Guardians of digital trust
Cybersecurity Awareness Month

Elevating **people.**
Elevating **business.**
Elevating **society.**

Top cybersecurity threats and predictions for 2025

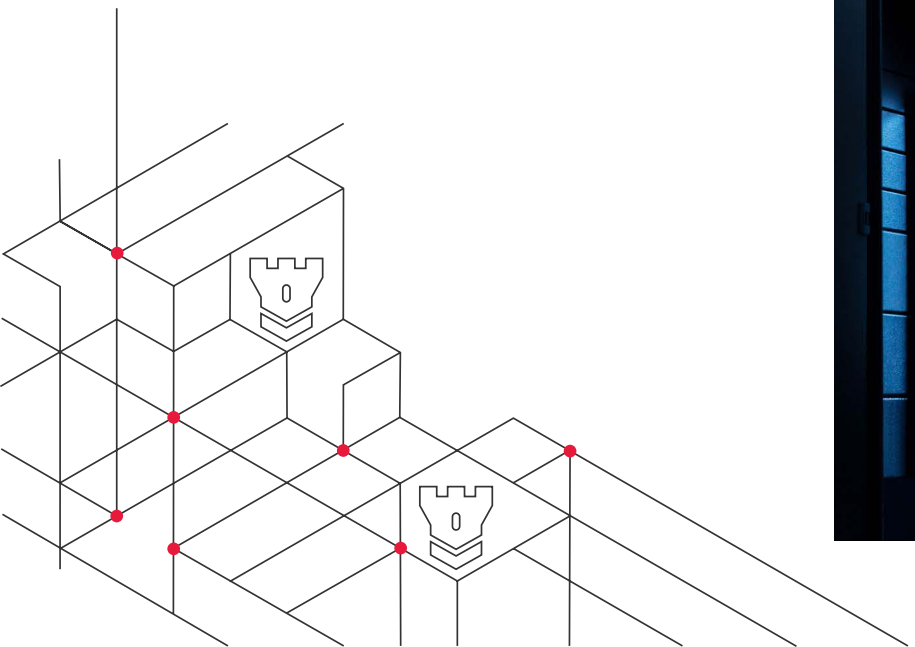
BDO
AUDIT • ADVISORY • TAX

Top cybersecurity threats and predictions for 2025

New technology has given enterprises greater data analytics, communication, and operational efficiency capabilities. However, it has also made threat actors, ranging from nation-state actors to cybercriminals, more sophisticated. As our world becomes more digitally interconnected, we see the integration of artificial intelligence with cyber-attacks, enhancing the severity of these attacks.

Staying one step ahead in this digital race requires adopting cutting-edge measures. For example, leveraging Generative AI-enabled security solutions can drastically improve how security teams operate, driving efficiencies and reducing risks. Gen AI-based security technologies can help surface higher priority risks and drive automated response procedures. These solutions can help your security team free up valuable time, improve detection, and drive faster response and recovery to keep your business thriving.

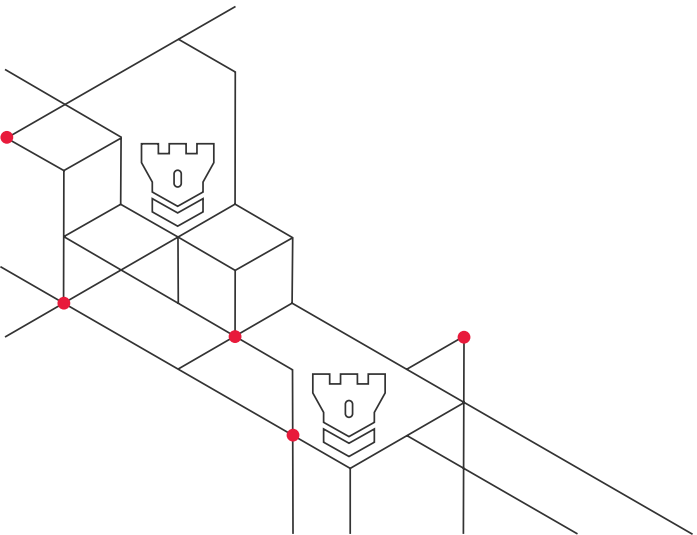
Understanding the emerging threats that businesses will face in 2025 is also critical. This article discusses the biggest threats and the key strategies to help you stay protected.



The rising cost of cyber-attacks and the importance of resilience

According to the 2024 IBM Cost of a Data Breach Report, breach costs increased 10% from the year prior, the largest yearly jump since the pandemic. Additionally, 26% more organisations faced severe staffing shortages compared to the prior year and observed an average of $1.76 million in higher breach costs than those with low level or no security staffing issues. This finding underscores the alarming gap in organisations' ability to identify, detect, and respond to cyber threats before the impact is felt by the organisation. There is, however, some good news. The report also found that 42% of data breaches were discovered by security teams, a 9% improvement from last year. This increase is attributed to greater investment in cyber planning and threat detection, as well as the adoption of AI technology to bridge resource gaps.

While these improvements are promising, there is still significant room for growth. The evolving threat landscape, fuelled by geopolitical tensions and innovative attack methods, underscores the need for organisations to develop and regularly stress test cyber resilience plans. Leveraging AI tools can free up valuable time for security teams to focus on continued improvements to their programmes. Empowering teams with tools and strategies to accomplish more with limited resources remains a critical challenge.



What are the top cybersecurity threats for businesses?

Your cybersecurity posture is not just an IT concern but a fundamental aspect of your overall business strategy and resilience. The ability to navigate the complex web of cybersecurity threats is no longer a matter of competitive advantage but a legal and ethical obligation. Stringent laws and regulations have been enacted, mandating businesses to remain vigilant and proactive in protecting their data to preserve their integrity and uphold the trust and privacy of their customers and partners.

To effectively mitigate risks, organisations must identify and address the following threats in 2025:

Nation-state actors

Nation-states are among the most organised and capable groups in the cyber threat landscape. These threat actors invest significantly in cyber capabilities, both offensive and defensive, to gain geo-political advantages. Their activities often dictate broader trends in cybersecurity. With current geopolitical tensions in Eastern Europe and the Western Pacific, these actors will continue to drive new trends in cybersecurity.

On the offensive side, nation-states develop cyber-attack platforms and tools that are often highly sensitive and secret, intended to be used stealthily at a time and place of their choosing. Sometimes, these systems are made public or exposed and used deliberately by criminal gangs or even leveraged by other nation-states.

On the defensive side, government agencies like the Securities and Exchange Commission (SEC) in the United States are tightening cybersecurity regulations for businesses, partly in response to the sophisticated threats posed by nation-states. In this case, company officers are held directly accountable for the cybersecurity measures they do or don't invest in.

The dual role of nation-state actors in advancing offensive and defensive cyber technologies can have a mixed impact on businesses.

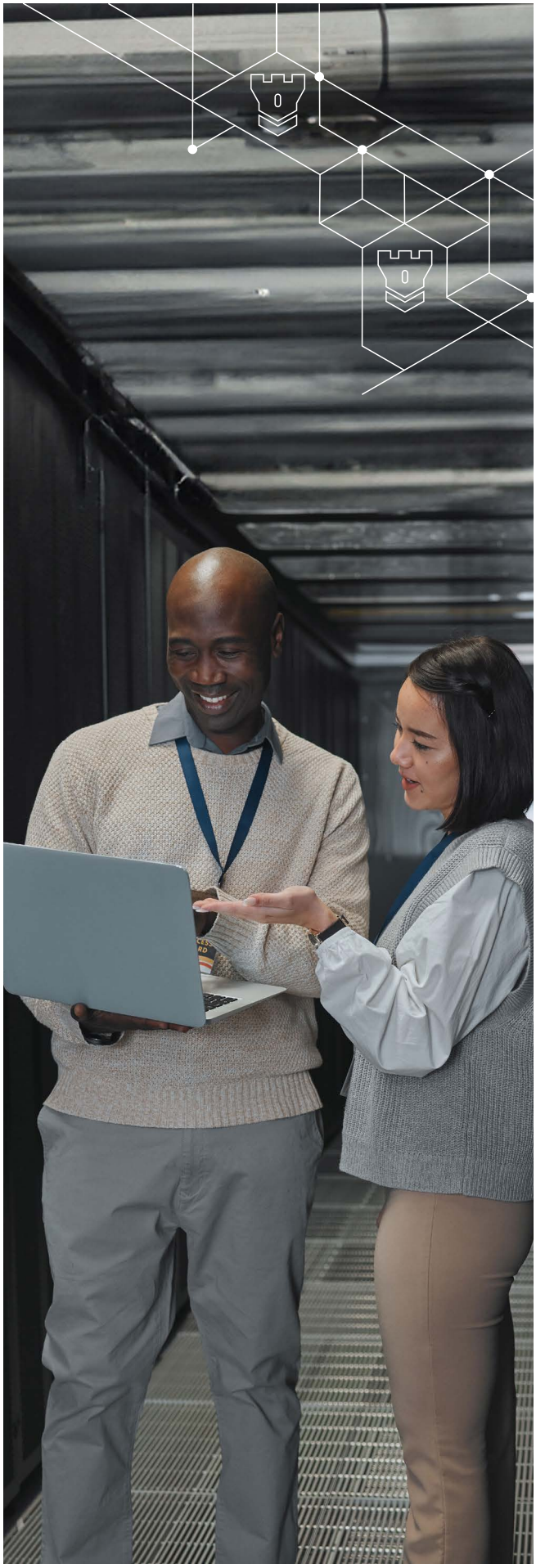
Cybercriminals

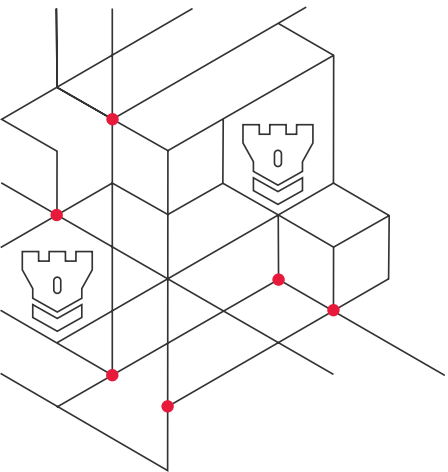
Cybercriminal groups often focus on financial gain and range from sophisticated outfits, sometimes operating with a degree of state backing (to act as proxies), to less organised but highly skilled teams. Additionally, the tools used by state actors sometimes find their way into the hands of these criminals, either deliberately or inadvertently, increasing the risks further.

Individual hackers

At the other end of the spectrum are individual hackers and small groups, often called hacker enthusiasts. While their motives vary from activism to financial gain or notoriety, they present different organisational challenges. Technologies that enable hacking are becoming more accessible through platforms that "hack-as-a-service", allowing even less experienced individuals to pose a significant risk.

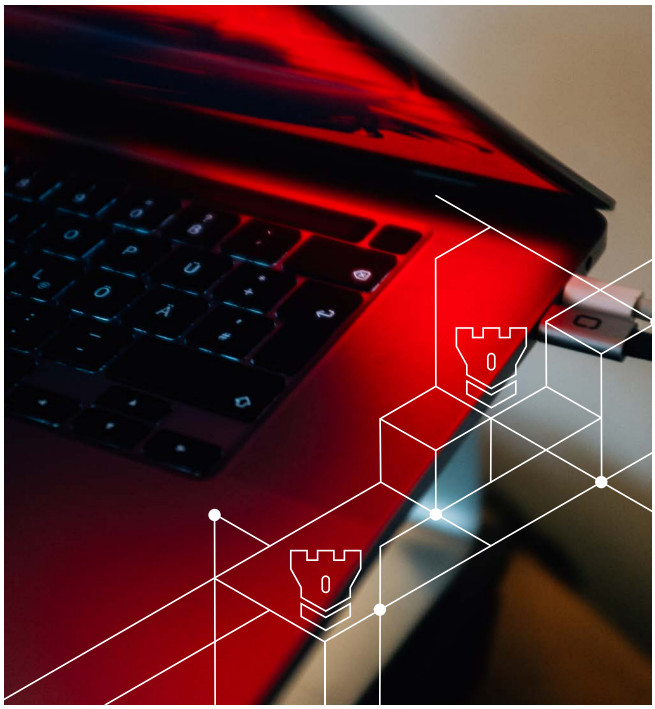
LEARN MORE ABOUT COMMODITY CYBER THREATS





Understanding the cyber threat landscape: Who are the threat actors?

In today's interconnected world, no organisation is completely safe from cyber threats, making it imperative for businesses to understand the evolving threat landscape. This ecosystem is a complex web of various actors, each with unique motivations and capabilities, posing a range of risks to the financial and operational integrity of organisations.



Cyber espionage

This covert threat involves unauthorised access to computer systems and networks with the intent to gather sensitive information, potentially causing severe consequences. It can range from shattered corporate reputations or loss of competitive advantage to compromised national security. In this context, understanding common cyber espionage tactics is critical to implement effective countermeasures.

Business email compromise

Characterised by its deceptive simplicity, business email attacks involve impersonating a trusted individual or entity through email communication to manipulate employees, clients, or consumers into revealing sensitive information or executing fraudulent financial transactions. This can often result in substantial economic losses and reputational damage.

Credential stuffing

Threat actors use stolen usernames and passwords from one website or service to gain access to other accounts, exploiting individuals who use the same login credentials across multiple platforms. This tactic relies on reused passwords, making it an effective method to compromise accounts and access sensitive information.

Insider threat

According to a recent Verizon report, the average external threat compromises about 200 million records, while incidents involving an inside threat actor have resulted in the exposure if 1 billion records or more. This is a significant cyber threat tactic wherein individuals with authorised access to an organisation's systems and data exploit their position. These individuals can be employees, contractors, or business partners.

Supply chain attacks

In these attacks, actors seek to compromise third-party vendors or suppliers to access the target organisation's systems or data. They can then undermine the security of the entire supply chain, potentially leading to data breaches, system compromises, or other adverse consequences. Proactive risk mitigation is essential to counter this multi-layered and evolving threat.

Cyber sabotage

This campaign involves deliberate acts to disrupt the digital infrastructure with the intent to compromise the integrity, confidentiality, or reputation of the target company for ideological, personal, or competitive reasons. It is crucial to understand what tactics to look for when developing effective defence strategies against cyber sabotage. Familiarise yourself with the following tactics:

Ransomware

The Microsoft Digital Defence Report 2023, indicated that organisations faced an increased rate of ransomware attacks from the previous year, the number of human-operated ransomware attacks went up more than 200%. Ransomware is characterised by the encryption, or at times, the modification of critical data to extort a ransom from targeted victims. Cybercriminals are increasingly collaborating, sharing tools and tactics, and casting a wider net to target organisations of all sizes. These factors have contributed to the escalating frequency and sophistication of ransomware incidents, posing a significant risk to businesses and critical infrastructure worldwide.

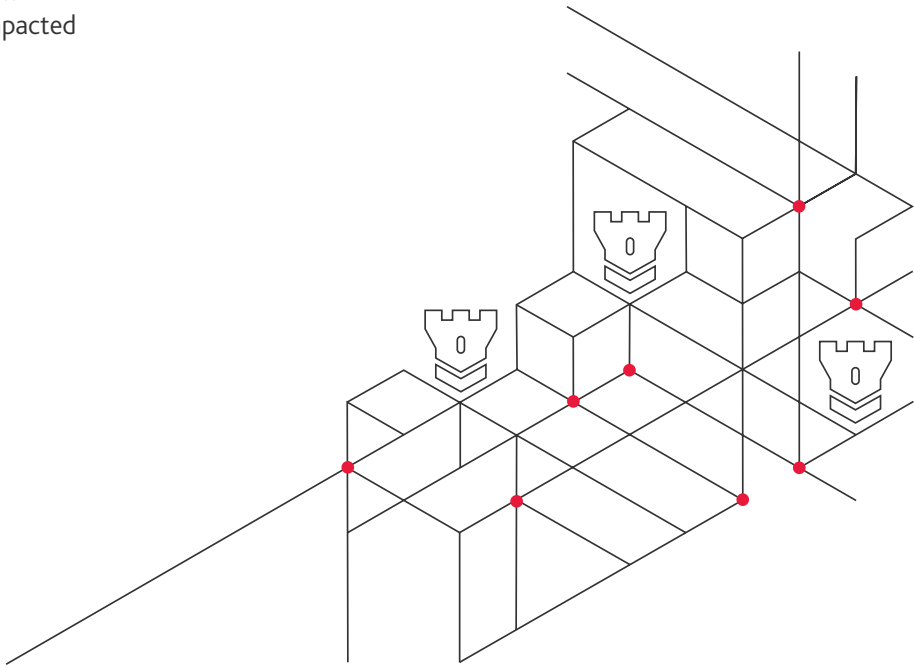
In October 2023, The Toronto Public Library, Canada's biggest library network, fell victim to a ransomware attack. Cybercriminals encrypted the library's computer systems and stole employee data, causing widespread disruption to services. In May 2024, Ascension, one of the largest nonprofit health systems in the U.S., was hit by a ransomware attack that disrupted operations for weeks. And back in February, Hyundai Motor Europe suffered a Black Basta ransomware attack in which three terabytes of corporate data was stolen. These are just a few examples of incidents that have significantly impacted organisations and people around the world.

Denial of service

Denial of service (DoS) attacks aim to disrupt the availability of online services or websites by overwhelming their servers with a flood of traffic, rendering them inaccessible to legitimate users. This typically involves using multiple compromised devices or a botnet to generate excessive requests or traffic. The main objective is not to steal data but to cause operational disruption to the targeted organisation.

Process sabotage

These attacks focus on data-dependent processes essential for smooth operations. By either altering or deleting critical data, the attacks render operational protocols ineffective. For example, consider a fleet of vehicles operating under a strict maintenance schedule. If the maintenance records were manipulated or deleted, vehicle readiness could be compromised, disrupting the entire logistical chain.



Cyber fraud

A pervasive and ever-evolving threat, cyber fraud is a blanket term for a wide range of illicit activities aimed at financial gain or data compromise. The tactics involve using emails and social engineering techniques to exploit vulnerabilities in an organisation, often leading to detrimental consequences. Countermeasures should include robust authentication protocols, employee awareness programmes, and monitoring systems to detect unusual activities.

Credential exposure

Perhaps one of the most elementary forms of cyber fraud, credential exposure often manifests through phishing attempts via email, phone calls, or even text messages. Usually, the narrative involves an urgent requirement for account verification or a refund process. Awareness is the frontline defence in this case — knowing, for example, that legitimate financial institutions or governmental bodies will never solicit personal information via unsolicited communications.

Account takeover

Account takeover (ATO) occurs when a malicious actor gains control of a legitimate account (bank, email, socials) without the owner's permission. It is often possible by exploiting weaknesses in authentication or security measures. Human inertia around password changes plays into the hands of fraudsters. ATO can be especially damaging for organisations where customer profiles in external applications can be monetised, such as in loyalty programmes.

Payment fraud

Often interconnected with business email compromise, payment fraud aims to initiate unauthorised financial transactions. It usually involves impersonating a trusted entity and requesting an accounts payable officer to alter banking details for a pending payment. The timing is often meticulously planned to coincide with periods when vigilance might be lowered — like the weekend onset or when senior management is out of the office.

Misinformation

A potent form of digital attack, this involves the deliberate dissemination of false or misleading information with the intent to deceive, manipulate, or cause confusion — it's a powerful tool used to manipulate public opinion and create unrest. These campaigns often use online channels like social media, email, and websites, underscoring the importance of media literacy, critical thinking, and fact-checking.

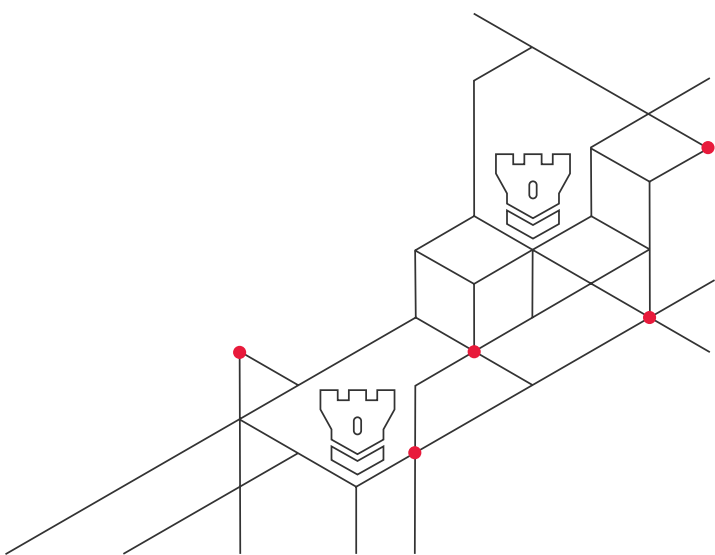
The impacts of misinformation are vast, ranging from the loss of public trust and credibility to actual financial or societal harm. Combating it requires a multi-faceted approach that involves individual vigilance and collective action. Using your organisation's digital risk protection capabilities like cyber threat intelligence, you can spot misinformation early and take it down to minimise its impact on the brand and the public. The main types of misinformation tactics are:

Brand Abuse

Cybercriminals or malicious actors can use misinformation to tarnish a brand's reputation. This can range from spreading false reviews and information, creating fake social media accounts that impersonate the brand, or setting up fraudulent websites like legitimate ones. Such tactics can confuse customers, harm the brand, and may even result in financial losses.

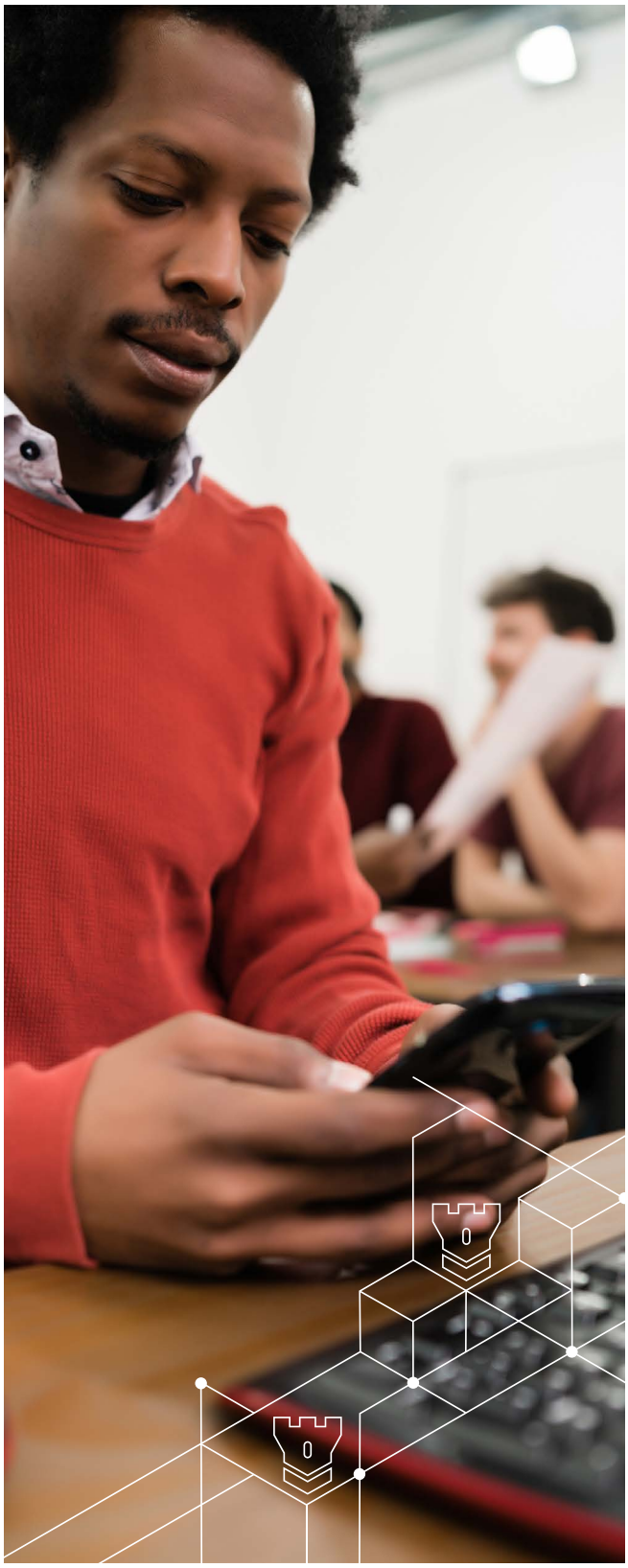
Election Fraud

Misinformation can also be weaponised to disrupt the democratic process. False narratives or doctored materials can be distributed to mislead voters, undermine candidates, or manipulate election outcomes.



Additional cybersecurity best practices for businesses

- Risk awareness and identifying blind spots is the first step toward protection. Implement targeted measures to safeguard your organisation's digital assets by pinpointing vulnerabilities and potential gaps in your security infrastructure.
- Monitor your exposure by leveraging intelligence for early threat detection, such as watching illicit online marketplaces and forums where cybercriminals often trade stolen data.
- Monitor and manage network behaviours 24/7 to prevent unauthorised entry into your digital infrastructure, reducing the risk of cyber threats and data breaches.
- Stay compliant with evolving privacy and security regulations to avoid legal and financial repercussions.
- Conduct a business continuity and resilience assessment. Evaluate your company's and supplier's ability to maintain operations during disruptions to ensure uninterrupted business continuity in the face of potential cyber threats.
- Align cyber risks with your overall business strategy, to help boards and investors make informed decisions and effectively allocate resources. Read our first article in the series: How boards can enhance their cybersecurity knowledge: six strategies to protect your organisation from cyber threats.
- The intricate nature of the cyber threat landscape shows that addressing cyber security is not solely the domain of IT departments. Instead, it's a shared responsibility requiring comprehensive risk management strategies that involve multiple stakeholders, including financial decision-makers like CFOs.

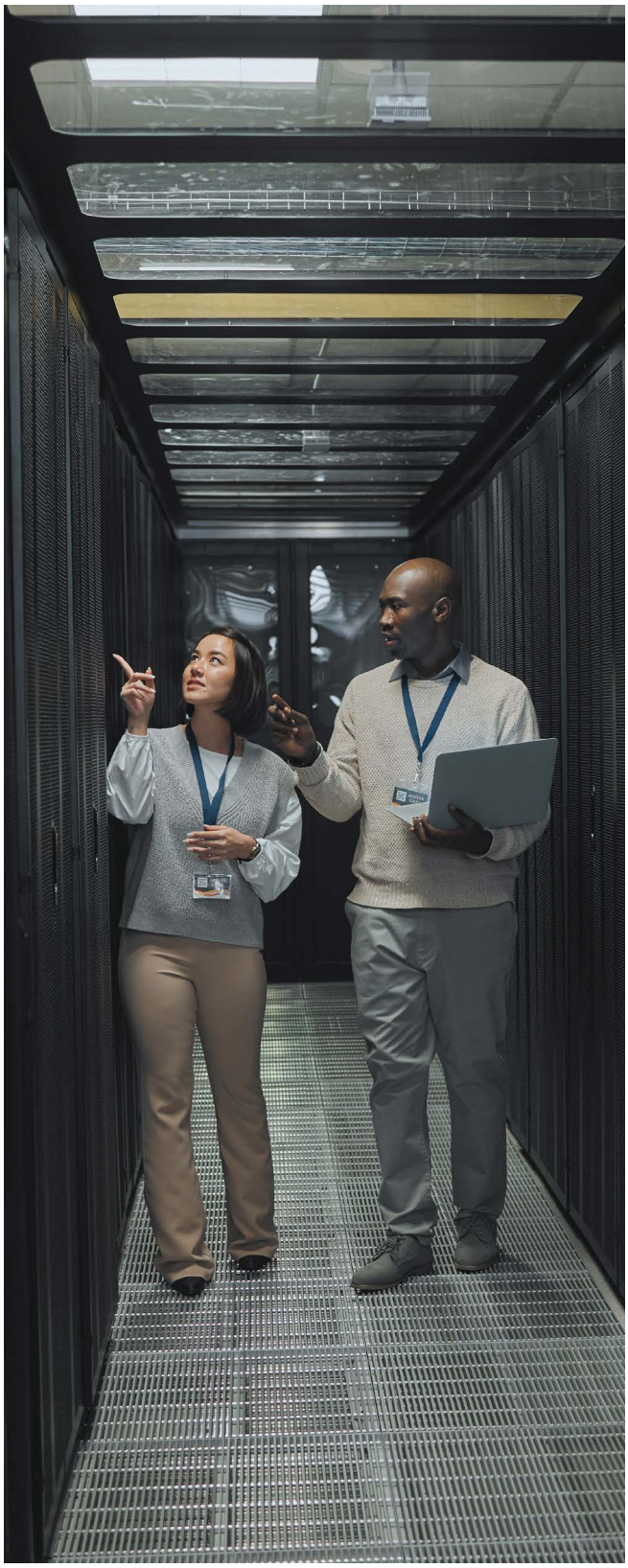


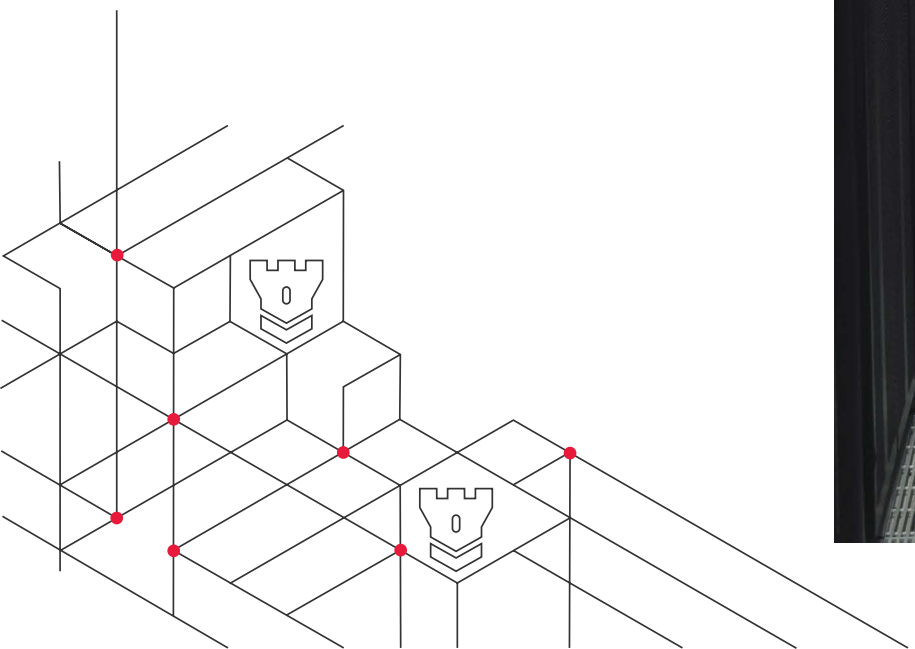
How BDO can help

BDO's cybersecurity team understands the risks associated with disruptive technology and offers a comprehensive suite of cybersecurity services designed to safeguard your organisation. Our approach includes thoroughly assessing your cybersecurity maturity level, testing your network for vulnerabilities, and assessing risk comprehensively. Set up a consultation with our team today to review your organisational structure for security concerns.

BDO has been recognised a winner of multiple 2024 Microsoft Partner of the Year Awards, and leading provider of cybersecurity solutions for business. We provide end-to-end solutions leveraging the advanced security and identity capabilities of Microsoft 365 and Microsoft Azure Security.

ADVANCED CYBERSECURITY FOR YOUR ORGANISATION | BDO - BDO





Gilchrist Mushwana

Advisory Director: **Cyber Security**
GMushwana@bdo.co.za

Elevating **people.**
Elevating **business.**
Elevating **society.**

BDO
AUDIT • ADVISORY • TAX