

RIMS Perk Session 2015 - Protecting the Crown Jewels

A Risk Manager's guide to
cyber security
March 18, 2015

Los Angeles RIMS

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

Jeff Phillips, Managing Director, PwC

Charles White, Director, PwC

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 organisations 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%

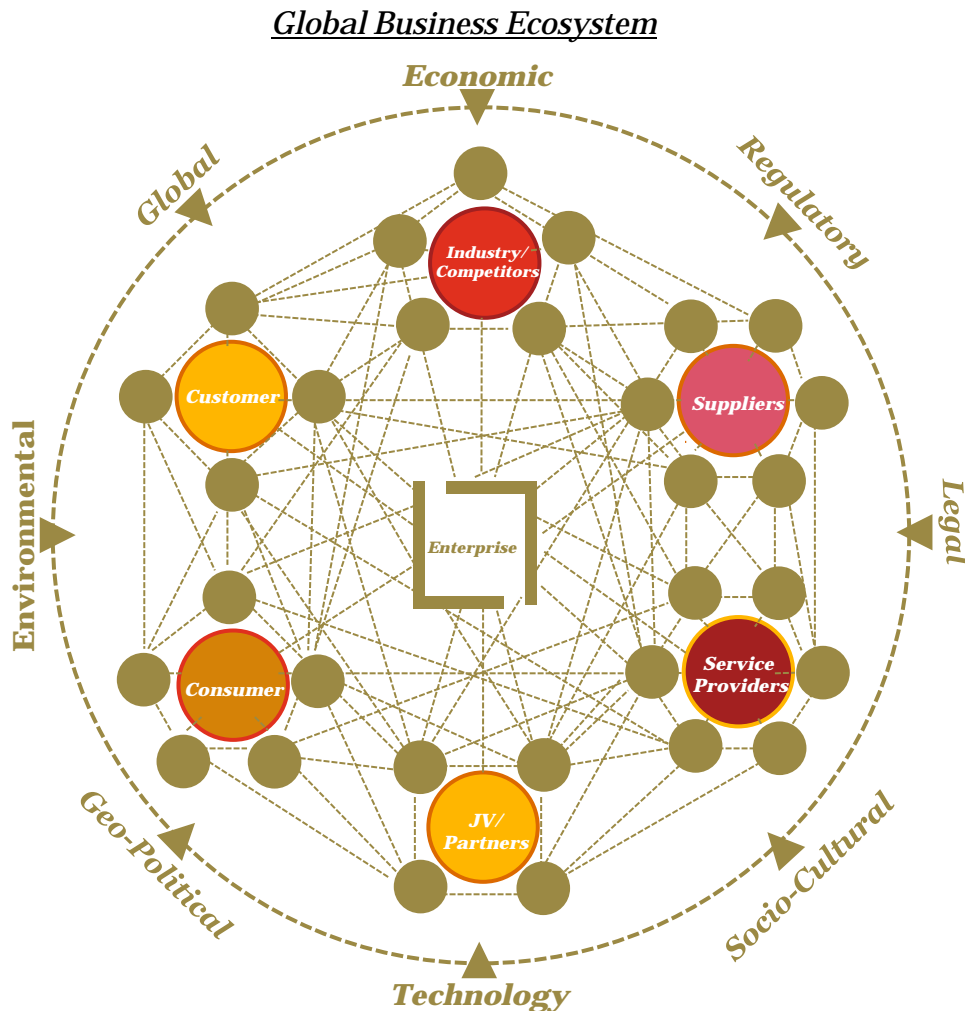
Investing in cybersecurity

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

The cyber challenge now extends beyond the enterprise



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**

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

Crown jewels - Examples

<u>Industry</u>	<u>Crown jewel</u>
Hospital / Healthcare	Patient records / PCI data
Retailer	Client PCI / email / personal data
Trading firm	Trading servers
Insurance firm	Insurance claim data / investment servers
Technology firm	Intellectual property
Law firm	Client data / Intellectual property
Military / defense	Intellectual property / intelligence
Telecom provider	Call processing and billing servers

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



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.

Securing Informational Assets (IAs)

Risk process:

- Identify assets
- Threats
- Vulnerabilities
- Likelihood
- Productivity impact
- Cost
- Compensating controls
- Risk migrating controls (Cyber insurance, 3rd party contracts, indemnifications, etc.)

Securing IAs - considerations

- Today, data breaches and data losses are unavoidable.
- In today's world, you continue with defenses, however...
- Prioritize security, assets, and users – what/who's most important?
- How fast can you respond?
- How can you expand and grow, and still respond to cyber risks?

Securing IAs - considerations

Do you completely understand all your assets, and where they are?

Does every employee need access to everything?

Does every department need access to everyone else's assets?


How do you protect?

How do you monitor?

Don't assume the "regular" entries are the only entry points

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

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

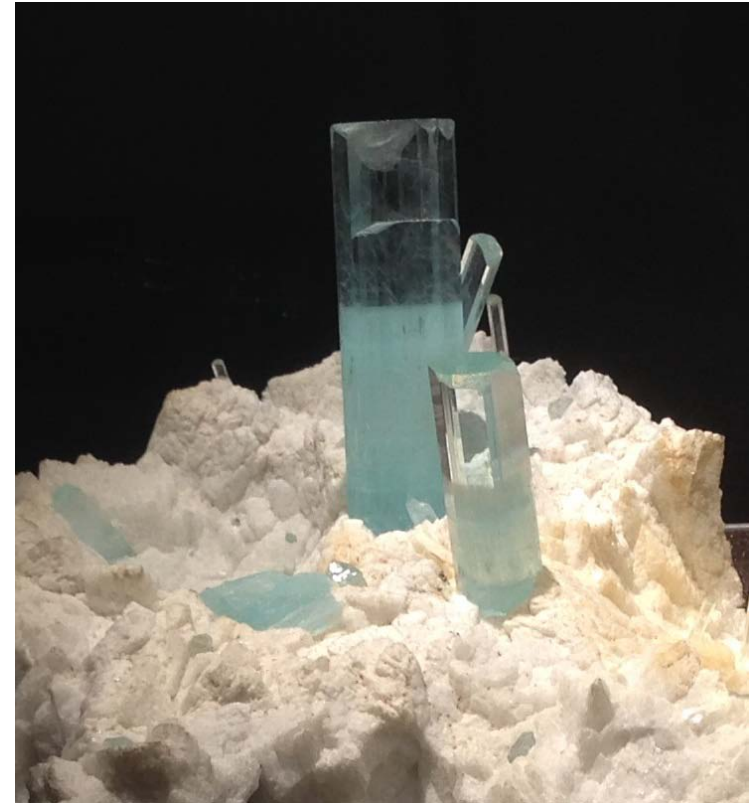
Sophisticated adversaries are actively exploiting cyber weaknesses in the business ecosystem for economic, monetary or political gain – requiring threat intelligence, proactive monitoring and deep response capabilities.

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.

© 2014 PricewaterhouseCoopers LLP. 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.