2023 Half Year Cybersecurity Reflection

By PwC Kenya

pwc

Executive Summary

The cybersecurity landscape has continued to witness unprecedented challenges, with cybercriminals becoming increasingly sophisticated and exploiting vulnerabilities in new and innovative ways. Our commitment to ensuring the security and resilience of systems, data and operations has never been stronger.

"According to PwC GECs 2022, technology developments such as the rise of AI, for example Chat GPT, has made phishing fraud more accessible to criminals and compounded the risks. 22% of the respondents in East Africa reported having encountered instances of cybercrime. They also observed that cyber criminals are becoming more sophisticated and perpetrating fewer but more lucrative cyber-attacks."

This report provides an analysis of the key cybersecurity threats and insights observed throughout the first half of 2023. It offers valuable insights into emerging threats, indicators of compromise and critical areas for organizations to focus on in fortifying their cybersecurity defenses in the second half of the year.

Over **16,000** vulnerabilities Discovered

Distributed Denial of Service attacks **DDOS** intensify in Q2.

Artificial Intelligence **(AI)** exposes organisations to sensitive data leakage and **privacy violations**

Cloud Security challenges intensify as attackers demonstrate advanced understanding of cloud architecture.

Ransomware continues to plague organisations - criminals adopt double extortion tactics.

> The cybersecurity landscape has continued to witness unprecedented challenges, with cybercriminals becoming increasingly sophisticated and exploiting vulnerabilities in new and innovative ways

Key themes and highlights from the report are as follows:

1 Over 16,000 Vulnerabilities Discovered

Over 50% of vulnerabilities reported in the Common Vulnerabilities and Exposures (CVE) database were high and medium risk vulnerabilities. These vulnerabilities presented risks such as unauthorized access, denial of service or manipulation of data within the affected systems.

2 Cloud Security Challenges Intensified

The challenges associated with securing cloud environments grew. Misconfigurations, inadequate access controls and weak security hygiene were the common themes. On the other hand, attackers demonstrated advanced understanding of cloud architecture through the different attacks reported.

3 Ransomware Continues to Plague Organizations

Ransomware attacks remained a prominent threat, targeting organizations of all sizes and across various sectors. Cybercriminals adopted double extortion tactics, combining encryption with data theft and subsequent threats to leak sensitive information, resulting in substantial financial losses and reputational damage for victims.

4 Data Privacy and Artificial Intelligence (AI)

The integration of AI technologies introduced new security and data privacy risks. Organizations faced the challenge of reducing data leakage through posting sensitive data on AI systems and staying ahead of AI based phishing attacks.

5 Denial of Service Attacks intensifies

The second quarter of 2023 witnessed a surge in meticuluously planned and customised DDoS attack initiatives. These activities encompassed DDoS assaults orchestrated by groups such as REvil, Killnet and Anonymous Sudan.

As we plan for the final half of 2023, organizations must prioritize comprehensive security measures, including robust incident response capabilities, supply chain risk management, cloud security practices, and privacy compliance.

By adopting a proactive and collaborative approach, organizations can navigate the dynamic threat landscape, enhance their cybersecurity posture, and safeguard their critical assets and sensitive information in the face of emerging cyber threats.

28%

of East African respondents reported experiencing increased risk in Cybercrime as a result of the COVID-19 pandemic.

50%

of vulnerabilities reported in the Common Vulnerabilities and Exposures (CVE) database were high and medium risk vulnerabilities.

2. Cyber Threat Landscape in Q1 & Q2:

Identifying Key Threats and Recommendations for Business Leaders

This section provides an overview of the top vulnerabilities observed in the first half of the year, with a focus on vulnerabilities that scored 9.0 and above on CVE list. We highlight top vulnerabilities recorded in firewalls, Network Access Control (NAC) systems, MOVEit Transfer, Microsoft Azure and network switches. The aim is to equip business leaders with insights on potential impacts of these threats, along with actionable recommendations to bolster their organization's cybersecurity posture.

> We highlight top vulnerabilities recorded in firewalls, Network Access Control (NAC) systems, MOVEit Transfer, Microsoft Azure, and network switches.

2.1 330,000+ firewalls expose companies to attacks

Critical security flaw (CVE-2023-33308) impacting Fortinet FortiOS and FortiProxy posed a significant risk to over 200,000 FortiGate firewall instances reachable from the internet. Furthermore, the XORtigate vulnerability (CVE-2023-27997) left more than 330,000 FortiGate firewalls exposed, particularly in industries such as government, manufacturing, and critical infrastructure sectors, making them susceptible to severe risks and threats. In addition, a vulnerability in FortiNAC (CVE-2023-33299) exposed organizations to unauthorized access to network resources and data breaches. Successful exploitation of these flaws exposed organizations to unauthorized access, data breaches, disruption of critical services and even full network compromise. Prompt patch deployment and regular security assessments were noted to be crucial in mitigating the above risks and protect against potential attacks.

2.2 MOVEit vulnerability

Organizations using MOVEit Transfer, a widely used managed file transfer application, faced a critical vulnerability (CVE-2023-34362) that allowed threat actors to steal sensitive data and even launch ransomware attacks. This security flaw targeted MySQL database engines, potentially compromising sensitive information. Prompt patch deployment and regular security assessments were noted to be crucial in mitigating the above risks and protect against potential attacks.

2.3 Cloud infrastructure abuse

Cloud environments saw an increase in abuse during the first half of 2023, with threat groups exploiting the Microsoft Azure serial console infrastructure to install third-party remote management tools. Misconfigurations in cloud environments continue to pose a significant risk, leaving assets vulnerable to malicious actors. Businesses should prioritize proper cloud security configurations and access controls to mitigate such threats.

2.4 Denial of service attacks

The second quarter of 2023 was characterized by thought-out, tailored, and persistent waves of DDoS attack campaigns on various fronts, including: Multiple DDoS offensives orchestrated by groups such as Anonymous Sudan, REvil, and Killnet. These attacks relied on access to multiple virtual private servers (VPS) in conjunction with rented cloud infrastructure, open proxies and DDoS tools.

“The second quarter of 2023 was characterized by thought-out, tailored, and persistent waves of DDoS attack campaigns

2.5 Flaws in Small Cisco Business Switches

A series of security flaws affecting the web-based user interface of Small Cisco Business Switches exposed businesses to potential unauthorized code execution and denial-of-service (DoS) attacks. Applying the released software updates is critical to addressing these vulnerabilities and reducing potential threats.

As cyber attackers continue to target unpatched systems, businesses must recognize that poor or inconsistent patching regimes remain a key factor behind successful intrusion. Many successful attacks exploit vulnerabilities that manufacturers have already remediated, making timely implementation of updates essential.

We recommend that organizations prioritize defense in depth and patching in their security strategies. By taking proactive measures to safeguard their networks, businesses can raise the barrier to entry for attackers, ensuring a resilient and protected digital environment.

Data Heists in the Cloud: Unveiling the Invisible Threats

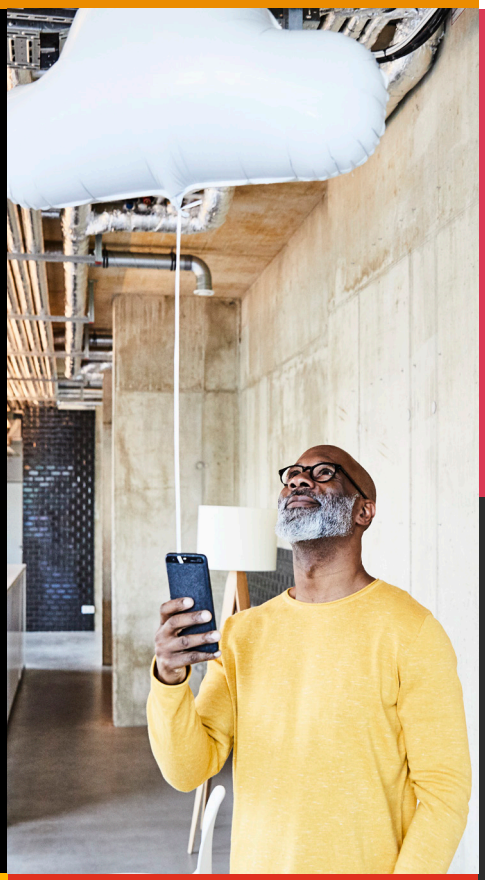
As businesses increasingly embrace cloud technology, cybercriminals are tailing closely behind, exploiting cloud vulnerabilities to execute data heists. Threat actors are keen on obtaining persistence in the cloud and exfiltrating sensitive data, posing significant challenges to organizations' security measures. In this section, we unravel the invisible threats that cloud environments faced over the last 6 months and shed light on the urgent need to bolster cloud security protocols.

Our Top 5 Notable Themes in Cloud Security

1

Credential harvesting in AWS, Azure, and Google Cloud Platforms:

Sophisticated attack campaigns have targeted major cloud service providers, particularly Amazon Web Services (AWS), Microsoft Azure and Google Cloud. Cybercriminals have employed techniques like the SCARLETEEL attack to exploit and extract credentials from within these cloud platforms. These stolen credentials grant unauthorized access, leading to data theft. In addition, deployment of crypto miners leads to rising cloud hosting costs for organizations



2

Credential leakage on cloud:

The secure remote connection service Azure Bastion became a target for attacks due to a cross-site scripting (XSS) vulnerability. This flaw allowed attackers to gain unauthorized access to user sessions, potentially resulting in unauthorized data access and disruptions. In addition, Azure Active Directory (Azure AD) misconfigurations exposed users' Office 365 data, posing a threat to sensitive information.

4

Email account compromise:

Attackers exploited a vulnerability in Microsoft Outlook to gain access to victims' network by simply sending a specially crafted email. Implementing Multi-Factor Authentication (MFA) and securing outbound TCP 445/SMB were seen to be essential preventive measures.

3

API compromise:

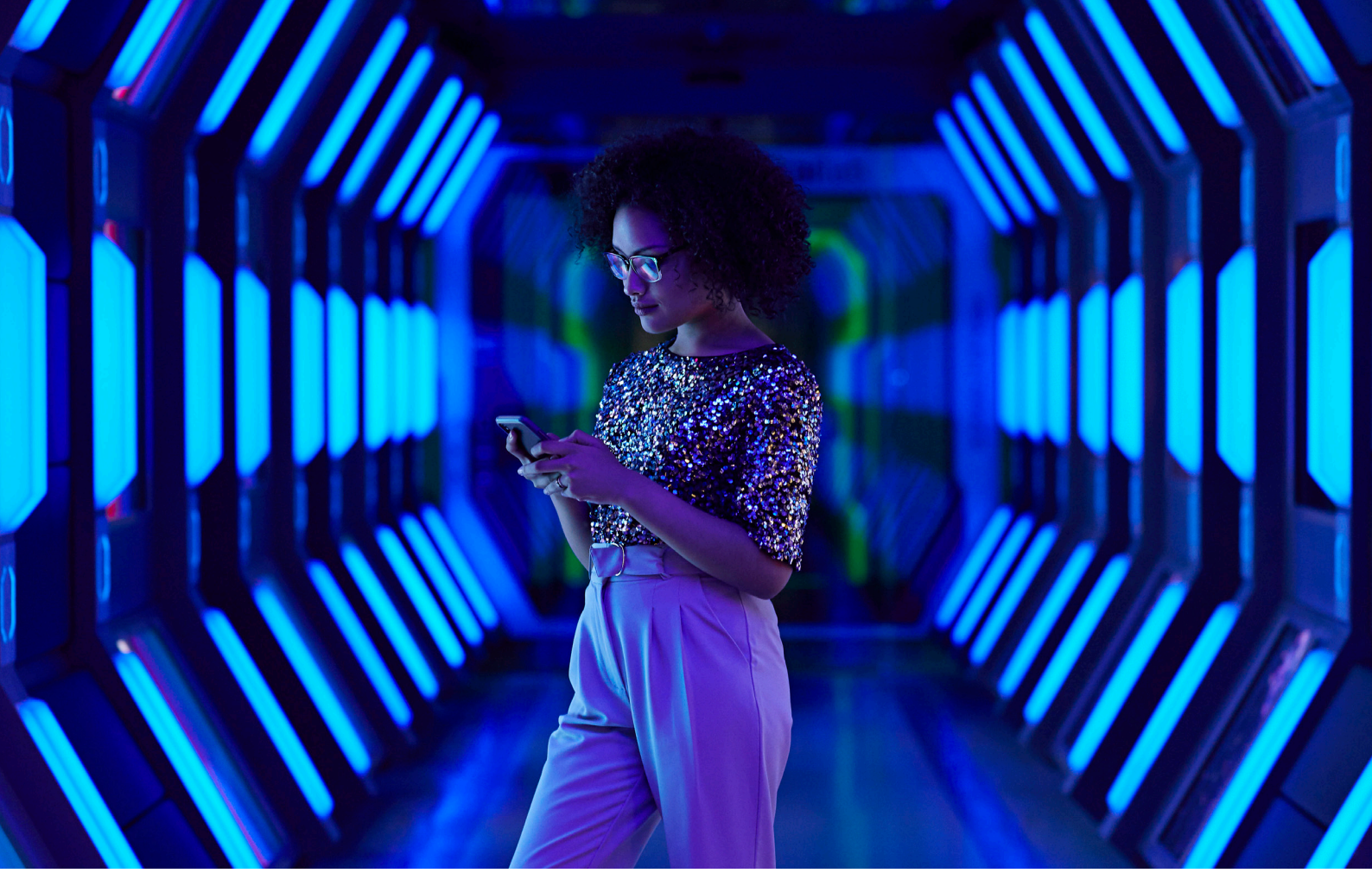
Attackers used malware (AlienFox) to target misconfigured servers to extract sensitive configuration files containing API keys and credentials from AWS, Google and Microsoft Cloud Services.

5

Virtual infrastructure compromise:

There was an increase in ransomware attacks targeting vulnerable ESXi hypervisor products. These systems typically host business critical data and compromise could lead to total operation shutdown.

The attacks witnessed in the cloud underscore the expertise of threat actors in cloud architecture, containers, serverless functions, and open-source infrastructures. Implementing the zero-trust principle and the principle of least privilege can significantly reduce the likelihood of compromise. Robust detections and alerts can help identify suspicious activities before they escalate. Organizations must prioritize strong identity protection capabilities to safeguard privileged accounts from misuse by rogue administrators.



3.1.1 Securing your Cloud-based Applications and Infrastructure:

As the cloud becomes the preferred hosting choice for businesses, hackers are adapting their attacks to exploit cloud vulnerabilities. To enhance cloud security in 2023, consider the following:

1. Cloud Security Strategy: Do you have a cloud security strategy to guide your cloud transformation journey?

2. People and Capacity: Does your team have the right competencies to handle cloud security challenges effectively?

3. Infrastructure Review: Have you configured your cloud infrastructure as per best practice?

4. Access Review: Have you implemented the principle of least privilege and segregation of duties?

5. Cloud Security Review: Have you conducted technical reviews to identify and address potential weaknesses?

By adopting a strategic and proactive approach to cloud security, organizations can thwart potential threat and safeguard their sensitive data effectively.

> The attacks witnessed in the cloud underscore the expertise the of the actors in cloud architecture containers, serverless functions and open-source infrastructure.

Rising Threat of Ransomware

Ransomware attacks have become a lucrative business for cybercriminals, with ransom demands soaring to alarming levels. These malicious actors encrypt files, holding them hostage and demanding hefty ransoms in cryptocurrency to prevent data exposure or dark web sales. Over the past few years, ransomware attacks have seen a dramatic increase, resulting in financial losses and damaging reputations for businesses. As business leaders, it is crucial to understand the key themes and impact of these attacks, and more importantly, to adopt effective strategies to fortify our organizations against these invisible threats.

Our Top 5 Notable Themes for Ransomware

1. The rapid evolution of Ransomware-as-a-Service (RaaS.
2. Companies without MFA are more vulnerable to Initial Access Attacks (IAA).
3. Prevention and early detection of credential dumping is crucial.
4. Small and medium sized business are attractive targets for Ransomware
5. Indicators of compromise that IT and security teams can check against.

Our Top 5 Notable Themes for Ransomware

- **The Rapid Evolution of Ransomware-as-a-Service (RaaS):**

The ransomware business model has evolved into a Ransomware-as-a-Service (RaaS) model. Affiliates pay for access to malware developed by operators, enabling them to launch attacks more efficiently. This streamlined approach has significantly reduced the time taken to complete a ransomware attack, escalating the threat posed by these malicious campaigns.

Bighead Ransomware

Initial access and distribution is through infected email attachments (macros), torrent websites and malicious ads.

Details: Appears as Microsoft Windows updates and Word installers. Once installed, the malware encrypts files and demands a ransom for decryption.

Affected platforms: Microsoft Windows.

Black Byte ransomware

Initial access is through exploiting Proxy Logon, a Microsoft Exchange Server vulnerability that allows attackers to bypass authentication and impersonate administrators.

Details: They exfiltrate data through WinRAR and other file-sharing sites and use tools such as Any Desk to gain a foothold on the victim machines.

Akira Ransomware

Initial access is through compromised credentials obtained from phishing or other rogue means to gain access to the victim's environment. Attackers also look for vulnerabilities in Multi-Factor Authentication (MFA) systems and Virtual Private Network (VPN) software.

Details: Once inside, they try to gather login information and move through your computer's network to gain more control and access to important information.

- **Companies without MFA are more vulnerable to Initial Access Attacks**

Most victim organizations, particularly from Akira attacks, did not have Multi-Factor Authentication (MFA) enabled on their VPNs. Implementing Multi-Factor Authentication (MFA) to replace password only authentication can enhance login security. Regularly auditing accounts for any MFA bypass exceptions, employing strong network perimeter controls, such as blocking inbound traffic from TOR networks, further fortifies the defense against ransomware attempts.

- **Prevention and Early Detection of Credential Dumping**

Credential dumping refers to the act of hackers gaining access to stored usernames and passwords, often from databases or local storage, through vulnerabilities or bugs. This allows the attackers to gain more foothold on the network. By implementing Multi-Factor Authentication (MFA) organizations can thwart credential dumping attacks. In addition, deploying endpoint Detection and Response (EDR), which have built-in capabilities to detect and counter these threats is essential.

- **Small and medium sized business as Attractive Targets:**

Ransomware attackers do not discriminate based on the size or industry of organizations they target. The attackers behind Akira for example went after various types of businesses like schools, financial companies, manufacturing companies, real estate, and medical organizations. Ransomware attackers may specifically target SMBs because they often have fewer cybersecurity resources and may be more likely to pay the ransom to quickly regain access to their data. Therefore, all businesses must remain vigilant and prioritize cybersecurity measures to protect against these indiscriminate threats.

- **Indicators of Compromise that IT and security teams can check against include:**

Understanding the signs and clues that indicate a potential ransomware incident is essential for early detection and effective response. We have identified indicators of compromise from Trend Micro and FortiGuard as follows:

Other common Indicators of Compromise (IoCs) that have been associated with ransomware attacks include:

- Unusual file extensions such as. locky, cerber, crypt etc.
- Unusual outbound network traffic to known Command and Control (C2) servers.
- Use of PowerShell scripts to download and execute ransomware payloads.
- Malicious email attachments such as .exe, .js, which execute the ransomware when opened.
- Registry modifications.

Malware	Indicator of compromise
Big Head Ransomware	SHA256 Indicator of compromise 2a36d1be9330a77f0bc0f7fdc0e903ddd99fcee0b9c93cb69d2f0773f0afd254 39caec2f2e9fda6e6a7ce8f22e29e1c77c8f1b4bde80c91f6f78cc819f031756 40e5050b894cb70c93260645bf9804f50580050eb131e24f30cb91eec9ad1a6e 64246b9455d76a094376b04a2584d16771cd6164db72287492078719a0c749ab 6d27c1b457a34ce9edfb4060d9e04eb44d021a7b03223ee72ca569c8c4215438 9c1c527a826d16419009a1b7797ed20990b9a04344da9c32deea00378a6eeee2 ae927feae84239c7f56a2c49aadb02dc318ef4be2860353b6a2428bdbbf0ae71 bcf8464d042171d7ecaada848b5403b6a810a91f7fd8f298b611e94fa7250463 dcfa0fca8c1dd710b4f40784d286c39e5d07b87700bdc87a48659c0426ec6cb6
BlackByteNT Executable	SHA 1 Indicator of compromise c0950ebfa3a63c705ca813cfd28364aa1d90bb09 990a762a0a80da13e716653d9ee1b7f5dc1a0172 adf4aae5160b26370e4f90620e9b0edcbb56c432 c2366ca1f869cb3579641b2de5796cb92afb67a1 6dc9c0eb798f35c123beb8868321a5e754ee889c b026c447ab06ab07c7d0c1505785f7e47f1ef860 4edd62b710e82bc380aa77cb536338669a8e7e49
AKIRA Executable	SHA 1 Indicator of compromise 923161f345ed3566707f9f878cc311bc6a0c5268 c4d6c1fd4c1a702a2302cc62bce7d770e5b7369c

Ransomware attackers do not discriminate based on the size or industry of organizations they target.

How can companies reduce their exposure moving forward?

Continuous monitoring and automated response mechanisms are vital to detect and counteract ransomware attacks swiftly. Equally important is educating employees on phishing mitigation and recognizing potential threats. Investing in modern end point detection and response tools, vulnerability and incident management solutions equipped with automation and AI capabilities will fortify defenses and streamline incident response.
Business leaders must take a proactive stance against ransomware, adopting a multi-layered defense strategy. In doing so, they can effectively combat these evolving cyber threats and secure their organizations from the rising tide of ransomware attacks.

What's your organization's exposure to ransomware? Get PwC Ransomware Simulation Service to find out.

> Business leaders must take a proactive stance against ransomware, adopting a multi-layered defense strategy.

Data Privacy in an AI Driven World

"Data privacy is the right of individuals to control their personal information. Data privacy is far more than just the security and protection of personal data. It all boils down to how organizations are using that personal data." - PwC Kenya Data Privacy Handbook.

Our Top 3 Notable Themes for Data Privacy and AI

1. 6% of employees paste sensitive data into GenAI tools such as ChatGPT

AI solutions such as ChatGPT are being used by employers in activities such as drafting emails, review of documents, source code review and routine office functions. Research report by browser security company LayerX has identified that a significant number of employees (6%) are pasting sensitive data into GenAI tools, posing a serious threat of data exfiltration.

"The Samsung and ChatGPT leaks - a case for caution: Samsung reported three different leaks of highly sensitive information by three employees that used ChatGPT for productivity purposes. One of the employees shared a confidential source code to check it for errors, another shared code for code optimization, and the third shared a recording of a meeting to convert into meeting notes for a presentation. All this information is now used by ChatGPT to train the AI models and can be shared across the web."

2. Use of unverified AI Apps by employees - a case for caution

The risky integration of untrusted generative AI apps with an organization's technologies can lead to sensitive data loss and phishing attacks. A case reported in Q2 involved "GPT for GMAIL" an untrusted AI app that employees integrated with their Google Workspace environment. This app granted high permissions, including the ability to read, compose, send, and delete emails. This example highlights the security concerns associated with connecting unverified generative AI apps to core systems.

3. AI Tools used to launch business email compromise attacks

Attackers were seen to use sophisticated AI model, WormGPT to craft convincing phishing emails and social engineering attacks. The AI can remember previous conversations, making its responses even more convincing.

"WormGPT can craft a fake email to fool finance teams into sending money to the wrong account or administrators into sharing sensitive information."

The use of AI-powered apps presents significant security risks for organizations. The potential impact of these risks includes data breaches, unintentional data sharing, sensitive information, and intellectual property exposure, leading to reputational damage and financial losses.

To address these risks, data protection stakeholders should take proactive measures. They can start by:

- Assessing GenAI usage patterns within the workforce to identify potential areas of risk.
- Developing tailored data protection plans for GenAI usage.
- Conducting risk analyses to identify departments or areas most likely to experience data exposure.

To enhance the security of AI-powered apps, organizations can implement several key steps including:

- Establishing robust data protection policies such as data classification, encryption, access controls, and regular security audits.
- Educating employees about data sharing risks and responsible app use through training programs raises awareness and ensures compliance with organizational policies.
- Vetting and verifying the security and trustworthiness of generative AI apps before integration is essential to reduce risks.

Taking proactive steps is essential as AI technology continues to evolve and become accessible to a broader spectrum of cyber criminals, making data protection and security even more critical in today's digital landscape.

> "...the risks that come with mobile device loss or theft are even greater if workers do not follow their organization's security procedures or have weak protection for their applications.

Sectoral Outlook

This section explores the specific cybersecurity threats and risks that the financial, infrastructure and public sectors confronted in the last 6 months of 2023. By understanding these threats, organizations can implement robust security measures to protect their sensitive data, customer trust, and overall stability in an ever-changing threat landscape.

6.1 Financial Services Sector

Phishing and use of scripts to drain accounts

These attacks typically involve compromised trusted vendors, indirect proxy usage, and sophisticated techniques to steal credentials and orchestrate attacks.

Misconfigured virtual infrastructure, APIs and Cloud environments

are a target for attackers. The limited skillsets on cloud and API security exposes the financial services sector to DDoS and Man-in-the-Middle attacks.

Mobile device security

The risks that come with mobile device loss or theft are even greater if workers do not follow their organization's security procedures or have weak protection for their applications.

6.2 Infrastructure Industry

Critical infrastructure attacks:
Infrastructure industries, such as energy, transportation, and utilities, are at risk of targeted cyberattacks aimed at disrupting essential services leading to service outages, safety risks, and economic impact.

Supply chain attacks:
Infrastructure entities often rely on a complex supply chain, making them susceptible to supply chain attacks. Malicious actors can infiltrate third-party vendors and suppliers to gain access to critical systems and compromise the entire infrastructure network.

IOT attacks
The increasing adoption of Internet of Things (IoT) devices in infrastructure systems presents security challenges. Vulnerable IoT devices can serve as entry points for cyber attackers to infiltrate and compromise critical infrastructure networks, leading to potential service disruptions and operational risks.

6.3 Public Sector

Nation-state attacks:

The public sector is a prime target for nation-state-sponsored cyber-attacks aiming to steal sensitive government data, disrupt operations, or influence political agendas. These attacks can have significant geopolitical implications.

Data breaches and denial of service attacks:

Public sector entities handle vast amounts of sensitive citizen data. Data breaches and identity theft incidents can expose personal information, erode public trust, and lead to legal and financial consequences.

Supply chain attacks:

Public sector entities are vulnerable to supply chain attacks, where cybercriminals compromise the software or hardware supply chain to infiltrate government systems. Such attacks can lead to data breaches, information theft, and potential disruption of public services.

Looking Ahead - Priorities for Business Leaders

Top 3 Priority areas for Board and Executives

- **Establish a Cybersecurity Strategy and Framework:** Develop a robust cybersecurity governance strategy and framework that clearly aligns with your business growth needs on matters Cloud API integrations and overall digitization needs.
- **Quantify your cyber exposure through regular assessments:** Identify key cyber risk scenarios and develop tools and metrics that enable you to quantify the exposure, maturity, and potential financial loss. These metrics are key in ensuring that the board has visibility on the extent of cyber risk, key areas of exposure and the level of maturity and return on investments made.
- **Cyber insurance:** Much like having an insurance plan for other aspects of life, a cyber insurance policy provides coverage in the event of cyber-related losses. Board members should carefully evaluate their organization's cyber insurance needs balancing the level of self-insurance vs extent of externally sourced cover depending on the risk appetite and accessibility of cyber insurance. The coverage should be customized to address specific risks and potential financial repercussions arising from cyber incidents.

Top 5 Priority areas for technical teams

- **Identity:**

Implement Multi-Factor Authentication (MFA) - Require users to provide multiple forms of identification (such as passwords and biometrics) before granting access to sensitive systems or data. MFA adds an extra layer of security, reducing the risk of unauthorized access due to compromised credentials.

- **Protect:**

Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. It uniquely addresses the modern challenges of today's business, including securing remote workers, hybrid cloud environments, and ransomware threats.

- **Detect:**

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) - Deploy IDS and IPS solutions to monitor network traffic and detect suspicious or malicious activities. These systems can help identify potential threats in real-time, allowing for prompt response and mitigation.

- **Respond:**

Develop a well-defined incident response plan that outlines specific actions to be taken in the event of a cyber incident. The plan should include roles and responsibilities, communication procedures, containment measures, and steps for restoring systems.

- **Recover:**

Implement a robust data backup strategy to ensure critical data is regularly and securely backed up. In the event of data loss due to a cyber incident, organizations can recover their data from backups, minimizing downtime and losses.

Technical teams can adopt industry frameworks such as MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) which is a widely adopted framework and knowledge base that outlines and categorizes the tactics, techniques, and procedures (TTPs) used in cyberattacks.

Cybersecurity is a continuous journey that requires proactive efforts and a multi-faceted approach. By prioritizing governance, technical controls, people, and cyber insurance, business leaders can fortify their organizations against cyber threats. Moreover, fostering a cybersecurity-aware culture and staying updated on emerging threats are essential for maintaining robust cyber defenses in an ever-evolving threat landscape. Implementing these recommendations will not only safeguard sensitive data but also protect the organization's reputation and foster trust among customers and stakeholders.

Top 3 Priority areas for Board and Executives

Partner with us

Our range of cutting-edge cybersecurity services are designed to fortify your organization's defenses and ensure a robust security posture. With a team of seasoned experts and industry-leading tools, we offer a diverse portfolio of services that address key cybersecurity challenges identified in this report.

8.1 Strategy & Transformation:

- **Cyber Strategy Design:** Tailored strategies to align cybersecurity with your business objectives, ensuring proactive defense against evolving threats.
- **Cyber Maturity Assessment:** Evaluate your current security posture and identify areas for improvement to strengthen your cybersecurity capabilities.
- **Cyber Governance Review:** Ensure robust governance practices and compliance with industry standards and regulations.
- **Security Compliance Reviews:** Comprehensive assessments to meet regulatory requirements and industry best practices.
- **Third Party Risk Management:** Mitigate risks posed by vendors and partners with thorough third-party risk assessments.
- **Cyber Risk Quantification:** Identifying key cyber risk scenarios and developing tools and metrics to enable quantification of the cyber exposure and extent of potential financial loss.
- **Cyber Risk Insurance:** Carefully balancing the how you protect against the financial loss of a cyber event by assessing the extent of risk you can retain vs cover purchased vs accessibility of cyber insurance.

8.2 Offensive Security:

- **Network Security:** Identify and address vulnerabilities in your network infrastructure to prevent unauthorized access.
- **Web Application Security:** Conduct thorough testing to ensure your web applications are free from potential exploits.
- **Mobile Security:** Assess and enhance the security of your mobile applications and devices.
- **API Security:** Secure your APIs from potential breaches and protect sensitive data.
- **Cloud Security:** Implement cloud security measures to safeguard your data and applications in the cloud.

8.3 Crisis Simulation:

- **Red Team Exercises:** Simulate real-world attacks to identify weaknesses in your defenses and enhance incident response capabilities.
- **Ransomware Simulation:** Prepare your team to respond effectively to ransomware threats and protect your critical data.

Our team is committed to providing customized, innovative solutions that address your unique cybersecurity needs. With an emphasis on excellence, reliability, and customer satisfaction, we strive to be your trusted partner in safeguarding your digital assets.

Contact us today to discuss how our services can fortify your organization's cybersecurity posture and ensure a secure and resilient future.

Jamila Aroi
Partner, Consulting & Risk Services,
PwC Kenya
T: +254 020 2855575
E: jamila.aroi@pwc.com

Brencil Kaimba
Cybersecurity Manager,
PwC Kenya
T: +254 020 2855000
E: brencil.kaimba@pwc.com