ORACLE

The Mission of the Cloud-Centric CISO

Uncovering the Cyberleader Priorities and Challenges from the Oracle and KPMG Cloud Threat Report

Defining an Evolving Role

Organizations are increasingly reliant on IT systems to store, process, and analyze information. As we shift more of these resources from the data center to the public cloud, there is an ever-increasing reliance on making sure this information remains secure, with effective risk-mitigation programs.

Over the years, the role of securing this information has shifted from Chief Information Officer (CIO) to the Chief Information Security Officer (CISO). This single point of ownership has relieved many of the day-to-day burdens on the CIO and placed responsibility security in the hands of one executive. It has also created a real challenge for those in the CISO role, because those executives must ensure overall data availability, privacy, and security.

Organizations that are finding success in the GDPR era have realized that security and risk are shared responsibilities among the C-suite. Proof of this is the adoption of Chief Privacy Officers (CPOs) and Chief Data-Protection Officers (CDOs), who provide far more focused mandates around protecting the increasing amounts of data and ensuring compliance. The entire C-suite plays a vital role in the overall success and security of the business.

This focus in security across the C-suite allows CISOs to play a more critical role in enablement—and not just "prevention." At the end of the day, the CISO's job is to manage risk for customers, partners, and the organization itself, and to do this in a way that enables the business to succeed.

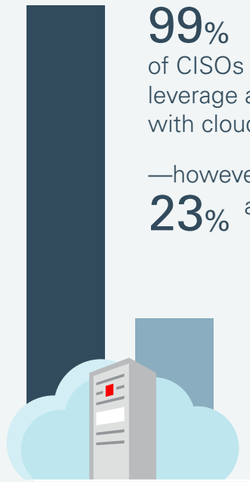
This enablement starts with the CISO having a seat at the table for all lines of business looking to adopt new services, data, users, or infrastructure. It is a red flag when the lines of business fail to engage the CISO in the initial planning discussions.

This highly strategic role that the CISO plays is critical in today's information-forward competitive environment, where cyberthreats are everywhere, where enterprises are breached daily, and where compliance is mandatory. The CISO is a key player critical to the success of these business initiatives. However, despite the best of intentions and planning often lead to challenges of communication and effective partnering with the very team that can ensure their success.

Let's see the research.

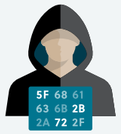
Realities of the CISO

Cloud Infrastructure



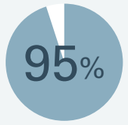
99%
of CISOs find it important/critical to leverage a web application firewall with cloud services

—however, only
23% actually do

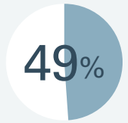


The top concern for CISOs and governments is **attacks/hacking by foreign governments** (Security in Age of AI)

1 in 10 organizations can see **75%** or more of their **security event telemetry**



of CISOs cite that the cloud is **"as secure"** as or **"more secure"** than their own data centers



of CISOs are focused on **leveraging cloud-infrastructure** security controls to **monitor** cloud-resident workloads

Data Management

38%
of CISOs find their **#1 challenge** is **maintaining secure cloud configurations**

48% have **delayed patching** due to impacts on **service level agreements (SLAs)**

#1
reason for **increased risk** to the organization is **"human error"**

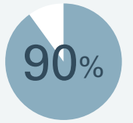
Nearly half (49%)
of all respondents expect to store the **majority of their data in a public cloud by 2020**

48%
of CISOs are **planning to deploy** automated patch management, starting with the **database environment**

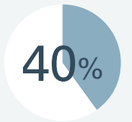
SaaS Applications

71%
of organizations are **relying on the cloud** for storing business-critical data

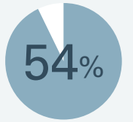
A notable **69%** of respondents stated that **more of the cloud services** they use are **business-critical compared** with **12 months** prior



90% of **CISOs do not fully understand** their team's role in the **shared responsibility security model**



40% of **CISOs** are challenged with **detecting** and **reacting** to security incidents in the cloud



54% are dealing with **rogue cloud-app usage** and 54% of CISOs state that this is **leading to the introduction of malware**

The CISO Shift into Business Enablement

of organizations report a lack of alignment between IT operations and security operations.

> Disparity between CISOs and CIOs is troublesome as it indicates a lack of visibility and transparency between leaders.
>
> *Greg Jensen, Oracle*

The effective CISO is an enabler. All too often, the CISO is seen as laser-focused on prevention versus enablement; a roadblock to corporate ambitions and departmental goals. To be effective, the CISO should not be seen as an executive who says, "No, you can't." Rather, the CISO should be known for saying, "Yes, you can, and here's how to do it safely."

The stressful CISO job allows little tolerance of failure. When a breach occurs, and especially if data is exfiltrated, the CISO's head will roll—perhaps along with the CIO's. This has contributed to the alternate definition of CISO as "Crisis-Induced Sacrificial Offering." More than ever, this responsibility must be shared across the C-suite to ensure success.

The savvy CISO must be an agent of change. Unlike traditional risk-averse IT staff, the effective CISO is always looking for a better way to reduce risk, respond to threats, and meet compliance targets while supporting the growth of the business.

The diplomatic CISO must bridge the ITOps, SecOps and DevSecOps gap. That's the gap between IT operations (who solve information-management problems), security operations (who reduce risk, protect data, and enable compliance) and DevSecOps (who bridge the gap between exposure and remediation efforts). Dysfunction between these teams creates gaps and opportunities that can be exploited by adversaries.

The forward-thinking CISO focuses on priorities and planning. This enterprise role is essential in helping business leaders map out a secure way to achieve business goals, while also reducing risk and enabling compliance.

Key Tasks for the Effective CISO

- Understand the business to become a trusted adviser for all security, risk, privacy, compliance, and data-integrity needs
- Develop risk-avoidance strategies against fraud, data loss, and threats
- Implement information security for employees, customers, partners, data, applications, and infrastructure
- Develop detection, response, remediation, and notification programs for new and emerging threats
- Ensure teams are following the Shared Responsibility Security Model for cloud services and service providers
- Assist in vetting all third-party providers who might have access to corporate information, especially sensitive data
- Work with regulatory oversight teams to define and implement processes and technology to help meet compliance targets
- Own corporate security standards, policies, and tech stack
- Define and manage vulnerability, configuration and patch-response program with IT and DevSecOps teams

Incident Prevention, Detection, Response, and Recovery

92% of CISOs are worried about data loss or breaches due to shadow IT, including unsanctioned or improper use of cloud services in violation of established security policies.

> Effective leadership is required to lower risk of an incident, and to mitigate impacts of an attack.
>
> *Laurent Gil, Oracle*

Every CISO would undoubtedly prefer to focus on proactive incident prevention rather than reactive incident detection. However, organizations are at risk of an attack 24/7, which means urgent detection and response often outweigh preventative measures.

Keys to successfully protecting the enterprise are critical patching and configuration management of cloud services, data center, infrastructure and the edge. This includes end-point systems, mobile devices, servers and the Internet of Things (IoT).

Yet 48% of organizational CIOs report their administrators are unable to patch on time because of downtime impacting service level agreements (SLA) or software incompatibility. In addition, 51% of IT teams have had to delay other projects due to patching priorities.

The good news: 89% of CISOs have indicated they currently employ or plan to employ automated patch-management solutions, with the database being the first environment to manage.

More good news: Machine learning and behavior analytics are enabling organizations to more effectively identify how corporate data may be at risk with noncompliant or misconfigured cloud services.

Indeed, machine learning with advanced automation has made tremendous strides in recent years in helping organizations identify points of risk and automate the remediation or risk-mitigation processes.

This capability helps ITOps, SecOps and DevSecOps teams to be more involved in strategic planning, rather than doing the reactive firefighting they deal with today.

The Human Risk Factors

53% of organizations report a shortage of cybersecurity skills in their ITOps and SecOps organizations

> You cannot recruit, train, and retain enough qualified people for SecOps. We cannot hire our way out of this issue and must look to technology and automation to address the cybersecurity challenges organizations face.

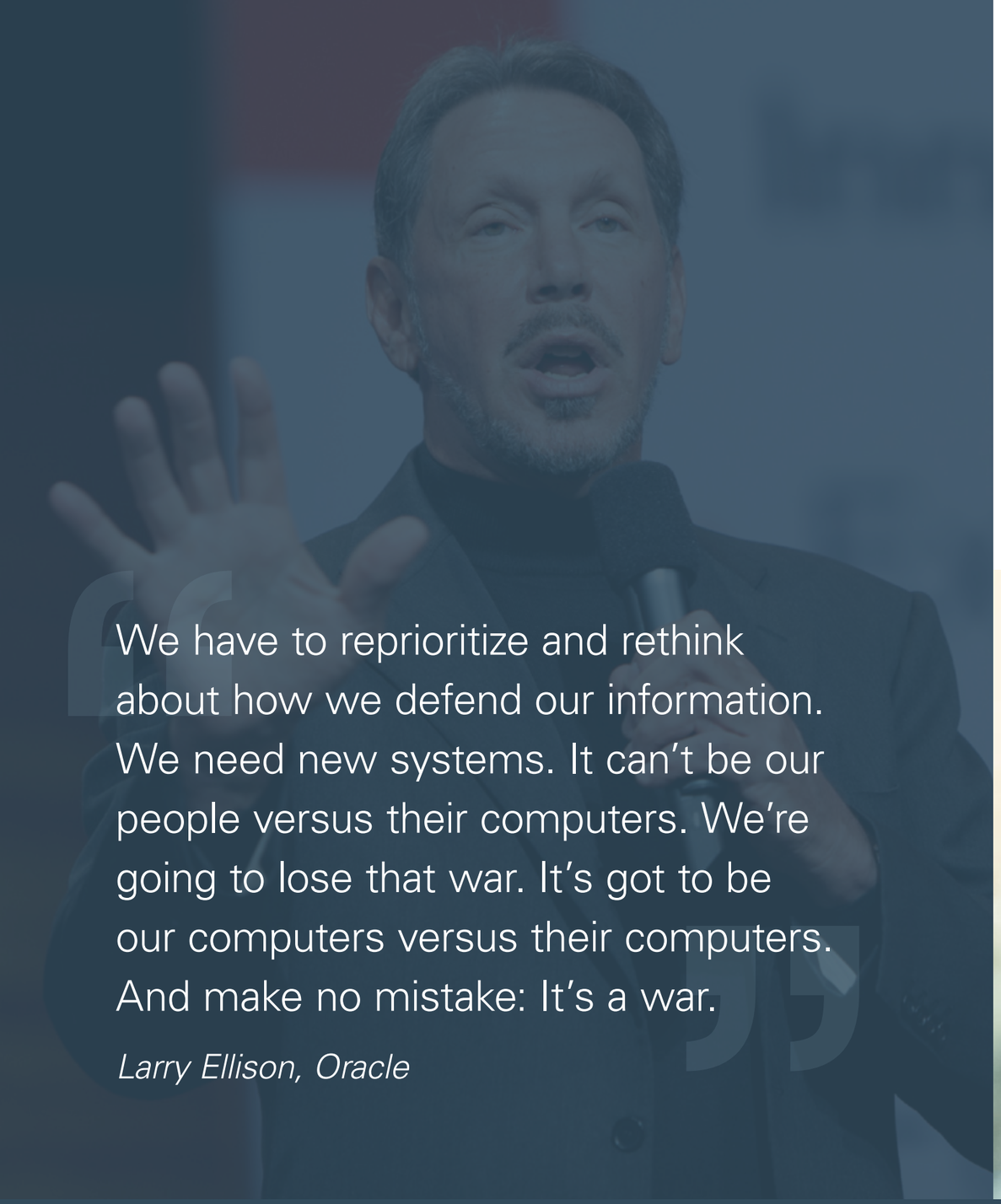
Fred Kost, Oracle

Today's businesses face a persistent shortage in qualified staff for the ITOps and SecOps teams, and the problem is getting worse. There are more services to secure, more users to train, more systems to patch, and more events to handle. A large number of megabreaches can be traced back to misconfigured cloud services as the result of human error or a lack of tools and processes to help identify and manage risk.

A key cause of the overload is too much data, particularly event-driven data, such as in log files and real-time alerts. Humans simply can't analyze and respond to that much information in a timely fashion—or at all. Current staffing lacks the ability, time, and knowledge to analyze the flow of events, proactively plan and monitor for misconfigurations, and address the overwhelming challenges.

Complications: Public-cloud infrastructure and platforms, as well as mission-critical SaaS solutions, contain a wealth of event-driven information to help identify potential fraud and data loss. All the security event telemetry must be collected, correlated with on-premises events, and analyzed for signs of anomalous behaviors.

In organizations, this, together with the impact of human error, is leading to the leaking of sensitive business data on these misconfigured cloud services. These types of data breaches are highly preventable, yet are often missed when staff overlook their responsibilities in managing access and configurations.



> We have to reprioritize and rethink about how we defend our information. We need new systems. It can't be our people versus their computers. We're going to lose that war. It's got to be our computers versus their computers. And make no mistake: It's a war.
>
> *Larry Ellison, Oracle*

Fortunately, automation removes the excessive event noise and repetitive tasks, and allows security practitioners to be enablers of new strategic initiatives.

Meanwhile, artificial intelligence, specifically machine learning and deep learning, identifies patterns that can rapidly discern variations and anomalies by correlating hundreds (or thousands) of disparate logs and information feeds.

With this, today's CISOs are now armed the tools necessary for identifying high-risk configurations, behaviors, and responses. In the war against cybercrime and insider threats, CISOs in the best organizations will have increased visibility into the areas that need it.

Opportunities for the CISO

of CISOs say that the top cybersecurity challenge is detecting and reacting to security incidents in the cloud.

> Defense-in-depth is cybersecurity best practice, but implementation can be challenging. Success requires access to comprehensive layered defense that's easy to use and embed into processes for safeguarding cloud workloads.
>
> *Johnnie Konstantas, Oracle*

The cloud is not magic: Whether it's software as a service or infrastructure as a service, the cloud represents servers, databases, networking infrastructure, applications, identity platforms, encryption methodologies, and entitlements, all working together to ensure regulatory compliance goals are met. Responsibility for secure cloud applications and cloud data is shared between the cloud service provider and its business customers.

CISOs often face an uphill battle explaining the Shared Responsibility Security Model (SRSM) for cloud computing to other C-level executives, ITOps teams, and line-of-business managers. That's a battle that must be fought, and won, as more departments shift workloads to the cloud, and unfortunately, sometimes leverage unsanctioned services in order to get there.

Whether it's the use of unvetted suppliers or unauthorized use of approved services, the cloud is simultaneously a security challenge for the CISO and an opportunity for the organization: 93% of CISOs report encountering rogue cloud-application usage in their organizations.

The CISO's top concerns don't end there, of course. General email phishing and targeted spearphishing are on the increase, and can be effective, even with end-user training and email security tools to gain a foothold into sensitive network and data resources. SecOps teams must be eternally vigilant.

SecOps must also ensure that ITOps stay current to limit exposure of zero-day threats, by patching software (and hardware) at every level of the stack, from the operating system to the network switch, from open-source libraries to mobile apps.

Another challenge: keeping pace at scale. Most organizations monitor only a small fraction of their security event data, providing an opportunity for malware and malicious actors to gain a foothold. As the number of devices and applications multiply, CISOs and SecOps will continue to see challenges in identifying and responding to these threats without new cloud-centric strategies.

It's a war. Cyberattackers are increasingly likely to employ AI, using deep learning and machine learning algorithms to extend the sophistication and capabilities of malware and targeted attacks, making it more important than ever to ensure CISOs are focused on fighting fire with fire.

Oracle has a well-established reputation for securing business-critical data and services. Security is part of the DNA of every Oracle offering, and extends into the key design principles and capabilities of Oracle Cloud Infrastructure (OCI). OCI delivers a highly scalable, secure and high-performance environment for the ever-increasing business-critical workloads, and every CISO and CIO should find value in it for decreasing risk and exposure to threats.

ORACLE

Contributors

Alan Zeichick,
Senior Technology Writer, Oracle

Greg Jensen,
Senior Director of Cloud Security, Oracle

To learn more about Oracle security and how security and IT leaders can get the most out of their cloud strategy, follow us at:

Or visit us at: **www.oracle.com/security**

To learn more, read the Oracle and KPMG Cloud Threat Report, which highlights the security gaps being exposed in the shift to business-critical cloud services, and suggests leading practices for CISOs and SecOps teams.