www.pwc.com

RIMS Perk Session 2015 - Protecting the Crown Jewels

A Risk Manager's guide to cybersecurity
February 9, 2016

Washington RIMS

pwc

Agenda

Introductions

What is Cybersecurity?

Crown jewels

The bad actors

Securing Informational Assets (IAs)

Computer Emergency Response Team (CERT)

Incident Response (IR) plan

Introductions

PwC

Aaron Weller, Senior Managing Director

PNW Practice Leader – Cybersecurity & Privacy Risk

Aaron.weller@pwc.com

Highlights from PwC Survey's

61%

CEOs' fastest-growing concern

61% of CEO's around the globe are concerned about cyberthreats.

70%

Protecting Intellectual Property

70% of organizations expressed concern about their inability to protect intellectual property or confidential customer data

53%

Cybersecurity tools of utmost strategic importance

53% of CEOs consider cybersecurity 'very important' to their organization

4%

Investing in cybersecurity

The average 2014 information security budget dipped to $4.1 million, down 4% compared to 2013.

Sources:
1 - PwC 18th Annual Global CEO Survey
2 - 2015 Global State of Information Security
3 - PwC 6th Annual Digital IQ Survey

What is cybersecurity?

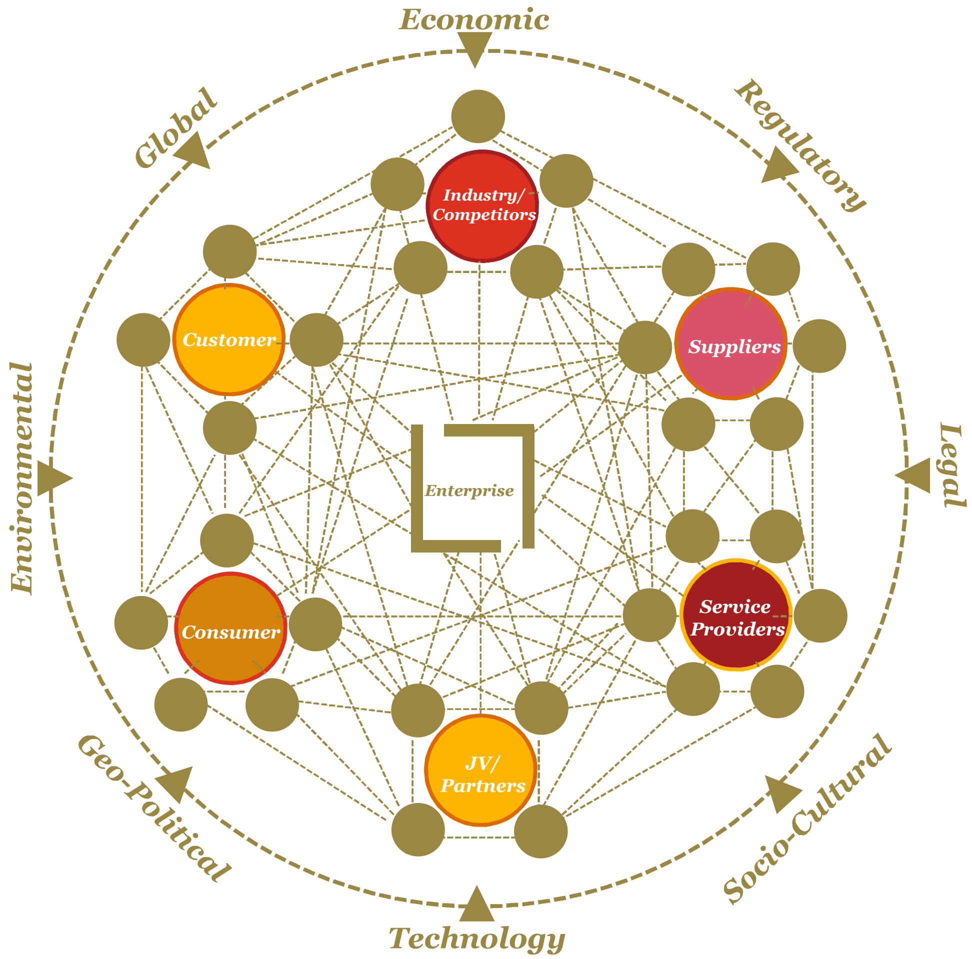
ECONOMIC ESPIONAGE
BIG DATA
NETWORKS
ORGANIZED CRIME
RISK
PROACTIVE MONITORING
UNAUTHORIZED ACCESS
CRITICAL ASSETS
INFORMATION TECHNOLOGY
PHYSICAL SECURITY
TECHNOLOGY
DIGITAL ECONOMY
PROCESS
ECOSYSTEM
IDENTITY
THREATS
EXPLOITS
ENCRYPTION
SPEAR PHISHING
PRIVACY
THREAT INTELLIGENCE
DETECT
CYBERSECURITY
BREACH
MOBILE
OUTSIDE IN
OPERATIONAL TECHNOLOGY
MALWARE
CLOUD
NATION STATE
PEOPLE
ADVERSARIES
INTERNET OF THINGS
CONSUMER TECHNOLOGY
CRISIS RESPONSE
INSIDER THREAT
COUNTERMEASURES
CONNECTIVITY
INFORMATION SECURITY
CYBER ATTACKS
SOCIAL MEDIA
VULNERABILITIES
PREVENT
IMPACT CRITICAL INFRASTRUCTURE
HACKTIVISTS

- Cybersecurity represents many things to many different people
- Key characteristics and attributes of cybersecurity:
  - ***Broader*** than just information technology and ***extends*** beyond the enterprise
  - ***Increasingly vulnerable*** due to technology connectivity and dependency
  - An 'outside-in view' of ***the threats*** *and* ***business impact*** facing an organization
  - Shared responsibility that requires ***cross functional disciplines*** in order to plan, protect, defend, react and respond

It is no longer just an IT challenge – it is a business imperative!

The cyber challenge now extends beyond the enterprise

Global Business Ecosystem



▲ *Pressures and changes which create opportunity and risk*

The Evolution:

- Technology-led innovation has enabled business models to evolve
- The extended enterprise has moved beyond supply chain and consumer integration
- Connectivity and collaboration now extends to all facets of business

Leading to:

- A dynamic environment that is increasingly interconnected, integrated, and interdependent
- Where changing business drivers create opportunity and risk

Scope of cybersecurity – Technology domain convergence

Information Technology	Computing resources and connectivity for processing and managing data to support organizational functions and transactions
Operational Technology	Systems and related automation assets for the purpose of monitoring and controlling physical processes and events or supporting the creation and delivery of products and services
Consumer *(Products and Services)* ***Technology***	Computing resources and connectivity integrated with or supporting external end-user focused products and services

Cybersecurity encompasses all three **technology types**

Evolving business risks…
…impacting brand, competitive advantage, and shareholder value

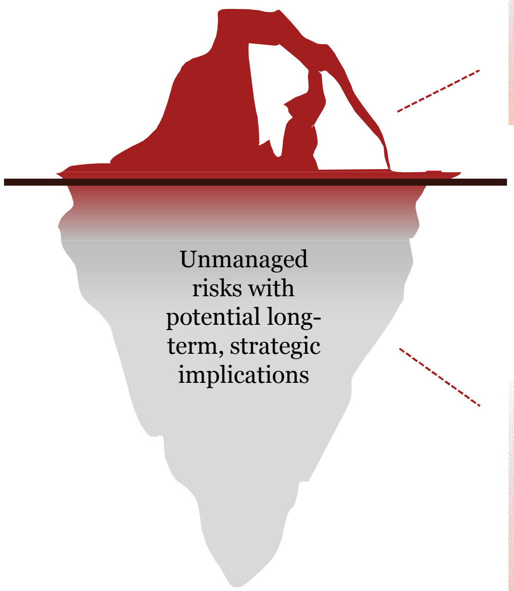
Highlights of activities impacting risk:

Advancements in and evolving use of technology – *adoption of cloud-enabled services; Internet of Things (“IoT”) security implications; BYOD usage*

Value chain collaboration and information sharing – *persistent ‘third party’ integration; tiered partner access requirements; usage and storage of critical assets throughout ecosystem*

Operational fragility – *Real-time operations; product manufacturing; service delivery; customer experience*

Business objectives and initiatives – *M&A transactions; emerging market expansion; sensitive activities of interest to adversaries*



Unmanaged risks with potential long-term, strategic implications

Historical headlines have primarily been driven by compliance and disclosure requirements

However, the real impact is often not recognized, appreciated, or reported

Cybersecurity must be viewed as a strategic business imperative in order to protect brand, competitive advantage, and shareholder value

Crown jewels

What do you notice about these jewels?

Crown jewels - definition

What is a “crown jewel”?

Definition - the most valuable or attractive thing in a collection or group (Merriam – Webster dictionary)

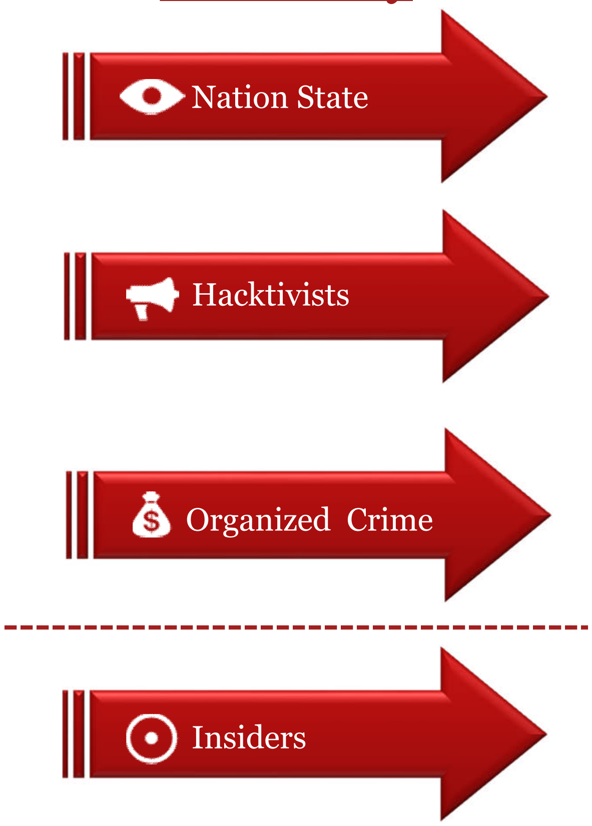
An Informational Asset (IA)

The asset, that if you lost it, you lose your:

- Competitive advantage
- Intellectual property rights
- Brand reputation
- Ability to conduct business

The actors and the information they target

Adversary



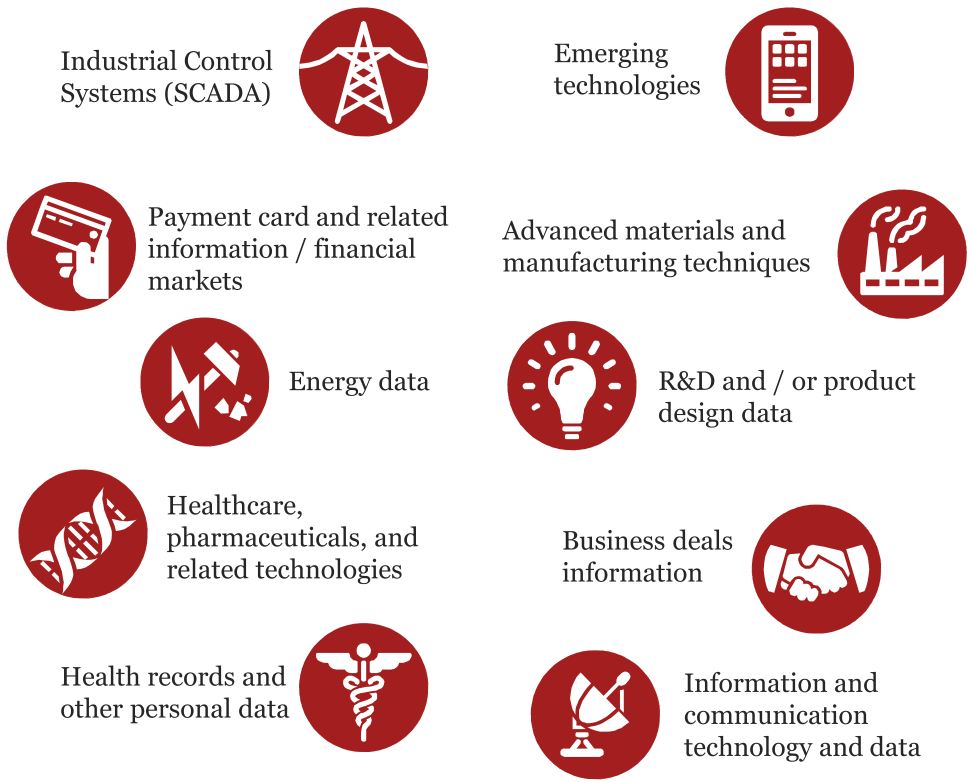
Nation State

Hacktivists

Organized Crime

Insiders

What's most at risk?



Industrial Control Systems (SCADA)

Emerging technologies

Payment card and related information / financial markets

Advanced materials and manufacturing techniques

Energy data

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.*

Motives and ***tactics*** evolve and what adversaries target vary depending on the organization and the products and services they provide.

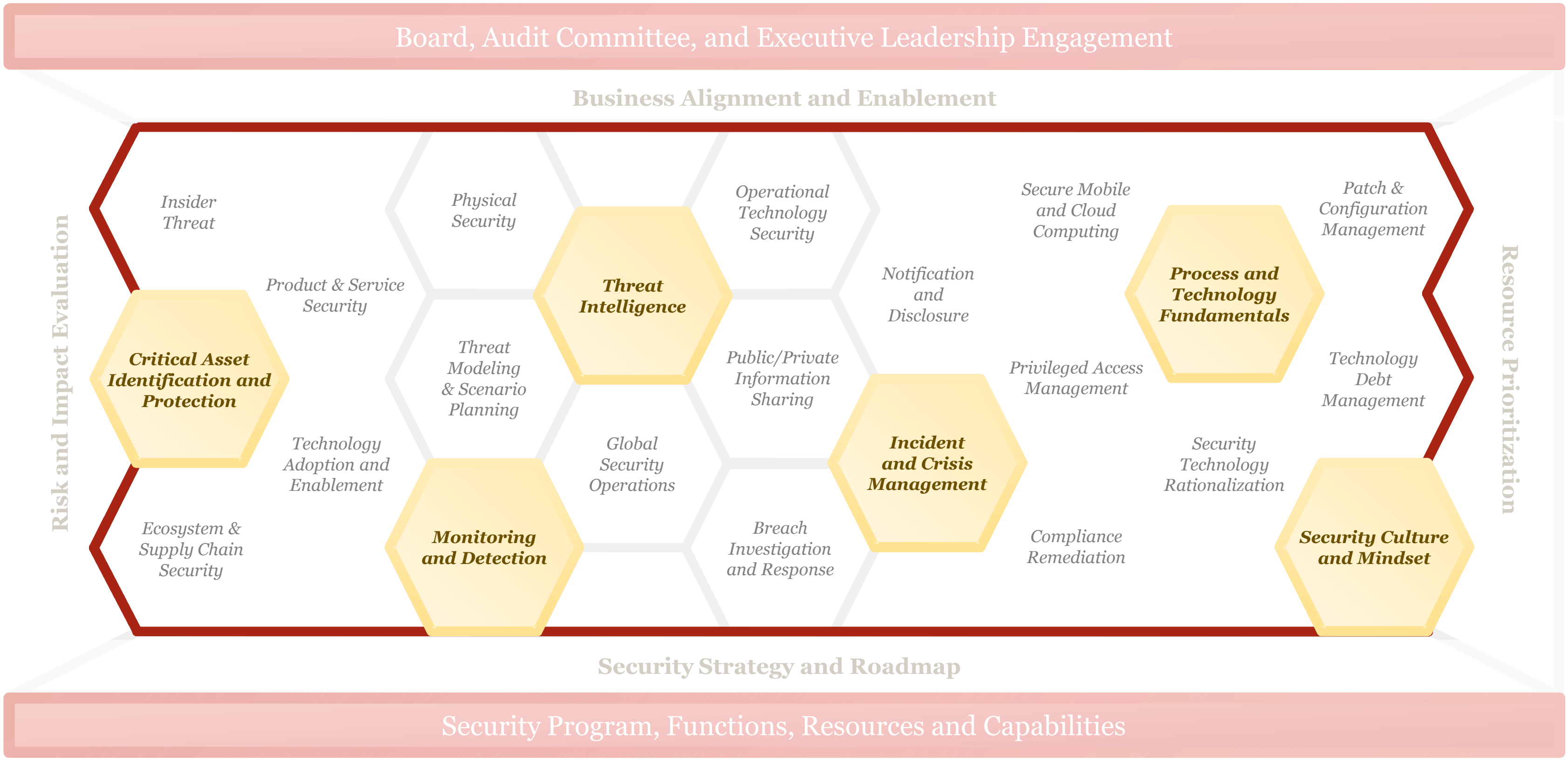
Evolving perspectives

Considerations for businesses adapting to the new reality

	Historical IT Security Perspectives	Today's Leading Cybersecurity Insights
Scope of the challenge	• Limited to your "four walls" and the extended enterprise	• Spans your interconnected global business ecosystem
Ownership and accountability	• IT led and operated	• Business-aligned and owned; CEO and board accountable
Adversaries' characteristics	• One-off and opportunistic; motivated by notoriety, technical challenge, and individual gain	• Organized, funded and targeted; motivated by economic, monetary and political gain
Information asset protection	• One-size-fits-all approach	• Prioritize and protect your "crown jewels"
Defense posture	• Protect the perimeter; respond *if* attacked	• Plan, monitor, and rapidly respond *when* attacked
Security intelligence and information sharing	• Keep to yourself	• Public/private partnerships; collaboration with industry working groups

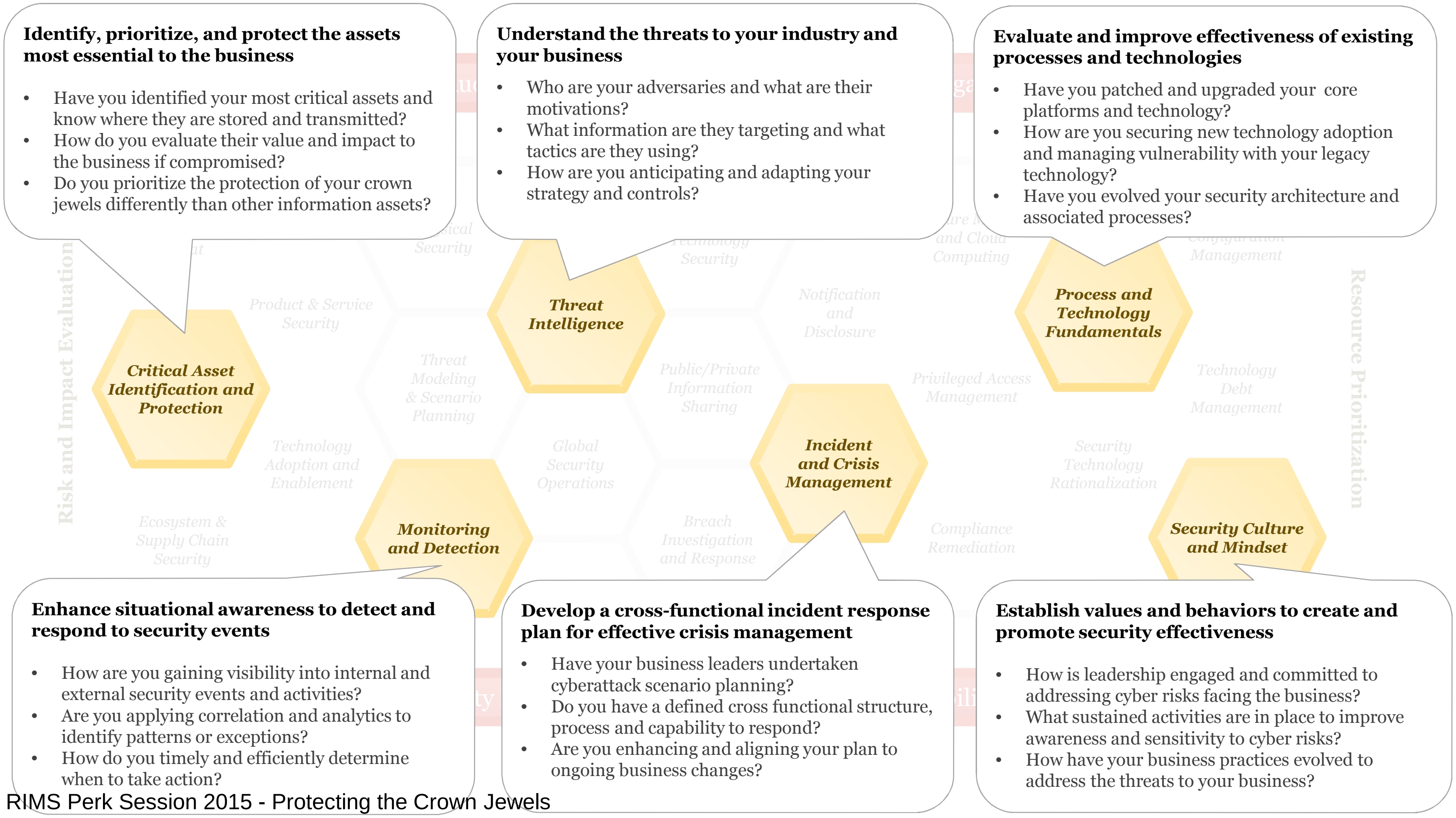
Why organizations have not kept pace

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


Board, Audit Committee, and Executive Leadership Engagement
Business Alignment and Enablement
Risk and Impact Evaluation
Resource Prioritization
Insider Threat
Physical Security
Operational Technology Security
Secure Mobile and Cloud Computing
Patch & Configuration Management
Product & Service Security
Threat Intelligence
Notification and Disclosure
Process and Technology Fundamentals
Critical Asset Identification and Protection
Threat Modeling & Scenario Planning
Public/Private Information Sharing
Privileged Access Management
Technology Debt Management
Technology Adoption and Enablement
Global Security Operations
Incident and Crisis Management
Security Technology Rationalization
Ecosystem & Supply Chain Security
Monitoring and Detection
Breach Investigation and Response
Compliance Remediation
Security Culture and Mindset
Security Strategy and Roadmap
Security Program, Functions, Resources and Capabilities

Have you kept pace?

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


Critical Asset Identification and Protection
Threat Intelligence
Process and Technology Fundamentals
Incident and Crisis Management
Monitoring and Detection
Security Culture and Mindset
Risk and Impact Evaluation
Resource Prioritization
Product & Service Security
Threat Modeling & Scenario Planning
Notification and Disclosure
Public/Private Information Sharing
Privileged Access Management
Technology Debt Management
Technology Adoption and Enablement
Global Security Operations
Security Technology Rationalization
Ecosystem & Supply Chain Security
Breach Investigation and Response
Compliance Remediation

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?

Computer Emergency Response Team (CERT)

Ensure you have formed a CERT, and the team consists of:

- Legal – (GC) General Counsel, Outside Counsel
- Risk – (CRO) Chief Risk Officer, Risk Manager, Internal audit, board representative
- Technology officer – (CIO) Chief Information Officer
- Security officer – (CISO) Chief Information Security Officer
- HR
- Accounting / finance
- Sales and Marketing
- Public relations
- Physical security
- Computer / network security
- Server manager
- Ecommerce manager
- Database manager
- Network manager
- PC / helpdesk manager
- Supply chain manager

Incident response (IR) plan

Have a clear plan of action, in the event of an incident

Documented

CERT should be familiar with the IR plan

Update regularly

Recap of key points to consider

1 ***The global business ecosystem has changed the risk landscape***

Business models have evolved, creating a dynamic environment that is increasingly interconnected, integrated, and interdependent - necessitating the transformation of your security practices to keep pace.

2 ***Focus on securing high value information and protecting what matters most***

Rather than treating everything equally, you should identify and enhance the protection of your "crown jewels" while maintaining a consistent security baseline within their environment.

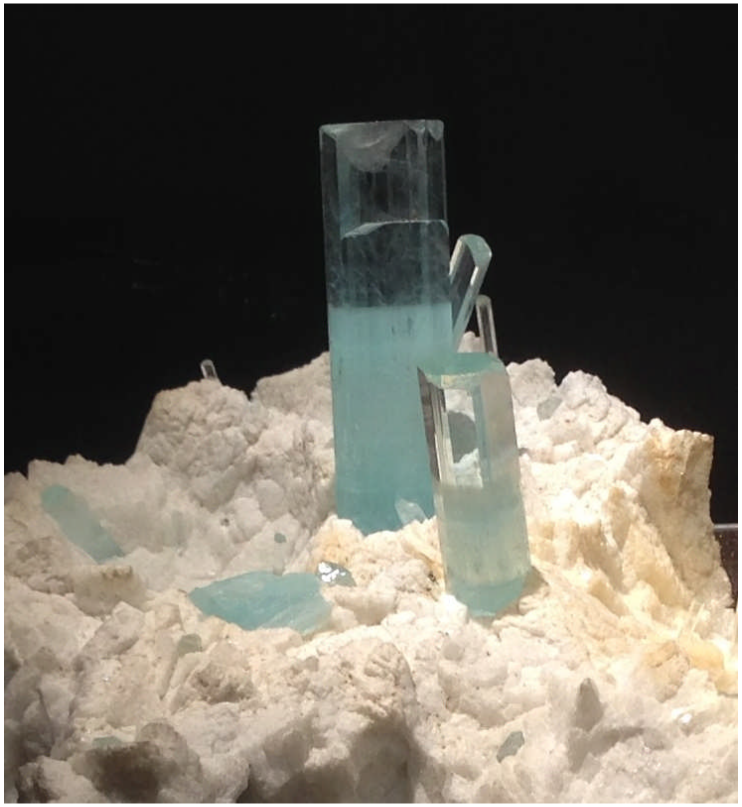
3 ***Know your adversary – motives, means, and methods***

Sophisticated adversaries are actively exploiting cyber weaknesses in the business ecosystem for economic, monetary or political gain – requiring threat intelligence, proactive monitoring and deep response capabilities.

4 ***Embed cybersecurity into board oversight and executive-level decision making***

Creating an integrated, business aligned security strategy and program requires awareness and commitment from the highest executive levels of the organization – in order to apply the appropriate resources and investments.

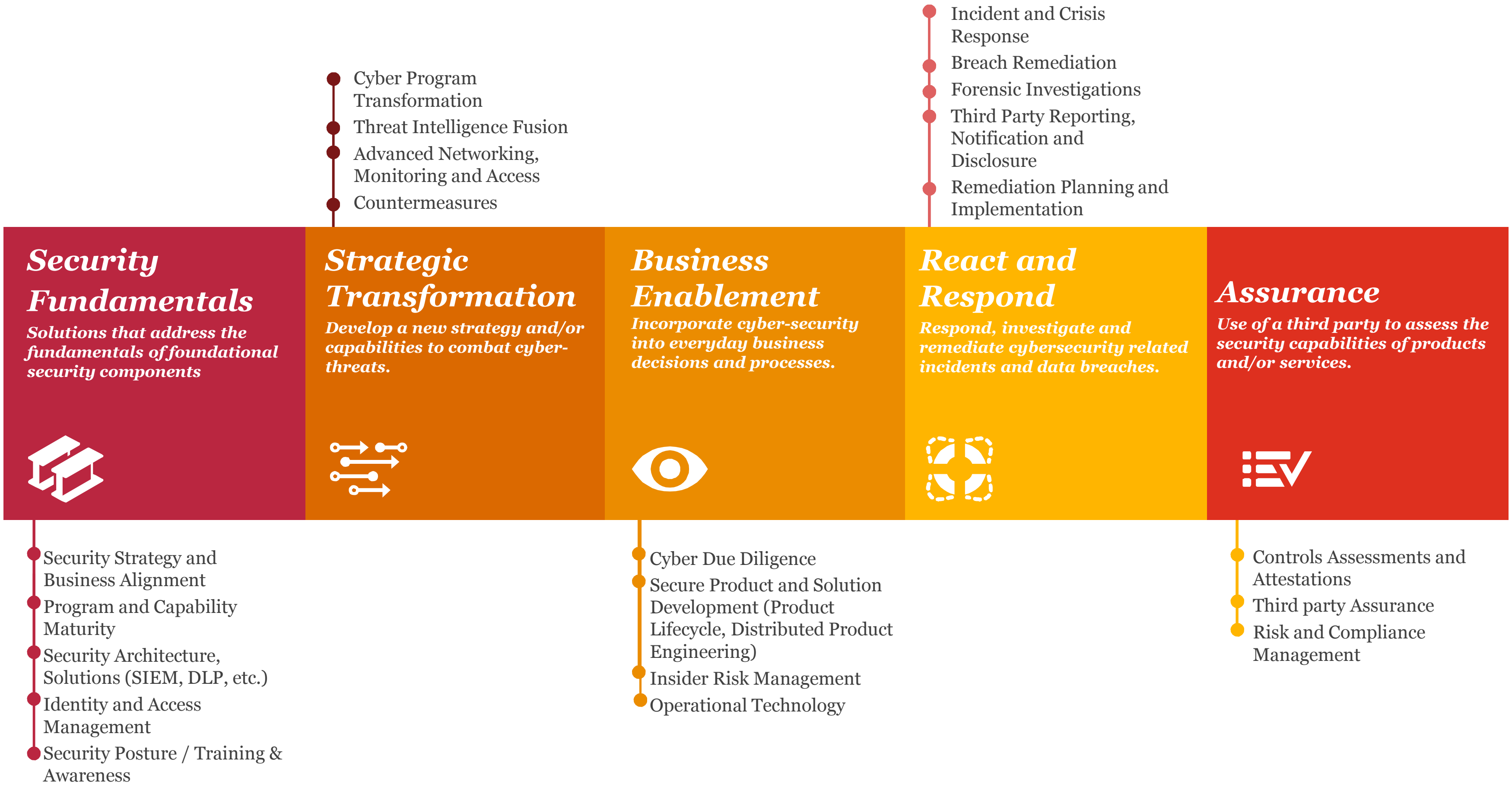
Remember, all jewels are different, but no less valuable…



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, PricewaterhouseCoopers LLP, 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.

A sampling of our solutions

We offer numerous solutions that help organizations understand their dynamic cyber challenges, adapt and respond to the risks inherent in their business ecosystem, and protect the assets most critical to their brand, competitive advantage and shareholder value.



Security Fundamentals

Solutions that address the fundamentals of foundational security components

- Security Strategy and Business Alignment
- Program and Capability Maturity
- Security Architecture, Solutions (SIEM, DLP, etc.)
- Identity and Access Management
- Security Posture / Training & Awareness

Strategic Transformation

Develop a new strategy and/or capabilities to combat cyber-threats.

- Cyber Program Transformation
- Threat Intelligence Fusion
- Advanced Networking, Monitoring and Access
- Countermeasures

Business Enablement

Incorporate cyber-security into everyday business decisions and processes.

- Cyber Due Diligence
- Secure Product and Solution Development (Product Lifecycle, Distributed Product Engineering)
- Insider Risk Management
- Operational Technology

React and Respond

Respond, investigate and remediate cybersecurity related incidents and data breaches.

- Incident and Crisis Response
- Breach Remediation
- Forensic Investigations
- Third Party Reporting, Notification and Disclosure
- Remediation Planning and Implementation

Assurance

Use of a third party to assess the security capabilities of products and/or services.

- Controls Assessments and Attestations
- Third party Assurance
- Risk and Compliance Management

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

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

Knowledge & Experience

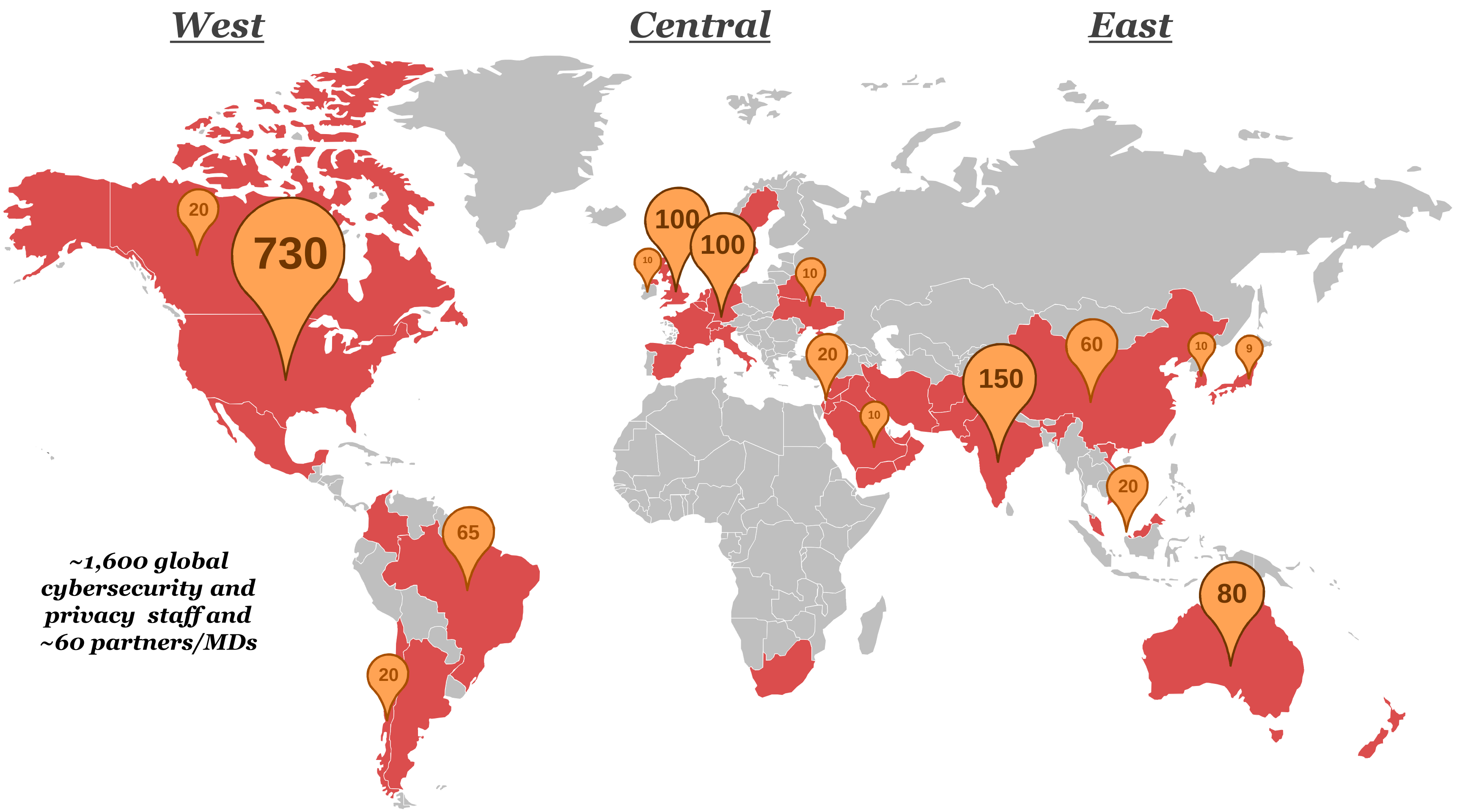
- Advanced degrees and certifications including
  - Certified Information System Security Professional (CISSP)
  - Encase Certified Examiner (EnCE)
  - Certified Information Security Manager (CISM)
  - Certified Ethical Hacker (CEH)
  - Oracle Diamond Partner – Identity Management Specialization
- Former 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

Map of practitioners



~1,600 global cybersecurity and privacy staff and ~60 partners/MDs