

Cyber Risk

A Threat to the Digital Agenda

Vincent Loy, PwC Singapore

*Strictly Private
and Confidential*

June 2015



Table of Contents

1 Cyber – Opportunities and Threats

2 Cyber Threats – Why, Who, What and How?

3 Putting Cyber Threats in Perspective



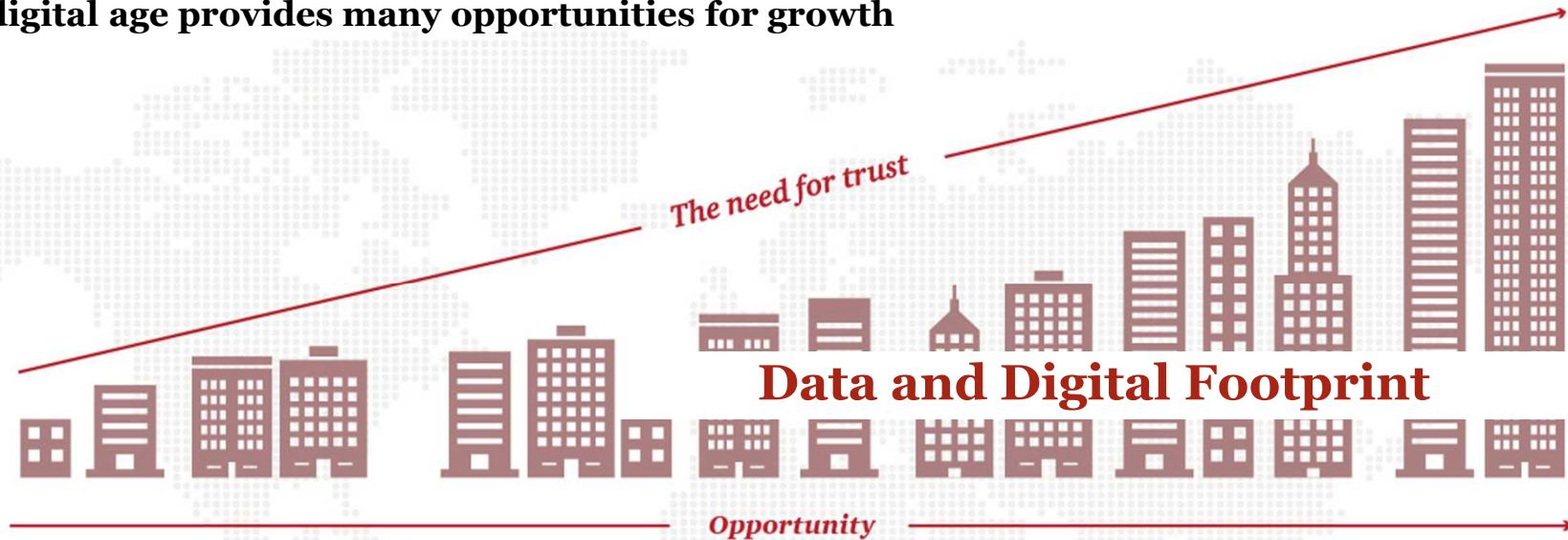
Section 1

Cyber – Opportunities and Threats



The New Dynamic- New Opportunities

The digital age provides many opportunities for growth



Automation



*Mobile/
Social
media*



Innovation



*Cost
efficiency-
Cloud*



*Hyper-
connectivity
& Integration*



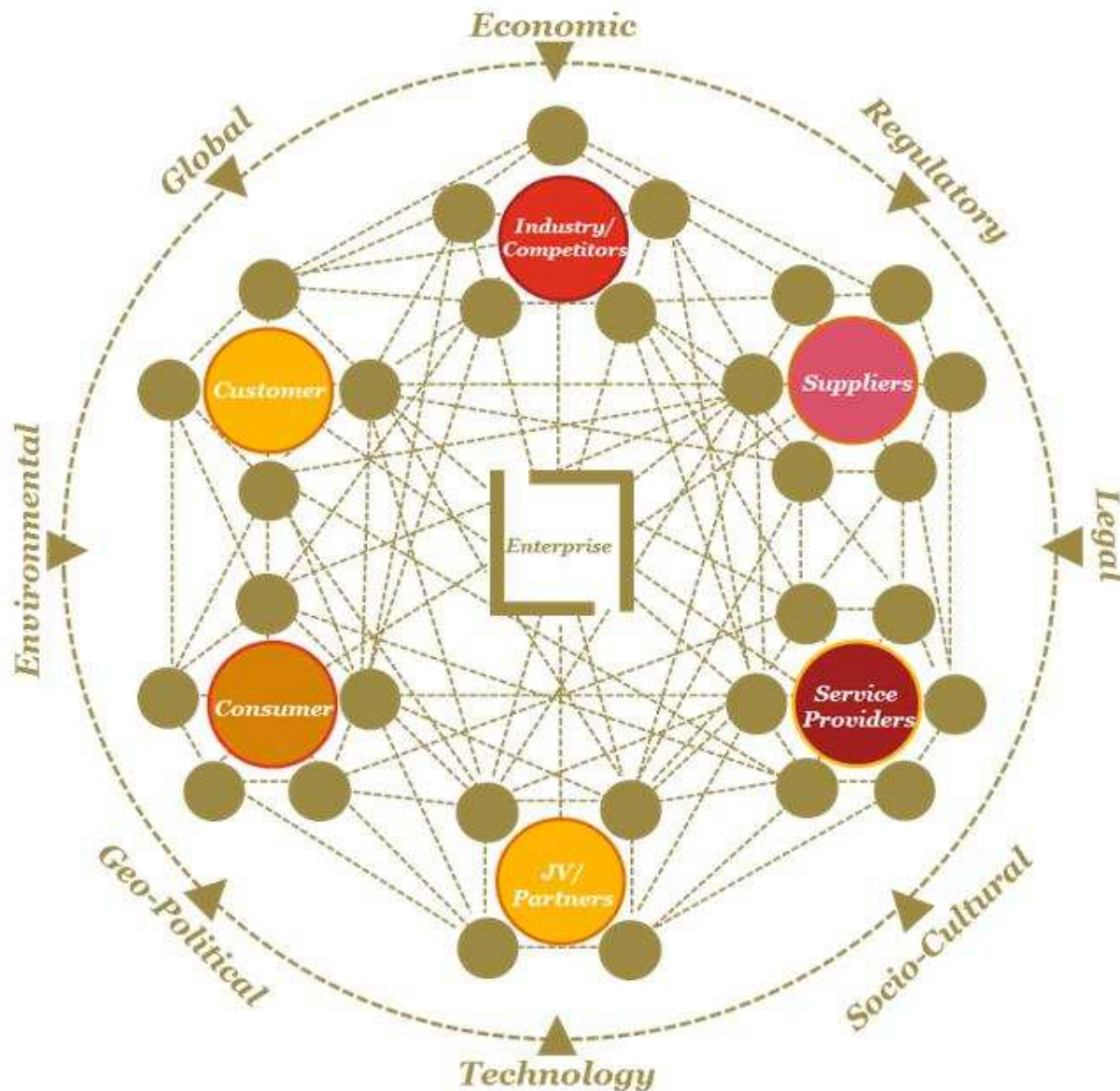
*Expanded
Sphere*



*Collaboration &
Trust*

Trust + Opportunity = Growth

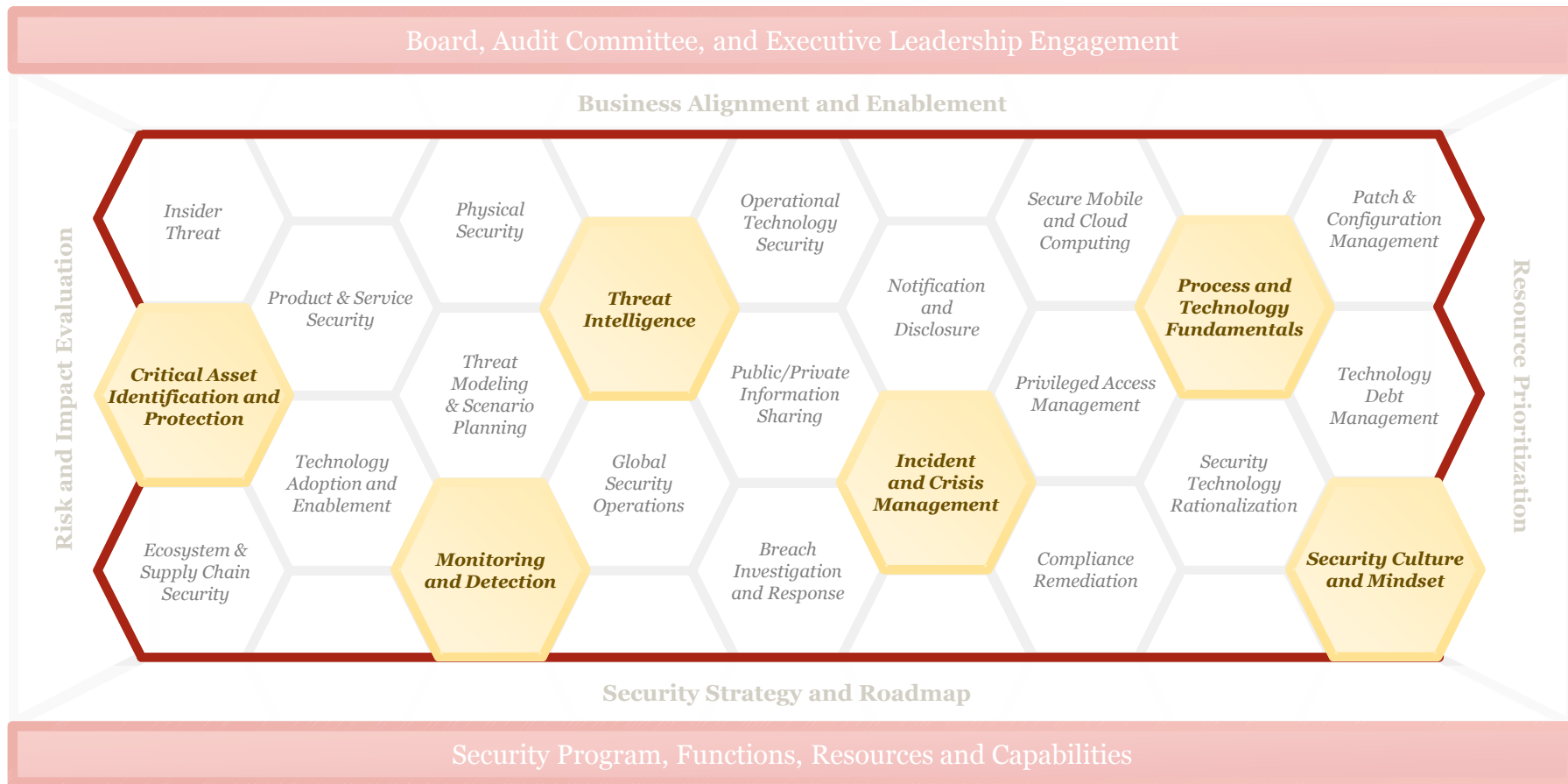
The New Global Business Ecosystem- The Risks



- **Interconnected, integrated, and interdependent** environments
- An ecosystem built around a model of **open collaboration and trust**
- **Constant information flow is the lifeblood** of the business ecosystem
- Adversaries are **actively targeting** critical assets
- Years of **underinvestment**

The Risks- Organizations have not kept pace

Years of underinvestment in certain areas has left organizations unable to adequately adapt and respond to dynamic cyber risks.



Section 2

Cyber Threats – Who, What and How?



Who are we protecting against



The Actors and The Information They Target

Adversary



What's most at risk?

Industrial Control Systems (SCADA)



Emerging technologies



Payment card and related information / financial markets



Advanced materials and manufacturing techniques



Military technologies



R&D and / or product design data



Healthcare, pharmaceuticals, and related technologies

Business deals information



Health records and other personal data



Information and communication technology and data





Input from Office of the National Counterintelligence Executive, Report to Congress on the Foreign Economic Collection and Industrial Espionage, 2009-2011, October 2011.

Cyber Attacks – Significant business impacts



- Financial losses
- Share price
- Regulatory
- Costs of remediation & investigation
- Brand & reputation

Profiles of Threat Actors

Adversary	Motives	Targets	Impact
 Nation State	<ul style="list-style-type: none"> Economic, political, and/or military advantage 	<ul style="list-style-type: none"> Trade secrets Sensitive business information Emerging technologies Critical infrastructure 	<ul style="list-style-type: none"> Loss of competitive advantage Disruption to critical infrastructure
 Organized Crime	<ul style="list-style-type: none"> Immediate financial gain Collect information for future financial gains 	<ul style="list-style-type: none"> Financial / Payment Systems Personally Identifiable Information Payment Card Information Protected Health Information 	<ul style="list-style-type: none"> Costly regulatory inquiries and penalties Consumer and shareholder lawsuits Loss of consumer confidence
 Hacktivists	<ul style="list-style-type: none"> Influence political and /or social change Pressure business to change their practices 	<ul style="list-style-type: none"> Corporate secrets Sensitive business information Information related to key executives, employees, customers & business partners 	<ul style="list-style-type: none"> Disruption of business activities Brand and reputation Loss of consumer confidence
 Insiders	<ul style="list-style-type: none"> Personal advantage, monetary gain Professional revenge Patriotism 	<ul style="list-style-type: none"> Sales, deals, market strategies Corporate secrets, IP, R&D Business operations Personnel information 	<ul style="list-style-type: none"> Trade secret disclosure Operational disruption Brand and reputation National security impact

Section 3

Putting Cyber Threats in Perspective



Putting cybersecurity into perspective




Cybersecurity represents many things to many different people

Key characteristics and attributes of cybersecurity :

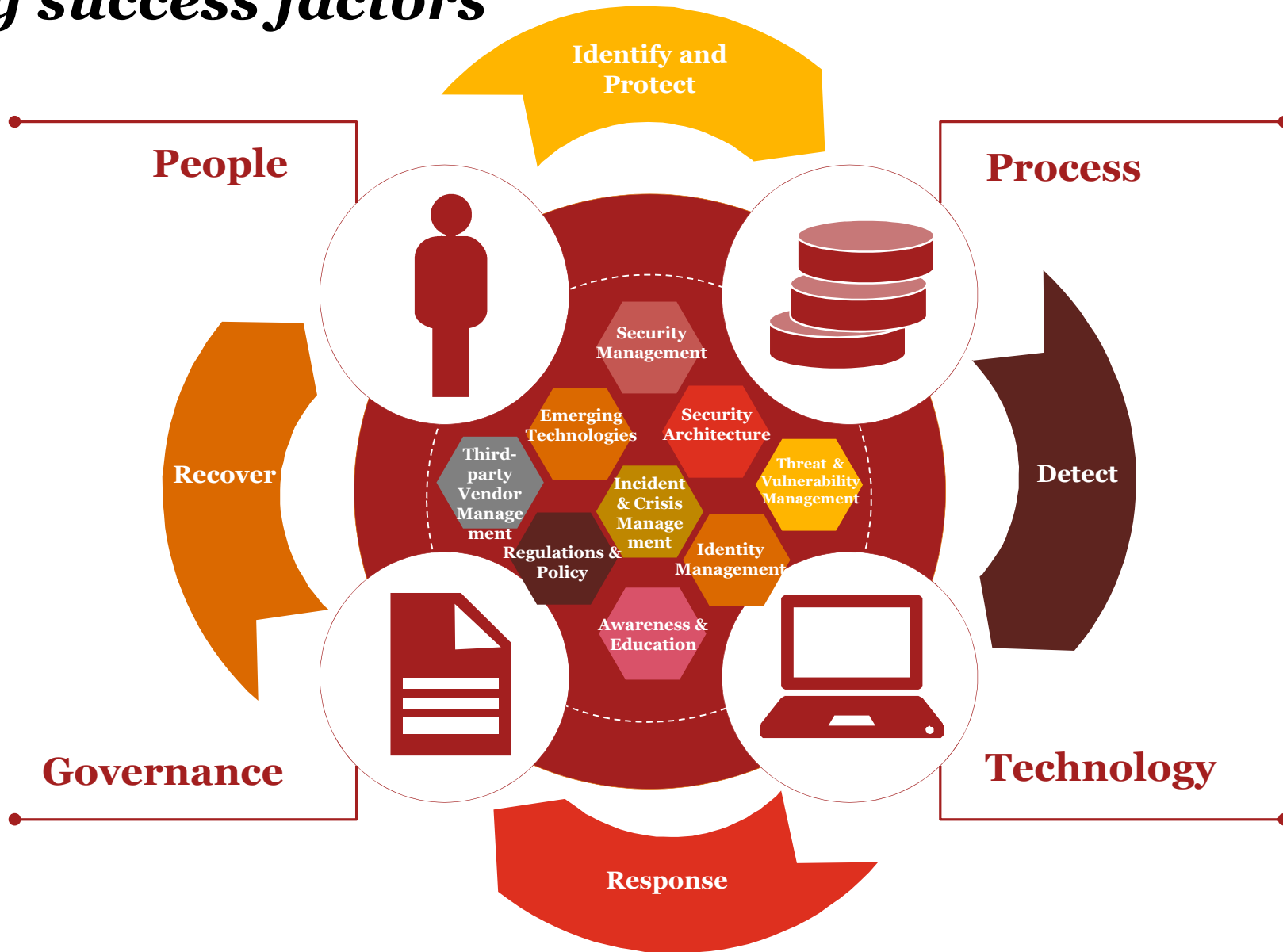
- **Broader** than just information technology and not limited to just the enterprise
- Increasing **attack surface** due to technology connectivity and convergence
- An ‘outside-in view’ of **the threats and potential impact** facing an organization
- Shared responsibility that requires **cross functional disciplines** in order to plan, protect, detect and respond

Evolving perspectives

Considerations for businesses adapting to the new reality

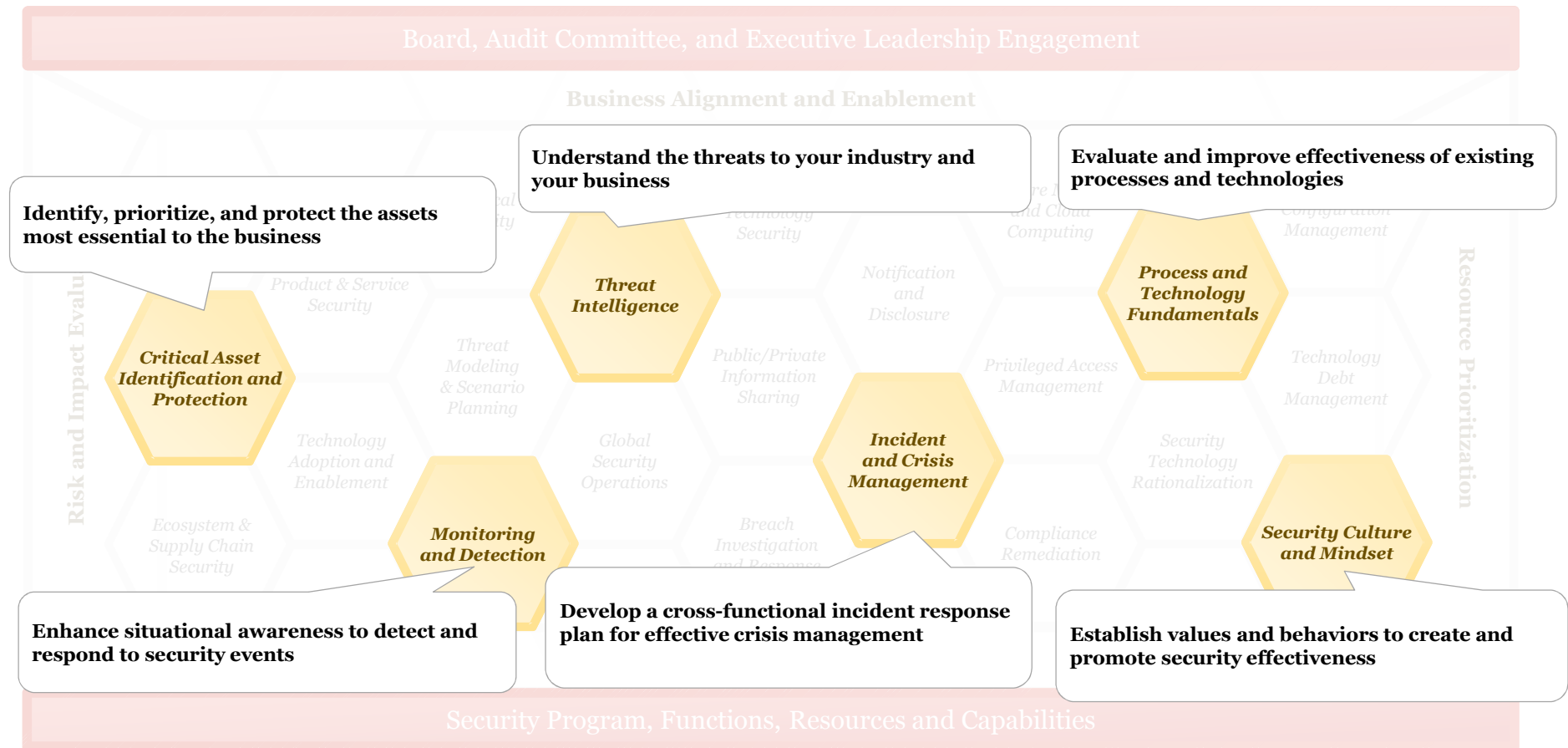
	Historical IT Security Perspectives	 Today's Leading Cybersecurity Insights
Scope of the challenge	<ul style="list-style-type: none"> Limited to your “four walls” and the extended enterprise 	<ul style="list-style-type: none"> Spans your interconnected global business ecosystem
Ownership and accountability	<ul style="list-style-type: none"> IT led and operated 	<ul style="list-style-type: none"> Business-aligned and owned; CEO and board accountable
Adversaries' characteristics	<ul style="list-style-type: none"> One-off and opportunistic; motivated by notoriety, technical challenge, and individual gain 	<ul style="list-style-type: none"> Organized, funded and targeted; motivated by economic, monetary and political gain
Information asset protection	<ul style="list-style-type: none"> One-size-fits-all approach 	<ul style="list-style-type: none"> Prioritize and protect your “crown jewels”
Defense posture	<ul style="list-style-type: none"> Protect the perimeter; respond <i>if</i> attacked 	<ul style="list-style-type: none"> Plan, monitor, and rapidly respond <i>when</i> attacked
Security intelligence and information sharing	<ul style="list-style-type: none"> Keep to yourself 	<ul style="list-style-type: none"> Public/private partnerships; collaboration with industry working groups

Key success factors



Process...

Questions to consider when evaluating your ability to respond to the new challenges.



Cyber Security Framework

Assess	Build	Manage	Respond
<p>Understanding your capabilities and maturity will help you prioritise your investment</p> <ul style="list-style-type: none"> Board-led maturity assessment Breach discovery assessment Cyber security diagnostic Cyber threat assessments and modelling Penetration testing Policy and contract review Privacy and cyber security legal assessment Standards compliance and certification Strategy and roadmap Third party assurance, including cloud Threat intelligence, detection and response maturity assessment 			

Assess	Build	Manage	Respond				
<p>Designing and delivering cyber security improvement programmes</p> <table border="0"> <tr> <td> <p>Framework development</p> <ul style="list-style-type: none"> Enterprise risk management Enterprise security architecture Information governance Privacy and cyber security legal strategy </td> <td> <p>Embedding security</p> <ul style="list-style-type: none"> Awareness and training Contracting for security CSIRT and policy development Insider threat management Legal policy development Product development support Security intelligence and analytics </td> </tr> <tr> <td colspan="2"> <p>Capability build</p> <ul style="list-style-type: none"> Cyber security programme delivery Security technologies and SOC development Threat intelligence, detection and response capability development </td> </tr> </table>				<p>Framework development</p> <ul style="list-style-type: none"> Enterprise risk management Enterprise security architecture Information governance Privacy and cyber security legal strategy 	<p>Embedding security</p> <ul style="list-style-type: none"> Awareness and training Contracting for security CSIRT and policy development Insider threat management Legal policy development Product development support Security intelligence and analytics 	<p>Capability build</p> <ul style="list-style-type: none"> Cyber security programme delivery Security technologies and SOC development Threat intelligence, detection and response capability development 	
<p>Framework development</p> <ul style="list-style-type: none"> Enterprise risk management Enterprise security architecture Information governance Privacy and cyber security legal strategy 	<p>Embedding security</p> <ul style="list-style-type: none"> Awareness and training Contracting for security CSIRT and policy development Insider threat management Legal policy development Product development support Security intelligence and analytics 						
<p>Capability build</p> <ul style="list-style-type: none"> Cyber security programme delivery Security technologies and SOC development Threat intelligence, detection and response capability development 							

Assess	Build	Manage	Respond
<p>Rapid, global access to leading cyber incident containment, investigation and crisis management expertise</p> <ul style="list-style-type: none"> Breach notification Computer, network and malware forensics Crisis management Cyber incident legal advice including privilege Cyber incident response and forensic investigation e-Discovery and disclosure Fraud and eCrime data analytics Human resource advice – employee breaches Network intrusion containment and remediation Regulatory proceedings Third party litigations 			

Assess	Build	Manage	Respond
<p>Managing and maintaining control of your business, enabling you to focus on strategic priorities</p> <ul style="list-style-type: none"> Advanced threat detection and monitoring Cyber defence team augmentation Data leakage monitoring Integrated managed security services Legal support to compliance officers and general counsel Managed vulnerability Retained incident response services Threat intelligence Security training 			

Cyber Risk

Challenges



**Lack of Board Cyber Education/
Training and CIO Briefings**



Understanding your current cyber security posture



Third party Security Risks



Cyber Risk: not part of ERM, poor MI



**Immature Cyber Incident Response
Management Process**



Difficulties in identifying/valuing Information Assets

Questions



Thank you.

Contacts Us:

Vincent Loy

Partner

Vincent.J.Loy@sg.pwc.com

Maggie Leong

Senior Manager

Maggie.Leong@sg.pwc.com

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, [insert legal name of the PwC firm], its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2015 PwC Singapore. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers LLP which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.