P2D
TECHNOLOGY SERVICES

ENHANCING CYBERSECURITY FOR A SECURE FUTURE

Understanding Cybersecurity

cybersecurity serves as a shield against unauthorised access and threats in the digital landscape, ensuring the confidentiality, integrity, and availability of our data. It is the frontline defence against cyber adversaries who seek to compromise our digital existence, making it an essential component of personal and organisational data protection.

THE IMPORTANCE OF CYBERSECURITY

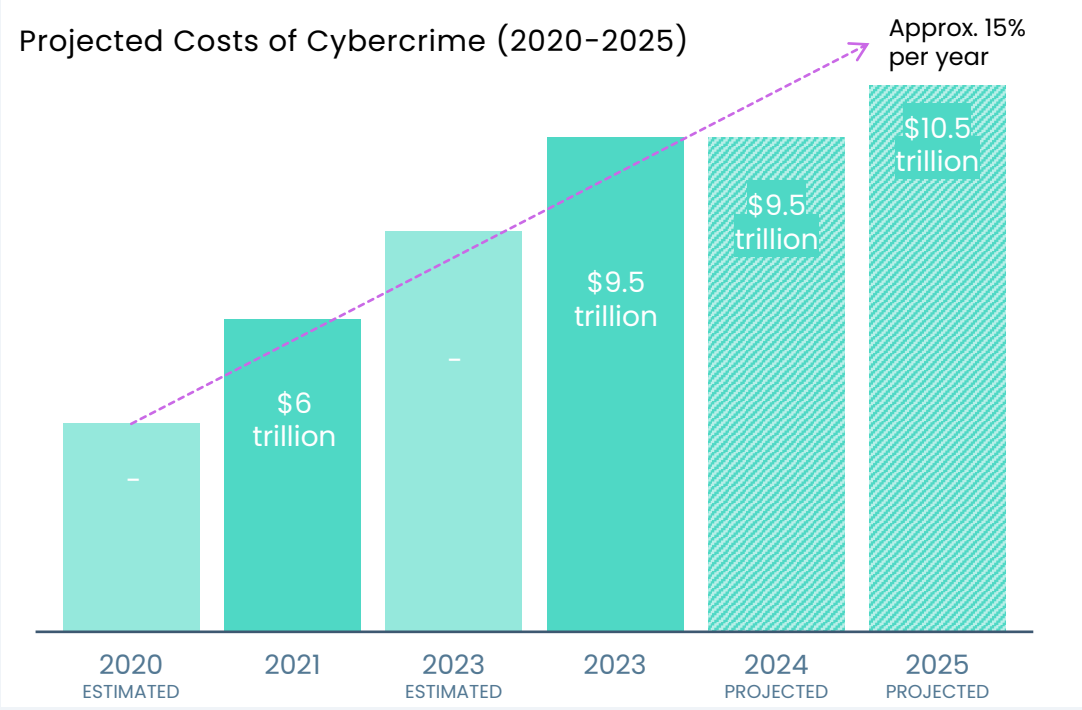
Cybersecurity is crucial in today's digital age, protecting our computers, networks, and data from unauthorised access and threats. It is essential for personal and organisational data protection.

It serves as the protector of supply chains, physical infrastructure, and external networks, including vital investment partnerships. Organisations that prioritise cyber resilience are better equipped to face the challenges of this new era, preserving the integrity and continuity of their operations in an increasingly interconnected world.

- 97% of organisations experiencing an increase in cyber threats.
- More than half of organisations prioritise strengthening third-party and external network defences, recognising these as the most vulnerable areas for attack.
- The cost of cybercrime is projected to reach a staggering $10.5 trillion annually by 2025.
- 86% of business leaders believe that global geopolitical instability is likely to result in a catastrophic cyber event within the next two years
- Levels of disruption have increased by 200% from 2017 to 2022.

These findings highlight the importance of incorporating cybersecurity measures into your business strategy and ecosystem to protect your assets, prevent threats, and build trust as your business grows.

To stay ahead of the curve, businesses must continuously update their cybersecurity measures and stay informed about the latest threats and trends in the industry.



HOW DOES CYBERSECURITY WORK?

Cybersecurity is a complex system that employs various technologies and protocols to protect digital assets. Its measures include access controls, firewalls, intrusion detection systems, encryption, endpoint security, security information and event management tools, penetration testing, security policies and training, incident response plans, continuous monitoring, and patch management. These measures work together to provide a comprehensive defence against evolving cyber threats.

BENEFITS OF CYBERSECURITY

Cybersecurity has numerous benefits, including operational excellence, growth acceleration, and strategic alignment. Robust cybersecurity practices across the organisation contribute to operational excellence. cybersecurity is a vital enabler, safeguarding critical assets and fostering trust with customers and stakeholders.

Organisations closely aligning cybersecurity with business objectives are 18% more likely to drive revenue growth, expand market share, and enhance customer satisfaction and employee productivity. Embedding cybersecurity from the start significantly improves transformation effectiveness.

Cybersecurity: Insights from 2023

In 2023, cybersecurity remains a key factor in enhancing enterprise innovation and supporting business continuity. In the changing environment of market challenges driven by technological developments, complex regulations, geopolitical changes, and economic variations, organisations globally face severe trials in risk management and resilience. The cybersecurity landscape is undergoing major changes with significant trends and shifts that are improving the digital protection strategies of organisations globally. With the emergence of advanced technologies such as artificial intelligence, quantum computing, and the Internet of Things (IoT), along with increasingly sophisticated cyber threats, businesses are required to strengthen their digital defences like never before.

HOW DO BUSINESSES UTILISE CYBERSECURITY?

Businesses have increasingly recognised the paramount importance of integrating cybersecurity from the inception of any transformation endeavour. Large organisations tend to undergo transformations at an accelerated pace and with greater frequency and some enterprises tend to use cybersecurity as a strategic advantage to achieve better business results.

Those organisations that strategically align their cybersecurity initiatives with overarching business objectives demonstrate an 18% increase in their capacity to foster revenue growth, expand market share, and elevate both customer satisfaction and employee productivity. Moreover, entities that seamlessly integrate crucial cybersecurity measures into their digital transformation endeavours, alongside implementing robust operational practices across their entire operational spectrum, are nearly six times more likely to achieve successful digital transformations compared to their counterparts who neglect these critical aspects.

Although an increasing number of organisations are beginning to recognise the importance of being secure from the start of any transformation effort, a significant proportion of organisations falter in engaging cybersecurity early in the transformational process, potentially hindering their ability to effectively tackle future challenges and capitalise on emerging opportunities. Some of these companies only deploy security controls post-transformation, often after vulnerabilities have been identified—a scenario epitomising the adage of 'too little, too late'. Recent studies underscore the substantial financial repercussions of such negligence, with errors detected in the coding phase costing five times more to rectify than if identified during initial planning, escalating to a staggering 30 times post-release.

> Organisations that strategically align their cybersecurity initiatives with overarching business objectives demonstrate an 18% increase in their capacity to foster revenue growth, expand market share, and elevate both customer satisfaction and employee productivity.

Key Cyber Threats And Their Impacts Over The Past Five Years

Key Cyber Threats And Their Impacts Over The Past Five Years

$53 BILLION
GLOBAL ECONOMY COSTS

Ransomware attacks have dramatically increased, particularly impacting the healthcare and education sectors. The education sector alone has seen ransomware attacks costing the global economy $53 billion in downtime.

35% GROWTH
IN JUST SIX MONTHS

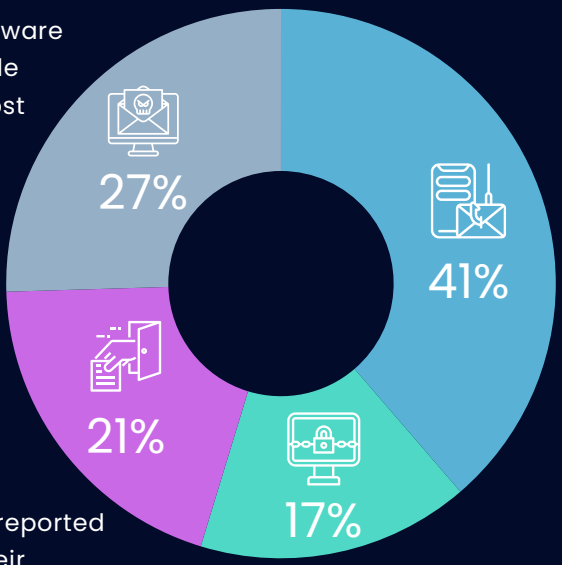
Significant increases in phishing and malware attacks have been noted, with IOT threats growing by approximately 35% in just six months from the second half of 2019 to the first half of 2020 (Norton Security) (Parachute).

$5M RANSOM
DEATH & ATTACKS

Notable cyber incidents include the ransomware attack on a German hospital that resulted in a patient death and the Colonial Pipeline attack, which led to a $5 million ransom payment (Norton Security).

Breakdown of Cyber Attack Types in 2023

EXTORTION
Extortion, evolving from ransomware and including threats like double and triple extortion, was the most common impact of attacks, seen in 27% of cases (Security Intelligence).

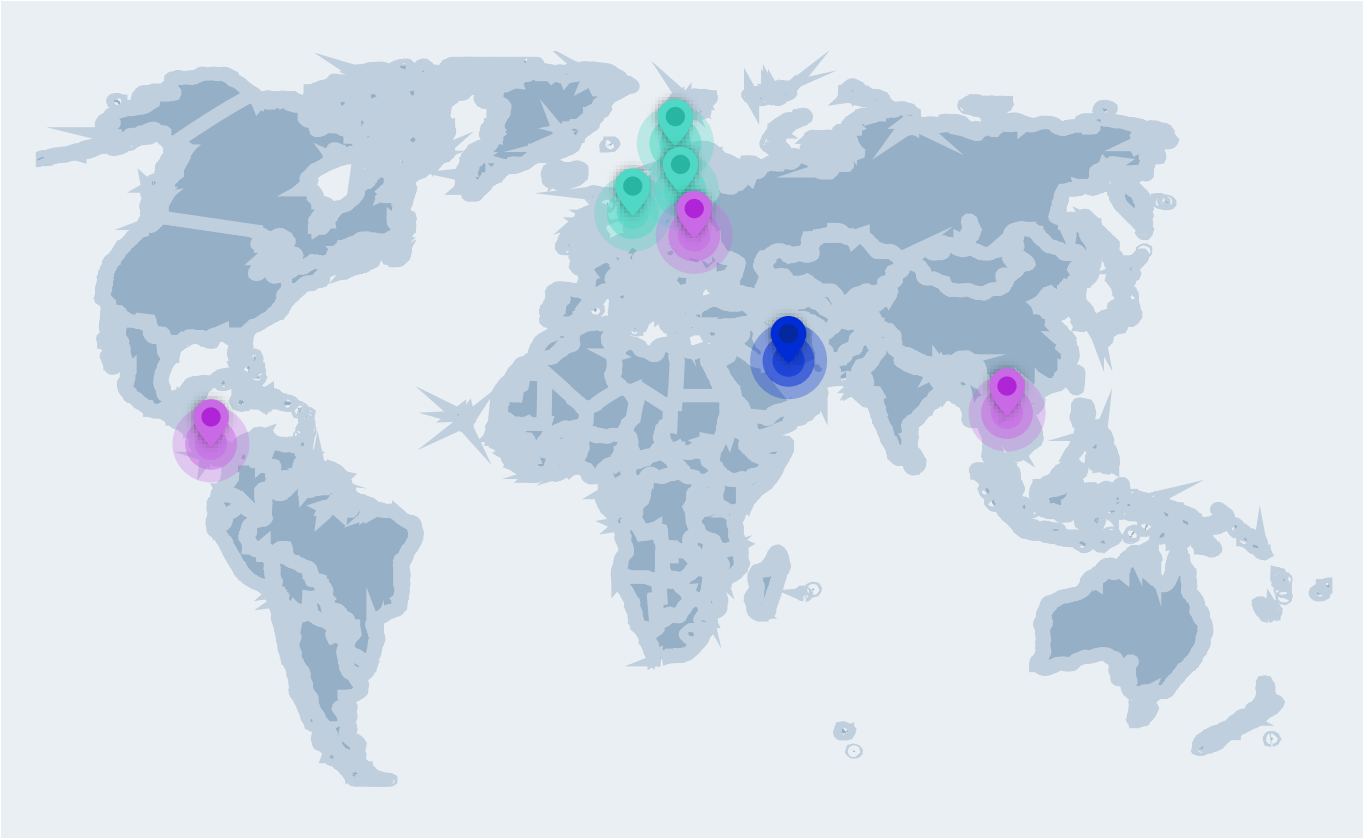


PHISHING ATTACKS
41% of incidents involved phishing as the initial access vector, highlighting its prevalence as a leading method used by attackers (Security Intelligence).

BACKDOORS
Deployment of backdoors was reported in 21% of cases, which shows their significant role in facilitating further malicious activities (Security Intelligence).

RANSOMWARE
Although previously the most common, ransomware now accounts for 17% of the incidents, indicating a slight decline as other attack types become more prevalent (Security Intelligence).

Key Cyber Threats And Their Impacts Over The Past Five Years



HIGH-RISK COUNTRIES:

Panama: Noted for its significant vulnerabilities due to poor digital development and a high Basel AML Index, making it highly susceptible to cyber threats.

Thailand and Belarus: Both countries also show high risk due to persistent challenges in digital development and legislative frameworks, with Belarus noted for the highest cybersecurity exposure.

NOTABLE REGIONS WITH HIGH CYBERCRIME COSTS:

United Arab Emirates: Specifically, Dubai faces one of the world's most costly cybercrime impacts, with each incident averaging $2.6 million despite recent updates to its cybersecurity strategy.

LOW-RISK NATIONS

Denmark: Stands out with a comprehensive national cyber and information security strategy, making it a model of effective cyber resilience.

Sweden and Finland: These Nordic countries are noted for their strong defences thanks to proactive cybersecurity strategies and high digital development levels.

WHO ARE THE CYBER TRANSFORMERS?

Some companies are leading the charge in digital transformation, earning the title "cyber transformers" through their successful implementation of cybersecurity measures. These organisations strike a crucial balance between strengthening cyber resilience and aligning with overarching business strategies, ultimately driving superior business outcomes.

One key aspect of these company's success is their integration of cybersecurity programs with core business objectives. By doing so, they increase their chances of achieving various key outcomes such as revenue growth, increased market share, enhanced customer satisfaction and trust, and greater employee productivity. What sets them apart is their proactive approach, involving the cybersecurity team from the outset of business planning, a practice that nearly doubles their effectiveness compared to others. Additionally, they demonstrate greater confidence in their organisation's internal cybersecurity planning processes.

Cyber transformers distinguish themselves by laying transformation foundations in two fundamental ways. Firstly, they embed three pivotal cybersecurity actions into their transformation efforts. Secondly, they establish robust groundwork by implementing stringent cybersecurity operational practices from the very beginning. These concerted efforts result in cyber transformers being nearly six times more likely to experience highly effective digital transformations compared to their counterparts. Their proficiency in utilising strong cybersecurity operational practices underscores their exceptional performance in navigating the complexities of the digital landscape.

STRATEGIES FOR SUCCESSFUL CYBERSECURITY IMPLEMENTATION

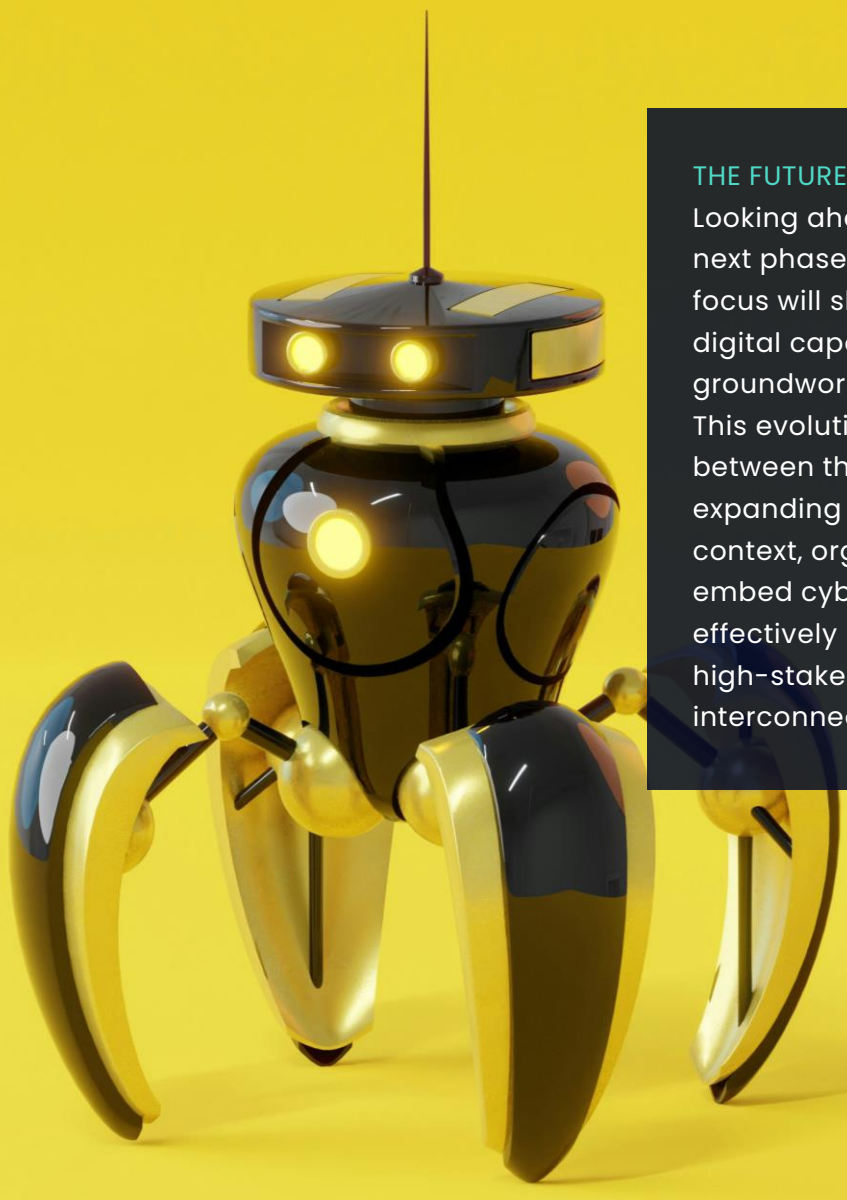
1. Ensure cybersecurity measures are in place before adopting new solutions.
2. Add cybersecurity progressively as digital transformation objectives are achieved.
3. Assign a cybersecurity representative to the main transformation team and a facilitator to oversee cybersecurity for all transformation projects.

HOW TO BE A CYBER TRANSFORMER:

Cyber transformers excel at cybersecurity operational practices that distinguish them from others.

1. Integration of risk management
2. The use of cybersecurity as a service to improve operational efficiency and address talent gaps with third-party services.
3. Commitment to protecting the ecosystem; include ecosystem partners in their incident response strategies and impose strict cybersecurity standards on them.
4. Automation is also important for cyber transformers, with 89% of them relying on it heavily.

The integration of cybersecurity is vital for the success of any transformation endeavour. By following the lead of cyber transformers, business leaders can extend the influence of cybersecurity beyond immediate protection to actively shaping continuous, dynamic reinvention.



THE FUTURE OF CYBERSECURITY

Looking ahead, as we transition towards the next phase of business transformation, the focus will shift from managing disparate digital capabilities towards laying the groundwork for a cohesive shared reality. This evolution will blur the boundaries between the physical realm and the rapidly expanding digital domain. Within this context, organisations must seamlessly embed cybersecurity at every juncture to effectively navigate the intricacies and high-stakes scenarios of this interconnected landscape.

How Generative AI Affects Cyber Threats

How do attackers and defenders compare in the field of generative AI and cybersecurity?

The World Economic Forum's Global Cybersecurity Outlook Report 2024 says that 56% of executives expect that attackers will keep having an edge over defenders in the next two years, showing the urgent need to change how cybersecurity is approached in the era of generative AI.

GENERATIVE AI IMPACT ON THE RISKS OF CYBERATTACKS

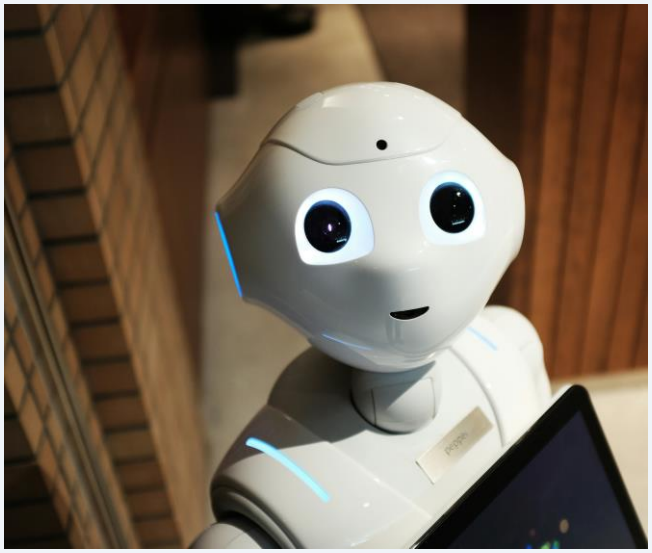
Generative AI is behind more and more cyberattacks, as cybercriminals use it to exploit businesses and government agencies. Ransomware attacks have gone up by 76% since ChatGPT came out at the end of 2022. These attacks usually start from generative AI phishing emails and hit sectors like local government, education, manufacturing, and healthcare. According to Accenture Cyber Intelligence research, specific industries such as financial services, government, and energy are prime targets for generative AI attacks due to their use of advanced technology, rendering them susceptible to sophisticated attacks.

Malicious large language models (LLMs), including Fraud GPT and PentestGPT, are being utilised to generate content facilitating cyberattacks, available for as little as $200 per month on the dark web. Moreover, there is a notable increase in voice deepfakes impersonating executives to deceitfully authorise financial transactions. For instance, a sophisticated deepfake scam resulted in a $25 million loss for Hong Kong Bank, where scammers digitally replicated the company's chief technology officer and other employees in a conference call instructing colleagues to transfer funds. Threat actors such as the hacktivist group Ghost Sec are experimenting with dark LLMs to develop Python-based ransomware, distributed with extensive obfuscation to enhance its success rate.

VULNERABILITIES OF GEN AI

Generative AI brings more threats, stronger attackers, and new weaknesses for organisations. As they use Gen AI more widely and deeply, cybersecurity risks grow. More scale and complexity of adoption, with more users, data, and integration, create risks like Gen AI model disruptions, prompt injections, data exposure, theft, and manipulation. These are new problems, and most organisations can't handle them. They need new abilities like shadow AI discovery, LLM prompt and response filtering, and specialised AI workload integration tests to deal with these changing risks.

Generative AI brings more threats, stronger attackers, and new weaknesses for organisations.



Benefits of Gen AI for Cybersecurity

Gen AI offers a chance for the transformation of cybersecurity and strengthening cyber defence capabilities. By using Gen AI to its full potential, organisations can efficiently deter potential attackers and improve their cyber defence capabilities. AI-powered threats cannot be stopped by conventional security measures. Organisations should adopt AI-powered protection technologies and perform tests using Gen AI technologies similar to those used by attackers. Examples include AI-powered red teaming and penetration testing, which are likely to become required as Gen AI regulations develop. AI security features are becoming more common among platform companies and hyperscalers, both for their own use and for others to access.

Enhancing the Safety of Gen AI Advancement

Forward-thinking companies recognise that security is not a hindrance but a catalyst for accelerating Gen AI success.

Companies should follow these suggestions to speed up the use of Gen AI and protect their Gen AI systems well:

1. Integrate Gen AI security into Governance, Risk, and Compliance (GRC): Incorporate Gen AI security into GRC frameworks to establish clear governance structures, policies, and processes. Organisations must stay abreast of evolving regulations to ensure compliance and influence future regulations through collaboration with regulators.
2. Measure Gen AI security risks: Use updated cyber intelligence to test how secure Gen AI environments are. Check if Gen AI architectures follow industry standards and conduct comprehensive security assessments.
3. **Protect every level of Gen AI environments:** Secure the whole Gen AI stack, including the data layer, foundational models, Gen AI applications, and identity access and controls. Besides usual security measures, organisations should look for AI-specific solutions to deal with the special risks of Gen AI environments.

Tools For Improving Cybersecurity Practices

cybersecurity SCORECARD

To further empower organisations in strengthening their cyber defences, this report introduces the "cybersecurity Scorecard" — a strategic tool designed to assess and visualise your cybersecurity readiness across key domains.

The scorecard evaluates areas such as Risk Management, Asset Management, Access Control, Threat Protection, Incident Response, and Recovery Plans. Each domain is scored based on a scale from 1 (Poor) to 5 (Excellent), reflecting the organisation's alignment with industry best practices such as those outlined in the NIST Cybersecurity Framework and ISO 27001. This comprehensive evaluation provides actionable insights, highlighting strengths and pinpointing critical areas for improvement. By integrating the cybersecurity Scorecard into your security strategy, your organisation can quantify its security posture, prioritise cybersecurity investments, and benchmark progress against the evolving threat landscape. This tool is essential for any business seeking to enhance its cybersecurity measures and safeguard its digital and physical assets in an increasingly interconnected world.

Example of a business performance scorecard:
This type of scorecard typically covers different functional areas to provide a holistic view of performance.

AREA	METRICS	CURRENT STATUS	TARGET	GAP ANALYSIS	RECOMMENDATIONS
Revenue	Total Revenue	$2M	$2.5M	$0.5M Short	Diversify product offerings
Revenue Growth Rate	5%	8%	3% Gap	Increase marketing efforts	
Costs	Operating Costs	$1M	$0.8M	$0.2M Over	Optimize supply chain
Cost Reduction	2%	5%	3% Gap	Implement lean practices	
Efficiency	Employee Productivity	70%	85%	15% Gap	Training and development
Production Efficiency	80%	90%	10% Gap	Upgrade equipment	
Customer	Customer Satisfaction Rate	80%	95%	15% Gap	Improve customer service
Net Promoter Score (NPS)	30	50	20 Points	Enhance customer engagement	
Innovation	New Products Launched	2	5	3 Short	Foster a culture of innovation
R&D Investment as % of Revenue	3%	5%	2% Gap	Increase R&D budget	
Compliance	Regulatory Compliance Violations	1	0	1 Violation	Strengthen compliance checks
Environmental Impact Reduction	10%	20%	10% Gap	Implement green technologies	

Explanation of Table Columns:

- Area: Broad categories like Revenue, Costs, Efficiency, Customer, Innovation, Compliance.
- Metrics: Specific indicators within each area.
- Current Status: The current measured value of the metric.
- Target: Desired or benchmark value for the metric.
- Gap Analysis: Difference between current status and target.
- Recommendations: Suggested actions to close the gap or improve performance.

Secure Your Future Today

In today's interconnected world, cybersecurity is no longer a luxury but a necessity. With cybercrime costs projected to reach $10.5 trillion annually by 2025, the urgency to bolster defenses is evident. As cyber threats increase by 97%, organisations must prioritize protecting their digital assets.

Businesses face numerous challenges, from ransomware attacks, which now constitute 17% of cyber incidents, to phishing, the leading method for initial breaches at 41% (Security Intelligence). Moreover, 86% of business leaders anticipate a major cyber event due to geopolitical instability within the next two years.

Proactive cybersecurity strategies not only safeguard assets but also enhance operational efficiency and foster customer trust. Companies integrating cybersecurity from the start of any transformation process see an 18% increase in revenue growth and market.

Don't wait until it's too late.

Fortify your business against cyber threats and ensure a secure future. Our expert team is here to help you navigate the complexities of cybersecurity.

Contact us to learn how we can help you navigate the complexities of cybersecurity, protect your business, and build a secure future.

P2D
TECHNOLOGY SERVICES

+44 (0) 2036 378 507

Orega 202, Marlow International,
Parkway, Marlow, SL7 1YL

info@p2dl.com