ORACLE KPMG

The Business Impacts of the Modern Data Breach

Oracle and KPMG Cloud Threat Report 2020 series

Volume 4

Research conducted in partnership with ESG

Contents

Executive Summary

Welcome to the fourth installment of the Cloud Threat Report series. The previous reports, The Oracle and KPMG Cloud Threat Report 2020, Demystifying the Cloud Security Shared Responsibility Model and Addressing Cyber Risk and Fraud in the Cloud highlighted the need for a cultural shift in security to close the cloud readiness gap and outlined how confusion over where provider responsibility for security ends and customer responsibility begins have impacted cloud security. But what happens when the readiness gap and confusion lead to a data breach?

While security has often been among the top concerns when adopting cloud services, it does not seem to have deterred many organizations from expanding their cloud footprint. The fact of the matter is that cloud adoption continues to move forward, with or without the input of the cybersecurity team. Even the threat of potential data loss will not prevent this. Thus, the security organization must embrace the shift to cloud and adapt culturally by engaging collaboratively with the business and modifying their tools and processes as necessary to better fit the decentralized model of cloud to help adopt effective incident response practices.

With this in mind, we wanted to understand the impacts resulting from the reliance on manual configuration management in today's dynamic cloud environments; the limited use of controls at the data layer; the lack of pervasive usage monitoring to prevent masquerading, misuse, and malicious insider activities; and ultimately, the consequences when the aforementioned issues lead to data loss. As such, the objective of this report is to highlight the frequency, causes, and business impacts of the modern data breach by exploring the following research findings:

- **Data breaches are on the rise, further raising the profile of cybersecurity.**

  Nearly 9 in 10 organizations (88%) reported public cloud data loss in the past year, and the increasing frequency of high-profile attacks has elevated cybersecurity to a board-level conversation. However, on an industry-wide basis, that executive-level focus has yet to significantly improve the situation.

- **Privilege abuse, misconfigurations, and poor visibility are among the leading causes of data loss**

  More than 35% of organizations reported experiencing at least one of these issues. Thus, despite the increased focus on cybersecurity overall, foundational practices such as encryption, access control, data masking, redacting, auditing, and enforcing separation of duties often remain overlooked and flawed, especially in cloud environments.

- **The impacts of a data breach can include both financial and human elements.**

  Most organizations (56%) report that as a result of public cloud data loss, they invested in additional cybersecurity technologies and services. However, the negative outcomes from a data breach, can include financial elements such as lost revenue, brand damage, career impacts for key personnel and reduced shareholder value.

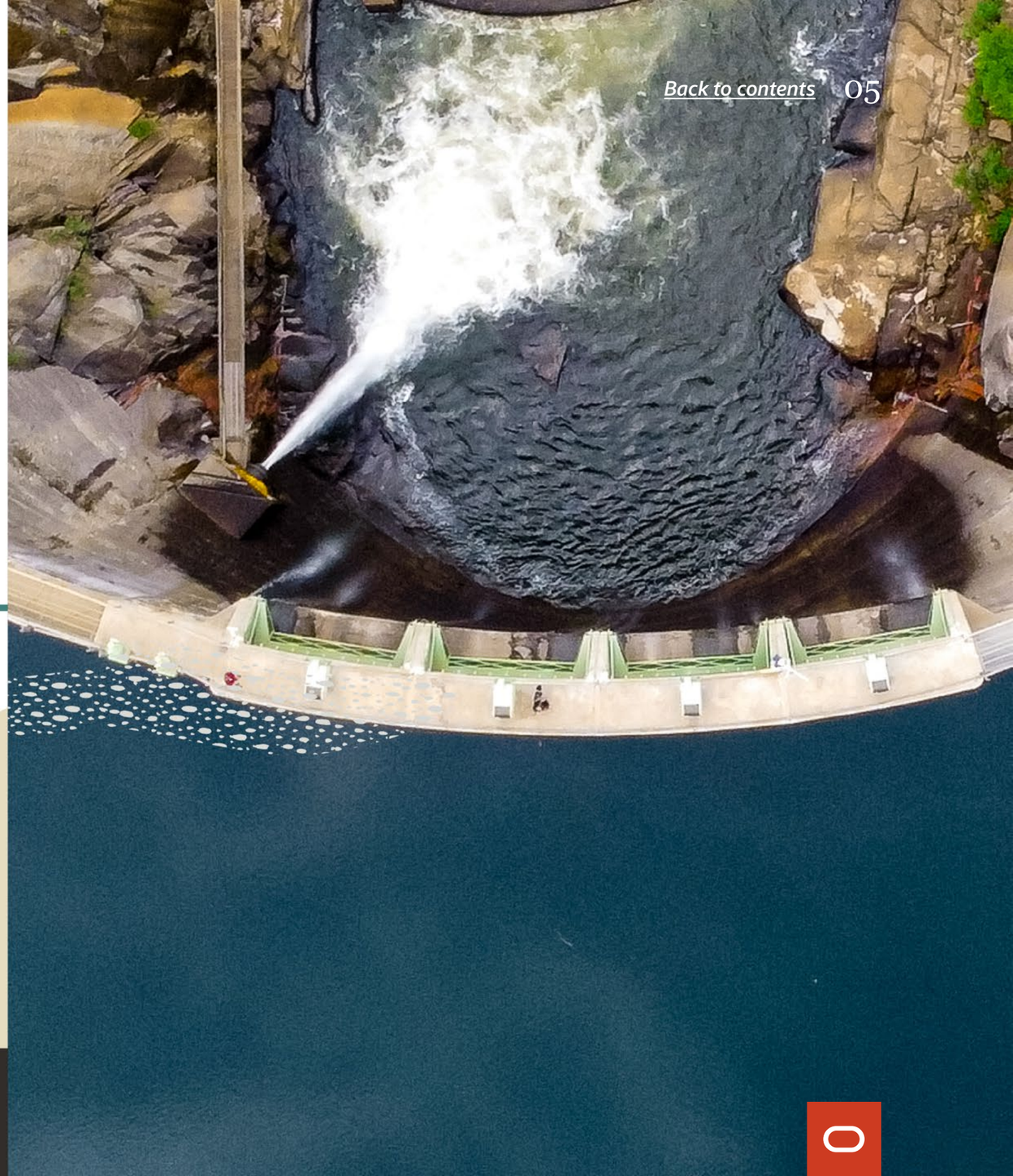
- **Improvements across data controls, visibility, and identity via automation are needed to fortify cybersecurity programs.**

  More than half of organizations (51%) said they experienced data loss as a direct result of the misconfiguration of cloud services. While there is no surefire way to guarantee avoidance of a data breach, improving configuration and patch management processes, data classification, identity and access management, and overall visibility into data access and usage are good starting points.

Data Breaches Are on the Rise, Further Raising the Profile of Cybersecurity

Data Breaches Are on the Rise, Further Raising the Profile of Cybersecurity

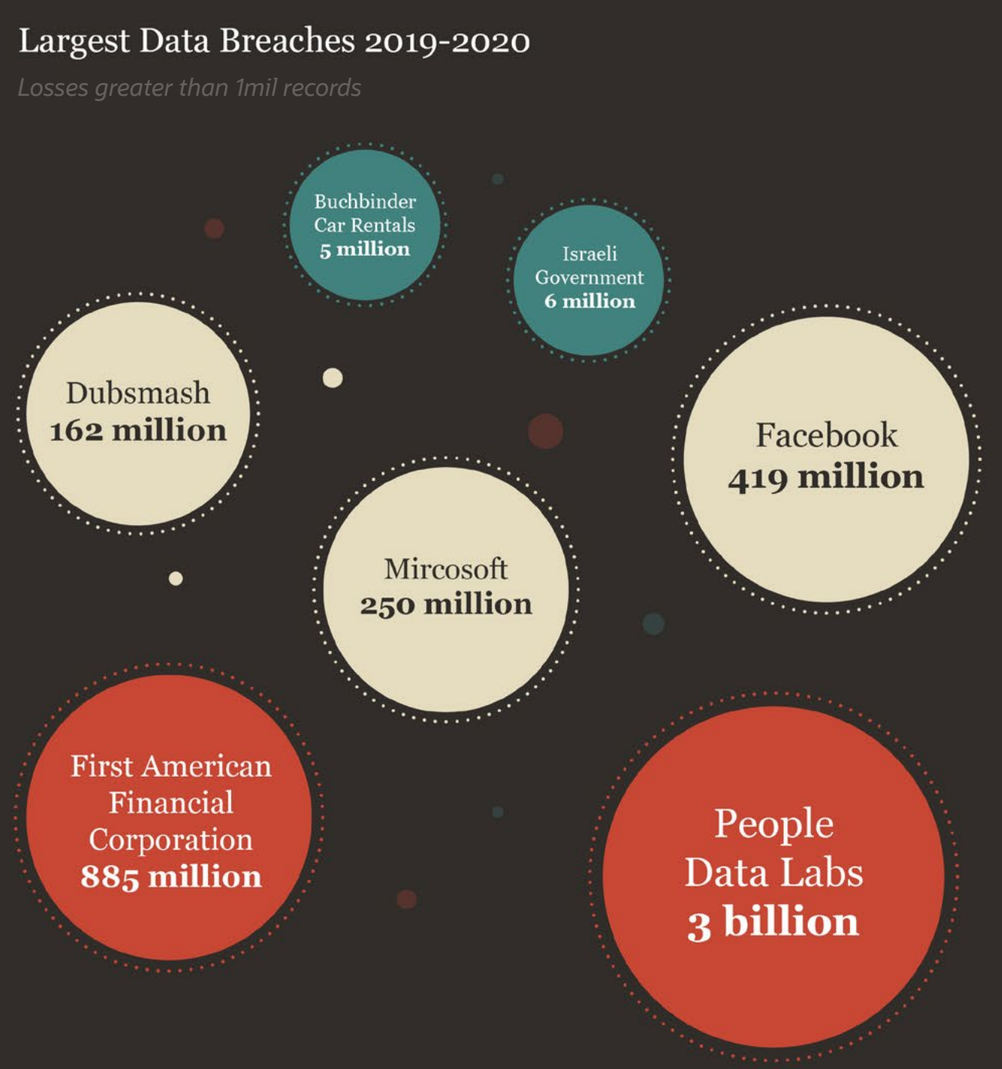
When big-box retailers were subjected to mega-breaches in 2013, part of the reason it garnered so much attention was that at the time, breaches of that scale and scope were far from an everyday occurrence. Fast forward just seven years and, based solely on the number of records lost, those initial examples no longer make the cut for the top ten largest breaches of the decade. This is not to minimize the importance or impact of these early events, but rather to highlight the new scale at which attackers operate. One of the lasting outcomes of these early mega-breaches was the heightened involvement in cybersecurity at the executive and board level. While this is still very much an ongoing transition, there has been some progress in getting the CISO a seat at the executive table.



However, this is not to say that the situation has improved. In just the last 18 months, there have been at least 12 incidents in which 10 million or more records were allegedly compromised. But the more jarring fact is that many of the breaches we continue to see highlighted across the media landscape are not the result of sophisticated attacks, but rather poor security. Some of these large-scale breaches due most directly to unforced errors include:[1]

- **1.2 billion records,** including names, email addresses, phone numbers, and social media profile information, were allegedly exposed due to an unsecured server that required no password for data access.
- **885 million records,** including account numbers, social security numbers, driver's license images, mortgage information, and more, were apparently exposed due to an insecure direct object reference error on a financial institution's website.
- **420 million records,** including social media user IDs and phone numbers, were claimed to have been exposed when several unprotected third-party databases were discovered online.
- **275 million records,** including the names, dates of birth, email addresses, phone numbers, and salaries of Indian citizens, were allegedly exposed when a database was left unsecured and its data accessible on the internet for a two-week period.
- **250 million records** of technical support conversations, which included customer email addresses, locations, case numbers, and more, were reported exposed when several servers were left unsecured and accessible without any authentication mechanisms.

To reiterate, these are not necessarily the largest or most impactful recent breaches overall. Rather, these five breaches, totaling 3 billion exposed customer records, are representative of alleged data exposure caused specifically by misconfigurations, improper permissions, or other poor security practices.

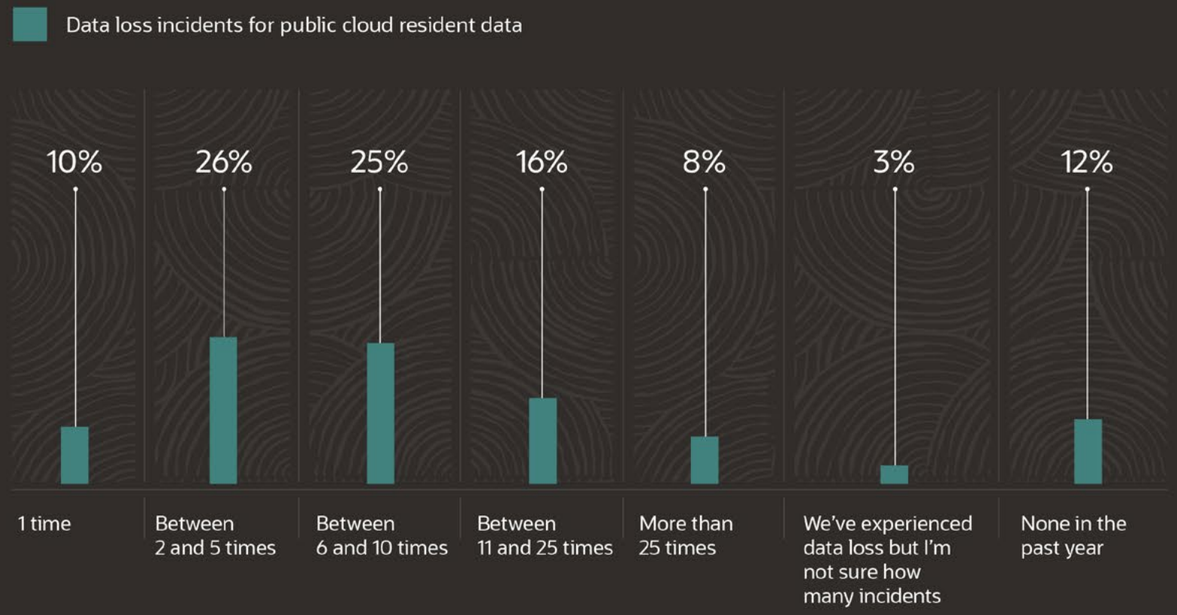


1 informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

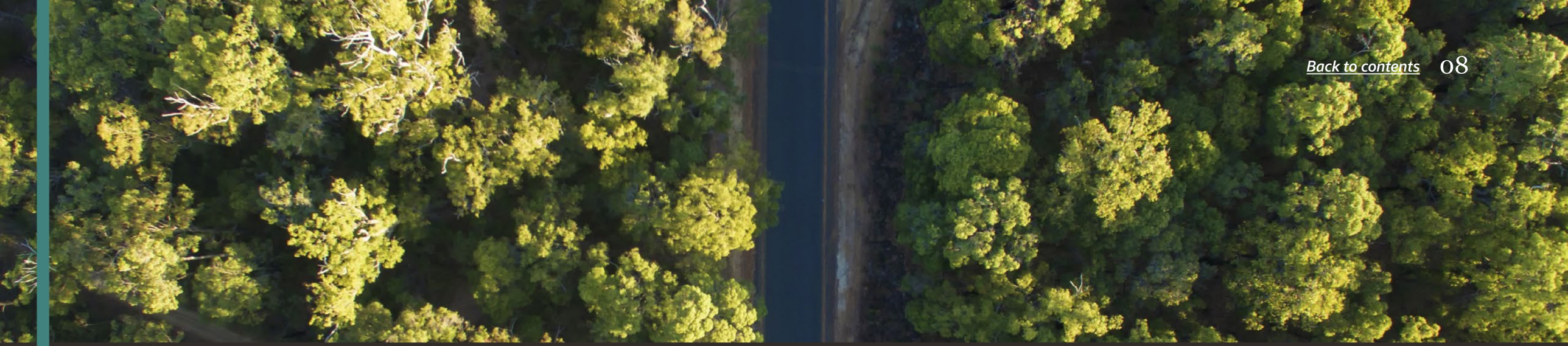
Troubling Rates of Cloud Data Loss Across All Organizations

The importance of this trend becomes clearer when viewed through the lens of the amount of data that is being shifted to the cloud. Overall, the amount of our respondents' organizational data in the cloud is expected to rise from a mean of 36% currently to 50% within the next 12-24 months. But more importantly, a significant portion of this data is sensitive, with 89% of our research respondents indicating that at least half their cloud-resident data is sensitive.

Putting aside the high-profile, claims of breaches, how often are our respondents experiencing incidents involving data loss each year? Unfortunately, much too frequently. In total, 88% of our research respondents said they experienced public cloud-resident data loss in the past year. The vast majority indicated it happened on more than one occasion. In fact, on average, our respondents reported 9 incidents of public cloud-resident data loss over the last 12 months. However, as we'll explore throughout this report, many of these incidents can be traced back to "unforced errors." That is to say, rather than being caused by nation-state actors or sophisticated adversaries, many incidents of data loss are the result of ineffective management and insufficient controls; specifically, not directly addressing the fundamental nature of cloud, which is different from on-premises infrastructure.



Question text: Approximately how many times has your organization experienced data loss in the past year specifically related to its public cloud-resident data? How many times has your organization experienced on-premises data loss? (Percent of respondents, N=750)



Privilege Abuse, Misconfigurations, and Poor Visibility Are Among the Leading Causes of Data Loss

Privilege Abuse, Misconfigurations, and Poor Visibility Are Among the Leading Causes of Data Loss

Ransomware, advanced persistent threats, targeted attacks, and zero-day exploits often dominate the headlines, garnering the lion's share of attention in the cybersecurity industry. Our previous report, The **Oracle and KPMG Cloud Threat Report 2020**, provided a view of the overall attack landscape with a focus on some of these types of attacks, including cyber business fraud and business email compromise. The focus is with good reason, as these types of attacks were reported by 40% and 39% of our research respondents, respectively.

However, the reality is that most organizations face a much broader range of attacks on an ongoing basis. Many of these attacks rely not just on sophisticated malware or the exploitation of undetected vulnerabilities, but rather the fact that we still struggle as an industry to address the basics, a fact borne out in our research. Specifically, many organizations reported attacks focused on exploiting known vulnerabilities, misconfigurations, and insufficient identity controls:

- The misuse of a privileged account by an inside employee (44%). While there is always the risk of motivated, correctly privileged users exploiting their access for malicious reasons, the proper implementation of a least-privilege model can prevent these individuals from taking advantage of broad access and more "curious" insiders from inadvertently accessing sensitive information.

- Exploits that take advantage of known vulnerabilities (40%). The fact that the exploitation of known vulnerabilities is the second most common type of attack cited by our respondents highlights the importance of identifying and addressing these issues as foundational DevSecOps dev-time and build-time use cases.

- The misuse of a privileged account via stolen credentials (38%). These types of identity-focused attacks, whether utilizing stolen credentials or credentials garnered through stuffing attacks, will become even more disruptive as the traditional perimeter dissolves and an identity-centric approach is adopted.

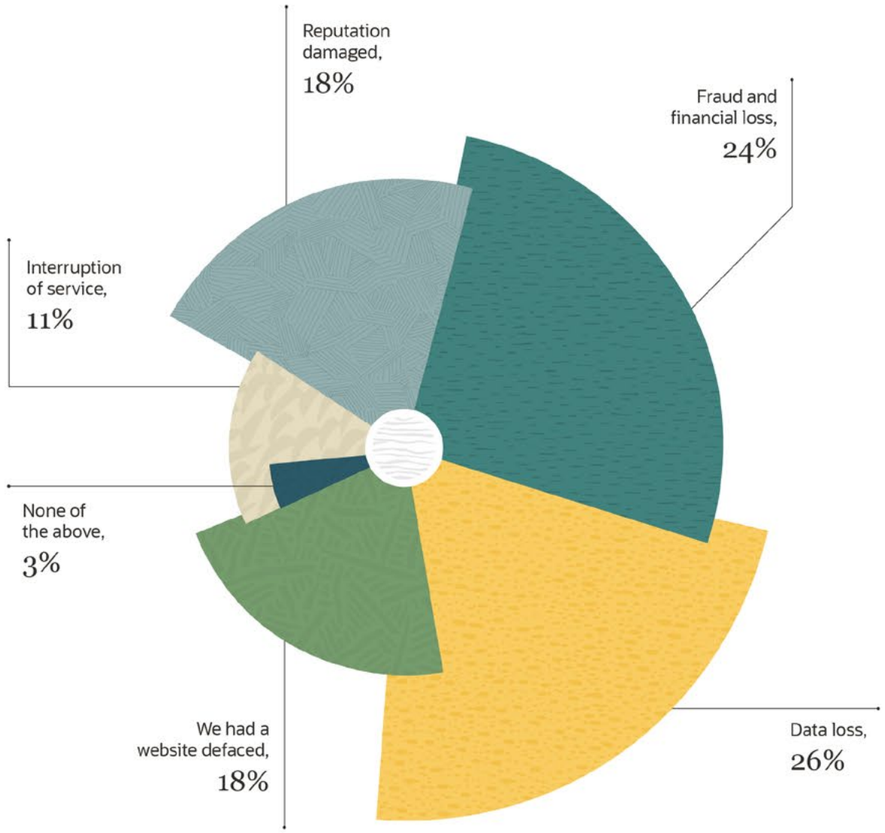
- Misconfigured systems that led to a successful compromise by a bad actor (36%). Cloud adoption has exacerbated the challenges associated with configuration management and maintenance of a secure baseline, and attackers have taken notice.

Privileged Cloud Credentials Are Used for a Variety of Adversarial Objectives

It should come as no surprise that privileged accounts (including those with administrative rights, or root or database access) and service accounts represent attractive targets to malicious actors. Attackers may get lucky by compromising an over-privileged account or an account that has direct access to high value data, whether privileged or not. Alternatively, attacks may focus on non-production or lower value data targets in the hope that less robust security controls and monitoring are in place, providing a beachhead from which to perform reconnaissance and plan lateral movement to higher value targets.

As highlighted in our first report in this series, The **Oracle and KPMG Cloud Threat Report 2020**, less than half of our research respondents report using multi-factor authentication and authorization for access to cloud management consoles, DevOps orchestration tools, and the administrative accounts of SaaS applications. This fact becomes important when you consider that 59% of our respondents reported that holders of privileged cloud accounts were compromised by a spear-phishing attack designed to steal their cloud credentials.

With a minimum amount of research on social media to identify potential targets based on employer, job title, and other basic information, attackers can potentially compromise an account with elevated privileges and quickly gain administrative access to systems with sensitive or business-critical data. Unsurprisingly, half of our respondents reported data loss and fraud or financial loss as the main outcomes from these types of attacks.



Question text: Which of the following outcomes has your organization experienced due to successful spear-phishing attacks that resulted in stolen privileged cloud credentials? (Percent of respondents, N=140)

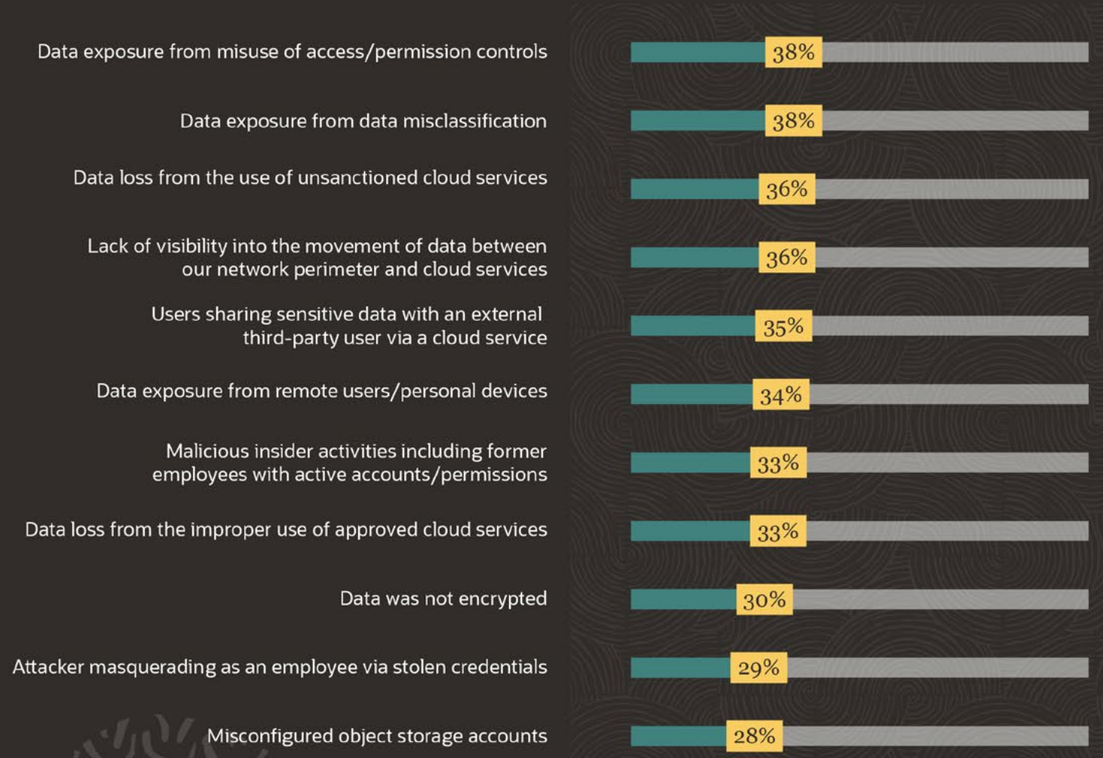
Automation and Visibility Must Improve to Prevent Data Loss

Unfortunately, there is no guaranteed approach to prevent data loss. But even understanding that a breach has occurred has become more difficult. The decentralization of IT caused by the adoption of cloud services has created a need for security information to be more broadly available, especially to cloud service administrators. The responsibility for protecting data no longer resides solely within the security operations center (SOC), but must be taken up across the organization. This idea was introduced in The **Oracle and KPMG Cloud Threat Report 2020**—using culture as the catalyst to close the cloud readiness gap.

One facet of this is making security a point of enablement across the DevOps lifecycle to help ensure cloud service administrators have visibility into misconfigurations and potential abuse of the services they are responsible for. In fact, over half of our respondents (51%) said they discovered data loss as a direct result of the misconfiguration of cloud services. To incorporate with DevOps and properly address cloud services, this must include automation. Half of our research respondents indicate they test and sign -off on patches before applying them to a production system. In a dynamic, cloud environment, this approach becomes unsustainable and adds time where the organization is out of compliance, and more importantly, insecure. The good news is that there is awareness of this issue—88% of our respondents agree that within the next three years, the majority of cloud-resident services will utilize intelligent and autonomous patching.

Lastly, visibility over data movement and user access of data that includes accurate data classification has become essential given the distributed nature of corporate resources and the wide range of locations in which sensitive data now resides.

Question text: Which of the following most often contributed to your organization's public cloud-related data loss? (Percent of respondents, N=661, five responses accepted)



The Impacts of a Data Breach Can Include Both Financial and Human Elements

The Impacts of a Data Breach Can Include Both Financial and Human Elements

One example of a high-profile incident involving data loss was the 2019 breach of Capital One. In that case, an external individual exploited a configuration vulnerability and accessed the personal information of approximately 100 million individuals in the United States and 6 million in Canada who had applied for, or were customers of, Capital One credit cards. Most of the data that was stolen consisted of names, addresses, phone numbers, email addresses, and similar information. However, 120,000 social security numbers, 80,000 linked bank account numbers, and 1 million Canadian Social Insurance Numbers were compromised as part of the incident.[2]

The breach was discovered nearly four months after it occurred, and only through the reporting of an external security researcher.[3] All told, the incident has so far cost Capital One $72 million in incremental expenses, though nearly half of that was offset by cyber insurance recoveries.[2] Additionally, Capital One has been named in 72 consumer class action cases across the US and Canada. Among other lessons learned, this is a good example of why data protection controls need to reside as close to the data as possible and travel with the data when copies are made. In this case, tokenization of such sensitive data could have helped to mitigate an ultimately catastrophic result.

Despite the focus on highly public incidents, the number of data breaches that do not make headlines, or at least the type of headlines the Capital One example did, continue to rise as well. Given the increasing prevalence of these types of incidents, we wanted to further explore the impacts from an incident involving data loss across all types of businesses.

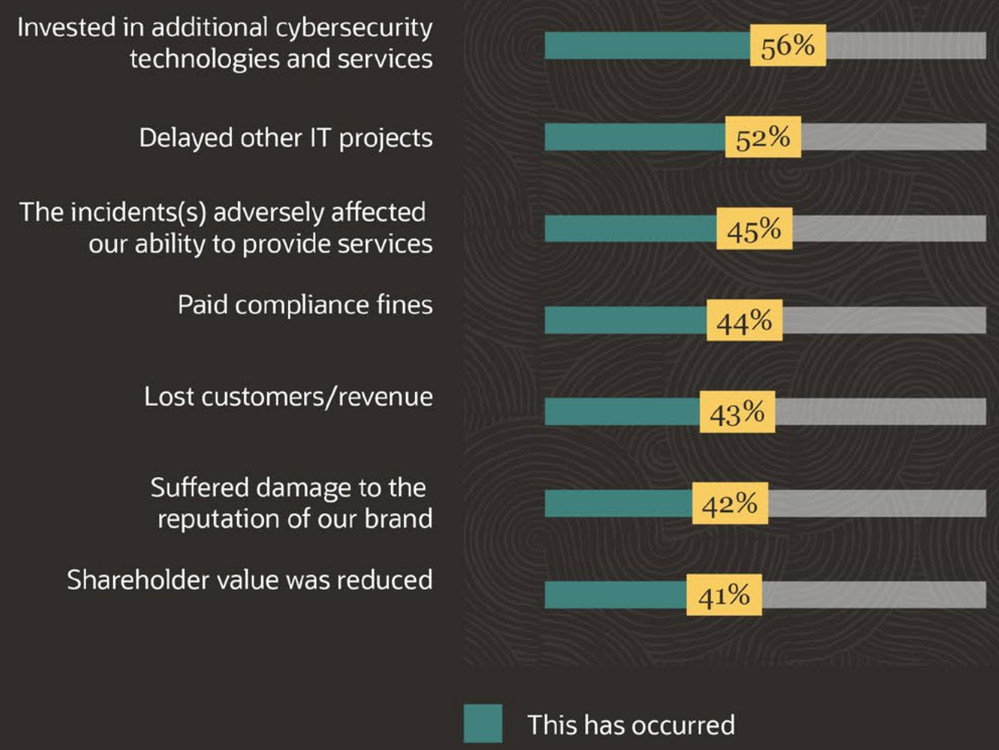
2 ir-capitalone.gcs-web.com/static-files/2f0f821a-0db0-4eab-9895-63013c4e59c2

3 capitalone.com/facts2019/2/

Both Direct and Indirect Financial Impacts Are Felt

The cost of a data breach continues to rise, and in 2019 was estimated to cost organizations impacted $3.9 million on average.[4] This is typically equated with lost revenue, brand damage, and diminished shareholder value. In fact, studies have shown that share prices fall by an average of more than 8% following a breach.[5] However, there are variables to consider based on the industry of the organization breached and type of information compromised. Financial institutions tend to see more of an impact to their share price, as do businesses that lose credit card information, social security numbers, or other highly sensitive data.6 Moving forward, compliance-related fines will be one of the increasing financial impacts of data breaches. In the first two years that GDPR has been in place, final and binding imposed fines have already totaled more than €150M, with an additional €300M in imposed fines still in process.[6]

However, the indirect costs associated with a breach are no less impactful. The cost of expanding security capabilities through the investment in additional tools and services is often unplanned and can reduce the budget for other areas of the business. Additionally, the "all hands on deck" nature of responding to a data breach can delay other scheduled IT projects and can adversely affect the organization's ability to provide services to their customers. These issues can result in a competitive disadvantage in the marketplace creating further downstream consequences from a data breach. As such, the impacts from a data breach are likely to touch a broad cross-section of the organization.



Question text: Did your organization suffer from any of the following business impacts as a result of its public cloud data loss? (Percent of respondents, N=661)

4 IBM/Ponemon Cost of a Data Breach Report https://databreachcalculator.mybluemix.net/

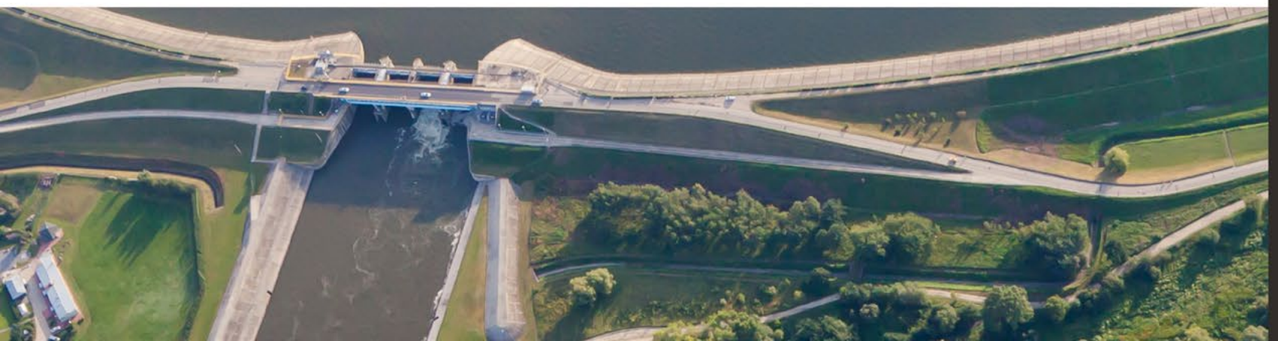
5 comparitech.com/blog/information-security/data-breach-share-price-analysis/

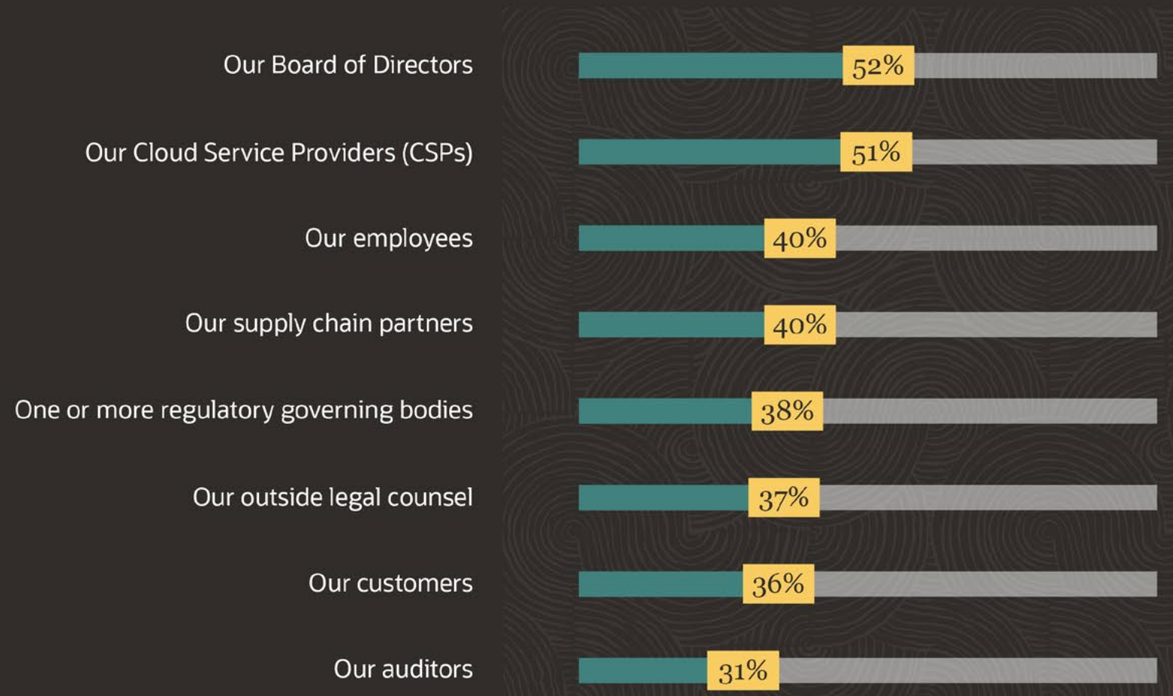
6 privacyaffairs.com/gdpr-fines/

Career Impacts Can Result from a Data Breach

Beyond the financial toll of a data breach, there are human impacts that result as well. As discussed, this began to shift with the mega-breaches of 2013, especially at the executive level. Today, 58% of our research respondents reported individuals were held accountable (including potential employment termination) as the result of a data breach. Interestingly, line-of-business leadership was just as likely to be impacted (38%) as security leadership (38%), pointing to the fact that security has become a cross-functional responsibility, whether employees actively realize it or not.

Healthcare and retail were the key exceptions where security leadership was more likely to be held accountable as the result of a data breach. These types of organizations are trusted with sensitive data including personal health information, medical histories, credit card numbers and more, making the result of a breach that much more damaging to the brand. Additionally, the regulated nature of these industries likely plays a role, wherein breaches involving healthcare or retail companies are likely to run afoul of HIPAA and PCI requirements, risking additional financial impacts to the company and making individuals more likely to be held accountable.



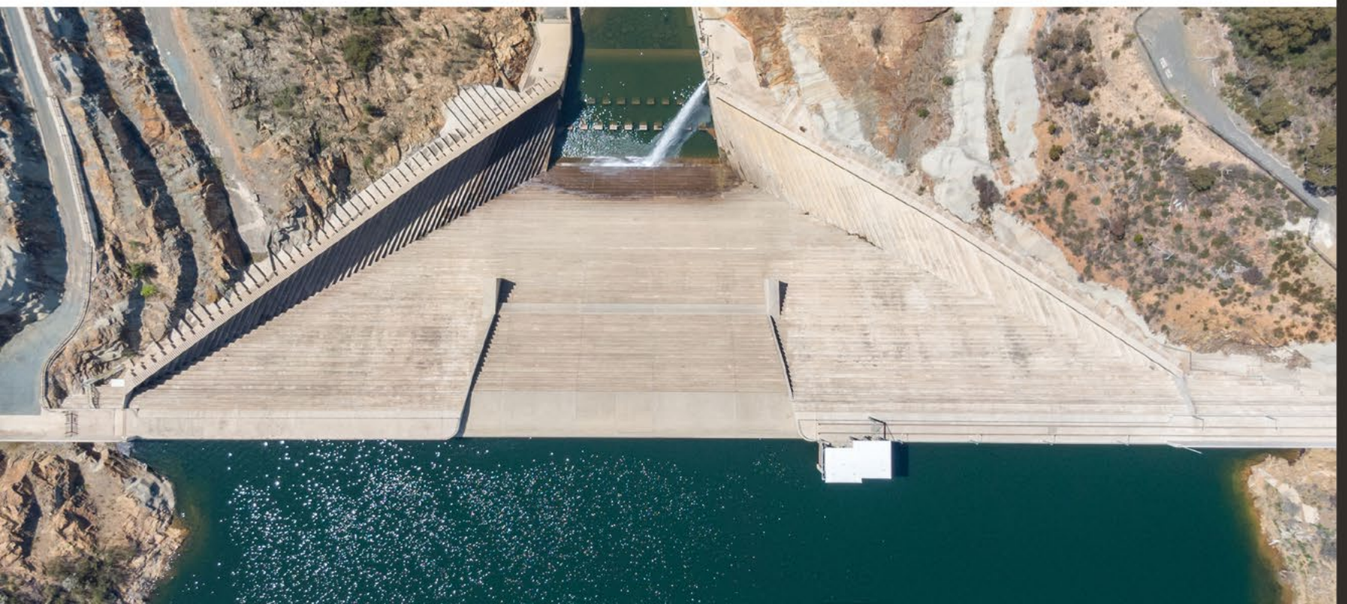


Question text: Which of the following parties did your organization need to inform of this public cloud data loss? (Percent of respondents, N=661, multiple responses accepted)

Improvements Across Data Controls, Visibility, and Identity via Automation Are Needed to Enhance Cybersecurity Programs

Improvements Across Data Controls, Visibility, and Identity via Automation Are Needed to Enhance Cybersecurity Programs

Of course, while a good response plan can help mitigate the effects of a data breach, the best result is for one not to occur in the first place. Clearly there are no actions an organization can undertake to guarantee they will not become the victim of a breach. However, improving cloud data controls, visibility, and identity by leveraging automation are good starting points to elevate security across the environment, ultimately presenting a less attractive target to attackers.



Implement Data Security Controls to Limit the Attack Surface

Implementing strong data controls, especially across the organization's most sensitive data, is essential to preventing data theft and misuse. Encryption is a good first step. One-quarter of our research respondents indicated that unencrypted sensitive data was a result they experienced with misconfigured cloud services within the past 12 months. In addition to encryption, automation must be introduced across the data lifecycle to help ensure that encryption travels with the data—at rest, in motion, and during export and backup—to be effective. However, encryption is only as effective as the encryption key management processes, so secure storage and distribution of keys and the separation of keys from data and backups must be addressed.

Encryption should not be seen as a silver bullet, but rather as one component of a broader approach. Good data hygiene is also an integral consideration. This includes reducing or removing unnecessary access to data at the data layer, including enforcement of separation of duties and narrowing the approved paths to access data to reduce the chances of data misuse or theft. Even those individuals who may have a valid business need for the data do not need to have access to it from anywhere, at any time, or from any tool. Effective access controls should be supplemented by auditing database activity to validate compliance with data access policies. Auditing has the added advantage of supporting post-incident investigations when needed. Finally, minimizing the amount of sensitive data on hand by statically masking the data, especially in non-production systems, helps narrow the potential for data loss. Implement data-driven security controls to restrict access based on these elements and further limit the attack surface from a data perspective.

Focus on Classification, Visibility, and Secure Configurations

Without a doubt, discovery and classification have become more difficult as cloud adoption has dispersed corporate data across a multitude of locations. However, this fact makes it all the more important to help ensure that, at a minimum, sensitive data is properly classified as such and discovered wherever it resides. Unfortunately, there appears to be a gap in understanding the importance of this aspect of cloud security. As we showed earlier, 38% of our research respondents say they have suffered data loss due to data misclassification. Yet only 24% say discovering and classifying all public cloud-resident sensitive data is one of the most important aspects of improving security visibility in the cloud. Clearly, there remains work to do.

of our research respondents say they have suffered data loss due to data misclassification.

Additional considerations include:

- Data security strategy should be focused on ongoing data classification to limit gaps in protection by applying policy the moment data is committed.
- Data tagging to help ensure policy follows data even when copied to a different database.
- SOC involvement in database monitoring to centralize responsibility across cloud and on-premises locations and help ensure hybrid -cloud approaches have the proper level of visibility.
- Visibility into cloud and data access and activity to understand potential unsanctioned or anomalous activity, especially relative to sensitive data.
- Utilize controls and capabilities built into database management systems to help ensure data is protected closest to the source.
- When using containers, separate data controls from the underlying infrastructure by leveraging the inherent RDDMS capabilities to control and monitor data access.
- Prioritize automated configuration controls to help ensure a secure-by-default approach to cloud services.

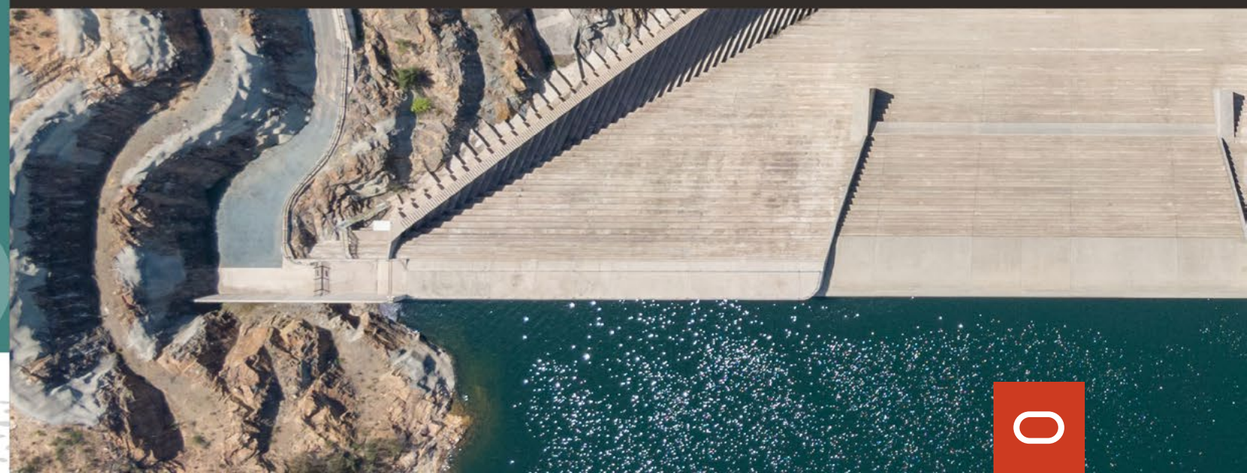
Consider Modern Identity and Access Management Solutions

Zero-trust architectures have received a lot of attention over the last few years as a way to modernize security to address increasingly distributed environments. One part of this approach is utilizing a least-privilege model to minimize the amount of permissions a user or entity has to the bare minimum required to perform their job or function. The second part involves improving authentication and authorization mechanisms by leveraging the context of users, locations, devices, time, and, most importantly, data to make enforcement decisions. The cloud has complicated identity and access management, a fact borne out by our research respondents with 31% agreeing that the use of cloud computing has made IAM controls and monitoring more difficult. With this in mind, both of the aforementioned aspects to a least-privilege approach require new methods that centralize identity management across all cloud and on-premises services for consistency.

Implementing a least-privilege approach requires new methods that centralize identity management across all cloud and on-premises services for consistency.

Additional considerations include:

- Separation of duties controls database administrators from accessing the data itself unless relevant to performing their job.
- Different approaches to privileged account management such as just-in-time privileged access. These mechanisms can reduce the risk that a compromised privileged account will be used for data theft by providing administrators elevated privileges only when required to perform a function, as opposed to those accounts carrying administrative rights on an ongoing basis.
- Integration of databases with directory services to allow vertical integration across the organization and improve on-boarding, off-boarding, and moves within the organization.



In Summary: Tenets for Limiting the Impacts of the Modern Data Breach

In Summary: Tenets for Limiting the Impacts of the Modern Data Breach

There is a reason that variations of the quote “there are only two types of companies, those who have been hacked, and those who will be” have been attributed to security leaders, technology CEOs, and FBI officials. Cybersecurity is hard and attackers are motivated, skilled, and relentless. However, the fact remains that many of the largest data breaches on record were not the result of sophisticated malware or state-sponsored hackers, though some certainly were. Rather, unforced errors caused by misconfigurations, elevated privileges, poor data security hygiene, and an inability to recognize when sensitive corporate data was being improperly accessed were at fault.

With that in mind, some tenets to avoid the impact of the modern data breach include:

1. **Classification.** The importance of discovering, classifying, and tagging sensitive, cloud-resident data cannot be overstated and is the lynchpin to a successful cloud data security program.
2. **Data security.** Apply holistic data security controls including encryption, masking, tokenization, redaction, separation of duties, key management, and key separation.
3. **Configuration management.** Implement secure-by-default configurations for all relevant cloud components/services, automate patching and updates, and identify and correct deviations from the secure baseline.
4. **Identity.** Utilize a least-privilege approach for cloud resources with ongoing assessments and contextual authentication and authorization.
5. **Visibility.** Employ cloud and data visibility and analytics and utilize audit trails and forensics tools to identify abnormal access to sensitive data.

Cloud providers can help address many of these components and assist customers in understanding their responsibilities and the tools available to them through education and a transparent partnership approach.

ORACLE KPMG

Research conducted in partnership with ESG