Deloitte.

The future of cyber survey 2019

Cyber everywhere. Succeed anywhere.

Cyber

Contents

Executive summary

The fourth industrial revolution is driving change and digitization at an exciting pace. New technologies are disrupting traditional ways of doing business, new markets are being created, and with every innovation the world becomes more and more digitally connected.

As the world becomes smaller, cyber is getting bigger, and it's moving in multiple dimensions across multiple disciplines—beyond an organization's walls and IT environments and into the products it creates, the factories where it makes them, the spaces where its employees conceive them, and where its customers use them. It is at the center of digital transformation. Understanding that is as transformative as cyber itself—and to be successful in this new era, organizations should embrace a "cyber everywhere" reality. From the results of this survey, Enterprise leadership are being called to align their priorities and work in concert to drive core business objectives. Cyber is everyone's responsibility.

Deloitte Cyber conducted the Future of Cyber Survey among 500 C-level executives who have visibility to and responsibility for cybersecurity in companies with at least $500 million in annual revenue to gain insights into how these leaders are embracing the concept of "cyber everywhere"—how they are operating in the new cyber norm and how they are collaborating with partners and other key stakeholders. As one of the leading and largest cybersecurity risk advisory practices globally, our team of more than 4,000 cyber risk professionals continues to walk alongside leading global organizations to help them more confidently plan and execute an integrated cyber strategy that empowers business growth through transformative innovation. The goal of this survey report is to put the numbers into context and to expand the dialogue and acceptance of cyber everywhere so that organizations are not limited by it but empowered to embrace the opportunities it will create.

The good news is the survey results indicate the organizations are no longer taking a wait-and-see philosophy to preparing for and responding to cyber incidents. Questions related to budgets, resource allocation, and prioritization of cyber defense efforts indicate that they are proactively addressing cyber risk from various aspects of security—data, application, identity, infrastructure, and incident response. But the findings also suggest that there is still much work to do in aligning cyber initiatives to executive management's digital transformation priorities. The survey responses prompt us to ask how organizations should integrate cyber into an enterprise-wide effort to achieve business outcomes.

Methodology

The Deloitte 2019 Future of Cyber Survey, in conjunction with Wakefield Research, polled 500 C-level executives who oversee cybersecurity at companies with at least $500 million in annual revenue including 100 CISOs, 100 CSOs, 100 CTOs, 100 CIOs, and 100 CROs between January 9, 2019, and January 25, 2019, using an online survey.

Cyber and the challenge of transformation

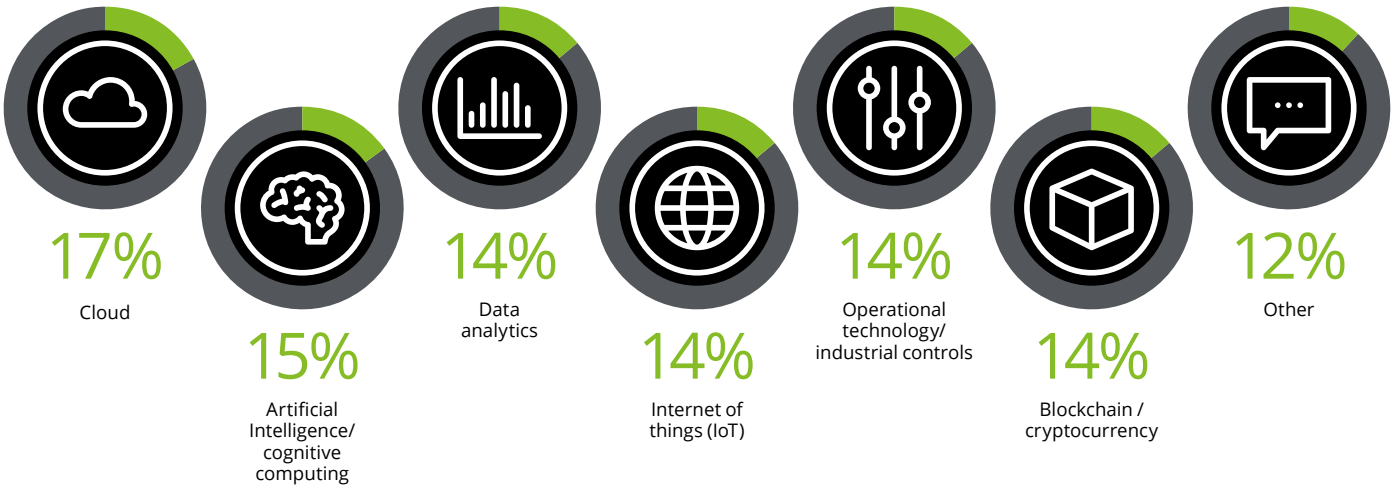
Today's cyber leaders are focused on digital transformation as an important strategy to achieve greater efficiencies while also better protecting the business. That puts a spotlight on emerging cloud, analytics, Internet of Things (IoT), and other transformational capabilities. These technology leaps are consistent with our survey findings, with cyber leaders giving cloud the edge when ranking against other top digital transformation initiatives.

Whether through artificial intelligence, cognitive computing to blockchain and operational technology/ industrial control systems, organizations are now more than ever envisioning the possibilities of digital transformation to simplify their environments and increase efficiencies. On the other hand, our survey reveals that executives across the organization are not necessarily aligned on the best course to steer. As noted in figure 1, there are a wide range of opinions as to which transformation initiative provides the biggest bang for the buck.

On its own, this result could lead us to believe that organizations are on track in their digital transformation, but if we dig into additional findings, the data tell a different story.

Figure 1. Top ranked digital transformation initiatives for the next 12 months

Total participants

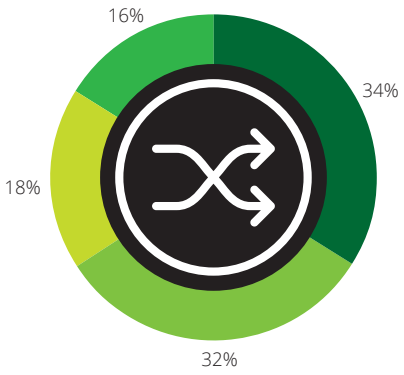


Survey respondents view cyber transformation as one of the most challenging aspects of cyber risk management (see figure 2) that are related to the entire infrastructure (32 percent), with the CSO (35 percent) and CIO (34 percent) respondents ranking cyber transformation as most challenging. This may be the most informative data point of the survey as the CISOs and the CIOs are putting a spotlight on the challenges ahead.

With finite budgets and resources, the ability to apply the level of cyber strategic input and security measures needed as well as deliver on day-to-day cyber management will likely tax even the highest-performing cyber teams. As the survey findings will further reveal, the challenges are not limited to budget and resources but to a collective enterprise alignment on integrating cyber into critical business strategy and operations.

Figure 2. Most challenging aspects of cybersecurity management across enterprise infrastructure

Cyber transformation is the second most challenging aspect of cyber risk management among total participants



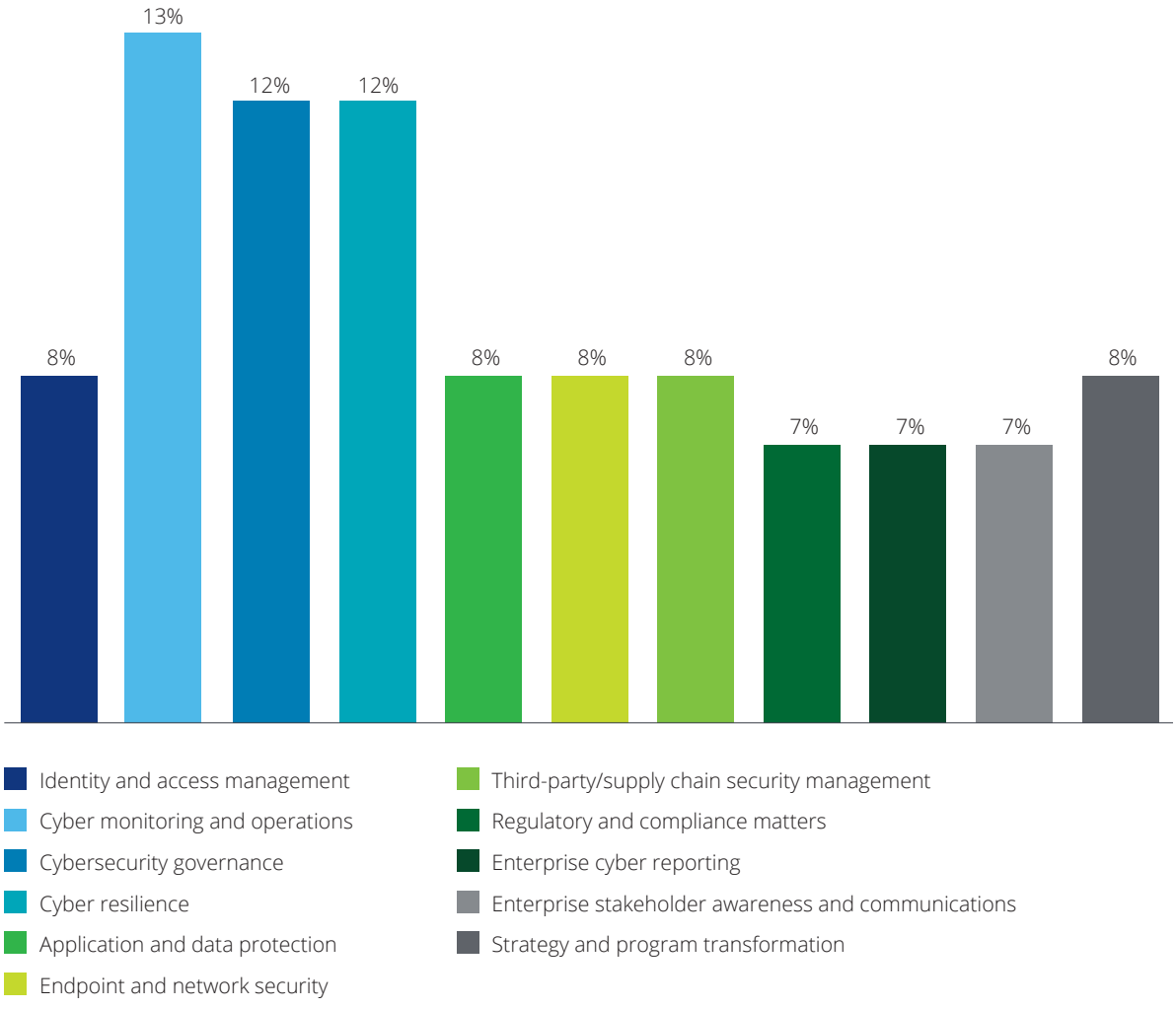
Cyber transformation is the most challenging aspect of cyber risk management for CSOs and CIOs

Shadow IT | Cyber transformation | Cyber hygiene | Hybrid IT

How cybersecurity organizations spend their time (and $$$)

A review of the survey data around time management suggests that many executives are spending a significant amount of their time in three specific areas: cyber governance, resilience, and cyber monitoring and operations (see figure 3). Given the recent surge in higher impact cyberattacks, these numbers confirm that organizations are heavily focusing on two of the five core functions of the National Institute of Standards and Technology (NIST) framework—detect, and respond and recovery—while cyber governance absorbs the third top spot. The remainder of time spent is spread evenly across the other cybersecurity domains.

Figure 3. Average percentage of time spent addressing various cyber domains



In parallel, budgets are seemingly distributed the same way, spreading dollars equitably across the cyber domains while just under 15 percent of the total budget spent is on transformation initiatives including cloud, analytics, and IoT (see figure 4). The results were insightful in that they point out that responding organizations are largely adopting a balanced spread of investment as the strategy of choice to reduce overall risk. But this isn't always necessarily strategic or aligned with organizational digital transformation efforts.

When given an additional opportunity within the survey to write in whatever number best represents the percentage of cyber budget allocated to digital transformation efforts (see figure 5), the answers again were telling with the majority (90 percent) surveyed citing 10 percent or less of budget dollars assigned for efforts such as cloud migration, software-as-a-service (SaaS) implementation, analytics, and machine learning (ML). This implies a stark disconnect between aspirational transformation goals and the reality of finite resources.

Figure 4. Organizations' cyber budget is somewhat evenly spread to broadly protect them from risks

Total participants

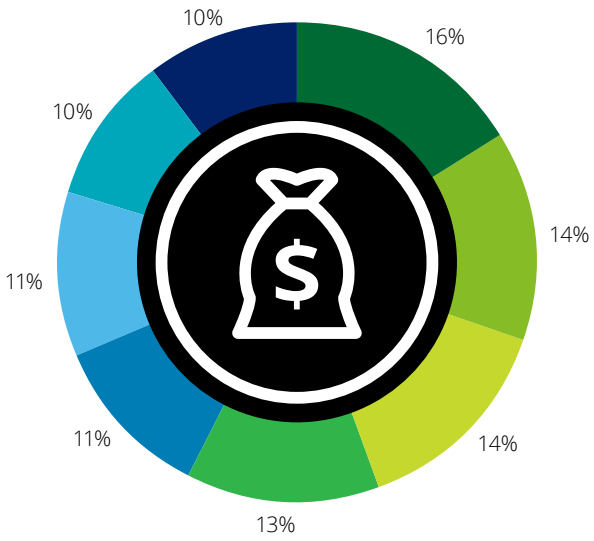
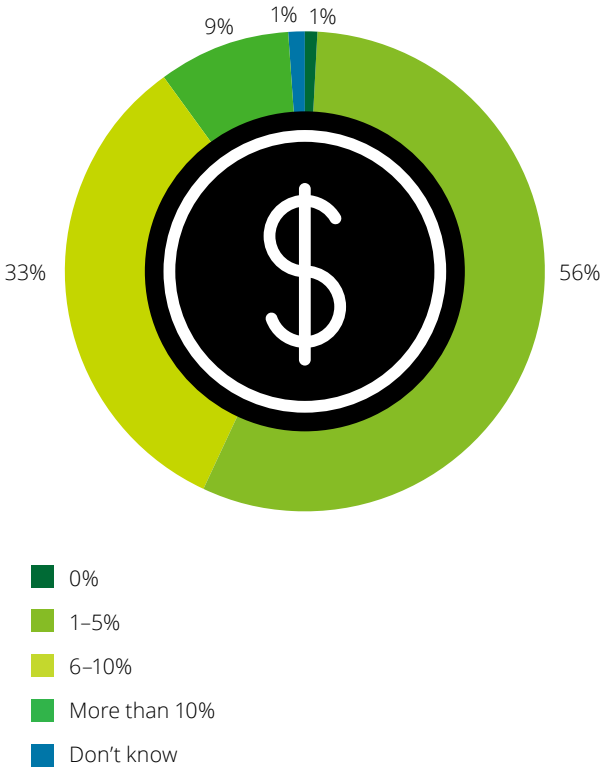


Figure 5. Percentage of cyber budget allocated to digital transformation

Total participants



The survey reveals that respondents believe there are notable gaps in organizational capabilities to meet today's cybersecurity demands. Cyber teams are challenged by their ability to help the organization better prioritize cyber risk across the enterprise (15 percent), followed closely behind by lack of management alignment on priorities (14 percent) and finally, by adequate funding (13 percent) (see figure 6). In addition, the results show a lack of skilled cyber professionals needed to address those priorities and the governance across the organization for it all.

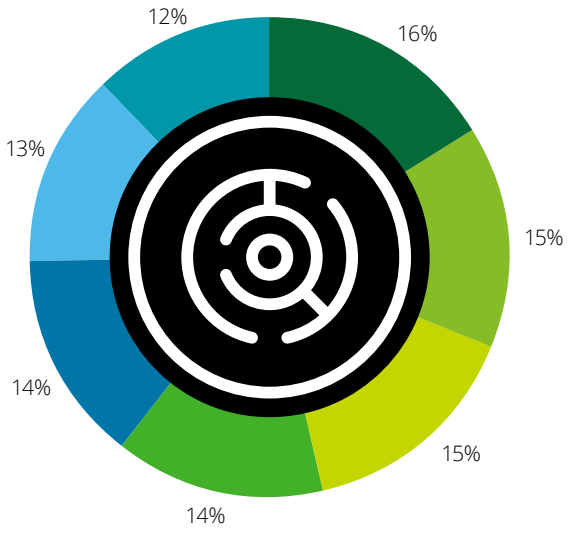
What is the most challenging aspect of cybersecurity management across your organization?

Often, there is a lack of ability to prioritize risks because executive teams haven't locked into a framework or governance model. Therefore, leaders may have a hard time determining how to focus remediation efforts necessary to mitigate the cyber risks to their organization. There are several different frameworks that exist to help an organization manage and report on its cyber risk posture with differing criteria and risk levels. Further complicating matters, we often see various internal teams using differing frameworks; for example, internal audit may focus their assessments using one framework while the CISO has built their program using another framework as the foundation. These teams should align on a collective framework, so they aren't spending unnecessary time and resources aligning objectives or doing twice the work for the same outcome. In order to effectively manage cyber risk, there also needs to be a stronger correlation between technical vulnerabilities, business impact, and value to the organization.

From the data discussed thus far, we can conclude that many organizations today aren't fully equipped to efficiently and effectively tackle today's cyber demands. And while they would like their cyber programs to, at a minimum, keep pace with change and ideally be a leading part in enabling transformation, they aren't adequately funded or positioned to accomplish goals with respect to resources, management alignment, and governance.

Figure 6. What is the most challenging aspect of cyber security management across your organization?

Participants were asked to select their cybersecurity management challenges. Below is the breakdown of their responses.

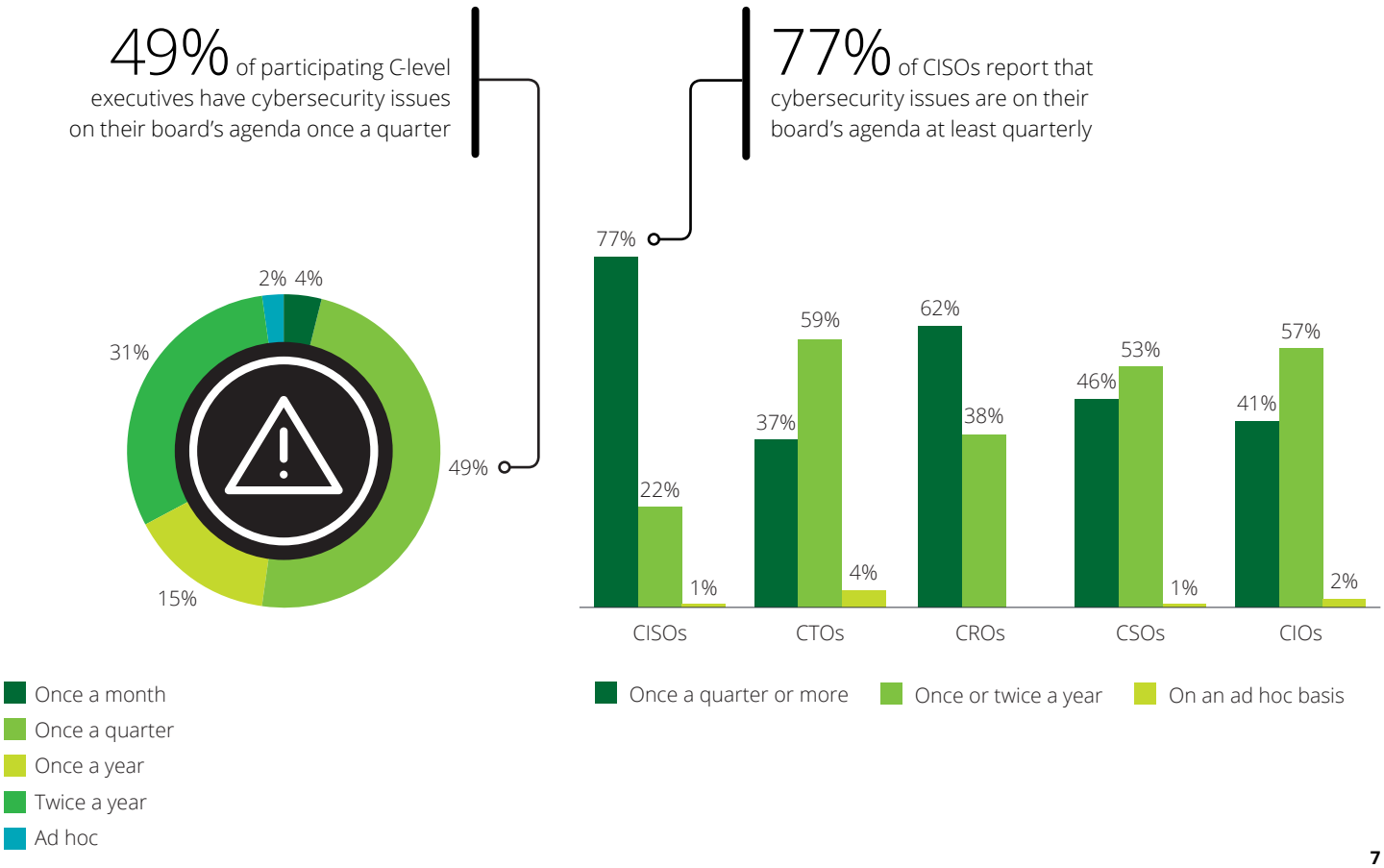


Cyber needs a leader with the authority to drive change

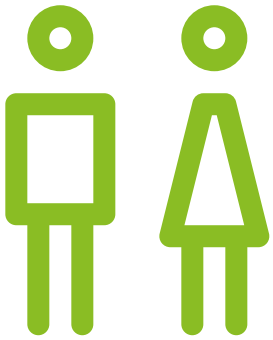
From the results illustrated (see figure 7), we see that nearly half of organizations (49 percent) have cybersecurity on their board agenda at least quarterly. However, at some level, it can be viewed that half of boards are not discussing cyber as often as they likely should be. After all, only 4 percent of respondents say cybersecurity is on the agenda once a month. With the level of risk associated with cyber, shouldn't it have some level of consideration at every board meeting? The answer is yes. Today's boards should have adequate access to cybersecurity expertise, and discussion about cyber risk management should be given regular and adequate time on the board meeting agenda. Askew in these results is the CISO perception of cyber on the board agenda—77 percent of CISOs reported that this occurred quarterly whereby the other C-suite leaders surveyed indicated much lower percentages. We feel that this data supports the fact that the CISO may not actually have line of sight to executive management and the board, whereas most of the other roles surveyed do. Therefore, it is our conclusion the CISO response is often more perception than reality.

Boards should also consider requiring management to provide a set of key performance indicators and key risk indicators that can enable them to quickly ascertain the state of cybersecurity in the company. Directors can work directly with senior management to develop these board-level metrics and benchmarking tools.[1] This topic has never been more important as executives and boards will continue to face mounting pressure to reassure customers, shareholders, and regulators that they are making the most informed cybersecurity investment decisions to protect the company.

Figure 7. How frequently cybersecurity issues are on board's agenda



The survey also tells us that when it comes to evaluating cyber investment decisions, half of participating C-level executives (50 percent) use risk quantitative tools and the other half rely on the experience of their cyber leadership or cyber maturity assessments.



50%

of participating C-level executives employ risk quantification tools to track and evaluate their cybersecurity investment decisions

Many tools are becoming available in the market to assist organizations in their risk maturity assessment, with varied methodologies, but all with the same underlying goal: to better estimate both the direct and intangible costs associated with a cyberattack, thereby providing greater clarity around the potential range and financial risks associated with an incident.

To drive effective execution of a cyber risk program, executive management needs to structure their cybersecurity leadership team to drive communication and implementation of security across the enterprise and have both the authority and expertise to do so. This is typically best achieved when the cyber function is represented in the C-suite so that the broader organization can better understand the priority and importance of adopting or creating a cyber-secure enterprise.

In most cases, the CISO is the de facto cyber champion of the enterprise. Over the course of 5 to 10 years, we have observed the role expanding beyond that of a technology champion to one of strategist and advisor to executive management. Given the previously shared imperative related to the need to prioritize across the enterprise and a need for increased executive buy-in, the next data point could be promising as an indicator that organizations are valuing cyber. When asked about the cyber chain-of-command, 43 percent of surveyed CISOs indicated they report directly to the CEO (see figure 8b). That finding is consistent across the total survey population where 32 percent of respondents indicated the CISO reported to the CEO, with only 19 percent indicating that the role reported to the CIO (see figure 8a). In Deloitte's experience facilitating hundreds of CISO transformation labs over the past five years and through informal collection of data, nearly 80 percent of CISOs report to a CIO or CSO. This indication that CISOs are, in fact, directly reporting to a CEO is quite encouraging but counter to what experience tells us. Did survey respondents share where they think the CISO should report or where it actually reports? It's hard to know. However, if true, this is an important shift to note, as access and influence are imperative in helping executives prioritize and understand what is needed to propel the enterprise forward in the realm of cyber everywhere.

Figure 8a. To whom does the CISO typically report in your organization?

Across companies, the CISO position can be a high-level strategic asset or an operational role focused on addressing technology or information risks, as it commonly answers to the CEO (32 percent) or one of the following members of the C-suite: CIO (19 percent), CTO (12 percent), or CRO (11 percent). Across the five C-level executive groups, participating CISOs appear to be more involved in strategic planning, as they (43 percent) are the most likely to say they report to the CEO directly, leading the other sub-audiences by 9 to 23 points.

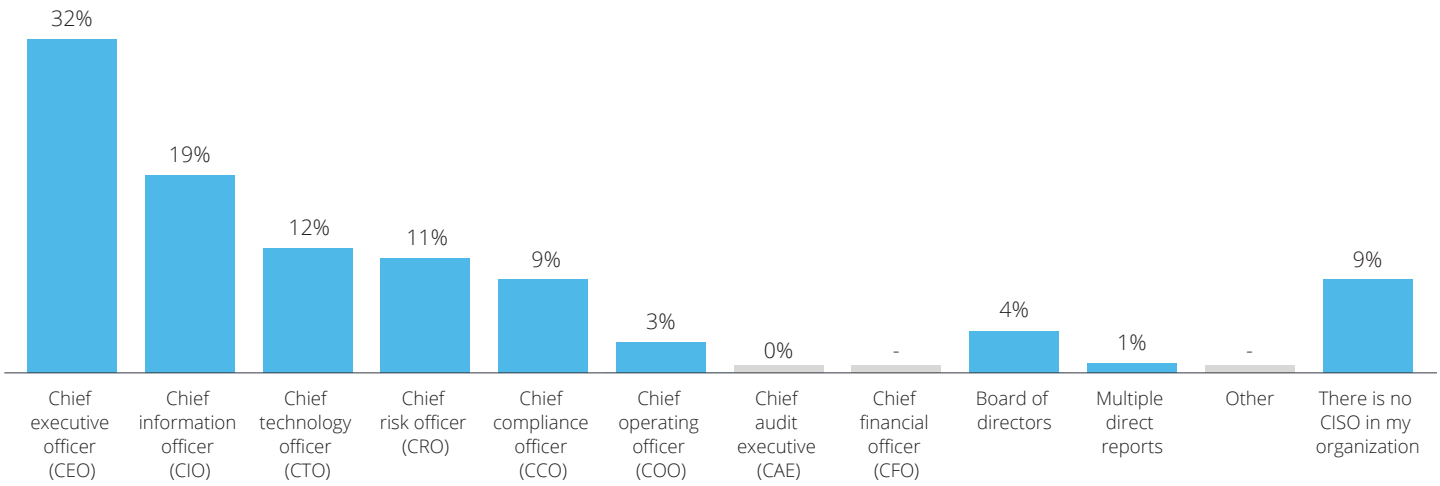
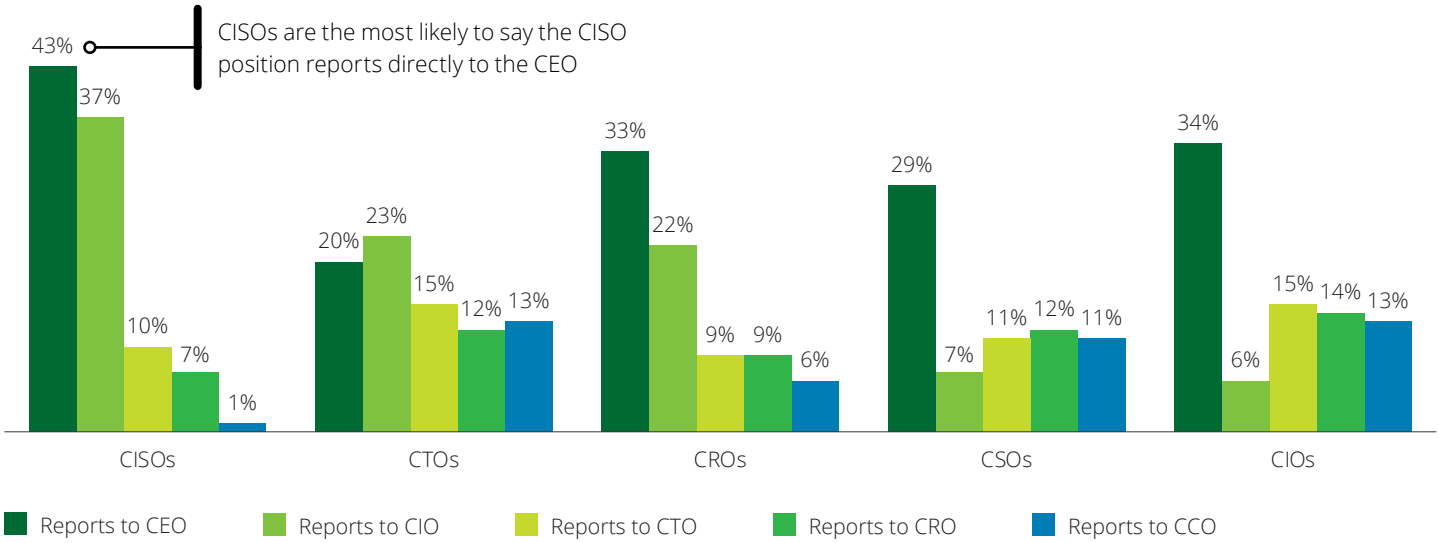


Figure 8b Top positions that the CISO typically reports to in a company



Top responses only

Many organizations still rely on the CISO without fully empowering those in the role to lead confidently across the enterprise. That said, we want to be careful not to get hung up on titles because what matters more is where the responsibility for managing cyber sits in the organization. Some organizations have it a couple layers down where, buried in bureaucracy, the role is nothing more than an IT function. Ensuring the cyber function is senior enough to have line of sight and influence into strategy and operations is critical to cyber transformation in the organization.

Here's what classically happens: cyber is stuck in IT, and IT reports to the CIO. IT security is often equated with cyber, but it is not the same strategic function. By nesting cyber in IT, the cyber budget rests under the IT budget, under the CIO, and that is why you often see the sort of results the survey results are indicating—that cyber isn't actually prioritized or resourced to meet the cyber everywhere realities of tomorrow. In many cases, this leads to situations where CISOs lack the ability to shape strategy and help organizations to prioritize effectively. Similarly, in another example, if cyber sits under the chief legal officer, then cyber may become a compliance-oriented program versus one focused on innovation and risk management.

Cyber is a top strategic business imperative; a pervasive issue that should inform management and sit alongside finance, legal, and operations. Cyber needs "a seat at the table" to help guide the enterprise and ensure it can effectively make the right decisions by looking internally at how the organization runs and looking externally at interactions with customers, suppliers, and business partners. The prolific impact of having cyber embedded in organizational strategy, planning, and the execution of operational or performance effort should not be underestimated. Cyber deserves organizational alignment, prioritization, and reporting structures.

The organizations that do this well today are ones that are typically large custodians of data. They are dialed in to the need for security, innovation, and customer services. In our experience, the organizations that relegate cyber to sub-layers within the organization are less mature in understanding their cyber risk. Seeing the role of the CISO elevated to the C-suite is a positive indication of organizational acceptance that the ubiquity of cyber warrants full senior leadership engagement, greater cyber risk governance, and integration across the enterprise.

Although it is impossible to prevent every cyber incident, with a well-governed, executive-led program it is possible to manage technology risk to acceptable levels. The cyber risk program, rather than being an ever-increasing cost to the business, is a necessary element of the investments made to achieve the strategic goals of the organization.

The future of cyber demands alignment and collaboration both internally and outside the organization

Digital transformation is enabling organizations to simplify their environments, employ stronger technology capabilities to collaborate more effectively, manage data more efficiently, and do what is needed to enable better delivery of their products and services. As you consider the role of cyber, the question becomes how can you integrate cyber and take a position that helps lead the organization and become a catalyst to direct transformation from legacy environments, disconnected data sources, and fragmented identity systems? How can you use this strategy and the supporting infrastructure as a catalyst for change?

Organizational alignment on the risks that matter most to the enterprise may seem obvious, but as the survey results have shown, leadership often struggles to achieve it. According to the survey, the ways in which today's cyber organizations interact with various business units is through security assessments or audits (29 percent), security steering committees that work with the business (29 percent), separate security organizations within each business (24 percent), and 18 percent through security liaisons within each business (see figure 9). We are seeing many organizations have great success with the latter. Cyber professionals embedded in the businesses are an effective approach to manage cyber risk across the enterprise and foster greater collaboration and innovation.

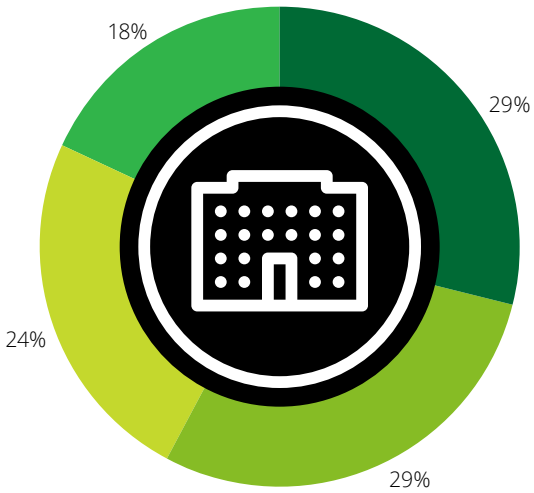
In the financial services industry, many banks have business security officers embedded in the business units. They know the business, and from their purview amongst business analysts and financial professionals, for example, their sole mission is to embed security in new initiatives, manage compliance, and foster collaboration and modernization. This model becomes a catalyst for better efficiency and risk management. This is one example of an organization creating a cyber-secure culture, embedding an ethos of integrated innovation and security within the business units.

But the fact that less than 30 percent of survey respondents selected some sort of security liaisons/champions within each business further supports the lack of readiness of organizations to embrace cyber everywhere.

Embedding cyber professionals into the businesses can enable the cyber organization, and its leader, to be strategic and better manage security in transformation efforts. It allows for the bifurcation of firefighting and strategic planning, because cyber certainly requires both. Within the businesses, cyber is able to represent the security interests of the enterprise and be a part of the discussions from the outset on user experiences, data risks, platform reliability, and so on. The CISO doesn't have time to be in every discussion, but integrating cyber team members who act as liaisons between cyber and the business can help to ensure alignment on organizational priorities and prevents siloed agendas, or worse having to remediate incidents that could have been prevented had cyber been a part of initial discussions.

Figure 9. Cyber department's interaction with other business units

Total participants



Who is the cyber team?

Tangentially, that leads us right back to the survey. When asked what percentage of their workforce supporting cybersecurity are full-time employees versus contractors and consultants, more than 30 percent of CTOs, CROs, and CSOs indicated that the majority (up to 80 percent) were full-time employees (see figure 10). Conversely, the majority of CISOs (81 percent) and CIOs (56 percent) indicated that full-time employees made up less than 20 percent of their cyber teams. The disparity in the findings is surprising until you consider that in many cases, CTOs, CROs, and CSOs are farther removed from the actual tactics of the cyber operation, including how it is staffed. They may have purview related to budget but have limited understanding as it relates to outsourcing and contractor usage. We would infer that the CISO and CIO perspective is likely more accurate in this case.

Much of what is being written about the future of cyber is addressing the looming cyber talent gap. Organizations today are already stressed to staff appropriately, and the cyber workforce is struggling to keep up with demand. By 2021, there is estimated to be an astounding 3.5 million unfilled cybersecurity positions worldwide.[2] That means cybersecurity professionals will have to find ways to compensate for those empty slots. There are too many facets to consider, too many vulnerabilities to take notice of, and too few IT professionals to manage every threat. According to our survey, 85 percent of the participants indicated some level of reliance on vendors and managed services providers to provide cybersecurity operations, with 66 percent of those outsourcing between 21 percent and 50 percent of cyber operations.

Figure 10. Percentage of full-time cybersecurity employees

	Total participants	CISOs	CTOs	CROs	CSOs	CIOs
10% or less	27%	**37%**	19%	27%	20%	**31%**
11–20%	29%	**44%**	25%	26%	23%	25%
21–50%	7%	3%	8%	6%	7%	12%
51–80%	29%	12%	**35%**	**31%**	**39%**	27%
More than 80%	9%	4%	**13%**	**10%**	**11%**	5%

Part of the challenge for organizations evolving their cyber risk capability is that many are limiting themselves by trying to build cyber capabilities in-house. Resources are hard to train and harder to retain. If organizations are going to prioritize cyber in the organization, then executive leadership should begin to explore talent models and strategies to keep up with the burgeoning resource demands. Contractors, or outsourcing entire capabilities, are more efficient and often can deliver at a higher service level. Consideration should also be given to automation of processes and services, which can help improve speed quality and help the organization to do more with less. The combination of these solutions can help address cyber risk. To succeed in the future of cyber, organizations need to become nimbler and more considerate of new channels to getting things accomplished. This includes the growing capabilities of third-party security providers.

We can get an idea from the survey results that organizations are already demonstrating the willingness to rely on third parties to help address cyber everywhere. Nearly all of the survey respondents indicated they had allocated cyber operations dollars toward third-party providers, with 14 percent of total respondents indicating that more than 50 percent of their cybersecurity operations are outsourced (see figure 11). When looking across the roles of survey respondents, 65 percent of CISOs put that percentage of outsourced cyber operations in the 21–30 percent range. The consistency of the CISO responses and differences in comparison to the other C-suite leaders surveyed help us to infer that the CISO is typically responsible for day-to-day cyber oversight.

Figure 11. Percentage of outsourced cybersecurity operations

	Total participants	CISOs	CTOs	CROs	CSOs	CIOs
0%	1%	1%	-	1%	1%	-
1–10%	6%	4%	13%	5%	4%	5%
11–20%	13%	10%	11%	11%	18%	17%
21–30%	44%	65%	29%	48%	31%	48%
31–50%	22%	4%	30%	22%	32%	20%
More than 50%	14%	16%	17%	13%	14%	10%

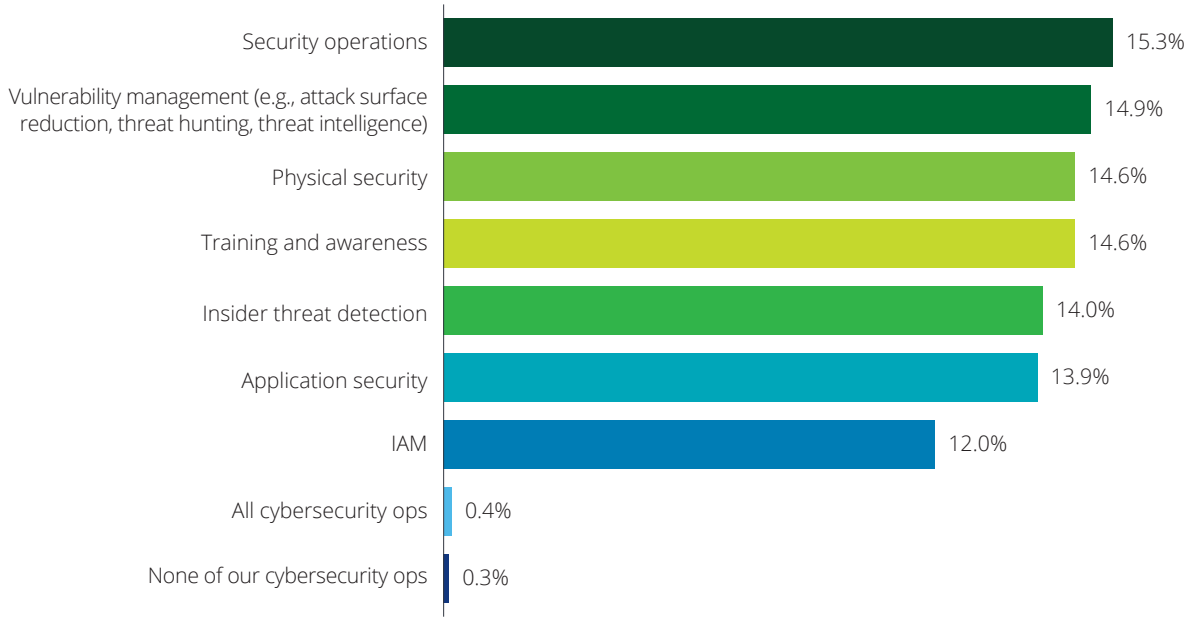
Cybersecurity functions outsourced to third parties

So where are these third-party dollars going? Survey respondents indicated a willingness to outsource a myriad of cybersecurity functions. The collective results of those surveyed is reflected in figure 12. Worth noting, 50 percent of CIOs most often selected security operations, and 48 percent of CISOs chose insider threat detection. Both of those selections stood out in the response data specific to the roles surveyed. But across the board, our survey respondents indicated that they turn to partners most often when it comes to security operations, vulnerability management, physical security, and training and awareness.

Third-party testing should continue to be a valuable tool that streamlines the decision-making process by addressing time and expertise gaps and giving actionable information that technical and business decision makers can use.

Partnerships can be a pathway to success, but failures of third parties have also led to some of the costliest cybersecurity breaches. Our survey data is consistent with what Deloitte is finding in the marketplace, which is many organizations need a little bit of help in a lot of places. To develop a well-rounded cybersecurity program, organizations should partner closely with suppliers, industry associations, governmental agencies, academic institutions, researchers, and other business partners.

Figure 12. Cybersecurity functions outsourced to third parties



Squeezing security into application development

You can see from figure 13 that the survey respondents believe the greatest challenge to managing application security risks is the lack of appropriate organizational structure to enable the integration of security into the application development life cycle. More importantly, it underscores that while organizations would like their cyber programs to, at a minimum, keep pace with change, without structure to enable security integration, awareness of the risks that could impact solutions being developed, and the tools that test and analyze software vulnerabilities, many of today's organizations are not positioned to manage the cyber challenges of tomorrow.

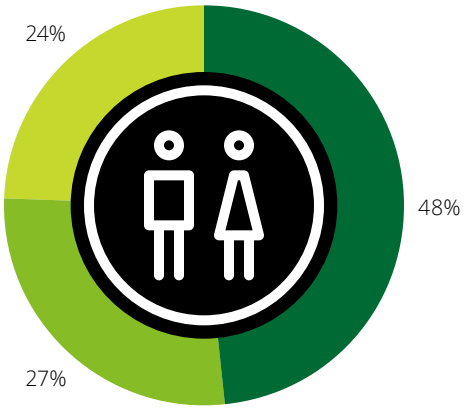
According to the survey (see figure 14), the majority (85 percent) of the C-suite leaders surveyed are leveraging Agile/DevOps to some extent—either fully adopted (48 percent) or in a limited capacity (37 percent). The adjustment needed in this approach for the future of application development is security: introducing DevSecOps.

To enhance their approach to cyber and other risks, forward-thinking organizations are embedding security, privacy, policy, and controls into their DevOps culture, processes, and tools.

As the DevSecOps trend gains momentum, more companies will likely make threat modeling, risk assessment, and security-task automation foundational components of product development initiatives, from ideation to iteration, to launch, to operations. DevSecOps fundamentally transforms cyber and risk management from being compliance-based activities—typically undertaken late in the development life cycle—into essential framing mindsets across the product journey.

Figure 13. Greatest challenge managing application security risks

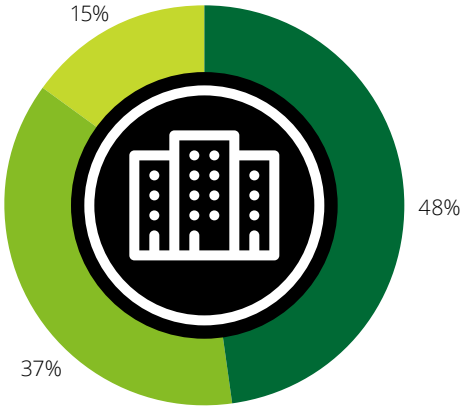
Total participants



- Lack of appropriate organizational structure to enable the integration of security into application development life cycle
- Lack of prioritization/awareness of cyber risks that could impact the solutions being developed
- Lack of tools or solutions that test and analyze software vulnerabilities

Figure 14. Organizational approach to agile/devops

Total participants



- We have fully adopted Agile/DevOps
- We have adopted Agile/DevOps in a limited capacity
- We continue to leverage traditional waterfall approach to software development and deployment

DevSecOps enables you to automate good cybersecurity practices into the toolchain, so they are utilized consistently.

Organizations should be vigilant in conducting risk analysis and threat modeling for both new and existing applications. Of our survey respondents—specifically C-suite leaders with visibility and responsibility for cybersecurity—47 percent indicated that they are doing the analysis and modeling at least once every quarter, with 52 percent of CISOs suggesting they do this once a month.

Secure operations centers (SOC) are increasingly taking on expanded responsibilities, becoming enterprise-wide risk management capabilities or "fusion centers," that service data and analytics requirements for other risk management functions such as physical security, fraud detection, and compliance. To accommodate all this additional data and alert management activity, many organizations are beginning to transform traditional SOC operations models—through the adoption and implementation of ML and artificial intelligence (AI)—to optimize, enhance, and automate threat/risk visibility, detection, and response capabilities.

SaaS environments require greater attention to authentication and access control because the user doesn't own the network. Governance standards need to be put in place to ensure that users take appropriate precautions with data and that all necessary regulatory and compliance guidelines are met.

Without employing DevSecOps, organizations will likely struggle to gain visibility into their hybrid cloud environments, making it almost impossible to determine which computing and storage tasks are taking place where, using which data, and under whose direction.

Cloud adoption also presents challenges to data risk if you don't have visibility into where your data is going, resides, and who has access to it. Hybrid cloud adoption grew 3x in the last year[3]—a mix of premise-based and cloud. There are challenges in protecting data appropriately in the cloud and not just in re-creating the protections that you have on premise. The future of cyber will require organizations to continue to look at data governance and protection more strategically as well as understand what sensitive data they are putting in the cloud and consider the potential controls around it.

Exponential data growth

44 billion GB

of data were created every day in 2016

463 billion GB

of data will be generated daily by 2026[4]

Source: Micro Focus, Growth of Data – 2017, Linkedin SlideShare, November 6, 2017.

Multitenancy risk is also inherent to cloud architectures because multiple virtual machines (VMs) share the same physical space. Major public cloud providers go to great lengths to mitigate the possibility that one tenant could access data in another VM, but on-premise infrastructure is susceptible if the servers are not configured properly. Changes made to one hybrid cloud environment may also inadvertently affect another.

That said, because many different users leverage the same cloud environment, cloud security is particularly suited to building a collaborative environment that rapidly predicts threats through a worldwide threat monitoring system and shares threats among all users under the cloud umbrella.

The Cloud Security Alliance[5] serves as a resource for IT and security professionals alike providing guidelines for building into hybrid infrastructure from the beginning. Organizations should familiarize themselves with these guidelines before beginning the migration process.

The agile and resilient infrastructure of the future

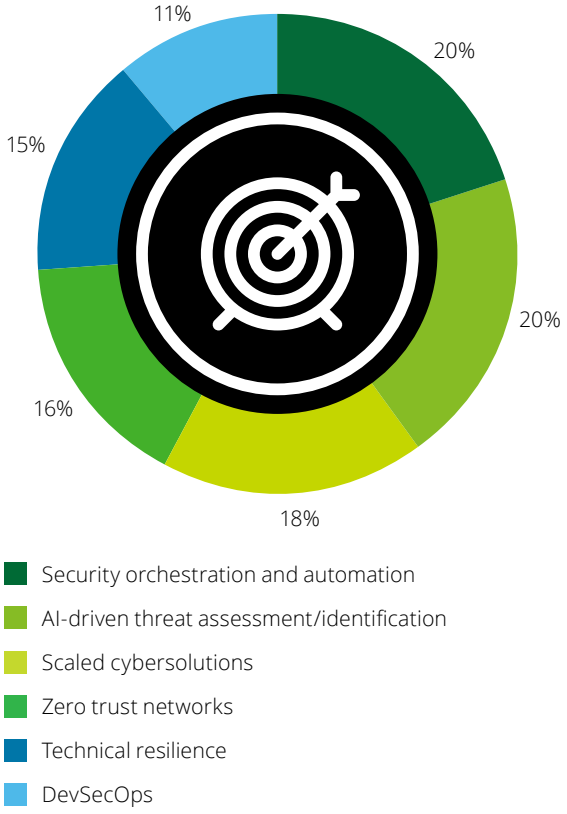
Technology priorities are evolving rapidly in response to digital transformation. New business strategies are driving rapid evolution and adoption of new technologies across four categories: physical, network, servers and storage, and endpoints. As technology continues to revolutionize business and threats to business operations become increasingly complex, organizations will need to rethink how security is integrated across the components that comprise a modernized infrastructure. If security is not adequately prioritized and funded to support this sort of transformation, there will likely be a disconnect in what can be safely delivered.

Enterprise infrastructures are large and complex, and adopting new models will present considerable risk if organizational leadership is not aligned on prioritizing such efforts to drive business outcomes. The transformation gap can arise as organizations adopt modern infrastructure concepts, while still operating their legacy environment—counterintuitively resulting in increased complexity, higher overhead, and talent and skills challenges. Automation, insight, and speed should be used to drive greater efficiency and effectively enable organizations to focus on the strategy behind their transformative efforts.

AI-driven threat assessments, security automation, and scaled solutions are top investment priorities

As it relates to infrastructure, the surveyed C-level executives most commonly selected AI-driven threat assessments (20 percent), security automation (20 percent), and scaled cyber solutions (18 percent) as the top ranked defense concepts that their companies are prioritizing for future investment (see figure 15).

Figure 15. Top ranked cyber defense priorities and investment areas among total participants



Organizations that do not incorporate security into every phase of their development and operations pipelines risk leaving much of their value on the table. Every product created should be a known entity—tested, secure, and reliable. Internal and external users should not have to waste time grappling with cyber surprises. The data in figure 15 is interesting because, again, there appears to be a disconnect between the transformation priorities of the enterprise and the security capabilities of the cyber organization. In this example, DevSecOps is the lowest ranked priority across the C-suite executives surveyed. Yet in the previous section, DevSecOps was highlighted as the necessary approach organizations must take to securely increase speed-to-market and product development. If 85 percent of application development teams are using DevOps in some capacity, a "secure by design" approach could potentially increase outcomes and efficiencies. But based on survey responses, it appears that many organizations are still not bridging the gap to infuse security at key points in the system development life cycle in order to drive transformation.

The goal of an agile and resilient modern infrastructure will require next-generation infrastructure security controls to manage risks and exposure. Although the targets remain the same, adversaries are using new channels and vectors through modern infrastructure attack surfaces. Active defense technologies and analytics such as anomalous detection, ML, and AI enable organizations to gain broader, real-time visibility into their changing threat landscape. As digital becomes the life blood of an organization, reliance on technology increases; therefore, organizations must shift from targeting "acceptable" outage times to "always on" strategies.

Figure 16. Top criteria used to assess potential infrastructure management and cyber risk management partners

	Total participants
Opportunities to outsource foundational cyber defense capabilities (e.g., security monitoring, vulnerability identification, security training and awareness)	22%
Outsourced specialized defense capabilities (e.g., threat hunting, vulnerability remediation, red teaming)	17%
Several integrated security components in a single platform	16%
Solutions that are part of an internally driven strategy/capability roadmap	15%
On-premise-based products and solutions	15%
Cloud-based security products and solutions	15%

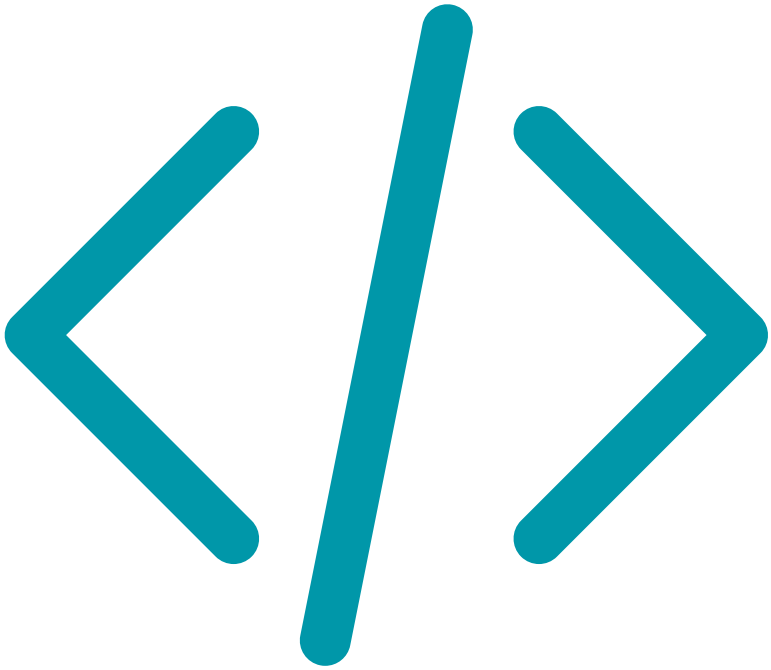
The future of the cyber infrastructure ecosystem uses automation, virtualization, hybrid data centers, software defined networks, and anytime and anywhere access, and requires massive changes in technology operations, all while keeping the lights on.

The survey data does reflect that responding organizations are aware of what is needed to architect flexible, secure operational environments. In the survey, participants were asked to indicate their top criteria for assessing infrastructure and risk management partners. The results, represented in Figure 16, indicate that C-suite leaders do know what to prioritize even if they have yet to fully integrate such capabilities and solutions.

Traditional security tools and approaches do not extend well to ephemeral virtual environments, workload shifting on demand, automation, cross-platform orchestration, etc. As the enterprise works toward transformation, it should consider the following:

- Managing cybersecurity in a modernized environment requires new skills and experience—talent can be difficult to find and retain.
- The pace of development using continuous integration and deployment (CI/CD) models is much, much faster than traditional waterfall or agilefall practices; security teams and processes will struggle to keep up unless automated and risk thresholds are adapted to the "new" world.
- Proper DevSecOps requires tight cross-functional teaming across operations, security, and development, which is likely a new model for many organizations.
- The security impacts of modernization are typically not well understood outside of the security team; this requires a cultural transformation program (communications, role-specific training, awareness, etc.) and balance between user experience and security.
- Unless starting greenfield, companies will be managing both traditional and modernized infrastructures at the same time and creating resource and bandwidth challenges, dual toolchains, and dual operational models.

In this age of digital transformation and hyper connectivity, executives should forego their previous beliefs and ask questions about their organization's infrastructure security capabilities. They will need to evolve their perspectives on traditional means using people, process, and technology and employ new methods in order to support business needs in these continually shifting environments. Cyber will spread across systems and platforms and leaders will have to correlate all of that to understand the actual risks.



Identity is the fabric of the digital economy

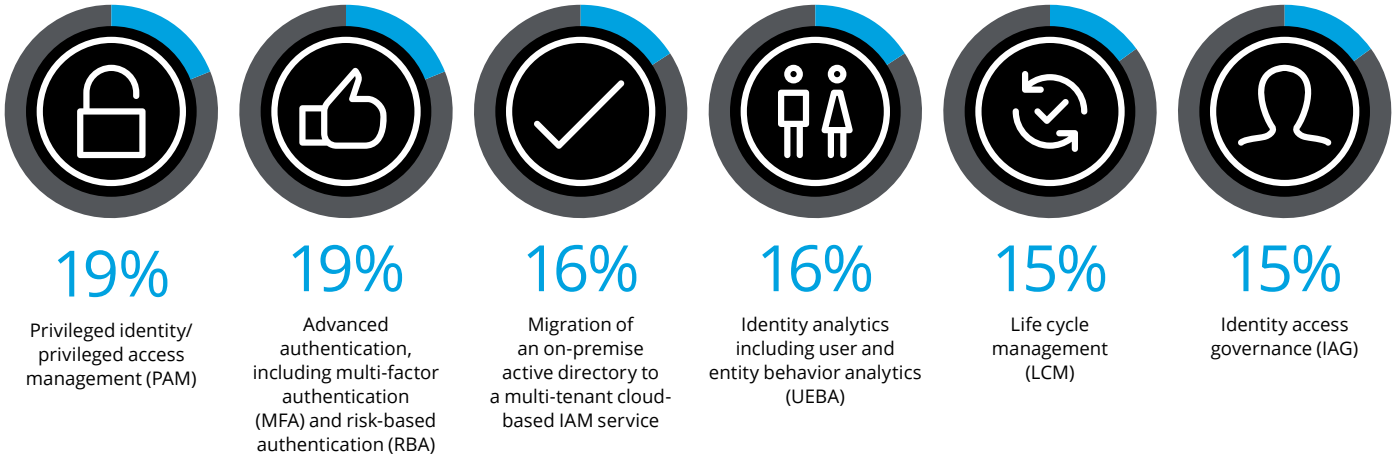
Today, managing access and identities are no longer back-office IT and compliance functions. It's an essential business enablement function at the heart of the digital economy. In fact, the amount being spent on identity management is projected to increase faster than the amount spent on all security measures.[6] In large part this is due to the growing recognition of how important identity management is to enable an effective security posture. It is literally the tie that binds. Identity is the foundation for e-commerce and enables the relationship that the enterprise has with its consumers as part of user experience improvement. Identity has a role in digital transformation, operational efficiency, compliance, and cyber risk. Through data protection, threat detection, resiliency, and application security, identity is woven across the enterprise and the extended enterprise and value chain.

The top ranked internal/enterprise identity security initiatives for the participating C-suite leaders included migration of on-premise active directory to a multi-tenant cloud-based identity access management service; identity analytics including user and entity behavior analytics (UEBA); privileged identity access management (PAM); and advanced authentication including multi-factor authentication (MFA) and risk-based authentication (RBA) (see figure 17).

Worth noting, many IT leaders are finding that long-standing approaches for integrating security into new products are not keeping pace with high-velocity, continuous delivery software development. Platforms typically include standard tools and methods that can promote good design habits and help developers build strong security into their solutions from the outset.

Figure 17. Top ranked internal/enterprise identity security initiatives

Total participants



These findings are consistent with the maturation of identity solutions. Hybrid cloud/on-premise is the new normal for identity management. Organizations need to realize that it isn't an either/or—on-premise or in the cloud. They still need to manage both. Identity analytics is becoming a next-generation security information and event management (SIEM) issue, as the environment that an organization will use to identify insider threats and even as a surveillance tool for continuous authentication.

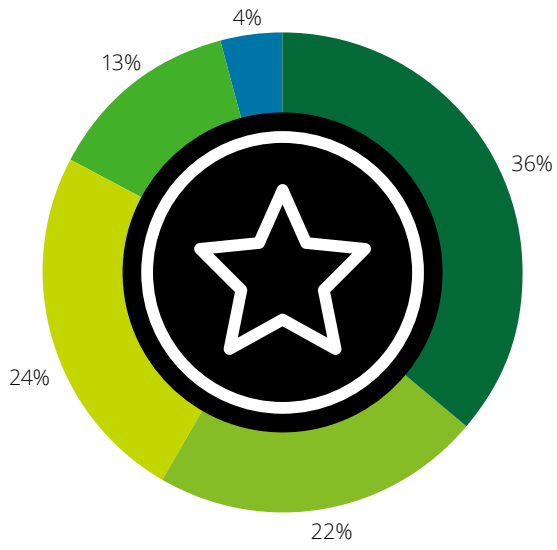
To focus a moment on breach detection: PAM and MFA are two primary breach prevention tools that organizations deploy. With cloud, the need for MFA has never been greater because the organizational front door is now out on the Internet, not behind a corporate firewall. Along with MFA, RBA is an advanced authentication tool that provides a higher efficacy of the authentication process and a better user experience. In most incidents there is an element of compromised credentials as part of the attack. What organizations need to be incorporating as part of their risk management is an understanding of where additional identity and access management controls are required. Through an understanding of their highest risk scenarios, organizations can determine where PAM and MFA can be used to reduce impact of compromised credentials, and to know what authentication is required not only for employees but for consumers.

This is also where organizational change must take place—in the consumer experience. The enterprise can no longer relegate consumer identities to be managed solely by the marketing and sales organizations; the security organization should also have input into consumer and third-party data, access, and compliance.

Survey respondents also indicated that their preferred way to procure, implement, and provide ongoing delivery of identity capabilities was through on-premise implementation with in-house and contractor resources (36 percent). This was notably true for 60 percent of the CISOs surveyed over the next highest leader, the CROs, who responded at 33 percent (see figure 18). In total, 24 percent of all C-suite executives surveyed chose cloud/Identity-as-a-Service (IDaaS) implementation as their preferred way to provide ongoing delivery of identity capabilities.

Figure 18. Preferred way to procure, implement, and provide ongoing delivery of identity capabilities

Total participants



Because CISOs are often uncomfortable having data outside "the four walls" of the enterprise, it's not surprising to see respondents choosing on-premise implementation. But the reality is, with the changing threat surface, a well-thought-out cloud solution with a quality provider may be able to provide a better cybersecurity posture than those created in-house. Access to data and systems may be easier to control when they are limited to hardwired, on-premise legacy platforms, but that's no longer realistic in today's digital economy. As businesses transform and tangible "walls" give way to a limitless cloud environment, the number of possible adversary entry points are growing, and controlling access will be a paramount concern.

According to Gartner, IDaaS will be the preferred delivery model for 80 percent of all new identity purchases by 2022.[7] IDaaS solutions extend on-premise directories into the cloud and provide single sign-on to thousands of cloud (SaaS) applications and access to web applications that run on-premise. With the same features organizations might expect from an on-premise solution, IDaaS can support both cloud and legacy applications while freeing in-house cyber professionals to focus on better business outcomes.

Digital transformation is reshaping identity, and the move to the cloud and the evolving relationships between businesses, users, and things demands a reevaluation of traditional identity services. Beyond the obvious efficiency gains, cloud-based identity management is likely to provide better options for addressing digital identity needs of the future. Identity models themselves are becoming more user-driven, enabled by analytics that process the rich troves of data available on the Internet. Federated digital identity models will become more common for managing identities that must be shared across multiple interdependent organizations. Done well, a move to the cloud can help innovative organizations both improve digital identity management today and establish a platform for future advancement.

Organizations will have to find the balance in identity management to avoid stifling vital business activities and enabling improper access that could inflict damage on competitiveness and reputation. The challenge is to find a balanced approach to systems access by establishing effective and flexible identity management controls.

When asked which cyber defense concepts survey respondents were prioritizing to transform security capabilities, 16 percent of the C-suite executives indicated Zero Trust Networks as their top ranked response. Many organizations in high-touch consumer industries are expected to move toward a Zero Trust framework to limit the risks associated with excessive user privileges and access, and significantly improve security detection and response with analytics and automation.

There's a recognition that just because a user is inside the network does not mean they should be or that their intentions are good. There's no longer a safe "in here" versus unsafe "out there" approach. The future of cyber is progressing to an understood state of "untrusted." Organizations will need to consider the infrastructure required to sustain ongoing monitoring. Continuous authentication will be a heavy lift for IT and security operations, especially in terms of the data to analyze. It is our opinion, continuous authentication will become the new norm… it's just a matter of how fast.

For many organizations, their identity and access management programs are not where they would like them to be. Over the next 18 to 24 months, organizations may need help maturing supporting processes; undertaking digital transformation objectives; or facing rapid growth or changes due to mergers and acquisitions. Each organization has its own challenges and requirements.

People and processes influence the effectiveness of identity and access programs just as much as technology does. When they align, organizations are better positioned to not only guard against risks, but also enhance the user's ability to profit from applications, systems, and data. Organizations that commit to anticipating problems caused by deficient data; addressing financial, technological, and operational challenges; aligning ownership of identity in the organization; and investing in the proper resources from staff and external resources, will likely find themselves better equipped to weave their way through the digital economy.

The data dilemma

In an increasingly data-centric world, many organizations are overwhelmed and challenged when it comes to protecting data. Throughout the survey, for each question where we have highlighted responses pertaining to transformation there is a data response also. Data management complexities was the top survey response when participants were asked about the top challenge (see figure 6), and below in figure 19, when asked which of the top three cybersecurity threats they were most concerned about, data integrity was most often selected.

Organizations need to balance risk with innovation, profits, and talent. There isn't enough time or resources available for an organization to protect all data created or ingested. Therefore, organizations must focus on securing the data that are most valuable to their businesses. In today's hyperconnected world, massive amounts of data are produced by a rapidly growing number of devices. But what happens if cybercriminals get their hands on the data? With such power to influence the public's behavior, the consequences could be significant.

Bad actors are constantly looking for any little weakness, and IoT greatly expands the universe of potential weaknesses—whether in a certain device, device-to-device communications, or the broader Internet. Even a single breach point may be enough to compromise the entire IoT network. IoT greatly expands the amount of data that can be affected. IoT data have the potential to be far more detailed and sensitive because data can be collected in real time directly at the source.[8] The challenges are mounting in managing AI processes and verifying the accuracy and availability of sensor and device data and resultant decisions.

When asked about data disclosures, 9 out of 10 organizations experienced disclosures of sensitive business production data in their test and development environments within the past 12 months. With their vulnerability in data security on full display, the surveyed C-level executives are likely not alone when they admit they are most concerned about data integrity.

Figure 19. Top three ranked most concerning cyber threats among total participants

Total participants

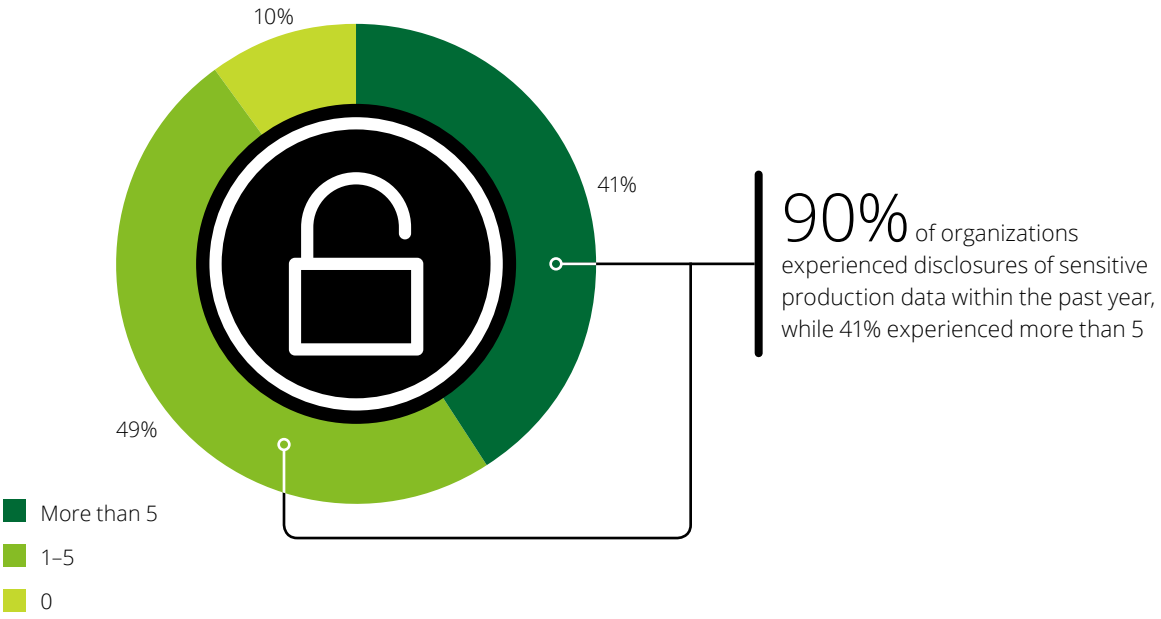
35%
Data integrity

32%
Actions of well-meaning employees

31%
Technical vulnerabilities

Figure 20. Number of sensitive production data disclosures within test and development environment in the last 12 months

Total participants



Nearly all C-level executives (92 percent) indicate a need for their companies to improve policies on how to avoid the disclosures of sensitive business production data. This result further underscores the need for DevSecOps as data is being lost in the production environment. Only 11 percent of surveyed C-level executives completely agree their companies' policies enable them to comply with data protection requirements from various regulatory organizations.

Multiple parts of the enterprise are creating ways to influence and better service customers, but they will need to be ever-aware of the data they are asking to collect, the superfluous data they are also ingesting, and ultimately what is being done with that data. Data must be analyzed equally as a liability and an asset. Data risk management is the responsibility of groups across the enterprise, including marketing, human resources, operations, information technology, legal, and compliance. However, many organizations are designating a data officer to be responsible for managing data risk and work in concert with enterprise executives to ensure the integrity of data.

Additionally, data analytics are driving product development, resulting in the enterprise's need to innovate or risk profit deterioration. Challenges posed here include governance of data, managing the integrity of the data as well as the results from analytics, and asking questions like: "Are the results in line with expectations?" "Are the data sets accurate?" "Are the results unbiased?"

Stringent compliance regulations such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are driving transparency and rights management for personal data belonging to employees and consumers alike. Consent management, the ability to modify data, and the ability to delete personal data are provisions that need to be addressed to avoid non-compliance fines.

Throughout the survey, in questions regarding where collective budget and/or resource allocations are spread, some variance of data protection is typically a chosen response among survey respondents. While collectively the responses indicate that budgets and resources are spread fairly evenly across cybersecurity initiatives, data interests top the list, and that finding is supported by the rising visibility and regulatory scrutiny regarding data integrity, privacy, and protection for organizations.

Strategizing for perpetual resilience

What can be learned from strategies should inform response plans, and what is learned from response should inform the next strategy. By 2021, cybercrime damage is estimated to hit $6 trillion annually.[9] To put that in perspective, that's almost 10 percent of the world's economy.

Many business leaders have begun to acknowledge that, despite strong security controls, cyber incidents will occur. How heavily they impact an organization's reputation, bottom line, and market standing depends—in part—on how well-prepared the organization is to analyze and contain an incident as it unfolds, respond decisively, and manage the aftermath.

Nearly all (95 percent) C-level executives surveyed admit their companies have experienced a wide range of cyberattacks, and well over half (57 percent) report their most recent cyber breach occurred within the past two years (see figure 21). These attacks caused serious impacts on their companies' revenue, reputation, and leadership stability.

There is a consensus among the surveyed executives that the loss of revenue due to operational disruption and the loss of customer trust are the biggest impacts cyber incidents can have on organizations. In 2016, Deloitte's report, "Beneath the surface of a cyberattack,"[10] illustrated, in financial terms, the broad business impacts a cyberattack can have, from the time an incident is discovered through the long-term recovery process. The study gave executives a true look at what they stood to lose, beyond data records. In the past two years alone, the fallout from data breaches and large-scale cyber incidents has led to massive revenue loss due to operational disruption, changes in leadership, reputational loss, drop in share price, and most recently, the levying of regulatory fines.

Figure 21. Timing of most recent cyber incident or breach among total participants*

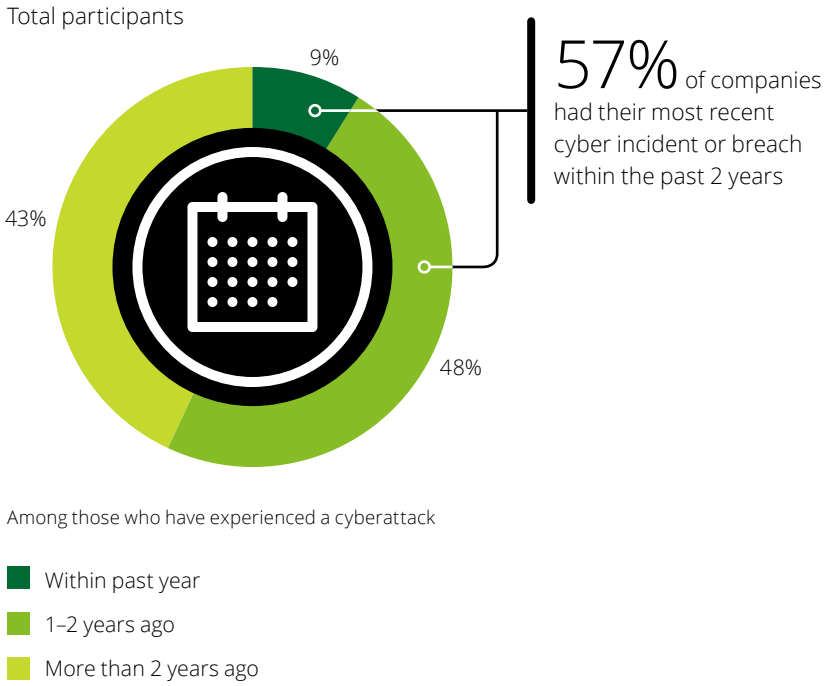
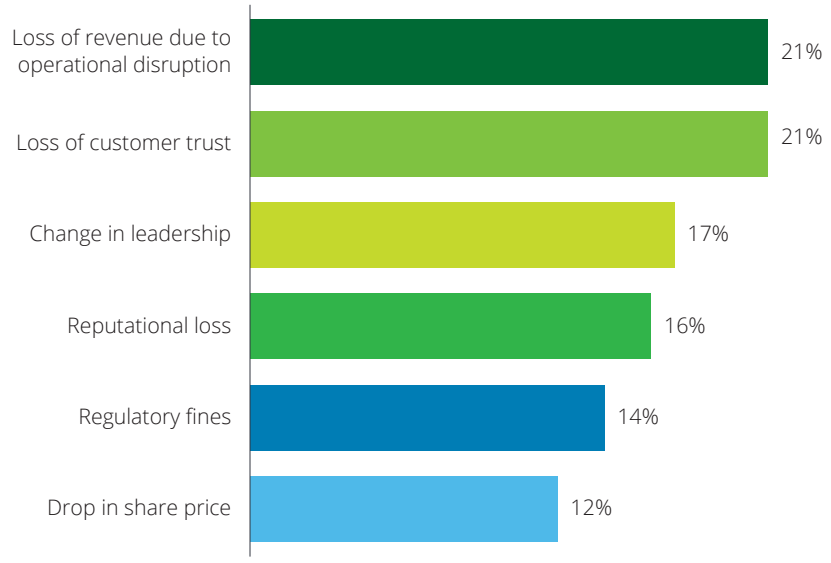


Figure 22. Biggest impacts of cyber incidents or breaches on organizations

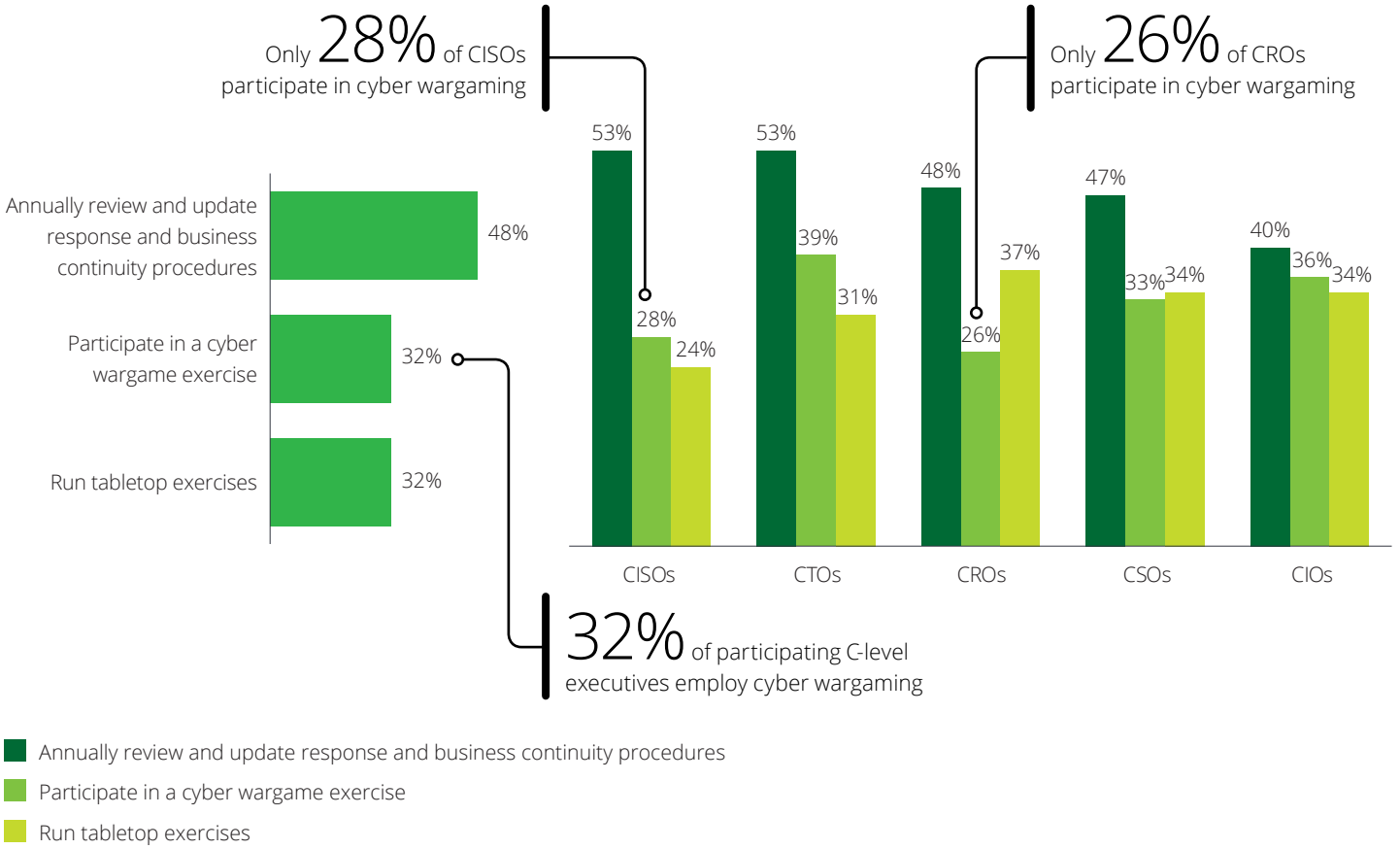


When it comes to cyber preparedness, constant change is often the most difficult to manage in any organization—and this provides the greatest advantage to the adversary. Implementing new ways of doing business, technology upgrades, personnel changes, regulatory adjustments, and changes in third-party systems can introduce new, unanticipated vulnerabilities. These changes, coupled with the constant evolution of cyber threat tactics, constantly alter an organization's cyber risk profile and decrease preparedness, causing a natural erosion of overall cyber readiness if left unchecked. Because the threat landscape changes rapidly and responses cannot be perfectly scripted, cyber wargaming has become a leading strategy in an effort to get ahead.

Cyber wargaming provides an interactive technique that immerses potential cyber incident responders in a simulated cyber scenario to help organizations evaluate their cyber incident response preparedness. These exercises test an organization's response reflexes, identify capability gaps, and train on and develop advanced preparedness techniques. Yet, despite the benefits of cyber wargaming, our survey indicated that only about one-third of participating C-level executives (32 percent) say their companies conduct cyber wargaming exercises to prepare them for real-world incidents (see figure 23). Wargaming involves the various business leaders in a very plausible scenario and creates that collective buy-in into everyone's role in cybersecurity.

Figure 23. Methods for reviewing and testing cyber incident response processes and procedures

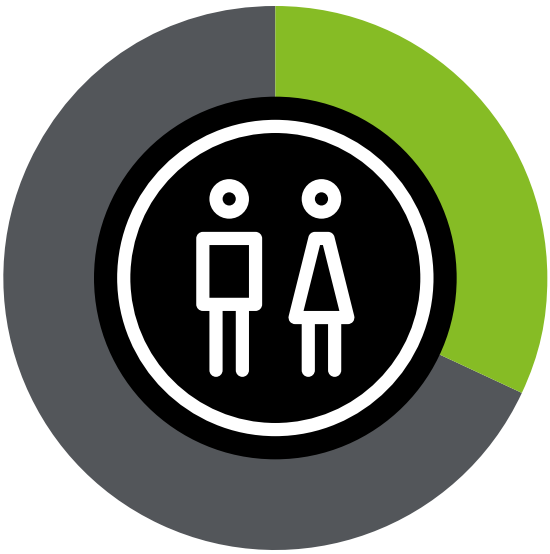
Only about one-third of participating C-level executives ((32 percent)) say their companies participate in cyber wargaming exercises to prepare them for incident responses, with CROs (26 percent) and CISOs (28 percent) reporting the least use among all the sub-audiences surveyed.



Thirty-two percent of cyber leaders surveyed say they plan to leverage their incident response (IR) processes to handle data destruction attacks that use advanced tactics, indicating that most companies still rely on standard disaster recovery or specific data backup protocols for data destruction events.

Over the past few years, several large businesses were "locked out" of their information technology globally, leaving them without any ability to run their operations—no IT; no phones; no data; and unable to keep the lights on after both production and backup data systems were targeted, locked down or destroyed. Attackers have demonstrated that they can now eradicate the ability to conduct business, and this trend is only getting worse. Some businesses are developing strategies, procedures, and other workarounds to allow their teams to continue to complete critical tasks, even after losing access to their technology. In parallel, we are seeing an uptick in cross-organization cyber response synchronization to reduce downtime while integrating cyber, business continuity, disaster recovery, and crisis management teams into response "cells" to collectively manage the response and recovery. Together organizations can innovate as they recover and learn with each adversarial advance.

Cyber threats are constantly evolving, and as companies prepare and implement new security measures, hackers and other cybercriminals are finding new ways to break through those same defenses. In the coming decade, nationally sponsored organizations will continue to develop cyberattack technologies for defense and offense; financially driven criminal groups will continue to seek ways to monetize cyberattacks; hacktivists will continue to use cyber to convey their messages; terrorist groups will also shift to cyberspace; and, finally people with no apparent motive, who seek to demonstrate their technical skills, will continue "contributing" to the attacker ecosystem.



32%

of participating C-level executives plan to leverage their IR processes to handle data destruction attacks that use advanced tactics

Conclusion

How are organizations adapting to the new realm of cyber everywhere? Well, some might say they are all building the plane, while they're flying it. Deloitte's Future of Cyber Survey asked C-suite leaders to explain how they were constructing their "planes" and what tools they were investing in to ensure that they could safely land and take off again tomorrow, and the next day and the day after that. The metaphor is accurate. New organizations can benefit from the opportunity to establish and grow a cyber-minded culture and secure by design approach with a strategic cyber risk framework from inception. However, for organizations already in existence today, executive management will need to reconsider how they achieve their business outcomes, reengineer strategies for addressing cyber risk, and create new "flight plans" without skipping an operational beat. With each evolving challenge will come extraordinary opportunity. As organizations develop and adopt increasingly disruptive technologies, including harnessing big data, cognitive computing, and IoT, the common thread among them remains cyber.

This report highlights the fact that the enterprise today is working to meet the demands of a "cyber everywhere" reality but may not be fully ready for what's coming and may need to reposition itself to succeed in tackling the cyber demands of the future. Transformation initiatives are often under-supported by organizational leadership, and cybersecurity budgets are still managed as if addressing traditional IT problems versus being prioritized to lead true organizational change. The survey results tell us that perception may actually be leading reality when it comes to cyber organizations' ability to keep pace with transformation and in leading enterprise adoption of a cyber-secure culture.

We conclude that:

- Cyber requires more executive attention, budget, prioritization, people, tools, processes, governance, and overall collective thought
- Cyber needs a leader with the authority to drive change
- Cyber will require organizations to become more nimble, more flexible, and more collaborative as they work to secure their organizations, their employees, their customers, and partners
- Data complexities will continue to challenge many organizations
- Automation, speed, and insights will power the future of cyber

The demands of cyber everywhere are too big for any one organization to manage on its own, regardless of how large, capable, and experienced their internal team may be. The far-reaching tentacles of cyber and evolving complexity and challenge of cyber threats, will continue to tax an organization's ability to effectively focus on business outcomes. Cyber necessitates a shift for greater collaboration and awareness across the enterprise to achieve business outcomes while ensuring security considerations from the outset.

Cyber is about starting things. Not stopping them. Organizations should feel equipped with control that enables the freedom to create. The goals for security operations have not changed, but how those goals are achieved is changing rapidly.

Endnotes

1. Mary Galligan and Bob Lamm, *On the board's agenda: Cyber risk in the boardroom*, Deloitte, 2018, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/center-for-board-effectiveness/us-cbe-feb-otba-risk-in-the-boardroom.pdf.
2. Steve Morgan, "Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021," CSO, June 6, 2017, https://www.csoonline.com/article/3200024/security/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html.
3. Louis Columbus, "2017 state of cloud adoption and security," *Forbes*, April 23, 2017, https://www.forbes.com/sites/louiscolumbus/2017/04/23/2017-state-of-cloud-adoption-and-security/#4c04c17d1848.
4. Micro Focus, Growth of Internet Data - 2017, LinkedIn SlideShare, November 6, 2017, https://www.slideshare.net/Micro-Focus/growth-of-internet-data-2017
5. Cloud Security Alliance (CSA) website, https://cloudsecurityalliance.org/.
6. Martin Gontovnikas, "The firewall of the future is identity," Auth0, May 29, 2017, https://auth0.com/blog/the-firewall-of-the-future-is-identity/.
7. Bill Briggs, Nishita Henry, and Andy Main, *Tech Trends 2019: Beyond the digital frontier*, 10th Anniversary edition, Deloitte Insights, https://www2.deloitte.com/insights/us/en/focus/tech-trends.html?id=us:2el:3dc:tt19:eng:cons:011619:spromo
8. Sean Peasley, Tyler Lewis, Brian Wolfe, Robert Schmid, and Mahesh Chandramouli, *Secure IoT by design: Cybersecurity capabilities to look for when choosing an IoT platform*, Deloitte, October 2018, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/us-IoT-platform-security.pdf.
9. US Department of Homeland Security, Secretary Kirstjen M. Nielsen Remarks at the RSA Conference, April 17, 2018, https://www.dhs.gov/news/2018/04/17/secretary-kirstjen-m-nielsen-remarks-rsa-conference#1.
10. Emily Mossburg, John Gelinne, and Hector Calzada, *Beneath the surface of a cyberattack: A deeper look at business impacts*, Deloitte, 2016, https://www2.deloitte.com/insights/us/en/industry/dcom/beneath-the-surface-of-a-cyberattack.html.

Contacts:

Ed Powers
National Managing Principal
Deloitte & Touche LLP
epowers@deloitte.com

Irfan Saif
Principal, Future of Cyber Leader
Deloitte & Touche LLP
isaif@deloitte.com

Emily Mossburg
Principal, Advise & Implement Leader
Deloitte & Touche LLP
emossburg@deloitte.com

Adnan Amjad
Partner, Managed Services & Products Leader
Deloitte & Touche LLP
aamjad@deloitte.com

Kieran Norton
Principal, Infrastructure Security Leader
Deloitte & Touche LLP
kinorton@deloitte.com

Vic Katyal
Principal, Data Risk Leader
Deloitte & Touche LLP
vkatyal@deloitte.com

Andrew Morrison
Principal, Strategy, Defense & Response Leader
Deloitte & Touche LLP
anmorrison@deloitte.com

Vikram Kunchala
Principal, Application Security Leader
Deloitte & Touche LLP
vkunchala@deloitte.com

Mike Wyatt
Principal, Identity Leader
Deloitte & Touche LLP
miwyatt@deloitte.com

Acknowledgements

We wish to thank:
John Gelinne, Managing Director (Deloitte & Touche LLP)
Nicole Hockin, Senior Manager (Deloitte & Touche LLP)
Dominic Conde, Graphic Designer (Deloitte Services LP)

We would also like to thank the rest of the survey team, and the many others who contributed their ideas and insights into this report.

Deloitte.