ORACLE KPMG

Addressing Cyber Risk and Fraud in the Cloud

Oracle and KPMG Cloud Threat Report 2020 series

Volume 3

Research conducted in partnership with ESG

Contents

03 Executive Summary

04 The Business Cloud Has Arrived

- 05 The Application Economy Is Shifting to the Cloud
- 07 Fast and Furious Cloud Adoption Often Bypasses Usage Policie
- 09 **Spotlight:** The Surge in Remote Work Has Increased the Role of Cloud Services

11 The Fraud Threat Landscape Is Increasingly Cloudy

- 12 Extortion and Impersonation Headline Cyber Fraud
- Ransomware Attacks Are Moving to the Clou
- Identity Fraud Is a Means to Payment Fraud
- 15 **Spotlight:** The Fraudster Within

16 Mitigating Cloud Risk Requires Defense-in-depth Controls and Processes

- 17 Employ a Zero-trust Approach to Secure the Identity Perimeter
- Securing the Matrix of Any-ness with a Dose of Pragmatism
- Privileged Access Management in a Cloud Context
- 20 Adapt Business Processes as Cloud Usage Changes
- 21 **Spotlight:** Leverage Machine Learning Data Analytics

23 In Summary: All Stakeholders Must be Vigilant

Executive Summary

Welcome to the third installment of the Oracle and KMPG Cloud Threat Report 2020 series, in which we will explore how the broad adoption of cloud services has affected cyber risk and fraud. The themes offered in the prior reports of the series remain relevant herein, including the need for a cybersecurity cultural shift that yields organizational alignment on balancing the business needs for leveraging cloud services and the associated risk, principally, cyber fraud.

Fraud itself is one of the oldest tricks in the book employed by criminals for financial gain dating back to the beginning of commerce. The use of cloud services, fueled by digital transformation initiatives, is yielding new business workflows that, in turn, are creating new opportunities for fraudulent activity. The increase in remote work has served as an additional catalyst for the use of cloud services. There is a conundrum, however, in addressing risk and fraud in the cloud—maintaining a frictionless user experience while introducing processes and controls that reduce risk.

The focus on hardened cloud configurations to secure the human perimeter discussed in the first report in the Cloud Threat Report series, Addressing Secure Configurations Amidst a State of Constant Change, is highly applicable for mitigating the risk of cyber fraud. This report will expand upon the notion of a human perimeter while also exploring a series of key findings, including:

The use of cloud services, fueled by digital transformation initiatives, is yielding new business workflows that, in turn, are creating new opportunities for fraudulent activity.

- **The business benefits of the cloud are changing the complexion of cloud usage.**

  No longer just an adjunct compute environment, public cloud services are strategic to business operations and objectives.

- **The shift of the application economy to the cloud creates a ripe environment for cyber fraud.**

  Ever opportunistic, cyber adversaries are exploiting the increased use of the cloud.

- **The surge in remote work expands cloud risk.**

  As remote knowledge workers rely more on cloud applications, their role as a potential target or insider threat grows.

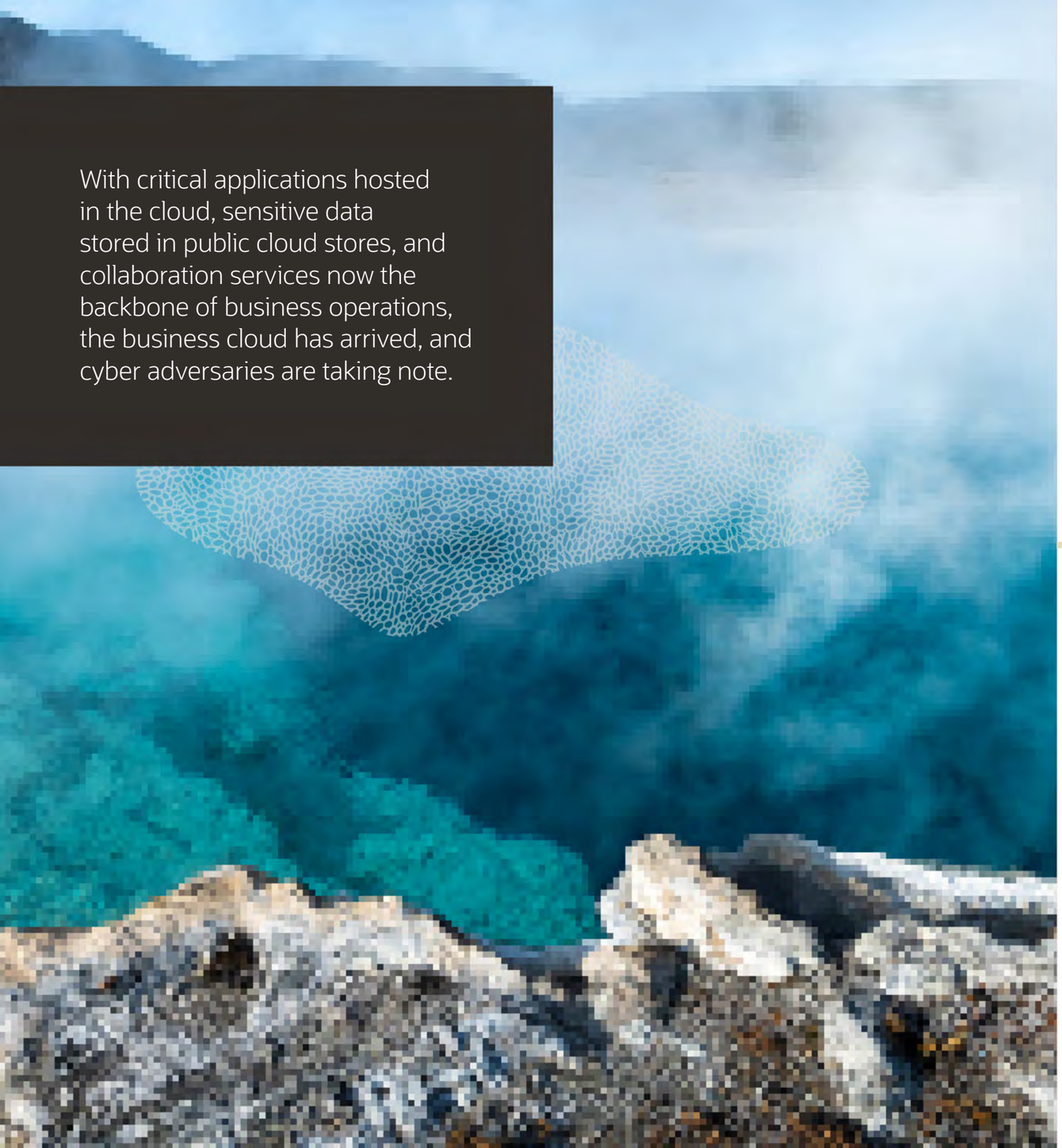
- **Identity fraud is an example of how the cloud has made cyber-crime easier to perpetrate.**

  Identity fraud, as a means to the end of financial fraud, tops a range of types of cloud cyber risk.

- **Mitigating cyber fraud necessitates a high degree of focus on managing user identities.**

  The combination of ways in which users access cloud applications requires well-defined roles to appropriately scopes privileges.

The Business Cloud Has Arrived



With critical applications hosted in the cloud, sensitive data stored in public cloud stores, and collaboration services now the backbone of business operations, the business cloud has arrived, and cyber adversaries are taking note.

The Application Economy Is Shifting to the Cloud

The concept of an application economy has evolved from an increased use of mobile applications to how a range of applications can enable digital transformation initiatives and run business operations. In fact, according to our research, the average organizations use nearly 1,000 sanctioned and un-sanctioned applications.

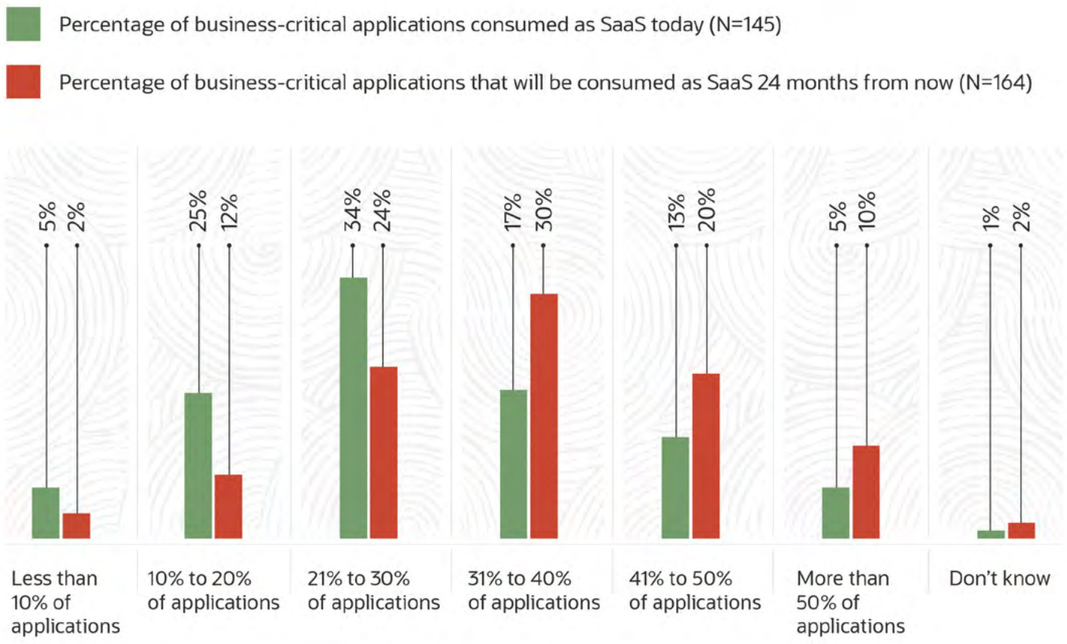
Approximately how many total sanctioned business applications does your company run worldwide? (Percent of respondents, N=164)

1,001

The average number of total sanctioned business applications companies run worldwide

But not all applications are the same in terms of their respective criticality to business success. On average, roughly 10% of these applications are considered business-critical, with enterprise organizations sharing they have, on average, 99 business-critical applications. These business-critical applications are migrating to public clouds at an appreciable rate, as evidenced by the average of cloud-hosted business-critical apps increasing from 29% today to 38% over the next 24 months.

Of all sanctioned business-critical applications used by your organization, approximately what percentage do you consume today as SaaS, and how do you expect to change over the next 24 months?



The risk associated with interconnected applications is that unauthorized access to one, especially with privileged credentials, can lead to access to others, a perfect scenario for fraudsters.

The full stack of business-critical applications, from customer-facing front-office interfaces through middle-office transaction processing to back-office operations, now have a cloud context. Many of these cloud applications are connected. Marketing automation is layered on top of customer relationship management, and supply chain apps may be part of an enterprise resource planning (ERP) application or connected as a third-party application. Yet more examples include human resources (HR), accounts receivable and payable (AR/AP), asset management, and more. The risk associated with interconnected applications is that unauthorized access to one, especially with privileged credentials, can lead to access to others, a perfect scenario for fraudsters.

As the primary means of communication, email is also business-critical. The shift to cloud-delivered email, per the 73% of respondents who now use cloud-based email,[1] creates new opportunities for account takeover (ATO) attacks via fictitious login pages.

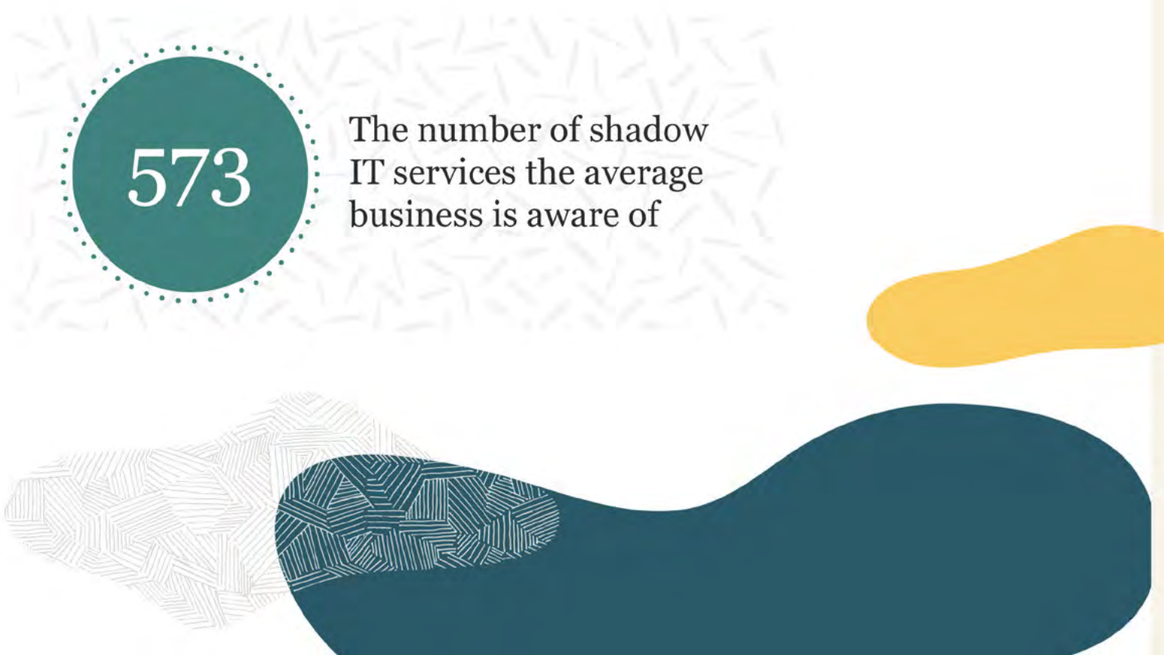
1 Source: ESG Research, Trends in Email Security, February 2020

Fast and Furious Cloud Adoption Often Bypasses Usage Policies

The decentralized adoption of cloud services often leads to non-compliant use. With an average of 573 shadow IT applications in the enterprise, many, by definition, have not been vetted by IT and cybersecurity teams, leading to loose configurations and unsupervised use.

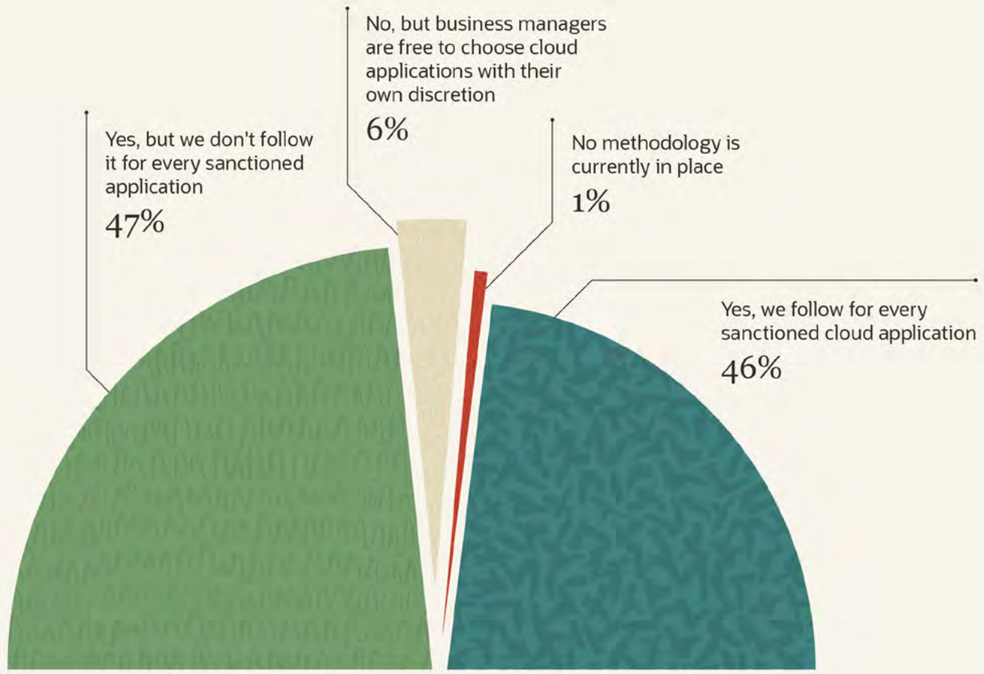
Considering your entire workforce, how many different shadow IT cloud applications do you believe are used regularly at your organization?

(Percent of respondents, N=300)



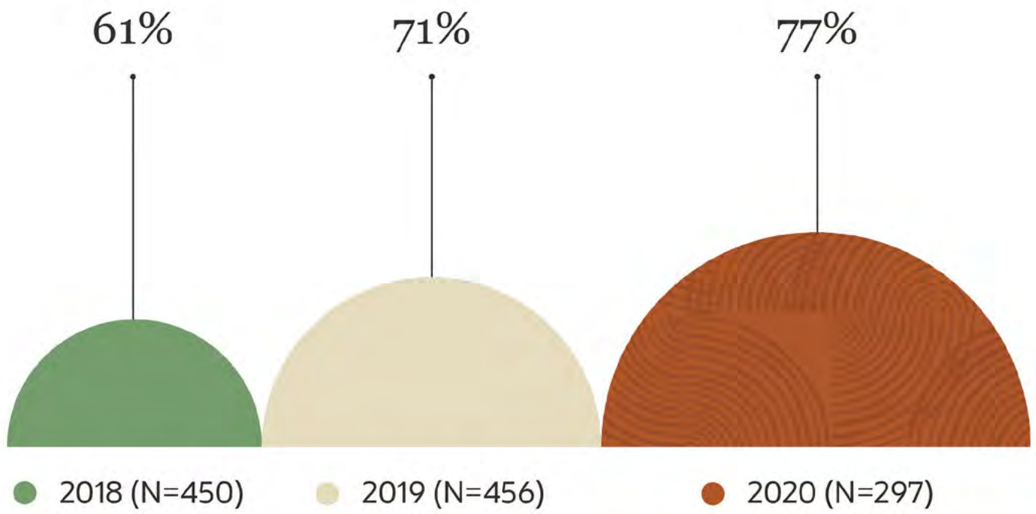
Policy violations are not the exclusive domain of unsanctioned, shadow IT applications. Nearly half of our research participants shared that their business does not follow a formal security methodology to address the security risk associated with every sanctioned cloud application.

Does your organization have a formal security methodology it follows to address the security risk associated with cloud applications before those applications are approved for use (i.e., sanctioned by IT)? (Percent of respondents, N=300)



The concern over violation of said policies is increasing appreciably, per the 16% increase from 2018 to 2020 that individuals and lines of business are not following policies and guidelines for using cloud applications.

How concerned are you that individuals, departments, and/or lines of business within your organization are in violation of your security policies/ guidelines for the use of cloud applications? (Percent of respondents, N=297)



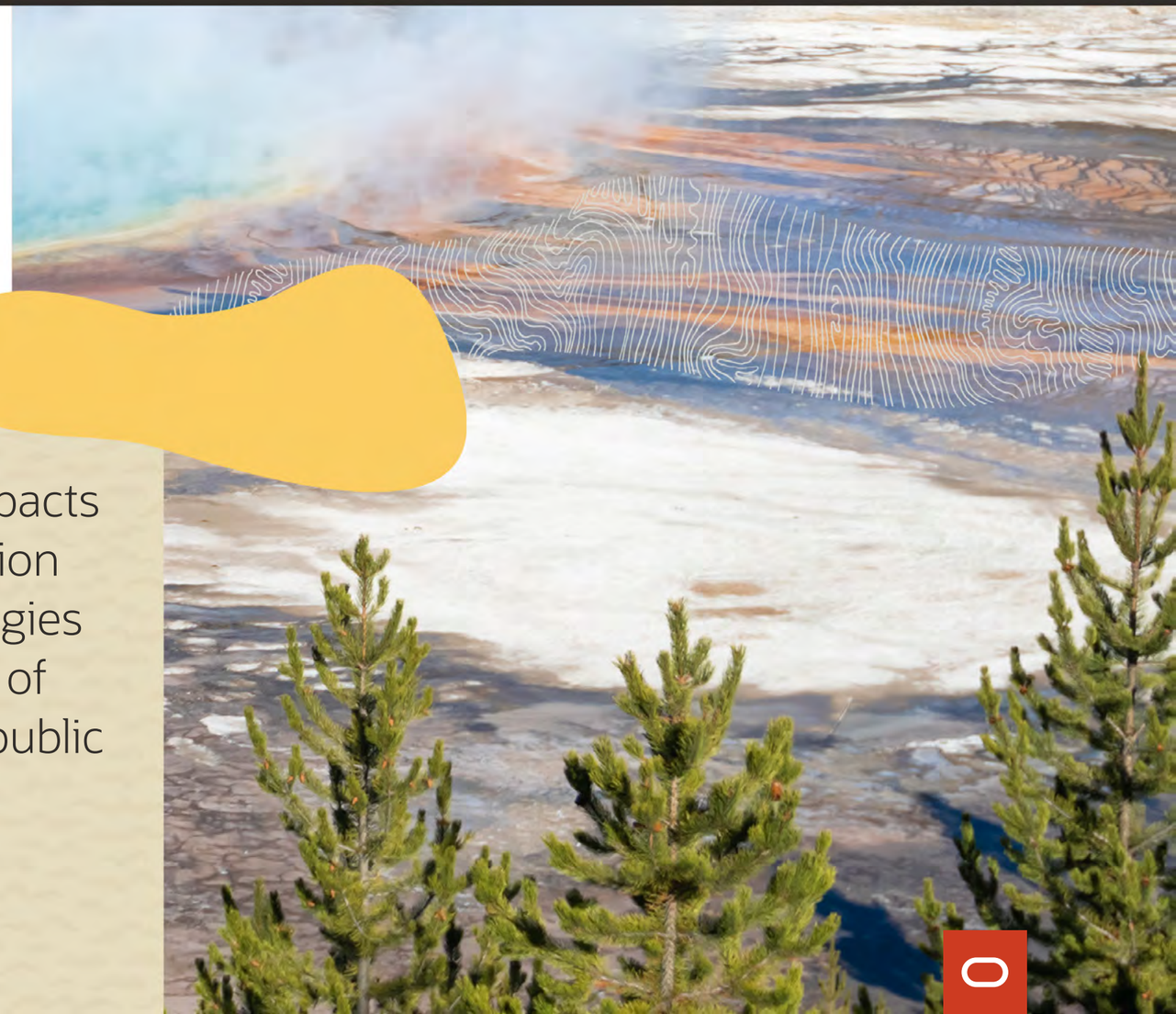
Ironically, our research indicates that senior leaders are as likely as individual contributors to be guilty of not following the rules. The results of policy violations are numerous, headlined by misconfigured cloud applications including overprivileged user accounts that are then targeted by spear phishing attacks.

Spotlight: The Surge in Remote Work Has Increased the Role of Cloud Services

The increase in remote work as a result of the COVID-19 disruption has had a dramatic impact on the IT landscape, accelerating an already robust level of cloud adoption. On average, over three-quarters of knowledge workers are now working from home, resulting in an increased use of collaboration platforms, file sharing services, and office productivity. This dynamic is not temporary. The most significant impacts of the COVID-19 disruption on longer-term IT strategies include the broader use of cloud applications and public cloud infrastructure.[2]

The surge in remote work has also created new opportunities for threat actors. 47% report an increase in cybersecurity attacks,[2] including phishing attacks. In fact, 31% share that protecting remote employees against increased COVID-19 phishing emails and cyber-attacks is one of the biggest security challenges associated with having more remote employees.[3]

The most significant impacts of the COVID-19 disruption on longer-term IT strategies include the broader use of cloud applications and public cloud infrastructure.[2]



2 ESG Research Report, The Impact of the COVID-19 Pandemic on Remote Work, 2020 IT Spending, and Future Tech Strategies, June 2020.

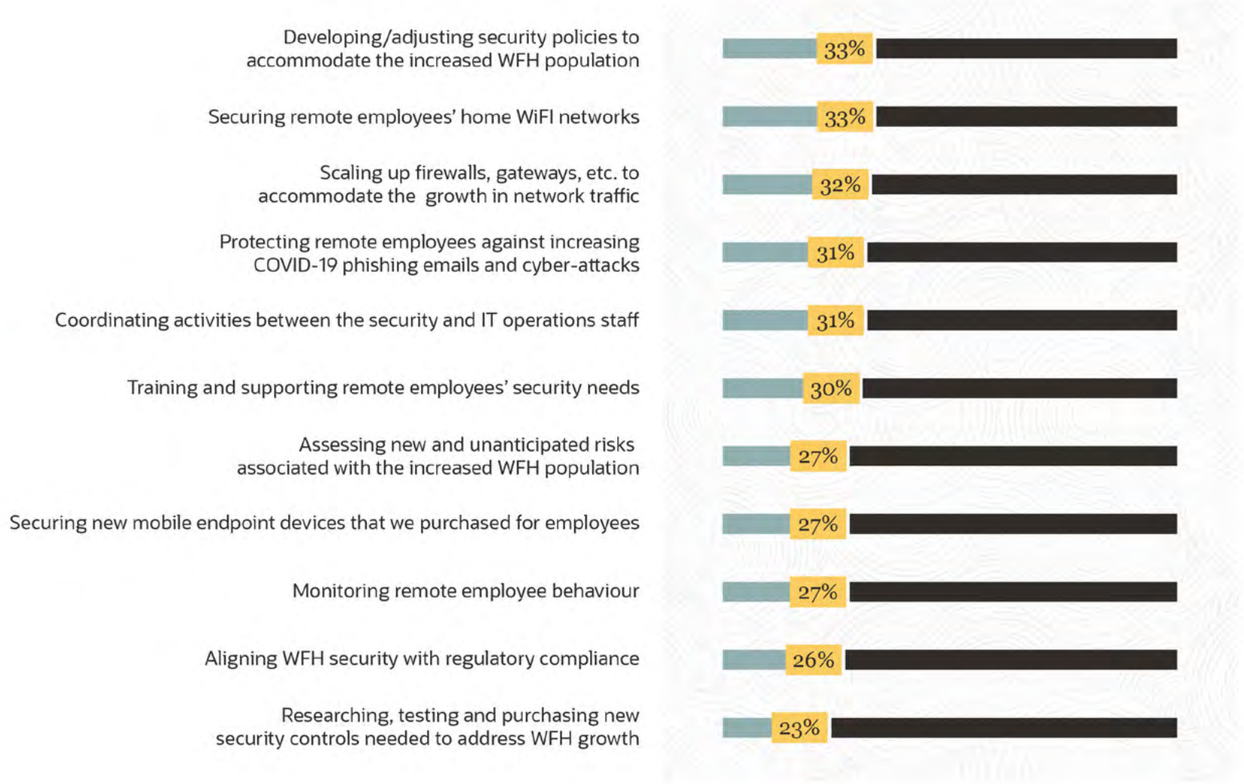
3 ESG Master Survey Results, Technology Impact of COVID-19: IT Decision Maker (ITDM) View, May 2020.

Working remotely has also created new concerns related to the insider threat, per the 27% who report that monitoring remote employee behaviors is one of their top security challenges. Malicious insiders now have more time to plan their fraudulent activity. Additionally, warning signs exhibited by malicious insiders are now all that much more difficult to detect as these individuals can conduct fraudulent activity in the darkness of their home.

Warning signs exhibited by malicious insiders are now all that much more difficult to detect as these individuals can conduct fraudulent activity in the darkness of their home.

Which of the following are the biggest security challenges associated with having more of your employees currently working from home?

(Percent of respondents, N=488, multiple responses accepted)



The Fraud Threat Landscape Is Increasingly Cloudy

Truth be told, fraud has always been cloudy, with the types of fraud as devious as the human mind is creative. Let's frame fraud in a cloud context. Cyber fraud that exploits the expanded use of cloud services represents the principal form of cloud risk, one of the more common types of cybersecurity attacks. 40% of research participants report that their organization has been a target of such an attack in the last 24 months.

Cyber fraud that exploits the expanded use of cloud services represents the principal form of cloud risk, one of the more common types of cybersecurity attacks.

of organizations have experienced cyber business fraud within the last 24 months

Extortion and Impersonation Headline Cyber Fraud

Fraudsters employ multiple means to monetize illicit activity, with lines between the types of cyber fraud and the tactics and methods employed by cyber criminals blurry. As such, we will focus on a few of the more prominent areas of cyber fraud.

Ransomware Attacks Are Moving to the Cloud

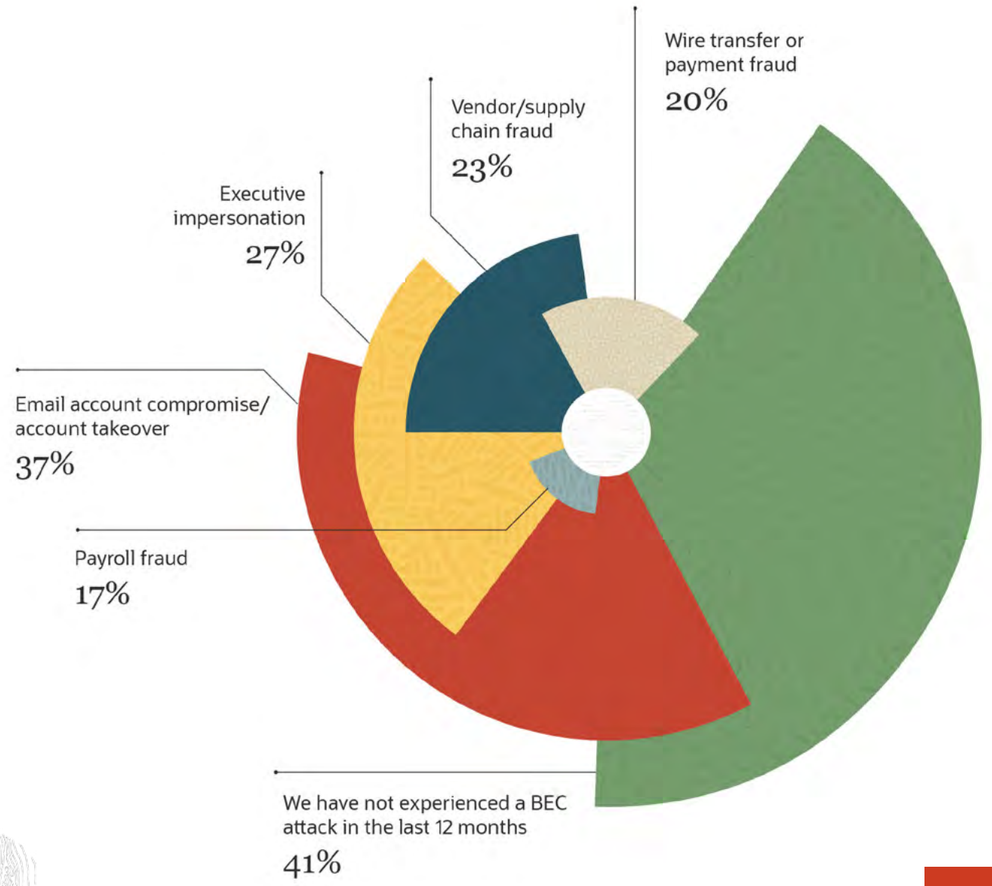
As a form of extortion, ransomware continues to be a big business for cyber criminals. Just as investigations follow the money, cyber criminals follow the data. his dynamic first surfaced in 2017 when the data in a significant number of Internet-facing MongoDB databases were wiped a held for ransom. These attacks that exploit mis-configured MongoDB databases continue today with tens of thousands MongoDB databases subject to the same form of extortion in the summer of 2020. Additional recent examples of ransomware attacks against cloud-resident data include dental records, chart histories, and x-rays of patients at hundreds of dental providers held for ransom.

The use of file synch and share services creates another vector for cyber criminals. As local files are encrypted by ransomware malware, those files are synched to the cloud, eliminating the ability to restore from a cloud-resident backup, increasing the likelihood the victim will pay the ransom.

Identity Fraud Is a Means to Payment Fraud

Impersonation, or identity fraud, is the predominant means for cyber criminals to conduct financial fraud. The rise in business email compromise (BEC) attacks is evidence of this point. The FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report reveals that BEC attacks in 2019 were quite profitable for cyber criminals, totaling $1.8B in losses, likely not a full picture of the actual financial impact, as many BEC incidents go unreported. Further, 39% of respondents stated that their organization had experienced a BEC attack in the last 24 months, including vendor/supply chain fraud, wire transfer or payment fraud, and payroll fraud.

What types of business email compromise (BEC) attacks has your organization experienced within the last 12 months? (Percent of respondents, N=403, multiple responses accepted)



Understanding the Attack Chain

In all cases, a recipient receives a bogus email, purportedly from an individual in a position of authority urgently instructing them to take an action that constitutes fraud, such as wiring funds to a supplier. But why can't the unwitting participant, the individual instructed to issue a wire transfer, be more capable of ferreting out such emails? Understanding this risk requires a look at the attack chain for each incident of a cyber attack.

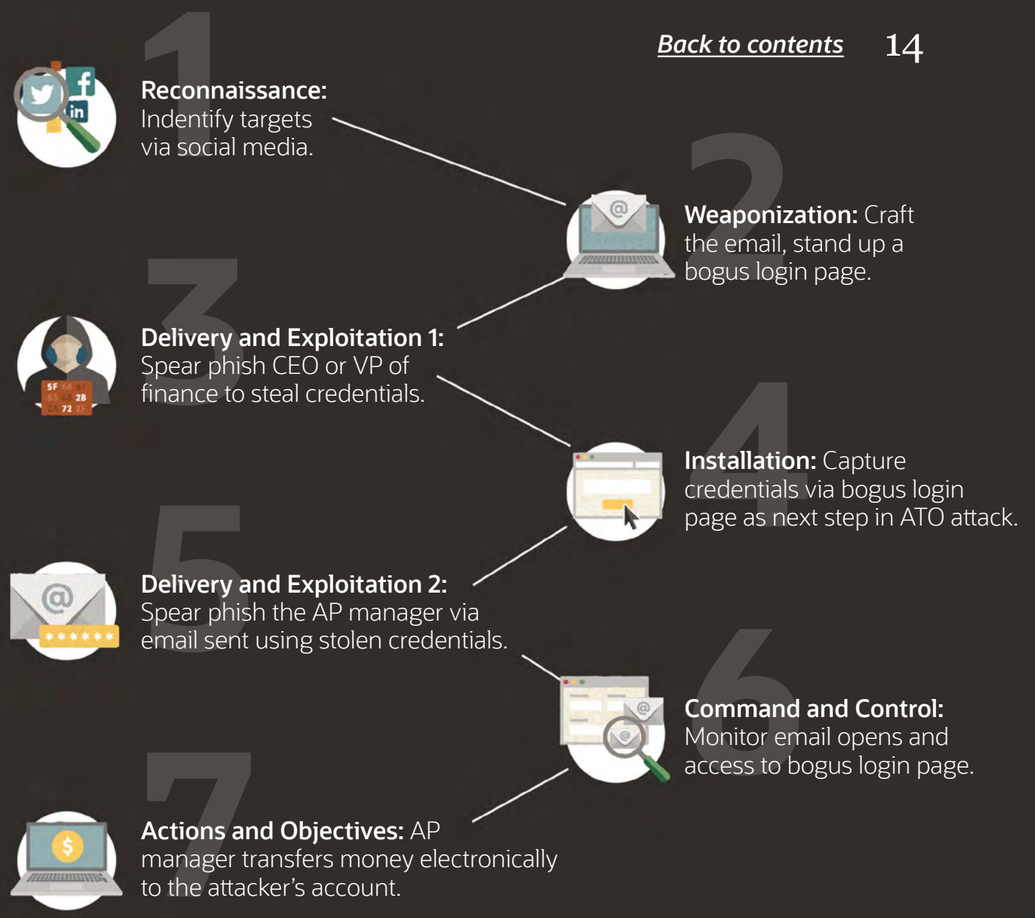
By performing reconnaissance on social media sites, cyber criminals target multiple employees via a campaign that blends methods, but with a common vector, email. The role of social media is a central factor in these attacks, with cyber criminals searching for and finding individuals responsible for certain job functions, accounts payable (AP), for example. In the AP example, the social media profile for an AP manager may also include a certification on a certain accounting system, information that can be used in a well-crafted phishing email. And since our professional network is part of our social media identity, a would-be attacker can also gain insight about the individuals from whom the prospective victim would reasonably receive emails. The next step is not only to author the email but send it from the actual email account of a colleague, making detecting such emails as an attack all the more difficult.

Adversaries often exploit the fact that end-users have become accustomed to receiving emails from IT instructing them to change their password. BEC attack chains often include spear phishing a colleague with an email that informs them it is time to update their cloud email credentials with a link to a well-designed login page that captures their credentials. Bad actors are, not surprisingly, exploiting the COVID-19 disruption by basing the need to change passwords on the fact that employees are now working from home. The FBI's report also notes that over three-quarters of cloud breaches include stolen cloud credentials.[5]

With stolen credentials in hand, the perpetrator can now send an email from, for example, the VP of finance's account, making it extremely difficult for the recipient, the AP manager in our example, to determine legitimacy.

The universe of "users of interest" who are subject to such account takeover (ATO) phishing attacks includes those with privileged access to the cloud-based systems and data stores: CRM administrators, developers, and more.

5 FBI Internet Crime Complaint Center (IC3), 2019 Internet Crime Report.



BEC attack chains often include spear phishing a colleague with an email that informs them it is time to update their cloud email credentials with a link to a well-designed login page that captures their credentials.

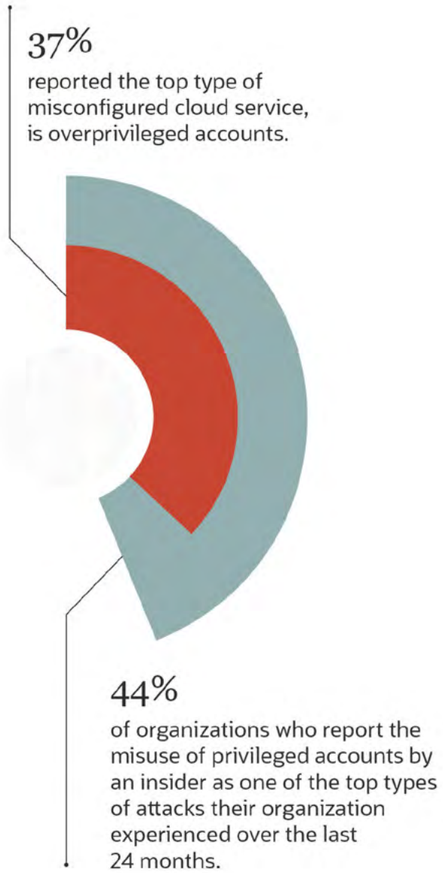
Spotlight: The Surge in Remote Work Has Increased the Role of Cloud Services

Business email compromise (BEC) attacks do not, however, have an exclusive claim on financial fraud. Accounting fraud and vendor fraud can also serve as viable means to conduct payment fraud, which may be perpetrated by the fraudster within.

The threat actors of cyber fraud include cyber criminals, insiders, and those who collude as part of group crime. While most data breaches are perpetrated at the hands of external adversaries, the 2020 Verizon Data Breach Report notes that 30% of the data breach investigating conducted by Verizon in 2019 involved a malicious insider. The report notes that not only are these insiders often in a position of seniority, but that the financial losses can be appreciable. Because of the insider's familiarity with both business process and business applications, the insider threat is harder to detect. Further, now being able to conduct fraud out of sight in their own home, remote work has exacerbated the internal threat.

Internal fraudsters can create ghost employees (hard to detect during periods of rapid new employee onboarding) as a means to steer paychecks to a personal account. Similarly, malicious insiders with access to accounting systems can also create fictitious suppliers and fictitious invoices from said suppliers, payment for which is ultimately funneled to a personal account. Or they can simply change the bank account and routing number for a legitimate supplier. Insiders may also work in collusion with a supplier who issues invoices for products not delivered and services never rendered. But why is the cloud a factor?

Many organizations have not adapted their application controls and identity and access management programs for the cloud such that they have overprivileged accounts and lack user monitoring to detect anomalous and potentially fraudulent activity. In fact, the top type of misconfigured cloud service, reported by 37% of our research respondents, is overprivileged accounts. The role of overprivileged accounts is clear per the 44% of organizations who report the misuse of privileged accounts by an insider as one of the top types of attacks their organization experienced over the last 24 months. It is important to note that these types of cyber incidents include both malicious insiders and unintentional insiders who did not realize they were abusing a privileged account. Afterall, people make innocent, yet impactful, mistakes.



> Insiders may also work in collusion with a supplier who issues invoices for products not delivered and services never rendered.

Mitigating Cloud Risk Requires Defense-in-depth Controls and Processes

Mitigating cloud risk requires revisiting business processes with a focus on access authentication and privilege authorization. Central to protecting an organization against cyber fraud is hardening the configuration of cloud applications and services with the least privileged access management principles of a zero-trust strategy.

Central to protecting an organization against cyber fraud is hardening the configuration of cloud applications and services with the least privileged access management principles of a zero-trust strategy.

Employ a Zero-trust Approach to Secure the Identity Perimeter

The concept of zero-trust introduced a decade ago challenged the best practice of "trust but verify" with an assumption that everyone and everything is a threat. While zero-trust contemplated increased knowledge worker mobility, it is a term coined well before the arrival of the business-critical cloud.

Securing the Matrix of Any-ness with a Dose of Pragmatism

Irrespective of its vintage, zero-trust provides a strategic framework to securing the matrix of any-ness, the combination of use cases IT and cybersecurity teams must enable and secure—any user from any device and any location accessing any application at any time. Such a matrix aptly conveys how we can think of the identity perimeter.

To secure the identity perimeter, we should evolve from a modality of "trust but verify" to one of "don't trust, continuously verify," which assumes, for example, that credentials have been stolen, that users have ill intent, and so on. At the same time, IT and cybersecurity leaders need to balance such an approach with one that also takes into account the end-user experience.

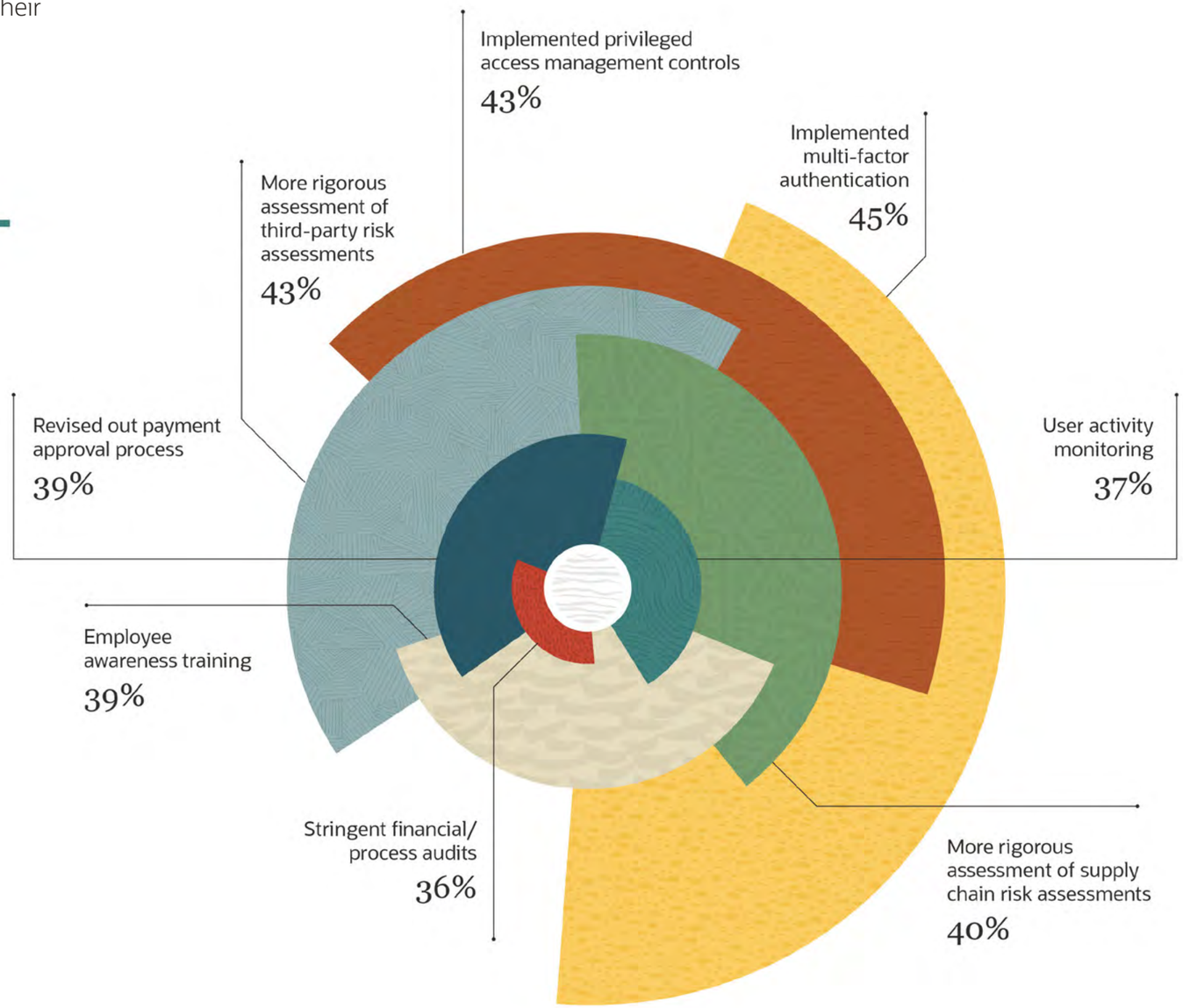
While multiple factors of authentication should be required in certain circumstances, including authenticating access to cloud management consoles and vaults that store cloud secrets, a context-based approach to multi-factor authentication is more pragmatic. Context allows for the use of adaptive authentication, which takes into account multiple attributes of a user session to drive a policy-based approach to triggering a second factor. Such session-specific attributes include the criticality of the application, the sensitivity of the data, and anomalies associated with the user's session. Anomalies that could be indicative of an attempt to conduct fraud align with the dimensions of any-ness, such as logging in from an unusual location or at an unusual time.

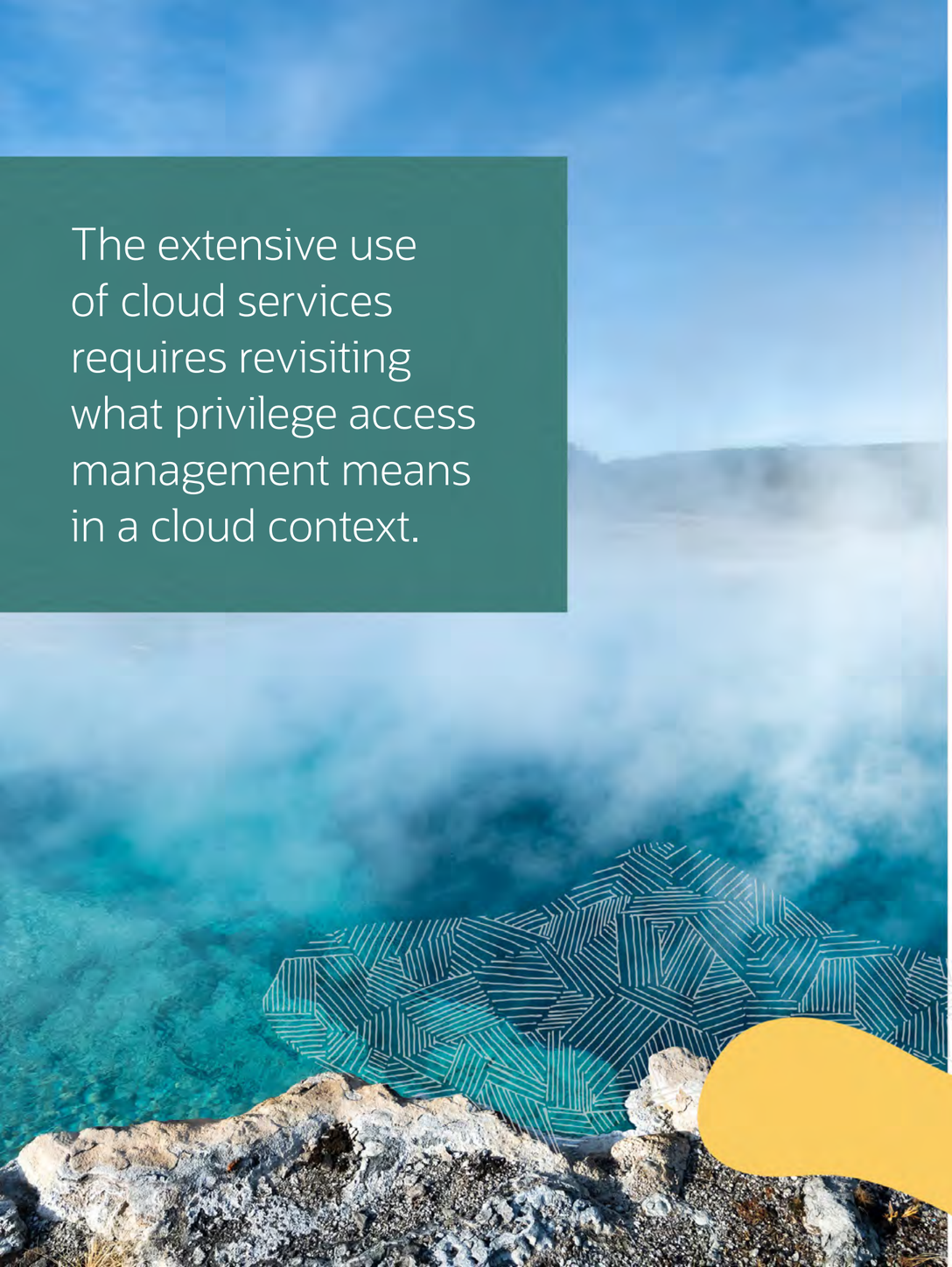
Our research participants agree with implementing MFA as the top action their organization has taken to prevent future incidents of cyber business fraud.

Context allows for the use of adaptive authentication, which takes into account multiple attributes of a user session to drive a policy-based approach to triggering a second factor.

Our research participants agree with implementing MFA as the top action their organization has taken to prevent future incidents of cyber business fraud.

Which of the following actions, if any, has your organization taken to prevent future incidents of cyber business fraud? (Percent of respondents, N=150, multiple responses accepted)





The extensive use of cloud services requires revisiting what privilege access management means in a cloud context.

Privileged Access Management in a Cloud Context

The extensive use of cloud services requires revisiting what privilege access management means in a cloud context. While managing escalated privileges on end-user desktops remains an important practice that can prevent malware from gaining administrative access, privilege access management (PAM) for cloud services is often application-specific.

Cloud PAM raises the question of what a user can do specific to the functional capabilities of a given cloud application. For example, in a cyber fraud context, placing sensitive data in a sanctioned cloud application, sharing data with a third party via the same application, changing bank account information for a supplier, and creating new employee records are examples of application-specific privileges. The same holds true for infrastructure-as-a-service (IaaS) services, in which case the least amount of people should have the least amount of privileges to perform tasks such as change the access control lists (ACL) on object stores. But how do we manage cloud privileges at scale?

The central construct managing privileges is roles, the swim lanes users are allowed to occupy to perform a given task as part of performing their job. Roles must be narrowly scoped based on job function. Those roles that grant risky privileges should be regularly reviewed to validate that all users assigned such roles do in fact require said privileges. Roles also serve another important purpose: to identify anomalous activity that could be indicative of stolen credentials or an insider threat since usage behavior of all users with a specific role should represent a normalized baseline of activity.

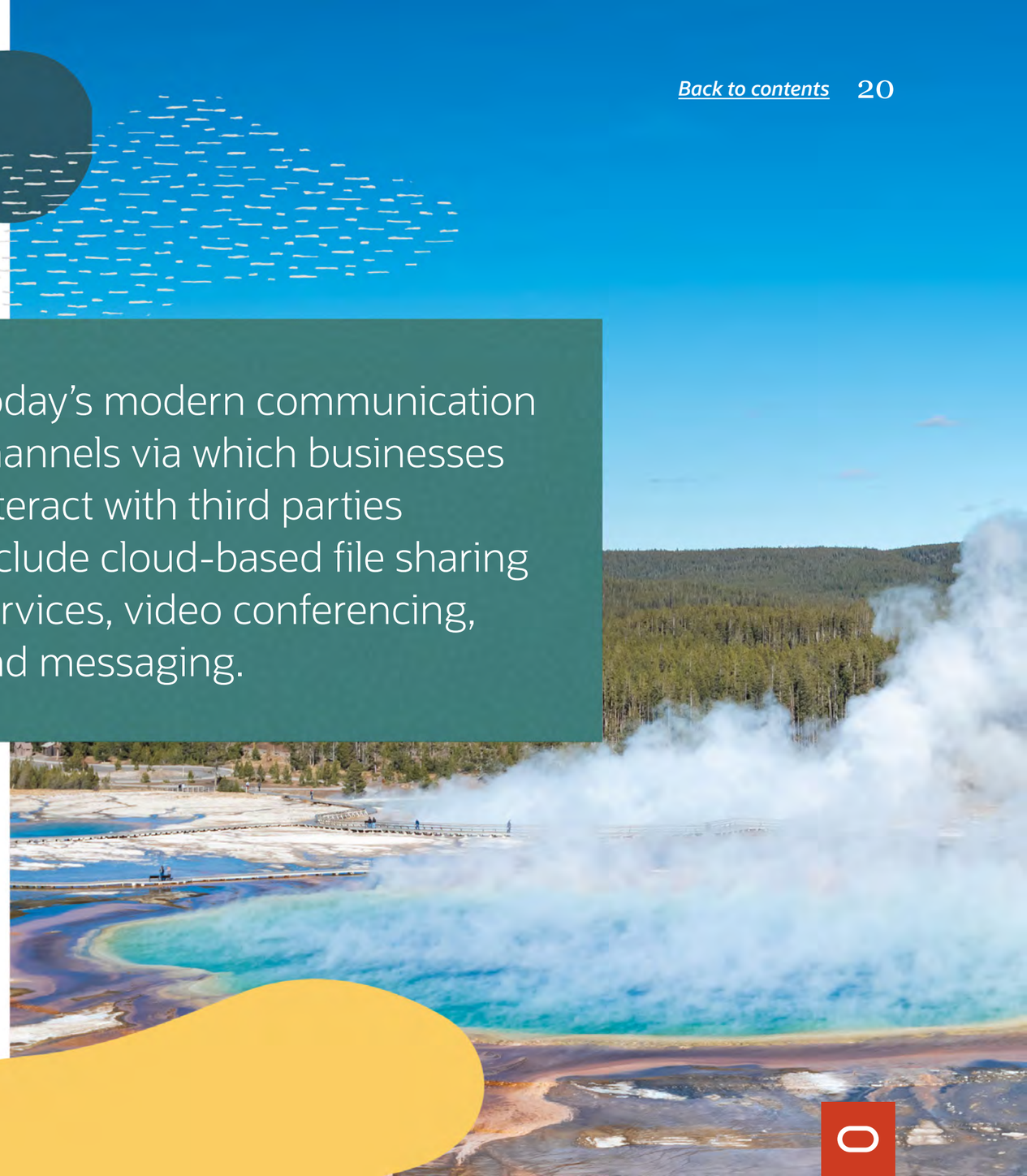
The central construct managing privileges is roles, the swim lanes users are allowed to occupy to perform a given task as part of performing their job.

Adapt Business Processes as Cloud Usage Changes

The prior discussion on the types of fraud included a number of examples of supply chain fraud, which is why 40% of our respondents cite a more rigorous assessment of supply chain risk as a top area in which they took action to prevent cyber business fraud. From a process perspective, the best practice of 3-way match for issuing a payment should be employed: approval of the purchase order (PO) issued to the supplier, approval of the invoice received from the supplier, and, finally, approval of the actual payment. Because the first two steps are required, checks cannot be sent and wire transfers cannot be made without approved POs and invoices validating the transaction. To implement 3-way match, the zero-trust practices discussed above apply: PAM for managing supplier records and MFA for making payments. And, of course, all such activity should be logged for auditing and investigative purposes.

Today's modern communication channels via which businesses interact with third parties include cloud-based file sharing services, video conferencing, and messaging. Users sharing sensitive information with third parties must be educated on the policies that govern what types of data are considered sensitive, whether there are compliance implications, who is authorized to receive such information, and more. As such, 43% of our respondents cite more rigorous assessment of third-party risk as an area they have focused on to prevent future incidents of cyber business fraud. Because the policies are often violated, enforcing tighter business processes is often difficult. As such, a strong dose of user activity monitoring is in order.

Today's modern communication channels via which businesses interact with third parties include cloud-based file sharing services, video conferencing, and messaging.



Spotlight: Leverage Machine Learning Data Analytics

Security operations center (SOC) teams are already dealing with a flood of security event telemetry. The increasingly strategic dependence on cloud services and applications necessitates gaining greater visibility into cloud usage, adding yet more events to an over-subscribed triage queue.

To detect fraudulent activities that exploit cloud services, cybersecurity teams will need complete observability inclusive of user activity, application activity, and access to cloud data stores. Doing so will serve to identify potentially risky end-user and anomalous behavior, such as changing a supplier's bank account information and data exfiltration.

But tracking the who, what, where, when, and how of user activity, including administrative changes to the configuration of cloud services, will trigger a lot of events. As such, SOC teams need to improve the signal-to-noise ratio of cloud security events to be more effective in detecting and responding to incidents of cyber fraud. Enter machine learning as a technology to augment human-based curation for a higher fidelity fraud detection system. When asked about the top use cases for which their organizations will employ artificial intelligence over the next 24 months, nearly half of our respondents cited fraud detection.

For which of the following cybersecurity use cases will your organization employ artificial intelligence within the next 24 months? (Percent of respondents, N=202, three responses accepted)

The increasingly strategic dependence on cloud services and applications necessitates gaining greater visibility into cloud usage, adding yet more events to an over-subscribed triage queue.

Of the different types of artificial intelligence and machine learning, one in particular is especially relevant for detecting business email compromise attacks, natural language understanding (NLU), a subset of natural language processing (NLP). While NLP deals more broadly with the interaction between computers and humans using the natural language, NLU is focused on analyzing text. NLU-enabled cybersecurity controls consider the scope of text with respect to email addresses, syntax, formatting, content, and style of a message body. The nature of BEC attacks makes them an ideal use case for NLU technology. For example, does the CEO typically send wire transfer instructions by email? Is the email written in a style and with language typically employed by the CEO? While the event telemetry generated by the matrix of any-ness is daunting, artificial intelligence technologies such as natural language understanding offer hope that needles can be found in haystacks of security events.

While the event telemetry generated by the matrix of any-ness is daunting, artificial intelligence technologies such as natural language understanding offer hope that needles can be found in haystacks of security events.

In Summary: All Stakeholders Must be Vigilant

Cyber adversaries are targeting not just cloud applications and cloud-resident data, but the workflows that utilize cloud services to conduct fraud. As a result, cyber business fraud has emerged as a central concern related to the risk associated with both modern business workflows and the increased reliance on cloud applications. The surge in remote work has punctuated this reality.

The cultural shift to gain organizational alignment on the cybersecurity imperative applies to preventing cyber fraud, as doing so requires vigilance on the part of all stakeholders. Knowledge workers need to be vigilant about business email compromise attacks while managers need to lead the way in tightening interaction with suppliers and other third parties. At the same time, all parties need to consider a cyber fraud threat model that looks both ways, at external cyber criminals and the insider threat.

Core to mitigating cyber fraud is the implementation of a zero-trust strategy that secures the identities that access cloud applications and data, the implementation of which must strike the right balance of enablement, security, and controls. Effective yet appropriate means of authentication, right-sized privileges, and machine-learning-powered monitoring are a few controls for a defense-in-depth approach central to preventing fraud. As with other aspects of cloud security, it is possible to secure agility with a collaborative approach to the people and processes of the digital enterprise.

The cultural shift to gain organizational alignment on the cybersecurity imperative applies to preventing cyber fraud, as doing so requires vigilance on the part of all stakeholders.

ORACLE KPMG

Research conducted in partnership with ESG