EXECUTIVE SUMMARY

CYBER WARS

THE ENTERPRISE STRIKES BACK

FROST & SULLIVAN

NTT Communications
Transform. Transcend.

NTT Security

Building a Cyber Resilient **Enterprise**

People and businesses are heavily reliant on technology and the internet in this day and age. With the advent of Internet of Things (IoT), this complex and interconnected environment, while convenient, is becoming increasingly vulnerable to cyber threats. Cyber threats hugely affect the operation of a business; its costs and impact are substantial.

The convergence and interdependency of technology make guaranteed protection impossible. Most frequently, cyber risks are caused by human behaviour rather than from system flaws or technological weaknesses. Organizations need to work with their internal stakeholders to promote awareness and understanding to minimize cyber risks by building cyber resilience.

A cyber resilient organization is one which strives to achieve the highest level of organizational readiness against any given cyber-physical security breach. It does this by cultivating the ability to manage, recover and learn from any security episode through the re-engineering of socio-behavioural tendencies, security expertise and operational protocols.

Re-thinking Cyber Security Through a **Cyber Risk Mindset**

Cyber-attacks cause real world harm.

According to Frost & Sullivan's research, most Asia-Pacific organizations take around a day to detect a major security incident and another day to respond.

This can potentially cause irreparable harm to an enterprise's business operations. How then can enterprises best plan their cyber security strategy?

SECURING THE HUMAN FACTOR

People working in and around an enterprise need to be a key consideration. Frost & Sullivan defines the human threat with 4E's:

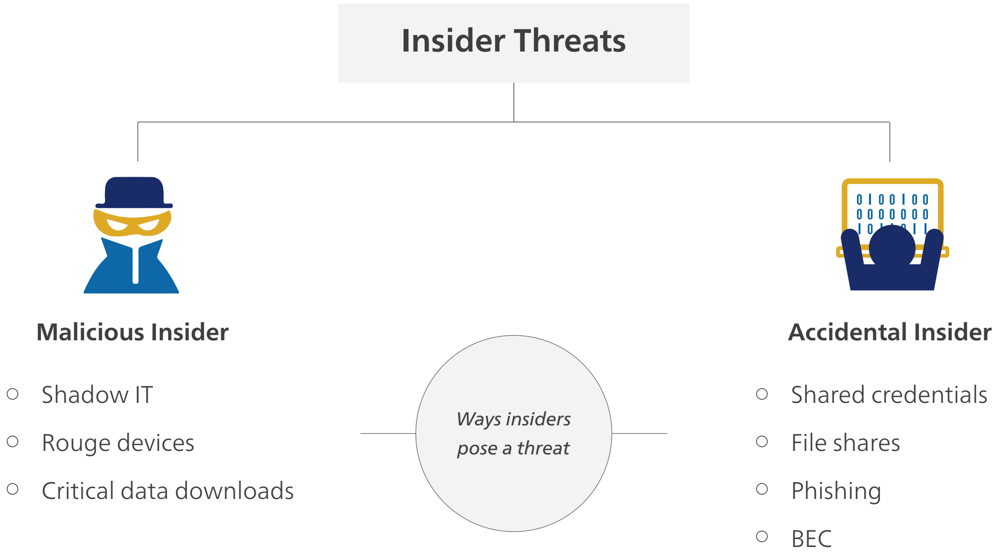
Employees
Perennial threat from the inside

Eco-system
Extension of the insider threat

End-users
Increasingly leveraged

Expertise
New threat on the inside

Frost & Sullivan proposes that organizations develop an insider threat program that holistically and effectively combines people, process and technology principles that covers both malicious and accidental insiders.



Insider Threats

Ways insiders pose a threat

Malicious Insider

- Shadow IT
- Rouge devices
- Critical data downloads

Accidental Insider

- Shared credentials
- File shares
- Phishing
- BEC

Security controls and practices needed to mitigate insider threats

Technology
People
Process

RISE OF THE MACHINES

With the increasing adoption of Internet of Things (IoT) in many businesses today, enterprises have to plan for cyber security in areas of IT, OT and IoT.

However, the IT and OT cultures are very different in terms of environment (equipment set up), skillset (IT and OT engineers has different knowledge) and business silos (ownership and responsibility). The cultural difference is one of the key challenges in IT/ OT convergence.

Frost & Sullivan recommends that organizations extend the cyber security paradigm. Traditionally, many organizations establish a 'Prevent', 'Detect' and 'Remediate' approach. Organizations need to use data and extend this paradigm further to gain 'Predict' and 'Measure' outcomes as well.

KEY TAKEAWAYS

1. *Insider threats are an organization's most significant weakness.*
2. *Cyber-Physical security is the new reality of enterprises and there needs to be 'IT', 'OT', and 'IoT' security protection.*
3. *Enterprises need to address cyber risk across the whole organization from assessment, to treatment and recovery.*

PREDICT	**PREVENT**	**DETECT**	**REMEDIATE**	**MEASURE**
Assessing the unknown	*Security by design*	*Real-time detection*	*Scope and quarantine*	*Evaluate and benchmark*
○ Security analytics ○ Security telematics ○ Cognitive security ○ Artificial intelligence	○ Deceptive security ○ Patch management ○ Secure coding	○ Threat hunting ○ Retrograde detection-breach assessment ○ Distributed forensics	○ Automated policy enhancement ○ Hardened code management	○ Single pane of discovery ○ Dashboard management ○ Management reporting ○ Workflow integration ○ Metric-based

Managing Cyber Risk in the **Boardroom**

There are 4 key elements from a global cyber risk outlook:

1. *Breaches will continue while penalties and costs will continue to burden the private sector*
2. *Boardroom digital diversity will improve slowly, until it is forced by external stakeholders*
3. *A tsunami of regulation will prove ineffective at lowering risk, and will be very costly*
4. *Self-governance and enhanced defence will become strategic advantage of nation state and private companies.*

When protecting an organization's data, organizations should take into account that data protection is not only the subject of CSO/CISO/CIO, but is now a fundamental issue across divisions such as ICT, Legal, Finance, and needs to be led by the CEO and C-suite.

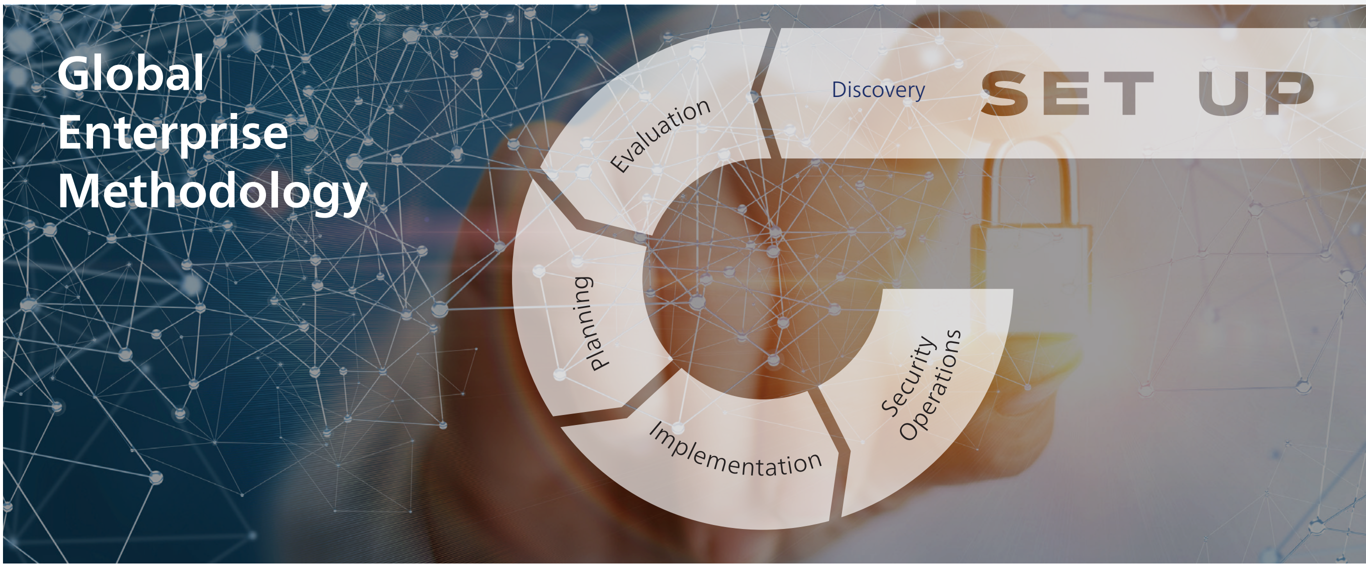
In addition, trust is the most important factor to an organization. Trust enables businesses and being cyber secure enables digital trust.

Therefore it can be said that 'Cyber security enables Business'. Cyber security is important in gaining the trust of customers.

The Global Enterprise Methodology is a five phase approach that enables organizations to understand their current risk exposure and make informed decisions for continuous risk management.

KEY TAKEAWAYS

1. *There is a need to understand the cyber security global mega-trends to address data protection in each organization.*
2. *Data protection in organizations is not only the responsibility of the IT division or CSO/ CISO/ CIO. It is the responsibility of the will be C-suites with involvement from respective business units such as legal, finance and others.*
3. *When organizations do business in this new digital world, cyber security and data protection are critical components in gaining customer trust and this can bring about better business growth.*



Building Cyber Ready Business - **What the Experts Say**

Kenny Yeo
Industry Principal
Frost & Sullivan

Humans remain the weakest security link. 91% of cyber attacks still start with a phishing mail and a lack of training in both people and process among enterprises can result in loss of brand trust, putting organizations and consumers at risk. It is critical to embrace a holistic 'people, process and technology' approach to cyber security.

Dr Leong Chou Ching
General Manager, IT
MindChamps

We need to understand the potential business impact of any disruption. How will your business be affected? For MindChamps, there is a strong focus on cyber security because we have a lot of sensitive information. We frequently review the security paradigm with a focus on user education, where users need to be well-aware of environmental threats.

Steven Sim Kok Leong
Vice President
ISACA Singapore

One of the biggest challenges large enterprises today face is reconciliation of the different security requirements of different offices within the organization. Firstly, you need to identify your organization's assets in terms of IT environment for the majority of the organization, as well as OT environment, if it exists.

K.K. Lim
Advocate & Solicitor
Lex Advocatus

It is important for companies to have a good cyber security framework. There must be buy in from top management. Policies have to be clear, along with the roles and responsibilities of the people in charge of cyber security. There must be a holistic approach; risk management cannot be treated in silos. From a legal stand point, make sure your organization takes care of its contracts with vendors and third parties.

Raymond Teo
Senior Vice President,
Business Development,
APAC
NTT Security

From a security service provider standpoint, there are no solutions that are 100% secure. Organizations need to change their mindset from viewing cyber security as a 'Cost' to that as a spending of "Necessity". Cyber security expenditure are similar to a country's military spend and cannot be viewed using a conventional business ROI lens.

NTT Communications

Transform. Transcend.

NTT Security

About NTT Communications

NTT Communications solves the world's technology challenges by helping enterprises overcome complexity and risk in their ICT environments with managed IT infrastructure solutions. These solutions are backed by our worldwide infrastructure, including industry leading, global tier-1 public and private networks reaching over 190 countries/regions, and more than 400,000m2 of the world's most advanced data center facilities. Our global professional services teams provide consultation and architecture for the resiliency and security required for your business success, and our scale and global capabilities are unsurpassed. Combined with NTT Data, NTT Security, NTT DOCOMO and Dimension Data, we are NTT Group.

For more information, please visit www.sg.ntt.com
Email enquiry@ntt.com.sg
Facebook @NTTSingapore
Linkedin @ntt-singapore
Twitter @NTTSingapore

About NTT Security

NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies to deliver resilient business solutions for clients' digital transformation needs. NTT Security has 10 SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit nttsecurity.com to learn more about NTT Security or visit www.ntt.co.jp/index_e.html to learn more about NTT Group

FROST & SULLIVAN

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? Contact us: Start the discussion

www.frost.com

For more about how to build resilience into your enterprise, please visit http://create.ntt.com.sg/security

Contact Us

Frost & Sullivan
apacfrost@frost.com
+65 6890 0999

NTT Communications
marketing@ntt.com.sg
+65 6438 3101

NTT Security
marketing-apac@nttsecurity.com