ThoughtLab

Cybersecurity Solutions for a Riskier World

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

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—the pandemic's acceleration of digital transformation, cloud adoption, and remote work; the rise of advanced technologies that interconnect assets and introduce new vulnerabilities; the emergence of new business ecosystems that expose companies to insidious risks outside their corporate perimeters; and a huge increase in cybercrime and nation-state-sponsored attacks—heightened by the war in Ukraine—have brought the world to a watershed moment that will force businesses and governments to think differently about security.

The risk landscape 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 and now a core area of risk. 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 collaborated with a coalition of cybersecurity experts from leading companies, associations, and universities to fill this information gap. We sought to answer a central question: How can organizations drive the best cybersecurity performance in an era 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 discussions and interviewed cybersecurity experts from around the world.

This eBook, released in May 2022, provides valuable quantitative insights from our research. It examines how cybersecurity leaders organize for success and which investments in people, process, and technology deliver the best results. It analyzes the cybersecurity steps they are taking to be more risk-ready, human-centric, risk-based, and digitally enabled. Crucially, it draws on reported performance data and uses correlation analysis to show which efforts yield the best outcomes.

We would like to thank our sponsors for funding this important research initiative as well as the corporate executives and academic experts who provided their valuable time and insights to produce this ground-breaking report. We would also like to thank Dr. Daniel Miles, director at Hatch, for conducting the performance impact analysis that enriched our findings and led to our conclusions.

We hope that this robust analysis will make an important contribution to the world by helping business and government leaders optimize their cybersecurity resources to succeed in today's new era of risk.

Lou Celi
Chief Executive Officer
ThoughtLab

Anna Szterenfeld
Editorial Director and
Project Manager
ThoughtLab

"This research was conducted by a diverse team of talented professionals with varying backgrounds and perspectives, rendering the panel effectively unbiased. Based on straightforward data, the analysis identified areas in which cybersecurity investments seem to be paying off, by reducing the number of material breaches and the time needed to detect and respond to them. The study shows clearly that, while cybersecurity is a growing serious problem, we know how organizations might address it."

Joseph Steinberg
Cybersecurity Expert Witness, Advisor, and Columnist

1. Research background

Sample profile

We surveyed 1,200 executives from four regions and 16 countries. Respondents were pre-screened to ensure they had full or partial responsibility for cybersecurity in their organizations. We conducted the survey using computer-assisted telephone interviews (CATI) to ensure accuracy and statistical rigor. Most of the companies surveyed were large: three-quarters had revenue over $1 billion (the average was $21.5 billion) and 55% had more than 10,000 employees (average 45,000). Our sample represents organizations that spend over $125 billion annually on cybersecurity, a substantial portion of the world total (forecast at $150.4 billion by Gartner for 2021).

Countries surveyed

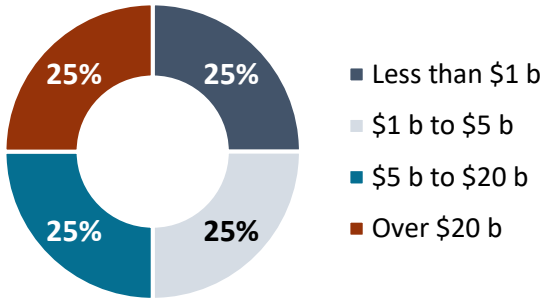
Asia Pacific 33%
Japan 8% | China/HK 8% | Australia 8%
India 4% | Singapore 4%

Latin America 8%
Brazil 8%

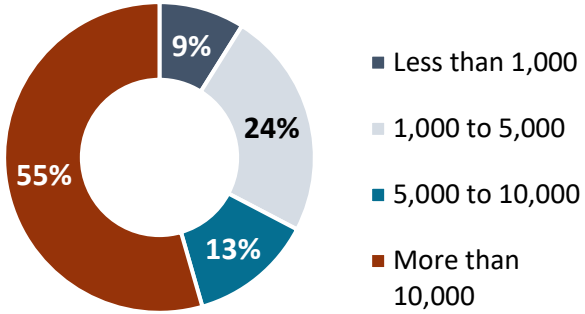
Europe 33%
France 10% | UK 8% | Germany 8% |
Nordics 4% | Netherlands 4%

North America 25%
US 17% | Canada 8%

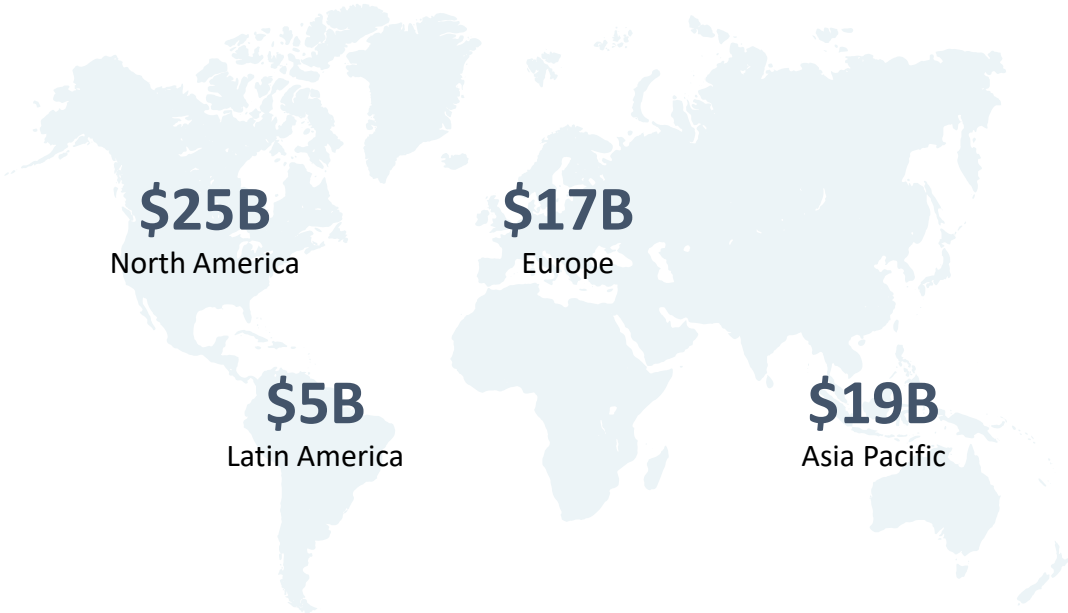
% respondents by revenue size



% respondents by employee numbers



Average respondent revenue size by region



Total annual cybersecurity spending

of all organizations in the sample:

$125.2B

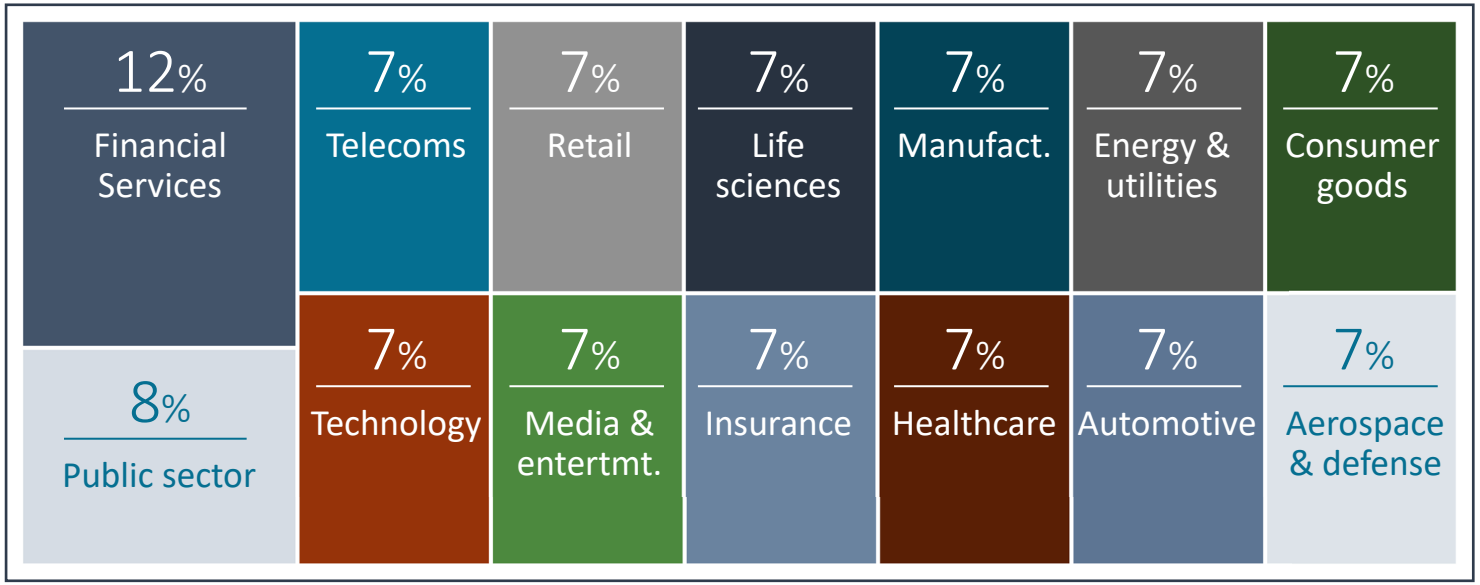
Industries and respondent profile

We surveyed a range of C-Suite executives and some direct reports, all with some level of responsibility for cybersecurity. Of those, 21% reported having overall responsibility, 36% were responsible for some areas of cybersecurity, and 43% said they were part of a cyber risk management team.

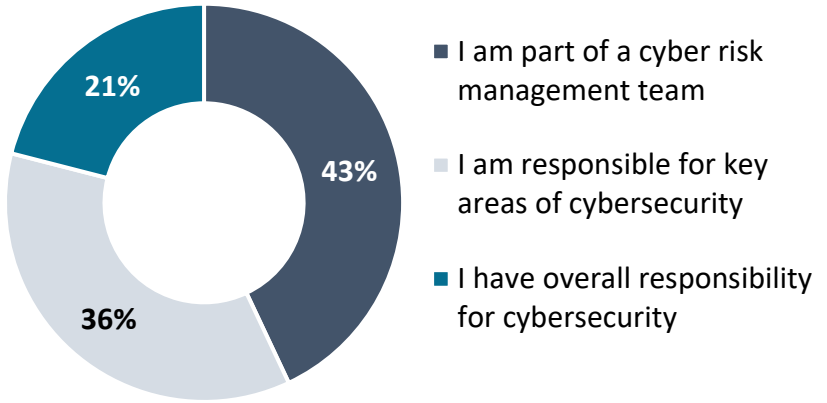
The executives hailed from 14 sectors, including the public sector, with the largest group from financial services firms.

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 cybersecurity responsibility



NIST maturity methodology

Our economists used the NIST framework to gauge the level of progress organizations have made in cybersecurity. Security executives surveyed rated their own progress in the five categories prescribed by NIST, which are common to other cybersecurity frameworks: identify, protect, detect, respond, and recover.

We asked respondents to rate their degree of progress as Levels 1-5 in the 23 activities that fall under the NIST pillars. Our economists averaged the scores for each underlying activity to arrive at a score for each NIST area. They then averaged the total scores for the NIST areas to arrive at the overall score for each respondent. The scores were normalized to provide a range between 0-100. Respondents were grouped into three stages of NIST implementation: those with average scores under 50 were categorized in the **early implementation** stage, those with scores of 50 to 70 in **mid-implementation**, and those with scores greater than 70 were categorized in the **advanced implementation** stage.

Identify	Protect	Detect	Respond	Recover
Asset management	Awareness & training	Anomalies & events	Analysis	Communications
Business environment	Data security	Continuous security monitoring	Communications	Improvements
Governance	Identity management & access control	Detection processes	Improvements	Recovery planning
Risk assessment	Information protection processes & procedures		Mitigation	
Risk management strategy	Maintenance		Response planning	
Supply chain risk management	Protective technology			

Our economists calculated scores for each respondent based on a ranking of 1 to 5 for progress made in each underlying NIST activity. Levels of progress for NIST were defined as:

Level 1:
Undefined
Starting to think about this. No plans in place.

Level 2:
Ad hoc
Beginning to put plans and processes in place. Taking action but not consistently.

Level 3:
Defined and repeatable
Have defined processes and plans. Making progress but not fully aligned with the business yet.

Level 4:
Managed
Continuous monitoring, with metrics in place, and seeing considerable benefits.

Level 5:
Optimized
We have fully acted on this activity. We are ahead of most of our peers and seeing significant benefits.

Stages of maturity against NIST framework

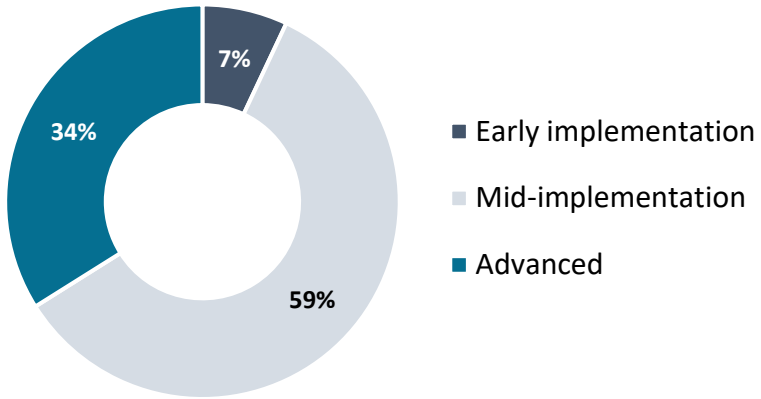
Based on our NIST maturity framework, 7% of organizations in our sample are in early implementation, 59% are in mid-implementation, and 34% are advanced.

The average score for early implementers was 46.5, for mid-implementers 62.4, and for advanced implementers 78.6 (out of a potential maximum score of 100).

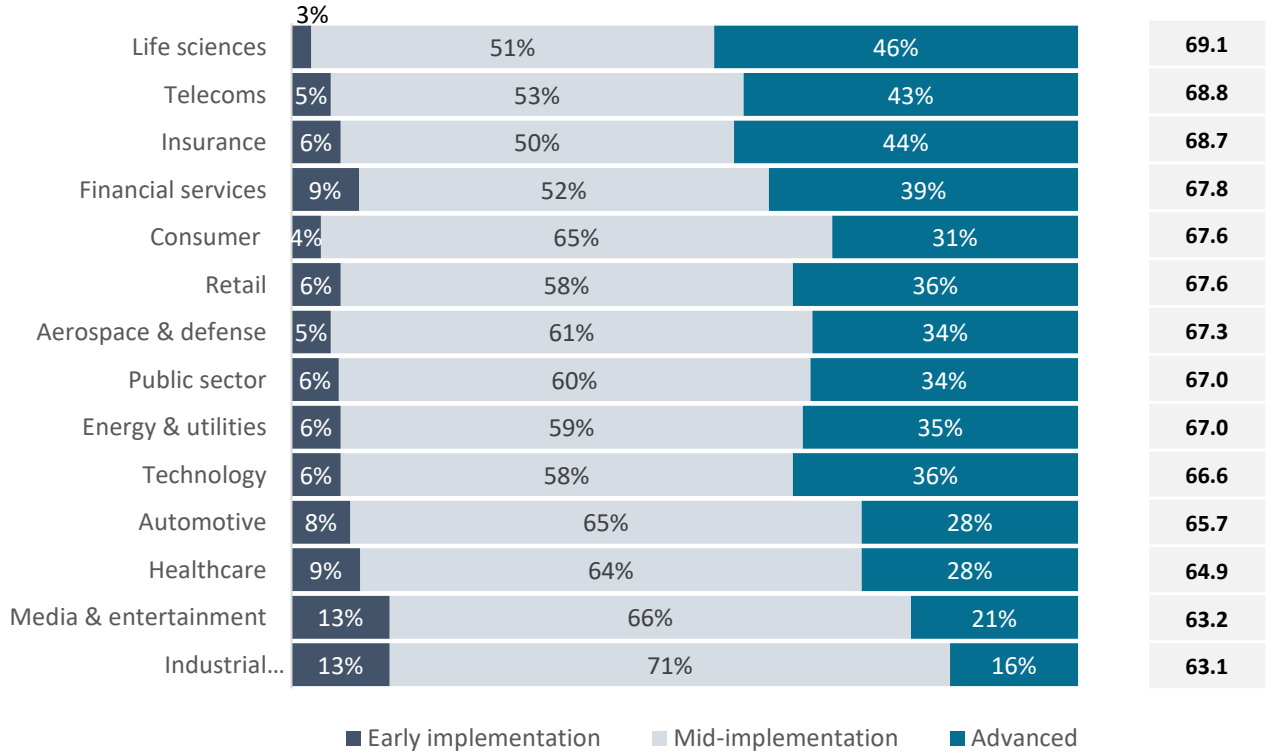
To get a view of which industries and regions are making the most progress within the NIST framework, we also calculated their average NIST maturity scores. The average score across industries was 66.8, indicating that compliance with maturity frameworks like NIST is still a work in progress.

On this basis, life sciences, telecoms, and insurance are the most mature industries in implementing the NIST framework, while industrial manufacturing, media and entertainment, and healthcare are the least. North America is the most mature region, while Latin America is furthest behind.

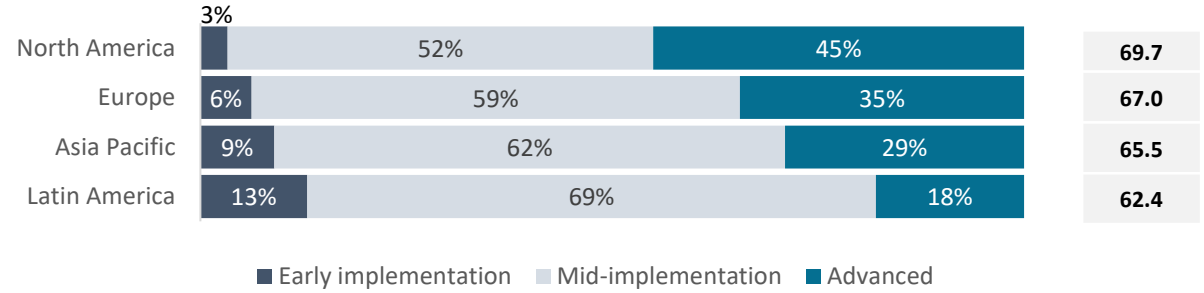
Respondents by NIST stages



Maturity by industry



Maturity by region



Progress on risk-based approach

To take cybersecurity to the next level, many organizations are implementing a risk-based focus to cybersecurity on top of their maturity approach. We asked respondents to rate their progress from 1-5 on seven key areas of risk-based management.

Attack surface visibility and context	**Vulnerability assessments**	**Technology assessments and consolidation**
Attack simulation	**Research**	
Exposure analysis	**Risk scoring**	

Stages of progress for risk-based management were defined as follows:

Stage 1: Starting—Developing and starting process

Stage 2: Early—Process in early implementation

Stage 3: Intermediate—Halfway through implementation

Stage 4: Mature—Three-quarters of the implementation completed

Stage 5: Advanced—Implementation completed/nearly completed

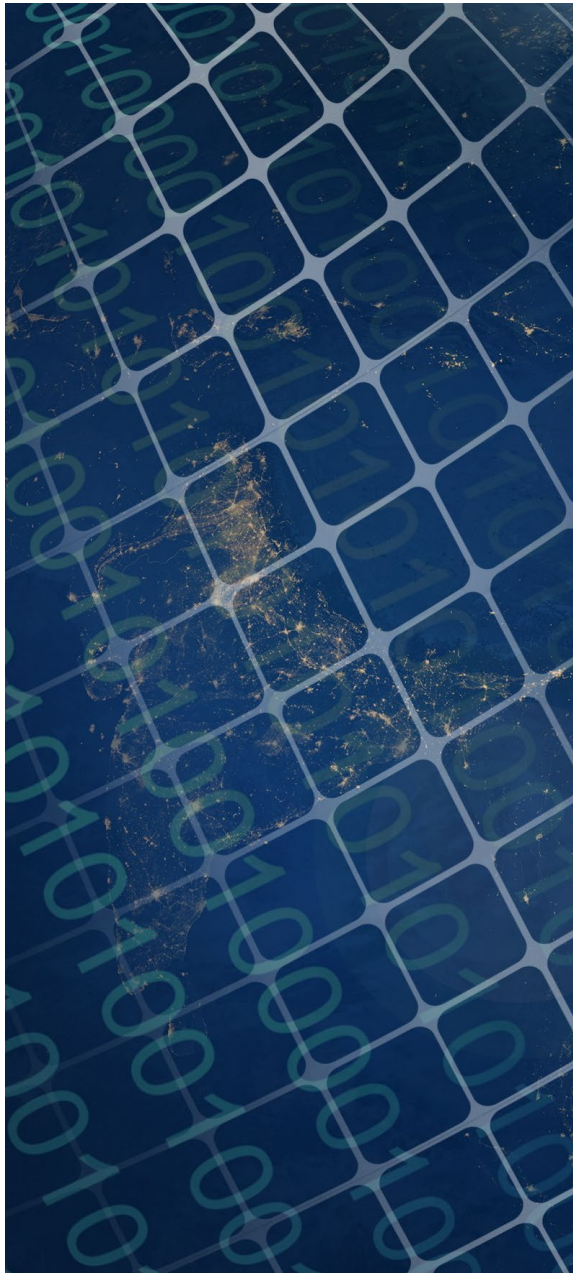
1 2 3 4 5

Risk-based maturity scores
Beginners: Up to 37 | Intermediates: 37-54 | Leaders: Over 54

Other risk factors measured in risk-based approach

To ensure the rigor of our risk-based framework, we also incorporated the progress that respondents have made on risk assessment, risk management strategy, and supply chain risk management as prescribed by the NIST framework. In addition, we adjusted our rankings to reflect their investments in conducting regular risk assessments, audits, stress tests, and penetration tests, as well as investments in cyber risk modelling and assessment platforms.

We then normalized our risk-based maturity rankings to provide an overall score range between 0 and 100. The average score for all respondents was 45.4, and the scores ranged from 15.0 to 91.0. We assigned each respondent to one of three groups: beginner, intermediate, and leader. Respondents with a score below 37 were classified as beginners in using a risk-based approach, those with a score greater than 54 were classified as leaders, and the remainder were classified as intermediates.



Stages of progress against a risk-based framework

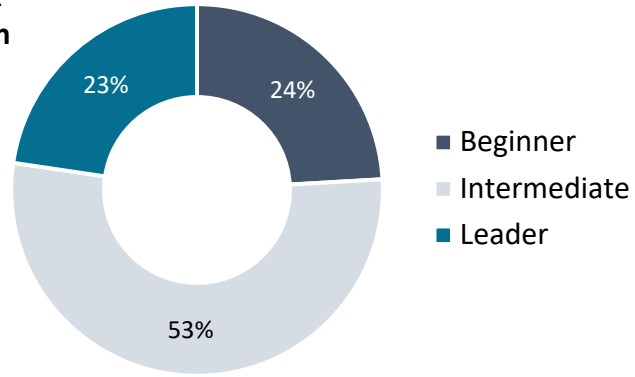
Against our risk-based framework, 24% of organizations in our sample qualified as beginners, 53% as intermediates, and 23% as leaders.

The average score for beginners was 30.1, for intermediates it was 45.4, and for leaders 61.6 (out of a potential maximum score of 100).

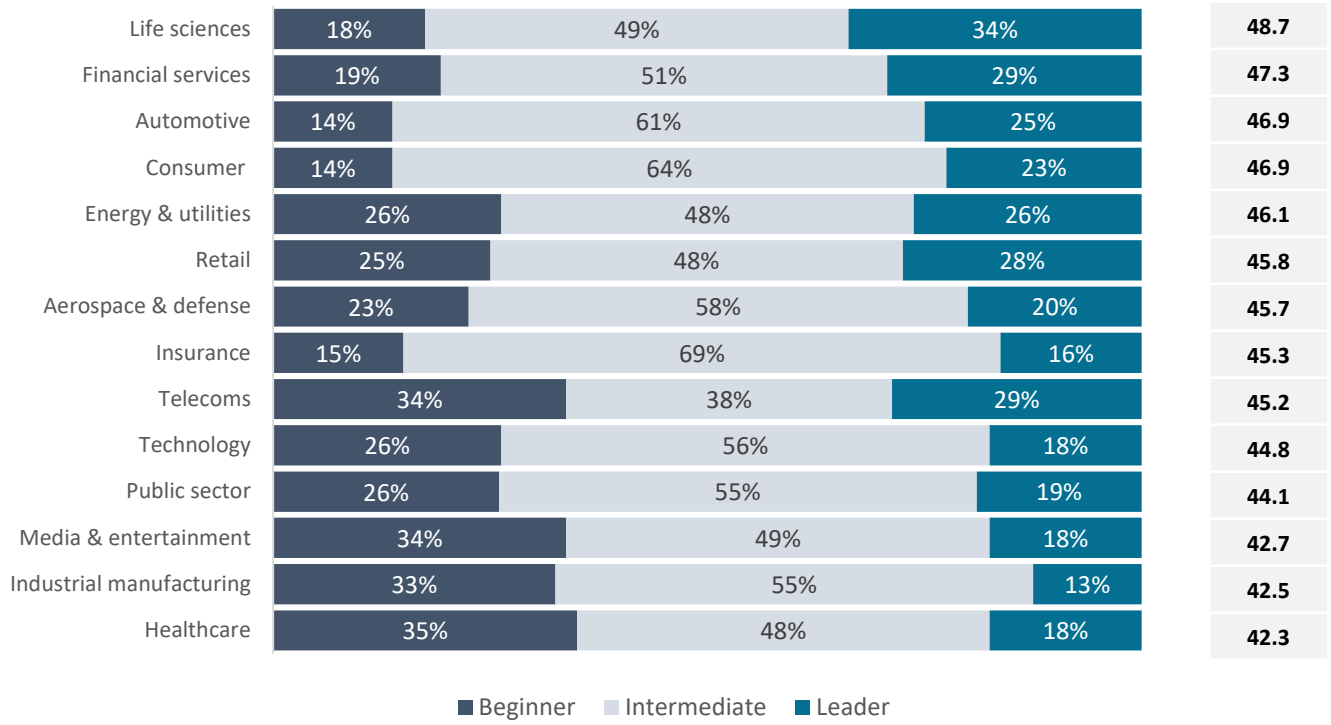
To get a view of which industries and regions are making the most progress in this area, we also calculated their average maturity scores. The average score across industries was 45.4. The scores ranged from 42.3 to 48.7.

On this basis, life sciences, financial services, and automotive are the most mature industries in utilizing a risk-based framework, while healthcare, manufacturing, and media and entertainment are again the least mature. As with the NIST maturity rankings, North America is the most mature region, while Latin America is the furthest behind.

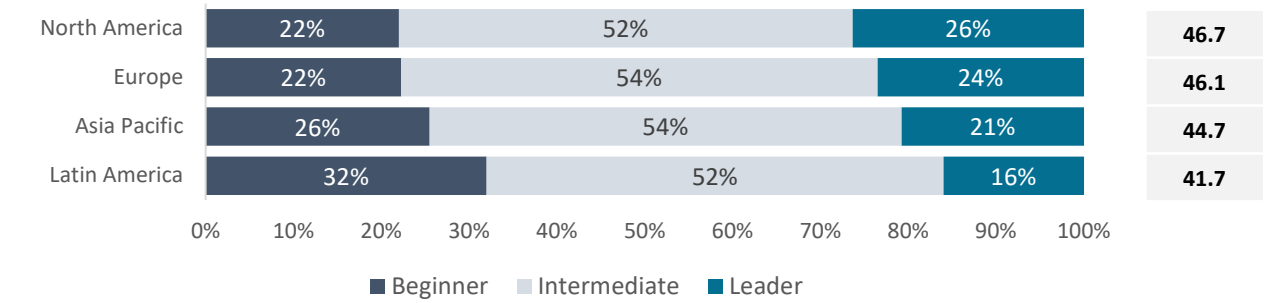
Respondents by maturity in risk-based approach



Maturity by industry



Maturity by region



Performance impact analysis

To identify the cybersecurity practices that deliver the best outcomes, our economists conducted rigorous performance impact analysis. As part of this analysis, we correlated a variety of cybersecurity activities with performance measurements supplied by respondents. These performance indicators included:

- **Number of material breaches in 2021.** Material breaches were defined as those generating a large loss, compromising many records, or having a significant impact on business operations. The number of material breaches were grouped into three categories: none, one, or multiple.
- **Time to detect.** The average amount of time it currently takes the cyber team to detect incidents in their environment.
- **Time to respond.** The average amount of time it takes the team to respond to a breach when it occurs.
- **Time to mitigate.** The average amount of time from the initial customer impact to resolution.
- **Dwell time.** The average amount of time that a threat actor has undetected access, including the time to detect and remediate.

For the metrics based on time, we classified performance into three categories: excellent, good, and poor. Excellent corresponds to results in the top 25th percentile of responses, good to results in the 50th to 75th percentile, and poor to results in the bottom 25th percentile.

Activities correlated with performance

Our economists correlated cybersecurity performance against a broad set of **best practices** under NIST as well as people, process, and technology investments. See the list of practices on the right.

- NIST maturity
- Level of cybersecurity spending
- Use of Zero Trust principles
- Human-centric security and training
- Skills acquisition and development
- Team-based C-Suite approach
- Progress on risk-based management
- Number of staff on cybersecurity teams
- Progress on third-party risk management
- Use of outsourcing
- CISO — Role of CISO
- SIEMs — Use of security information and event management systems

> “We don’t know what tomorrow’s threat will be, anything from another wave of the pandemic or something totally different, such as negative outcomes arising from geopolitical tensions in Russia and Ukraine.”
>
> **Curley Henry, Vice President, Deputy CISO Southern Company**

2. The cybersecurity landscape

Cybersecurity is at a critical inflection point

Our in-depth study of 1,200 worldwide organizations across 14 industries revealed that cybersecurity is at a major turning point. Eight mutually reinforcing megatrends are making the cybersecurity landscape riskier, more complex, and costlier to manage. Cybersecurity has moved from an IT issue to a core area of business risk and performance management, requiring the vigilant attention of senior executives and the board of directors.

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 big 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 Asia.

Experts see a step-change in cyber risks

Executives agree that we have entered a new era of cyber risk. In this new phase, organizations will need to take their cybersecurity approach to the next level by making it more risk-based, human-centric, team-managed, well-funded, and fully aligned with the business. Governments will need to take a more active role.

Everything goes digital

"Attack surfaces grew significantly during the pandemic. Accelerated digital transformation, cloud migration, and increased remote working all contributed to this growth."

Gidi Cohen, CEO and Founder Skybox Security

Work becomes riskier

"The balance between the office and remote work will not return to previous norms. Enterprises will have to make employees and data as secure when they are home as they are behind the firm's firewall."

Darren Thomson, Head of Cyber Intelligence Services CyberCube

Cyberwarfare creates new threats

"Geopolitical issues present a whole different level of risk to all industry verticals. It's incumbent upon us all to understand those risks and the threat actors behind them and to ensure we've taken all steps necessary to protect our company's computing and data assets."

Deborah Wheeler, CISO Delta Air Lines

Cyber adversaries up their game

"Companies are vastly over-matched by the growing sophistication of criminal syndicates accessing increasingly sophisticated attack methods and technologies."

Larry Clinton, President and CEO, Internet Security Alliance

Regulations become more complex

"As cyberattacks grow in scope and scale, the government is taking a more active role in defining and prescribing new security regulations. In addition, data privacy laws are becoming more rigid and complex. In already regulated sectors, the requirements are increasing even more."

Gary McAlum, Board Director, National Cybersecurity Center

Ecosystems replace organizations

"Digitizing old business processes fosters the use of more supply chain connections. This leads to bad actors exploiting these new digital services."

Ravi Srinivasan, CEO, Votiro

New technologies emerge

"The shift in landscape produced by the pandemic has required organizations to reprioritize strategic objectives and key risks from accelerating digital transformation programs and migration to the cloud."

Steve Durbin, CEO, Information Security Forum

Physical and digital worlds collide

"We have seen a huge increase in the volume of malware impacts on industrial environments, from oil and gas and water to healthcare and manufacturing. Protection of cyber-physical systems will be the biggest challenge over the next two years."

Simon Chassar, Chief Revenue Officer, Claroty

Attacks and breaches multiply in today's world of digital disruption

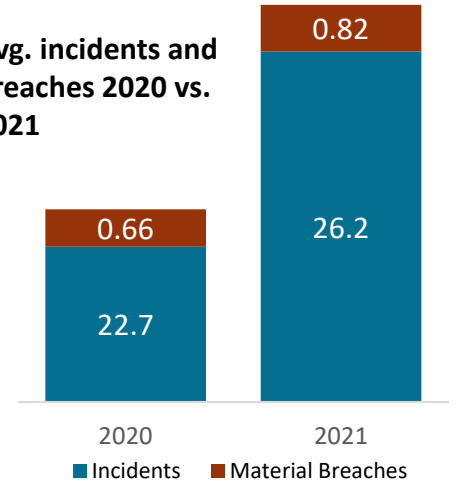
The average number of attacks and breaches rose sharply in 2021—the number of incidents rose 15.1%, while the number of material breaches jumped 24.5%, according to our research. In fact, these figures may be underestimated because of the potential for some organizations to fail to detect and to under-report attacks.

Based on respondent reports and our calculations, organizations saw an average of 22.7 cybersecurity incidents in 2020. These increased to 26.2 in 2021 as attacks climbed during the pandemic. While technology firms were hardest hit in 2020, healthcare firms had the most detected incidents in 2021. Material breaches—those generating a large loss, compromising many records, or having a significant impact on business operations—rose even more, by 24.5%, with retailers experiencing the largest number.

The greatest impact of those breaches was reputational loss, with consequences for customer trust, market share, and cost of capital. Business interruption was the second biggest impact, followed by the costs and work involved in response. Impacts varied by industry: for example, direct financial losses loomed larger for technology firms; replacement costs for healthcare firms.

With cyberattacks and breaches rising substantially, and corporate reputations at stake, it is not surprising that cybersecurity is now a top management imperative across industries.

Avg. incidents and breaches 2020 vs. 2021



% citing as the main impacts of material breaches

	All	Industry high
Reputational loss—reduced market share, higher capital cost, rating downgrade	37%	Life sciences 48%
Business disruption—staff downtime, costs of business interruption	31%	Retail 40%
Response costs—managing disruption, notifying customers/stakeholders	27%	Media & ent. 39%
Direct losses—financial theft, compensation to victims	21%	Technology 26%
Opportunity costs—foregone gains due to diverted management attention	19%	Retail 26%
Replacement costs—repair/replace capital assets, recover data	19%	Healthcare 29%
Customer (or citizen) losses—lower client retention, sales	14%	Public sector 22%
Fines and legal expenses—litigation, regulatory fines	13%	Telecoms 20%
Intellectual property—loss of IP and confidential data	13%	Automotive 19%
Supply chain/ecosystem losses—disruption, higher costs	11%	Consumer, mfg., retail 18%

Industry highs, avg. incidents and breaches

	Incidents	Material breaches
2020	Technology **25.1**	Retail **1.0**
2021*	Healthcare **27.8**	Retail **1.1**

*Industry averages for 2021 based on approximately nine months of data.

Q26. Approximately how many cybersecurity incidents did your organization experience in 2020 and 2021? How many were material breaches? Q27. What were the main impacts of those breaches?

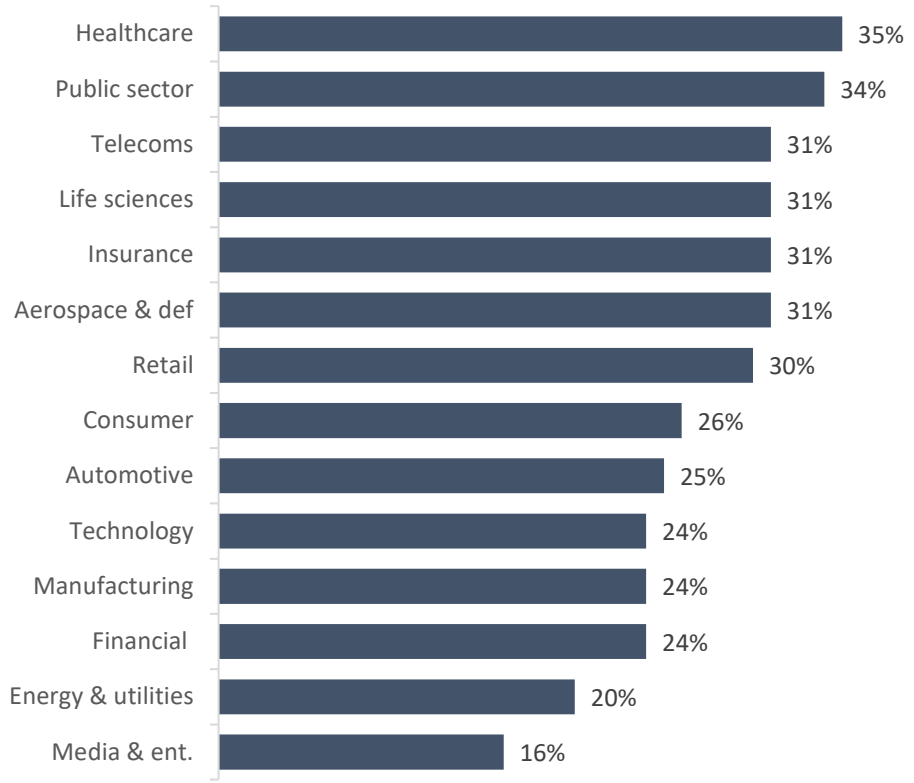
Yet many organizations are not well prepared for the risks ahead

Even before the outbreak of the Ukraine war, our research revealed that 27% of executives believed their organizations were not well prepared for today's rapidly changing threat landscape. The percentage was even higher among key executives: 29% of CEOs and CISOs and a staggering 40% of chief security officers. Slightly more firms that are advanced in NIST said their organizations were not well prepared (29%) than those earlier in their journey (26%), a sign that the uninitiated may not fully appreciate the risks to come.

% saying organizations not well prepared for changing threat landscape

All executives	27%
Chief Security Officers	40%
Chief Information Security Officers	29%
Chief Executive Officers	29%
NIST advanced firms	29%
Others	26%

% organizations not well prepared for rapidly changing threat landscape, by industry



Q20. Which of the following statements regarding cybersecurity at your organization do you agree with?

> "I've dealt with foreign cyberattacks. America isn't ready for what's coming."
>
> **Glenn Gerstall**
> Former general counsel of the National Security Agency and Central Security Service

> "Instead of the standard slope, we have seen a hockey stick rise in cybersecurity risks from more connections between everything and the adoption of new technologies. At the same time, the threat environment has significantly increased in scope, intensity, and sophistication. Then you throw in the pandemic and its massive strain on workforces and supply chains, and now the geopolitical environment. Given all that, you could argue that cybersecurity is at an inflection point."
>
> **Gary McAlum**
> Board Director, National Cybersecurity Center

Why executives feel unprepared for a new world of risk

For executives around the world, data security risks are escalating faster than their ability to mitigate them. Our research uncovered many reasons why executives believe they are not ready for the risks ahead.

44% of executives **> 50%** of CEOs, CIOs, COOs

say their organization's growing use of partners and suppliers exposes them to a major cybersecurity risk.

41% of executives **46%** of CIOs

think that cyber risk initiatives at their organizations have not kept pace with digital transformation.

30% of executives **39%** of CEOs

say they have inadequate budgets to ensure cybersecurity.

13% say cyber adversaries are better funded.

28% of respondents

cite the lack of executive support as a cybersecurity challenge and

16% cite a non-supportive corporate culture.

27% of executives

report say emerging technologies are their largest cybersecurity worry.

In two years, the percentage will grow to **37%** of executives and **47%** of CISOs.

25% of respondents **34%** of CSOs

believe that convergence of digital and physical systems, enabled by IoT technology, has increased their organization's exposure to cyber risks.

24% of executives **36%** of CIOS

see the shortage of skilled workers as their key cybersecurity challenge.

22% cite ineffective training programs.

Q20. Which of the following statements regarding cybersecurity at your organization do you agree with? Q21. What are the biggest cybersecurity challenges that your organization faces now and what will be the biggest challenges it faces over the next two years?

Adversaries are upping their game

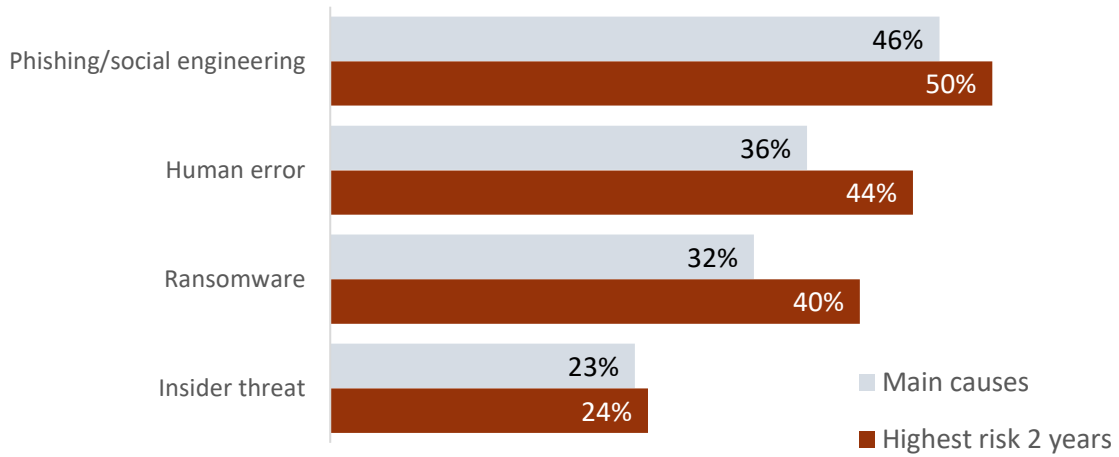
Ransomware and phishing attacks will climb over the next two years as cybercriminals become even more cunning in following the money.

Denial of service incidents were behind most major breaches in the past year, but executives expect to get a better handle on these attack vectors in the future, as well as on privilege misuse, zero day, and basic web app break-ins.

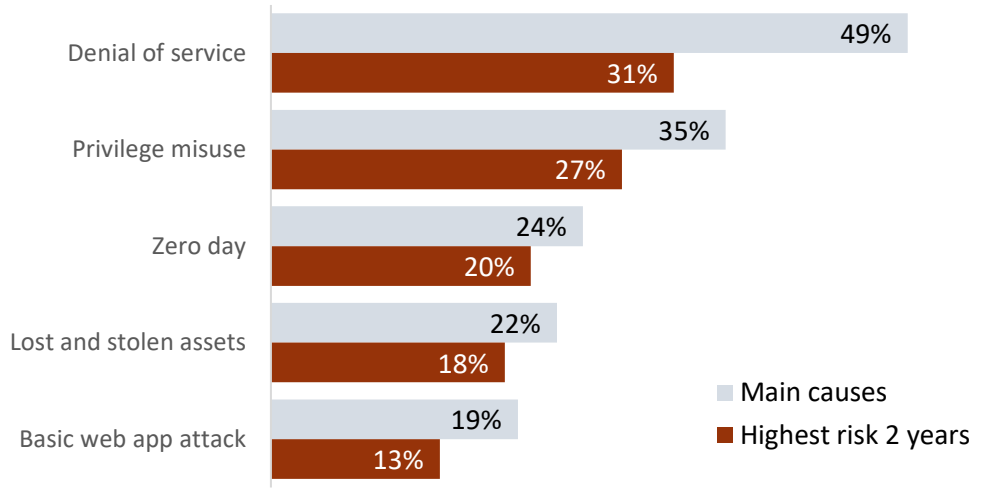
At the same time, criminal groups and nation-states are upping their game, using more advanced phishing and ransomware attacks to profit from human error. The head of information security and compliance at a US educational services company summed it up: “Ransomware and social engineering are easy, cheap, and make money—a low cost of entry for a big payout.”

Ransomware events are expected to jump the most over the next two years, from a main cause of breaches for 32% of entities now to a future risk for 40%. Government entities and healthcare organizations are often the main targets for ransomware attacks. “Ransomware is our number one external threat,” said Duc Lai, CISO at University of Maryland Medical System. Ron Mehring, CISO at Texas Health Resources, agreed: “Ransomware attacks are a big deal in healthcare because they impact safety and the data itself. They are becoming more frequent, targeted and sophisticated.”

Attack types likely to increase as cause of a breach



Attack types likely to decrease as cause of a breach



Q28. Overall, which of the following types of attacks were responsible for the breaches that your organization experienced? Which types of attacks pose the highest risk for your business over the next two years?

Calls to action: Ransomware and phishing

Draw on managed EDR

Duc Lai
CISO, University of Maryland Medical System

"Ransomware can have all kinds of operational and financial impacts that can bring a company to its knees. This can happen even if it just affects third-party vendors. The strongest defense against ransomware is a managed endpoint detection and response solution, because it can detect and block signs of an attack. It will ensure that security experts are watching those endpoints twenty-four seven, three-sixty-five, and that they are able to contain devices if they are compromised."

Reinforce security awareness

Stu Sjouwerman
CEO and President, KnowBe4

"The focus today is too much on trying to prevent data from leaving, instead of stopping attackers from ever getting in. I would expect to see more focus on security awareness training to reduce the threat surface of phishing—a primary attack vector in nearly every kind of cyberattack. This kind of training helps to establish good cyber hygiene, a sense of vigilance, and has been shown to reduce the risk of users falling for social engineering tactics employed within phishing attacks."

Don't just train, empower

Sydney Klein
CISO, Bristol Myers Squibb

"It's important to create a culture of cyber vigilance. We use a platform that gives everyone a monthly score that tells them how they're doing. How many mock phishes did they correctly identify? How many real phishing emails did they identify? What are their data protection habits and is there anything that can be improved there? What is their internet browsing record? Are they going to any sites that could be risky? That scoring has done wonders. We try to make sure that it doesn't feel like training, but like empowering people. We try to make it fun."

Follow the data

Ravi Srinivasan
CEO, Votiro

"Most ransomware attacks happen when the bad actors have gotten your data and locked it up. So, the key thing is to follow the data. It's like they say with understanding political corruption, follow the money. If you want to understand ransomware, follow the data. You will find it moving from server to endpoint to the cloud to file shares—and that chain is what you want to protect. If you can protect that data chain before the bad actor is able to compromise it, you've successfully prevented ransomware."

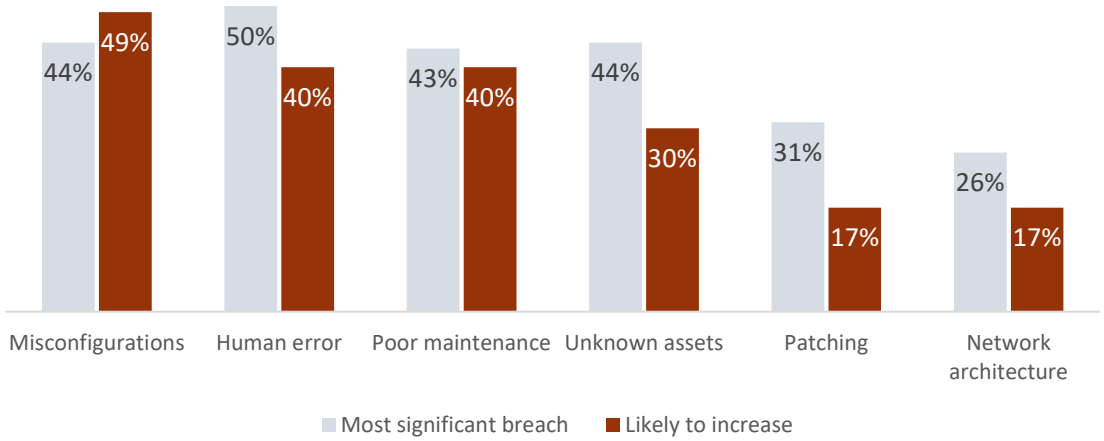
Technology adoption will lead to more breaches from misconfiguration

The advance of digital transformation—and the growing reliance on cloud, open systems, IoT, and other technologies—requires organizations to rebuild their IT infrastructures and platforms. That creates greater room for mistakes in configuration and maintenance and complicates adherence to best practice frameworks.

Misconfigurations across applications, systems, platforms, and servers—and neglecting to put new default settings in place—can create dangerous pathways for hackers. For example, while cloud hyper-scalers often have superior built-in security, the intricate maze of cloud formations and services used by organizations exposes them to new vulnerabilities. "In reality there is a shared responsibility between cloud providers and the organization using their services," said Gary McAlum, board director, National Cybersecurity Center. This includes configuration of storage containers, access management, and security protocols. He also pointed to what he calls the challenge of change control. "With many things shifting in the environment, it's easy to make a mistake. And you can get 'configuration drift'—your settings were good, but three days later so much has happened, and something has changed in the IT environment."

Overwhelmed and under-resourced security teams often let hygiene slip: poor maintenance remains a nagging issue and potential cause of breaches in many organizations. Currently, 15% of entities are just starting to install proper maintenance processes, and another 45% are only now beginning to make progress.

Main cause of largest recent breach and causes likely to increase in 2 years



% citing misconfiguration as the cause of a breach

	Mfg.	Energy & utilities	Life sciences	Consumer goods
Most significant breach	51%	48%	39%	38%
Likely to increase	53%	55%	58%	53%

> An effective way to mitigate misconfiguration risk starts with the automation of workflows that are prone to human error, such as change request provisioning, firewall rule validation and recertification, as well as ensuring access, firewall, and network configuration compliance.

Gidi Cohen
CEO and Founder
Skybox Security

Q29. For the most significant breach that your organization had over the last two years, what was the root cause of the attack and which causes are likely to increase over the next two years?

Inadequate budgets and other internal challenges are holding organizations back

As the digital world gets riskier, the private and public sectors face internal cybersecurity hurdles that are difficult to overcome.

The most stubborn challenge for all is **inadequate budget** as the need for greater cybersecurity investment continues to grow and organizations kick their security initiatives into high gear. Our research shows that proper spending on cybersecurity is critical for driving results (see Section 7: Supercharging cybersecurity results). "If security is treated as a tax on value, we will always have these issues. It must be integrated into the value stream," said Ron Mehring, CISO at Texas Health Resources.

Convincing boards and CEOs to make that investment will be key: while a **lack of prioritization of cyber risk** will fade over the next two years as boards and CEOs brace for escalating threats, **lack of executive support** will remain an issue for organizations seeking a balance between digital growth and safety. That is particularly challenging for advanced organizations as they speed ahead in embracing new technologies and exploiting new digital market opportunities.

With the rapid proliferation of devices, connections, and attacks**, inadequate identification of key risks** and **insufficient incident detection and response** are major headaches. Executives expect to get better at identifying key risks but believe their incident detection and response capabilities will struggle to stay ahead of slippery adversaries.

With digital transformation accelerating across sectors, organizations will continue to struggle to keep security up with the **pace of automation of key workflows and processes.** Executives expect the **shortage of skilled cyber professionals** to remain a ticklish issue. Although survey respondents see **ineffective cybersecurity training programs** as a smaller road bump, it may be a larger problem than they think. Our research reveals that human error is still a main cause for more than a third of breaches now, and it will continue to rise over the next two years.

% citing as biggest challenges, now and in 2 years

Challenge	Now	2 years*	Highest in 2 years by NIST maturity
Inadequate identification of key risks	31%	23%	Early implementation 33%
Inadequate budget for high level of cybersecurity	30%	38%	Mid implementation 40%
Insufficient incident detection/response abilities	29%	28%	Mid implementation 29%
Lack of executive support	28%	27%	Advanced implementation 30%
Lack of prioritization of cyber risk	28%	21%	Early implementation 29%
Pace of automation of workflows and processes	25%	23%	Early implementation 24%
Shortage of skilled cybersecurity professionals	24%	27%	Early implementation 30%
Inadequate governance across the organization	22%	24%	Early implementation 27%
Ineffective cybersecurity training programs	22%	19%	Early implementation 20%
Functional silos	16%	17%	Mid implementation 17%
Increasing supply chain vulnerabilities	16%	13%	Advanced implementation 14%
Non-supportive corporate culture	16%	8%	Advanced implementation 9%

*Green=increase orange=decrease

Q21. What are the biggest cybersecurity challenges that your organization now faces and what will be the biggest challenges it faces over the next two years?

Challenges vary by industry and job function

Every industry has its own unique set of cybersecurity challenges. In addition, executives across the C-Suite see these challenges differently.

Life sciences firms, which are the most mature in cybersecurity, experience more impediments than others, with 24% citing each challenge on average vs. 21% of all industries. The pace of automation, inadequate budget, and lack of executive support loom larger for life sciences companies as they strive for cybersecurity excellence. Magnets for criminal activity and now cyber warfare because of banking sanctions, financial firms worry more than most about insufficient incident detection and response—and along with insurers and life sciences firms, about the shortage of skilled cyber professionals. In their drive to innovate, technology companies sometimes do not adequately prioritize cyber risk.

CEOs and CSOs are more attuned to the budget challenge, while COOs are more sensitive to the pace of workflow automation. With more visibility into digital operations, CTOs and CDOs better understand difficulties around the identification of risks. CIOs think more about the shortage of cyber talent and supply chain vulnerabilities. CISOs are more concerned about the lack of prioritization of cyber risk, while chief privacy officers understand firsthand the limitations of training programs and steps to create more vigilant corporate cultures.

Challenge	All
Inadequate identification of key risks	31%
Inadequate budget	30%
Insufficient incident detection and response	29%
Lack of executive support	28%
Lack of prioritization of cyber risk	28%
Pace of automation of key workflows	25%
Shortage of skilled cybersecurity professionals	24%
Inadequate governance	22%
Ineffective cybersecurity training programs	22%
Functional silos	16%
Non-supportive corporate culture	16%
Increasing supply chain vulnerabilities	16%

Industry high		C-level function high	
Public sector	37%	Chief legal officer	36%
Life sciences	36%	CEO, CSO	39%
Financial services	38%	CTO, CDO	33%
Life sciences	36%	Chief security officer/architect	36%
Technology	38%	CISO	34%
Life sciences	38%	COO	31%
Financial, insurance, LS	29%	CIO	36%
Aerospace, auto, LS	26%	Chief compliance officer	26%
Consumer, retail	31%	Chief privacy/data officer	27%
Automotive, technology	21%	Chief security architect	22%
Energy & utilities	23%	Chief privacy/data officer	21%
Retail	26%	CIO	23%

> "Supply chain complexity could be a big cybersecurity risk, which we mitigate by employing best practices such as code signing."
>
> **CIO**, US medical devices firm

> "Our cyber training includes updated content and materials that cover new threats and operational requirements to prevent malicious activity."
>
> **CRO**, consumer manufacturer, India

Q21. What are the biggest cybersecurity challenges that your organization now faces and what will be the biggest challenges it faces over the next two years?

> "Cybersecurity is no longer only IT's job. The accelerated digital transformation of back-office processes, rapid application migration to multiple clouds, and modernization of the data platforms have brought business and security leaders together to collaborate on new cyber strategies and execution."
>
> **Ravi Srinivasan, CEO, Votiro**

3. Organizing for a riskier cyber world

Cybersecurity is best managed as a C-Suite team effort

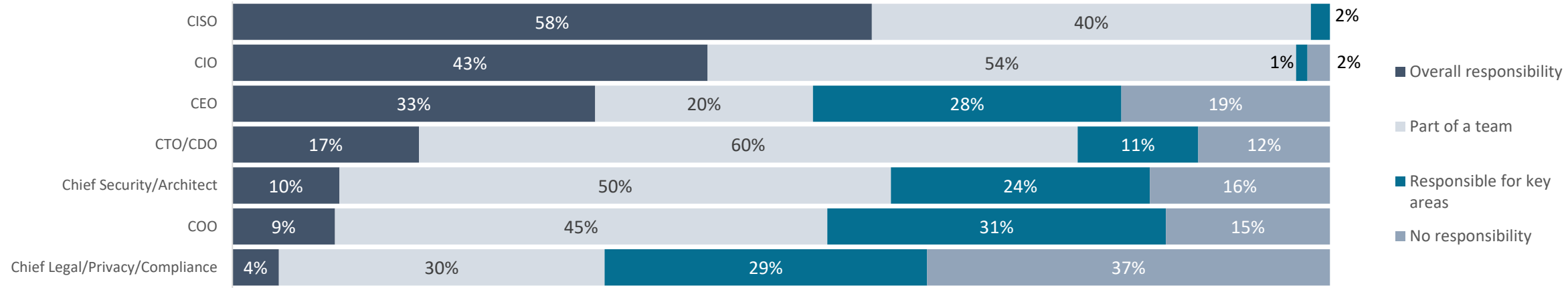
Cybersecurity is no longer simply relegated to the CISO or the technology function. As organizations go digital, cybersecurity has become a strategic business imperative that requires the CEO, CIO, and other members of the C-Suite to work together to mitigate risks and meet the expectations of stakeholders.

CISOs are the most prominent player in cybersecurity: 58% of those surveyed report they have sole overall responsibility in their organizations, while 40% are part of wider cyber risk management teams. Some 43% of CIOs report being in charge, while most others act as part of a team. With cybersecurity now a business priority, CEOs also are heavily engaged: 33% say they are ultimately in charge while 48% are responsible for some areas or are part of the team. Not only are CEOs the logical leaders for an effective executive team approach, but the board, shareholders, customers, and regulators are holding them accountable for attacks that can bring down the business—as occurred with the 2021 hacking of Colonial Pipeline.

Given their seniority and knowledge of operations, COOs are also more involved: 9% have overall responsibility for cybersecurity and 76% are responsible for some areas or play a role on teams. Legal, operations, data privacy, and risk management executives are working more closely with cybersecurity teams—in a small number of cases, they are even running those security activities. The active participation of these functions can be critical as entities strive to ensure privacy and regulatory compliance, prevent massive fines and liability, and fend off reputational damage.

In a digital world where risks are proliferating, cyber risk needs to be part of an overall enterprise risk approach. The C-Suite will need to work even more closely to enhance cyber governance and best practices and to build a cybersecurity-minded culture. The CISO may have day-to-day oversight, but all senior management will need to play a role.

Cybersecurity responsibility by title*



Q1: Are you responsible for cybersecurity in your organization? *Percentages may not add because they reflect survey respondents who reported responsibility, plus those excluded from the survey because of their lack of responsibility.

Calls to action: Managing cybersecurity through the C-Suite

Build a C-Suite team approach

Larry Clinton
President and CEO, Internet Security Alliance

"Organizations need to consider adapting their organizational structures to better address the new enterprise landscape. Technology now integrates modern organizations, whether co-workers are across the hall or halfway around the world. But the existing reporting structures and decision-making processes at many companies are legacies of a siloed operating model, where each department and business unit makes decisions and manages risks relatively independently.

To address this problem, leading organizations are moving toward a more integrated team approach. This approach recognizes that cyber risk is not separate from other business risks and should not be thought of as the responsibility of just IT experts. Even with good technical controls, a secure culture nurtured by top management is a critical aspect of cybersecurity. With the need for increased and better calibrated cybersecurity budgets, finance is a critical function, as is R&D and marketing. Cyber events can also raise concerns regarding reputational risk, making it important for the public relations, communications, and legal departments to contribute to cyber risk management.

Cybersecurity needs to be managed across the enterprise and many different parts of the organization must take responsibility for specific activities and be held accountable for the contribution to an effective enterprise-wide program."

Take on a more strategic role

Simon Chassar
Chief Revenue Officer, Claroty

"In about a third of organizations, CISOs are communicating more with the board and senior management and taking on more strategic responsibilities. The biggest change in the role of the CISO is the need to be a business partner at the board level, protecting the organization's corporate strategy, along with continued production of products, acquisitions or new market entry. The CISO is a critical digital transformation advisor, keeping the corporate strategy functioning securely."

Be the cybersecurity evangelist for the C-Suite

Duc Lai
CISO, University of Maryland Medical System

"I have a team of security experts to select and deploy the technology. My role is to partner with the right leaders to make sure that cybersecurity becomes part of the organization's DNA, so that executives think about it whenever they have any business initiative in mind. In other words, it's important to be a cybersecurity evangelist. Getting other leaders engaged is a big part of my responsibility, as well as putting together our investment proposals, and communicating about our security program, organizational plan, architecture plan, and financial plan. I make sure that senior leaders understand that we are doing the right things with our program."

In today's digital world, the role of the CISO is expanding

Cybersecurity is central to today's digitally enabled businesses. With physical and digital worlds melding, technology advancing, and cyber risks, vulnerabilities, and regulations multiplying, CISOs must take on a wider remit that spans functions across the enterprise.

Cyber threats permeate every area of today's hyperconnected enterprise. This requires a more holistic cybersecurity approach and a broader CISO mandate for greater oversight. Traditional demarcations between data security and privacy are blurring, with almost half of executives saying CISOs are taking on more accountability for privacy and compliance. CISOs are also doing more to reduce fraud, manage vendor and supply chain risk, and ensure resilience and business continuity. Their activity related to supply chain—a growing source of risk—is particularly notable.

CISOs are shifting from an IT to a security focus, but not fast enough. As part of this transition, three out of 10 CISOs are more involved in enterprise and geopolitical risk management, a trend that will gather momentum as nation-states step up their attacks. CISOs also are becoming more strategic, with greater influence over their organization's business and digital transformation plans. This is particularly true of CISOs in industrial manufacturing (38%), who are working with management teams to create smart factories of the future. About a third of CISOs are interacting more with the board and senior management; for technology firms, the share is even higher (40%). This is another best practice that likely will increase as boards give CISOs a seat at the table within their committee structures and as CISOs take on a wider advisory role within organizations.

% citing as a change in the CISO's role over the last two years

	All	Industry high	Industry low
Expanded responsibility relating to data privacy and compliance	49%	Consumer 56%	Healthcare 39%
Greater management of customer and insider fraud	42%	Media, public sector 50%	Insurance 33%
Growing role in vendor, third-party, and supply chain management	34%	Consumer 44%	Public sector 27%
Greater role in operational resiliency and business continuity	33%	Healthcare 41%	Manufacturing 24%
Greater focus on security posture than IT	32%	Aerospace & defense 40%	Telecoms 25%
Increasing interaction with the board of directors and senior management	32%	Technology 40%	Public sector 22%
Greater involvement in enterprise and geopolitical risk management	30%	Insurance, tech 38%	Retail 20%
Greater influence over the organization's strategy and operations	29%	Automotive 40%	Healthcare 18%
Bigger role in digital transformation and business strategy	29%	Manufacturing 38%	Automotive 23%
Greater management of operational technology	28%	Healthcare 41%	Technology 16%

Q25. How has the role of the CISO changed in your organization over the last two years?

> "The CISO is thinking more broadly and strategically about the business as a whole and the impact of cyber on the broader business and planning for resiliency outside of just the cyber space."
>
> **Deborah Wheeler**
> CISO, Delta Air Lines

Calls to action: The new role of the CISO

Take a holistic approach

Steve Durbin
CEO, Information Security Forum

The value of CISOs in organizations is still being fully recognized, with some CISOs remaining anchored to the more traditional domains of information security and risk management. The CISO's relationship with the business needs to develop further; this relationship is a two-way street. CISOs need to become more business-aligned, while business leaders need to be more aware of the relevance of cybersecurity to their personal and corporate accountabilities.

Organizations with a more mature, holistic approach to enterprise risk management are able to bring multiple risk domains together so that they can become more complementary in establishing an aggregate risk position.

Organizations with a maturing risk management framework and culture may still have separation, treating differing risk management domains in isolation to each other with some notable gaps, such as geopolitical risk.

Organizations with a weak or no risk management framework and culture will be in a reactionary mode when it comes to geopolitical risk and certainly the current situation; likely they are contemplating the challenges of Russia-Ukraine, for example, as an operational hurdle rather than a strategic risk that will have longer-term consequences.

Engage in geopolitical risk management

Cory Simpson
Executive Vice President, Resolute

Every CISO needs to have an awareness of the geopolitical risk factors in the organization's operating environment and be a part of the strategy for best mitigating such risk. Just as the role of the CFO has evolved in the last 30 years from a budgetary gatekeeper to a strategic partner of the CEO, we need the CISO's role to quickly evolve to help corporate leaders better manage geopolitical risk for their organizations.

Companies should ensure cohesion between their cybersecurity and political risk management strategies. How this is best done will vary from company to company and market to market, but it all begins by ensuring a comprehensive, inclusive, and collaborative planning process.

.

Make the business case to the board

Gidi Cohen
CEO and Founder, Skybox Security

CISOs have a starring role in the new normal. Cybersecurity has become a central part of how businesses grow and operate. CISOs' influence with the CEO and board has greatly increased. Radical change brings an opportunity for a dramatic shift in how organizations approach their security programs. The CISO role will no longer be primarily technical. CISOs will broaden their purview to include the 'business of cybersecurity'. Modern CISOs will make the business case for cyber initiatives and address overall business risk. They will also need to quantify the return on investment of those initiatives. CISOs will be highly knowledgeable about the state of cybersecurity and the threat landscape. They will share this knowledge with the board in business terms and build proactive security posture management programs that take this global picture into account.

The skills imperative: Getting needed talent in place

The global shortage of skilled cybersecurity professionals is one of the biggest cybersecurity challenges that organizations face, cited by about a quarter of respondents. Having the right level and quality of talent and skills—whether hired, trained, or outsourced—can make a difference in cybersecurity preparedness and effectiveness.

Organizations that are advanced in cybersecurity generally have larger IT, OT, and cybersecurity staffs. Their IT staffs make up a larger share of the overall staff count, and their cybersecurity specialists represent a larger share of their IT staffs, than at other organizations.

As more entities take their cybersecurity strategies to the next level, hiring cyber professionals will become harder. "In the face of increased digitization and a rising tide of attacks, the global cybersecurity workforce of 4.2 million people needs to grow 65% to keep up with demand," said Mandy Andress, CISO at Elastic.

Outsourcing is a clear way to secure needed talent. Although advanced organizations have more in-house cyber personnel than others, they also employ more full-time equivalent (FTE) specialists, who work for external firms to manage specific cyber functions for them.

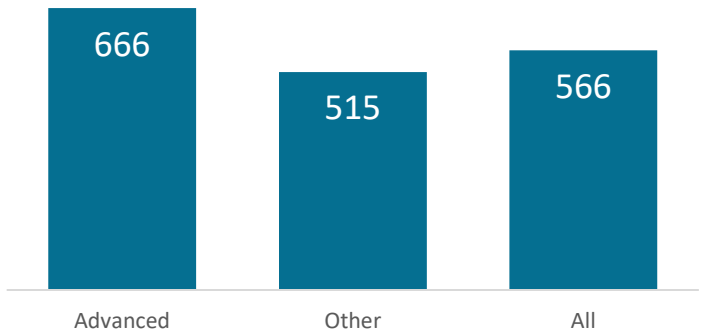
> "While the threat of malware, ransomware, and data breaches will only continue to rise, the biggest challenge in front of many security executives is finding the next generation of cybersecurity professionals."
>
> **Mandy Andress**
> CISO, Elastic

> "Many industries are seeking talent where perhaps before they thought they could get away without hiring, or with hiring one or two resources. Now they realize teams of cyber experts may be needed because these threats are here to stay."
>
> **Deborah Wheeler**
> CISO, Delta Air Lines

Average staff size by NIST maturity

	Advanced	Others	All
Worldwide staff	57,538	38,398	44,890
IT staff % of total staff	7.80%	7.60%	7.70%
OT staff % of total staff	5.50%	5.00%	5.30%
Cybersecurity staff as a % of IT staff	14.60%	11.80%	13.20%
Mean total cybersecurity staff	675	372	475

Average outsourced FTEs by NIST maturity



Q7. Please indicate the number of employees that work for your organization worldwide. Q7. What percentage of those employees that are in information technology (dealing with information) and operational technology (dealing with machines). What percentage of the IT staff focuses on cybersecurity? Q24a. Please estimate the number of full-time equivalent employees these outsourcing resources represent. Q31. Please provide us with the latest information for the metrics that you track.

Outsourcing fills resource gaps and frees up internal resources

The security operations center and threat intelligence, two of the most resource-intensive cybersecurity functions, are most often outsourced.

Experts agree outsourcing is a good move, particularly for organizations that struggle to hire talent—a pain point that will grow as demand for cyber expertise swells. Ravi Srinivasan, CEO at Votiro, a provider of security file transfer software, advises firms to "outsource security operations and response so that you can free up resources to focus internal efforts on securing data and the usability of new digital business services." Healthcare firms are more likely than others to outsource security operations. "It's quite costly to run your own SOC, and with the quality of the managed services provided nowadays, it's a better decision to invest in that type of service, especially to manage your endpoint detection and response," said Duc Lai, CISO at University of Maryland Medical System.

Firms advanced in NIST are more apt to outsource the security operations center, bug bounty programs, and privacy management than others. They tend to outsource other areas less, such as threat intelligence, firewall management, and risk assessment, since they have built up their own internal staff for these activities that work together across risk and security functions. Still, 37% of advanced firms do outsource threat intelligence and 35% outsource risk assessment, looking for outside help to gather data from a wide variety of sources and the specialized talent needed to interpret this information. Ensuring the right approach for threat intelligence is critical as geopolitical tensions spill over into the cyber world. Insurers, with their broader risk perspective, already are more likely to outsource threat intelligence, while tech firms—more focused on growth than risk—draw on external risk resources less.

% outsourcing cybersecurity function by NIST maturity, with industry highs and lows

Function	Advanced	Others	All	Industry high	Industry low
Security operations center	50%	48%	49%	Healthcare 60%	Manufacturing 41%
Threat intelligence	37%	42%	40%	Insurance 53%	Technology 29%
Firewall management	34%	39%	38%	Manufacturing 48%	Aerospace & defense, retail 33%
Incident response	37%	37%	37%	Consumer 44%	Healthcare 31%
Risk assessment	35%	36%	36%	Aerospace & defense 44%	Insurance 24%
Threat detection/response	34%	33%	34%	Automotive 44%	Public sector 23%
Governance	27%	31%	30%	Energy 36%	Manufacturing 21%
Bug bounty (responsible disclosure)	28%	24%	25%	Energy, financial 30%	Technology 19%
Red team	16%	18%	18%	Automotive 28%	Manufacturing 9%
Privacy management	15%	13%	14%	Manufacturing 20%	Telecoms 6%

Q24. Which of the following cybersecurity functions does your organization outsource?

Which outsourcing approaches drive the best results?

Outsourcing plays an important role in optimizing resources and furnishing organizations with the expertise they need. But contracting out some functions provides a bigger bang for the buck than others. Outsourcing the security operations center yields the best results in terms of fewer breaches, and faster time to detect, respond, and mitigate.

All firms outsource some cybersecurity functions, but to varying degrees. We used our survey results to correlate organizations' reported breaches in 2021 to the functions they outsource to understand where contracting third parties could help to deliver better outcomes. We also evaluated which outsourcing approaches seemed to support better results in time to detect, respond to, and mitigate a breach. Our research revealed that outsourcing the security operations center tended to help generate better outcomes across all these categories.

Outsourcing threat intelligence, firewall management, incident response, and threat detection also can reduce the probability of a breach. For excellent time to detect (the top 25 percentile), outsourcing SOC, firewall management, and risk assessment gets the best results; for time to respond, SOC, threat intelligence, and risk assessment; and for time to mitigate, SOC and threat intelligence.

Outsourcing effectiveness by results

Function	No breaches	One breach	Multiple breaches	Excellent time to detect	Excellent time to respond	Excellent time to mitigate
Security operations center	52%	49%	41%	58%	61%	52%
Threat intelligence	42%	41%	36%	41%	52%	43%
Firewall management	41%	36%	33%	42%	39%	39%
Incident response	41%	35%	33%	39%	30%	35%
Risk assessment	36%	39%	28%	44%	52%	26%
Threat detection/response	39%	30%	28%	41%	35%	39%
Governance	26%	31%	35%	20%	22%	30%
Bug bounty (responsible disclosure)	24%	23%	33%	22%	24%	30%
Red team	12%	21%	25%	7%	17%	22%
Privacy management	10%	15%	21%	10%	11%	9%

Q24. Which of the following cybersecurity functions does your organization outsource? Q26. Approximately how many cybersecurity incidents did your organization experience in the 2020 and 2021? How many were material breaches? Q31. Please provide us with the latest information for the metrics that you track.

Case study: Peachtree Corners

Partnering with start-ups to secure smart city innovation

Brandon Branham
Assistant City Manager and CTO
Peachtree Corners, Georgia

Peachtree Corners, a municipality in the Atlanta metropolitan area, has been making a name for itself in the smart city world as a leader in connected infrastructure and new technologies through its Curiosity Lab innovation hub. But that digital leadership must include a focus on cybersecurity.

Curiosity Lab at Peachtree Corners is a unique public-private partnership that provides start-ups, universities, and Fortune 500 companies with a real-world environment to test technological innovation free of charge. “Our Curiosity Lab is a publicly funded living laboratory for testing emerging technologies integrated with public infrastructure,” says Brandon Branham, assistant city manager and CTO of Peachtree Corner. According to Branham, the lab enables the municipality to “address potential vulnerabilities that could take down their networks as more and more things in a city are connected.” This is critical for Branham, whose biggest cybersecurity challenge is protecting infrastructure against cyberattacks—a growing worry given rising global geopolitical risks.

Located within a 500-acre technology park where more than 1,000 people live, Curiosity Lab includes a three-mile roadway with fiber optics and 5G built in for testing smart city applications, IoT, and autonomous vehicles. It currently has three fully electric autonomous shuttles undergoing testing and provides interaction with human drivers. The lab also has a segmented network—one that doesn’t connect with the rest of the city—that companies can use to test video analytics, environmental sensing, connected vehicles, and light detection and ranging (LiDAR). They are partnering with Georgia Tech to add digital twins to the facility.

Making security top of mind

The lab helps Branham develop cybersecurity solutions for smart city initiatives. “These start-ups have amazing technology that really help move cities forward,” says Branham. “But security isn’t always top of mind for them. That’s a big part of what we do through the Curiosity Lab program—we help them layer in the security.”

Branham points out that with connected vehicle applications, there is a lot of information going from the infrastructure to the vehicle. “It’s crucial to ensure a secure connection for that communication because if our traffic signal tells the shuttle that it's green, but it's really red, that’s a big problem,” he says. But there must be a balance, he says—it’s impossible to segment every device from every other one, because the connection is then lost. “The important thing is building security into applications and devices from the beginning, and that’s something that we really drive home with the start-ups we work with,” says Branham. “Security can’t be a second thought after you come onto a network.”

Branham says this kind of thinking is crucial for start-ups that want to scale up their products and services and work with other governments. Public entities are still much more risk-averse than private companies. “All it takes is one incident due to a vulnerability through your device,” says Branham, “and you're done in the government sector.”

> “Stemming the tide of breaches will require an evolution in the way we think about cybersecurity. Organizations no longer have the luxury of believing that reducing cyber risk is a technology-centric problem that can be adequately addressed via technology-only controls. Our next evolutionary step requires us to look back and revisit first principles—it requires a multifaceted approach across people, process, and technology.”
>
> **Perry Carpenter, Chief Evangelist and Strategy Officer KnowBe4**

4. Taking cybersecurity to the next level

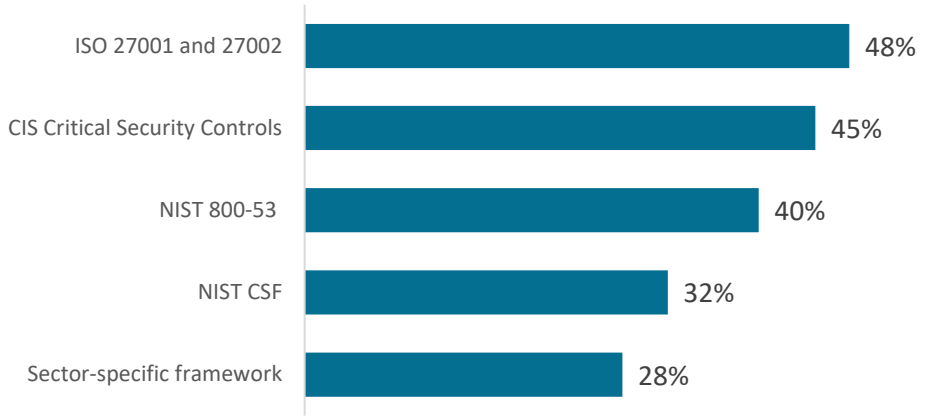
Assessing and driving performance through cybersecurity frameworks

Almost half of organizations have adopted the ISO frameworks, which offer international recognition and a third-party audit and certification process. Slightly fewer use NIST. Our research shows that leading organizations often use more than one framework to meet global standards and improve cybersecurity results.

The certification offered by ISO is important, especially for entities with an international footprint or that are vendors to other organizations. Of course, most private and public entities use more than one framework. This includes the more prescriptive CIS Critical Security Controls, a relatively short list of preliminary actions that map well to other frameworks. “From a strategic view of what a strong security program should accomplish, the CIS Critical Controls are a great starting point,” said Gary McAlum, board director, National Cybersecurity Center**.** Some 4 in 10 firms use NIST 800-53, which offers security controls needed for compliance with US standards for federal government agencies and contractors. About a third use NIST CSF, a subset of NIST 800-53 that offers a flexible framework that can be adapted to any entity, and which is compatible with the ISO standards. The Information Security Forum also offers an aggregator framework, SOGP. But too many frameworks can lead to too many tools in use, said Ravi Srinivasan, CEO, Votiro. “It’s best to rationalize based on a business-led security strategy. Flexibility is important, as each firm is unique and should fashion its cybersecurity program to meet its specific needs.”

However, organizations need to do more than compliance and build on a framework to create an effective program. “They need to go beyond a check-box approach to a framework to a continuous state of security,” said one US-based security leader. “I’ve worked for some firms where before auditors come in, they do a big cleanup. It’s fantastic for the next three months, but then it slowly deteriorates. You need to make frameworks a part of daily life.”

% using each cybersecurity framework



Industry high	Industry low
Automotive 59%	**Consumer 36%**
Consumer 53%	**Healthcare 38%**
Life sciences 50%	**Telecoms 29%**
Insurance 43%	**Telecoms 18%**
Consumer 38%	**Insurance 21%**

Q8. Which cybersecurity frameworks, if any, does your organization use to benchmark its cybersecurity strategies?

> “The most important point is not to confuse regulatory compliance with actual security. The technical best practices probably ought to be a mixture of the various frameworks, but they need to be adjusted based on the uniqueness of the organization's technology, culture, and business plan.”
>
> **Larry Clinton**
> President/CEO
> Internet Security Alliance

As organizations advance, they conduct more cyber maturity assessments internally

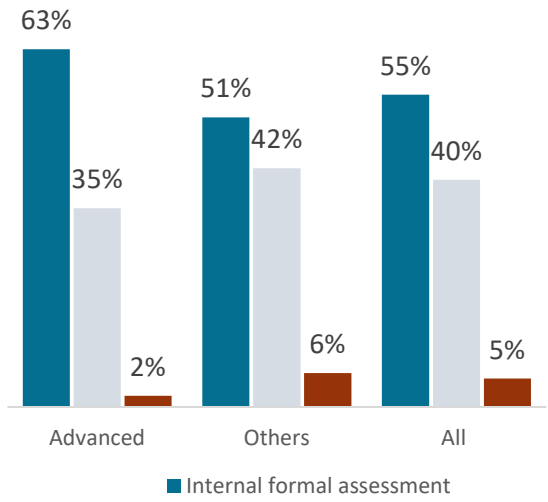
Most organizations formally evaluate their cybersecurity maturity: 55% conduct internal assessments, and 40% use external consultants. As organizations mature, they often bring development of KPIs in-house and build them into ongoing governance.

Attention to cybersecurity frameworks enables organizations to better communicate progress to senior management teams, manage data security and privacy more effectively, and cement their reputation among stakeholders. That is why most organizations conduct formal assessments. But for some firms, like financial institutions, regulators may require formal assessments.

Only 5% of respondents have not conducted assessments, although that number is higher among those early in their cybersecurity journeys. Automotive, life sciences, public sector, and technology players have done more to formally assess their cybersecurity maturity.

While measuring maturity is critical for assessing progress, forward-looking CISOs are striving to link maturity to outcomes. Juan Morales, CISO of Realogy, said his team is working to develop accurate KPIs for its cybersecurity program and investments. “We’ve improved the maturity of our information security program dramatically against our cybersecurity framework, but ultimately I want to tie it back to how our dollars are being spent and the return that we're getting on those investments.”

% undertaking formal assessments by NIST maturity stage



> Internal and external assessment are best seen as complementary mechanisms for continuous improvement. Top-performing organizations correlate improvements in operational metrics to sequential improvements in framework maturity as gauged by an independent advisor. Measuring the benefits of investment in cybersecurity with both ‘inside out’ and ‘outside in’ perspectives can send a compelling message to senior business leaders.
>
> **Paul Sussman**
> Vice President, Cybersecurity Strategy Consulting, Booz Allen Hamilton

% firms undertaking formal assessments by industry

	Aerospace	Automotive	Consumer	Energy	Financial	Healthcare	Mfg.	Insurance	Life sci.	Media	Public	Retail	Tech.	Telecoms
Yes, we have done it internally	63%	64%	60%	44%	60%	44%	39%	56%	59%	53%	64%	55%	55%	55%
Yes, we hired an outside consultant	33%	35%	34%	51%	36%	53%	54%	38%	39%	40%	33%	40%	43%	39%
No formal assessment	5%	1%	6%	5%	4%	4%	8%	6%	3%	8%	3%	5%	3%	6%

Q9. Have you undertaken a formal assessment of your organization’s cybersecurity maturity?

Identify: Organizations have made most progress in governance and risk assessment

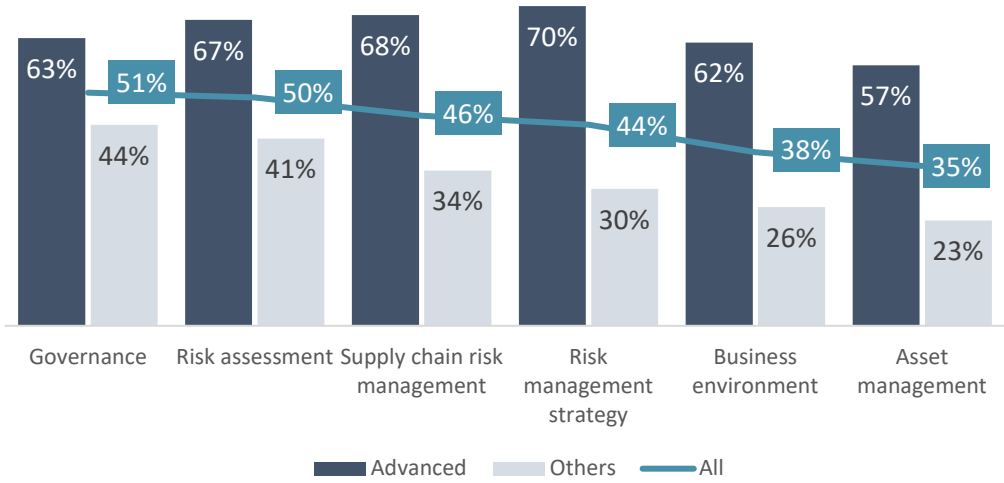
Developing an understanding of cybersecurity risks across the organization is the first step in building a successful cybersecurity strategy. But less than half of all firms have fully implemented this area of NIST.

So far, organizations have made the most progress in setting the foundation for governance and risk assessment. Those advanced in NIST implementation are ahead in all areas, particularly in creating a risk management strategy centered on a risk-based approach and supply chain risk management, a huge concern in the wake of disruptions caused by the pandemic and the war in Ukraine.

As supply chain risks grow, CISOs are playing a growing role in vendor and partner management, said 34% of respondents. “Supply chain attacks are getting very common these days. We are identifying and protecting all the vulnerable resources to mitigate these risks,” said a C-level executive at an Australian ecommerce firm. Our research shows that organizations that are most advanced in supply chain risk management generate faster times to detect, mitigate, and respond. (See Section 7: Supercharging cybersecurity results.)

Life sciences and aerospace and defense firms have made more progress than others in governance, while energy firms are ahead in risk assessment. Overall, insurance and telecoms firms are the most advanced in “identify” areas, while media firms and manufacturers trail behind.

% managed or optimized in each area by NIST maturity



% managed or optimized in each area, by industry Green = highest percentage across industries; red = lowest percentage across industries.

	Insurance	Telecoms	Aerospace	Financial	Life sci.	Energy	Retail	Consumer	Tech.	Automotive	Public	Healthcare	Media	Mfg.
Governance	43%	50%	60%	54%	65%	55%	54%	50%	55%	49%	48%	49%	34%	43%
Risk assessment	55%	56%	55%	54%	51%	58%	48%	51%	49%	51%	50%	39%	45%	39%
Supply chain risk mgmt.	54%	46%	51%	54%	48%	46%	59%	45%	44%	36%	47%	41%	31%	33%
Risk management strategy	54%	55%	41%	45%	51%	46%	45%	46%	38%	38%	36%	41%	40%	36%
Business environment	45%	51%	40%	36%	35%	35%	34%	38%	45%	43%	35%	39%	34%	31%
Asset management	40%	33%	34%	37%	30%	38%	30%	33%	31%	41%	39%	36%	38%	28%
Average	**49%**	**49%**	**47%**	**47%**	**47%**	**46%**	**45%**	**44%**	**44%**	**43%**	**43%**	**41%**	**37%**	**35%**

Q10. What progress have you made in each of the following activities to identify cybersecurity risks? (Top 2 managed or optimized)

Calls to action: Mitigating supply chain risks

Understand your suppliers better

Steve Durbin
CEO, Information Security Forum

"Organizations need to understand their supply chains much better—most understand their tier-one suppliers, and possibly tier two, but very few can claim understanding beyond that. Transparency is key—a lot of your suppliers may not know your security requirements, even if you assume they do. If you want your supplier firms to be more secure, you need to show them how. But it needs to be simple because some of your suppliers will not have security departments, and most won't have one of the same size as yours.

In addition, you need a really mature and current view of regulation across your supply chain, because some of your suppliers may be operating in a way that is alien to you for very good local regulatory or legislative reasons. . And if you don't understand that, then you're going to be making the wrong assumptions—and some of your suppliers may not tell you."

Develop a third-party risk management process

Duc Lai
CISO, University of Maryland Medical System

"As organizations become more dependent on a vendor ecosystem, they become more susceptible to third-party risks. So, you have to make sure you complete your due diligence before you engage with those vendors, and continue to monitor them, maintaining open communications about what their security posture is. Vetting can be a complicated process and should be done in collaboration with compliance and legal, since requirements must be incorporated into the contract. Otherwise, it's very difficult to enforce anything with a vendor once a contract is signed.

It's best to apply the 'least privilege' principle, so that they only access what they need to access and continue to review that to ensure that there are no stale, unused connections. It's important to take a third-party lifecycle management approach—when you stop using a vendor, you must make sure it is properly off-boarded and that your data is accounted for."

Continuously assess supply chain risk and connectedness

Deborah Wheeler
CISO, Delta Air Lines

"We are continuously risk-assessing our environment and monitoring threat actors and others with an interest in our industry sector. Supply chains present unique risks that were brought to the forefront through SolarWinds. These kinds of events help us to be more specific in our questions of third parties and require that we spend more time understanding our supply chain connectedness."

Case study: Motorola

Handling third-party risk

Richard Rushing
CISO
Motorola Mobility, a Lenovo company

As third-party risks rise amid supply chain complexity and disruption, companies need to get a better handle on their ecosystems of vendors and partners. That is something Richard Rushing, CISO at Motorola Mobility, strives to do, but with some 16,000 relationships, it is no easy task.

"While 99% of our suppliers are great at their jobs and have good security practices, the 1% can still do a lot of damage to your organization," says Rushing. "Unfortunately, the bad guys know it." Hackers are likely to target vendors with weak cybersecurity practices to use them as a route into their better-protected customers, Rushing adds.

That's why both thorough investigation of third parties and contracts with explicit provisions for reporting breaches and incidents are crucial. "In cloud and multi-tenant environments, it's important to be notified within 72 hours of an incident regardless of whether it involves your data or not," Rushing says. "This provision is probably not in 95% of vendor contracts unless the corporate purchaser was very proactive about it. Most organizations find out about a third-party breach by reading a news article."

For Rushing, his time clock is key for lowering risk. "If you have one critical thing in your organization, it's time, because it's a finite resource; you have to be careful about what uses that time. So, the sooner I know about an incident, the better I can respond to it and effectively manage our time resources."

Know your interconnections with vendors

Another way to reduce cybersecurity risks is to understand the digital connections that your business has with its vendors and partners, according to Rushing. "Some vendors have been around 15 years. Some have direct connections to your network through a VPN or through an IPsec tunnel. You need to know what is going on with your vendors. Which servers are they are accessing, and which applications," Rushing says. "You need to know the ramifications of any actions you take on the business—if you cut off a network connection, will you cut off a call center that serves all of Europe?"

Rushing does simulation exercises to see what would happen if he were forced to turn different networks off in the event of an attack. "We have to ask: Do you know how many network connections we have, and which network connection goes to which company? Can they still do business? Do you know what processes are affected, who to contact, and what information you are able to give them? If you don't know where those stumbling blocks are, you will hit things."

He says it's vital to do this kind of planning in advance, but also to find out if it works in a real-life situation. "Once you build an end-to-end process, the only way to test it is to take down a network for an hour or so," he says. Often, he says, this reveals unexpected problems missed in a simulation. "It takes a bit of time, but as a result, you are better organized and prepared for an attack—to avoid additional stress in an already stressful situation."

Protect: Organizations prioritize technology and data security

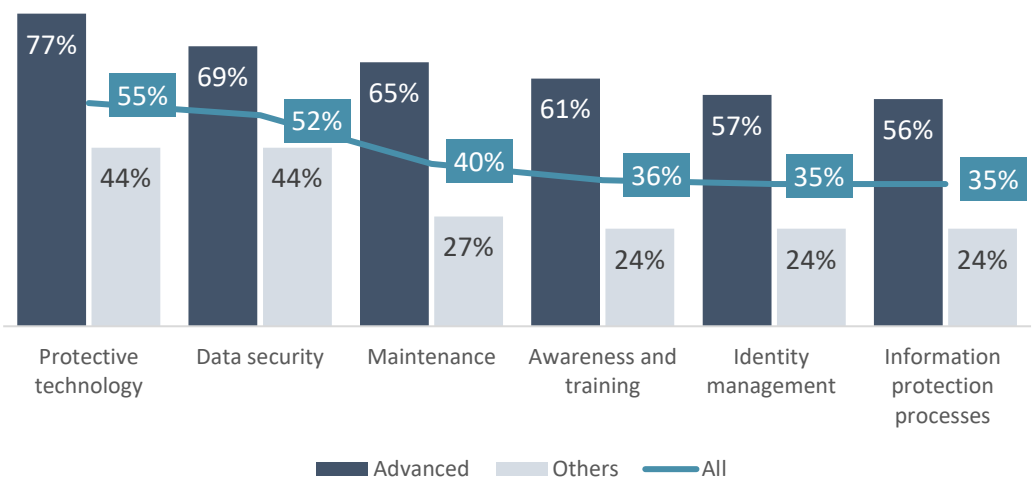
The front line for CISOs is to protect their technical security solutions and assets as well as their data.

More than half of all organizations are in the managed or optimized stage for protective technology and data security. But their progress falls off sharply for maintenance, awareness and training, identity management, and information protection processes—all key areas for safeguarding a firm's network and data.

Organizations advanced in NIST show the way: they have made far more progress in all areas, but especially in those where fundamental cyber hygiene is vital, such as maintenance and information protection processes. Maintenance is a weak point for many organizations.

Telecoms firms and insurers are the furthest ahead in protection activities, while media firms and manufacturers are lagging. Yet insurers need to get up to speed on identity management—an area where consumer firms have made firm progress. "Identity management and access controls are critical—the keys to the kingdom, so to speak," said Deborah Wheeler, global CISO at Delta Air Lines. "If you can't do those right, nothing else you do is really going to make any difference."

% managed or optimized in each area by NIST maturity



% managed or optimized in each area, by industry Green = highest percentage(s) across industries; red = lowest percentage(s) across industries.

	Telecoms	Insurance	Life sci.	Aerospace	Financial	Technology	Retail	Consumer	Energy	Automotive	Public	Healthcare	Media	Mfg.
Protective technology	63%	63%	55%	49%	59%	61%	55%	59%	53%	59%	62%	48%	48%	38%
Data security	56%	56%	55%	58%	46%	58%	56%	50%	54%	51%	45%	55%	48%	51%
Maintenance	45%	45%	44%	40%	44%	39%	39%	40%	45%	39%	31%	43%	28%	35%
Awareness and training	40%	44%	43%	44%	37%	38%	36%	31%	40%	29%	28%	29%	33%	41%
Identity mgmt./access control	43%	34%	41%	39%	38%	36%	40%	43%	31%	35%	34%	21%	30%	25%
Information protection processes	40%	38%	33%	40%	39%	31%	33%	35%	33%	40%	44%	33%	28%	18%
Average	**48%**	**47%**	**45%**	**45%**	**44%**	**44%**	**43%**	**43%**	**43%**	**42%**	**41%**	**38%**	**36%**	**35%**

Q11. What progress have you made in each of the following activities to proactively manage your security posture to *protect* against cybersecurity risks? (Top 2 managed or optimized)

Detect: Organizations need to go beyond detection to continuous monitoring

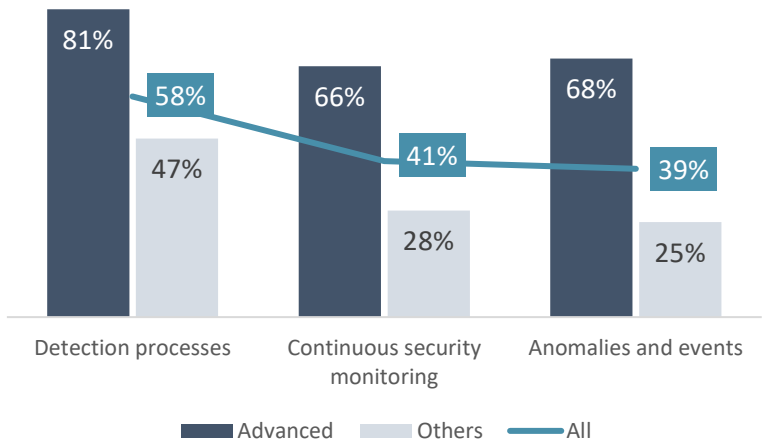
Most organizations need to do much more to catch up in detection activities as they face more complex and insidious cyber threats.

Almost 6 in 10 organizations are in the managed or optimized stage for detection processes. While this is good progress, most are doing less well in continuous security monitoring, particularly around anomalies and detected events. Those in the NIST advanced stage have these areas particularly well covered—but the gulf with other firms is wide, especially in anomalies and events detection.

Most entities need to pay closer attention to detection, a critical tool in the cybersecurity arsenal. This is underscored by the fact that, according to our survey, it takes organizations 128 days on average to detect a breach—a delay that can be extremely damaging and costly. Investing in advanced SIEM and SOAR platforms can help drive results (see page 57).

"Proactive action such as continuously monitoring network traffic helps us in truly enabling real-time threat detection," said the CEO of a medical device maker in Canada. Agreed another C-level executive at a US-based software firm: "Real-time monitoring and analysis of end-user activity assist our organization in detecting anomalies that depart from usual usage patterns, such as logins from previously unknown IP addresses or devices."

% managed or optimized in each area by NIST maturity



% managed or optimized in each area, by industry

Green = highest percentage(s) across industries; red = lowest percentage(s) across industries.

	Public	Consumer	Financial	Life sci.	Insurance	Retail	Telecoms	Tech.	Automotive	Aerospace	Energy	Healthcare	Media	Mfg.
Detection processes	65%	63%	65%	63%	55%	65%	68%	64%	59%	55%	53%	48%	46%	45%
Continuous security monitoring	51%	45%	44%	46%	50%	44%	41%	36%	35%	43%	33%	38%	36%	31%
Anomalies and events	44%	44%	41%	41%	44%	36%	36%	41%	44%	36%	43%	31%	35%	33%
Average	**53%**	**51%**	**50%**	**50%**	**50%**	**48%**	**48%**	**47%**	**46%**	**45%**	**43%**	**39%**	**39%**	**36%**

Q12. What progress have you made in each of the following activities to *detect* cybersecurity risks? (Top 2 managed or optimized)

Respond: Many organizations fall short

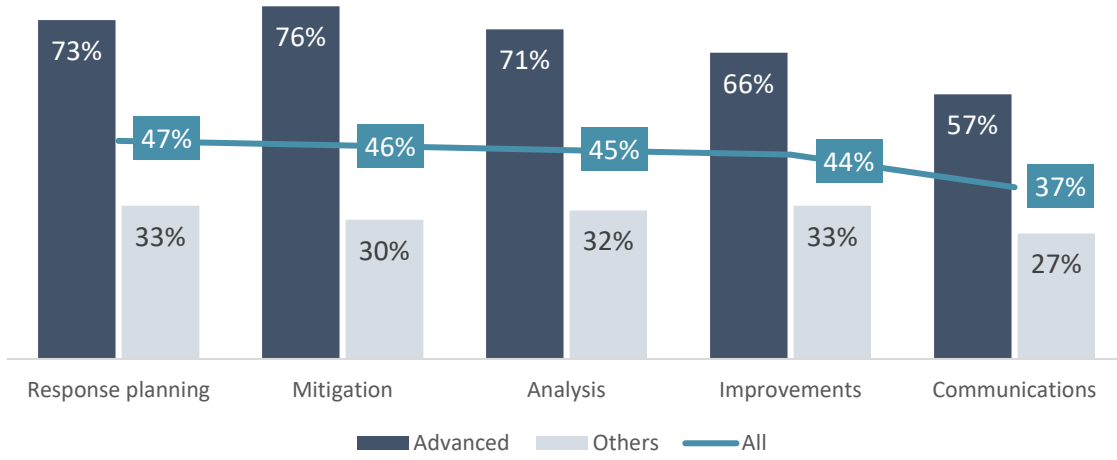
With cyber incidents inevitable in today's world, response planning, mitigation, and communications have become essential. Many organizations are not doing enough.

"One of the most important components of managing cyber risk in the organization's developing network is an incident response plan," said the CTO at a US medical device maker. Nevertheless, less than half of organizations are in the managed or optimized stage for most response areas.

Communications is a particular weak spot, despite the importance of reaching out to all stakeholders and law enforcement agencies to contain the effects of a breach. "Robust incident response planning is table stakes for any organization today. And given the significant reputational risks associated with today's evolving cybersecurity landscape, an increasingly critical component of that process is comprehensive cybersecurity crisis communications planning," said Jamie Singer, executive vice president at Resolute.

"It is imperative that organizations invest the time and resources in developing clear and consistent communications protocols, including streamlining internal messaging review and approval processes, to ensure timely and effective communications responses to these complex issues," she added.

% managed or optimized in each area by NIST maturity



% managed or optimized in each area, by industry Green = highest percentage(s) across industries; red = lowest percentage(s) across industries.

	Life sci.	Telecoms	Financial	Consumer	Insurance	Energy	Aerospace	Tech.	Retail	Automotive	Public	Healthcare	Mfg.	Media
Response planning	55%	51%	48%	45%	60%	49%	44%	41%	38%	43%	53%	46%	45%	35%
Mitigation	53%	53%	53%	45%	49%	43%	41%	44%	45%	50%	43%	43%	40%	34%
Analysis	58%	48%	53%	39%	51%	51%	49%	44%	44%	40%	39%	45%	31%	38%
Improvements	45%	53%	51%	59%	41%	48%	48%	36%	48%	40%	31%	38%	39%	40%
Communications	44%	40%	34%	50%	35%	35%	35%	51%	39%	38%	37%	30%	29%	26%
Average	**51%**	**49%**	**48%**	**48%**	**47%**	**45%**	**43%**	**43%**	**43%**	**42%**	**41%**	**40%**	**37%**	**35%**

Q13. What progress have you made in each of the following activities to *respond* to cybersecurity risks? (Top 2 managed or optimized)

Calls to action: Be risk ready

Run simulations at every level

Sydney Klein
CISO, Bristol Myers Squibb

"Companies need to be really excellent in their response and their recovery. That is where we make sure that we focus a good amount of time, everything from what are our business continuity plans to, how would we communicate within the organization. We are very diligent in practicing our response through simulations, which we do throughout the company with different lines of business. We want to ensure that we're really practiced at the individual level all the way up to our CEO and their leadership team to make sure that the leadership really knows how to guide us in those times where we're responding to an incident and every single minute counts."

Don't underinvest in reactive measures

Augusto Barros
Vice President, Cybersecurity Evangelist, Securonix

"Organizations need to find the right balance between protective and reactive measures, such as detection and response. Security executives often invest more in protective measures and not enough to handle situations when they fail. These investments should allocate resources appropriately across people, process, and technology. Responding successfully to an attack is often human driven but it also requires effective processes and latest technologies, such as SOAR and EDR."

Develop an actionable playbook

Kevin Powers
Founder and Director, MS in Cybersecurity Policy, Boston College

"When you have a breach, regulators will not only be looking at that, but also will be judging you on how you respond, mitigate, and recover, focusing on your incident response plan and whether it was effective and how you utilized it. Many organizations are using an off-the-shelf response plan from a vendor, which is not tailored to their unique circumstances. You need an actionable playbook detailing what you are going to do and who is in charge of what. Everyone should know they are on the team and understand their roles—and their deputies should be trained as well, just in case the general counsel happens to be in Hawaii.

You need to have answers to a multitude of questions: Who makes the call on whether it's a data breach? Who calls the FBI? If you plan to pay off ransomware, do you have Bitcoin to pay with? Will you get in trouble with the FBI or the Office of Foreign Assets Control if you do? What happens if you whole website goes down? Do you have an assist site ready to go right up?

And do you have a communication team in place to deal with outside parties, vendors, and customers? What about your employees—do you have a plan for them, what they should do, and who they should communicate with?"

Recover: Organizations make plans, but do not always revisit them

Planning for recovery after a cyber incident is crucial, and most organizations are making progress. However, they often neglect to make needed improvements after a breach—a mission-critical activity in the recovery phase.

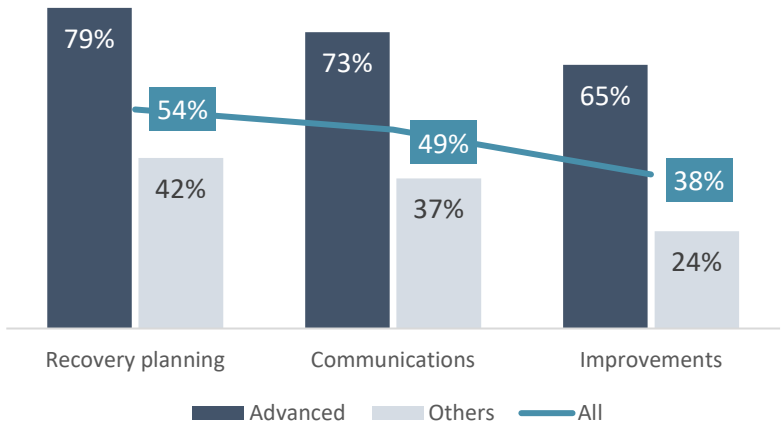
More than half of organizations are advanced in recovery planning. "We invest in security and resilience, and forge relationships internally and externally as part of our planning, response, and recovery procedures from cyberattacks," said the CTO of a UK wealth manager.

But only 38% have made good progress in improvements after a breach, failing to apply lessons learned after an incident to prevent future events. Those advanced in NIST maturity are doing better, but less than a quarter of others are managed or optimized in this area.

Communications with stakeholders and the public after a breach is critical for organizations to safeguard their reputations. Reputational risk can be huge: 37% of organizations in our study believed the biggest cost of a security incident was lost brand value. The reputational costs are even higher for sensitive industries, such as life sciences (48%), energy and utilities (41%), automotive (41%), and financial services (39%).

"You really have to invest in response and recovery, because incidents will happen—and how fast and how effectively you react will mitigate a great amount of potential damage," said Gary McAlum, board director, National Cybersecurity Center.

% managed or optimized in each area



% managed or optimized in each area, by industry Green = highest percentage across industries; red = lowest percentage across industries.

	Telecoms	Retail	Insurance	Consumer	Life sci.	Financial	Public	Aerospace	Energy	Technology	Automotive	Healthcare	Media	Mfg.
Recovery planning	63%	59%	60%	60%	64%	62%	52%	50%	56%	49%	45%	43%	45%	48%
Communications	56%	55%	49%	40%	40%	47%	53%	61%	51%	58%	48%	41%	49%	39%
Improvements	45%	44%	45%	50%	44%	36%	39%	31%	35%	34%	31%	40%	29%	30%
Average	**55%**	**53%**	**51%**	**50%**	**49%**	**48%**	**48%**	**47%**	**47%**	**47%**	**41%**	**41%**	**41%**	**39%**
% ranking reputation losses as main impact	**33%**	**35%**	**31%**	**38%**	**48%**	**39%**	**41%**	**33%**	**41%**	**39%**	**41%**	**35%**	**38%**	**30%**

Q14. What progress have you made in each of the following activities to *recover* from cybersecurity risks? (Top 2 managed or optimized)

Case study: Southern Company

How a resilience mindset helps a utility cope with upheaval

Curley Henry
Vice President and
Deputy CISO
Southern Company

For gas and electric utility Southern Company, resilience in troubling times comes down to extensive preparation, according to its deputy CISO, Curley Henry.

Because Southern Company is part of the national grid and therefore houses critical infrastructure, it has a resilience mindset that involves being prepared for a variety of threats—from hurricanes and physical interruptions to cyber attacks. This mindset has helped to persuade top management to invest more in cybersecurity, because the goal for the company is 98% uptime for its assets. Unlike at other types of companies where he has worked, a breach at Southern Company would not just be about bad publicity or a hit to the share price. "It's about how this will impact our customers and communities that rely on power for everything they are doing day in and day out," he says.

The aim, Henry says, is to change the conversation from a jargon-heavy discussion to one about resilience and preparing for adverse events. "We don't know what tomorrow's threat will be, anything from another wave of pandemic or something totally different, such as negative outcomes for our company arising from geopolitical tensions," notes Henry.

One potential scenario would be cyber attacks on critical infrastructure like the kind operated by Southern Company as a result of the conflict between Russia and Ukraine. "Ransomware was already originating in places where a government is allowing those types of activities to occur—such as Russia," he says. "What might they ask those groups to do in response to heavy sanctions? What if the 200% increase that we've seen in ransomware and other attacks over the past couple years is just a blip on the radar for what could be tomorrow?"

The key is practice. "We do tabletop exercises going through every part of the business to see how it would respond if an incident were to occur," he explains. These sessions include not just the security and IT teams but all parts of the firm, such as power production, customer service, corporate communications, and legal. "The entirety of the business comes into play," says Henry. His team does these exercises for the entire company at least once per year, plus individual exercises for particular areas where it sees the need. The exercises use real equipment as much as possible and address vital issues such as how to find the source of an outage, and how to recover the grid and bring the power back up.

The pandemic served as a test case

Southern Company continued to serve 9 million customers daily, either on-site, in the field, or while working remotely during the pandemic. Its preparations helped it to do well. "There was a thoughtfulness ahead of the pandemic regarding our infrastructure—and securing that infrastructure—that allowed us to both survive and then thrive during this timeframe," he says. "We had to consider the types of attacks that would affect us if everyone were remote. While we had to make some adjustments and adaptations for these new areas of risks and gaps, on the whole I was pleased with our response, which allowed people to continue working in a secure manner."

Its precautions included having a flexible security architecture that allowed for a huge surge in remote working through VPN access to the network. "While the previous high was around 6,000 people, we were able to immediately quadruple that when everyone had to go home," says Henry.

Building a risk-based approach into maturity models

To ensure the best results, organizations are combining a risk-based approach with the use of cybersecurity maturity frameworks. Such an approach involves regularly assessing risk probabilities and impacts, conducting advanced quantitative and scenario analysis, incorporating cybersecurity into enterprise-wide risk management, and working with business leaders to proactively mitigate risks. Over 4 in 10 organizations now take a risk-based approach to cybersecurity and have the needed governance processes in place.

A risk-based approach is key to achieving cybersecurity proficiency: it enables organizations to identify, measure, prioritize, and manage the cyber threats they face in line with their enterprise risk management framework. Not surprisingly, insurers are furthest along in having a risk-based approach and governance, while the public sector is furthest behind. A risk-based approach is more common among enterprises with over $20 billion in revenue (46%) and those based in Australia (51%), the UK (49%), and the US (47%).

Yet only a third of executives say that benchmarking and quantitative analysis are crucial for their cybersecurity planning, and even fewer say that the board and senior management teams understand cyber metrics. Part of the solution is for CISOs to communicate better with boards and senior executives in understandable business terms. “CISOs must drive the conversation with the board, fighting for time beyond quarterly meetings where cyber is only a small part of the agenda,” said Steve Durbin, CEO, Information Security Forum. “They must help address and answer difficult questions regarding cybersecurity and clarify misconceptions.”

Better collaboration across teams is another best practice. Some 37% of executives report that their cyber teams are working with IT and business teams when they develop tech-enabled processes, products, and services. Such up-front cooperation should be further encouraged in order to foster a cyber mindset and practices across the enterprise.

% agreeing with statement about risk-based cybersecurity at their organization, with industry highs and lows

Statement	All	Industry high	Industry low
We have adopted a risk-based approach to cybersecurity and have the governance processes in place that enables effective decision-making.	43%	Insurance 58%	Public sector 31%
Our cybersecurity team works up front with the IT and business team to develop technology-enabled processes, products, and services.	37%	Consumer products (45%)	Automotive (28%)
Benchmarking and quantitative analysis are crucial for setting our cybersecurity plans.	32%	Media & ent. 43%	Insurance 25%
Our cybersecurity metrics are well understood by the board and senior executives.	23%	Public sector 31%	Manufacturing 15%

Q20. Which of the following statements regarding cybersecurity at your organization do you agree with?

> “Risk-based management aligns security priorities with the business and helps security leaders become more strategic in their views and outcomes. The board, business heads, CFOs, and CROs all think about risks and tradeoffs. Mature organizations work with IT and the GRC teams to operationalize risk decisions within technical and process controls. The whole team goes faster, with less risk and friction, and more visibility.”
>
> **Barbara Kay**
> Senior Director, Product Marketing, Risk, Security, and ESG, ServiceNow

How organizations cultivate a risk-based approach

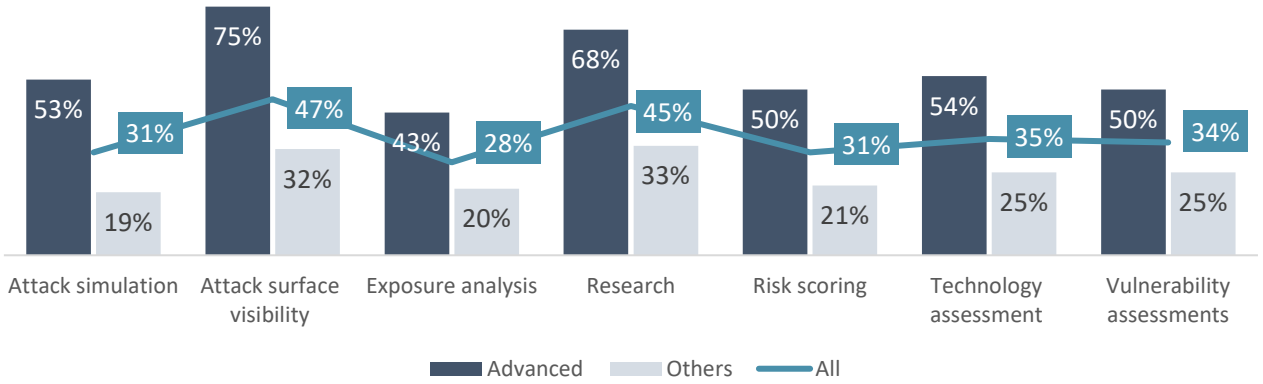
A risk-based approach to cybersecurity can help organizations stay safe in a world of interconnected risks, where major disruptions, such as COVID-19 and the war in Ukraine, can happen suddenly and have cascading impacts on business and government. But what does it mean to be risk-based?

A risk-based approach builds on the NIST framework's recommendation for a risk management strategy that establishes risk tolerances, assessments, and response activities for the business and its supply chain. Our research revealed a link between NIST and risk-based maturity: organizations that are advanced in NIST are well ahead of others in key areas of risk-based management. Three-quarters of those advanced in NIST have made significant progress in attack surface visibility vs. only 32% of others. With the pandemic extending the boundaries of work and expanding entry points for malicious access, CISOs understand all too well the need for greater attack surface visibility.

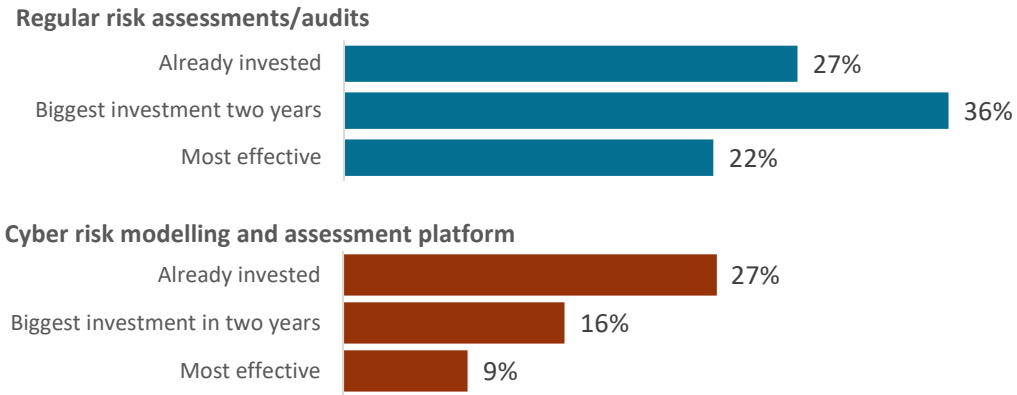
"To take a risk-based approach, it is critical to understand your true exposure to a cyberattack and focus remediation efforts accordingly. Firms need to have the visibility and context across their attack surface to understand which vulnerabilities, if exploited, can cause the greatest harm to the business," said Gidi Cohen, CEO, Skybox Security. "By conducting exposure analysis, they can identify vulnerabilities and correlate them with their unique infrastructure and security controls to determine where cyberattacks pose the highest risk."

Only 27% of firms have invested in risk audits and modeling platforms. More than a third will make a big outlay in audits in two years. Fewer will invest in modeling platforms. Dr. Ivo Pezzuto, professor of digital transformation at the International School of Management, notes that sometimes in the models the worst-case assumptions are not severe enough. Richard Rushing, CISO at Motorola Mobility, a Lenovo Company, agreed: "You need to think outside the box on worst-case scenarios, with a whole spectrum of what could happen and how you'd respond. These should include the most awkward scenarios—such as compromise of a CEO's email or extortion."

% managed or optimized in each area by NIST maturity



Investment and effectiveness



Q15. What progress have you made in each of the following activities to *proactively manage* cybersecurity risks? (Top 2 managed or optimized).
Q18. Which of the following cybersecurity initiatives around process have you invested in, which have been the most effective, and in which will you be making the biggest investment in two years?

Calls to action: Taking a risk-based approach

Follow a risk-based approach

Gary McAlum
Board Director, National Cybersecurity Center

"You must take a risk-based approach because you can't secure everything a hundred percent. There are a lot of questions to ask: What is the business of the business? What does the risk profile look like? What are the threats? What are the implications? And what is the governance process that an organization goes through to make risk-based decisions?

Today, risk assessment is mostly subjective, but there are start-ups out there with new tools that will allow a much more quantitative model—the cyber world isn't there yet, but it's heading there. You need to do your homework on the highest probability of risk and highest impact and decide if you will avoid it, accept it, transfer it or mitigate it, and how much you are willing to spend to do that mitigation. Having a zero appetite for any cybersecurity risk is not affordable, nor feasible. Companies should work on a better capability for quantifying risk, but they must accept a certain amount of risk based on their risk appetites."

Build a multidimensional lens

Gidi Cohen
CEO and Founder, Skybox Security

"Proactive security posture management starts with gaining holistic visibility across the entire attack surface, including IT, OT, and hybrid environments. This is possible by developing a multidimensional network model representing the connections and security configurations across these environments. Then an organization can simulate and analyze all possible paths and interactions across its unique network to analyze security controls and identify exposure and compliance risk.

Organizations can leverage this insight to optimize security controls and access, validate configurations and changes, and precisely measure and identify their exposure to potential cyberattacks. With insight into true exposure and business risk, organizations can quantify their cyber risk and make informed decisions about where to focus remediation efforts."

Map your risk profile to your business

Steve Durbin
CEO, Information Security Forum

"Security is all about the management of risk, and the key element in any risk assessment is the business impact—your risk profile has to map to what you are trying to do as an organization. Generally, across the enterprise, you will probably be doing qualitative-based risk assessments, but in some areas a quantitative approach will be the way to go because your board or finance director will want to know the numbers. Because the threat landscape changes so very quickly, forecasting threats—particularly when they will come to pass—is increasingly difficult, even though mature organizations are getting very good at forecasting what those threats might be. Many large companies already have competency in risk assessment in the enterprise risk management group, but often it may not be accessible to the cybersecurity group because of internal politics and corporate silos—that needs to change."

"We invest in people, process, and technology. But the people side is the most critical area for investment. Technology comes and goes. The challenge is trying to ascertain what you actually need—what's worth investing in while fully utilizing what you already have in house."

Deborah Wheeler, Global CISO, Delta Air Lines

5. Investing in people, process, and technology

Recalibrating cybersecurity investment around people, process, and technology

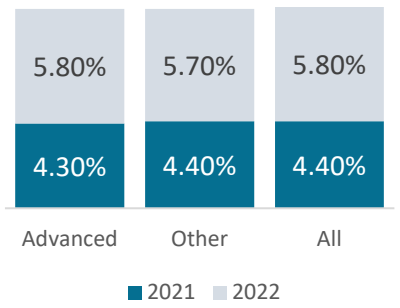
To keep up with digital transformation and attacks from adversaries, organizations are making a step-change in cyber spending from 2021 to 2022. In the past, allocating 5-7% of IT spending to cybersecurity was considered the gold standard. In 2022, the target will be about 12-15%.

Average enterprise IT spending will increase from 4.4% of revenue in 2021 to 5.8% in 2022. Cybersecurity spending as a share of that IT budget will go up even more—almost two percentage points on average. And cybersecurity investment as a share of overall revenue is also jumping, by almost 30 basis points, from 0.53% to 0.80%. (These percentages are significantly higher than the average cybersecurity spending of 0.09% of revenue when we last conducted the study at the end of 2019.) Our analysis shows that having adequate cybersecurity budgets is critical for ensuring the best outcomes (see page 71).

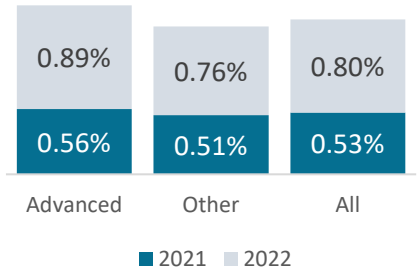
Cybersecurity spending on the cloud is also climbing as firms expand their use of cloud platforms and services. "CISOs will prioritize investments in more cloud-native, usable security services—not large security platforms—to enable secure digital business," said Ravi Srinivasan, CEO of Votiro. Firms advanced in NIST are spending a larger percentage of their IT budgets on cybersecurity and on cloud cybersecurity than others—and plan heftier increases in 2022.

Investment must be properly allocated to support plans around people, process, and technology. Juan Morales, CISO of Realogy, believes it best to apportion spending equally among the three pillars (see next page). Regardless of that balance, spending will need to continue to rise. "CISOs must ensure they develop their people, processes, and technologies with the speed and agility required by today's volatile, uncertain, complex, ambiguous, and interconnected environment," said Cory Simpson, executive vice president with Resolute.

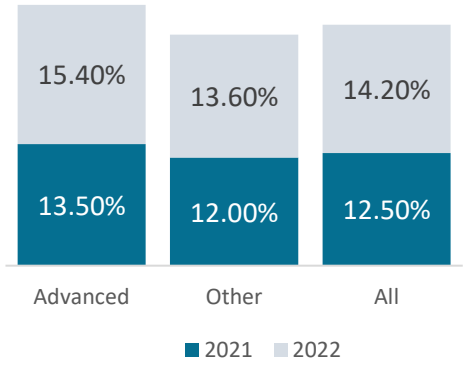
Overall enterprise IT spend by NIST maturity (% of revenue)



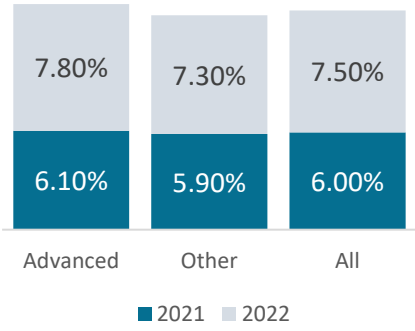
Cyber spend by NIST maturity (% of revenue)



Cyber spend by NIST maturity (% of IT spending)



Cloud cyber spend by NIST maturity (% of IT spending)



Inadequate budgets are the biggest cybersecurity hurdle for **30%** of organizations in our study and **34%** of NIST early implementers.

Q16. Please tell us your organization's total annual enterprise IT spending, total cybersecurity spending, and total spending on cloud cybersecurity tools in 2021, and what you expect them to be in 2022.

Case study: Realogy

Finding the right balance between people, process, and technology

Juan Morales
CISO
Realogy

Juan Morales, CISO at real estate giant Realogy, sees cybersecurity as a three-legged stool that requires equal distribution of resources across people, process, and technology.

For Morales, it is all about finding the best balance between the three pillars of people, process, and technology. “You can never rely on one more than the other in order to have a sound and comprehensive security program,” he says. Without the right people to understand the technology, an organization won’t be able to get the most from it, he argues, but on the other hand, great talent needs the right tools to push the effort forward. “And ultimately, if you don't understand the processes and workings of an organization, it doesn't matter that you have the right talent or the right technology,” says Morales. “It has to be an equal distribution of focus among the three.”

“One problem in information security culture today is we've gotten away from the fundamentals, and we are looking instead to technology to solve our problems—a lot of us get lost in the next new shiny object to come along,” he says. “But where we can really make a lot of difference is just leveraging basic controls and simple things to protect our environments that that can be addressed without a huge investment in technology.”

Rather than technology adoption, Morales sees his biggest success as a CISO around people. He has been able to hold onto the talent built over the years by “ keeping people engaged, motivated, and excited about the work we are doing.”

That said, Morales does take advantage of technology advances that help Realogy’s cybersecurity team enhance its focus on anomaly detection and response. “We've worked towards building extreme insights into all our systems, logging sources, and entry points,” he says. “But to make sure we continue to develop and evolve our capabilities we are now taking a more preventative approach.”

To this end, Realogy is shifting to a next-generation endpoint detection and response (EDR) solution that will give it more capabilities. The new EDR system will add a blocking function and advanced detection/response abilities using more sophisticated machine learning.

Signatures vs. behaviors

“Moving away from simpler, signature-based technology toward true behavioral analysis-based detection is one of the key capabilities required nowadays, given the way malware operates,” says Morales. “The most sophisticated malware can bypass traditional controls and evade signature-based detections. Behavioral detection powered by machine learning moves the needle forward.”

Behavioral detection looks at what the malware is set up to do, evaluating every line of code executed by the object for malicious or even suspicious activity, and if needed, shutting it down. “Our old EDR system had very limited blocking capabilities, but when our new one sees particular behaviors, it will automatically block them from fully executing,” notes Morales.

People

Investment in training and skills in a time of high demand

With cybersecurity talent in short supply, upskilling of cyber and IT staff will be the top people-related investment over the next two years—cited by nearly half of organizations. Risk preparedness training for management and securing the human layer will also be high on the priority list.

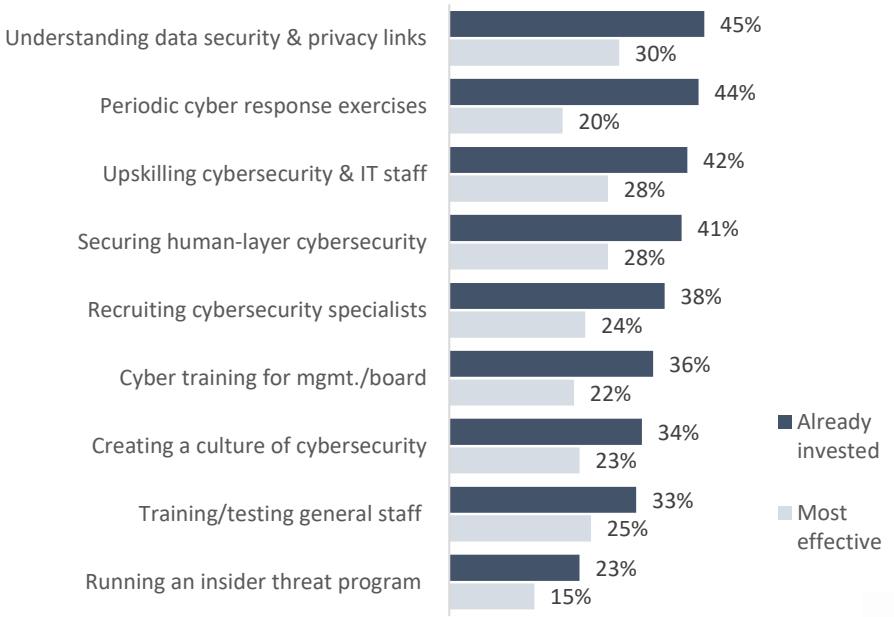
"We are growing and training our cyber staff to secure our organization from potential threats," said the CTO of a German capital equipment maker. Juan Morales, CISO of Realogy agreed: "We are continuously investing in the training and development of our people and making sure they are up to speed and engaged."

Nearly a third of entities also plan to invest in recruiting and retaining cyber specialists, a task that may grow more difficult—and costly—as demand for cyber expertise continues to grow.

With human error the cause of many breaches, a third of entities intend to invest more in securing human-layer cybersecurity. This builds on training methods by delving into human communication patterns and behaviors of employees, so they can improve on skills geared to their own security behavior. The CTO of a Japanese entertainment firm said his company has benefited from implementing user behavior analytics.

Around a third of firms will boost outlays for risk preparedness training for management and the board, and for cyber response exercises for key internal and external stakeholders. The best results come from involving the full team, including C-Suite executives, and from creating intense environments that mimic actual attacks.

Top investments now in people initiatives and effectiveness



Top people investments over the next two years

Area	% investing
Upskilling cybersecurity and IT staff	46%
Cyber risk preparedness training for management and board	34%
Securing your organization's human-layer cybersecurity	34%
Recruiting and retaining cybersecurity specialists	31%
Periodic cyber response exercises for key internal and external stakeholders	31%
Ensuring understanding of cybersecurity and data privacy linkages	30%
Training/testing of general staff in cybersecurity	27%

> Deepfake is a big concern. Our staffs are our first line of defense in the fight against deepfakes. Our firm provides deepfake technology training sessions that cover all areas of the technology.
>
> **Chief compliance officer**, life sciences firm, US

> We have adopted a 'privacy by design' approach that keeps valuable biometrics on a user's device that provides protection against insider threats.
>
> **Chief legal officer**, public sector, Brazil

Q17. Which of the following cybersecurity initiatives around *people* have you already invested in, which have been the most effective for your organization, and where do you plan to make the biggest investments over the next two years?

People

Calls to action: Human layer and culture

Improve cyber culture through regular training

Erich Kron
Security Awareness Advocate, KnowBe4

"Because modern cyber threats are so significant, organizations should strive to improve their security culture and the secure behaviors of employees through regular and consistent education and training. Even with high-tech exploits being used in cyberattacks once within the networks, the initial network intrusions most often start with a low-tech phishing attack, making the humans the biggest target and the best point of prevention."

Focus on changing attitudes, not on knowledge

Joseph Steinberg
Cybersecurity Expert Witness and Advisor, Cybersecurity and Artificial Intelligence Expert Services

"You must ensure that every single person within your organization understands that they are real targets; sometimes, even a single, short conversation can help employees understand that such is the case. This is not the same thing as training—the goal of this effort is to change *attitudes*, not to increase knowledge. People who believe that criminals want to breach their computers and phones, and steal their data, respond differently to various stimuli than do people who don't understand this reality. This can make a world of difference when it comes to information security."

Communicate risks in a common language

Moayad Aiash
Cyber Security Lead, Hatch

"A company breach has become a matter of 'when' for any operating organization of any size in today's world. It is a fact that the cyber world ahead of us is going to be even riskier. In our journey to defend against cyber threats, we must work on shifting the organization's culture to be more cyber aware and risk averse. This can be most efficiently done when cyber leaders and professionals engage with the business and communicate the cyber risk in a common language that the business understands. Cybersecurity is the responsibility of everyone and must be seen as a business imperative."

Develop training to go with the times

Kevin Powers
Founder & Director, MS in Cybersecurity Policy, Boston College

"You must focus on business continuity and think of what happens if you go down today. You can't only rely on the annual cybersecurity training; you need a proper cyber culture and real, targeted training that goes with the times. All employees within an organization, whether in or outside the IT department, must be properly trained on cybersecurity as that is part of their job—the business of cybersecurity is business!"

Case study: Texas Health Resources

Making staff part of your security team

Ron Mehring
CISO
Texas Health Resources

As it struggled to cope with the shocks of the last two years, Texas Health Resources, like many other healthcare providers, put digital transformation on the fast track as a matter of necessity.

Like many healthcare firms, Texas Health Resources was moving conservatively on digital transformation before the pandemic hit. "We were on a very slow trajectory, like turning an aircraft carrier, but we had to shrink everything into months or weeks instead of years," says Ron Mehring, the non-profit's chief information security officer. "We went from a long-range plan to a very short-range plan."

The acceleration involved not only remote working by non-front-line employees, but also increased use of telehealth and patient video communications. The company also sped up cloud migration for key applications. These measures required new security procedures and controls.

Mehring says that it's important in a complex organization like Texas Health—with a mix of modern and legacy systems—to understand how people are interacting with data and their use cases, to create procedures and controls that are both effective and not so onerous that people stop cooperating.

"It's important to ensure that you haven't created an environment that's forcing the user to come up with creative workarounds," he says. "And that requires just good, solid collaboration and communication and understanding people's friction when using these systems."

Building a security mindset across the organization

Mehring says communication is crucial. "The first thing the CISO has to do is to deputize everyone. No security team is ever big enough, but you can tackle problems by bringing people into the equation and letting them understand that they have a specific role in ensuring that security practices are maintained within their areas." Mehring's team assigned people within each different organizational domain to help develop standards and specifications with their peers to drive security in those areas.

Mehring explains that the culture at Texas Health—based on "high reliability" principles that encourage trust and transparent, honest communication—has helped him in getting people to take on additional security roles. "Our values influence people to want to help secure our systems, help enforce privacy, and ensure that we are doing things ethically," he says. The role of senior executives is critical in reinforcing this culture, Mehring adds.

Whether communicating the importance of cybersecurity to the board, mid-level committees, physician groups, or general employees, Mehring says the key is exceptional storytelling and brutal honesty. "My staff has been trained on how to do data visualization and storytelling, as well as how to convey appropriate messages effectively to each group," Mehring explains.

The aim is to engage people and make them part of the company's security. "Everyone at Texas Health is part of our cybersecurity program—it's is not just 30 people, it's 25,000 people with different roles in that program," he says.

Process

Process investments are boosting capabilities

Firms have invested in a variety of process improvements to strengthen their cybersecurity capabilities. Security monitoring and threat detection, test of backups and disaster recovery, and protecting IT and OT assets have been their top investments so far.

In recent years, developing a security monitoring and threat detection capability has been a major area of effective investment for 31% of organizations, one they intend to continue over the next few years. For some, this could include upgrading or replacing a SIEM system (see page 57). The same share of respondents have invested in setting up a backup and disaster recovery site, although executives will be reducing their investment in this area in the future. Another prominent area of investment is protection and remediation of growing IoT and OT vulnerabilities. However, entities have struggled to make these investments effective, because of the complexity of OT vulnerability management, unsecured older devices, and patchworks of legacy systems. Organizations plan to make big investments over the next two years to harden these attack surfaces. (See pages 53 and 56 for IT-OT solutions.)

One area gaining momentum is conducting risk assessments and audits—an important part of a quantitative risk-based approach to cybersecurity. Another is developing a cyber incident response and recovery plan, a key step to stay risk-ready and resilient. The process area that will see the largest relative drop in investment is the application of Zero Trust principles, which has proven harder in practice than many expected (see page 55). Yet CISOs still stress some of the most basic processes: “Fundamental security hygiene is still the best protection,” says Mandy Andress, CISO at Elastic. “Understand your environment. Change defaults, disable unnecessary services, default deny inbound network traffic, and patch.”

Top investments now and in two years in process initiatives and their effectiveness Green = higher notable percentages; red = lower notable percentages.

Initiative	Already invested	Most effective	Biggest investment 2 years	Difference now and 2 years
Developing and maintaining a security monitoring and threat detection capability	31%	20%	33%	2%
Creating, maintaining, and testing of backups and disaster recovery assets/sites	31%	26%	18%	-13%
Prioritizing IT and OT assets to protect as well as vulnerabilities to remediate	30%	9%	33%	3%
Creating access control policies	29%	17%	20%	-9%
Applying Zero Trust principles	29%	18%	12%	-17%
Setting out responsibilities, governance practices, and documentation	29%	13%	26%	-3%
Hunting cyber threats by proactively searching out malicious or suspicious behavior	28%	16%	21%	-7%
Conducting regular risk assessments, audits, stress tests, penetration tests, etc.	27%	22%	36%	8%
Developing and maintaining a cyber incident response and recovery plan	27%	20%	35%	8%
Optimizing security policy management	27%	14%	30%	4%

Q18. Which of the following cybersecurity initiatives around *process* have you already invested in, which have been the most effective for your organization, and where do you plan to make the biggest investments over the next two years?

Process

Calls to action: Solutions to secure IT and OT

Make hyperconnectivity more secure

Simon Chassar
Chief Risk Officer, Claroty

As digital transformation continues to drive the convergence of IT and OT assets—particularly in industrial, healthcare, and other types of critical infrastructure environments—the only way to mitigate risk is to make hyperconnectivity more secure. There are several steps security leaders can take to protect their IT and OT environments and enable their businesses in today's hyperconnected world:

- Extend risk governance to include cyber-physical assets, including OT, industrial IoT, Internet of Medical Things, and enterprise IoT.
- Maintain proper segmentation between IT and OT networks to stop the lateral spread of ransomware and other malware.
- Ensure that good cyber hygiene practices extend to OT and IoT devices.
- Implement a robust system monitoring program that covers both IT and OT networks as well as the connections between them.
- Assess and build preparedness, such as running tabletop exercises of ransomware attacks, to improve incident response and resiliency.

The cybersecurity industry has made tremendous progress in creating technology solutions that help eliminate blind spots and close security gaps to build resilience. Solutions that can be implemented without burdening existing infrastructure and personnel with unnecessary traffic, hardware, complex configurations, lengthy deployments, or steep learning curves are crucial given the hiring challenges nearly every organization is facing.

Tap support from equipment suppliers

Wayne Dorris
Business Development Manager, Axis Communications

Physical security devices like network cameras, AV systems, and access control devices are a blend of OT and IoT end points. Hardening these devices and managing vulnerabilities to the same requirements of your IT policies is often overlooked.

In many cases an enterprise customer can have anywhere from 1,000 to 100,000+ of these devices in their environment. As a result of the analytics advancements on these types of edge sensors, such as IP cameras, the devices provide more and more business intelligence all the time.

Since most traditional IT security and cybersecurity teams do not have the knowledge or the tool sets to properly configure and manage these devices independently, it's important that they work closely with manufacturers that are leading in the space and can provide support.

Safeguard the urban environment

Brandon Branham
Assistant City Manager and CTO, Peachtree Corners, Georgia

Our biggest cyber investment will be in vehicle protection, particularly as we move more and more into outfitting vehicles with connected technology. I have a corridor that pushes 65,000 cars a day through it, which can cause a lot of problems if our systems are not secure. Just think what happens if a bad guy turns on a left turn signal when the driver—and the car—thinks it is going straight.

Case study: Delta Air Lines

Collaborating to protect digital and physical assets

Deborah Wheeler
Global CISO
Delta Air Lines

Deborah Wheeler, who joined Delta Air Lines as CISO in 2017 after a 20-year career in financial services, faced a new challenge. She needed to draw on her expertise in the financial industry to build the airline's cybersecurity program from the ground up.

"I was hired specifically to bring the best practices from the financial services industry to bear on aviation," she says. While the cybersecurity best practices of a financial institution are often similar to those of an airline, there is one key difference. As part of its airport operations and on board its aircraft, Delta has a base of IoT and connected operational technology (OT) that pose a cybersecurity risk.

Coordination is critical

The key, says Wheeler, is a team approach. "Companies that have both a CSO and a CISO, or have separated physical security from cyber, need them to be collaborating to understand how material physical threats can play out in cyber and vice versa," says Wheeler.

Wheeler must work closely with executives in charge of physical and operational security for flights, aircraft, and airport operations, as well as other related areas. To accomplish this, Delta has a joint working group comprising various teams: cybersecurity, fraud, legal, physical security, and technical operations. It also includes a threat intelligence monitoring and collection team that shares information with the government.

Today's riskier cybersecurity landscape means that this kind of close cooperation, both internally and with external groups, is more important than ever.

"We make sure that we are taking a comprehensive look at physical, cyber, and kinetic threats. (Kinetic threats, which arise from the dynamics of motion, are unique to the airline industry.) Our teams share information and tools, so that we can stay on top of these potential threats and work collectively to mitigate them," she says.

Bringing it all together

The key lesson Wheeler learned over the years is the need for all strands of a cybersecurity approach to mesh together. "You cannot do identity and access management effectively if you don't know what you are trying to protect. Likewise, if you don't have a full regulatory perspective, then you can't properly assess risks. Without these pieces coming together, a cybersecurity program will fall apart."

Process

Zero Trust investments have had mixed results

Over 4 out of 10 organizations now build their cybersecurity programs on Zero Trust principles, and even more risk-based leaders do so. By embracing the credo of "never trust, always verify," these organizations aim to prevent data breaches. But that is often easier said than done, and organizations may invest less in the future.

A German public-sector executive said Zero Trust had been the most effective initiative to mitigate cyber risks: "We have implemented a robust infrastructure that provides full inline inspection, Zero Trust access control, and AI-powered threat prevention to secure us from network attacks." Others find building effective Zero Trust programs to be an uphill battle.

"Zero Trust is great on paper, but in application it brings a lot of challenges," said Brandon Branham, assistant city manager and CTO, Peachtree Corners, Georgia. "If you truly implement Zero Trust and you have multiple systems spread across multiple locations, accessing those systems from a single point becomes difficult." Our research underscores that difficulty. While 41% of organizations have built their cybersecurity programs on Zero Trust principles, and 29% have invested in Zero Trust applications, only a moderate 18% have found them effective. Zero Trust is not yet translating into fewer breaches. Entities with multiple breaches and with no breaches are both investing similarly in Zero Trust.

Implementation is complex

Part of the problem is that continuously authenticating and validating all internal and external network users can be a daunting task. "People talk about applying Zero Trust principles, but that's more of a philosophy. Truly implementing the technical architecture for a Zero Trust security model is a complex journey that is not easy or cheap," said Gary McAlum, board director, National Cybersecurity Center. "The biggest mistake a CISO should avoid is thinking Zero Trust can be achieved with just a new technology solution." He explained that firms will need to rework the existing security architecture to incorporate more micro-segmentation and encryption, and implement continuous monitoring and analysis, as well as attribute-based adaptive authentication. "This will be a significant investment in time, energy, and persistence."

Another CISO mentioned a different hurdle: it's difficult or even impossible to completely implement Zero Trust by retrofitting existing systems. "From a practical standpoint, Zero Trust should be chiefly built around systems that you don't control, such as SaaS providers, where you are validating the connections each and every time--and validating the data that comes through each and every time," he said.

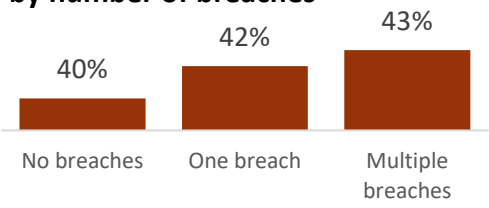
% respondents agreeing

Statement	All	Risk-based leaders	Industry high	Industry low
Our cybersecurity program is built on Zero Trust principles.	41%	44%	Healthcare, telecoms, tech, 48%	Automotive 31%

% investing in applying Zero Trust principles

	All
Already invested	29%
Most effective	18%
Biggest investments in two years	12%

% building on Zero Trust principles by number of breaches



Q20. Which of the following statements regarding cybersecurity at your organization do you agree with? 19.Which of the following cybersecurity initiatives around technology have you already invested in, which have been the most effective for your organization, and where do you plan to make the biggest investments over the next two years?

Technology

Building a tech stack for cybersecurity

Nearly two-thirds of survey respondents have put money into email security technology. For firms with no breaches, it was the biggest investment.

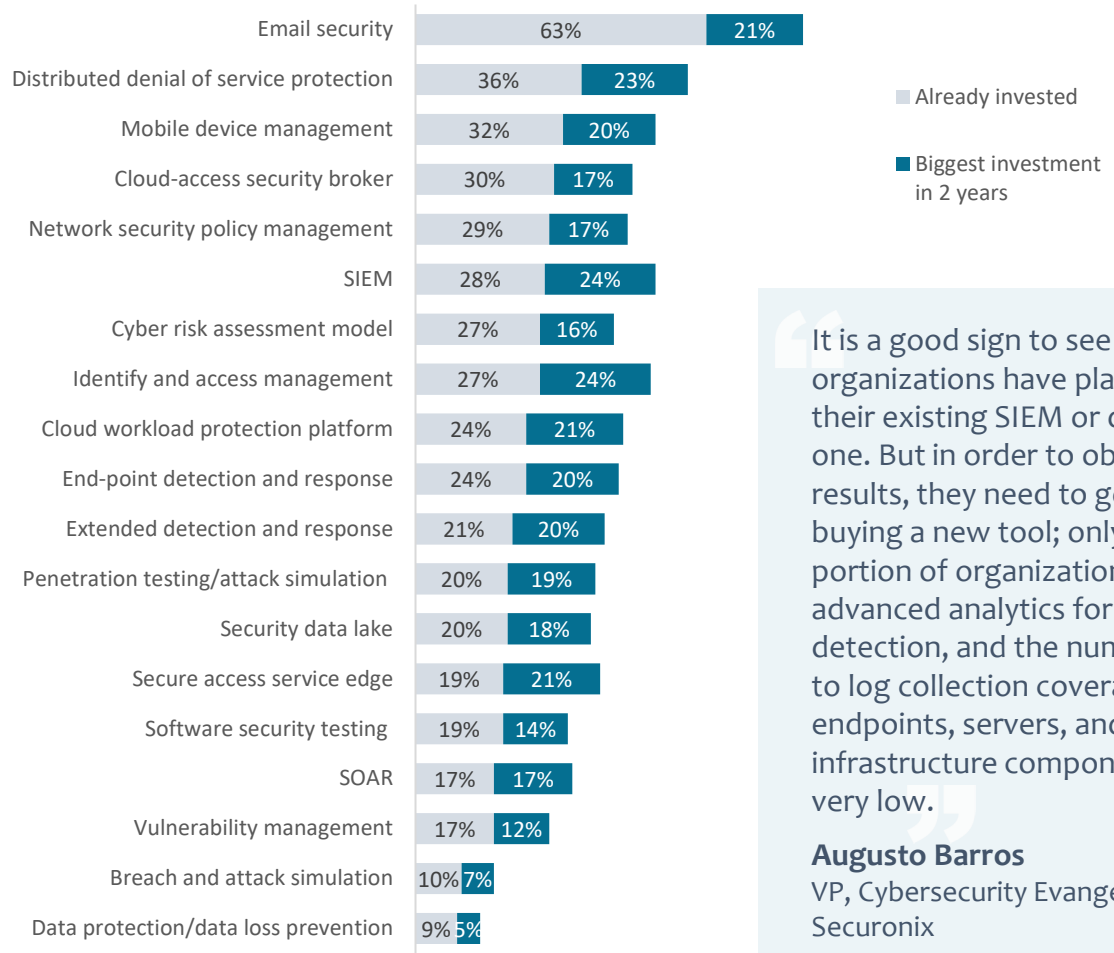
Email security is a wise investment since it reduces time to detect, respond to, and mitigate a breach. However, spending on email security cannot be to the detriment of other defense-in-depth investments. DoS protection is another top investment area—understandably, since DoS is the most common attack vector today. Other top investments include mobile device management, which can help secure remote working; cloud-access security brokers, crucial for securing diverse and open cloud structures; and network security policy management, which can help organizations avoid costly misconfigurations.

Identity management, SIEM, and risk modeling

Nearly a quarter of entities will make identity and access management technology their biggest near-term investment—vital in a world of extended ecosystems and remote working. The same share plan to invest in a security information and event management (SIEM) system, which can provide "more visibility and data points to help make more granular decisions," said Duc Lai, CISO of University of Maryland Medical System. A SIEM can make it easier to filter and spot patterns in huge amounts of security data, but only if it has the right analytical capabilities (see next page). "It will help you find the needle in the haystack," said Lai.

More than a quarter of executives have already invested in cyber risk modeling, used to run scenarios and quantify the probability and potential impact of cyber threats. Richard Rushing of Motorola Mobility and Ron Mehring of Texas Health Services use cyber modeling to make decisions and communicate critical changes in the risk landscape to the board. Other technologies attracting investment include cloud workload protection platforms, end-point detection and response systems, and extended detection and response tools.

Top technology investments



> It is a good sign to see that many organizations have plans to upgrade their existing SIEM or deploy a new one. But in order to obtain better results, they need to go beyond just buying a new tool; only a small portion of organizations are using advanced analytics for threat detection, and the numbers related to log collection coverage from user endpoints, servers, and other infrastructure components are still very low.
>
> **Augusto Barros**
> VP, Cybersecurity Evangelist
> Securonix

Q19. Which of the following cybersecurity initiatives around *technology* have you already invested in, which have been the most effective for your organization, and where do you plan to make the biggest investments over the next two years?

Technology

Improving detection, analysis, and response through SIEMs and SOARs

To defend against growing cyber risks, many are turning to platforms enabling security information and event management (SIEM) or security orchestration, automation, and response (SOAR).

More than a quarter of organizations already have invested in SIEMs, while just under a quarter plan to make a substantial investment over the next two years—and even more among entities advanced in NIST. SIEMs provide a host of benefits, from faster threat detection to higher quality security data. Indeed, the COO of a German healthcare provider said that its most effective cybersecurity investment was in a SIEM. Over the next two years, he said the SIEM solution would be used to "manage and compile our logs to identify threats, suggest a remediation plan, and look for suspicious activity."

But applying the right SIEM solution is essential for success. Our research shows that more than 4 in 10 respondents intend to augment or replace their current SIEM system. And only 11% said it was among their most effective investments. While more basic SIEM systems are rules-based or use a correlation engine, more advanced versions use AI and may include user and entity behavior analytics (UEBA) and a SOAR. In fact, 17% of organizations surveyed have already invested in a SOAR, and another 17% are planning to make a big investment.

A better mouse trap

"One big trend driving SIEM replacement is the cloud," said Mandy Andress, CISO at Elastic. "As workloads migrate to the cloud, monitoring cloud deployments becomes essential to the business. Some older SIEMs needed a lot of care. Today's IT environments provide a firehose of data. While traditional SIEMs can ingest a lot of data, they don't always embed advanced analytics; it could take hours or days to analyze that data, which impacts the ability to quickly investigate suspicious activity."

Newer XDR platforms, said Andress, address broader security operations with several embedded capabilities, including out-of-the-box cloud rules, analytics, and machine learning to draw out anomalies, integrated endpoint capabilities for faster and deeper investigations, and workflow integrations for response automation.

Q20. Which of the following statements regarding cybersecurity at your organization do you agree with? Q19.Which of the following cybersecurity initiatives around technology have you already invested in, which have been the most effective for your organization, and where do you plan to make the biggest investments over the next two years?

% respondents agreeing

Statement	All	Industry high	Industry low
We are looking to replace or augment current SIEM strategy.	44%	Life science 55%	Media & ent. 31%

% respondents investing in SIEMs by NIST maturity

SIEM	All	Advanced	Others
Already invested	28%	28%	28%
Most effective	11%	12%	10%
Biggest investment in two years	24%	28%	22%

% respondents investing in SOARs by NIST maturity

SOAR	All	Advanced	Others
Already invested	17%	18%	16%
Most effective	9%	10%	9%
Biggest investment in two years	17%	19%	15%

> A SIEM-independent SOAR is invaluable for those companies that have multiple SIEMs (very common with M&A), enabling centralized prioritization of SIEM-driven incidents. It can also make it easy to enrich with business data and orchestrate with non-security apps used by IT, legal, risk, procurement, HR, and compliance.
>
> **Barbara Kay,** Senior Director, Product Marketing, Risk, Security, and ESG ServiceNow

Technology

The cloud conundrum

While modern cloud platforms are often more secure than the legacy systems they replace, they can also increase risks when combined with different cloud services and digital solutions. Specialized cloud security tools can help mitigate the risks.

Twenty-two percent of executives surveyed say that increased cloud usage has exposed their organizations to a new set of cybersecurity risks. Chief compliance officers (31%) and CROs (30%) are particularly worried.

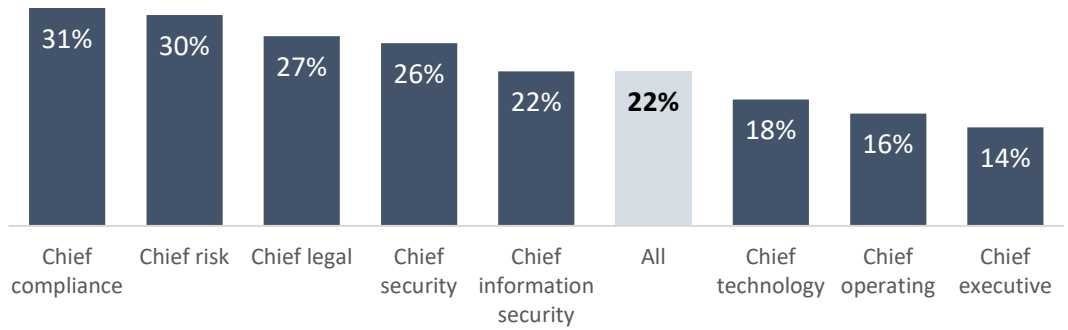
"Because of the pandemic, all of us have increased our interconnectedness," said the CISO of a Wall Street firm. "Part of this expansion is an increasing reliance on open-source software, software and outsourcing providers, and, especially, on cloud providers—which, while generating many benefits, also produce new risks. On balance the cloud is more secure. But it does create this new set of connections, and we are all vulnerable."

To mitigate these risks, organizations are drawing on cloud workload protection platforms that protect cloud workflows. Around a quarter have already invested in these platforms; the figure is higher for more mature firms, which find the solution more effective than others. Nearly a third of entities also use cloud access security brokers that place an intermediary between users, devices, and the cloud. This is especially the case among aerospace and defense companies, which need to air gap their critical assets and data.

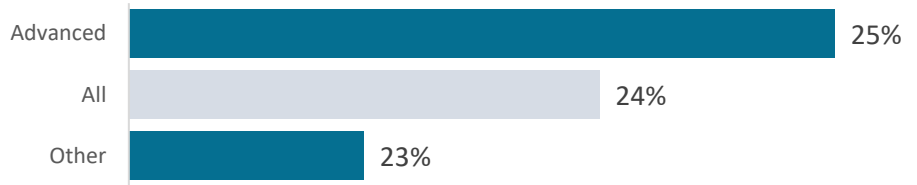
Other cloud tools that help

With the expansion of remote work and, with it, cloud reliance, one firm is using a Secure Access Service Edge approach. That single, cloud-delivered service model brings together wide area networking with various network security services, including Zero Trust, to deliver immediate, uninterrupted access for users at any location. The firm is also strengthening its processes for systems it is building in the cloud, using security orchestration, automation, and response tools. "Like other firms that have large legacy on-premises networks, we know all the mistakes made in building them, and we don't want to repeat them in the cloud," says the firm's CISO.

Executives citing new cyber threats due to increased cloud use



% investing in cloud workload protection platforms, by NIST maturity



% citing cloud workload protection platforms as most effective, by NIST maturity

Q20. Which of the following statements regarding cybersecurity at your organization do you agree with? Q19. Which of the following cybersecurity initiatives around *technology* have you already invested in, which have been the most effective, and in which will you be making the biggest investment in two years?

Technology

Consolidating tools and adopting a platform approach

Around one-third of organizations intend to address a proliferation of cyber tools and infrastructure by consolidating them. A similar percentage is combining security technologies into a platform.

A higher percentage of insurance firms (41%) will be consolidating their tools and infrastructure. Those in earlier stages of NIST maturity are slightly more likely to seek to do so, since more advanced entities have probably already made more progress in this area.

Nearly a third of organizations also are adopting technologies that bring together capabilities that work as a platform, rather than relying on individual "best in breed" components.

The benefits of consolidation

Consolidating tools and infrastructure—and especially, adopting technologies and capabilities as part of a platform—are important strategies for organizations that want to ensure that they don't just have a disparate, non-connecting set of solutions and systems.

Such an approach can also reduce costs. "To lower the cost of creating a trustworthy environment for endpoints, we are utilizing a technology that combines numerous security services into a single platform," said the chief security officer of a Chinese capital equipment manufacturer.

Consolidation and platforms not only boost efficiencies and cost savings; they also provide a higher quality approach and make training easier. As they evolve and become more sophisticated in cybersecurity, private and public entities are increasingly looking to adopt an efficient and cohesive approach to ensure that all parts work well together.

Q20. Which of the following statements regarding cybersecurity at your organization do you agree with?

% respondents agreeing

Statement	All	Advanced in NIST	Other	Industry high	Industry low
We plan to accelerate how we are consolidating tools and infrastructure.	32%	30%	33%	Insurance 41%	Life sciences 26%
We adopt security technologies providing a set of capabilities as a 'platform'.	31%	31%	31%	Consumer goods 44%	Energy & utilities 20%

> I would rather see a tool fully used right in its full capabilities than a spread of tools that are each doing just 40%. I'd prefer to use fewer tools at higher capacity than more tools at lower capacity. One reason is because it's cheaper. Another is that your engineers and the people that are running it get more knowledge about it.
>
> **Head of Information Security and Compliance**
> Educational services, US

> We have a tool that provides a cybersecurity platform with a full suite of services for protecting our organization from phishing attacks, including brand protection, as well as backup for our enterprise email services to assist us in maintaining service continuity.
>
> **Chief Security Officer**
> Industrial manufacturing, Canada

Technology

Calls to action: Making automation work

Automation helps the talent gap

Curley Henry
Vice President, Deputy CISO, Southern Company

"Automation will become even more critically important going forward. The war for talent is tough in our discipline, and automation can help you fill in the gaps when you don't have all of the people that you need all of the time. Automation also helps you retain talent, because they can avoid working on lower-level tasks. Work becomes less monotonous."

You still need humans

Augusto Barros
VP and Cybersecurity Evangelist, Securonix

"Response is still driven by humans. You need a person to at least vet the detection findings before triggering the automated parts of the response process. You need humans to know which steps to take when an incident occurs. And from the technical side, you need the right technology in your environment to help you respond. Is my environment prepared for me to take actions quickly and effectively? You need to have people who know how to respond with a regular, adequate, and tested response process and have the environment properly instrumented to allow you to respond fast."

Automation is one piece of the whole

Barbara Kay
Senior Director, Product Marketing, Risk, Security, and ESG, ServiceNow

"Most companies have longstanding investments in prevention and defense—so today's emphasis is on review and upgrade of response visibility and readiness across systems and organizations. Using the MITRE ATT@CK framework to assess and enhance defense, monitoring, and response is a key element. But we are also helping people tighten up their security operations, especially incident response, through automation, along with prioritization, and structurally linking security, IT, and other teams involved in reducing vulnerabilities and responding to a major incident."

Adapting to evolving risks through automation

Ravi Srinivasan
CEO, Votiro

"Smart automation helps security programs keep up with the changing threat landscape and support digital transformation initiatives. Many companies still use a manual process for security. They wait for the staff to detect a vulnerability. Then they apply the CBE patch and make sure it is working. They continue to run around in that circle. Automation, AI, and machine learning help CISOs break out of that cycle by not just automating processes but using AI and machine learning to continuously learn and adapt."

Case study: University of Maryland Medical System

Taking security technology to the next level

Duc Lai
CISO
University of Maryland Medical System

Since joining the University of Maryland Medical System in 2021, CISO Duc Lai has been working to increase the company's defenses against the escalating risks of ransomware attacks and vendor compromises.

UMMS was one of many healthcare providers affected when timekeeping software provider Kronos was shut down in January 2022 by a ransomware attack. "Fortunately, we were able to find workarounds to collect hours for all our employees punching in and out," says Lai.

He has focused mainly on investment in technology platforms to mitigate those risks—including security information event management (SIEM), log management, and network segmentation initiatives—as well as on modifying outdated processes and developing new ones. With backing from senior management, Lai has increased the UMMS security team by 20% to help support these initiatives and overcome organizational challenges. "We are in a race against time to get these new capabilities deployed and shore up our defenses before we get attacked," he says.

One recent initiative was a tabletop exercise for ransomware, which allowed UMMS to revise its incident response plans and to validate them with a third-party facilitator. "We have takeaways and lessons learned that tell us where our focus areas should be," says Lai.

Security in a new world of connected devices

UMMS faces some challenges common in the healthcare world, including a patchwork of networks and systems arising from a growth strategy based on mergers and acquisitions, as well as dealing with the growing risks from operational technology (OT), specifically, connected biomedical devices. These can include things like a controller for a CT scanner, or for lab equipment analyzing blood samples. "It is very challenging to patch those systems, especially since the vendors are hardware manufacturers, not software specialists, so their patching and upgrade cycles could take years. In the dynamic, rapidly evolving world of cybersecurity risks, that's too slow. We have to find ways to segment and secure these devices from our network while putting security controls in place to detect vulnerabilities and respond to intrusions," says Lai.

This ties in with the UMMS cybersecurity investment he considers most crucial: a managed endpoint detection and response solution put in place before he joined the company. "With a managed service solution, you have security experts watching those endpoints 24/7/365 who are able to immediately contain those devices if they were to be compromised," says Lai. This outsourced function takes some of the burden off the in-house security team to detect and stop an attack.

Lai believes a managed EDR is also one of the strongest defenses currently available against the top cybersecurity risks like ransomware. "Investing in that one strategic platform will give you a lot of return on your investment. But it's important to deploy it universally across the enterprise—you can't have any unmanaged devices out there, because inevitably the attacker's going to find that unmanaged device."

> "We are focusing on building out actual KPIs to be able to use data in a meaningful way and tie it back to the investments that are being made within the organization to really show our value."
>
> **Juan Morales, CISO, Realogy**

6. Measuring cybersecurity performance

The most important metrics for measuring cybersecurity performance

KPIs and metrics are vital for monitoring security performance. Our research reveals the importance of 16 key metrics tracked by cybersecurity teams.

A comprehensive security metrics program can help organizations improve their decision-making, enhance visibility across their organization, benchmark their performance against their peers, and demonstrate the value of cybersecurity to the C-Suite and the board.

Cybersecurity metrics can vary widely among organizations across industries. For example, energy and utility companies focus more than others on time to respond to a breach while retailers look more often at the share of clients using multifactor authentication. On average, organizations track four to five metrics, with media tracking the least (average 3.9) and life sciences, the most (average 4.6).

Metrics that matter most

To understand the metrics that can help deliver results, we ranked the top metrics that organizations with no breaches found to be the most important. At the top of the list is the number of times per year a scan is conducted on internet-facing infrastructure, followed by the time to detect a breach, percentage of machines running operating systems that are two or more generations old, the time between employee departure and elimination of their access, and the percentage of systems not covered by vulnerability scans.

These metrics are commonly used by CISOs and CIOs to assess vulnerabilities in IT infrastructure. But to communicate with top management effectively, CISOs should translate these metrics into business and financial results that they can understand.

Metrics tracked and most important to organizations with no breaches and to industries

Metric	% that track	Importance ranking by those with no breaches	Industry that uses metric most
No. of times/year for a scan on internet-facing infrastructure	26%	**1**	Mfg.; life sc.
% of business-critical systems monitored	23%	7	Telecoms
% of servers using multifactor authentication (MFA)	23%	7	Financial
Time to detect the breach	21%	**2**	Life sciences
% of security sensors in common, searchable, data repository	21%	7	Insurance
% of security solutions deployed in the cloud or as SaaS	20%	6	Consumer goods
% of clients using multifactor authentication	20%	12	Retail
% of users monitored by user behavior analytics	20%	12	Insurance
% of machines running systems that are two generations old	19%	**3**	Public sector
Time between employee departure & elimination of access	18%	**4**	Insurance
% of systems not covered by vulnerability scans	18%	**4**	Life sciences
Time to get 90% of external facing system patched	18%	7	Technology
Dwell time	18%	12	Technology
Time to respond to the breach	17%	7	Energy & util.
Number of domain admin accounts	17%	12	Retail
Number of times each year phishing tests are conducted	17%	12	Life sciences

Q30. Which of the following cybersecurity metrics does your organization track, and which metrics are most important?

Calls to action: Communicating successfully to top management and the board

Use business language

Darren Thomson
Head of Cyber Intelligence Services, CyberCube

As security and resilience become top of mind for corporate boards, the CISO needs to adapt culturally to demonstrate the impact of their efforts on the business. It is important for CISOs to talk to a board of directors in a language that they understand in order to take a strategic, top-down approach to risk management in cyber.

CISOs should avoid taking a 'technology first' approach to risk mitigation. Start with business strategy, governance, and gap analysis. Technology needs to be deployed in line with these and not in a reactionary way. One of the challenges here is having the ability to translate cyber risk into financial terms. What will be the ROI from my invest in security? How much risk is the organization carrying? What is our preferred risk posture?

There are world-class solutions in the market that bring together threat intelligence, data, analytics, and modeling approaches to provide insight into the financial impact of events that might occur to an enterprise. These arm the CISO with a dollar translation of the risk posture of their company as well as the ROI on security investments.

Share insightful data

Steve Durbin
CEO, Information Security Forum

The metrics tracked by CISOs are often more IT-focused than risk-based, and therefore may not be worthy of the board room. To engage the board, CISOs should report metrics that cover control effectiveness, threats, exposures, losses, or asset values. In addition, they should furnish insightful trending data with predictive and prescriptive analytics.

The board of directors is responsible for the risk profile across the organization. So there needs to be that constant review reiteration over the course of the annual cycle as to whether the most appropriate risk controls are in place. And it should map across what an organization is trying to do and consider how world changes will affect specific lines of business.

Provide an overview of the threat landscape

Sydney Klein
CISO, Bristol Myers Squibb

Every single board update that I give starts with the external threat landscape, how we're seeing that affect the company, and what we're doing to address that. When there are big cyberattacks dominating the news, I talk about our level of preparation to respond to a similar attack. I also discuss regulatory changes, what they mean for us, and how we're staying ahead of them. Another topic may be changes that we're making in our workforce and how that is protecting us. My main objective is to make sure they have a very realistic view of the cyber risks that exist

Key metrics vary by industry

Players across industries measure many of the same cybersecurity elements, but there are some differences in the top metrics tracked, and those considered most important.

This often reflects the nature of the industry. For example, only three industries—**insurance**, **media and entertainment**, and **retail**—rank the percentage of users monitored by user behavior analytics to be the most important metric. Not surprisingly, entities in the **public sector**—which often do not enjoy the most state-of-the-art technology—are the only ones to rank as most important the share of machines running on systems that are two or more generations old. Firms in **telecoms**, considered to be critical infrastructure, cite percentage of business-critical systems monitored internally or by a third party, a metric that is not at the top of the list for any other industry.

	Aerospace/defense	Automotive	Consumer goods	Energy & utilities	Financial services	Healthcare	Manufacturing
Metric most often tracked	Times per year scan is conducted on internet-facing infrastructure (29%)	Servers using MFA (28%)	Times per year scan conducted on internet-facing infrastructure (26%) Security sensors feeding into common, searchable, data repository (26%)	Time to detect breach (31%)	Servers using MFA (31%)	Times per year scan conducted on internet-facing infrastructure (29%)	Times per year scan conducted on internet-facing infrastructure (30%)
Most important metric	Security solutions deployed in cloud or as SaaS (21%)	Security sensors that feed into common, searchable, data repository (18%)	Times per year scan conducted on internet-facing infrastructure (23%) Security solutions deployed in cloud or as SaaS (23%)	Time to detect breach (21%)	Time to detect breach (21%) Servers using MFA (21%)	For given critical patch for internal mission critical systems, time to get to 90% patched (21%)	Times per year scan conducted on internet-facing infrastructure (20%)

	Insurance	Life sciences	Media/ent.	Public sector	Retail	Technology	Telecoms
Metric most often tracked	Security sensors that feed into common, searchable, data repository (30%)	Times per year scan is conducted on internet-facing infrastructure (30%)	Times per year scan conducted on internet-facing infrastructure (25%)	Security sensors that feed into common, searchable, data repository (25%) Machines running operating system two or more generations old (25%)	Clients using MFA (29%)	Servers using MFA (29%)	Business-critical systems monitored internally or by third party (34%)
Most important metric	Users monitored by user behavior analytics (24%)	Time to detect breach (23%)	Users monitored by user behavior analytics (23%)	Machines running operating system two or more generations old (21%)	Users monitored by user behavior analytics (23%) Clients using MFA (23%) Number of domain admin accounts (23%)	Servers using MFA (20%)	Business-critical systems monitored internally or by third party (23%)

Q30. Which of the following cybersecurity metrics does your organization track, and which metrics are most important?

Benchmarking cybersecurity performance

Benchmarking helps organizations to assess the weaknesses and strengths of their risk posture. Our research shows the performance against 26 metrics.

The table on the right shows the average value for each of the metrics tracked, together with the minimum and maximum values by percentile, and the percentage of respondents that track each metric. Across most metrics there is a notable difference between the top 25th and lowest 25th percentiles, revealing that there is considerable room for organizations to improve their performance.

What the metrics show

Despite growing ransomware threats, organizations, on average, have less than 60% of their mission critical systems covered by a backup and they only conduct backup restoration once a quarter.

While phishing is a main cause of breaches, an average of only 21% of employees report phishing incidents. Organizations may want to increase the number of times phishing tests are conducted during the year up from the average of 4.6 times.

Average dwell time—the time attackers spend undetected on a system—is now about 25 days, although the top 25th percentile of organizations have reduced it to 20 days.

Metric	Average	Top 25th percentile	Lowest 25th percentile	% that track
Number of domain admin accounts	5.1	4	6	17%
Times/year a scan is conducted on internet-facing infrastructure	4.6	4	6	26%
Times/year phishing tests are conducted	4.6	3	6	17%
Times/year a backup restoration drill is required by policy	4.2	3	5	12%
% business-critical systems or datastores covered by backups	59%	50%	70%	13%
% security solutions deployed in the cloud or as SaaS	33%	23%	40%	20%
% business-critical systems monitored internally or by a third party	31%	20%	40%	23%
% users monitored by user behavior analytics	31%	20%	41%	20%
% security sensors which feed into a common data repository	27%	20%	35%	21%
% servers sending logs to a common, searchable, data repository	27%	15%	37%	12%
% clients using multifactor authentication	26%	15%	35%	20%
% critical open security vulnerabilities in products remediated in SLA	25%	17%	35%	10%
% servers using multifactor authentication	23%	15%	32%	23%
% user end points sending logs to a common data repository	22%	15%	30%	8%
% employees reporting incidents like phishing	21%	15%	25%	14%
% cloud services sending logs to common, searchable, data repository	18%	15%	20%	13%
% machines running operating system 2 or more generations old	15%	10%	18%	19%
% systems not covered by vulnerability scans	7%	6%	8%	18%
Time to detect breach (days)	128.7	120	150	21%
Time to mitigate impacts of breach (days)	63.9	60	65.5	10%
Time to get to 90% patched for internal mission critical systems (days)	58.9	45	70	16%
Time to get to 90% patched for external facing systems (days)	52.3	40	62	18%
Time to respond to breach (days)	47.3	35	50	17%
Dwell time (days)	24.8	20	28	18%
Time between employee departure and elimination of access (days)	21.3	15	25	18%

Q30. Which of the following cybersecurity metrics does your organization track, and which metrics are most important? Q31. Please provide us with the latest information for the metrics that you track.

Mean time to detect and respond are key indicators to watch

Mean time to detect and mean time to respond to a breach are critical metrics for assessing cybersecurity performance. They are essential for mitigating risks across industries.

These are some of the most important metrics to track to ensure effective cybersecurity. They are huge contributors to breach costs—the longer that it takes to detect a breach and then to act, the greater the potential for damage to be done.

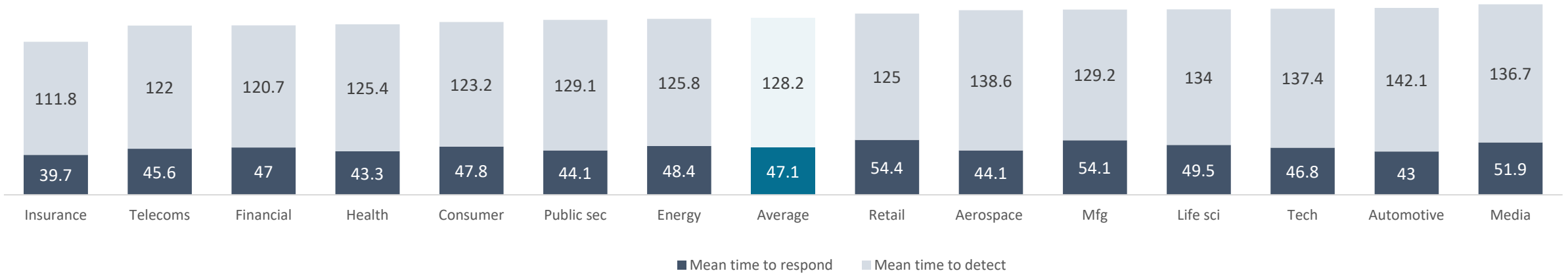
Entities surveyed reported that it took an average of 128 days to detect a breach and an additional 47 days to respond. However, firms that did not have a major breach over the last year said they were able to detect a breach almost 20 days faster than firms that had multiple major breaches, and they also responded by almost a week quicker. This suggests a correlation between organizations that did not suffer breaches in the past year and their better ability to detect and respond to them when they do happen—a best practice that others should nurture.

Among industries, insurance firms perform the best, on average detecting a breach about a month quicker than automotive firms, the worst performer on this metric. Insurers also respond more rapidly, over two weeks faster than manufacturers and retailers.

Mean time to detect and respond by number of breaches (days)

	Mean time to detect (days)	Mean time to respond (days)	Total (days)
No breaches	120.4	45.6	166.0
Multiple breaches	139.9	52.2	192.1
Difference	19.5	6.6	26.1

Mean time to detect and respond by industry (days)



Q31. Please provide us with the latest information for the metrics that you track.

"Make sure the fundamentals are sound first. You need to understand the fundamentals of your organization and your operation and know the gaps. If your foundation isn't solid, it doesn't matter what you throw on top of it, it will collapse."

Duc Lai, CISO
University of Maryland Medical System

7. Supercharging cybersecurity results

10 best practices to turbo-boost cybersecurity performance

By analyzing organizations with fewer breaches and faster times to detect, respond, and mitigate, we found 10 best practices that can deliver better cybersecurity results.

1. Take cybersecurity maturity to the highest level
2. Ensure cybersecurity budgets are adequate
3. Build a rigorous risk-based approach
4. Make cybersecurity people-centric
5. Secure the supply chain
6. Develop an integrated platform of latest technologies
7. Prioritize protection of linked IT and OT assets
8. Harness intelligent automation
9. Improve controls for expanded attack surfaces
10. Do more to measure performance

1. Take cybersecurity maturity to the highest level

Organizations that are most advanced in NIST maturity outperform others on key cybersecurity metrics.

One hallmark of entities advanced in NIST is their ability to detect a breach faster than others, and therefore, to be able to fix problems sooner. They similarly report shorter times to respond to a breach. Speedier response times can spell the difference between a major or a minor breach.

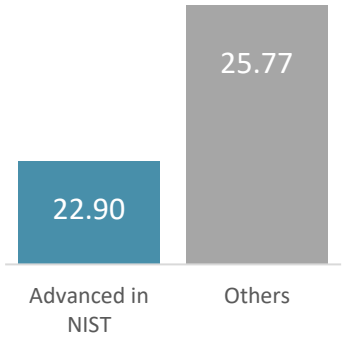
Advanced organizations also outperform others earlier in their NIST journey on the percentage of server clients using multifactor authentication, a growing best practice as identity theft rises. Those ahead on the NIST framework likewise report shorter times for patching external-facing systems—an important metric given the expanded networks needed to meet the needs of customers, vendors, and remote-working staff. Advanced entities do better as well on the number of times that they conduct scans and the time to eliminate employee access after they leave the organization.

Most importantly, advanced organizations see fewer incidents and material breaches. In 2021, they recorded 22.9 incidents vs. 25.8 for others, and 0.76 material breaches vs. 0.81 for others. Due to the growing financial and reputational costs of material breaches, these percentage differences can have outsized impacts.

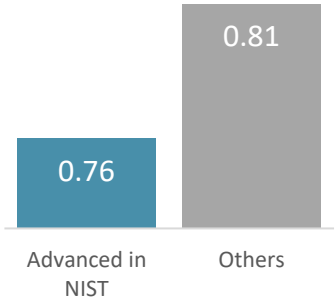
Metrics for organizations advanced in NIST vs. others

Metric	Advanced	Others	All
Time to detect a breach (days)	**118.9**	132.0	128.2
Percent 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
Number of times a year scan conducted on internet-facing infrastructure	**5.8**	4.7	5.0
Time between employee departure and elimination of their access (days)	**20**	22.7	21.8

Number of incidents in 2021



Number of material breaches in 2021



> For me, the most important metrics relate to time. Time is a critical resource that I can measure. It can measure the hours people are working, and the costs associated with a breach. Time metrics reduce decisions to simple math. If I am supposed to get x number of things done in a quarter, and I just wasted 100 hours of my team working on an incident, then I can't make up that time unless I add more people.
>
> **Richard Rushing**
> CISO, Motorola Mobility, a Lenovo Company

Q30. Which of the following cybersecurity metrics does your organization track, and which metrics are most important? Q31. Please provide us with the latest information for the metrics that you track.

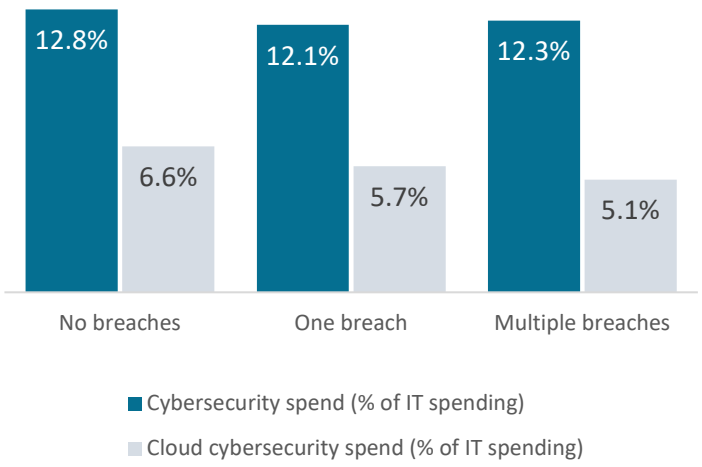
2. Ensure cybersecurity budgets are adequate

Greater spending on cybersecurity helps to generate better outcomes. Organizations that invest more in cybersecurity experience fewer material breaches and faster times to detect and mitigate.

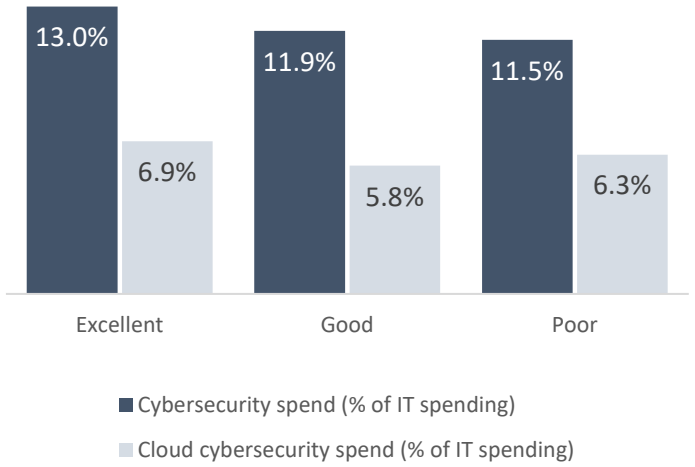
Our analysis found a clear correlation between cybersecurity investment and results. Organizations with no material breaches in 2021 spent an average of 12.8% of their IT budgets on cybersecurity vs. an average of 12.3% for organizations with multiple breaches. That difference is not inconsequential: given that the average IT budget for respondents was $946 million in 2021, that additional spending by organizations with no breaches amounts to $4.7 million. Similarly, organizations with no material breaches in 2021 spent 6.6% of their IT budgets on cloud cybersecurity vs. 5.1% for those with multiple breaches.

The same positive correlation holds true between cybersecurity spending and times to detect breaches and mitigate them. In 2021, organizations that had excellent times to detect spent 13% of their IT budgets on cybersecurity vs. 11.5% for those with poor times to detect. Likewise, organizations with excellent times to mitigate in 2021 spent 14.1% of their IT budgets on cybersecurity vs. 12.8% for organizations with poor times to mitigate.

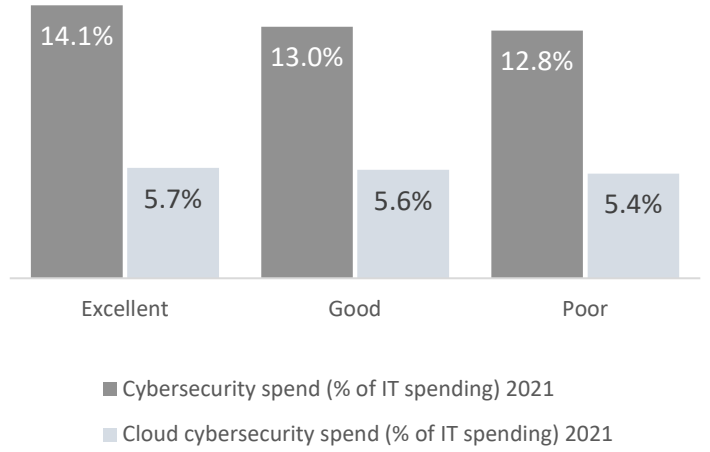
Impact of cybersecurity spending on number of breaches in 2021



Impact of cybersecurity spending on time to detect in 2021



Impact of cybersecurity spending on time to mitigate in 2021



Q16. Please tell us your organization's total annual enterprise IT spending, total cybersecurity spending, and total spending on cloud cybersecurity tools in 2021, and what you expect them to be in 2022.

3. Build a rigorous risk-based approach

Combining a risk-based approach* with a maturity model boosts cybersecurity results. Our research shows that organizations that excel in the areas of risk-based management saw fewer incidents and material breaches than others in both 2020 and 2021. Over 4 out of 10 risk-based leaders embrace Zero Trust principles.

Organizations that take a risk-based approach—i.e., make decisions to mitigate, transfer, or accept a risk based on its probability and potential impact—see better outcomes. According to our study of 1,200 organizations, risk-based leaders experienced 21.3 incidents in 2020 and 22.5 in 2021, compared with 24.4 and 27.1 incidents for risk beginners. Crucially, the number of material breaches for risk leaders was also lower than for beginners: Leaders suffered 0.60 breaches in 2020 and 0.75 in 2021, vs. 0.72 and 0.88, respectively, for beginners.

In fact, 48% of organizations with no breaches in 2021 took a risk-based approach vs. 40% of those that experienced multiple breaches. Our analysis also shows a clear correlation between a risk-based orientation and improvements in time to respond and mitigate. Indeed, 46% of the top performers in time to respond took a risk-based approach vs. 36% of poor performers.

The results were even more impressive with time to mitigate: 50% of the top performers on that metric were advanced in a risk-based approach vs. 17% of poor performers. Given that today's risk leaders have still more progress to make on implementing risk-based management, these performance correlations understate the full potential of applying this discipline.

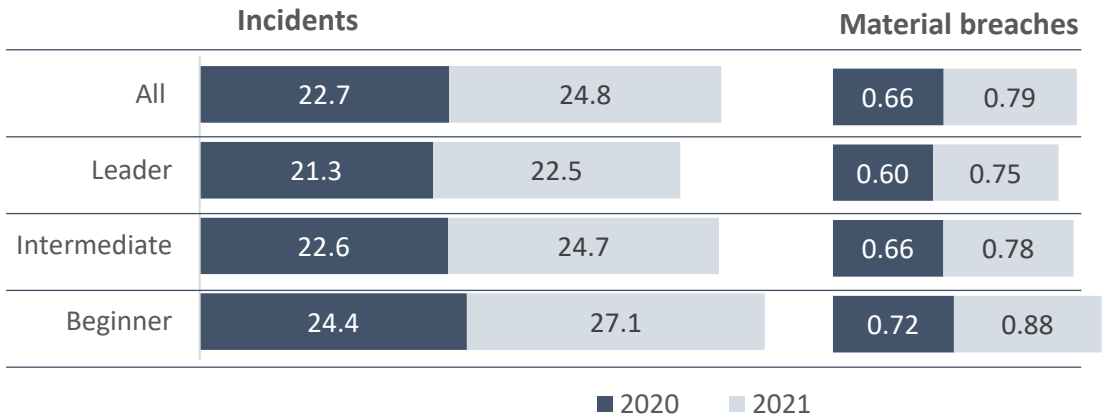
50% of top performers in time to mitigate took a risk-based approach vs. **17%** of poor performers.

48% of organizations with no breaches in 2021 took a risk-based approach vs. **40%** of those that experienced multiple breaches.

46% of the top performers in time to respond took a risk-based approach vs. **36%** of poor performers.

44% of risk-based leaders build their cybersecurity programs around Zero-Trust principles.

Performance by risk-based approach progress*



Q15. What progress have you made in each of the following activities to *proactively manage* risks? (Top 2 managed or optimized). * Elements of a 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.

4. Make cybersecurity people-centric

Cybersecurity is as much about humans as it is about technology. Employees are the first line of defense, and organizations that cultivate human-centric cybersecurity see fewer breaches and faster times to detect and respond.

Our research shows that organizations take five key steps to drive human-centric cybersecurity:

1

Build human-layer security by assessing staff reflexes, behaviors, and patterns

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

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

2

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 to respond.

3

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 poor times to respond.

4

Create clear processes to recruit, upskill, and retain specialists

43% that had no breach have invested in recruiting and retaining specialists vs. **31%** with multiple breaches.

61% that had excellent times to detect have invested in recruiting and retaining specialists vs. **39%** that have poor times to detect.

5

Ensure that cybersecurity teams are correctly staffed

48.8 (average) cyber professionals are on staff per $1B revenue for firms with no breaches vs. **43.7** for those with multiple breaches. Organizations with larger staffs also report better times to detect a breach and dwell time.

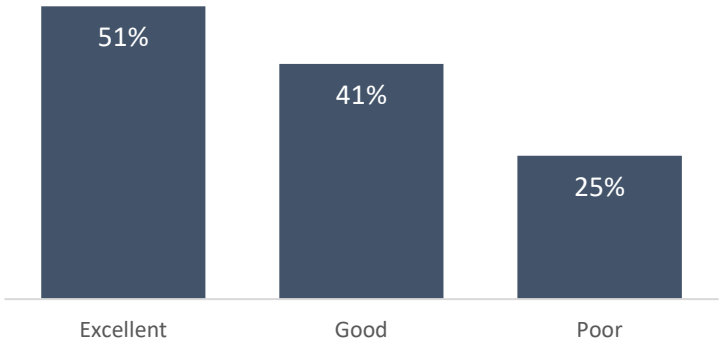
5. Secure the supply chain

As companies morph into ecosystems of partners and vendors—exposed to external shocks such as the pandemic and now the war in Ukraine—mitigating supply chain risk will become vital and more challenging. Those organizations that turn third-party risk management into a best practice will reap the rewards.

For 44% of organizations, the growing use of suppliers is exposing them to major cybersecurity risks. The percentages are even higher for industries with more complex supply chains, such as auto makers (51%) and industrial manufacturers (51%). The NIST framework prescribes that organizations take a range of steps to secure their supply chains, from improving third-party risk management processes to running routine supply chain audits and tests. Our research reveals that organizations that are in advanced stages of supply chain maturity under the NIST framework can detect, respond to, and mitigate breaches faster. On the other hand, only 16% of organizations see increasing supply chain vulnerabilities as a challenge, falling to 13% in two years, which may reflect complacency or wishful thinking.

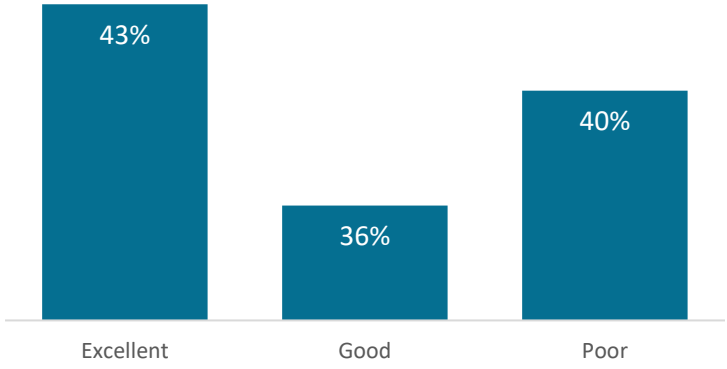
Time to detect: % advanced in supply chain management

51% of organizations with excellent times to detect are advanced in supply chain management.



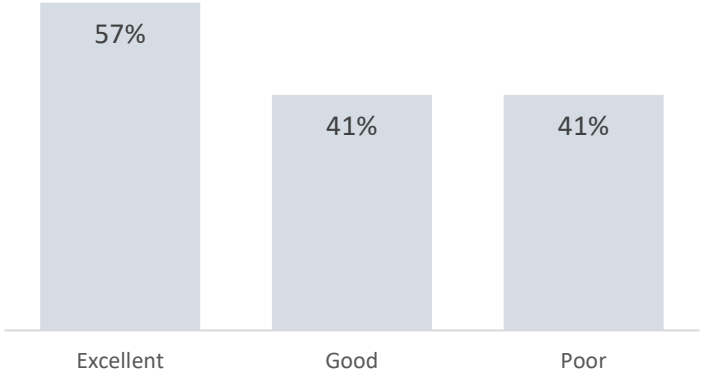
Time to respond: % advanced in supply chain management

43% organizations with excellent times to respond are advanced in supply chain management.



Time to mitigate: % advanced in supply chain management

57% of organizations with excellent times to mitigate are advanced in supply chain management.



6. Draw on latest technologies, but avoid product proliferation

CISOs are in an arms race with threat actors. To defend against future risks, they need to implement an integrated set of best-of-breed technologies.

Organizations with no breaches most commonly invest in 10 technologies:

- **Email security** to protect against rising ransomware and phishing attacks.
- **Distributed DOS protection technology**, which works well to mitigate most forms of denial-of-service attacks.
- **Cloud access security broker**, which eliminates cloud vulnerability by putting an intermediary between users, devices, and cloud providers.
- **Network security policy management software** that provides a suite of tools for managing configurations and security settings across networks.
- **Identity and access management**, with many upgrading to MFA.
- **Mobile device management**, vital for rising smart phone use by staff and customers.
- **Cyber risk modeling and assessment,** whereby organizations create a variety of scenarios and their probability and likely impacts.
- **End-point detection and response (EDR)** that combines real-time monitoring with rules-based automated response.
- **Security information and events management (SIEM),** which enables CISOs to analyze a firehose of data as workloads migrate to the cloud.
- **Secure access service edge (SASE),** which grew in importance during the pandemic as work became hybrid and cloud-based.

Yet experts warn against getting lost in a blizzard of technologies. Those advanced in NIST are moving to a platform approach rather than using many individual solutions, and more than a third of entities with no breaches plan to consolidate their tools. Security leaders are more likely to take a multi-layered, multi-vendor approach to monitor and manage risks better through a strong infrastructure.

Top 10 investments by those 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

Q19. Which of the following cybersecurity initiatives around *technology* have you already invested in, which have been the most effective for your organization, and where do you plan to make the biggest investments over the next two years?

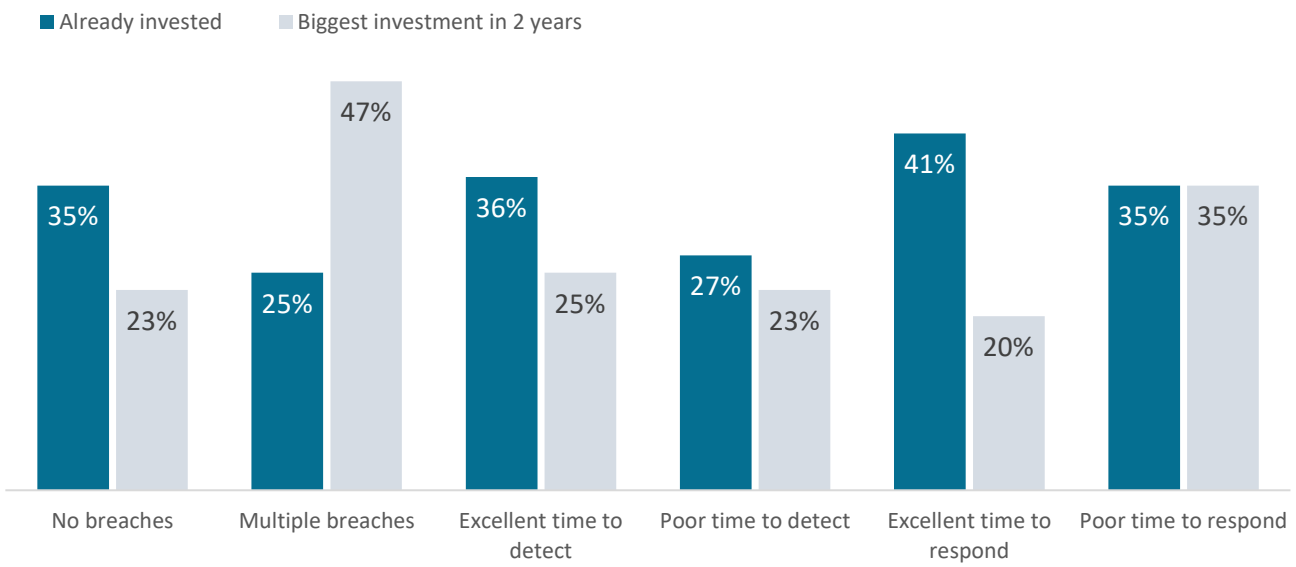
7. Prioritize protection of linked IT and OT assets

The interconnection of physical assets and digital networks has widened the attack surface for the private and public sectors. Organizations that prioritize protecting their IT and OT assets and remediating any resulting vulnerabilities see fewer material breaches and faster times to respond and mitigate.

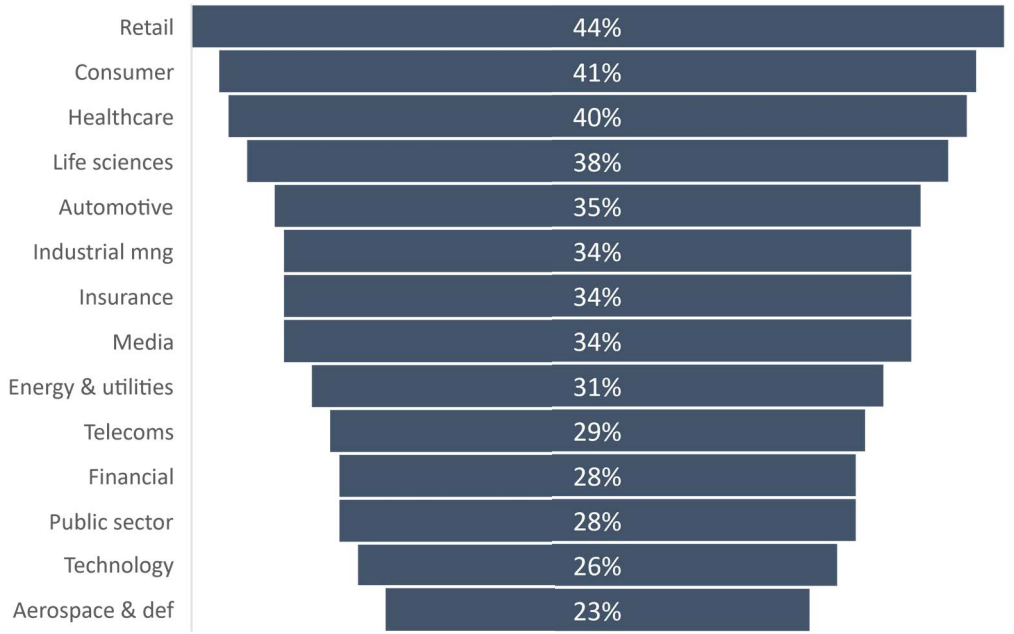
Our analysis reveals that prioritizing the protection of interconnected IT and OT assets leads to improved cybersecurity performance. Indeed, 35% of organizations with no material breaches have invested in prioritizing the protection of these interlinked assets vs. 25% of those with multiple breaches. Nearly half of organizations with multiple breaches will be making large investments over the next two years to close vulnerabilities from converging IT and OT assets. Retail, consumer goods, and healthcare have the highest percentages of firms that plan to make big investments in protecting risks from interconnected IT and OT assets.

Among top performers in time to detect a breach, 36% have invested in prioritizing IT and OT asset protection vs. 27% among poor performers. Similarly, 41% of organizations with excellent time to respond to a breach have invested in prioritizing IT and OT protection vs. 35% of poor performers.

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



% planning large investments in IT & OT assets protection by industry



Q18. Which of the following cybersecurity initiatives around *process* have you already invested in, which have been the most effective for your organization, and where do you plan to make the biggest investments over the next two years?

8. Harness intelligent automation

Use of cybersecurity automation, combined with AI and machine learning, is growing as organizations seek to boost efficiency and speed.

Automation helps to deliver better results. It reduces mundane work, drives efficiencies, frees up staff, and enables a more blanket approach to cybersecurity: fighting machines with machines. One CEO notes that companies are embracing automation at record levels to optimize workflows, implement changes, validate network security policies, and accelerate detection and response time.

Automation also supplements the work of humans at a time when cyber talent is becoming harder to find. Said the CISO of a US energy firm: "We could institute more automation and processes to reduce our dependence on people. But I think automation also can help us to retain and attract talent, since we can bring people to the organization who know they will not be working on lower-level, mundane tasks."

Making automation smarter

Use of AI and machine learning to identify security vulnerabilities and threats also improves some areas of cybersecurity performance. Our data shows that organizations that use these technologies do better in terms of dwell time and time to mitigate. Of those that are excellent at dwell time, 29% use AI and machine learning vs. 17% of those with poor dwell time performance. Similarly, 22% of organizations with excellent time to mitigate use AI and ML against 17% of those with poor time to mitigate.

Automotive and aerospace firms are ahead of others in use of AI and ML, while consumer goods firms and public-sector entities trail behind.

% respondents agreeing

Statement	All	Advanced in NIST	Other	Industry high	Industry low
We use advanced analytics such as AI and ML, to identify security vulnerabilities or threats.	26%	28%	25%	Automotive 43%	Consumer goods 15%

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.

"Because a vulnerability is usually mitigated by one or more methods, we use a combination of techniques, such as security automation technologies combined with security configuration checklists and patch management."

COO, healthcare firm, Netherlands

"We rely on automation tools for our security operations centers to provide rich analysis of the security landscape, as well as to automatically enforce security policies."

CTO, internet service provider, US

Q20. Which of the following statements regarding cybersecurity at your organization do you agree with?

9. Improve security controls for expanded attack surfaces

Attack surfaces widened during the pandemic because of greater digital transformation, cloud migration, remote working, and supply chain complexity. Yet our research shows that companies are not taking adequate steps to use security controls to cover their expanding technology environments.

Multiple metrics tracked by respondents show insufficient use of security controls. For example, only 26% of the respondents' clients are using multifactor authentication, and the percentages of servers using MFA are even lower (23%). Only 31% of users are monitored by user behavior analytics. Security coverage for cloud is even more worrying: just 18% of organizations have cloud services sending logs to a common data repository.

Performance varies by industry. Energy and utility firms, for instance, report the highest percentage of business-critical systems covered by backups (65%), while retailers report the lowest (49%). But retailers are doing a better job with business-critical systems monitored internally or by third parties (34%) compared with aerospace and defense companies (27%).

These metrics show a dangerous gap, since organizations cannot mitigate problems that they cannot see. As Augusto Barros, vice president and cybersecurity evangelist at Securonix points out: "Even the most mature incident response practices cannot protect against breaches when attacks hit part of the environment that are not visible or protected by the security infrastructure."

Metrics tracked

	Average	Top performer	Bottom performer
% of business-critical systems or datastores covered by backups	59%	Energy & utilities (65%)	Retail (49%)
% of business-critical systems monitored internally or by third party	31%	Retail, technology (34%)	Aerospace & def (27%)
% of users monitored by user behavior analytics, such as via SIEM	31%	Manufacturing (39%)	Automotive (20%)
% of clients using multifactor authentication	26%	Life sciences (35%)	Manufacturing (20%)
% of servers using multifactor authentication	23%	Manufacturing (29%)	Insurance, tech, life sciences (20%)
% of end user end points sending logs to a common data repository	21%	Health, media, telecoms (24%)	Aerospace, life sciences, retail (18%)
% of cloud services sending logs to a common data repository	18%	Public sector and media (21%)	Healthcare and retail (15%)
% of systems not covered by vulnerability scans	7%	Insurance (10%)	Manufacturing (6%)

Q31. Please provide us with the latest information for the metrics that you track.

> "In order to take a risk-based approach to cybersecurity, it is critical to understand your true exposure to a cyber-attack and focus remediation efforts accordingly. Not every vulnerability will turn into a breach, and organizations can't feasibly patch all vulnerabilities. They need to have the visibility and context across their attack surface to understand which vulnerabilities, if exploited, can cause the greatest harm to their business."
>
> **Gidi Cohen**
> CEO and Founder, Skybox Security

10. Do more to measure performance

Currently, organizations track just 4.2 metrics on average. Cybersecurity 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.

As Peter Drucker once said, "What gets measured gets managed." That is particularly true for cybersecurity, according to our research. Specifically, organizations that track six or more metrics saw fewer incidents than those that monitor 4-5 metrics (20.6 incidents vs. 23.4), as well as fewer material breaches (0.60 vs. 0.675). With the average cost of a material breach estimated at $3.4 million in 2020, the cost savings would amount to $242,000 a year from reviewing more metrics.

The results were even more impressive for 2021. Respondents tracking six or more metrics had 23.1 incidents and 0.734 material breaches, compared with 25.3 incidents and 0.811 material breaches for respondents watching 4-5 metrics. Given that our estimated cost of a material breach was $4.2 million for 2021, the average cost savings would amount to $322,000 for the year if more metrics were tracked.

Our analysis also suggests that the board and C-Suite can bring value to reducing digital risks when they better under cybersecurity metrics. Indeed, we found that organizations that tracked six or more metrics had boards and management teams that had deeper knowledge of cybersecurity metrics (34%) than those in organizations that tracked just 4-5 metrics (20%). Monitoring more metrics also enabled organizations to achieve greater progress on key areas of risk-based management, such as exposure analysis and risk scoring.

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

Q26. Approximately how many cybersecurity incidents did your organization experience in 2020 and 2021? How many were material breaches?

Top management teams that know metrics well track more indicators

34%
of organizations with C-Suites and boards that understand metrics well track six or more KPIs

vs.

only 20%
of organizations with C-Suites and boards with lower knowledge of metrics.

8. Our sponsors and advisors

Our coalition

Lead sponsors

AXIS COMMUNICATIONS

CLAROTY

elastic

KnowBe4 Human error. Conquered.

securonix

SKYBOX SECURITY

VOTIRO

ZENKEY

Supporting sponsors

CyberCube

servicenow

RESOLUTE. STRATEGIC SERVICES

Lead sponsor and global consulting sponsor

Booz | Allen | Hamilton®

Association partners

INTERNET SECURITY ALLIANCE

ISF

Program sponsors: Advisory board and marketing committee members

Name	Title	Organization
Wayne Dorris	Business Development Manager- Cybersecurity	Axis Communications
Madeline Robson	Content and Communications Specialist	Axis Communications
Fredrik Larsson	Expert Security Architect	Axis Communications
Per Bjorkdahl	Director, Sustainable Sales Engagements	Axis Communications
Matt Feenan	Team Lead, Products and Solutions Marketing	Axis Communications
Paul Sussman	Vice President, Cybersecurity Strategy Consulting	Booz Allen Hamilton
Mark Taylor	Head of Commercial Strategic Alliances and Partnerships	Booz Allen Hamilton
Christopher Smith	Principal, Commercial Cyber Practice	Booz Allen Hamilton
Ken Yao	Senior Associate, Cyber Fusion Center	Booz Allen Hamilton
Simon Chassar	Chief Risk Officer	Claroty
Grant Geyer	Chief Product Officer and CISO	Claroty
Upa Campbell	Chief Marketing Officer	Claroty
Chelsea Sawicki	Senior Director of Product and Content Marketing	Claroty
Rebecca Bole	Head of Industry Engagement	Cyber Cube
Megan Radogna	Thought Leadership Content and Research Manager	Elastic
Riva Froymovich	Senior Director, Thought Leadership	Elastic

Program sponsors: Advisory board and marketing committee members

Name	Title	Organization
Joanna Huisman	Senior Vice President, Strategic Insights & Research	KnowBe4
Augusto Barros	Vice President and Cyber Security Evangelist	Securonix
Oliver Rochford	Senior Director, Security Evangelist	Securonix
Isabelle Coste	Senior Director, Demand Generation	Securonix
Sara Kingsley	Director of Product Marketing	Securonix
Raunika Nayyar	Manager, Marketing & Communications	Securonix
Richard Murphy	Editor in Chief, Director, C-Suite Communications	ServiceNow
Barbara Kay	Senior Director, Product Marketing, Risk, Security, and ESG	ServiceNow
Kathy O'Connell	Vice President, Corporate Marketing and Communications	Skybox Security
Ashley Nakano	Corporate Communications Director	Skybox Security
Rob Rosiello	Chief Revenue Officer	Skybox Security
Kristin Melville	Vice President of Growth Marketing	Skybox Security
Ravi Srinivasan	CEO	Votiro
Gianna Whitver	Vice President of Marketing	Votiro
Alex Schlager	Chief Executive Officer	ZenKey
Yinka Daramola	Vice President, Marketing	ZenKey

Program advisors

Name	Title	Organization
Larry Clinton	President/CEO	Internet Security Alliance
Jeff Brown	Former VP and CISO	Raytheon
Gary McAlum	Board Director	National Cybersecurity Center
Ron Mehring	CISO	Texas Health Resources
Peter Keenan	CISO	Lazard
Andrew Jenkinson	Group CEO	Cybersec Innovation Partners
Juan Morales	CISO, Global Information Security	Realogy Holdings
Dr. Ivo Pezzuto	Core Professor of Digital Transformation, Disruptive Innovation	International School of Management
Richard Rushing	CISO	Motorola Mobility, a Lenovo company
Dave Estlick	CISO	Chipotle Mexican Grill
Ilan Abadi	Global CISO	Teva Pharmaceuticals
Deborah Wheeler	SVP, Chief Information Security Officer	Delta Air Lines
Joseph Steinberg	Cybersecurity Expert Witness and Advisor	Cybersecurity and Artificial Intelligence Expert Services
Steve Durbin	CEO	Information Security Forum
June Chambers	Head of PR and Corporate Communications	Information Security Forum
Jamie Singer	Executive Vice President	Resolute Strategic Services
Curley Henry	Vice President, Deputy CISO	Southern Company
Mandy Andress	CISO	Elastic
Alim Somani	Managing Director	Hatch Digital

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

Barry Rutizer, Corporate Director
barryrutizer@thoughtlabgroup.com