www.pwc.com/ca/security

The convergence of everything digital

How the fusion of information, operational and consumer technologies will transform the security landscape for business and society

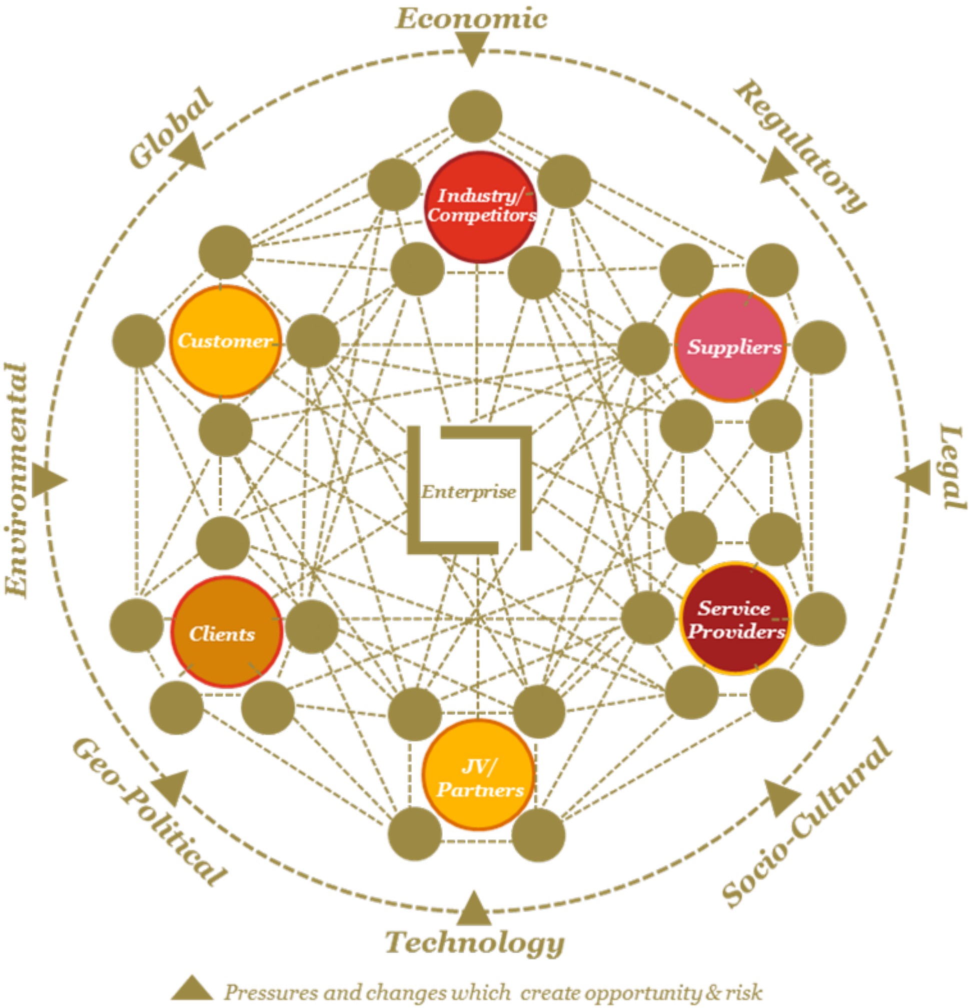
Concordia University
Engineering and Computer Science

IEEE
Signal Processing Society

November 2016

pwc

Digital convergence presents risks and opportunities



The Evolution:

- **Technology-led innovation** is transforming the busines models.
- Companies operate in a **dynamic environment** that is increasingly **hyper-connected** and **interdependent**.
- The ecosystem is built around a model of **open collaboration and trust**.
- **Constant information flow** is the lifeblood of the business ecosystem.

Leading to:

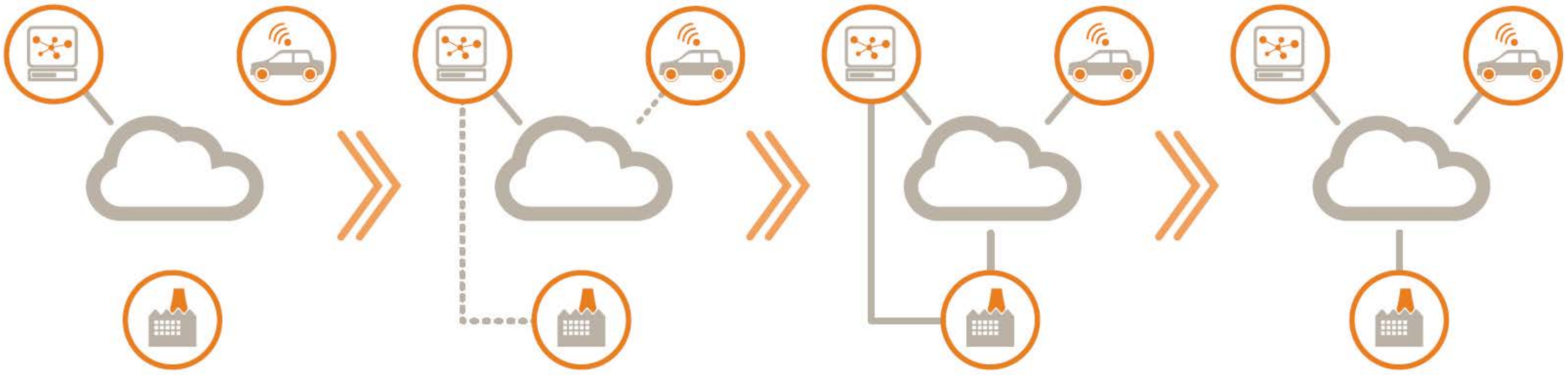
- **Benefits of same technological advances** are being **exploited by** an increasing number of global **cyber adversaries**.
- **Traditional threats** are manifesting increasingly through digital channels.
- Adversaries are **actively targeting critical assets** throughout the ecosystem.
- **Data is distributed and disbursed**, increasing the potential for loss and exposure.

Technology domains driving digital 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 Technology	Computing resources and connectivity integrated with or supporting external end-user focused products and services

Security programs should include all three technology types

A brief history of digital convergence



1980's

- IT, OT and CT operate in different environments and on different platforms
- OT and CT are based on proprietary platforms
- Data is not shared between technologies
- OT and CT face little to no cyber risk since they are not connected to a network

1990's

- OT is networked to allow centralized operation
- CT remains in a separate environment
- OT becomes vulnerable due to the connection, but is partially protected by the obscurity of proprietary solutions

2000's

- OT connects to IT using standardized IT channels to reduce costs and increase compatibility
- Boundaries between IT and OT start to blur
- CT connects to IT through purpose built channels
- OT is no longer protected by obscurity and CT is now vulnerable. Traditional IT security does not cover either

2010's

- The technology underlying IT has become ubiquitous across OT and CT
- The combination of these three represents the integrated technology ecosystem
- IT, OT and CT are all vulnerable to cyber threats. Businesses must adapt their security model to include the full scope of technologies

Information Technology

Operational Technology

Consumer Technology

☁ Internet

------ Proprietary Connection

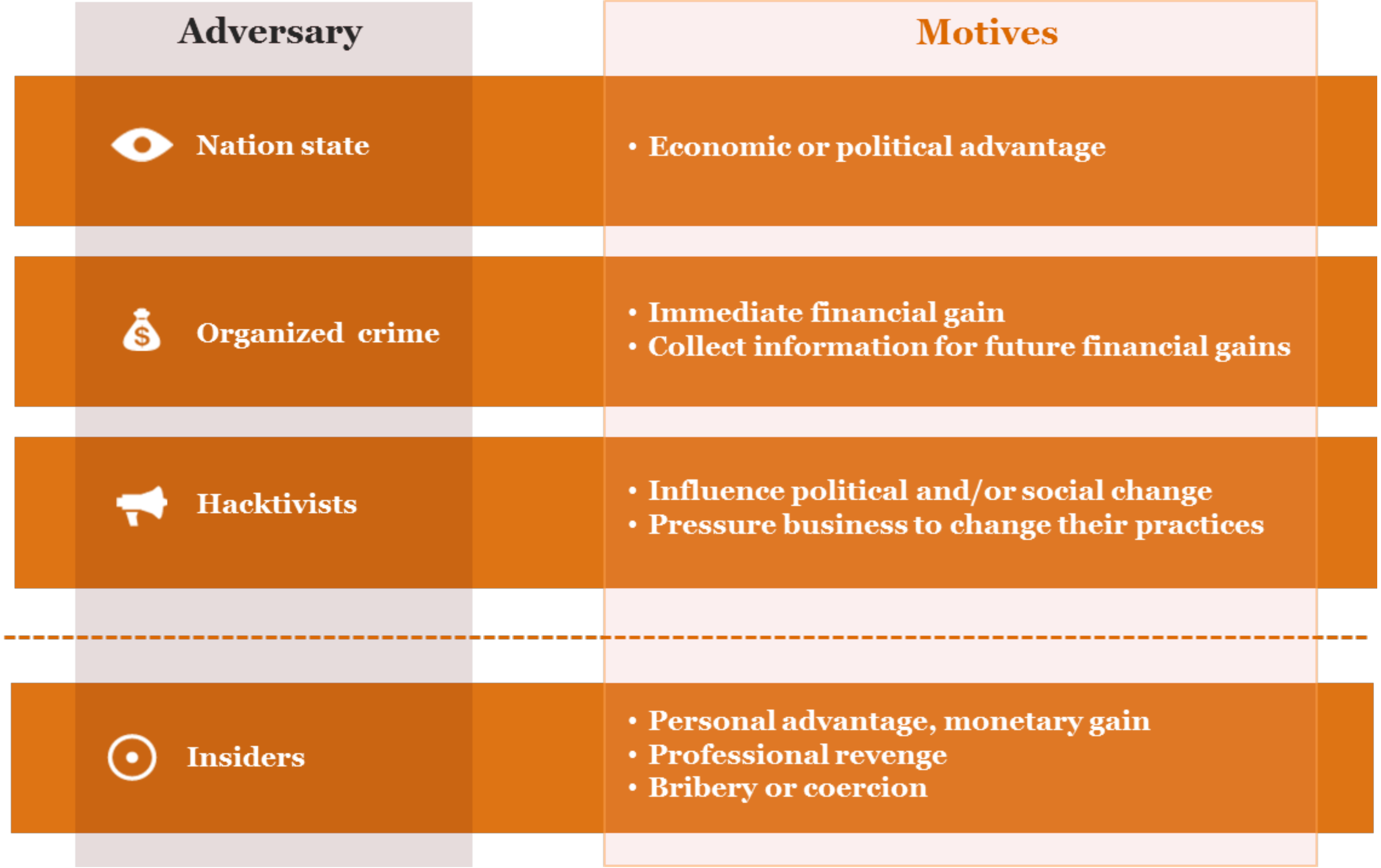
—— IT Protocol Based Connection

New cybersecurity liabilities: examples across industries

Sector	Operational technology examples	Consumer technology examples
Automotive	Automated manufacturing & logistics	In-vehicle communications & navigation systems, remote diagnostics & maintenance, Highway of the Future
Consumer products	Automated manufacturing & logistics	Home automation & security, smart appliances, wearable devices, smartphones & tablets
Energy & utilities	Generation & transmission, smart grid, intelligent asset management, automated meter reading	Smart meter apps, smart thermostats, digital communications with utilities
Entertainment, media, & communications	Cable distribution networks, broadcasting equipment	Set-top boxes, on-demand services, video streaming
Financial services	ATMs, branch equipment, transaction & payment processing	Online banking, alternative currencies, digital wallets
Healthcare provider/ payer	Electronic medical records, automated pharmacy dispensing systems, RFID real-time location	Wearable fitness devices, remote-patient monitoring, e-doctor services, patient portals & apps
Retail & consumer	Point-of-sale systems, RFID inventory management, location-based advertising	Shopping apps, in-store Wi-Fi, digital wallets, e-commerce
Technology	Data centers, cloud services, communications protocols, product life cycle management	Embedded technology & connectivity, consumer cloud services, social networking

Organizations today face four main types of cyber adversaries

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.



Adversary	Motives
Nation state	• Economic or political advantage
Organized crime	• Immediate financial gain • Collect information for future financial gains
Hacktivists	• Influence political and/or social change • Pressure business to change their practices
Insiders	• Personal advantage, monetary gain • Professional revenge • Bribery or coercion

Top 10 security vulnerabilities for OT and CT systems

Inadequate secure coding and testing

Insecure remote connectivity

Insufficient currency and patching

Poor password practices

Insecure firewall management

Insufficient monitoring and restriction of privileged access

Weak protection of the corporate IT network from OT and CT systems

Lack of network segmentation within OT environment

Unrestricted outbound internet access from OT networks

Insecure encryption and authentication of wireless communication

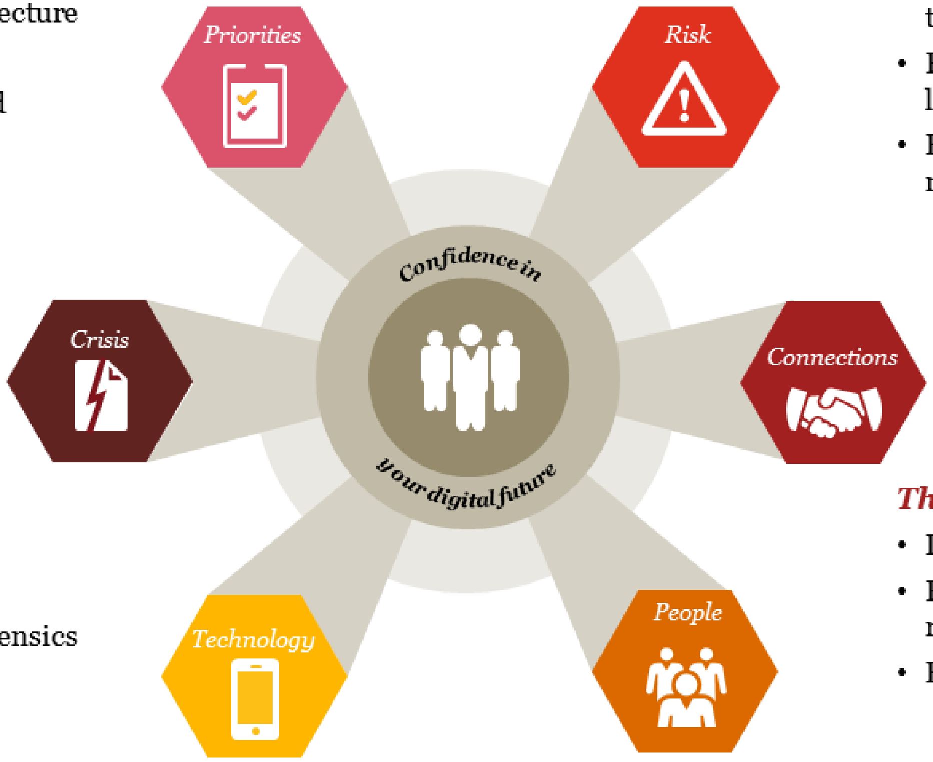
Cybersecurity isn't just about technology

You can't secure everything

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

Seize the advantage

- Digital trust is embedded in the strategy
- Privacy and cyber security legal compliance
- Risk management and risk appetite



It's not if but when

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

Their risk is your risk

- Digital channels
- Partner and supplier management
- Robust contracts

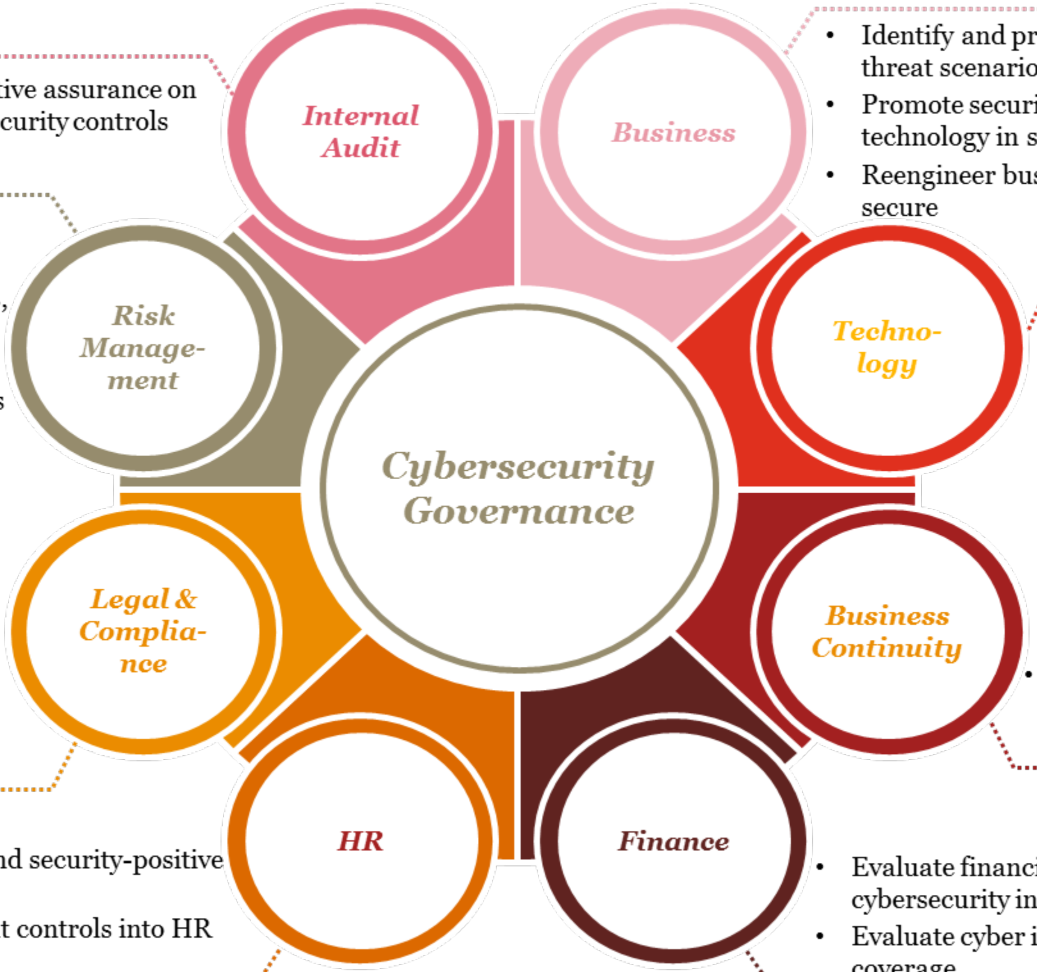
Fix the basics

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

People matter

- Insider threat management
- People and 'moments that matter'
- Security culture and awareness

Cybersecurity is a shared enterprise responsibility which requires cross functional governance



- Independent and objective assurance on effectiveness of cybersecurity controls

- Identify and prioritize “crown jewels” and cyber threat scenarios
- Promote security-positive culture and use technology in secure manner
- Reengineer business processes to be more secure

- Define cybersecurity risk appetite
- Challenge cybersecurity policies, risk assessments and strategy
- Measure and report on cybersecurity key risk indicators

- Define security policies and standards
- Perform security risk assessments
- Design, implement and operate security controls

- Evaluate legal and compliance implications of cybersecurity incidents
- Define/review third-party contracts for cybersecurity requirements
- Preserve legal privilege before and after cybersecurity incident

- Develop, rehearse and maintain cyber incident and crisis response plan

- Training, awareness and security-positive culture
- Integrate insider threat controls into HR processes

- Evaluate financial implications of cybersecurity incidents
- Evaluate cyber insurance policy and coverage

For more information, please contact:

Sajith (Saj) Nair, Partner, Cybersecurity & Privacy
+1 416 815 5185
s.nair@pwc.com

www.pwc.com/ca/security

The content of this presentation is for general information purposes only, and should not be used as a substitute for consultation with professional advisers.