techforce.co.uk

CYBER SECURITY REPORT

2024

#CYBERTRENDSUK2024

TechForce™ Cyber

Dear Readers,

As we move into 2024, the UK cyber landscape continues to be a dynamic space to review, where innovation meets with ever-evolving threats in cyber.

In this digital era we live in, where our interconnected world presents both unprecedented opportunities and challenges, staying ahead of the cybersecurity curve is not merely a goal but a necessity. This report serves as a road map, guiding organisations through the wide range of cyber threats and illuminating the strategic avenues to improve our digital defences.

Zero Trust Architecture, the infusion of Artificial Intelligence and Machine Learning into our defence strategies, and the imperative adoption of quantum-resistant cryptography—these are not just trends but imperatives in the ever-escalating cyber arms race. In the following pages, we explore these trends and their implications on the digital landscape. From cloud security evolvement to the resilience required to combat the rise of ransomware, each section is crafted to empower organisations with key insights. As someone who is passionate about your organisation's digital resilience, I encourage you to not only read this report but to engage with its recommendations, integrate its insights, and embark on a journey of continuous improvement in your cybersecurity posture. As we navigate the complexities of 2024, let us strengthen our defences, cultivate a culture of cyber resilience, and together, defy the ever-advancing threats that seek to compromise our digital future. Wishing you a secure and successful 2024.

Sincerely,

JaiAenugu

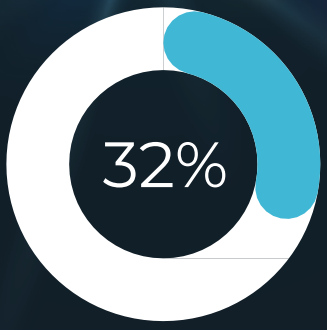
Founder and CEO TechForceCyber

jai@techforce.co.uk

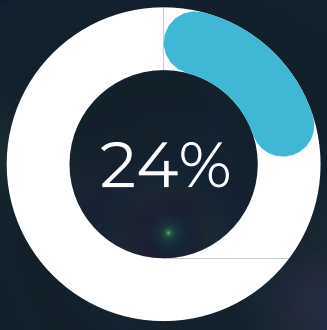
www.linkedin.com/in/jai23155/

Table of Contents

A brief retrospective of 2023 in the UK



Of businesses

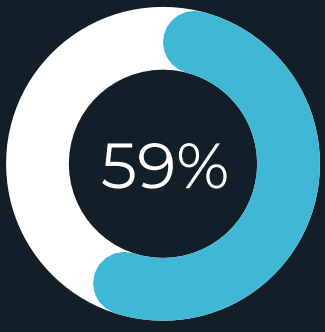


Of charities

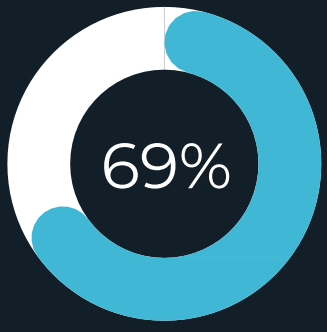
Were breached in the last 12 months.

If we drilldown further; This is much higher for

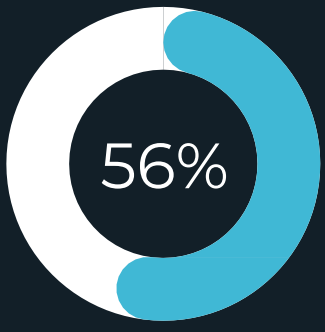
Medium Businesses



Large Businesses



High-income charities with £500,000 or more in Annual income



GOV.UK.(2023). CyberSecurity Breaches Survey 2023. [online] Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023[Accessed15Nov.2023].

A brief retrospective of 2023
Top data breach stats in the UK

Number of incidents in 2023

2,814

Number of breached records in 2023

8,214,886,660

Biggest data breach in the UK

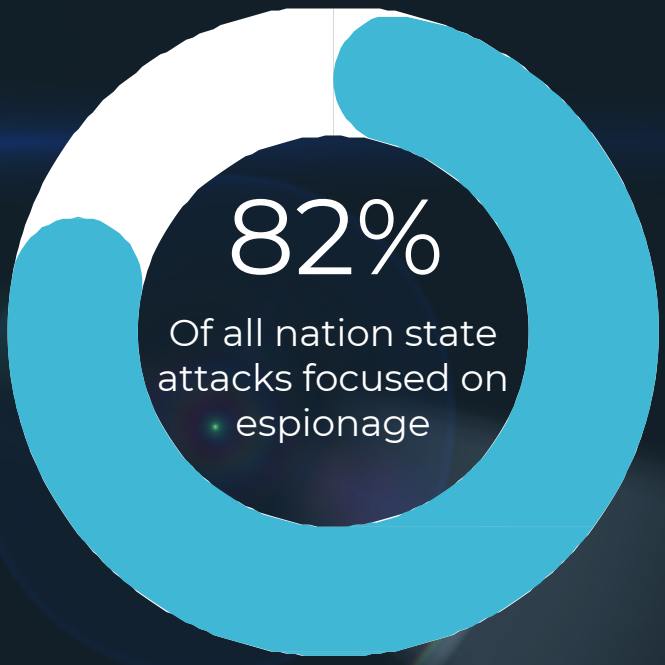
Dark Beam

3.8 billion

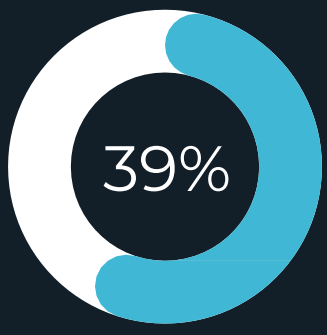
Breached records

A brief retrospective of 2023

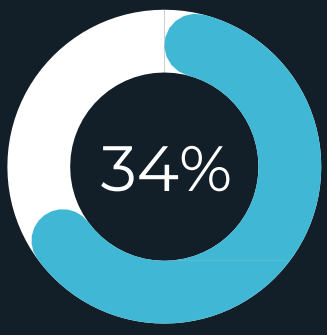
Attacks on public and private sectors were on the rise



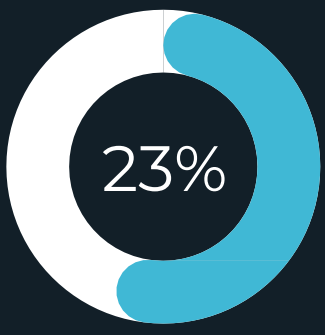
The Targets



Private sctors were attacked



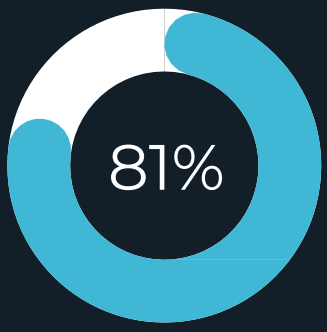
Government organisations were attacked



Attacks on Civil Society

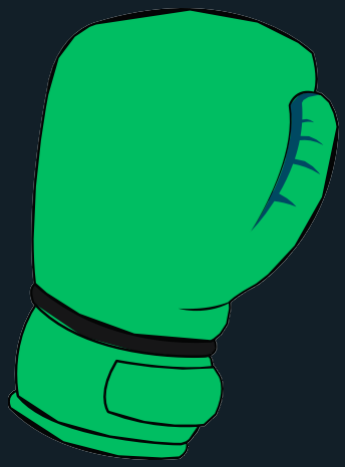
A brief retrospective of 2023

Although the tactics are becoming more sophisticated the top threats are:

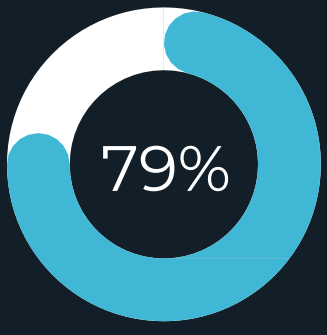


Email Phishing

VS



Ransomware Attacks



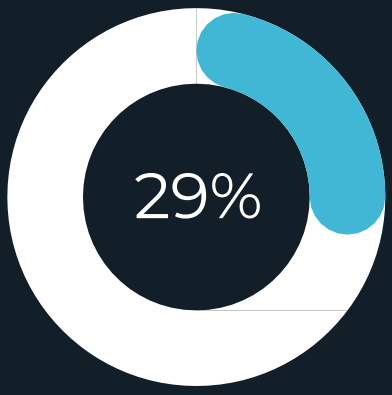
Getting back to business

65%

of the businesses experienced more than

6 Days

downtown after a ransomware attack



of breached organizations experience repeated attacks in 3 years

WIPRO State of CyberSecurity Report. [online] Available at: https://www.wipro.com/cybersecurity/state-of-cybersecurity-report-2023/ [Accessed20 Dec. 2023].

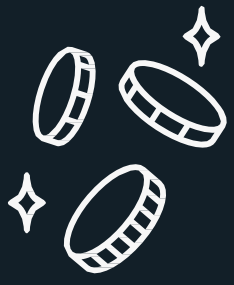
Damage Limitation-companies

75%

Brand Reputation

42%

Consumer Trust



42%

Revenue Loss Due To Downtime

9%

of CIOs are confident that they can recover quickly from attacks

WIPRO State of CyberSecurity Report. [online] Available at: https://www.wipro.com/cybersecurity/state-of-cybersecurity-report-2023 /[Accessed20 Dec. 2023].

Risk management and supply chains

A larger proportion of businesses take actions to identify cyber risks than charities. Larger businesses are the most advanced in this regard. For the first time, the majority of large businesses are reviewing supply chain risks, although this is still relatively rare across organisations overall.

- Three in ten businesses have undertaken cybersecurity risk assessments (29%, vs. 27% of charities)in the last year – rising to 51% of medium businesses and 63% of large businesses.

- A similar proportion of businesses deployed security monitoring tools (30%, vs. 19% of charities) – rising to 53% of medium businesses and 72% of large businesses.

- Under four in ten businesses (37%) and a third of charities (33%) report being insured against cybersecurity risks – rising to 63% of medium businesses and 55% of large businesses (i.e. cyber insurance is more common in medium businesses than large ones).

GOV.UK. (2023). Cyber Security Breaches Survey 2023. [online] Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023[Accessed 15 Nov. 2023].

1 A brief retrospective of 2023 with real life cases:

The common trends and concerns in cybersecurity that were prevalent leading upto 2022, and these may have continued or evolved in 2023

Ransomware Attacks:

Ransomware continued to be a significant threat, targeting individuals, businesses, and even critical infrastructure. Cyber criminals often demanded hefty ransom payments in cryptocurrencies.

Barts Health NHS Trust, the largest health trust in the UK, was hit by a ransomware attack in June which was claimed by ALPHV, aka BlackCat. The gang stated that it had stolen 7TB of sensitive data in what is claimed to be the biggest breach of healthcare data in the United Kingdom.

2 Supply Chain Vulnerabilities: Concerns around supply chain

Security increased, with attackers exploiting weaknesses in the supply chain to compromise larger targets. This included attacks on software providers and suppliers.

okta

One of the latest hacks has seen identity and access management provider Okta hit by a breach that exposed private customer information.

Cyber criminals leveraged stolen credentials to gain access to Okta's customers data–particularly the credentials of an access management provider, which gave the hackers the additional bonus of appearing completely legitimate.

The nature of Okta's business means that it is a tempting target for cyber criminals as once they have secured access, they can quickly get into multiple customers infrastructure. As a result, Okta has been the victim of multiple breaches, including twice in 2022. Ironically, Okta has also been the end victim recently of a supply chain attack, where its healthcare benefits partner, Right way Healthcare was hacked, leaving the details of Okta employees exposed.

Source-https://www.consultancy.uk/news/35847/cybercriminals-continue-to-target-supply-chain-weaknesses

3 Nation-State Cyber Threats

Cybersecurity threats from nation-states and state-sponsored actors remained a major concern. Espionage, cyberwarfare, and attacks targeting critical infrastructure were issues of international significance.

ISRAELRAIL
EXPLORE ISRAEL BY TRAIN

September 2023:

Iranian hackers launched a cyber-attack against Israel's rail road network. The hackers used a phishing campaign to target the network's electrical infrastructure. Brazilian and UAE companies were also reportedly targeted in the same attack.

4 IoT and Smart Device Security:

As the use of Internet of Things (IoT) devices and smart technologies expanded, so did the vulnerabilities associated with them. Inadequate security measures on these devices posed risks to both individuals and organisations.

Phishing and Social Engineering:

Phishing attacks and social engineering tactics continued to evolve, becoming more sophisticated and harder to detect. Organisations faced challenges in educating users to recognise and avoid these threats.

$100 Million Google and Facebook Spear Phishing Scam

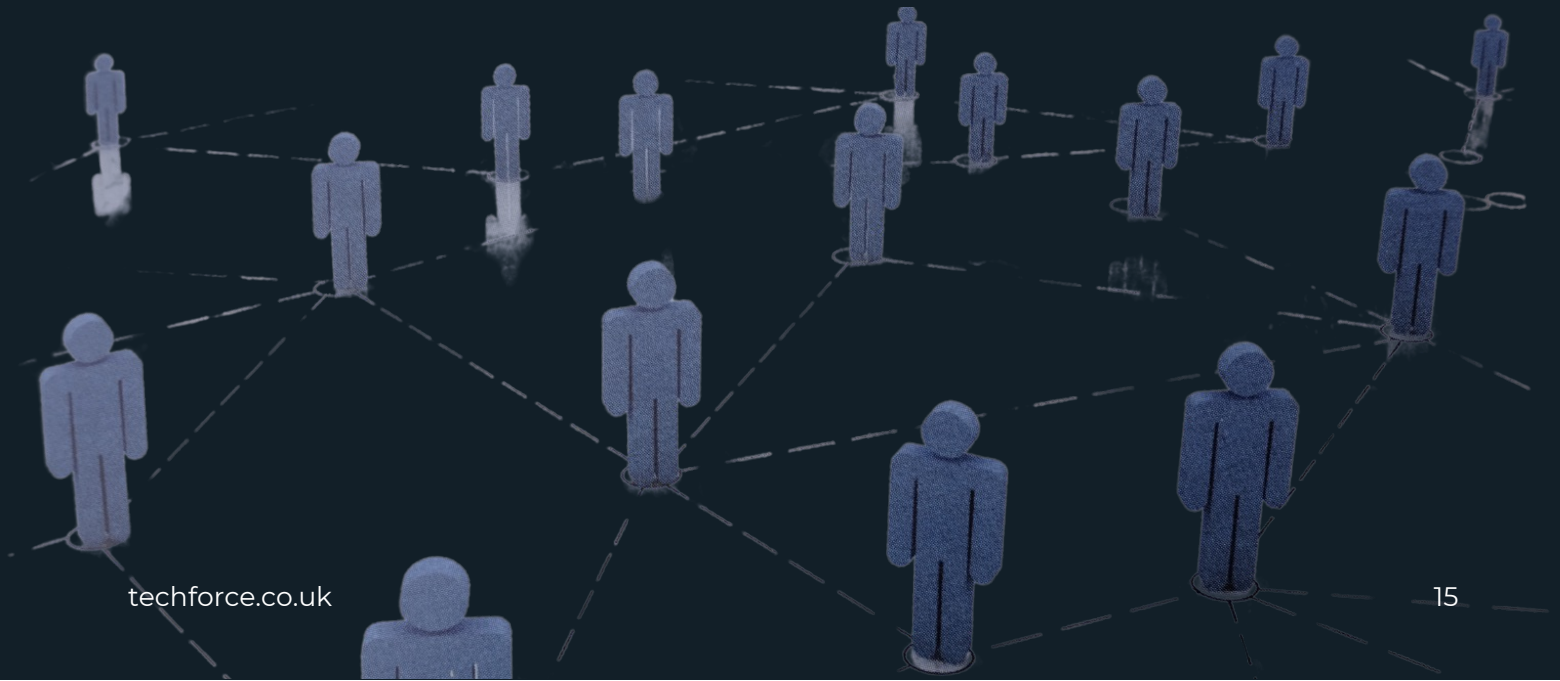
The scammers then sent phishing emails to specific Google and Facebook employees, invoicing them for goods and services that the manufacturer had genuinely provided—but directing them to deposit money into their fraudulent accounts.

5 Cloud Security Concerns:

With the widespread adoption of cloud services, ensuring the security of data stored in the cloud became a priority. Misconfigurations, data breaches, and unauthorised access were persistent issues.

6 Cyber security Workforce Shortage:

The shortage of skilled cybersecurity professionals remained a challenge for organisations. This shortage affected the ability to effectively respond to and mitigate cyberthreats.

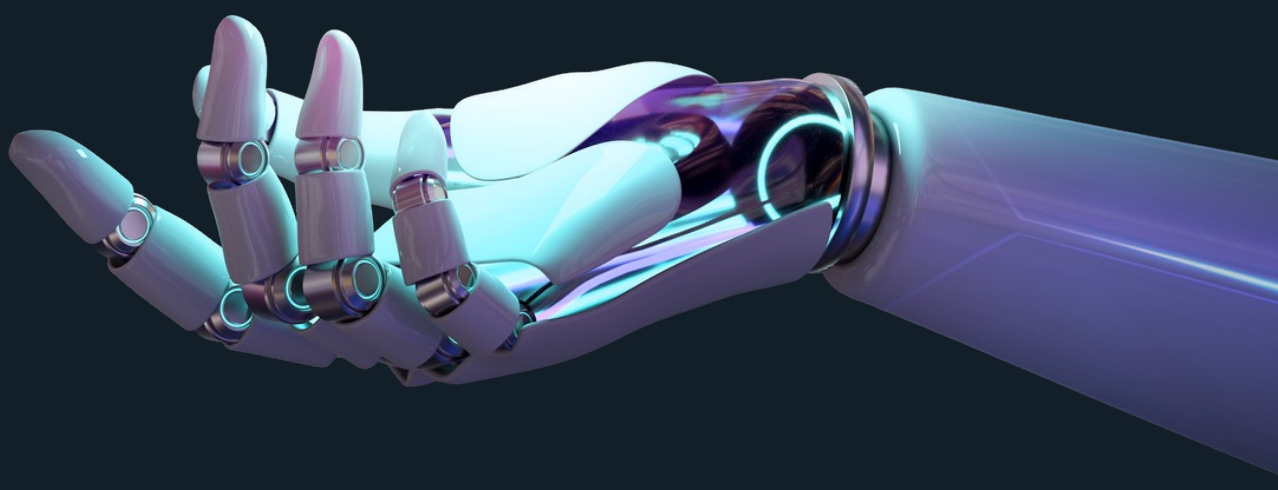


7 Regulatory Compliance and Data Protection:

Compliance with data protection regulations, such as GDPR, continued to be a focus. Organisations faced legal and financial consequences for inadequate protection of sensitive information.

8 Emergence of AI in Cyber Attacks:

The use of artificial intelligence (AI) and machine learning in cyber attacks increased. Attackers leveraged AI for more sophisticated and automated threat activities.



Cybersecurity Trends Report2024: Safeguarding the DigitalFrontier

Executive Summary:

As we enter 2024, the digital landscape faces unprecedented challenges and opportunities in cybersecurity. This report looks at the key trends that will shape the cybersecurity landscape in the coming year, focusing on strategies and technologies crucial for safeguarding the digital arena.

Zero Trust Paradigm:

Zero Trust Architecture emerges as a cornerstone for cybersecurity. This report explores the principles of trust elimination, continuous verification, and adaptive access controls, emphasising the need for organisations to abandon the traditional perimeter-based security approach.

BUSINESS PERSPECTIVE

Key Take aways from a business to business perspective

Adoption of Zero Trust Architecture:

Businesses should consider adopting a Zero Trust Architecture to enhance cybersecurity.

Emphasises trust elimination, continuous verification, and adaptive access controls over traditional perimeter-based security.

Strategic Shift in Security Approach:

Organisations need to shift their security approach from relying solely on perimeters to a more dynamic and adaptive model.

Recognising that threats can emerge from both internal and external sources, B2B entities must prioritise continuous verification.

Continuous Adaptation to Emerging Threats:

Acknowledges the evolving nature of cybersecurity threats in 2024.

B2B entities should focus on continuous adaptation to emerging threats, staying proactive rather than reactive.

Investment in Cybersecurity Technologies:

Encourages B2B organisations to invest in cutting-edge cybersecurity technologies.

With the increasing complexity of threats, staying technologically updated is crucial for robust protection.

Collaboration and Information Sharing:

Highlights the importance of collaboration and information sharing within the B2B ecosystem.

Businesses should actively engage in sharing threat intelligence and best practices to collectively strengthen defences.

Employee Training and Awareness:

Emphasises the role of employees in maintaining cybersecurity.

B2B organisations should invest incomprehensive training programs to enhance employee awareness and mitigate potential risks associated with human error.

Holistic Cybersecurity Strategies:

Encourages B2B entities to develop holistic cybersecurity strategies.

We would suggest an integrated approach that combines technology, policies, and employee awareness to create a comprehensive defence against cyberthreats.

Compliance with Zero Trust Principles:

B2B organisations should align their cybersecurity practices with Zero Trust principles.

Compliance with these principles ensures a higher level of security and resilience against cyberthreats.

Zero Trust Architecture: Transforming Cybersecurity Defenses

In an era where traditional security models fall short against sophisticated cyberthreats, the Zero Trust Architecture emerges as a pivotal shift in cybersecurity strategies. The foundational principle of Zero Trust can been capsulated in its name: trust is never assumed, and verification is continuous. This approach acknowledges that threats can come from both external and internal sources, requiring are evaluation of the traditional perimeter-based security model.

Key Principles

01. Trust Elimination:

Zero Trust challenges the notion of a trusted internal network. Instead of assuming trust based on location within the network, it operates on the principle of "never trust, always verify." Every user, device, and application is treated as potentially untrusted until proven otherwise.

---

02. Continuous Verification:

Unlike conventional security models that authenticate users at the point of entry and trust them throughout their session, Zero Trust adopts continuous verification. This means ongoing authentication and authorisation at various stages of a user's interaction with the network, applications, and data.

---

03. Adaptive Access Controls:

Zero Trust advocates for dynamic, context-aware access controls. Access permissions are not static but evolve based on real-time assessments of user behavior, device health, and other contextual factors. This adaptability ensures that access is granted or restricted based on the specific circumstances of each interaction.

Rationale for Abandoning Perimeter-Based Security

01. **Changing Perimeter Dynamics:**

The traditional approach of securing the perimeter assumed that once inside, users and devices could be trusted. However, with the rise of remote work, cloud computing, and the prolife ration of mobile devices, the concept of a fixed perimeter has become obsolete.

---

02. **Advanced Threat Landscape:**

Cyberthreats have evolved beyond straight forward attacks. Sophisticated adversaries often exploit trusted network relationships. Zero Trust recognises that threats can originate from compromised insiders or external entities with legitimate access.

---

03. **Data-Centric Security:**

Zero Trust shifts the focus from network security to data-centric security. It acknowledges that the ultimate goal is to protect sensitive data, regardless of where it resides or how it is accessed. This requires a granular understanding of data flows and user interactions.

Implementation Challenges and Considerations:

01. Cultural Shift:

Adopting Zero Trust is not just a technological shift but a cultural one. It requires organisations to move away from a mindset of implicit trust towards one of continuous scrutiny and verification.

---

02. Integrated Technologies:

Implementing Zero Trust necessitates the integration of various technologies, including identity and access management, endpoint security, network security, and behavioural analytics. Coordination and seamless integration between these components are critical.

---

03. User Experience:

While enhancing security, organisations must ensure that the implementation of Zero Trust does not compromise user experience. Balancing stringent security measures with user-friendly access is vital for successful adoption.

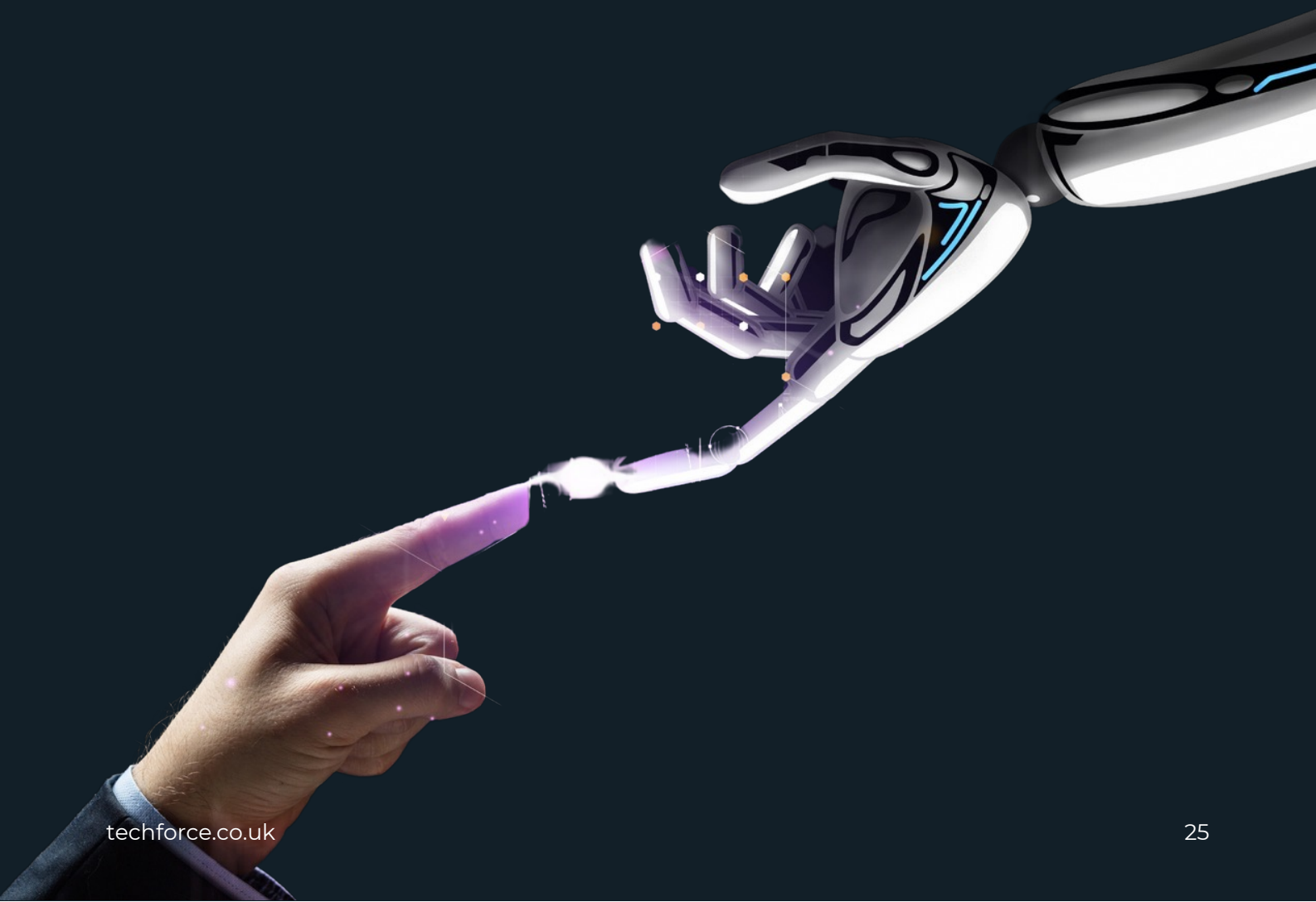
To summarise, the Zero Trust Architecture stands as a transformative approach in cybersecurity, urging organisations to reevaluate their assumptions, fortify their defences, and adapt to the dynamic and ever-evolving threat landscape. By embracing continuous verification and adaptive access controls, organisations can establish a robust security posture in an environment where trust is earned, not assumed.

AI AND ML INTEGRATION

AI and ML Integration:

In 2024 Artificial Intelligence (AI) and Machine Learning (ML) will take centre stage in cyber defence.

We will now investigate how these technologies enhance threat detection, automate response mechanisms, and predict vulnerabilities, ushering in a new era of proactive cybersecurity.



Threat Detection Enhancement:
Traditional cybersecurity measures often rely on predefined signature sand patterns to identify threats. AI and ML revolutionise this approach by introducing a dynamic, learning-based model. These technologies analyse vast data sets in real-time, identifying anomalies and deviations from established patterns. By understanding the normal behaviour of systems and users, AI and ML can swiftly detect unusual activities that may indicate a potential security threat.

Behavioural Analytics:
AI and ML algorithms employ behavioural analytics to establish baselines of normal behaviour for users, devices, and applications. Any deviation from these baselines triggers alerts, enabling early detection of potentially malicious activities.

Advanced Anomaly Detection:
Machine learning models excel at recognising patterns, even subtle deviations that might elude traditional rule-based systems. This advanced anomaly detection capability allows organisations to identify emerging threats that might not have recognisable signatures.

Automated Response Mechanisms:
In the face of cyber threats that move at machine speed, the manual response is often insufficient. AI and ML bring automation to the forefront, enabling swift responses to detected threats. Automated response mechanisms not only reduce response times but also alleviate the burden on cybersecurity teams.

Incident Response Automation:
AI- driven incident response systems can automate the identification, containment, and mitigation of security incidents. This includes isolating affected systems, blocking malicious activities, and even initiating predefined response actions without human intervention.

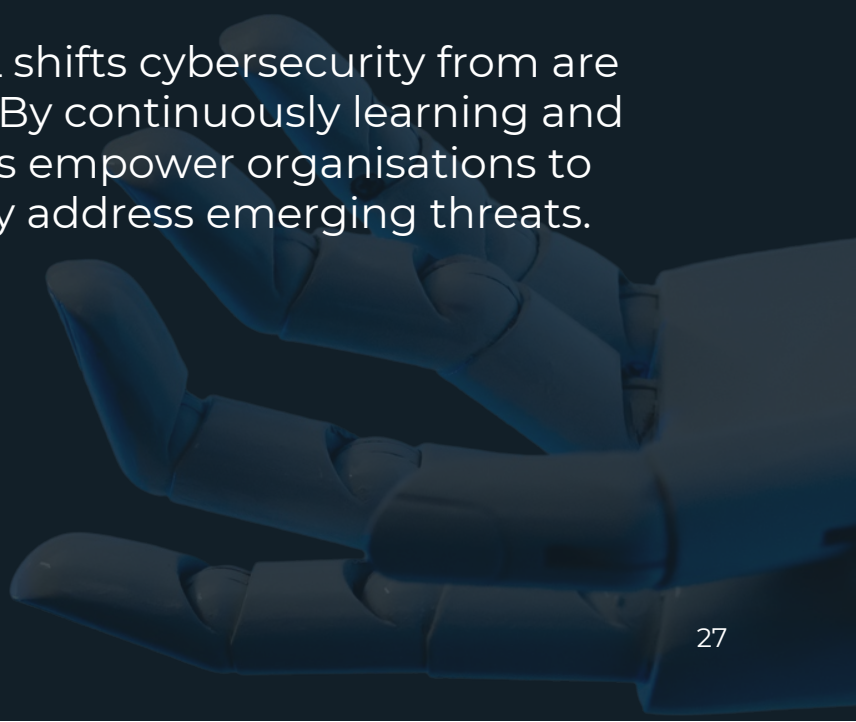
Adaptive Security Orchestration:
ML algorithms continuously learn from past incidents, improving the efficiency and effectiveness of automated responses overtime. This adaptive security orchestration allows for increasingly sophisticated responses that align with evolving threat landscapes.

Predictive Vulnerability Management:
Traditionally, vulnerability management involved identifying and patching known vulnerabilities. AI and ML bring a predictive dimension to this process, anticipating potential vulnerabilities and proactively fortifying defences.

Dynamic Threat Modelling:
Machine learning models can analyse historical threat data, user behaviour, and system vulnerabilities to predict where future threats may emerge. Dynamic threat modelling helps organisations stay ahead of potential vulnerabilities before they are exploited.

Automated Patch Prioritisation:
AI-driven systems can assess the criticality of vulnerabilities based on potential impact and exploitability. This automated patch prioritisation ensures that cybersecurity teams focus on addressing the most significant threats first, optimising resource allocation.

Proactive Cybersecurity:
The integration of AI and ML shifts cybersecurity from are active to a proactive stance. By continuously learning and adapting, these technologies empower organisations to anticipate and pre-emptively address emerging threats.



Threat Intelligence Augmentation:
AI enhances threat intelligence by processing and analysing massive datasets to identify patterns and trends.

This augmented threat intelligence provides a comprehensive understanding of the evolving threat landscape.

Adaptive Defense Strategies:
Machine learning models can adapt defence strategies based on real-time threat assessments. This adaptability ensures that cybersecurity measures evolve alongside the threat landscape, providing a more robust and resilient defence. Overall, the integration of AI and ML in cybersecurity represents a paradigm shift, ushering in an era where defence s are not only more intelligent but also proactive. These technologies empower organisations to detect threats with greater accuracy, respond swiftly and automatically, predict vulnerabilities before exploitation, and foster a cybersecurity posture that evolves in tandem with the ever-changing threat landscape.

Quantum-Resistant Cryptography:
With the rise of quantum computing, traditional cryptographic methods face unprecedented threats. The report outlines the urgency of adopting quantum-resistant cryptography to future- proof data protection against quantum-enabled attacks.

Quantum-Resistant Cryptography:
Fortifying Data Protection Against Quantum Threats
As we stand on the brink of the quantum computing era, the traditional cryptographic methods that have long been the stalwarts of data protection face an imminent threat. The rise of quantum computing poses unprecedented challenges to the security landscape, demanding a strategic response. This section delves into the urgency of adopting quantum-resistant cryptography, emphasising the need to future-proof data protection against quantum-enabled attacks.

Quantum Computing Threat Landscape:
Quantum computers, harnessing the principles of quantum mechanics, possess immense computational power that could render traditional encryption algorithms obsolete. Algorithms such as Shor's algorithm, when execute done quantum computer, can efficiently factorise large numbers, breaking widely-used public-key crypto systems like RSA and ECC. This paradigm shift necessitates a fundamental revaluation of cryptographic strategies.

Factorisation Vulnerability:
Traditional public-key cryptography relies on the difficulty of factoring large numbers into their prime components. Quantum computers, with their ability to perform parallel computations, threaten to undermine this foundational premise.

Shor's Algorithm:
Shor's algorithm, a quantum algorithm designed for integer factorisation, poses a significant risk to widely-used cryptographic protocols. It can efficiently factorise large numbers exponentially faster than the best-known classical algorithms.

Urgency of Quantum-Resistant Cryptography:
Recognising the urgency of the quantum threat, the adoption of quantum-resistant cryptography becomes a critical imperative. Quantum-resistant algorithms are designed to with stand the computational power of quantum computers, providing a robust defence against potential quantum-enabled attacks.

Long-Term Security Considerations:
The transition to quantum-resistant cryptography is not merely a future-proofing measure; it's a long-term security consideration. The cryptographic protocols currently in use may still be secure against classical attacks but become vulnerable in the face of quantum adversaries.

Data Sensitivity and Lifespan:
For organisations dealing with sensitive information and long-term data storage, the urgency to adopt quantum-resistant cryptography is amplified. As quantum computers mature, data encrypted with current methods may be exposed, posing risks to privacy and security.

Quantum-Resistant Cryptographic Approaches:
Several quantum-resistant cryptographic approaches are under exploration and development. These approaches leverage mathematical challenges that are not efficiently solvable even with quantum computers, ensuring data security in a post-quantum world.

Lattice-Based Cryptography:
Lattice-based cryptography relies on the hardness of problems associated with mathematical lattices. The computational complexity of lattice problems makes them resistant to quantum attacks, making lattice-based cryptography a promising avenue.

Hash-Based Cryptography:
Hash-based cryptographic schemes leverage the one-way ness property of cryptographic hash functions. While quantum computers can solve the problem of pre-image resistance for classical hash functions, quantum-resistant hash-based schemes offer a robust alternative.

Industry and Standardisation Efforts:
The urgency to address quantum threats has spurred industry collaborations and standardisation efforts. Organisations and consortiums are actively working towards defining quantum-resistant cryptographic standards that can be universally adopted.

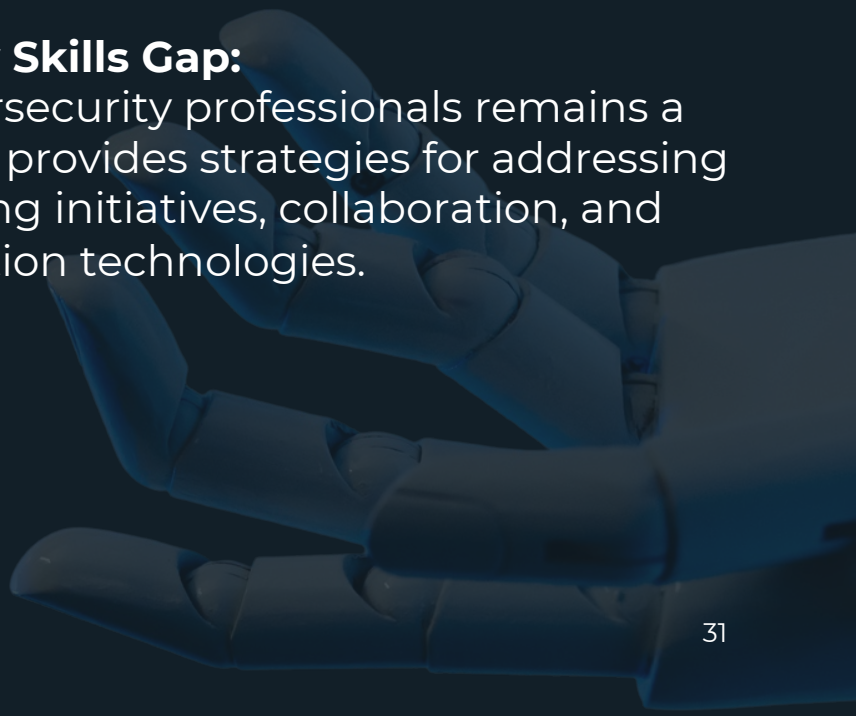
NIST Post-Quantum Cryptography Standardisation:
The National Institute of Standards and Technology (NIST) is at the forefront of global efforts in standardising post-quantum cryptographic algorithms. The ongoing NIST Post-Quantum Cryptography Standardisation project aims to identify cryptographic algorithms that can resist quantum attacks.

Ransomware Landscape:
Ransomware continues to evolve in sophistication and scale. There port provides in sights into the changing tactics of ransomware actors and outlines resilience strategies, including robust backup protocols, employee training, and threat intelligence integration.

IoT Security Challenges:
The expanding Internet of Things (IoT) eco system introduces new security challenges. This section addresses vulnerabilities in IoT devices and networks, offering recommendations for comprehensive security measures to counter emerging threats.

Regulatory Impact:
The regulatory landscape plays a pivotal role in shaping cybersecurity practices. The report analyses the influence of existing and upcoming regulations on data privacy, breach reporting, and the development of cybersecurity frameworks to guide organisations in compliance efforts.

Bridging the Cybersecurity Skills Gap:
The shortage of skilled cybersecurity professionals remains a critical concern. This section provides strategies for addressing the skills gap through training initiatives, collaboration, and the strategic use of automation technologies.



Conclusion

To conclude this 2024 report; As organisations navigate the complexities of the digital age, a proactive and adaptive cybersecurity stance is paramount. The Cybersecurity Trends Report 2024serves as a guide, offering insights and recommendations to fortify defences, mitigate risks, and safeguard the digital frontier in the face of evolving cyber threats.

TechForce Cyber emerges as the unparalleled choice for ensuring optimal cyber wellness. With a proven track record of expertise, innovation, and a proactive approach, TechForce Cyber goes beyond conventional solutions. Their commitment to staying ahead of emerging threats, coupled with a customer-centric ethos, positions them as the vanguard of cybersecurity providers. In an era where security is paramount, TechForce Cyber is the trusted ally, dedicated to keeping your digital domain secure and resilient. Choose confidence, choose TechForce Cyber, because your digital well-being deserves nothing less.

Stay Safe in 2024 and remember TechForce Cyber ifyou want to ensure you are in the best hands when it comes to cyber protection.


TechForce™
Cyber
STAY SAFE!
techforce.co.uk