

Cyber Risk

– a threat to energy security

By Vincent Loy, PwC

October 2014



Agenda

- **Cyber- Opportunities and Threats**
- **Cyber Threats – Why, Who, What and How?**
- **Where are We?**
- **Putting Cyber Threats in Perspective**

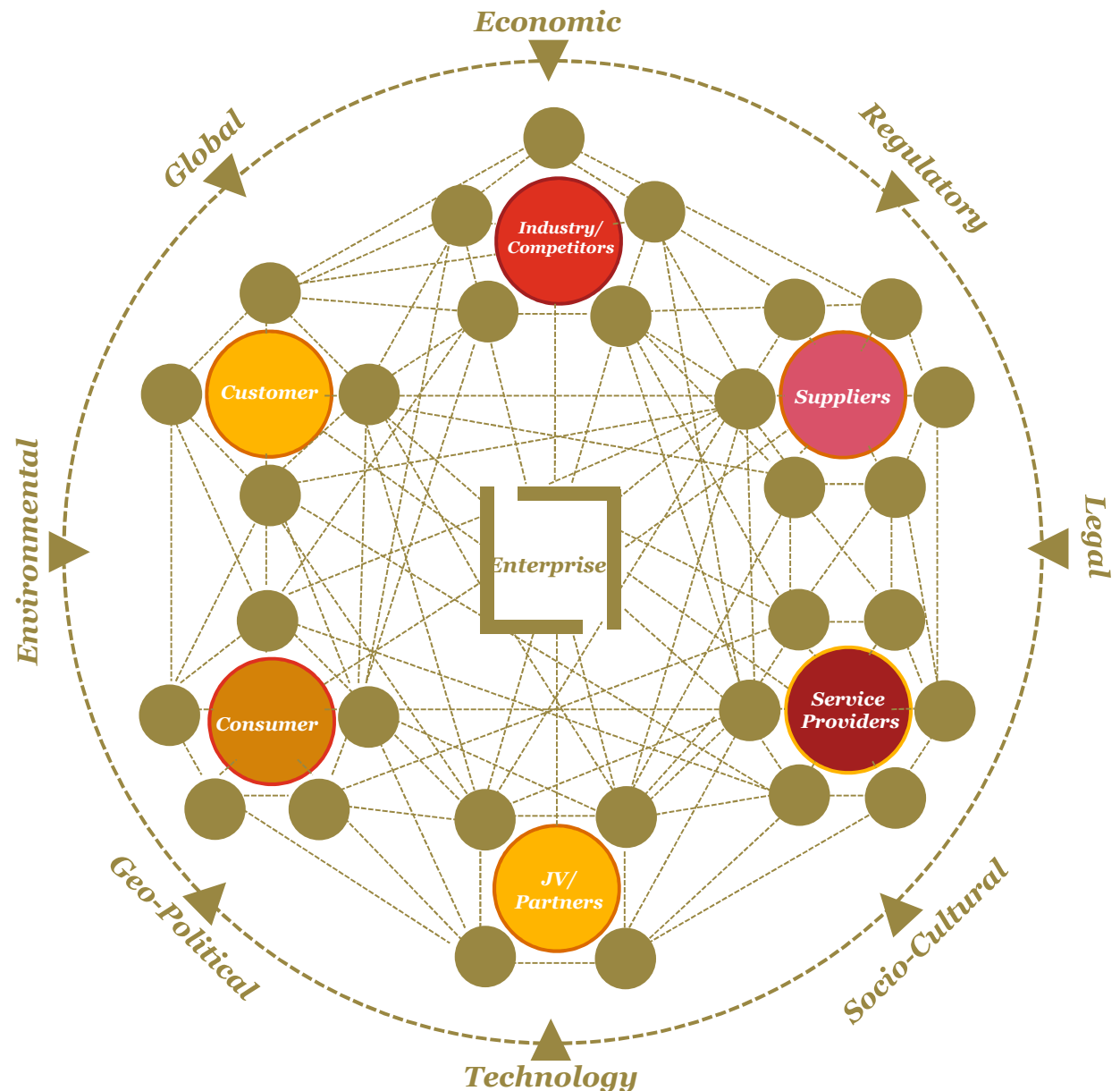
- **Cyber- Opportunities and Threats**

Everything has changed...

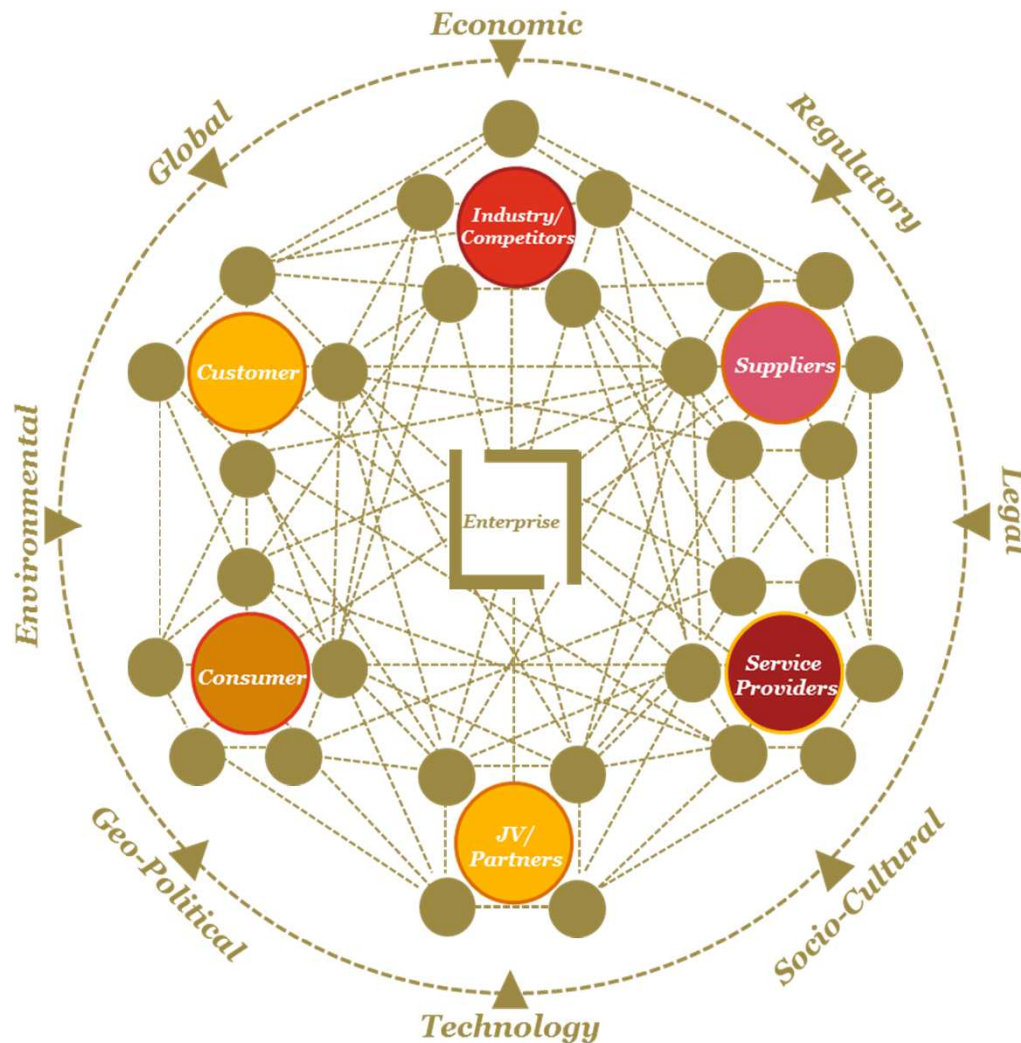


The New Global Business Ecosystem- The Opportunities

- An increase in reliance on technology
- Technology-led innovation has enabled business models to evolve
- Convergence of information technology, operational technology and consumer technology
- Information and data throughout the business ecosystem
- The extended enterprise has moved beyond supply chain and consumer integration
- Connectivity and collaboration now extends to all facets of business
- Transactions and operations spanning multiple parties
- Organisations built on trust and collaboration



The New Global Business Ecosystem- The Risks



- Traditional boundaries have shifted; companies operate in a dynamic environment that is increasingly **interconnected, integrated, and interdependent**.
- The ecosystem is **built around a model of open collaboration and trust**—the very attributes being exploited by an increasing number of global adversaries.
- Constant **information flow is the lifeblood of the business ecosystem**. Data is distributed and disbursed throughout the ecosystem, expanding the domain requiring protection.
- **Adversaries are actively targeting critical assets** throughout the ecosystem—significantly increasing the exposure and impact to businesses.
- **Years of underinvestment** in security has impacted organizations' ability to adapt and respond to evolving, dynamic cyber risks.

-
- **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.

Adversary motives and tactics evolve as business strategies change and business activities are executed; **'crown jewels' must be identified** and their protection **prioritized, monitored** and **adjusted** accordingly.

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

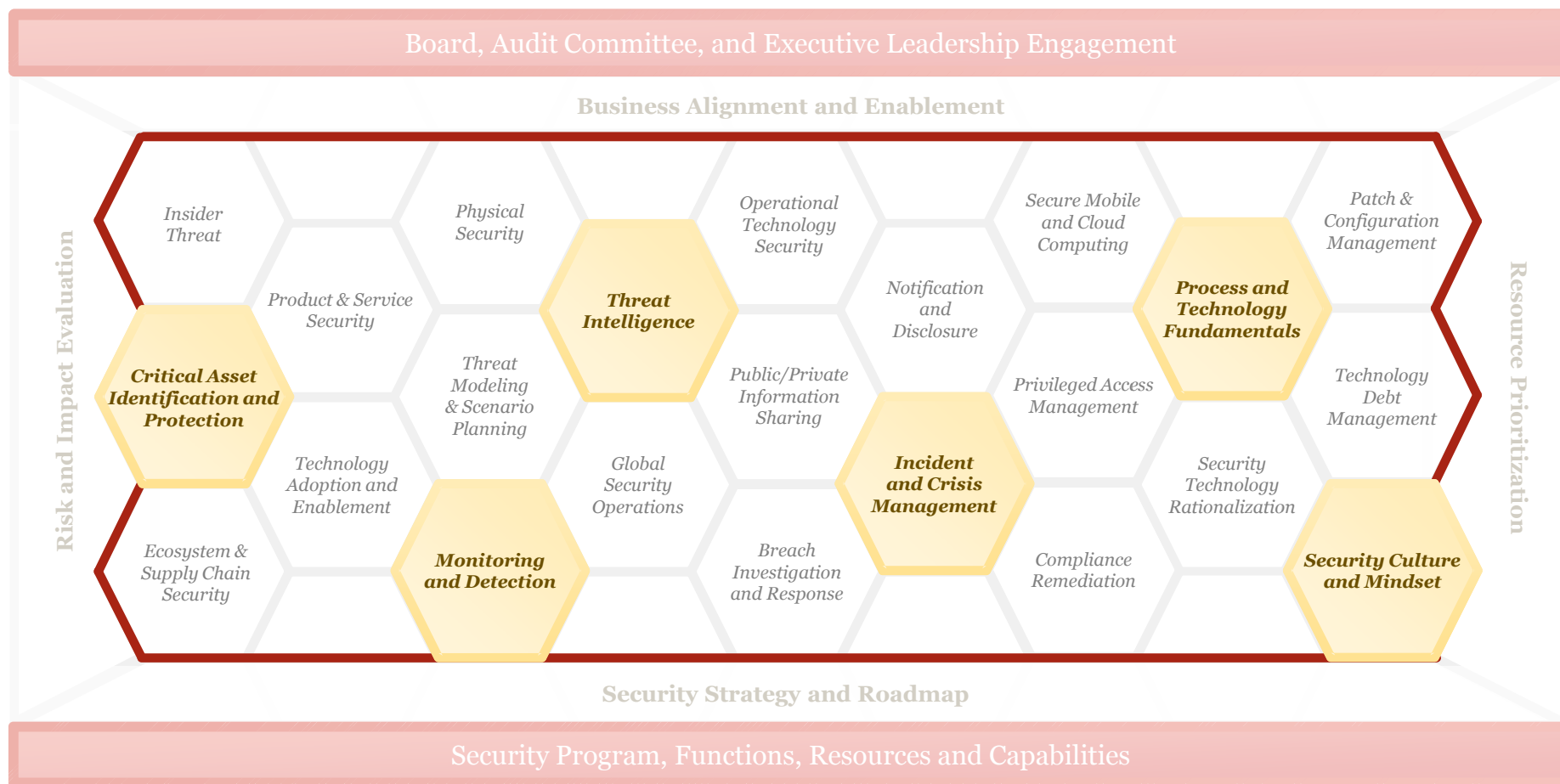
Current snapshot of cyber threats

Some topical issues of concern

- Leakage of customer records at scale (eg JP Morgan)
- State-related targeting and penetration
 - Destructive attacks (eg data deletion)
 - Industrial control systems of increasing interest
- Increasing engagement of organised criminal groups
 - New criminal enterprises (eg extortion)
 - Greatly-increased complexity of attack tools (eg ransomware)
 - Cyber as enabler of physical crime (eg ports)
- Denial of service against banking and exchanges (goal: destabilise)
- Insider threat: scale and impact
- Continued growth of mobile attack techniques
- Focus on supply chains and professional service providers

Organizations have not kept pace

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



-
- **Where are We?**

(Based on PwC Global Information Security Survey 2015)

High growth in high-profile crimes

Incidents attributed to **nation-states**, **organised crime**, and **competitors** increased sharply in 2014.

86% jump in incidents by nation-states (with China, HK and India with the highest values)

64% rise in compromises by competitors

26% increase in incidents by organised crime.

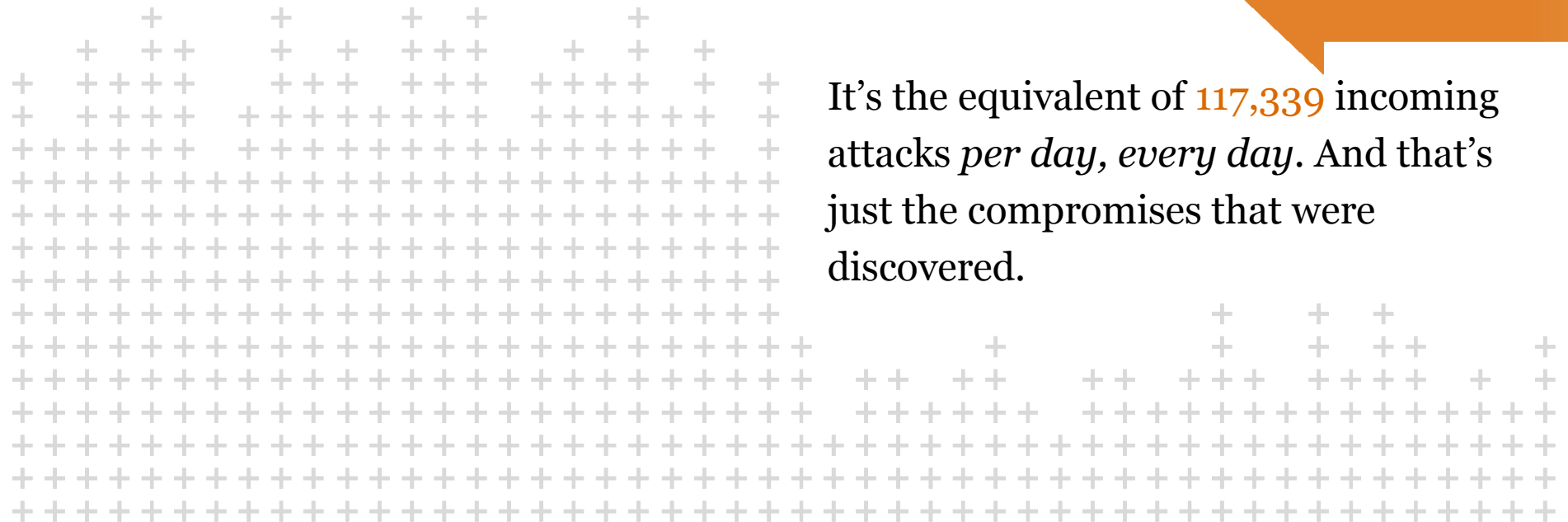


The number of security incidents continues to soar

The total number of security incidents detected globally by survey respondents climbed to **42.8 million** this year, an increase of 48% over 2013.



It's the equivalent of **117,339** incoming attacks *per day, every day*. And that's just the compromises that were discovered.



The financial cost of security incidents is high and rising

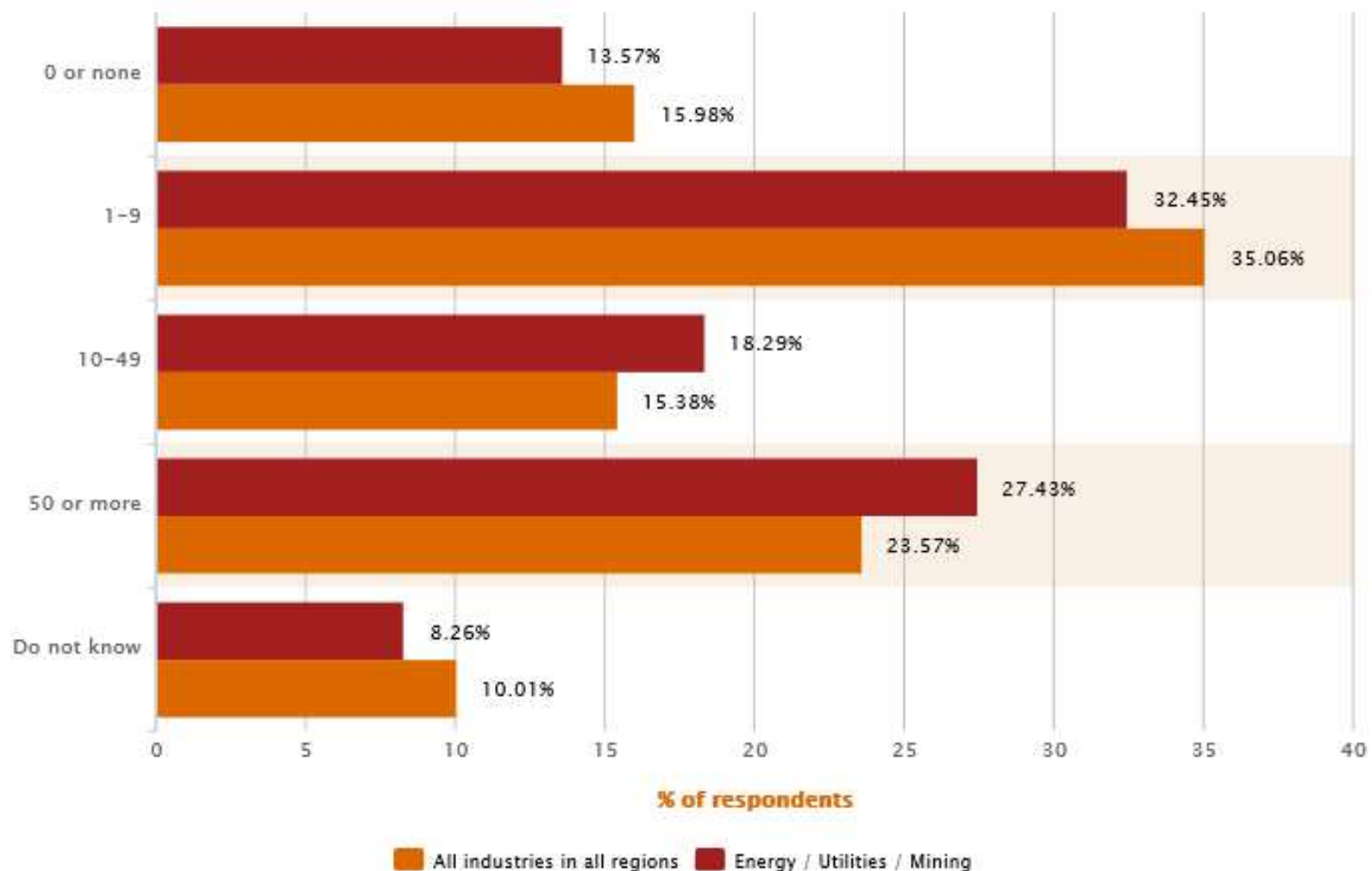
As security incidents grow in frequency, the costs of managing and mitigating breaches also are rising.

Globally, the annual estimated reported average financial loss attributed to cybersecurity incidents was **US\$2.7 million**, a jump of 34% over 2013.

Not surprising, but certainly attention grabbing, is the finding that big losses are more common: Organisations reporting financial hits of US\$20 million or more **increased 92%** over 2013.

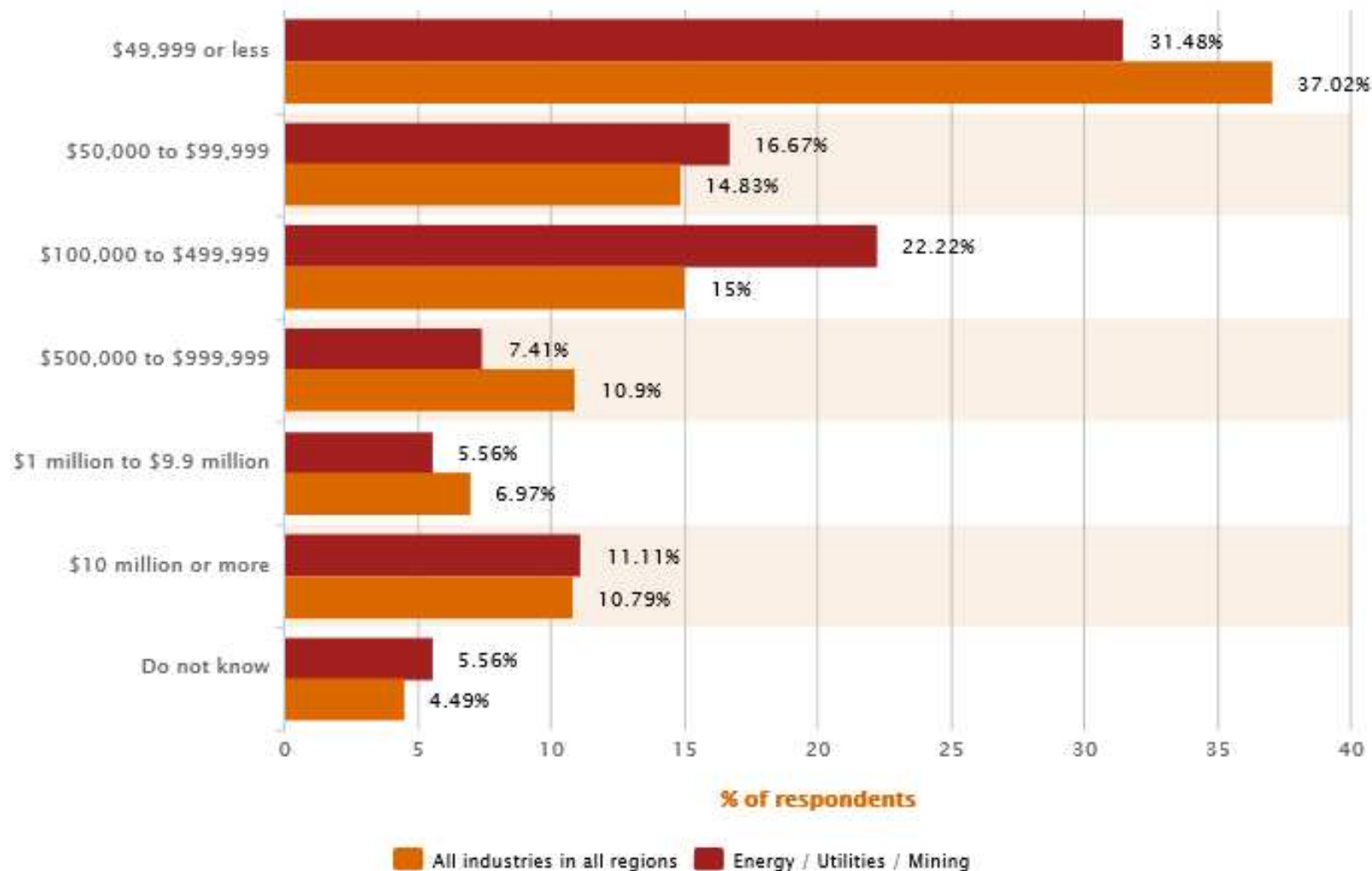


Number of Security incidents detected in the past 12 months



Source: The Global State of Information Security® Survey 2015. Not all factors may be shown. Totals may not add up to 100%.

Estimated total financial losses as a result of all security incidents (USD)



Source: The Global State of Information Security® Survey 2015. Not all factors may be shown. Totals may not add up to 100%.

Monetary losses stretch into the billions of dollars...

The estimated global cost of cybercrime detected by respondents this year is more than **US\$23 billion**.

Again, it's important to note this figure represents only *detected* compromises.

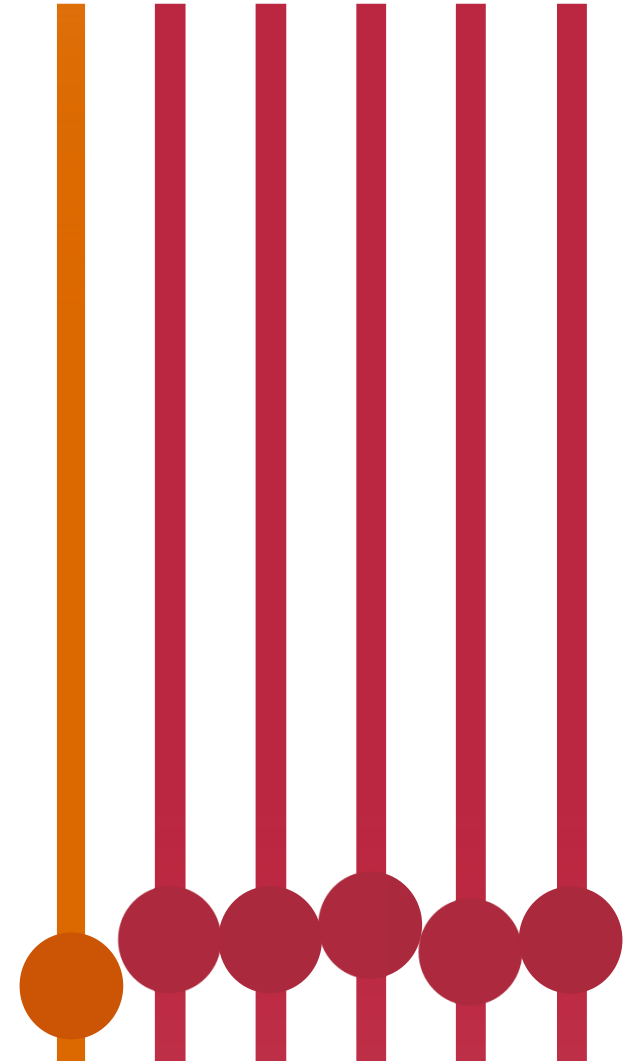
It is almost important to note that the value of certain kinds of information – intellectual property and trade secrets, in particular – is very difficult to ascertain.



Despite elevated risks, security budgets decline in 2014

Many organisations are undoubtedly worried about the rising tide of cybercrime, yet most have not increased their investment security initiatives.

In fact, global IS budgets actually **decreased 4%** compared with 2013. And security spending as a percentage of the total IT budget has remained stalled at **4% or less** for the past five years.



Employees are the most cited culprits of incidents

Incidents attributed to insiders rises while security preparedness falls

Current and **former employees** are the most-cited culprits of security incidents, but implementation of key insider-threat safeguards is declining.

- 56% **have privileged user-access** tools (65% in 2013) as compared to 61% of respondents in APAC.

- 51% have an **employee security training and awareness program** (60% in 2013) as compared to 55.6% in APAC.

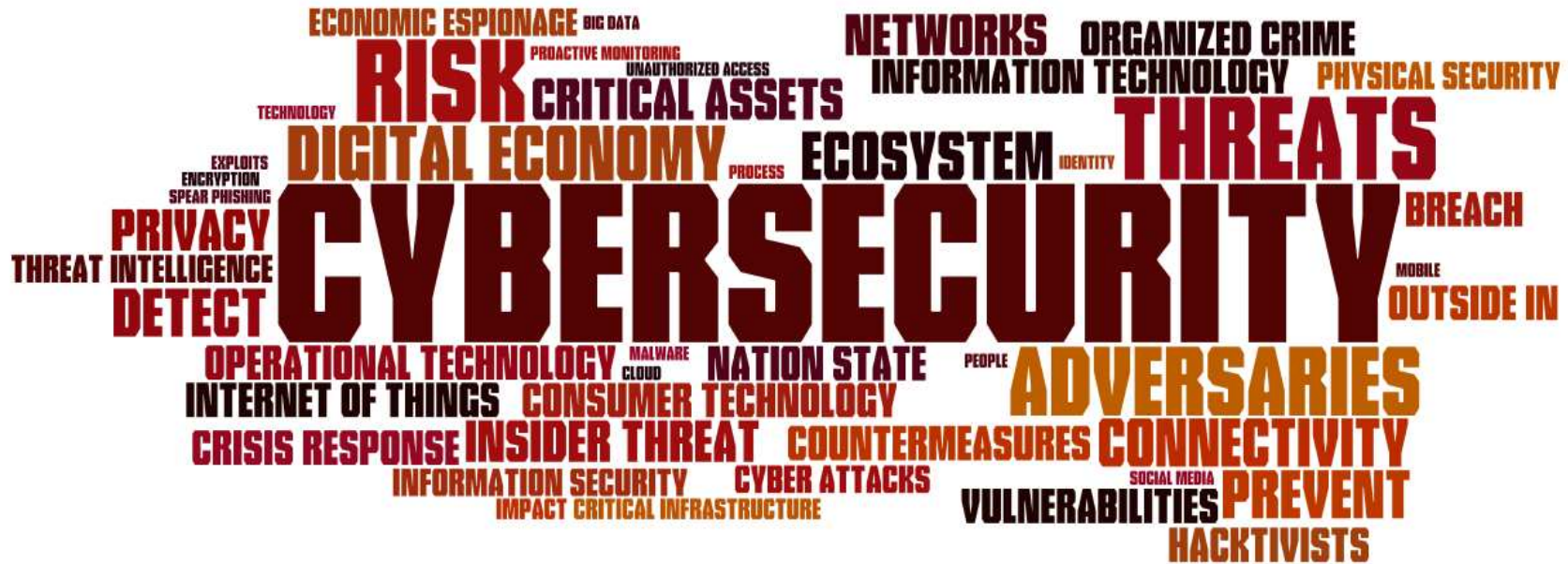


Compromises attributed to **third parties with trusted access** increases while due diligence weakens.

- In Asia Pacific, 55% of respondents **require third parties to comply with their privacy policies** (vs. 53.55% of the global average).

-
- **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, defend 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

Managing the risk requires an enterprise approach

You can't secure everything

Set the right priorities.

- Protect what matters
- Strategy, organisation, governance and enterprise security architecture
- Threat intelligence

Seize the advantage

Exploit the next digital opportunity with confidence.

- Compliance with privacy and regulation
- Digital trust is embedded in the strategy
- Risk management and risk appetite

It's not if but when

Build an intelligence-led defence, enabling rapid cyber response.

- Continuity and resilience
- Crisis management
- Incident response
- Monitoring and detection

Fix the basics

Use technology to your advantage, maximising return from technology investments.

- Identity and access management
- Information technology hygiene
- Information technology, operations technology and consumer technology
- Security intelligence and analytics



Their risk is your risk

Understand and manage risk in your interconnected business ecosystem.

- Digital channels
- Partner and supplier management
- Robust contracts

People Matter

Build and maintain a secure culture, where people are aware of their critical security decisions.

- Insider threat management
- People and 'Moments that Matter'
- Security culture and awareness

Have you kept pace?

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

Identify, prioritize, and protect the assets most essential to the business

- Have you identified your most critical assets and know where they are stored and transmitted?
- How do you evaluate their value and impact to the business if compromised?
- Do you prioritize the protection of your crown jewels differently than other information assets?

Understand the threats to your industry and your business

- Who are your adversaries and what are their motivations?
- What information are they targeting and what tactics are they using?
- How are you anticipating and adapting your strategy and controls?

Evaluate and improve effectiveness of existing processes and technologies

- Have you patched and upgraded your core platforms and technology?
- How are you securing new technology adoption and managing vulnerability with your legacy technology?
- Have you evolved your security architecture and associated processes?

Enhance situational awareness to detect and respond to security events

- How are you gaining visibility into internal and external security events and activities?
- Are you applying correlation and analytics to identify patterns or exceptions?
- How do you timely and efficiently determine when to take action?

Develop a cross-functional incident response plan for effective crisis management

- Have your business leaders undertaken cyberattack scenario planning?
- Do you have a defined cross functional structure, process and capability to respond?
- Are you enhancing and aligning your plan to ongoing business changes?

Establish values and behaviors to create and promote security effectiveness

- How is leadership engaged and committed to addressing cyber risks facing the business?
- What sustained activities are in place to improve awareness and sensitivity to cyber risks?
- How have your business practices evolved to address the threats to your business?

Recap of Key points to takeaway

Know your ecosystem and the risk landscape

New Ecosystem - Business models have evolved into a more interconnected, integrated, and interdependent environment.

Q: What is the cyber risk strategy of your service provider?

Know your adversary – motives, means, and methods

OSHI - Sophisticated groups are actively exploiting cyber weaknesses; organized crime , State Sponsored, Hacktivists and Internal.

Q: Who are your enemies and what is being said about your company in social media?

Know your Crown Jewels

Crown Jewels - identify and enhance the protection of “crown jewels”.

Q: What information assets can impact your market value?

Know your culture

Tone at the top - awareness and commitment from the highest executive levels.

Q: What is your role in cybersecurity?

Know your business risks

Embed cyber risk into board oversight and executive-level decision making

Q: How has cyber risk been considered as a business issue?

For more information on Cyber Risks...



United States:

www.pwc.com/cybersecurity

- [Results of 2014 Global State of Information Security](#)
- [10Minutes on the stark realities of cybersecurity](#) (available in several languages)
- [Cybersecurity risk on the board's agenda](#)
- [Cyber Video Series](#)
- [A response to the President's Cybersecurity Executive Order](#)

United Kingdom:

<http://www.pwc.co.uk/cyber-security/cyber-security>

- [Insights](#)
- [Cyber Video Series](#)

Australia:

<http://www.pwc.com.au/consulting/cyber/>

Others:

[Belgium](#)

[Germany](#)

[Switzerland](#)

[Scandinavia](#)

Our global team and credentials

Our team helps organizations understand dynamic cyber challenges, adapt and respond to risks inherent to their business ecosystem, and prioritize and protect the most valuable assets fundamental to their business strategy.

1,600+ professionals

- Focused on consulting, solution implementation, incident response, and forensic investigation
- Knowledge and experience across key industries and sectors
- Largest professional security consulting provider as ranked by Gartner¹

‘Leader’ ranking by Forrester Research

"PwC has very strong global delivery capabilities, and the firm offers solid, comprehensive services with the ability to address almost all of the security and risk challenges that clients will face"²

Knowledge & Experience

- Advanced degrees and certifications including
 - Certified Information System Security Professional (CISSP)
 - Encase Certified Examiner (EnCE)
 - Certified Information Security Manager (CISM)
 - Certified Ethical Hacker (CEH)
 - Oracle Diamond Partner – Identity Management Specialization
- Former federal and international law enforcement and intelligence officers
- Security clearances that allow for classified discussions that often stem from cyber related incidents

We provide pragmatic insight and a balanced view of how to prioritize investments in people, processes and technology solutions needed to address the cybersecurity challenge

60+ labs

- Technical security and forensics labs located in forty countries
- Designed to conduct assessments, design and test security solutions, and conduct cyber forensic analysis and investigations

Proprietary tools and methods

- Extensive library of templates, tools, and accelerators
- Cyber threat intelligence fusion and big data analysis platforms to process data related to cyber threats and incidents

¹Gartner: Competitive Landscape: Professional Security Consulting Services, Worldwide, 2013

²The Forrester Wave: Information Security and Risk Consulting Services, Q1 2013, Forrester Research, Ed Ferrara and Andrew Rose, February 1, 2013

Questions

Thank you.

© 2014 PricewaterhouseCoopers Consulting Hong Kong Limited. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers Consulting Hong Kong Limited, which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.

This proposal is provided solely in connection with your Request for Proposal received 24th October 2013 - MetLife Asia Digital Direct 2.0 Project. This is a proposal and does not constitute a contract of engagement with PwC. In the event that our proposal to you is successful, we will agree formal contractual terms with you before we begin any substantive work. In the meantime, this document is provided on the basis that PwC accepts no liability—whether in contract, tort (including negligence), or otherwise—to MetLife, Inc ("MetLife") or to any other person in respect of MetLife Asia Digital Direct 2.0 Project. In addition, our acceptance of the engagement will be contingent upon the completion of all our internal engagement acceptance procedures.

This proposal must not be made available or copied in whole or in part to any other person without our express written permission.