

Cybersecurity – Threats in the Digital Era

Tassos Procopiou

February 2017

What is cybersecurity?

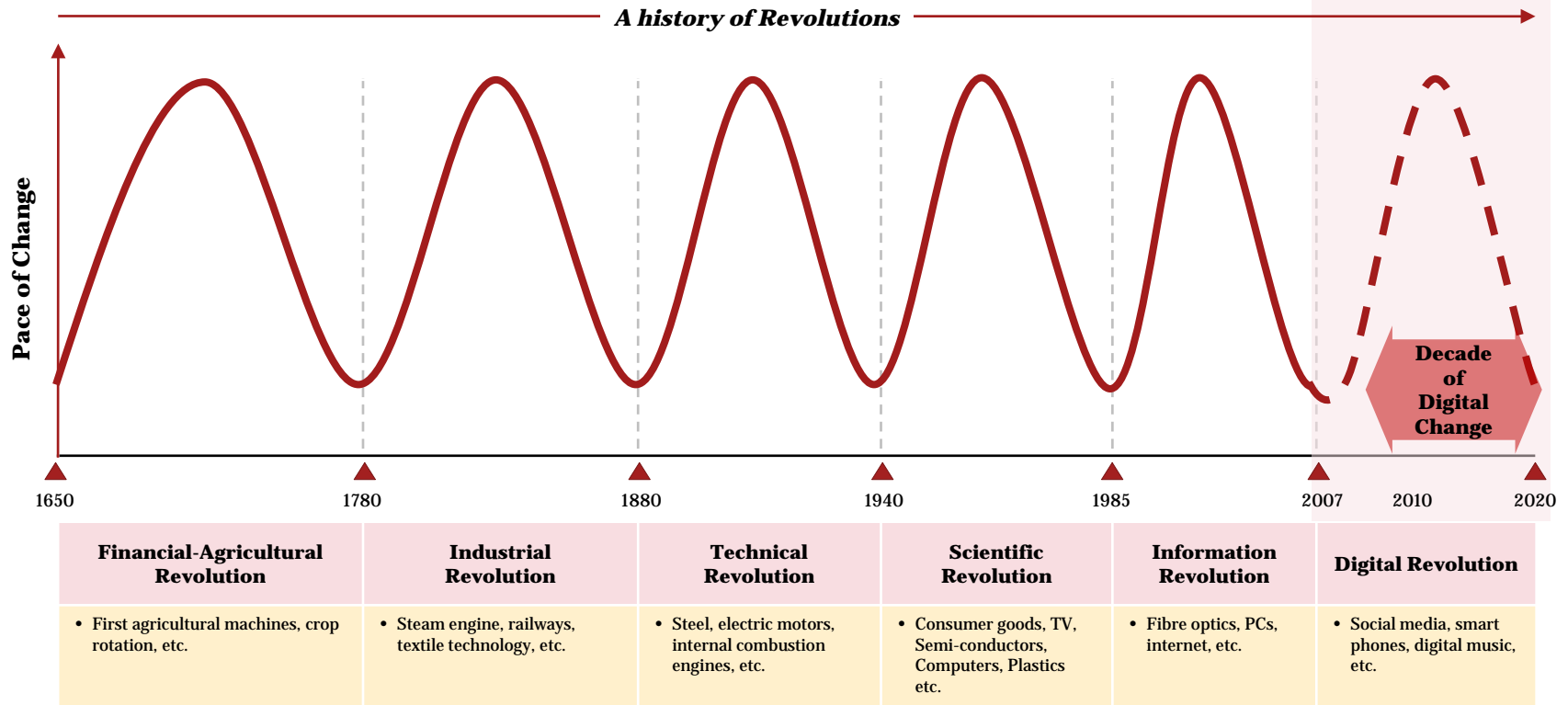


- Cybersecurity represents many things to many different people
- Key characteristics and attributes of cybersecurity:
 - **Broader** than just information technology and **extends** beyond the enterprise
 - **Increasingly vulnerable** due to technology connectivity and dependency
 - An ‘outside-in view’ 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!

Cybersecurity: The new reality

We live in a Digital Revolution, with associated threats and opportunities



Social media, “smart Mobility”, new consumption Analytics and Cloud computing are already shaping the Decade of Change

1999–2007

Product digitisation

Process digitisation

Pulling and aggregating info

Creating centralised marketplaces

Web = another channel to market

The ‘disruptors’

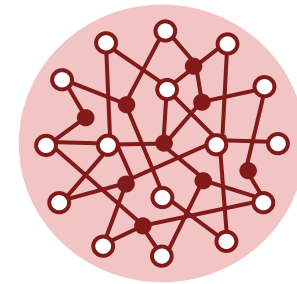
Social media

Smart Mobility

**Analytics
(incl. consumption data)**

Cloud computing

Today’s digital ecosystem



Integrated

Customer – centric

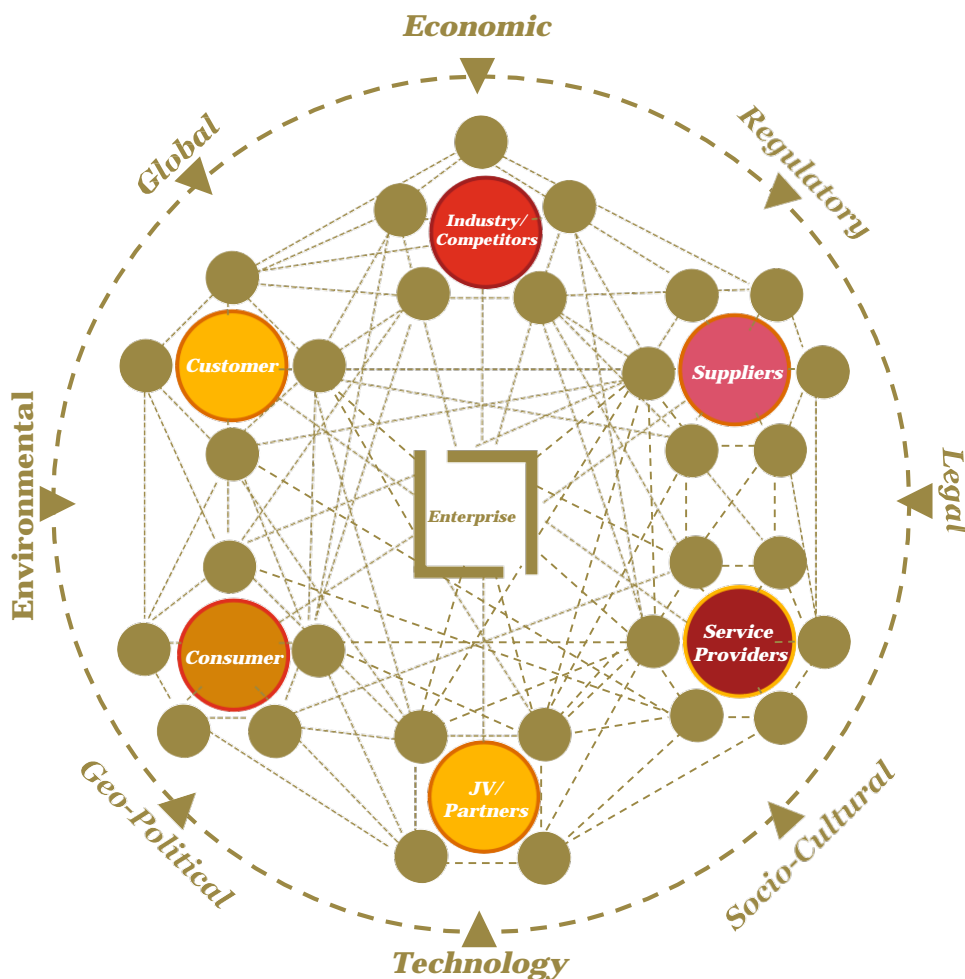
Continuous interaction

Collaboration

Revolutionary change to how information—based products are sold (Media – SW – Insurance – FS – etc.).
Revolutionary change to how customers are serviced in any sector.

The cyber challenge now extends beyond the enterprise

Global Business Ecosystem



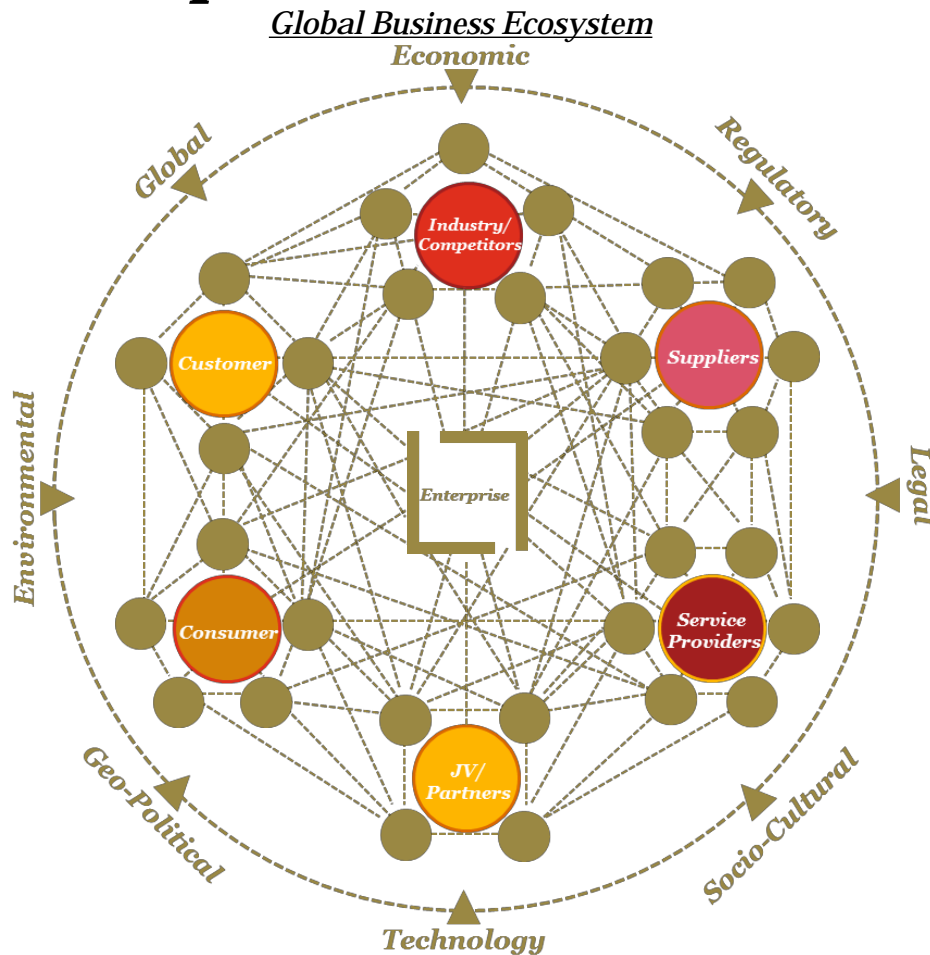
The Evolution:

- 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

The cyber challenge now extends beyond the enterprise



- 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.

Evolving business risks... *...impacting brand, competitive advantage, and shareholder value*

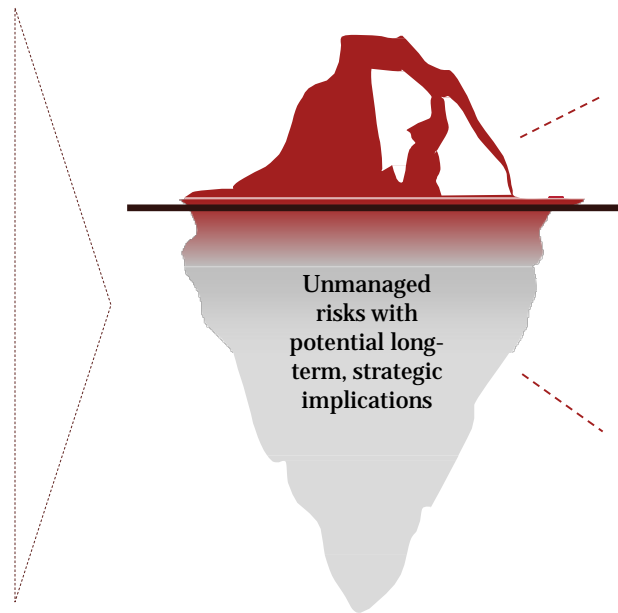
Highlights of activities impacting risk:

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*







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

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

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

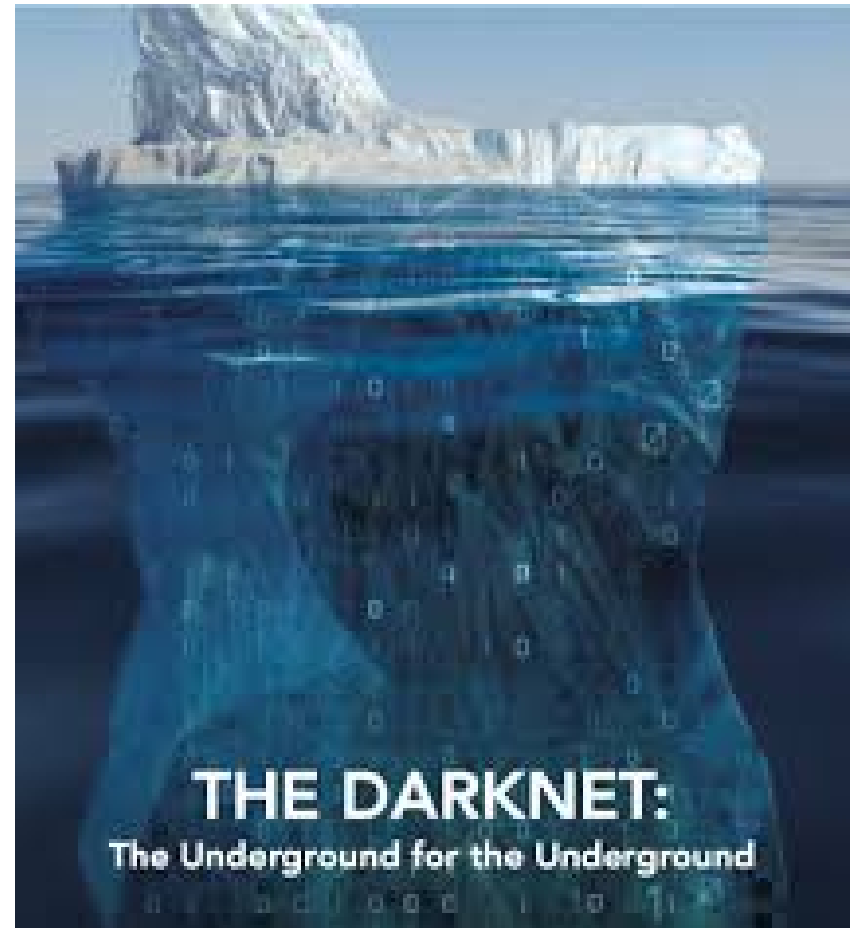
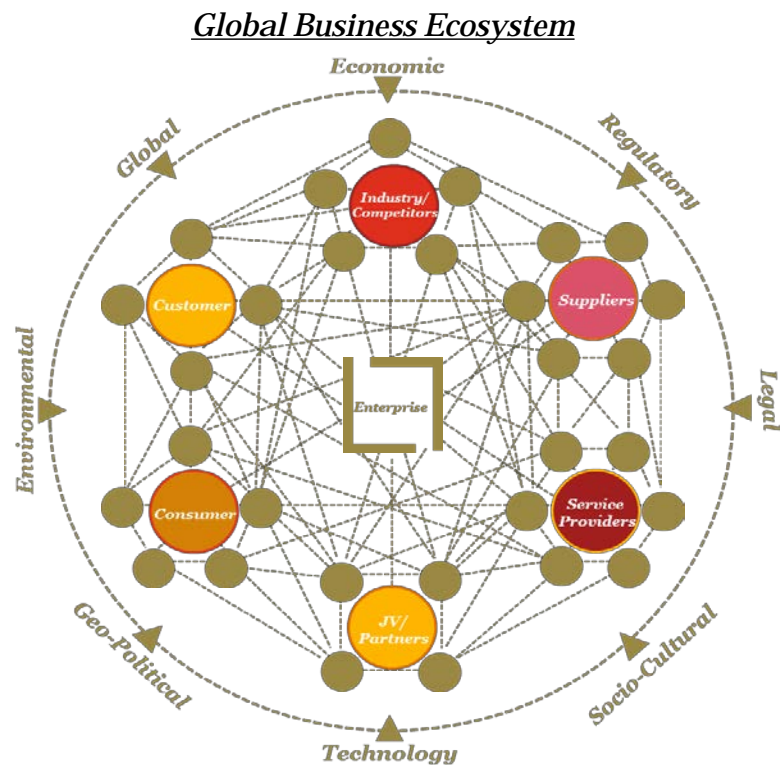


Information and communication technology and data

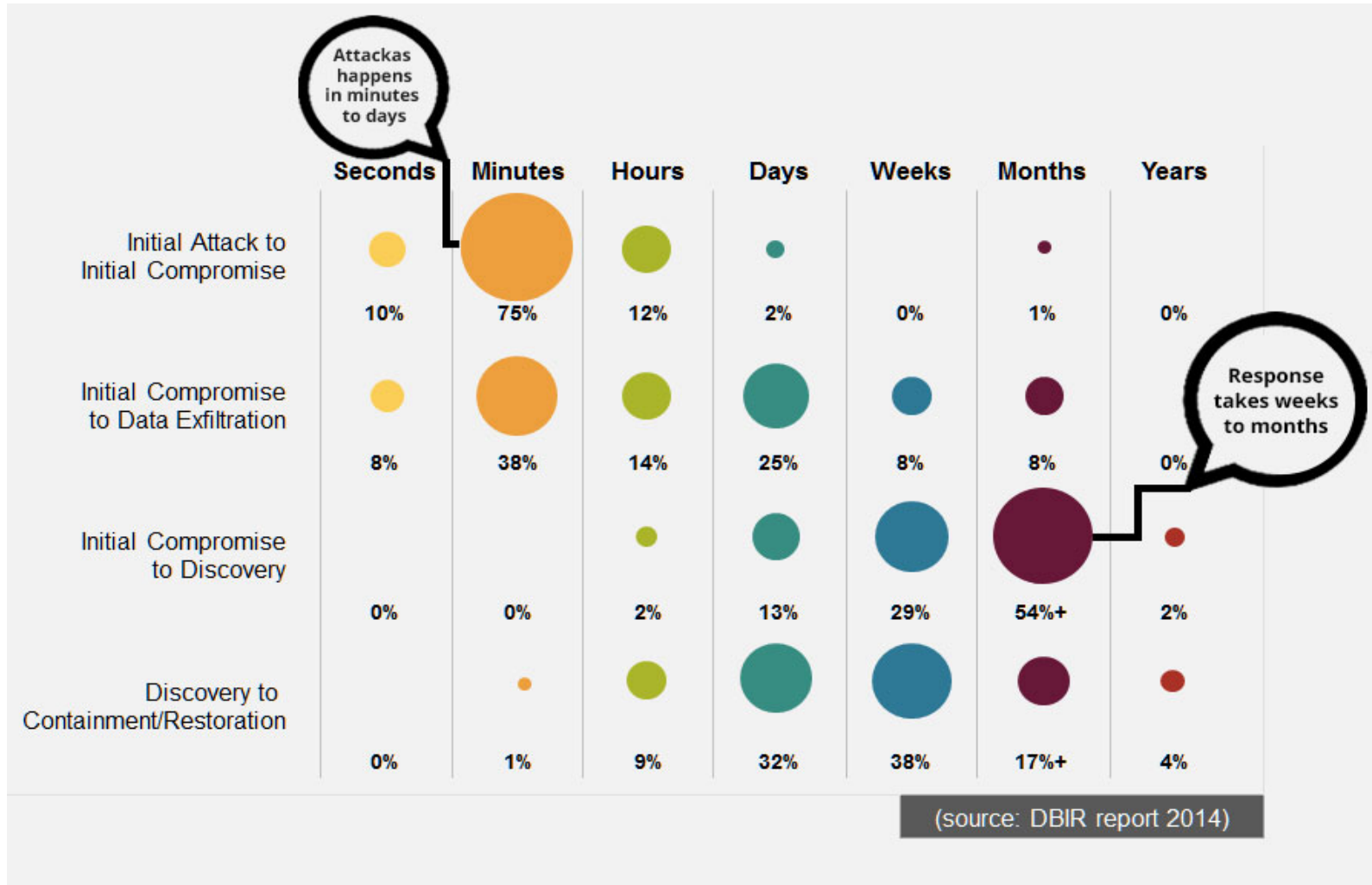
Input from Office of the National Counterintelligence Executive, *Report to Congress on the Foreign Economic Collection and Industrial Espionage, 2009-2011*, October 2011.

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

There is the Internet but there is also the Darknet



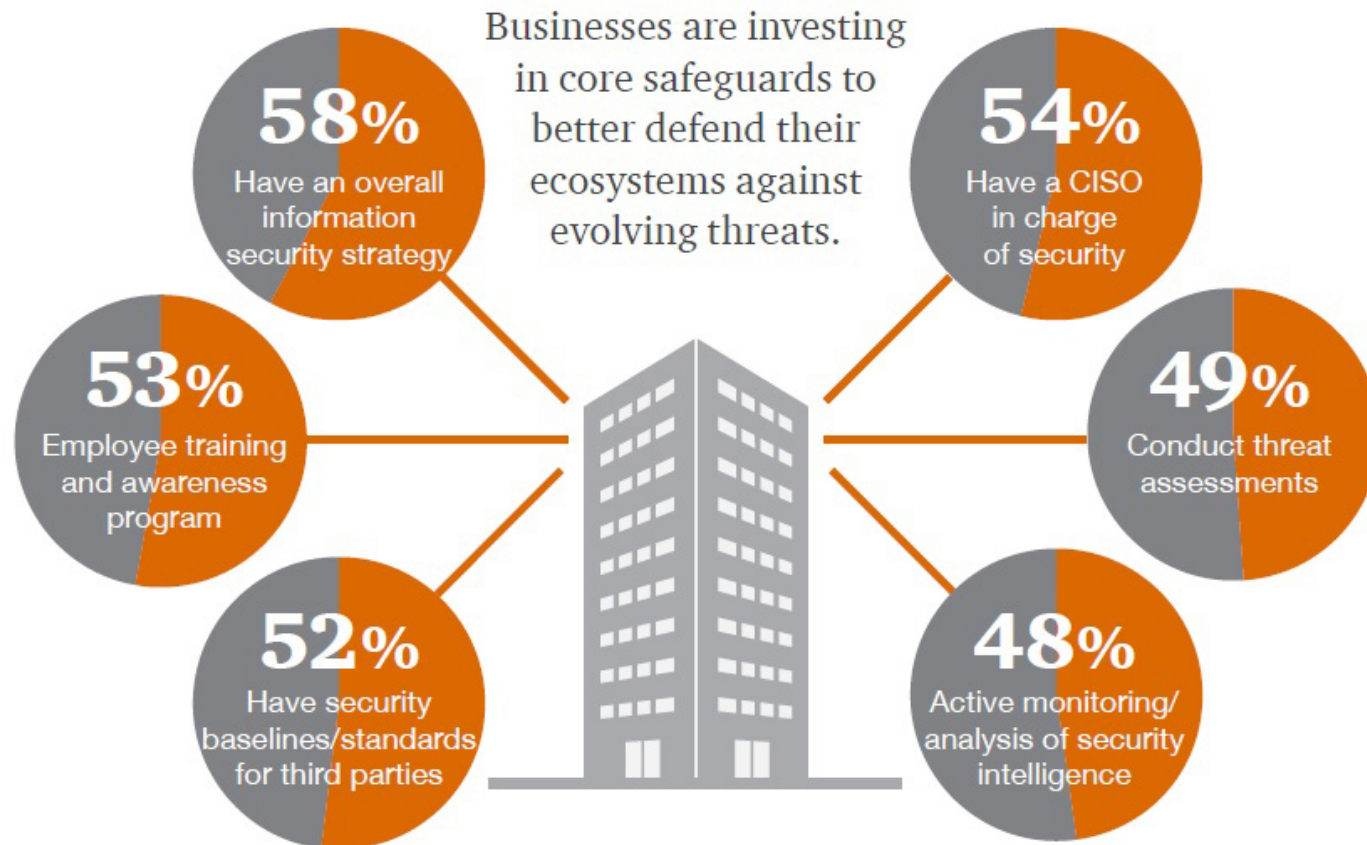
Speed will be the new determinant for cyber security



Adapting to the new reality

How are organisations responding to the Cyber security challenge?

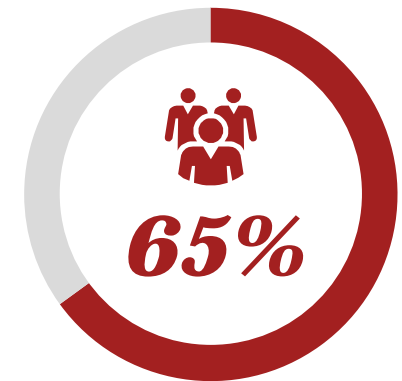
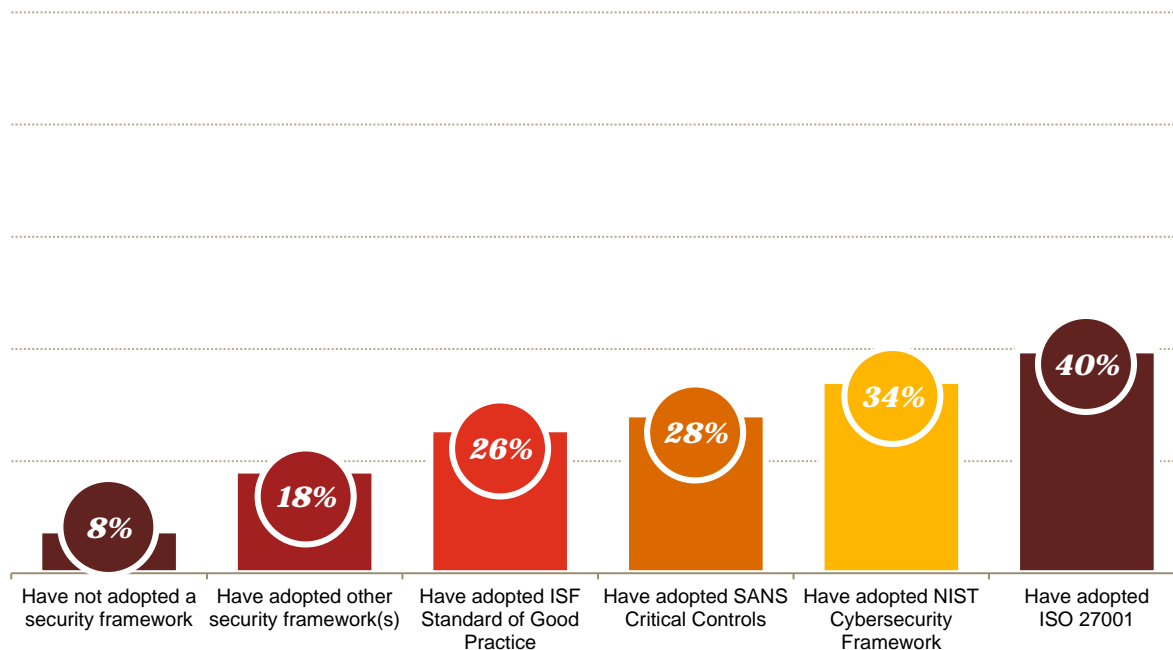
Implementation of key security safeguards



Most respondents (91%) have implemented one or more risk-based information security frameworks.

A majority of organizations also say they collaborate with external industry partners to improve security and reduce risks.

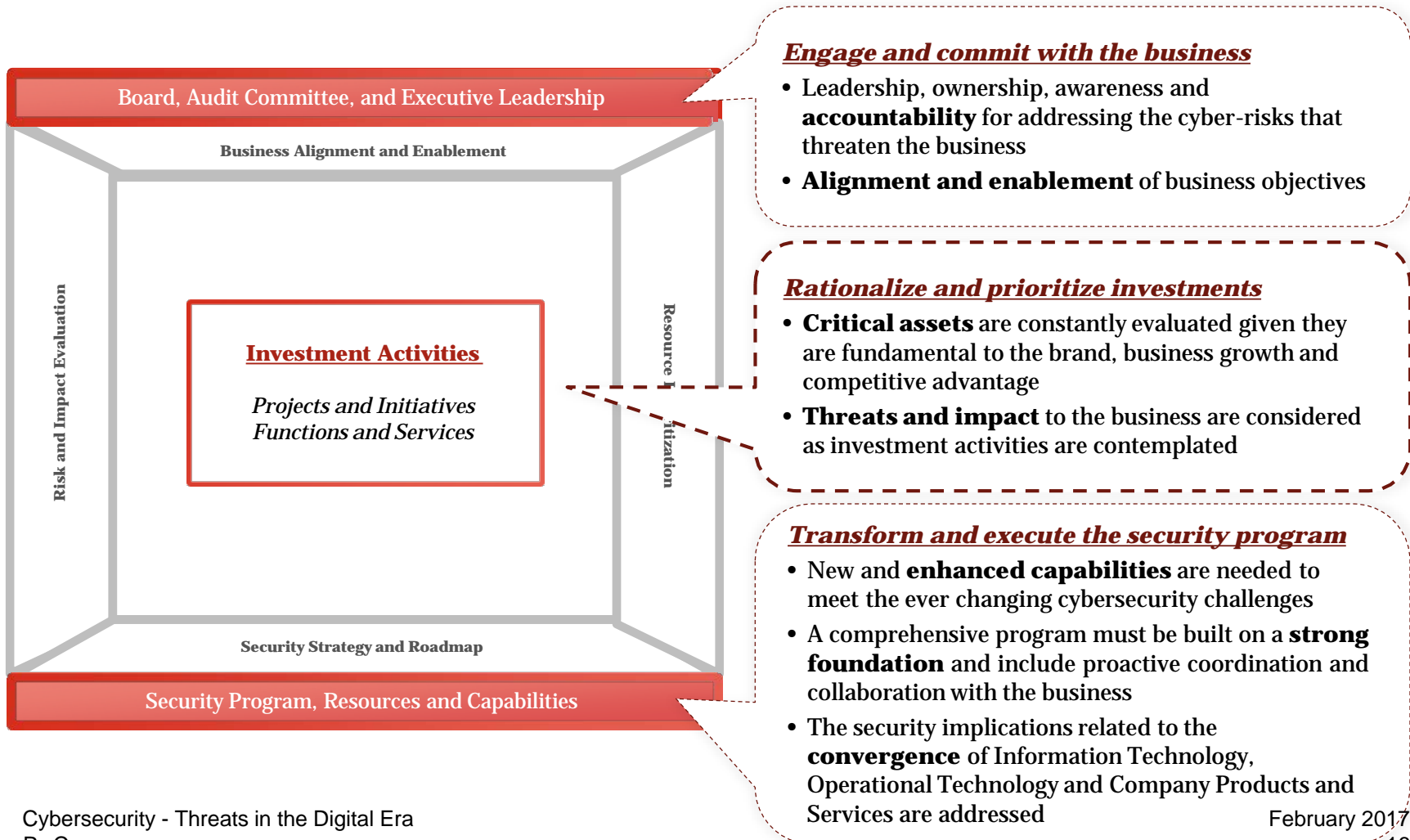
Adoption of risk-based security frameworks



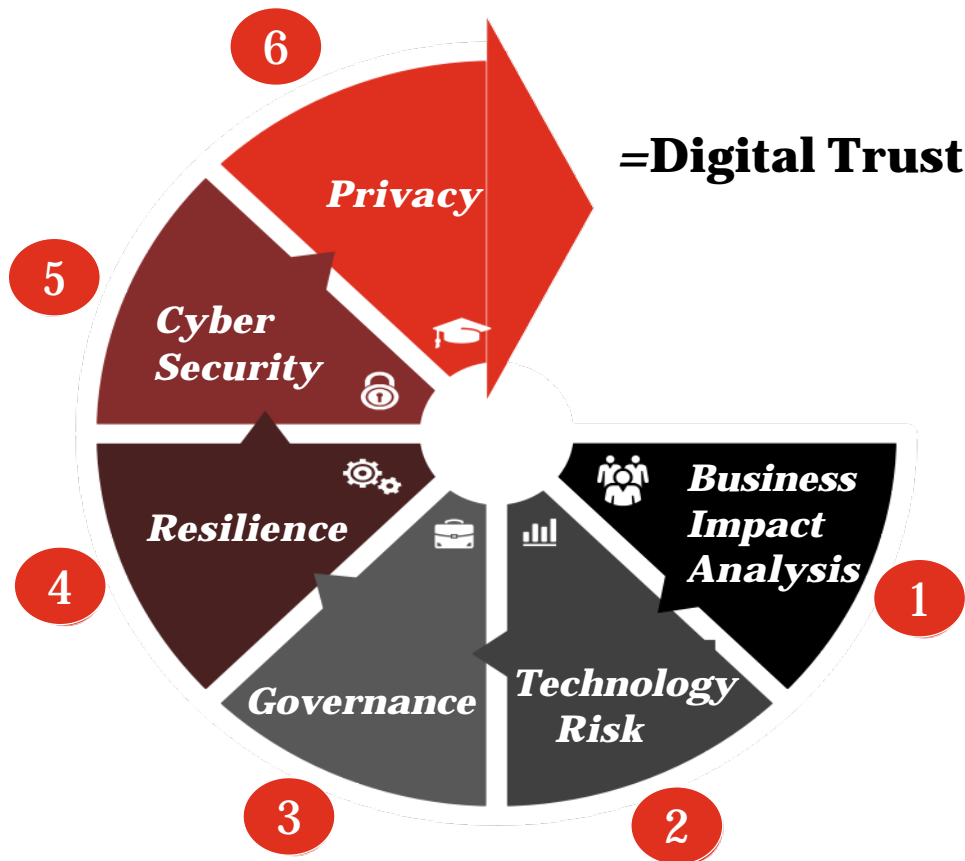
of respondents say they collaborate with others to improve information security

Keeping pace with the new reality – Key considerations

Operating in the global business ecosystem requires you to think differently about your security program and investments.



It is impossible to mitigate all risks; instead we need to focus on those with the highest probability and impact



-  1 Identify critical Business Processes and supporting data
-  2 Technology Risks (incl 3rd party risk) threatening the critical business processes
-  3 Define Risk Appetite, Governance and oversight mechanisms including continuous monitoring with metrics
-  4 Build IT resilience capabilities.
-  5 Cyber Security Program design Protect the data
-  6 Build Privacy by design & default and execute Data Cleansing on legacy systems

Digital Trust – the foundation needed to win in the digital era



The trust dynamic
Trust + Opportunity = Growth



Digital Trust = the baseline from which to digitize businesses, engage customers and disrupt industries



Protect the digital crown jewels. If not protected successfully can businesses see growth?



Digital Trust helps build the organizational confidence needed for the business to take the digitalization leap



The approach to achieve Digital Trust

Cyber Security

Protect the data
Cyber Security Program design

Technology Risk

Technology Risks (incl 3rdparty risk)
threatening the critical business processes

**Digital
Trust**

Resilience

Build IT resilience capabilities

Privacy

Build Privacy by design
Data Cleansing on legacy systems

Indicative projects – how we support our Clients

Threat & Vulnerability Management (Ethical Hacking)

- **Penetration Testing**
 - External
 - Internal
 - Wireless
 - Physical
- **Social Engineering Attacks**
- **Application security assessment**

Technology Risk, Incident & Crisis Management

- **Incident Response**
 - Forensic investigation of cyber-based intrusions and data theft. Containment of intrusion; remediation of security control weaknesses.
- **Insider Threat Investigations**
 - Network, computer, and internet surveillance: social media data leakage, data theft, fraud, workplace violence, policy violations
- **Business Continuity Program**

IT Security Strategy, Governance & Architecture

- **Information Security Strategy**
 - Cyber Security Program design and implementation
 - Policy, Standards, and Procedures
 - Security Controls Design
 - Security Risk Assessments
 - 3rd Party Attestations

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.

2,750+ practitioners and growing



Thank you



Tassos Procopiou
Partner
tassos.procopiou@cy.pwc.com
PwC Central
43 Demosthenis Severi Avenue
1080 Nicosia
Tel: 22555000
Fax: 22555016

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 Ltd, 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.

© 2017 PricewaterhouseCoopers Ltd. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers Ltd which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.