DARKReading RESEARCH

NOVEMBER 2021

The state of CISO influence 2021

The maturing CISO role

COALFIRE

Executive summary

Increasingly, security leaders are breaking out of the role of compliance coordinators or breach scapegoats. As they work to not only advise their business colleagues about how to manage cyber risk but also safely enable digital transformation, today's CISOs are expanding and deepening their influence across the typical organization.

Data from Dark Reading's **The state of CISO influence 2021** survey indicates momentum for security leaders on a number of influential fronts. CISOs are more likely than ever to report directly to the CEO. Cyber executives often bring a high degree of business acumen in how they measure and represent risk not only to their bosses, but across all business stakeholders. The needle has moved past the tipping point where the majority of CISOs now must show ROI for their effort, i.e., and those who do are getting increased authority and credibility as a result.

Still, staying ahead of the security threats is always a work in progress. The survey this year shows that while security leaders are confident in their broad coverage of security controls, they still struggle to integrate their tools and practices beyond the typical security silos. Similarly, CISOs today are running programs that still involve a high degree of manual work.

Nevertheless, the progress CISOs have made in recent years is increasingly reflected in how they're perceived across organizations. Security teams are an integrated part of strategic business planning at many organizations, and many CISOs are frequently valued by their peers and the executive leadership team.

Key findings

This year's survey found that:

Operational basics

- 27% of top security leaders report directly to the CEO, a big bump compared to many previous industry surveys.
- Even at large organizations with 1,000 or more employees, 56% of security teams have 20 or fewer staffers.
- The top three services that information security leaders outsource are:
  - » Penetration testing
  - » Independent risk assessments
  - » Roadmap/major initiative planning

Dimensions of success

- 97% of security leaders provide some level of visibility to executive leadership, the C-suite, and/or the board.
- Almost a third provide performance updates on-demand, yet only 18% of them have access to continually delivered metrics through a dashboard.
- Almost one in four security leaders personally do all of their own security metrics analysis, but at the same time over another third say they now have a dedicated data scientist to do this work, whether on their team or outside the security group.
- Fewer than a third of security leaders use significant automation in security work, and almost a third said security controls and risk management programs are not fully integrated.
- Over half of cyber leadership needs to show ROI for security spend, but when they do show positive ROI they get increased authority and credibility.

Security culture & influence

- 42% of respondents say their head of security is valued by the business, and just 10% say that leader is a check-the-box figurehead.
- Nearly eight out of 10 organizations report that security is an integrated part of annual business planning.
- Only 29% of security leaders sometimes feel that their security team is the only one that is aware of the importance of cybersecurity.
- 35% of organizations say that their organizations tie product managers' compensation to security KPIs.

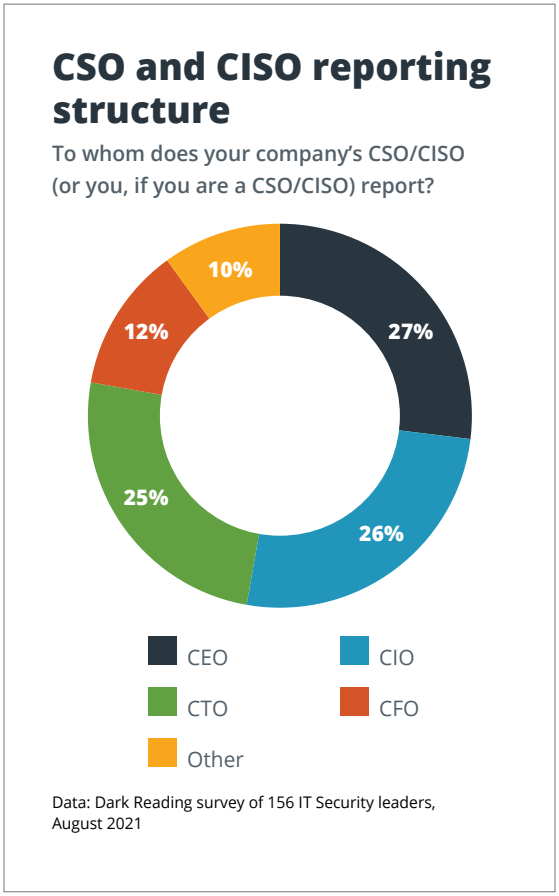
These findings, along with perspective and key insights from Coalfire and Dark Reading, are outlined in the following pages.

Operational basics

As the importance of cybersecurity grows in the eyes of top executives and boards, CISO influence continues to expand as well. One of the most simple litmus tests for that is in organizational structure and chain of command.

While this is the first year of this particular survey, industry surveys of the past have indicated fairly low levels of CISOs with a direct line of reporting to the CEO. Our study now shows a significant proportion of CISOs who report directly to the CEO. This is the leading reporting schema in our survey by a thin margin, with 27% who say the CEO is the CISO's boss **(Figure 1)**.

Figure 1.



That reporting structure runs neck-and-neck with two others: Approximately 26% of CISOs report to the CIO and 25% to the CTO. CISOs reporting to CFOs now seem to be a significant minority, with just 12% of organizations saying they're set up this way.

The security leaders in the survey have significant breadth of operational reach in the controls that their team directly manages or influences through collaboration with other stakeholders. The most common security controls directly managed by these leaders are vulnerability management, identity and access management, and business resilience and recovery programs **(Figure 2)**. Meanwhile, the security functions most likely to be indirectly managed through collaboration and influence included application testing and physical security.

In terms of team size, the survey showed that most organizations run very lean security teams, with 75% of respondents reporting that they operate with 20 or fewer security staffers. Nearly 40% of respondents say they run a very small staff of five or fewer security professionals. This is telling, especially considering that the sampling in this survey definitely skews toward larger sized enterprises. We broke out this question by organization size and found that regardless of how large the company, security teams were still very small. For organizations with 1,000 or more employees, about 56% reported they have 20 or fewer staffers and even 50% of the organizations with 5,000 or more employees reported the same, though the sample size for that latter group was relatively small.

Figure 2.

Influence on security controls

Which security controls are in your direct control and which do you influence?

	Direct control (myself and my direct reports)	Influence through stakeholders outside of security team	No control or input
Vulnerability management	62%	34%	4%
Identity and access management	55%	41%	4%
Business resilience and recovery tools	54%	41%	5%
Application testing	46%	46%	8%
GRC platform	43%	42%	15%
Physical security and building access management	40%	46%	14%

Data: Dark Reading survey of 156 IT Security leaders, August 2021

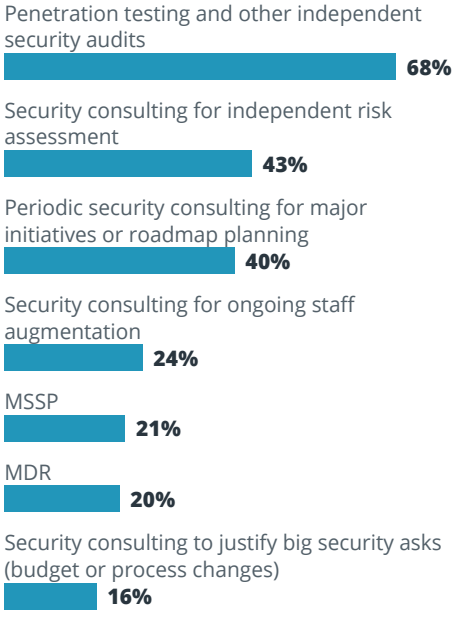
Given the small contingent of in-house staff, it would logically follow that many of these programs depend on consultants and service providers to help supplement staff to fill talent, coverage, or credibility gaps. Interestingly, however, managed service providers and consultants brought in only for straight staff augmentation purposes were not the driving use case in these instances. The number one outsourced duty was for penetration testing and other independent security audits, which was named by 68% of security leaders **(Figure 3)**. Second and third place were almost even or nearly even, with 43% reporting they used security consultants for independent risk assessments, and 40% reporting the use of consultants for roadmap planning or carrying out major initiatives.

This indicates that outsourced help is primarily acquired by CISOs for strategic insight and impartial third-party assessment or guidance. The day-to-day work still remains mostly in the hands of internal staffers.

Figure 3.

Filling talent and coverage gaps

How do you supplement your staff to fill talent, coverage, or credibility gaps?



Note: Multiple responses allowed
Data: Dark Reading survey of 156 IT Security leaders, August 2021

The typical security leaders in our survey are called upon to protect their organizations with tight budgets. Approximately eight in 10 organizations say that their cybersecurity budget comprises 10% or less of the overall IT budget. Fewer than a quarter of respondents operate with more than $5 million per year and 57% say that they run their program with less than $1 million annually.

Unlike with staff size, organization size tends to impact these numbers more significantly. Some 40% of organizations with 1,000 or more employees spend $5 million or more on security. Approximately 14% of these larger organizations have budgets of more than $20 million. This could indicate that many security teams at large enterprises are choosing to spend more on automation, process improvement, and delegating execution of security tasks across the entire organization rather than just throwing bodies at their biggest security problems.

Coalfire expert takeaways

While CISOs are finally getting "a seat at the table" with other business leaders, they are being held to the same expectation to do more with less.

Even at large enterprises, security team sizes are relatively small, but security leaders shouldn't view it as a positive status quo since many organizations still struggle with security coverage gaps (see 'Dimensions of success')

The trend is to reduce more expensive in-house staff by automation and outside contractors.

CISOs gaining more visibility at the top also requires greater accountability for demonstrating the return on investment.

The costs of new tooling must take into consideration the difficult task of growing the team size to manage more and more security tools.

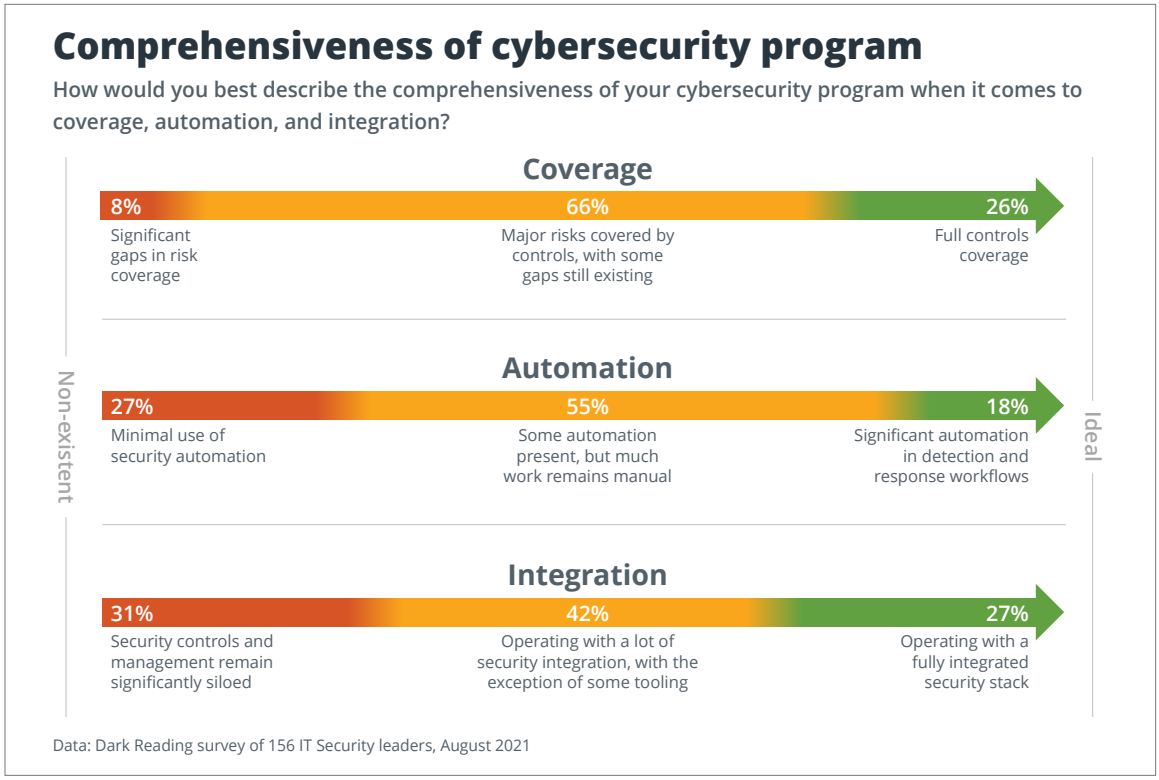
Dimensions of success

Security leaders are notoriously skeptical and cautious folk, so one of the most promising pieces of news from our survey is the confidence that our respondents have in their security programs. When asked a general question about coverage of cyber risk, a full 80% reported that they were confident or very confident that their programs covered all major areas of cyber risk in their organization.

To dig a little further into participants' self-assessment of the comprehensiveness of their programs, we asked them to rate their capabilities in three major areas: controls coverage, automation, and integration. On the controls front, only 8% of security leaders reported significant gaps in their coverage and 26% said they believed their organization was fully covered by a breadth of controls. The majority, 66%, said their organization was somewhere in between, with major risks covered and some gaps still presenting themselves.

Meantime, automation still remains a struggle for most security leaders. Fewer than a third say they use significant automation in detection and response workflows, with the rest reporting a substantial amount of security work that remains manual **(Figure 4)**. Breaking things down by organization size shows that larger organizations are definitely more likely than smaller ones to invest in automation.

Figure 4.



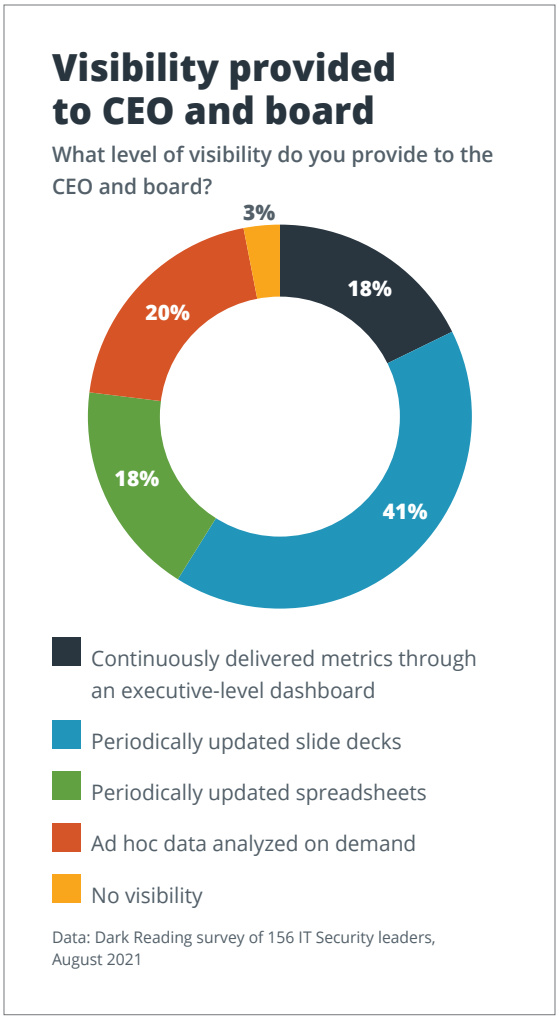
Approximately 34% of companies with more than 1,000 employees say they have significant automation, compared to just 20% of companies with fewer than 1,000 employees. Many CISOs are also similarly battling integration issues in their security stack. Almost a third of respondents said their security controls and risk management programs remain significantly siloed and another 42% have at least some tools remaining outside the integrated security stack.

As security leaders make progress on these programmatic challenges, they must also tie that progress to how the work reduces risk for the organization since that is the top way to communicate the value of cybersecurity for the board, C-suite, and other stakeholders. The survey shows that a sizeable contingent of CISOs consistently track and communicate to numerous stakeholders how their work translates to risk reduction. Our study shows that 43% of security leaders present security metrics to the CEO. Rounding out the top five stakeholders to whom CISOs provide metrics visibility, 37% present to the CIO, 32% present to the CTO, 27% present to the board, and 26% to the CFO. While not as likely to be kept in the loop, other likely informed stakeholders include product managers, chief risk officers, and chief digital officers.

CISO updates on metrics and the current state of security are done regularly at a significant number of organizations. Approximately two-thirds of CISOs provide performance updates at least quarterly to their C-suite, with 48% providing similarly regular updates to the board. In many instances CISOs are also called upon by the C-suite and board to provide on-demand updates, i.e., approximately a third of security leaders say they must be ready for these ad-hoc presentations.

For the most part, CISOs still struggle to mature their practices in providing security visibility to the CEO and board. Only about 18% of security leaders say they continuously deliver metrics through an executive level dashboard **(Figure 5)**.

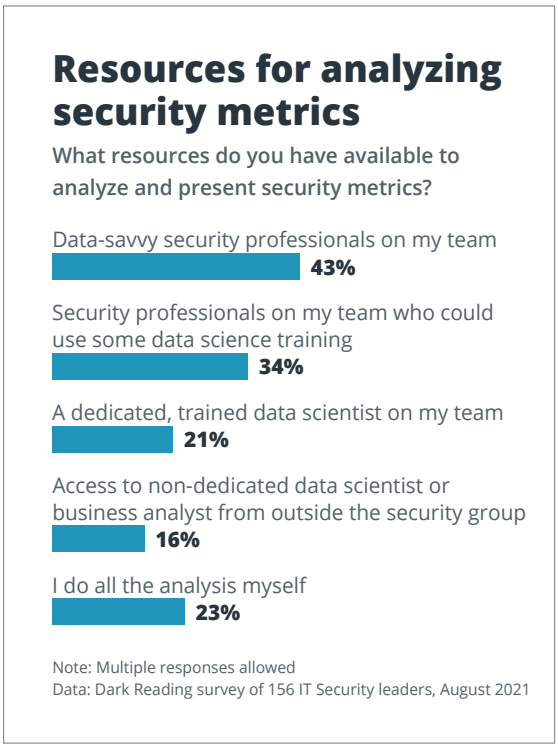
Figure 5.



The majority still deliver metrics and analysis through periodically updated slide decks and spreadsheets. And as many as one in five security leaders must scurry around to do ad-hoc analysis of data when the CEO or board asks for it.

What's more, many of these CISOs are literally doing this scurrying all by themselves. Nearly one in four security leaders report that they do all of the number crunching themselves when it comes to analyzing and presenting security metrics **(Figure 6)**.

Figure 6.



Fortunately, it appears that a sizeable number of CISOs can draw upon various resources to delegate that analysis. The most likely place they turn to are data-savvy security professionals within their team, named by 43% of respondents. Another 34% delegate to security pros who may need more training on data science. Most promisingly, 21% of leaders say they now have a dedicated, trained data scientist on their staff to do this work. Given the typically lean size of security teams, this is a telling indicator of how important security metrics are to CISOs and the executive leadership teams today.

Whether presented to the board, C-suite, or other executive leaders, risk is the number one category of data points used to prove cybersecurity value. These include measurements on number of incidents, severity, frequency, time to recover, and so on. This tracks with respondents' general attitude of how they show value to relevant stakeholders in their organization.

Approximately 61% say they report on risk reduction across business functions to show value, and 59% report on improved security outcomes through cyber-specific metrics **(Figure 7)**.

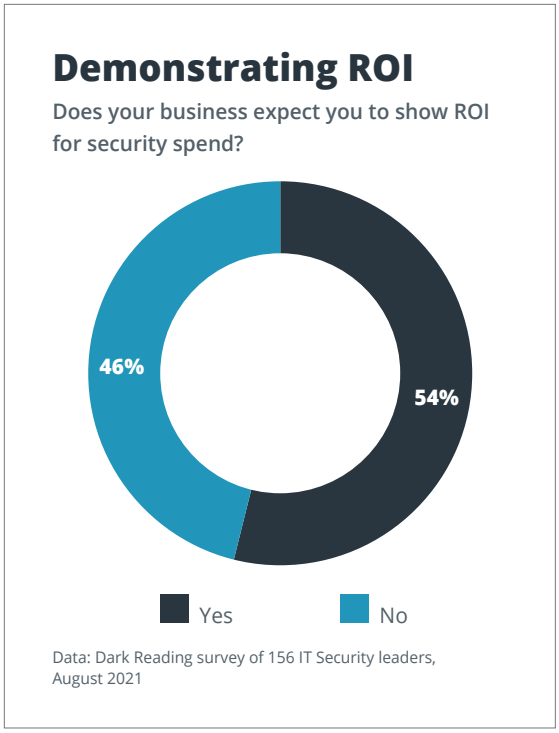
Figure 7.

Cost management and revenue generation also play a part in how many security leaders communicate the value of their program and demonstrate ROI.

Approximately 37% say they report on improvements in spending efficiency to show value, and 25% report on lowered cost per acquisition. On the top-line side, 26% of leaders report on new product development by adding security features, 19% do so on increased lifetime value, and 16% tie brand loyalty metrics to security to communicate its role in driving revenue.

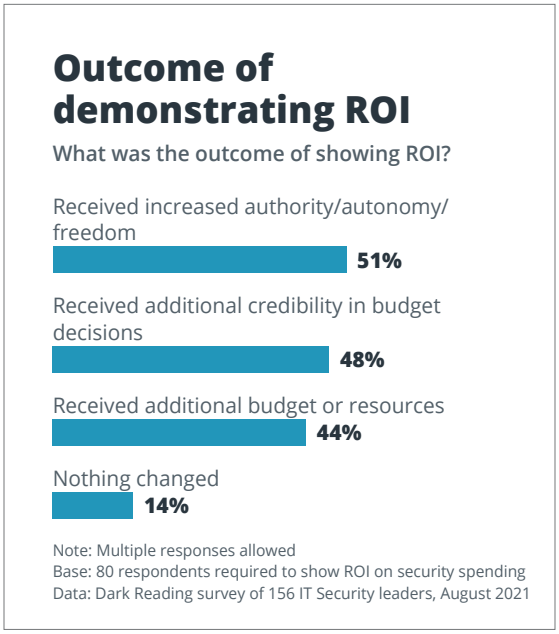
Just over half of security leaders says that they are expected to show ROI for security spending **(Figure 8)**.

Figure 8.



When they are able to do this, the top two results are increased authority and added credibility when it comes to making budget decisions **(Figure 9)**.

Figure 9.



Coalfire expert takeaways

CISOs need to be prepared to demonstrate the value of their programs in dimensions the business cares about, i.e., reduced risk exposure.

Metrics alone don't tell the story. When speaking with non-cybersecurity professionals, the ability to put the data into business context is critical when trying to demonstrate value of the cybersecurity program over time.

CISOs should always be apprised of current cybersecurity events and how well their organization is prepared, particularly with executive leadership and boards requesting spur of the moment updates on items of interest.

As CISOs increase their presence, focusing on managing horizontal relationships as well as managing upward will help build a support network with their peers in other functions, broadening their reach and sphere of influence.

Security culture and influence

Both the executive- and director-level responses from this survey showed a great deal of optimism as to the value of the role of the CISO in today's typical organization. The non-C-level respondents who report that their head of security is a check-box figurehead is minimal, i.e., just 10% of respondents. Of those with a CISO or similar title, just 5% view themselves as a check-box figurehead. What's more, 42% of non-C-level respondents say that their head of security is valued and has significant influence in how the organization makes risk decisions, and 40% of CISOs feel the same about themselves **(Figure 10)**.

Even more promising is the fact that 79% of respondents report that security is an integrated part of annual business planning. And rare is the organization today that doesn't have business stakeholders consult someone in the security team about the risks of new business initiatives before moving forward. Only 5% of respondents said that happens at their organization.

Meanwhile 40% say they're asked for input when business objectives are identified, 49% are asked for input early on as a new product or process is developed, and 55% are asked to check the security of an initiative before it goes live.

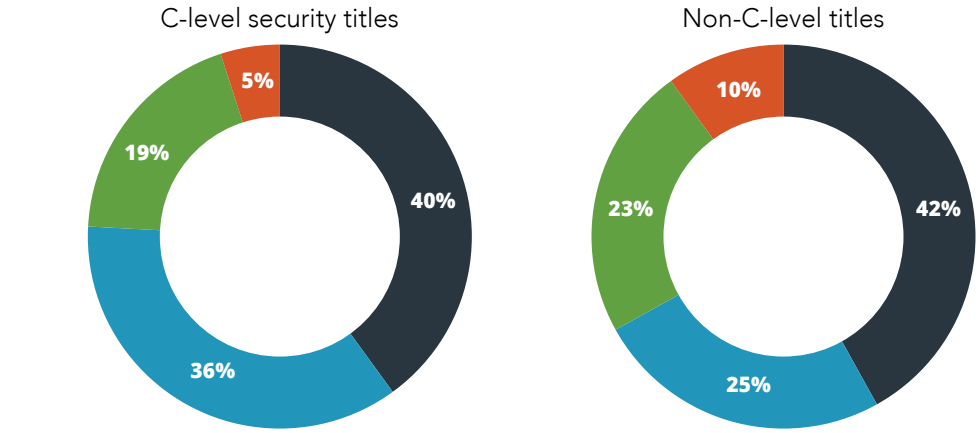
This is leading to a lot less fatalism amongst CISOs these days.

When asked if they sometimes felt that they and their security team were the only ones in their organization aware of the importance of the security team, 71% said no **(Figure 11)**.

Figure 10.

Head of security's value to executive team

How valued do you feel (or how valued do you think your head of security is valued) as part of the executive team?

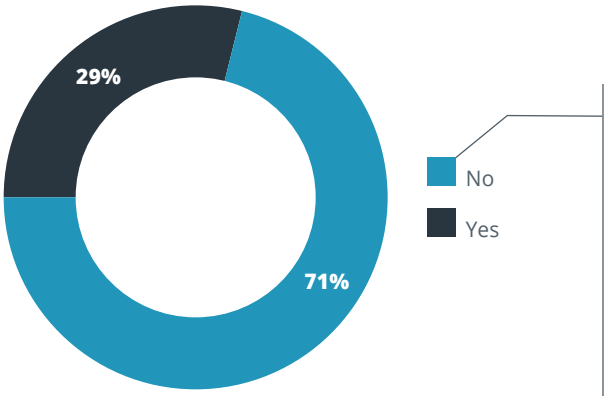


Base: 57 respondents with a title of CISO, CSO, CRO, CPO, CIO, CTO, or VP of Security
Base: 98 respondents with a non-C-level or VP job title
Data: Dark Reading survey of 156 IT Security leaders, August 2021

Figure 11.

Others' awareness of importance of cybersecurity

Do you sometimes feel that you and your reports are the only people in your organization who are truly aware of the importance of cybersecurity?



Responses of those who said "no."

Other technical executives are aware	51%
The CEO is aware	40%
Non-technical executives are aware	36%
The board is aware	31%
Business stakeholders are aware	22%

Data: Dark Reading survey of 156 IT Security leaders, August 2021

They reported that other technical executives, the CEO, the board, non-technical executives, and business stakeholders all had varying degrees of awareness about the importance of security issues.

This growing awareness likely comes from a number of fronts. Not only from external news cycles dedicated to public breach disclosures, and internal efforts by the CISO, but also increasingly by the board and CEO having management put their money where their mouths are. A sizeable number of organizations now tie security KPIs to compensation for non-security employees. Some 35% of respondents say their organization does this for product managers, 27% say they do it for the C-suite, and 19% say this is done for various business stakeholders.

Coalfire expert takeaways

While the CISO role is challenging, very few organizations look at the role as solely checking a box. In fact, a significant number of executives see the CISO as a positive influence on the organization.

CISOs need to understand the impact security decisions have on new initiatives. Risk can never be totally eliminated, but it can be managed down to an acceptable level. No risk most often equates to no reward.

When other executives have security KPIs tied to their compensation, the CISO is in a great position to help others succeed.

Leadership philosophy

The CISOs and CSOs interviewed for this survey tended to have a decent amount of experience under their belts. Approximately 40% of them have had stints of five years or longer at a single organization and 72% said they've been in their current role for three or more years.

That translates to a lot of war stories and lessons learned the hard way. When asked in an open question about what it takes for security leaders to transform their leadership role from tactical program builder to a trusted thought leader, the answers varied but they tended to focus on non-technical efforts around communication, collaboration, and relationship-building with business colleagues, with the number one goal of managing risks while enabling the business.

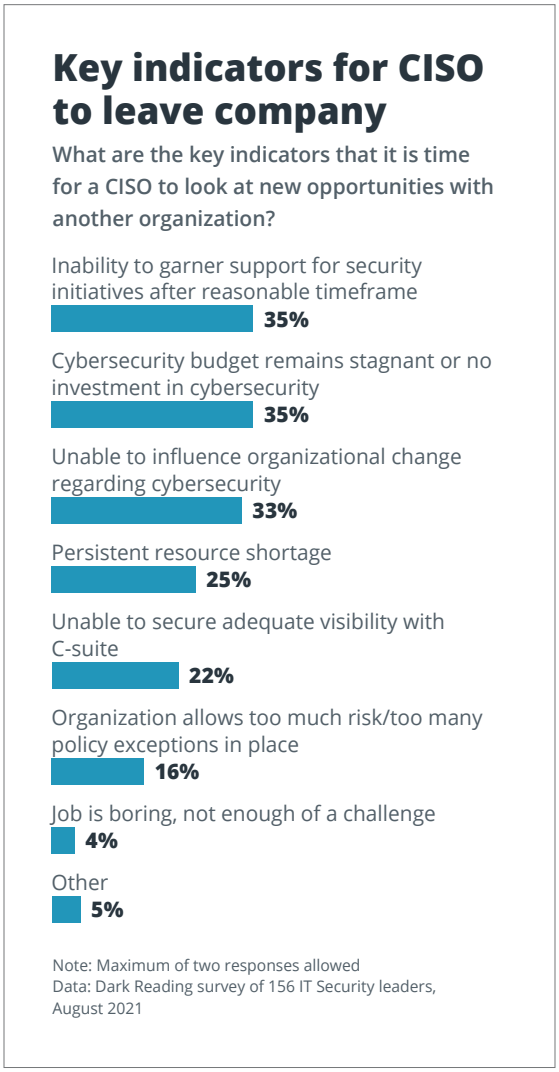
As one respondent put it, the key ingredient to making this jump is "understanding business need and structuring security to deliver business value rather than technical proficiency." Many CISOs believe this translates into metrics that not only measure risk reduction, but also show how security is making improvements to the business. For example, one respondent said they are reporting to the board KPIs showing productivity gain for employees and customers' employees, lowered the cost of ownership from realistic security policies, and faster compliance times to prove their team's value.

"The ROI, value chains, and intrinsic strength of various security elements have lasting, ongoing positive impacts on the company's competitive positioning and success in all aspects of the market share gains for us as a player," that respondent

stated, explaining that this was a big part of solidifying their strategic role in the organization.

Sometimes it may be time to cut bait and seek out new opportunities. The top three red flags named by security leaders as signs that it was time to look for new opportunities were the inability to garner support for initiatives after reasonable timeframes, stagnant security budgets, and an inability to influence organizational change **(Figure 12)**.

Figure 12.



Coalfire expert takeaways

The longer a CISO's tenure at an organization, the more likely the longevity is the result of aligning security strategy to the business objectives and relating it back to ROI.

If the CISO fails to demonstrate how they add value to the business, the business generally will not support the CISO's initiatives.

If the CISO aligns their security program to business objectives, positive organizational change follows.

Conclusion

While there is clearly still work to be done by security leaders in strengthening their role in the enterprise, the results from this survey indicate positive signs that the modern CISO is making meaningful impacts at many organizations today.

Security leadership has moved the needle on true risk reduction versus basic security blocking and tackling, and that is reflected in the discipline and rigor with which the CISO has taken in measuring and reporting risk performance across the organization. Additionally, like all good executives in the enterprise, the typical CISO is getting the most out of their people through a programmatic approach that frequently weaves in outside insight and support to keep teams lean and efficient.

About

COALFIRE

The world's leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS organizations – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success.

For more information visit coalfire.com.

Survey methodology

Dark Reading conducted an online survey on behalf of Coalfire in August 2021 to explore the current function of cybersecurity leaders, such as CSOs, CISOs, chief risk officers and others who manage a cybersecurity team. The final data set is made up of 156 IT and cybersecurity managers who manage an IT security team or report up to senior security management. All respondents were primarily from North American organizations.

Eleven percent held CISO job title, and 18% were other C-level cybersecurity managers such as CSO, CRO, CPO, or VP of security. One-quarter of respondents work at large companies of 5,000 or more employees, 28% are from companies with 1,000 to 4,999 employees, 24% from companies with 100 to 999 employees, and 23% from small companies of under 100 employees. Respondents hailed from a variety of more than 20 industries.

The survey was conducted online. Respondents were recruited via emailed invitations containing an embedded link to the survey. The emails were sent to a select group of Informa Tech's qualified database. Informa Tech was responsible for all survey administration, data collection, and data analysis. Informa is the parent company of Dark Reading. These procedures were carried out in strict accordance with standard market research practices and existing US privacy laws.