CYBERARK

CYBERARK GLOBAL ADVANCED THREAT LANDSCAPE 2019 REPORT

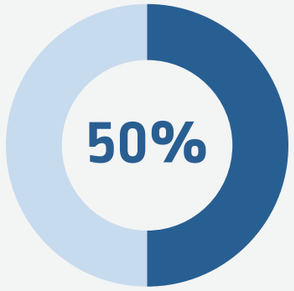
EXECUTIVE SUMMARY

About the CyberArk Global Advanced Threat Landscape 2019 Report

Welcome to the 12th annual edition of the CyberArk Global Advanced Threat Landscape Report. This year's report examines business leaders' engagement with cybersecurity as global organizations transition to true digital businesses, and continues our longstanding focus on the practice of privileged access security.

In total, 1,000 IT security decision makers were surveyed in early 2019, with respondents based in the US, UK, France, Germany, Singapore, Australia and Israel. The majority of respondents (88 percent) surveyed were manager level or above. Of those, 21 percent were C-level executives, while 35 percent represented companies of 3,000 employees or more.

Respondents were from organizations with at least 250 employees in any private and public sector (excluding consumer services). All respondents were interviewed online using a rigorous, multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.



agree that attackers can't be prevented from penetrating the network each time they try.

Strategic Security Investments to Break the Cyber Kill Chain

Cyber threats – from cyber criminals, competitors, nation states, insiders and other actors – are a given, and the cost to business is increasing. The survey shows that over half (53 percent) have suffered business impact from an attack in the previous three years and that 50 percent agree that attackers can't be prevented from penetrating the network each time they try. Meanwhile, the impact and demands of digital transformation are creating the need for more risk-aware security investments.

Experienced organizations know that compromised privileged access provides attackers a shortcut to their goals. The survey reveals a shift in security spend, extending beyond perimeter protection to also contain attacker movement inside the network at critical points along the cyber kill chain. More than a quarter of planned security budgets will address preventing privileged escalation and subsequent lateral movement (28 percent on average when combined) in 24 months' time – a good indication of increasing security robustness. Additional data revealed:

- 78 percent said hackers represented one of their top three greatest threats to critical assets
- Respondents said external attacks such as phishing were among their greatest security risks (60 percent)
- 20 percent report that their organization runs regular Red Team exercises (the average frequency being every three months)

CyberArk View

As businesses embrace digital transformation, the increasing reliance on automation and investments in cloud and DevOps processes mean added pressure on security teams. Often, the need to respond to rapidly changing markets leads to security being overlooked or deprioritized, even as an expanded or altered attack surface increases the risk of security incidents.

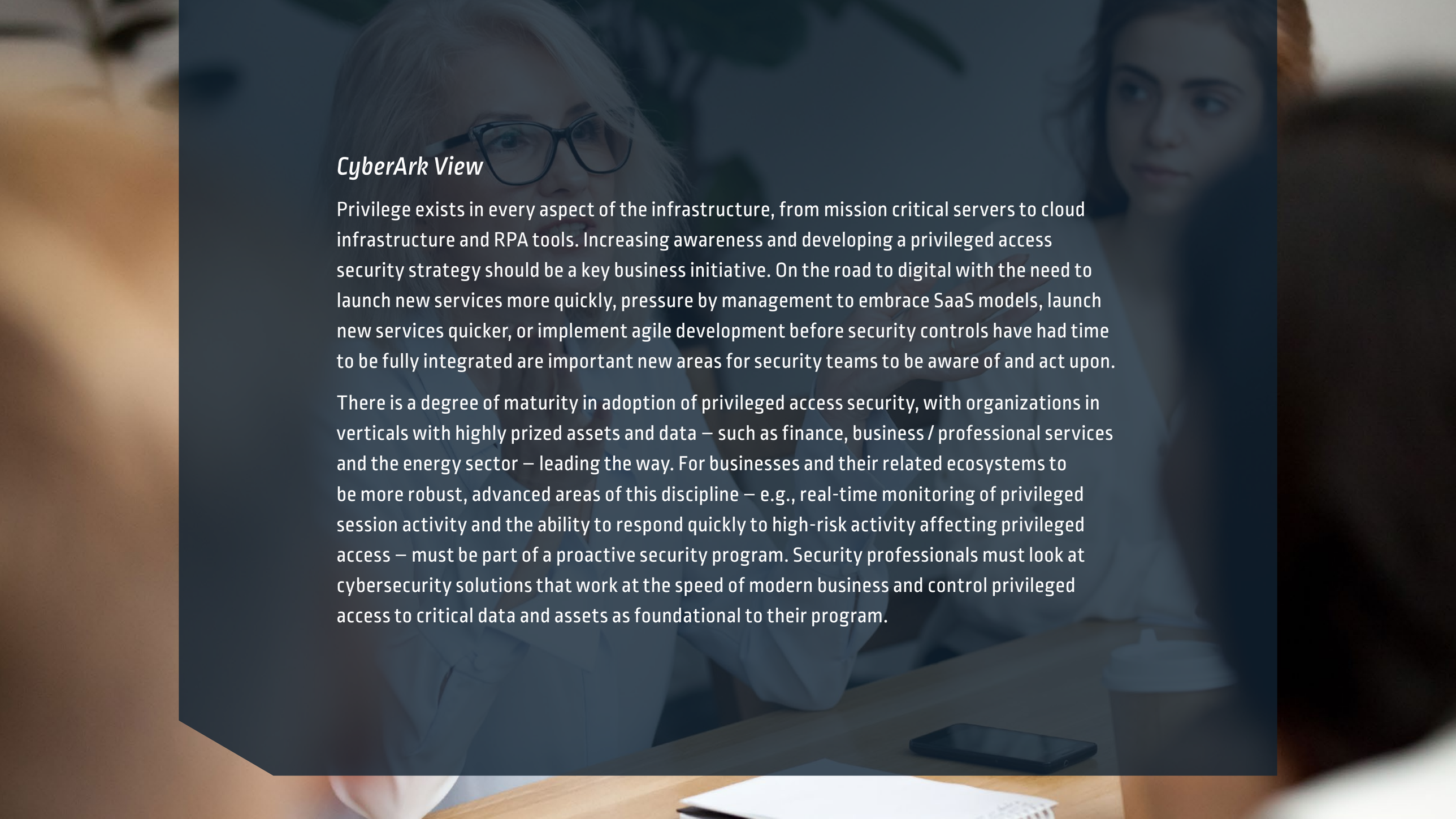
With attacks continuing unabated, it is critical to direct cyber investments toward security controls and skilled personnel that can combat attackers' ability to move laterally in the IT environment, compromise privileged credentials that allow them to gain control of targeted assets, and discover additional resources and assets to exfiltrate or compromise.

There was not one area we asked about where more than half of respondents reported that a privileged access security strategy was in place

Security Barriers to Digital Transformation and the Privilege Priority

We found that many organizations are stepping up to the challenge of controlling access to critical assets, with evidence that privileged access security strategies exist across certain aspects of the infrastructure, from mission critical servers to Internet of Things (IoT). While there is some visibility into where privilege exists across the IT environment – including user machines, robotic process automation (RPA), IoT, Infrastructure-as-a-Service (Iaas) and Platform-as-Service (PaaS) environments and more – there is an opportunity to drive greater awareness about the expanding privileged attack surface – especially across foundational digital transformation technologies.

- 84 percent agree that IT infrastructure and critical data are not fully protected unless privileged accounts, credentials and secrets are secured
- Yet, **only 35 percent have a privileged access security strategy for DevOps** or CI/CD pipelines and only 32 percent for the Internet of Things (IoT)
- In fact, **there was not one area we asked about where more than half of respondents reported that a privileged access security strategy was in place**



CyberArk View

Privilege exists in every aspect of the infrastructure, from mission critical servers to cloud infrastructure and RPA tools. Increasing awareness and developing a privileged access security strategy should be a key business initiative. On the road to digital with the need to launch new services more quickly, pressure by management to embrace SaaS models, launch new services quicker, or implement agile development before security controls have had time to be fully integrated are important new areas for security teams to be aware of and act upon.

There is a degree of maturity in adoption of privileged access security, with organizations in verticals with highly prized assets and data – such as finance, business / professional services and the energy sector – leading the way. For businesses and their related ecosystems to be more robust, advanced areas of this discipline – e.g., real-time monitoring of privileged session activity and the ability to respond quickly to high-risk activity affecting privileged access – must be part of a proactive security program. Security professionals must look at cybersecurity solutions that work at the speed of modern business and control privileged access to critical data and assets as foundational to their program.

Compliance Resistance and Reactive Mindsets Persist

Despite the shift toward more risk-aware security investment and practices, persisting levels of cybersecurity inertia and reactive mindsets continue to put sensitive data, infrastructure and assets at risk. A troubling 41 percent of respondents said their organization would prefer to pay a fine for losing data after a successful cyber attack rather than change their security policy.

Our study examines organizations' preparedness to meet increasing compliance demands and avoid record-breaking financial penalties.

- **EU General Data Protection Regulation (GDPR):** Less than half (46 percent) are completely prepared for breach investigation and notification in the mandated 72-hour time period
- **California Consumer Privacy Act (CCPA):** Only 37 percent are ready for this regulation to take effect in 2020 – though 39 percent are actively working to be able to meet it
- **Australia's data breach notification law:** 62 percent of Australian respondents reported that their organization was completely prepared, more than a year after it came into law

CyberArk View

While only investing in security to meet compliance regulation is not necessarily good news for overall cybersecurity posture, enforcement of regulations like GDPR and CCPA, plus the prospective amendments to Singapore's Personal Data Protection Act in 2019, are meaningful and comprehensive requirements that require significant investment for organizations.

Often, the time-specified need to notify to a supervisory authority following a data breach will mean businesses will not only need to detect and respond to breaches quickly, but also be able to account for what records, how many, likely impact and steps taken to mitigate the breach. To rapidly and accurately report on a breach – or better yet, detect a threat before a breach occurs – robust operational and security controls are necessary.

CYBERARK GLOBAL ADVANCED THREAT LANDSCAPE 2019 REPORT

THREAT PERCEPTION, SECURITY INVESTMENT AND THE CYBER KILL CHAIN

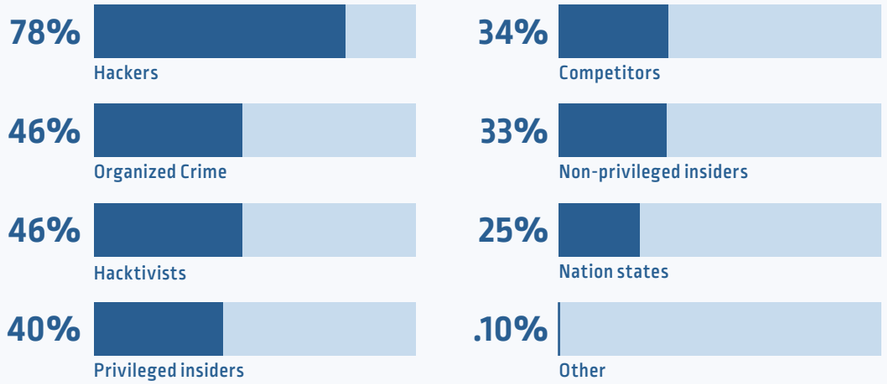
The threats to organizations from cyber crime, attackers, nation states, malicious insiders and simple human error are now an established fact of business life. The cost to business is increasing along with the number of successful attacks.

According to independent research, the average number of security breaches in the last year grew by 11 percent from 130 to 145. In the same period, the average cost of cyber crime increased US$1.4 million to US$13.0 million.[i] Additionally, a global median attacker dwell time of 78 days translates into elevated risk.[ii] Survey respondents demonstrate strong awareness of these trends, with 82 percent agreeing that their organization prioritizes cyber risk as an important business investment.

In fact, over half (53 percent) report having suffered impact to their business from a cyber attack in the previous three years and **50 percent agreed that attackers can't be prevented from breaking in each time they try**. This view is shared by attackers: A 2018 survey by Nuix[iii] found that 71 percent of attackers believed that they could breach the perimeter of a target within 10 hours.

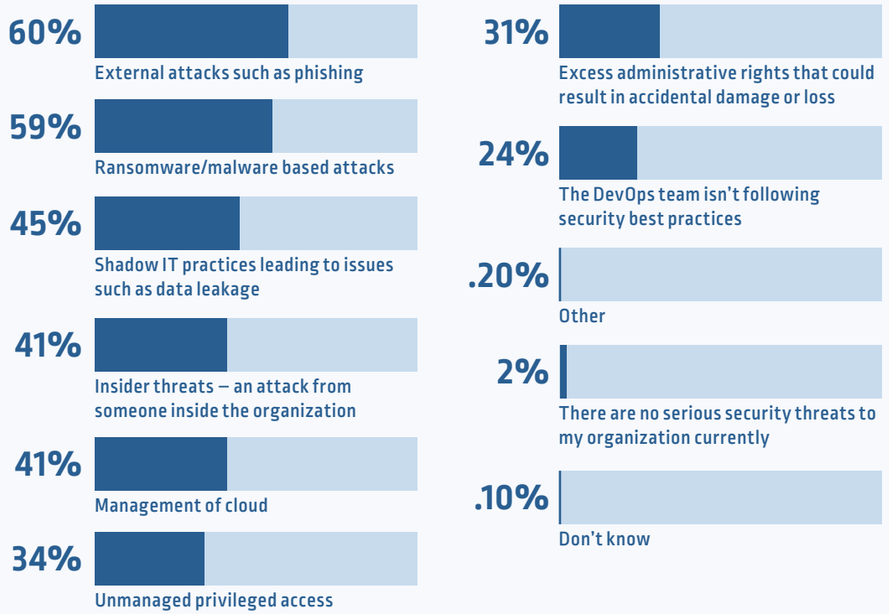
In terms of threat actors, hackers represent the most clear and present danger, with **78 percent of respondents stating they were among their top three greatest threats to critical assets**. Organized crime (46 percent) and hacktivists (46 percent) also ranked highly – while attempted attacks from actual market competitors (34 percent) was a surprise threat concern this year.

Which of the following threat actors poses the greatest security risk to your organization's critical assets?



Combination of responses ranked first – third

Which of the below do you believe are the greatest security risks to your organization currently?



Survey responses showed that respondents perceived a range of security risks. External attacks such as phishing were named as the top security risk, cited by 60 percent. This was followed by ransomware / malware-based attacks (59 percent), shadow IT practices (45 percent), insider threats (41 percent), management of cloud (41 percent) and unmanaged privileged access (34 percent). These techniques can, of course, be part of the same attack; unmanaged privileged access is often exploited by malicious insiders, for example.

For many organizations, the most damaging scenario is attackers having the ability to access high-value data and assets. Not surprisingly, the majority (92 percent) of respondents agreed that it is critical to implement security controls that protect critical assets from threats that have penetrated the network perimeter – but the key is to understand where to invest. Is cybersecurity spend in the right areas and does it effectively protect a business's most valuable assets?

To answer that question, it's important to first understand the cyber kill chain.

STRATEGIC SECURITY INVESTMENTS TO BREAK THE CYBER KILL CHAIN

The motivations for cyber attacks can vary: organized crime typically seeks data and assets that can be monetized; hacktivists wreak havoc based on ideology; nation states may be after intellectual property, or trying to create social disruption by making citizens question information or trusted processes.

Whatever the motive, attackers first conduct reconnaissance or study successful attacks on similar organizations to chart a step-by-step pathway to execute the attack and achieve their target goal. While each attack has its differences, one thing remains constant: attackers will consistently seek the path of least resistance.

If they can target a highly privileged individual's machine at the outset to accelerate the attack, they will. That's why organizations must carefully analyze their environment, consider various attack methodologies and take a risk-prioritized approach to securing the potential steps along this pathway to break the cyber kill chain.

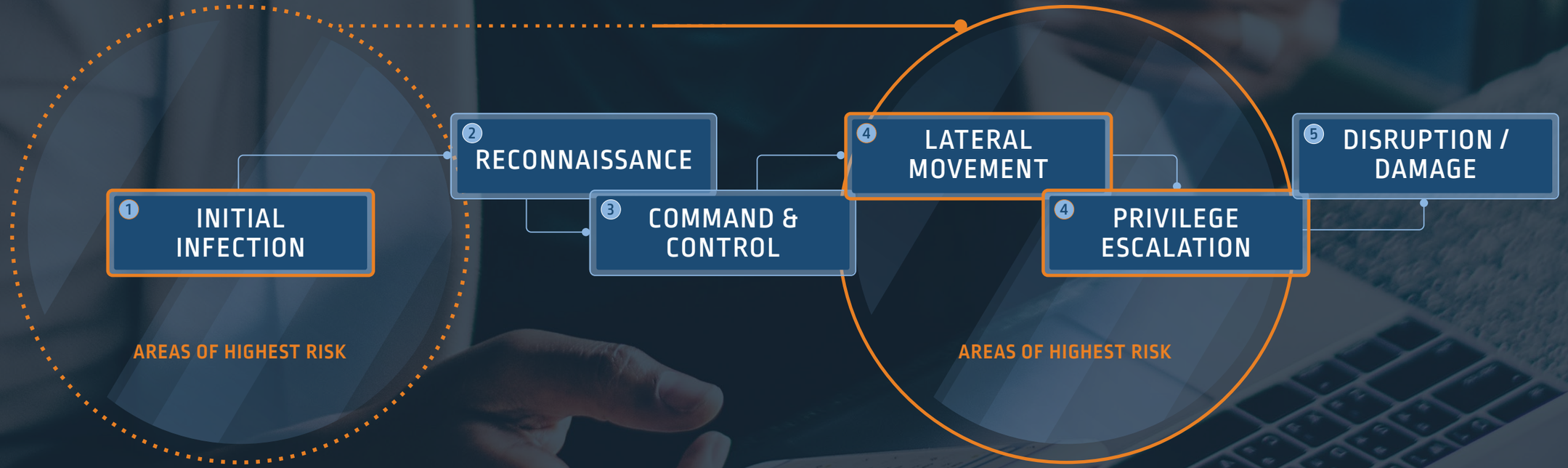
With many years of experience analyzing data breaches and cyber attacks worldwide, the CyberArk Labs team defines the critical steps in any attack – and the points where the chain can be broken – as follows:

Cyber Kill Chain Steps

1. **Initial infection** is the moment the attacker establishes a foothold into the target by compromising an endpoint such as a desktop, laptop, mobile device or server. This represents one of the most vital points in the kill chain.
2. **Reconnaissance** starts early in the kill chain and continues throughout the attack. Security teams face challenges in not only detecting network probing, but also rapidly differentiating between legitimate information gathering and actual threats.
3. **Command and control** communications are often difficult to detect. Attackers utilize social networks and legitimate services that encrypt data, making inbound commands and outbound data nearly invisible to SOC teams.
4. **Privilege escalation and lateral movement** go hand-in-hand and represent the critical point in which the attacker gains access to credentials needed to get into a specific system, then begins moving toward their target. During this phase, the attacker is exposed and both the target (e.g., databases, systems, cloud infrastructure) and the means (e.g., compromised credentials, vulnerable software) are revealed. But to detect the threat, the organization must have a strong handle on what legitimate communications and authentication look like – or the attacker can easily slip under the radar.
5. **Disruption / damage** is the outcome of a successful attack, and represents the end of the kill chain. By successfully navigating the network or cloud environment and gaining access to target systems and data, the attacker's hold on the network may be tight enough to overcome security controls. Ransomware and data leaks are some of the most noticeable consequences of recent breaches.

ATTACKERS SEEK TO SHORTCUT THE PATH TO PRIVILEGED CREDENTIALS COMPROMISE

The Cyber Kill Chain



24% of total planned security spend in the next 24 months

28% of total planned security spend in the next 24 months

In examining cyber kill chain investment, the survey shows **that organizations plan to spend more than a quarter of their total security budgets on preventing privileged escalation and subsequent lateral movement (28 percent on average when combined) in 24 months' time**.

The largest single planned investment is the prevention of initial infection (24 percent on average), which could include preventing malware from acquiring the privileges required to persist. That was followed by prevention of disruption/damage (18 percent on average); prevention of reconnaissance (15 percent on average); and spend on prevention of command and control (15 percent on average).

This heightened focus on security that extends beyond the perimeter to contain attacker access and movement and break the cyber kill chain is positive news. Effective cybersecurity means understanding that attackers will eventually get in and establishing a critical layer of IT security to protect data, infrastructure and assets across the enterprise – on premises, in the cloud, on endpoints and throughout the DevOps pipeline – for when they inevitably do.

Privileged Access Security Adoption Trends

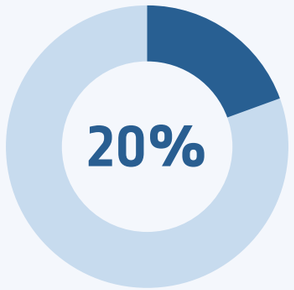
While 89 percent of organizations have implemented – or plan to implement – new measures for managing privileged access in the last two years, it was clear (as the graph shows) that most organizations were some way from fully adopting the discipline.

60 percent use a privileged access security solution to store and manage passwords, one important aspect of a privileged access security strategy.

Top three privileged access security measures / focus areas introduced:

Companies in verticals with highly sought-after assets and data, such as finance, business / professional services and the energy sector, led the way in privileged access security program implementation.

Healthcare, utilities, energy and other companies considered critical infrastructure reported high levels of implementation in advanced areas of privileged access security.



of respondents report that their organization runs regular Red Team exercises

The survey also shows a growing maturity towards investment in security controls, with 63 percent taking a proactive approach – meaning they identify vulnerable data or assets and ensure that the necessary controls are in place to reduce exploitation. In ranking these investments by perceived ROI,[1] 69 percent cited data encryption in their top five, 65 percent named identity and access control, and 62 percent identified email and web browser protection. Along with those investments, 20 percent of respondents report that their organization runs regular Red Team exercises (the average frequency being every three months).

France, Australia, the US and Singapore (all at 68 percent) are the leaders in practicing proactive security. Across verticals, the construction and energy sectors were most prominently focused on proactivity, with both at 72 percent.

[1] By this we mean the risk to critical assets mitigated per dollar spent, i.e. which delivers the most efficient spend

PRIVILEGED ACCESS SECURITY MUST BE A STRATEGIC SECURITY PRIORITY

High-profile breaches have demonstrated time and again that attackers follow the path of least resistance, almost always targeting privileged credentials they can exploit to escalate access and move laterally until they reach their target.

Many organizations view privileged access security as foundational to an effective cybersecurity program, as evidenced by the increase in planned security investments for this critical area of the cyber kill chain.

Similarly to 2018's Global Advanced Threat Landscape Survey findings, **the majority of respondents (84 percent) agree that IT infrastructure and critical data are not fully protected unless privileged accounts, credentials and secrets are secured**.

However, there are some contradictions: While 84 percent of respondents agree that their organization does a good job of managing privileged access throughout the organization, **only 46 percent of organizations have a privileged access security strategy for something as fundamental as protecting mission critical servers (e.g., domain controllers).** The compromise of a domain controller represents a total loss of control of the network to an attacker.

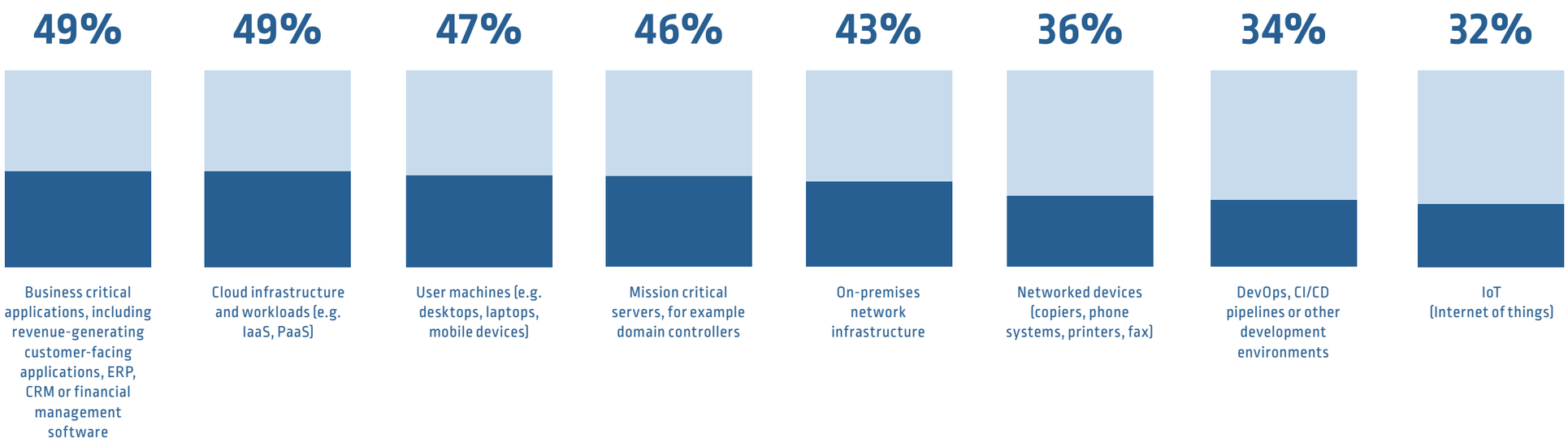
This underscores an opportunity to further educate organizations about where privileged access controls can be applied to bolster overall cybersecurity posture.

PRIVILEGE IS EVERYWHERE: DIGITAL TRANSFORMATION AND RISK

The survey shows that while organizations are embracing digital transformation to maximize operational efficiency and business value, many have not yet integrated privileged access security controls into these critical initiatives, despite recognizing the risks.

In looking at the foundational technologies of digital businesses, only 35 percent have a privileged access security strategy for DevOps or CI/CD pipelines and only 32 percent for the Internet of Things (IoT). In fact, there was not one area we asked about where more than half of respondents reported that a privileged access security strategy was in place.

For which of the below environments and devices does your organization have a privileged access management strategy in place?



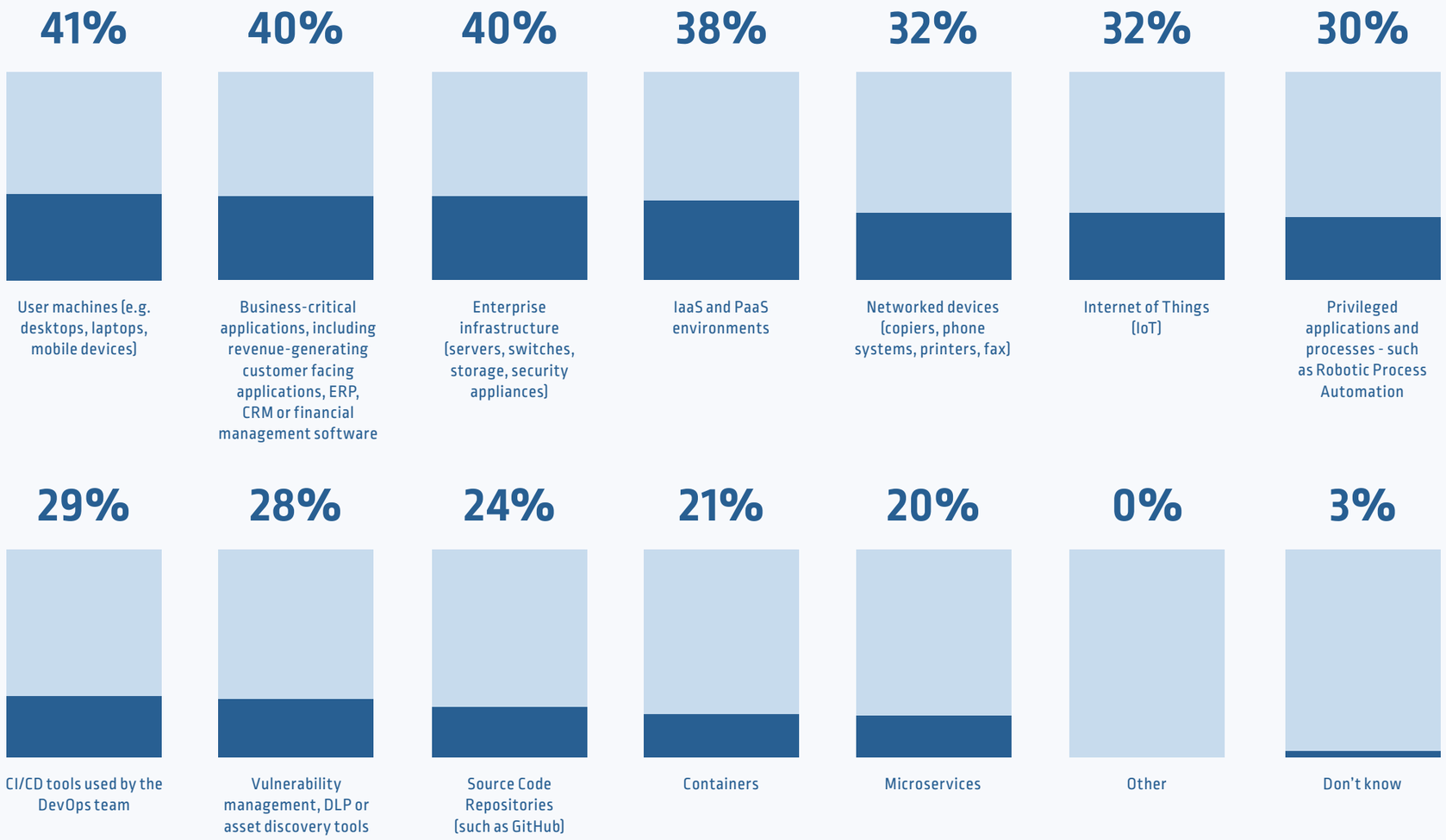
We asked where privileged accounts, credentials and secrets exist in various areas of their organization's IT environment, including those associated with digital transformation. **While many respondents understood that privileged credentials exist within an array of technologies that we asked about, overall awareness was not high**.

Only 20 percent understood that privileged accounts, credentials and secrets exist in microservices, 21 percent that they exist in containers and just 30 percent believed that they are present in privileged applications and processes such as Robotic Process Automation (RPA).

There is an opportunity, therefore, to be drive more knowledge and understanding about the expanding privileged attack surface – especially across foundational digital transformation technologies.

There was not one area we asked about where more than half of respondents reported that a privileged access security strategy was in place, from business critical applications (only 49 percent had a strategy in place) to DevOps environments (35 percent)

Where do you believe privileged accounts, credentials and secrets exist in your organization's IT environment?



Once attackers obtain privileged credentials and secrets, they can gain full access to DevOps pipelines, sensitive databases and even an organization's entire cloud. One only has to look at recent breaches – Uber, CityComp, SingHealth and many more – to see how these new digital technologies are translating to greater cyber risk for the business.

The majority of surveyed organizations recognize these threats and reported plans to increase risk-aware security investments to better protect their digital transformation initiatives: 52 percent said they planned to increase investment in securing the cloud, 47 percent in IoT, and 42 percent in better securing and managing SaaS applications.

REGULATORY ENFORCEMENT AND IMPACT ON ORGANIZATIONAL BEHAVIOR

Despite this progress, 35 percent of organizations are taking a more passive or reactive approach to cybersecurity, saying they only spend on security when they have to in order to meet compliance mandates, to keep pace when a competitor makes an investment, or after an attack or breach occurs. As identified in the 2018 report, persisting levels of cybersecurity inertia and failure to learn from past incidents continue to put sensitive data, infrastructure and assets at risk.

A surprising 41 percent of respondents said their organization would prefer to pay a fine for losing data, rather than change their security policy after experiencing a successful cyber attack. Perhaps organizations have analyzed and found the cost of security investments to outweigh the cost of non-compliance. Or, perhaps they're betting that regulatory bodies won't enforce fines. More likely, however, is that they've failed to account for costs that are more difficult to quantify such as brand damage, erosion of trust, and lost or reduced customer loyalty.

The survey examined major regulations around the world including:

- **EU General Data Protection Regulation (GDPR):** Since the law went into effect in May 2018, less than half (46 percent) are completely prepared for breach investigation and notification in the mandated 72 hour time period
- **Australia's Data Breach Notification Law:** 62 percent of Australian respondents reported that their organization was completely prepared more than a year after it came into law
- **California's Consumer Privacy Act (CCPA):** Only 37 percent are ready for this major piece of legislation slated to take effect in 2020, though 39 percent are actively working to meet requirements

HOW GLOBAL ORGANIZATIONS MANAGE CYBER RISK PRACTICES

While only five percent of respondents do not measure or report on cyber risk at all, **29 percent of security leaders still use a 'traffic light' approach to communicate risk to boards and executives**.

There are many different ways of assessing the strength of a cybersecurity risk program. When asked what drove decision-making in these areas, about one-third (35 percent) said they had defined an acceptable level of loss exposure. This reveals an opportunity for greater maturity around building strategies that take the financial "ripple effect" of a successful attack into account – rather than just trying to identify and mitigate one-off vulnerabilities.

On the flip side, 52 percent stated that cyber risk programs are assessed through a compliance exercise. But as we've seen, compliance-driven security – from check box to mandated controls (such as those contained in the SWIFT Customer Security Program) – is rarely good enough.

Assessing Cyber Risk

The survey shows that nearly all (94 percent) organizations use a form of risk assessment tool or framework to assess cyber risk. For example, 28 percent of respondents use the FAIR (Factor Analysis of Information Risk) methodology to measure, manage and report on information risk from the business perspective. Some of the other frameworks we asked about, like TARA (Threat Agent Risk Assessment) and NIST RMF (National Institute of Standards and Technology's Risk Management Framework), are helpful in identifying vulnerabilities and suggesting mitigation strategies, but do not evaluate the financial impact of vulnerabilities on the business.

CONCLUSION

The CyberArk Global Advanced Threat Landscape 2019 Report shows that organizations demonstrate solid awareness of cyber risks and the potential corresponding damage to the business. They increasingly understand that the greatest risk comes from an inability to contain attackers from affecting or accessing critical data and assets – not from the initial attacker infiltration, which is nearly impossible to stop.

At the same time, business and security leaders know that changing business processes and new technology investments to support digital transformation mean increased risk. They recognize the need to embrace the new models of security that digital transformation demands, but the challenge is to accrue the benefits without expanding the attack surface.

Organizations need to make the right decisions on security spending for maximum return and cyber risk reduction. Fortunately, signs indicate that security professionals realize this. The survey results show a solid understanding of the role that privileged access security plays in protecting critical assets, infrastructure and data – from traditional on-premises systems to cloud and DevOps environments.

But the survey also highlights some glaring contradictions. It is not possible to effectively and confidently identify, manage and secure all areas in which privilege exists, while at the same time not having a privileged access security strategy in place for fundamental components such as business critical applications, development environments and domain controllers.

There continues to be an opportunity to further educate security leaders on the expanding, privilege-related attack surface to help them make informed, risk-prioritized technology investments that achieve more robust protection of critical data and assets to, ultimately, better support the business.

About CyberArk

CyberArk (NASDAQ: CYBR) is the global leader in privileged access security, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. CyberArk delivers the industry's most complete solution to reduce risk created by privileged credentials and secrets. The company is trusted by the world's leading organizations, including more than 50 percent of the Fortune 500, to protect against external attackers and malicious insiders. A global company, CyberArk is headquartered in Petach Tikva, Israel, with U.S. headquarters located in Newton, Mass. The company also has offices throughout the Americas, EMEA, Asia Pacific and Japan. To learn more about CyberArk, visit www.cyberark.com, read the CyberArk blogs or follow on Twitter via @CyberArk, LinkedIn or Facebook.

[i] Accenture Cost of Cybercrime Study, March 2019: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study
[ii] Mandiant M-Trends 2019, March 2019: https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html
[iii] Nuix Black Report, April 2018: https://www.nuix.com/black-report/black-report-2018

CYBERARK®

07.19. Doc. 373314832