CIO | EXCHANGE

5 considerations for establishing cyber resiliency

CIO Exchange Brief

This CIO Exchange Brief is the first in a series that summarizes key discussion points in Oracle's CIO Exchange events. In these virtual events, hosted by Oracle CIO Jae Evans, global IT leaders and peers discuss the latest topics with thought leaders.

In September 2021, our CIO Exchange covered the topic of cyber resiliency, and this brief covers the key takeaways from the event.

1. Understand the importance of data security in your operation
2. Assess strengths and weaknesses in cybersecurity strategy
3. Leverage cloud technology to gain deeper visibility into security
4. Aggregate workloads in the cloud to improve defense against threats
5. Take a customer-centric approach to privacy and security

Cyberattacks occurred every **11** seconds

According to Cybersecurity Ventures[1], cyberattacks were estimated to occur, on average, every 11 seconds in 2021, costing roughly US$6 trillion in damages globally.

Global cybercrime is predicted to cost **10.5** trillion USD

By 2025, global cybercrime is predicted to cost US$10.5 trillion annually. [2]To stay ahead of the increasing number of cyberattacks, organizations should consider the role of cyber resiliency in their security strategy.

[1] Cybersecurity Ventures, "Top 5 Cybersecurity Facts, Figures, Predictions, And Statistics For 2020 To 2021"

[2] Oracle, "Leading the war on cyber"

1 Understand the importance of data security in your operation

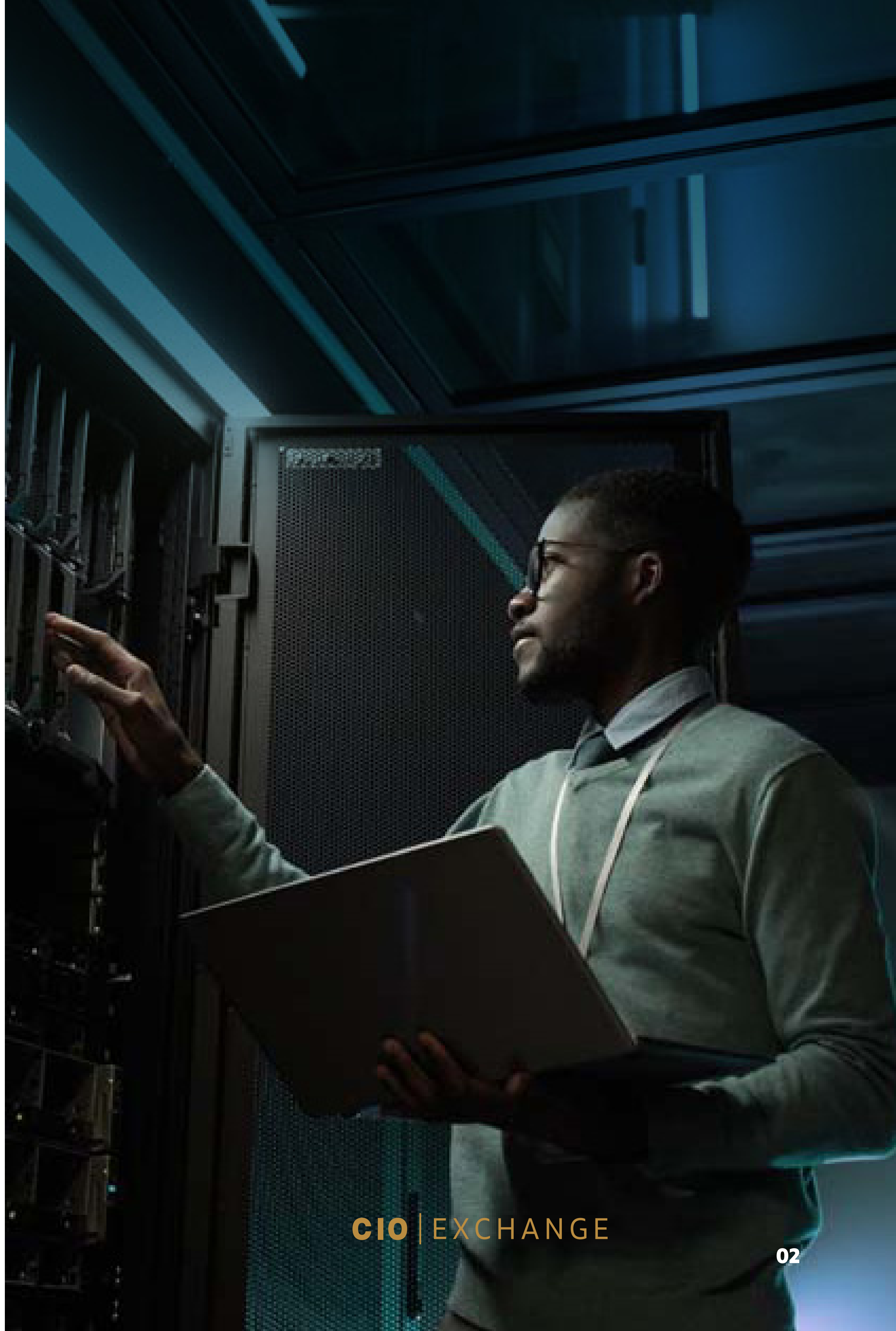
Any organization—no matter where it's located—is vulnerable to cyberattacks. Developing a security strategy is an important step toward ensuring that data is protected in the event of a cyberattack. And as cyberattacks become more sophisticated, ongoing innovation is needed to develop security technologies that help protect against them.

Response plans, self-defense plans, cyber awareness training, and cyber hygiene are listed as baseline measures of cyber defense by Deloitte. According to results from a Deloitte survey, only 9% of respondents had implemented all four measures. 53% of respondents have a fully implemented self-defense plan, and less than half have fully implemented response plans, cyber hygiene practices, or regular cyber awareness training[3].

In an increasingly virtual world, companies are now in a position where they need to defend themselves against advanced threats. And as more companies continue to transition to remote work, cyberattacks such as phishing and ransomware are increasing at unprecedented rates.

Research from Ponemon shows that phishing attacks were the second-most common and expensive data breach attacks in 2021[4].

[3] Cybersecurity Ventures, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025"
[4] Deloitte, "Financial Cyber Survey May 2021"



2 Assess strengths and weaknesses in cybersecurity strategy

As more information becomes digital, organizations need to take stock of how digital inventory and systems are secured.

When beginning to evaluate cybersecurity strategy, these questions provide a helpful place to start:

- ☑ **Where are we vulnerable?**
- ☑ **How are our vendors securing their software?**
- ☑ **How secure are our on-premises facilities?**
- ☑ **Are we implementing authentication, compartmentalization, and zero trust?**
- ☑ **Are employees trained on phishing attacks and other cybersecurity threats?**

For municipalities and other public agencies, the role of private-sector partnerships in security strategies should also be evaluated. As cyber-attack methods continue to evolve and advance, more attacks are taking place on municipalities and other public agencies. By working together with expert cloud providers who can help automate security at scale, public agencies can accelerate deterrence against attacks, create long-term resiliency, and invest in the best technology for the future.

3

Leverage cloud technology to gain deeper visibility into security

Analysis shows that the victims who are paying ransomware costs are almost 80% more likely to be hit again, often by the same group. Of the companies hit by ransomware attacks, more than 66% report a dramatic and significant revenue loss[5].

A key strategy in cybersecurity involves using behavior analysis to gain control of—and visibility into—training, partnerships, and threat detection. With this information, organizations can detect activity around threats, helping unify cloud security and get ahead of data breaches and ransomware attacks. To gain this visibility, some companies hire researchers to analyze the behavior of cybercriminals. While many large organizations spend enormous amounts of resources on IT and security, hiring, retaining, and building a security team to do this work is often cost prohibitive and inefficient.

> "Concentrating the world's most important data in a cloud like Oracle Cloud means that we can spend huge amounts [of resources] securing that data, amortized over tens of thousands of customers. And from a basic economic view...cloud makes tremendous sense in terms of security."
>
> **– Edward Screven, Oracle's chief corporate architect**

As cyber threats have become more apparent to business leaders, companies are starting to think about the cloud and security differently.

[5] UpGuard, "What is the cost of a data breach in 2021"

3 Leverage cloud technology to gain deeper visibility into security

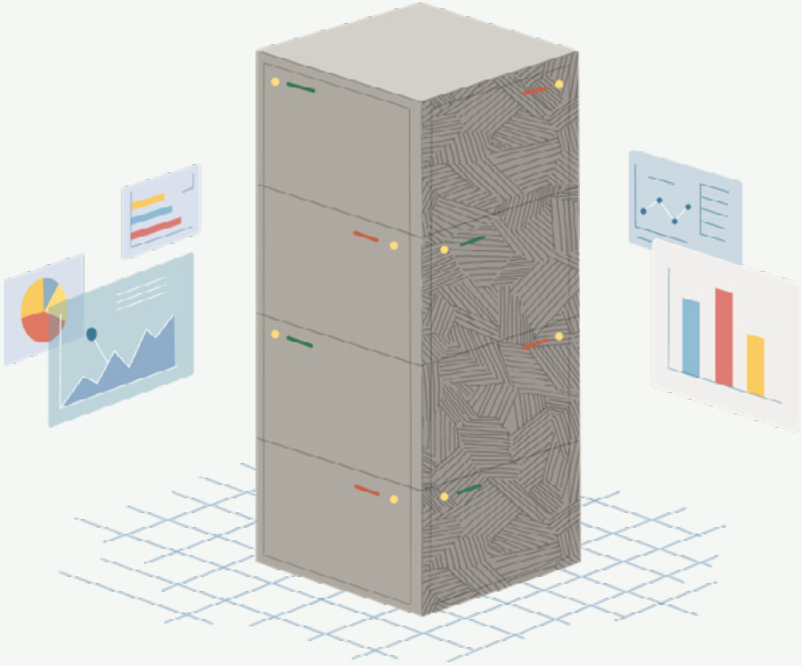
Attackers have become more sophisticated with attacks that are more automated and scalable, often resulting in multiple attacks on different places happening all at once. Cloud service providers (CSPs) can invest more resources in security than most individual organizations, ultimately providing more advanced, affordable technology that can be used to secure multiple customers. With the built-in security features offered by CSPs such as Oracle, organizations can spend less on security because they can benefit from the investments that CSPs are already making.

Tanium, a cybersecurity leader trusted by some the world's largest and most sophisticated organizations, provides a good example of the efficiencies that the cloud can provide. By using Oracle Cloud Infrastructure, Tanium gains built-in security, high availability, and proven price-performance for its endpoint management and security product, Tanium as a Service (TaaS). This ultimately helps them reach a broader set of customers.

> "With Oracle, we can expand our customer base to help small enterprises and the midsize take control of their endpoints by offering a competitively priced solution with zero infrastructure."

– Orion Hindawi, Tanium's cofounder and CEO.

TaaS customers benefit from Oracle Cloud Infrastructure's sophisticated AI and ML capabilities to automatically respond to cyberattacks, in concert with Tanium's real-time data, visibility, and control.



CIO | EXCHANGE

4

Aggregate workloads in the cloud to improve defense

Even with the increasing sophistication and frequency of cyberattacks, the cybersecurity battle is winnable. Organizations can strengthen their security posture through cloud services such as data and analytics to evaluate data risks and monitor activity. This improves cyber resiliency and better equips organizations to predict and respond to attacks.

While on-premises facilities have been considered highly secure, many organizations are starting to think differently. In fact, 75% of organizations now see public clouds as more secure than on-premises systems. By taking advantage of the security services that are built into public cloud infrastructure, businesses who build their applications on the cloud can leverage built-in security features without having to spend their own resources to create them.

They can also benefit from the aggregated data made available by the cloud that provides insights about attacker behavior and helps organizations proactively prepare for attacks.

Despite the inherent security benefits, managing workloads in the cloud can create complexity. Automation can help address this challenge head-on by helping to automate provisioning and configuration, encryption, patching and updating, scaling, and performance tuning. With Oracle's autonomous services, organizations can reduce risk introduced by manual processes and save time on labor from managing cloud-scale data.

75% of organizations now see public clouds as more secure than on-premises systems

5 Take a customer-centric approach to privacy and security

Cyberattacks are a threat that companies can no longer ignore. And with digital transformation occurring across every industry, data breaches and cyber resilience are now top of mind, presenting interesting opportunities for innovation.

PayPal—one of the world's largest payment processors, with over [900 billion transactions](#) processed in 2020 alone—is taking a customer-centric approach to security. They see cybersecurity as a commitment to customers, with every process in the company designed for privacy and security. Sri Shivananda, executive vice president and CTO of PayPal, says that a company's relationship with customers should be based on a foundation of trust. And one of the most important aspects of that trust is safety.

PayPal—one of the world's largest payment processors, with over **900** Billion transactions processed in 2020

> "In the past, most of us would think of disaster recovery as maybe being the pinnacle of technology resilience, but now that is being replaced by cyber resilience."
>
> **– Sri Shivananda, EVP and CTO of PayPal**

Now move forward, fast

A myth in the technology industry is that secure is not fast. But it is possible to execute security experiences that are delightful for the customer and are fast at the same time. This can be achieved with a platform-centric mindset. By creating common security platforms that can be leveraged companywide, organizations can quickly create products and experiences that delight customers and are built on solid security foundations.

When a security strategy is defined and implemented across the organization, businesses are enabled to do their best work. Oracle's security-first approach helps protect our customers' data with the highest levels of security across infrastructure, applications, and users, allowing them to focus more on innovation.

> "I've had the opportunity to meet with various other technology leaders and hear their thoughts and insights on protecting their customers and their own environments from cyber threats.
>
> We all agree on the importance of security and maintaining the confidentiality, integrity, and availability of data and services to our employees, partners, consumers, and customers."
>
> **– Jae Evans, CIO, Oracle**

Get started with Oracle Cloud Security

oracle.com/security

Learn more about our CIO Exchange events

oracle.com/events/cio-exchange

ORACLE