ORACLE KPMG

Mission of the Cloud-centric CISO

Part of the Oracle and KPMG
Cloud Threat Report series

Research conducted in partnership with ESG

Contents

Executive Summary

Welcome to the fifth and final installment of the Cloud Threat Report series. The previous reports, The Oracle and KPMG Cloud Threat Report, Demystifying the Cloud Security Shared Responsibility Model, Addressing Cyber Risk and Fraud in the Cloud, and The Business Impact of a Data Breach, highlighted the need for a cultural shift to close the cloud security readiness gap, outlined the confusion over the demarcation line between cloud service provider (CSP) and the customer, elevated the conversation around business fraud and quantified data breaches in business terms.

There are several common themes across the Cloud Threat Report series by Oracle and KPMG. Organizations are pursuing new types of digital transformation initiatives to increase revenue opportunities, cut costs, streamline operations, and improve relationships with customers.

For the purposes of this report, digital transformation is defined as follows:

> Digital transformation is based upon the integration of digital technology into all areas of a business. In this way, DX profoundly changes business operations, organizational culture, and customer relationships.

Public cloud computing (IaaS, PaaS, SaaS) has often been a foundation for these projects. More recently however, public cloud computing is teaming up with other technology trends like IoT/OT adoption, 5G proliferation, and work from home (WFH) momentum to accelerate the pace of digital transformation initiatives. Unfortunately, one of the primary conclusions of the Oracle and KPMG research is that there is a consistent mismatch between the scale, velocity, and temporal nature of cloud computing and rigid cybersecurity programs that continue to underscore the level of preparedness businesses have with regards to their cloud security programs.

The report further explores the cloud security readiness gap as it relates to business executives and CISOs. This report concludes:

- **CISOs are more engaged with DX and cloud computing.** In the past, the term CISO was sometimes mocked as the "crisis induced sacrificial offering" because data security responsibility and accountability began and ended with this position. This is changing however as CISOs are spending more time working with line-of-business (LOB) leaders aligning business processes with cloud computing, explaining cloud computing cyber-risks to executives and boards, updating threat models tied to cloud computing, and identifying instances of shadow IT applications. Taken together, it's clear that CISOs are scrambling to support DX and cloud computing initiatives but challenges remain—92% of organizations say they have a cloud readiness gap.
- **Many organizations demand more cloud-centric expertise.** While traditional CISOs are adjusting to cloud computing, the research indicates that they may not have the right expertise for the job. In fact, 73% of organizations have hired or plan to hire a CISO with greater cloud computing skills while 53% of organizations employ or plan to employ a business information security officer (BISO) to work with LOB managers to integrate cybersecurity into business processes. Clearly, there is a need to transition the CISO position from a technology to a business focus. As part of this shift, CISO cloud computing acumen is paramount.
- **Business requirements demand new CISO skills and priorities.** Emerging CISO skill set requirements can be summarized by a new role—the DX CISO. Digital transformation CISOs will become part of the executive team and report directly to CEOs. Their primary business tasks include educating executives and board of directors on cybersecurity, measuring and managing DX-driven cyber-risks, and champion a cybersecurity culture within their organizations. On the technology side, DX CISOs will be responsible for monitoring the security of hybrid IT from end to end, advancing cloud security skills to technical and non-technical users, establishing automated DevSecOps processes, creating/enforcing least privilege policies, and rationalizing the security stack to improve efficacy and operational efficiency.

Organizations are Moving Toward Digital Transformation and Cloud Computing

Data from the Oracle and KPMG Cloud Threat Report indicates a clear and growing trend – large organizations are embracing cloud computing as a foundation for their business strategies. For example:

- **Business-critical applications are moving to IaaS/PaaS…**
  40% of survey respondents (i.e. from the Oracle and KPMG Cloud Threat Report research survey) said that at least 30% of their business-critical applications have been "lifted and shifted" to IaaS/PaaS today. Security professionals believe this will increase to 58% of business-critical applications moving to IaaS/PaaS within the next 24 months (see ***Figure 1***).

- **And organizations are embracing SaaS.**
  The Oracle and KPMG data points to a similar trend with SaaS —35% of organizations consume at least 30% of their business-critical applications as SaaS today. This will increase to 60% over the next 24 months (see ***Figure 2***).

The migration to the cloud is often part of a broader business strategy centered around digital transformation (DX)

DX is increasingly pervasive in multiple industries. Retailers have replaced printed catalogues and mailing campaigns with targeted digital marketing. Manufacturers are using data analytics to improve demand forecasting and supply chain management. Automobile companies are monitoring vehicle health and customer behavior throughout the ownership lifecycle, while health care providers have adopted DX initiatives like telemedicine, artificial intelligence (AI)-enabled medical devices, and blockchain electronic health records. DX initiatives like these have a strong dependency on cloud computing for rapid application development/deployment, data analytics, and rapid scalability based upon user demand.

Figure 1.

Of all sanctioned business-critical applications used by your organization, approximately what percentage have been lifted and shifted to public cloud infrastructure services (i.e. IaaS/PaaS) today? How do you expect this to change—if at all—over the next 24 months?

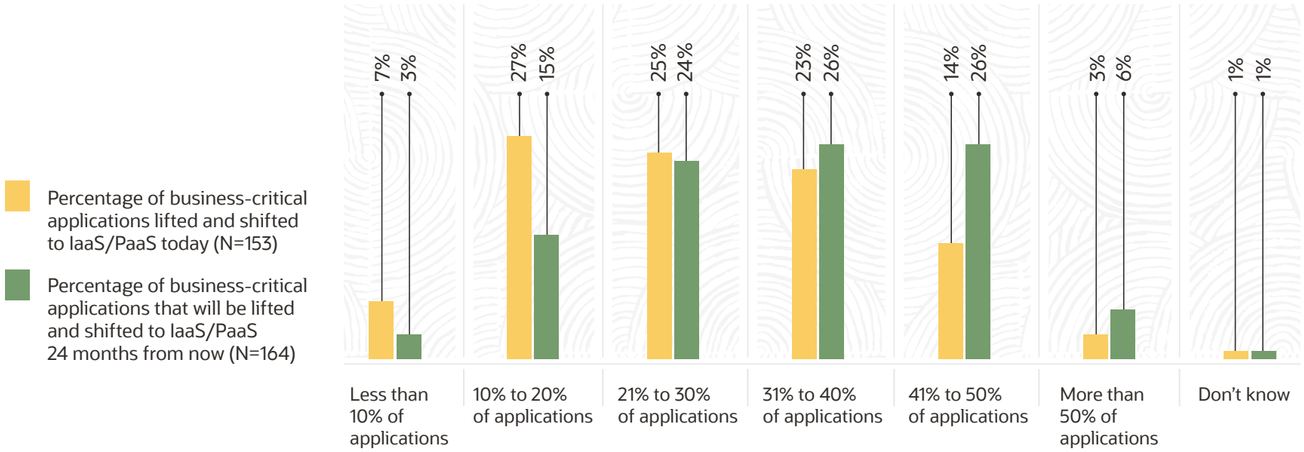
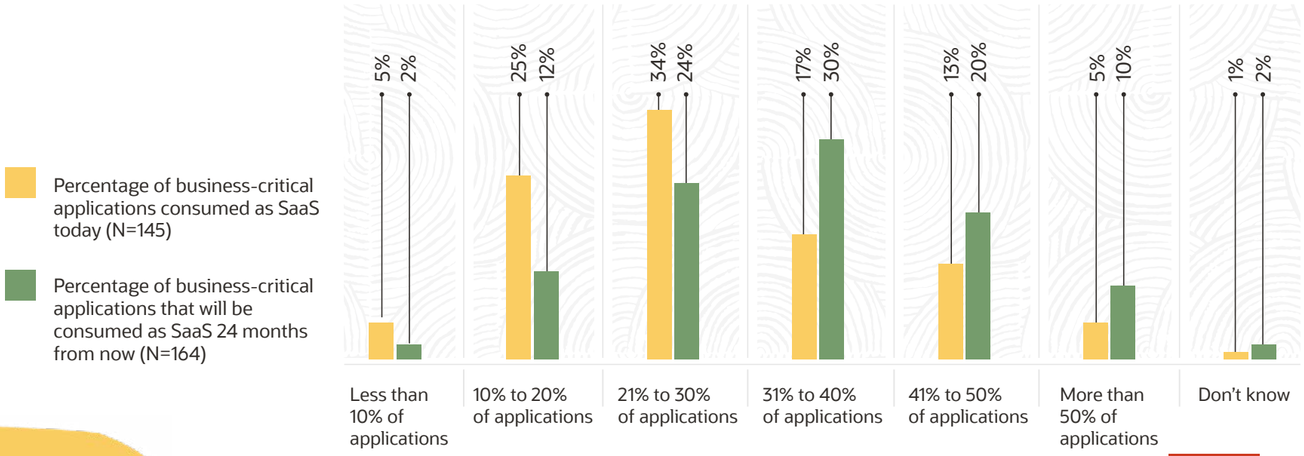


Figure 2.

Of all sanctioned business-critical applications used by your organization, approximately what percentage do you consume as SaaS? How do you expect this to change – if at all – over the next 24 months? (Percentage of respondents)

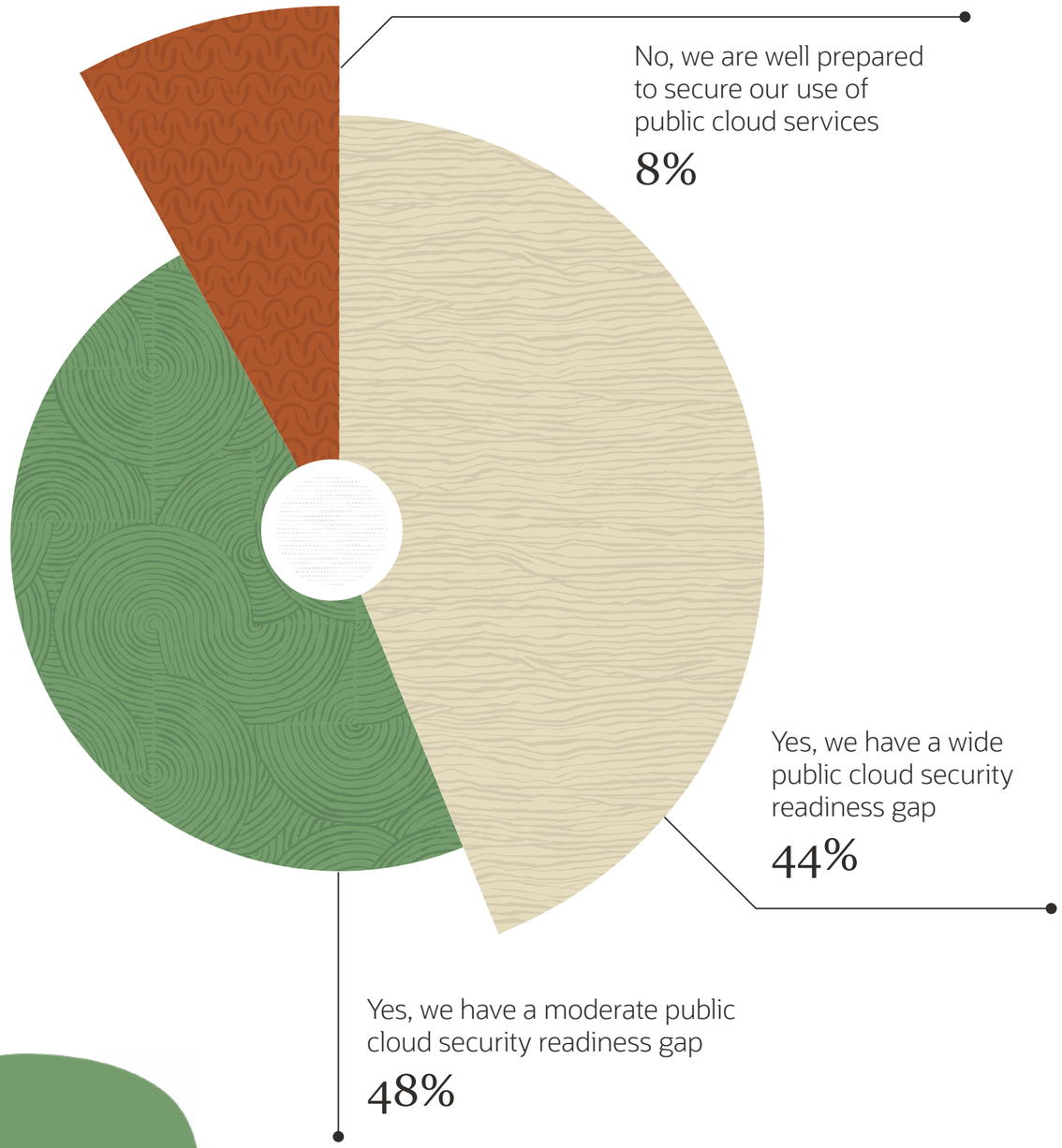


Cloud Security Challenges

Public cloud infrastructure opens a world of possibilities for DX as organizations take advantage of new technologies like containers, serverless computing, and hybrid architectures that have enabled a greater extend of scalability and portability of services. While these technologies can lead to business benefits, they may also introduce a multitude of new security concerns. Little wonder then why 92% of respondents indicated that their organization suffers from a cloud security readiness gap (see ***Figure 3***):

Figure 3

Do you feel your organization has a readiness gap created by its current cloud use and rate of expansion and the maturity of its cloud security program? (Percent of respondents, N=750)



The pervasive cloud security readiness gap is not a surprise as many organizations have numerous cloud security issues in areas like:

- **Application security.** Cloud native applications are loosely coupled and temporal, typically using microservices to facilitate scale up/scale down capabilities. Cloud-native applications also take advantage of things like containers, agile development, DevOps processes, and a continuous integration/continuous delivery (CI/CD) pipeline. From a security perspective, cloud-native applications introduce new tools, processes, and personas that are often immature and lacking the same level of security oversight as traditional applications. Furthermore, cloud infrastructure has freed organizations from "racking and stacking" servers, reducing cost and operations overhead and leading to greater application deployment velocity. This means that organizations have less oversight and control over cloud-native applications while developing more applications and increasing the attack surface. This leads to a cycle where cyber-risk continually increases—an unacceptable situation for any CISO.

- **Shadow IT**. Growth in SaaS options has given rise to business managers that may work around IT departments and choose their SaaS applications directly. Security teams may be blind to these SaaS-based business processes or lack the right levels of visibility into things like access policies and sensitive data flows. Obviously, cyber-risk escalates when the security team struggles to achieve full visibility across ALL applications and infrastructure.

- **Data security**. The amount of structured, semi-structured, and unstructured data that is flowing through cloud-based workloads, cloud storage repositories, and SaaS applications is dramatically increasing. It makes data discovery and classification increasingly difficult. And once the data migrates to the cloud, security teams are still obligated to create, enforce, and monitor access policies. These already arduous tasks can become extremely challenging when combined with the scale, scope, velocity, and variety associated with IaaS, PaaS, and SaaS options. Data security challenges like these are fairly prevalent – according to the Oracle and KPMG research, 30% of organizations have discovered "cloud secrets" like passwords, encryption keys, API keys, etc. on in source code libraries, cloud object stores, and stored on

cloud-based servers.

- **Identity and access management (IAM).** Cloud computing has led to massive identity sprawl at some organizations. This means too many identities – especially service accounts. Security teams find it difficult to understand who has cloud access, what privileges they have, and what they are doing. Cloud development can also involve open source software, source code management repositories, and open communication channels like Slack. The lack of structure makes identity monitoring and management especially cumbersome.

- **A shared responsibility security model.** Cloud computing introduces a shared security model with blurred lines of demarcation about what CSPs and customers are responsible for, depending largely on each CSP. Since many large organizations work with numerous IaaS, PaaS, and SaaS providers, each with its own shared responsibility model, this can become quite confusing. According to the Oracle and KPMG research, 54% of organizations find the SaaS shared responsibility model confusing, 47% find the IaaS shared responsibility model confusing, and 43% find the PaaS shared responsibility model confusing (see the Oracle and KPMG report, Demystifying the Cloud Security Shared Security Model). Without a clear understanding of shared responsibility security models for each cloud computing provider, organizations are susceptible to misconfigurations, software vulnerabilities, human error, and process redundancy.

As if these challenges weren't enough, cloud computing complicates threat detection and response processes as well. Cyber-attacks can exploit cloud-based assets like developer credentials to gain a foothold into hybrid IT infrastructure and move laterally from there. This is already happening – the Oracle and KPMG research reveals that 59% of respondents claim that a member of their organization with privileged cloud account access has been exploited by phishing attacks designed to steal credentials. Alternatively, hackers use phishing and social engineering tactics to compromise user endpoints, establish beachheads, steal administrator credentials, and move laterally toward sensitive data assets in SaaS applications and cloud-based workloads. CISOs will need cloud-based sensors for threat monitoring and new types of controls to block threats to and from the cloud.

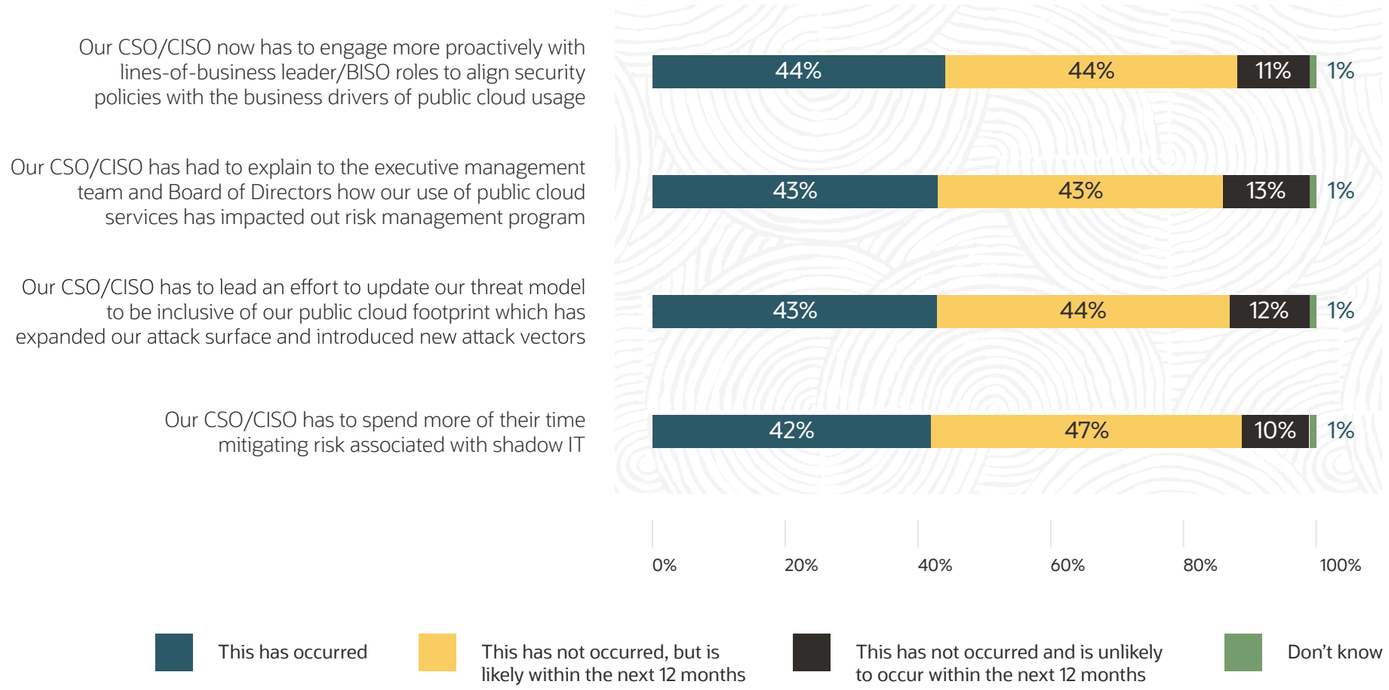
Cloud Computing Must Drive a New Model for Cybersecurity Leadership

The transition to cloud computing and DX represents a real change in direction for many CISOs who started their careers as cybersecurity technologists and climbed the corporate ladder. These security leaders have lots of experience with security technologies like firewalls, antivirus software, and IDS/IPS appliances but may be unfamiliar with things like the shared cloud security responsibility model as only 8% of cyber-leaders indicated they have confidence in this area. Worse yet, some technology focused CISOs are not prepared to manage new types of risks associated with DX initiatives and business processes.

The Oracle and KPMG research indicates that DX and cloud computing is impacting CISO activities. For example, 44% of organizations claim that the CISO/CSO had to get more involved with line of business managers to align security policies with cloud-based business drivers, 43% of CISOs/CSOs had to explain how public cloud services impact cyber-risk, 43% of CISOs/CSOs had to update their threat model to include the impact of cloud computing risks, and 42% of CISOs/CSOs spend more time mitigating shadow IT risks (see ***Figure 4***). It's also worth noting that a significant percentage of organizations believe that it's likely their CISO/CSO will have to do these things within the next 12 months.

Figure 4.

Which of the following impacts to the CISO/CSO role have occurred at your organization due to its use of public cloud services? (Percent of respondents, N=479)



Within a year, CISOs will find themselves spending more of their time on cloud security oversight. The question remains however: Are they up for this transition?

The Digital Transformation CISO

Transitioning to public cloud computing while supporting DX initiatives may simply be beyond the skill sets of many CISOs. The research seems to support this as 73% have hired or plan to hire a CISO with more cloud security experience. These executives will be called upon to drive cybersecurity into the corporate culture, integrate cybersecurity into DX initiatives, and embed strong cybersecurity within all aspects of IT technology – especially public cloud computing. ESG believes these responsibilities create the need for a new type of cybersecurity executive: The Digital Transformation CISO.

To be clear, the DX CISO is not just a new title, but rather a transformation to the CISO role and his or her relationship with the business. To ensure the right level of participation, organizations must change their reporting structures. DX should no longer report to CIOs as this relegates them to a technology role. Rather, DX CISOs should report directly to CEOs and be considered critical members of the executive team. Along with this new reporting structure, DX CISOs must:

- **Participate in business planning around new initiatives.** Many organizations bring the security team into DX projects well into the application testing phase of projects. This forces a "bolted on" security model where security testing and controls are added to applications and infrastructure after initial development. This introduces inefficiencies and operational overhead, not to mention the upfront exposure if services go live prior to the involvement of the CISO, thus creating a "pace gap". This pace-gap is best exemplified when the business unit moves at a more rapid pace with application deployments, than the rate of the security organization to incorporate into existing frameworks and compliance programs. As part of his or her role, DX CISOs must insist upon getting the security team involved in DX initiatives during early planning stages. For example, CISOs should insist upon data classification upfront so the security team can apply tight controls and continuous monitoring to sensitive data assets. Security teams can then create threat models and introduce the right controls that can be "baked" into applications, data security controls, and infrastructure provisioning during the development phase of projects. In this way, DX initiatives can be designed and built for strong security from their genesis and throughout their lifecycles.

- **Actively educate executives and directors about cyber-risk.** Executives and corporate boards make digital transformation decisions to pursue new opportunities to increase revenue while streamlining operations. What's often missing however is the right level of oversight around new types of cyber-risks or risk mitigation strategies. DX CISOs must take it upon themselves to educate the leadership team about new types of cyber-risks on a proactive basis. Before establishing a program to monitor patients remotely, health care executives must fully understand that IP-based monitoring systems can be hacked, disrupting devices, or compromising the integrity of their data. Knowing the risks, DX CISOs and business teams can identify the right controls for risk mitigation.

- **Monitor and report on changing cyber-risks in real-time.** Organizations need to be able to make business and cybersecurity decisions based upon changing risk factors like cyber-adversary tactics, techniques, and procedures (TTPs), discovered vulnerabilities, emergency patches, ongoing cyber-attacks, etc. When cyber-risk escalates, CISOs, business executives, and corporate directors should be able to review real-time data that can help them make decisions to manage risk while maintaining business operations.

- **Establish a cybersecurity culture within the organization.** Despite years of lip service, many organizations still treat cybersecurity as an IT-based necessary evil. DX CISOs must break through this wall and establish a cybersecurity culture within their organizations. Aside from working with executives on planning, DX CISO must collaborate with these managers to establish business policies that enable business agility while mitigating cyber-risk. DX CISOs should also push an aggressive cybersecurity training agenda. For example, software developers, IT operations, and security personnel need continuous training on cloud security and the shared security responsibility model so they can "bake" security into DX projects and day-to-day processes. Finally, DX CISOs must be seen as visible cheerleaders for cybersecurity within all business units, directly to employees, and within all business processes.

53%

of organizations now employ BISOs to help the CISO create a cybersecurity culture and get more involved with cloud-based DX projects. In this way, BISOs serve a positive role as change agent.

DX CISOs can't be expected to accomplish these goals alone – especially at large global organizations. The Oracle and KPMG research indicates that 53% of organizations now employ BISOs to help the CISO create a cybersecurity culture and get more involved with cloud-based DX projects. In this way, BISOs serve a positive role as change agent.

The DX CISO's Changing Role with Security Technology

While DX CISOs are more business than technology executives, they still own the responsibility of selecting, deploying, and operating the right security controls that enable the business while addressing cyber-risk. This should include:

- **Focusing on visibility.** DX initiatives can be extensive in scope as they may include hybrid deployments of applications accessed by geographically distributed remote employees and third parties. Strong security depends upon end-to-end visibility with no blind spots supported by stream processing of data for real-time analytics. In this way, DX CISOs can work with business executives to evaluate security defense effectiveness while measuring ROI on security and mitigate risk.

- **Advancing a cloud security skill set.** Security teams must become experts on the nuances of cloud computing so they can apply the right controls in the right places. This means understanding the shared security responsibility model as it applies to each IaaS, PaaS, and SaaS provider used by the organization. This knowledge should help organizations take advantage of native CSP security controls as part of a comprehensive cloud security program. Large organizations with aggressive DX initiatives may want to hire or train cloud security architects as part of a larger cloud center of excellence agenda.

- **Leveraging DevSecOps automation.** To fully "bake" security into the cloud, DX CISO should integrate security with DevOps as part of establishing a cybersecurity culture. This effort should contain a software development lifecycle (SDLC) including interactive development environments (IDEs), folding security into source code management (SCM) repositories, integrating security tools into automated build tools and agile development project management systems, and providing security support for collaborative messaging platforms. To standardize this process, DX CISOs should insist on the consensus assessment initiative questionnaire (CAIQ) from the cloud security alliance (CSA), an industry-accepted, fully transparent way to document what security controls exist in IaaS, PaaS, and SaaS services. These and other public cloud computing best practices can help DX CISOs "shift left, embedding security into software development and deployment as standard operating procedures.

Security teams must become experts on the nuances of cloud computing so they can apply the right controls in the right places

- **Establishing and enforce policies for least privilege.** While least privilege policies should apply to all user access, DX CISOs should start by locking down privileged accounts. This means assessing all cloud accounts and SCM repositories to understand who is accessing these and what they are doing. This will help the security team establish the right rules for administrator access and entitlements using controls like zero-trust network access and privileged account management systems. As part of this process, DX CISOs must perform the same type of assessment on SaaS accounts – especially those controlled by business units. This assessment should lead to the right SaaS security controls and monitoring systems to safeguard sensitive data in flight and at rest on SaaS applications.

- **Rationalizing and integrate the security stack.** Security technologies grew organically over many years with new controls deployed as countermeasures for emerging risks. Unfortunately, this ad-hoc strategy has resulted in an army of disconnected point tools and operational overhead. DX CISOs must do all they can to rationalize this portfolio and transform it into a tightly integrated scalable security stack. This requires a high-performance data pipeline for stream and batch data processing, API integration between tools, threat intelligence ingestion for data enrichment, and process automation for immediate incident response and risk mitigation.

Measuring the DX CISO

As organizations embrace DX applications, IoT devices, and 5G networks, they will need DX CISOs more than ever. How should business leaders measure DX CISO success? ESG believes CEOs and corporate boards should focus on metrics like:

- **Cyber-risk management.** DX CISOs have visibility across IT assets and third-party connections including within all IaaS, PaaS, and SaaS providers. Changing risk factors like cyber-attacks and software vulnerabilities are identified in real-time while urgent changes are immediately reviewed with executives and corporate boards ASAP. Risk mitigation decisions are data driven and measured for effectiveness. Risk measurement and mitigation decisions are closely tied to the business.

- **Security efficacy**. Organization deploys ubiquitous security controls across the hybrid infrastructure for threat prevention. Controls are continuously updated and tuned based upon threat intelligence analysis of the tactics, techniques, and procedures (TTPs) used in cyber-attack campaigns (i.e. Ransomware, phishing, etc.) aimed at specific industries. The security operations team has visibility across the hybrid infrastructure and uses correlation rules, heuristics, and machine learning algorithms for threat detection. Formal processes are in place for incident response that includes business, IT, and security people and processes. Continuous improvement in mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR). Increasing use of automation for security operations and incident response that can be measured by employee productivity gains like increasing numbers of investigations per analyst.

- **Operational efficiency**. Organization embraces artificial intelligence and machine learning to gain measurable results in staff capacity and productivity. DevSecOps processes are integrated into DevOps, embedding security into cloud development and deployment. This should result in fewer security vulnerabilities in homegrown software, faster bug fixes, and stronger risk mitigation and security as part of CI/CD pipeline automation.

- **Business enablement.** This is the true objective of DX CISOs. Strong results should include faster application on-boarding times, more effective access policies, granular entitlements and governance, and greater application uptime as well as increased capabilities in meeting regulatory compliance goals. In aggregate, DX CISOs should be able to help accelerate business operations and user productivity while minimizing cyber-risks.

- **Compliance and governance.** Regulations are constantly changing – especially as they relate to data privacy (i.e. GDPR, CCPA, etc.). In this changing regulatory landscape, CISOs are often called upon to work side-by-side with chief privacy officers (CPOs) and legal teams to operationalize data governance policies. Doing this effectively demands detailed planning and a strong working relationship between the DX CISO and line of business managers to discover and classify sensitive data, create data usage policies, enforce policies with strong identity and data security controls, and then monitor compliance at all time. In this way, DX DISOs and business managers can unleash DX business processes while managing cyber-risk.

The Bigger Truth

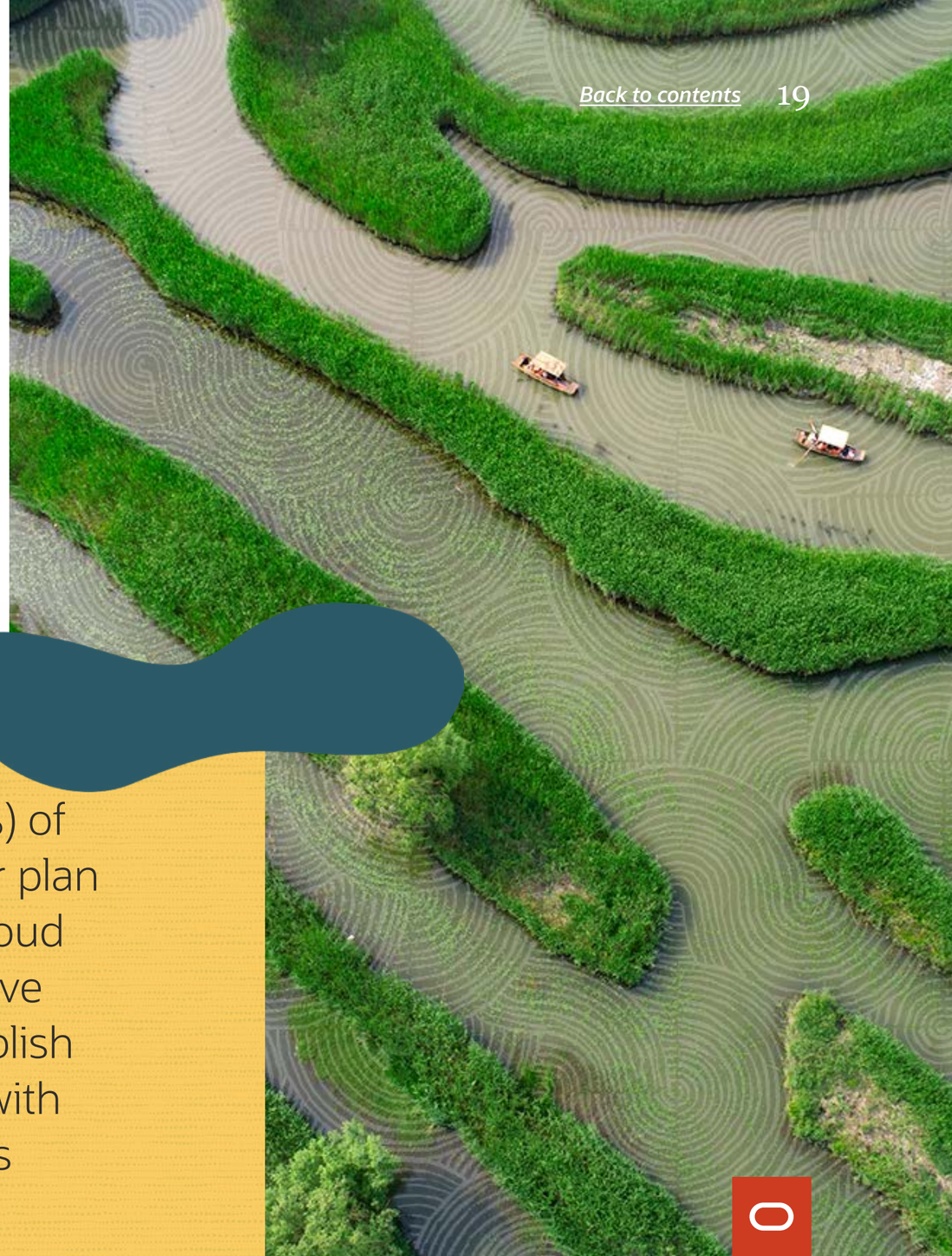
For enterprise organizations, cybersecurity is at a crossroads. Point tools and manual processes were already overwhelming the cybersecurity staff, but as organizations moved workloads to the public cloud, developed cloud-native applications, and embraced multi-cloud SaaS/PaaS/IaaS, legacy security models moved from ineffective to obsolete.

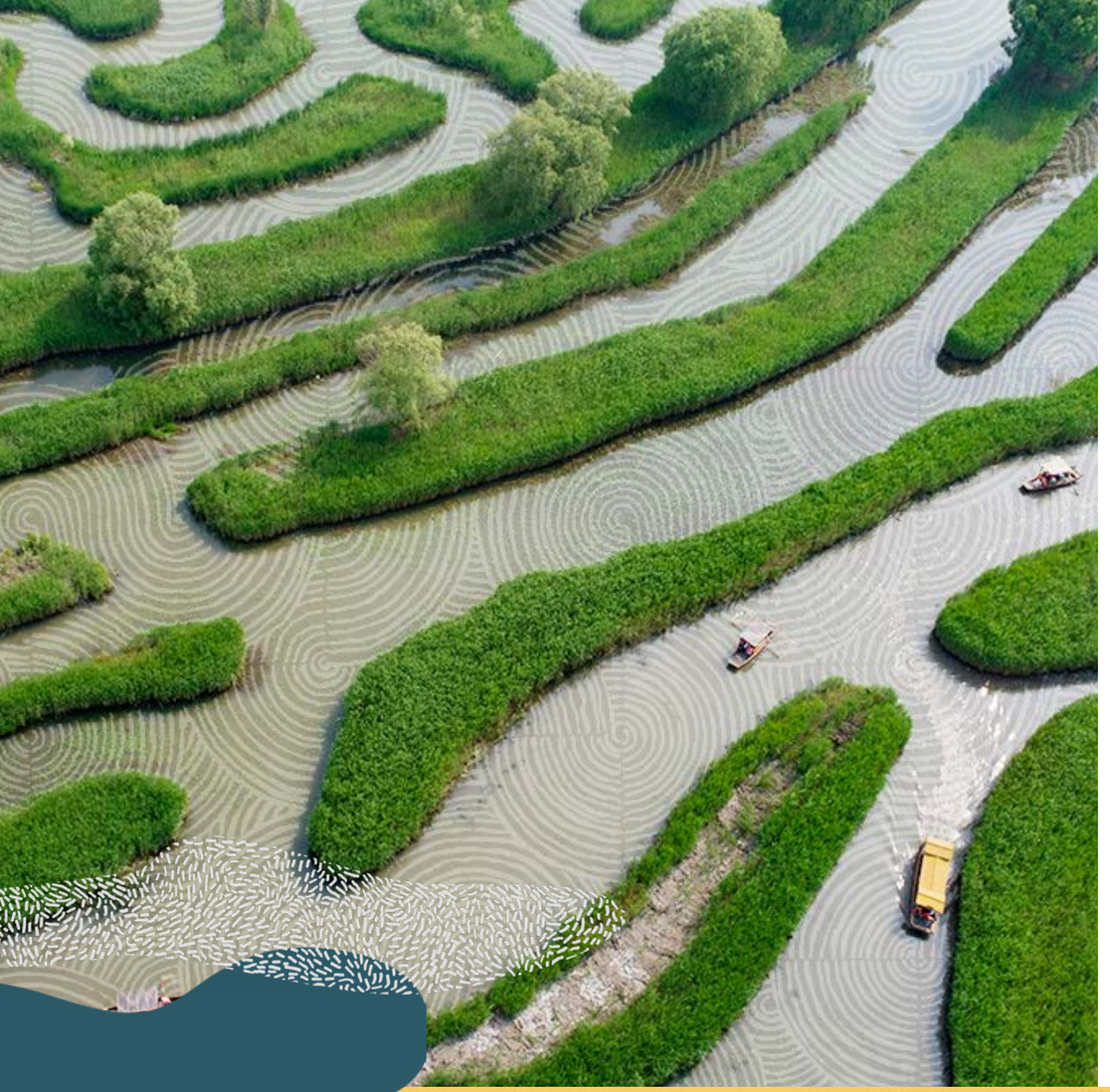
Beyond security people, processes, and technologies, many security executives also hit a wall. Technically focused CISOs were no match for the velocity and volume of digital transformation initiatives built using public cloud infrastructure, while business minded CISOs lacked the skills to drive the right processes, technology controls, and program oversight into burgeoning cloud security architectures.

This report built using data collected for the Oracle and KPMG Cloud Threat Report, illustrates the scope of the problem and offers a solutions path. Nearly three-quarters (73%) of organizations have hired or plan to hire a CISO with more cloud security skills while 53% have established or plan to establish BISOs to work collectively with CISOs and lines-of-business, and then embed cybersecurity into business processes and corporate culture.

As DX CISOs join organizations, they will be asked to drive a series of transformational changes. To succeed, DX CISOs must create a cybersecurity culture across the organization while pushing a cybersecurity agenda to organizational executives, corporate boards, and line-of-business managers. The goal? Align cybersecurity and DX objectives for business enablement and risk management. Meanwhile, line of business managers must fully participate by championing cybersecurity, cooperating with DX CISOs on policy creation around roles and data classification, and bring security into all business planning activities as early as possible.

Nearly three-quarters (73%) of organizations have hired or plan to hire a CISO with more cloud security skills while 53% have established or plan to establish BISOs to work collectively with CISOs and lines of business





DX CISOs will also have their hands full transforming security technology programs as well. It's critical that they integrate security with agile development, DevOps, and automated CI/CD pipelines. Furthermore, they must get their teams to fully understand the cloud shared security responsibility model, and then build a synergistic hybrid security model that covers all aspects of IT infrastructure. Finally, DX CISOs must work with the business to create and enforce the right policies for least privilege that can lockdown accounts, manage privileged users, and safeguard sensitive data.

For many years, CISOs had to accept the fact that the business didn't want good security, it wanted good enough security. Thus, firms viewed security in terms of regulatory compliance requirements only. The transition to cloud computing and digital transformation marks an end to this cybersecurity myopia. DX CISO's jobs won't be easy, but as organizations adopt cloud computing for digital transformation, their success becomes critically important. Visionary DX CISOs won't just propose these initiatives, they will champion their cause, guiding and leading the organization through the transition.

Individuals with DX CISO skills will be in high demand and should receive full support from executives and corporate boards. Those that can drive their organizations through this transformation will not only be successful but will also be viewed as heroes.

Those that can drive their organizations through this transformation will not only be successful but will also be viewed as heroes.

ORACLE KPMG

Research conducted in partnership with ESG