effective cybersecurity awareness and training

38% of organizations that had no breach are advanced in awareness and training vs. **29%** with multiple breaches.

50% that had excellent times to respond are advanced in awareness and training vs. **25%** that have with poor times to respond.

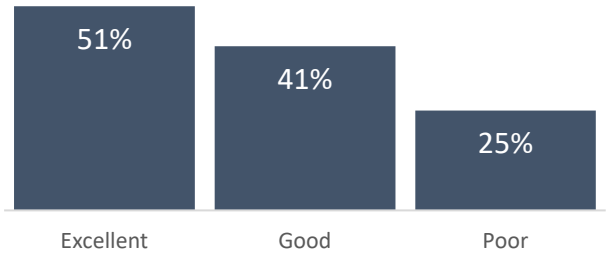
* Elements of risk-based approach: attack surface visibility and context, attack simulation, exposure analysis, vulnerability assessments, research, risk scoring, technology assessment and consolidation, risk assessment, risk management strategy, and supply chain risk management.

10 best practices to turbo-boost cybersecurity performance

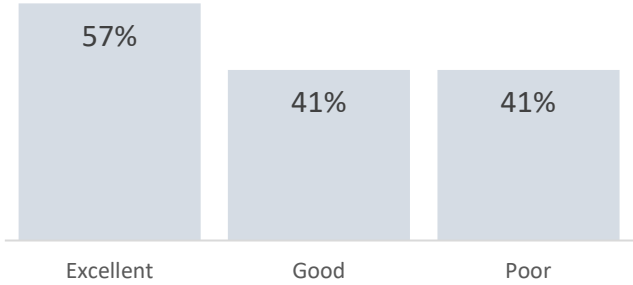
5 Secure the supply chain

For 44% of respondents, the growing use of suppliers is exposing them to major cybersecurity risks. Top performers in time to detect, respond, and mitigate are far more mature in supply chain security. For example, over half of organizations with excellent times to detect are advanced in supply chain security vs. 25% of those with poor times to detect.

Time to detect: % advanced in supply chain management.



Time to mitigate: % advanced in supply chain management



6 Draw on latest technology, but avoid product proliferation

Organizations with no breaches invest in a variety of technologies, from the fundamentals such email security and identity management, to more specialized solutions such as cloud access security brokers, cyber risk models, and SIEMs. Security leaders are more likely to take a multi-layered, multi-vendor approach to monitor and manage risks better through a strong infrastructure. They also favor consolidation over product proliferation: 35% with no breaches consolidate infrastructure and tools vs. 28% with multiple material breaches.

Top 10 investments by firms with no breaches
1 Email security
2 Distributed DOS protection
3 Cloud access security broker
4 Network security policy management
5 Identity and access management
6 Mobile device management
7 Cyber risk modeling and assessment
8 End-point detections and response
9 Security information and events management
10 Secure access service edge

35%
of organizations with no breaches are planning to accelerate how they consolidate tools and infrastructure vs. **28%** of those with multiple material breaches.

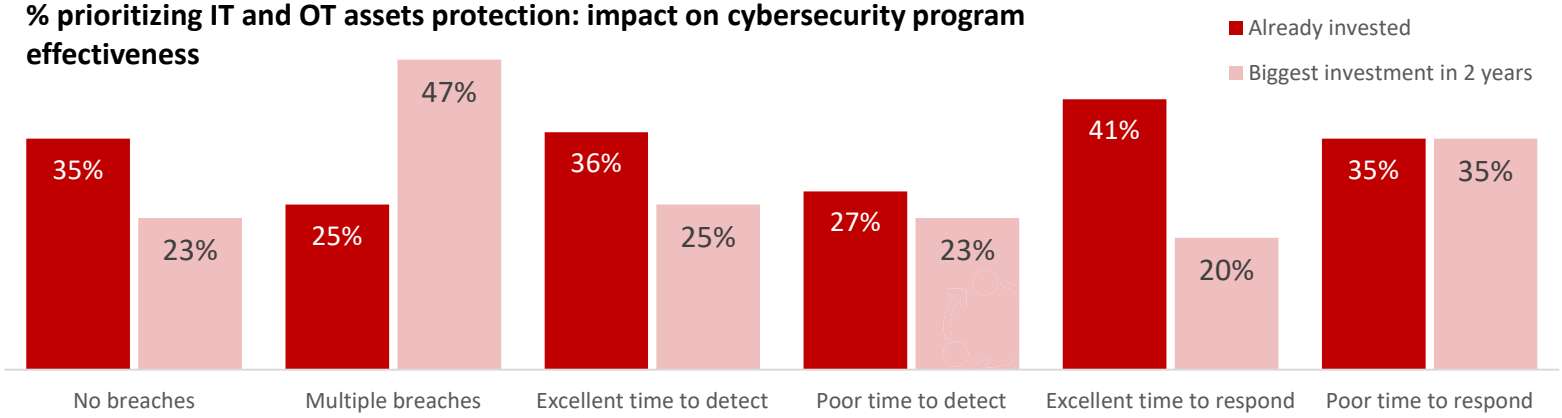
31%
of organizations advanced in NIST adopt security technologies providing a set of capabilities as a "platform" vs. **24%** of NIST beginners.

10 best practices to turbo-boost cybersecurity performance

7 Prioritize protection of linked IT and OT assets

With digital and physical worlds converging, the attack surfaces for respondents are widening. Organizations that prioritize protection of interconnected IT and OT assets experience fewer material breaches and faster times to detect and respond. For example, 36% of top performers in time to detect have invested in prioritizing IT and OT asset protection vs. 27% of poor performers.

% prioritizing IT and OT assets protection: impact on cybersecurity program effectiveness



8 Harness intelligent automation

Automation, combined with AI and machine learning, helps CISOs deliver results while freeing up staff from mundane tasks. For example, about 3 out of 10 organizations with excellent dwell times use smart automation vs. 17% of organizations with poor dwell times.

29%
of organizations with excellent dwell time performance use AI and ML vs. **17%** of those with poor dwell time.

22%
of the top performers in time to mitigate use AI and ML against **17%** of those with poor time to mitigate.

% of respondents agreeing

Statement	All	Advanced in NIST	Other
We use advanced analytics such as AI and ML to identify security vulnerabilities or threats.	26%	28%	25%

10 best practices to turbo-boost cybersecurity performance

9 Improve controls for expanded attack surfaces

Attack surfaces widened during the pandemic. Yet multiple metrics tracked by respondents show insufficient use of security controls. For example, only 26% of the respondents' clients now use multifactor authentication, and the percentages of servers with MFA are even lower (23%). Only 31% of users are monitored by user behavior analytics.

Metrics tracked

Metrics	Average	Bottom performer
% business-critical systems or datastores covered by backups	59%	Retail (49%)
% business-critical systems monitored internally or by third party	31%	Aerospace & def (27%)
% users monitored by user behavior analytics, such as via SIEM	31%	Automotive (20%)
% clients using multifactor authentication	26%	Manufacturing (20%)
% servers using multifactor authentication	23%	Insurance, tech, life sciences (20%)
% end user end points sending logs to a common data repository	21%	Aerospace, life sciences, retail (18%)
% cloud services sending logs to a common data repository	18%	Healthcare and retail (15%)
% systems not covered by vulnerability scans	7%	Manufacturing (6%)

10 Do more to measure performance

Currently organizations just track four to five metrics on average. Security leaders and executive teams that are more assiduous—monitoring six or more metrics—experience fewer incidents and material breaches. They also respond faster to attacks.

Average number of attacks by number of metrics tracked

Year	Attacks	Fewer than 6 metrics tracked	6 or more metrics tracked	All
2020	Incidents	23.38	20.58	22.73
2020	Material breaches	0.675	0.604	0.658
2021	Incidents	25.32	23.05	24.80
2021	Material breaches	0.811	0.734	0.793

Our coalition

Lead sponsors

AXIS COMMUNICATIONS

CLAROTY

elastic

KnowBe4 Human error. Conquered.

securonix

SKYBOX SECURITY

VOTIRO

ZENKEY

Supporting sponsors

CyberCube

servicenow

RESOLUTE. STRATEGIC SERVICES

Global consulting sponsor

Booz | Allen | Hamilton®

Association partners

INTERNET SECURITY ALLIANCE

ISF

ThoughtLab

ThoughtLab is an innovative thought leadership and economic research firm providing fresh ideas and evidence-based analysis to help business and government leaders cope with transformative change. We specialize in analyzing the impact of technological, economic, and demographic shifts on industries, cities, and companies.

To learn more about ThoughtLab, visit: **www.thoughtlabgroup.com**

For further information about this study, please contact:

Lou Celi, Chief Executive Officer
louceli@thoughtlabgroup.com

Anna Szterenfeld, Editorial Director
annaszterenfeld@thoughtlabgroup.com

Laura Garcell, Associate Editor
lauragarcell@thoughtlabgroup.com