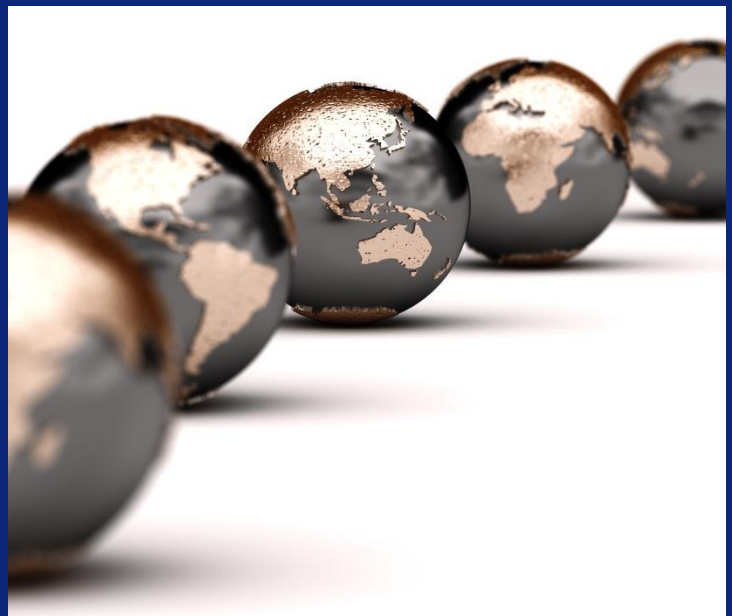
Deloitte.

Meeting the Cyber Risk Challenge—A Secure, Vigilant, and Resilient Business Case

Adnan Amjad
Partner
Deloitte & Touche LLP



The innovations that drive growth also create cyber risk

- **Threat actors exploit weaknesses that are byproducts of business growth and technology innovation.**
  - M&A or corporate restructuring
  - New customer service and sales models
  - New sourcing and supply chain models
  - New applications and mobility tools
  - Use of new technologies for efficiency gains and cost reduction
- **Perfect security is not feasible. Instead, minimize the impact of cyber incidents by becoming:**
  - **SECURE —**
    Enabling business innovation by protecting critical assets against known and emerging threats across the ecosystem
  - **VIGILANT —**
    Gaining detective visibility and preemptive threat insight to detect both known and unknown adversarial activity
  - **RESILIENT —**
    Strengthening your ability to recover when incidents occur

Cyber threats are asymmetrical risks

- Small, highly skilled groups exact disproportionate damage
- They often have very targeted motives
- They're spread across the globe, often beyond the reach of law enforcement
- Threat velocity is increasing
- The window to respond is shrinking

Rather than being a necessary burden, the cyber risk program is a positive aspect of managing business performance.

Copyright © 2014 Deloitte Development LLC. All rights reserved.

Executives must set risk appetite, and drive focus on what matters

It starts by understanding who might want to attack, why, and how

Copyright © 2014 Deloitte Development LLC. All rights reserved.

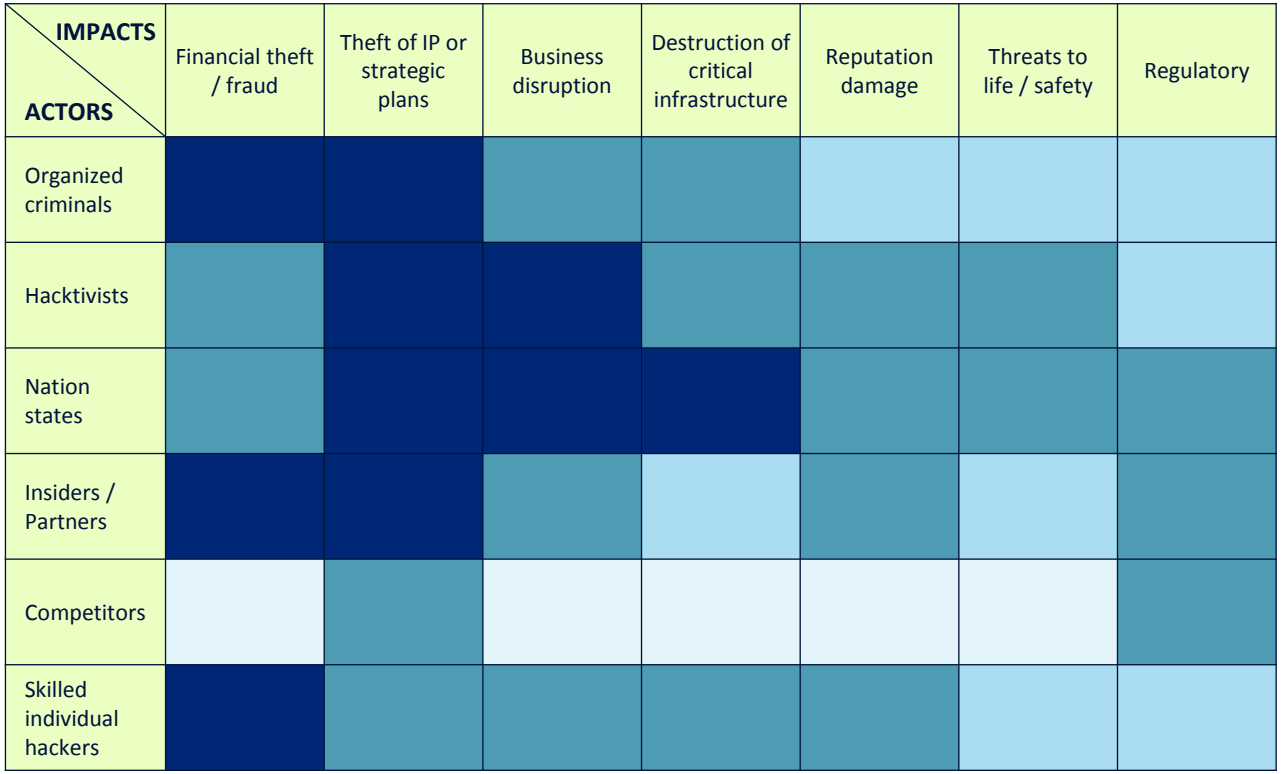
Threat actors and their motives vary by industry and organization

A typical cyber risk heat map for the Oil & Gas sector

Notable insights:

Cyber risks differ widely between upstream and downstream entities

- **Upstream** entities are concerned about competitive advantage being undercut by foreign nationals stealing bid information or strategic decision insights gained from data analysis.
- Tampering with Industrial Control Systems (ICS) by ideologically or politically-motivated actors could cause significant business disruption, leading to fines and other costs, revenue loss, decline of shareholder value, and impact to the environment and human life. Though unlikely, damage from failure of physical fail-safes mechanisms could be catastrophic.
- **Downstream** entities have greater concerns data privacy concerns pertaining to marketing manipulation and fraud associated with abuse of inventory, metering and accounting systems.



- Globalization of ecosystems driven by business expansion, including cloud computing, mobility and connected ICS, provides a greater attack surface for adversaries to exploit.
- Across the board, regulatory impact resulting from cyber incidents is fairly high.

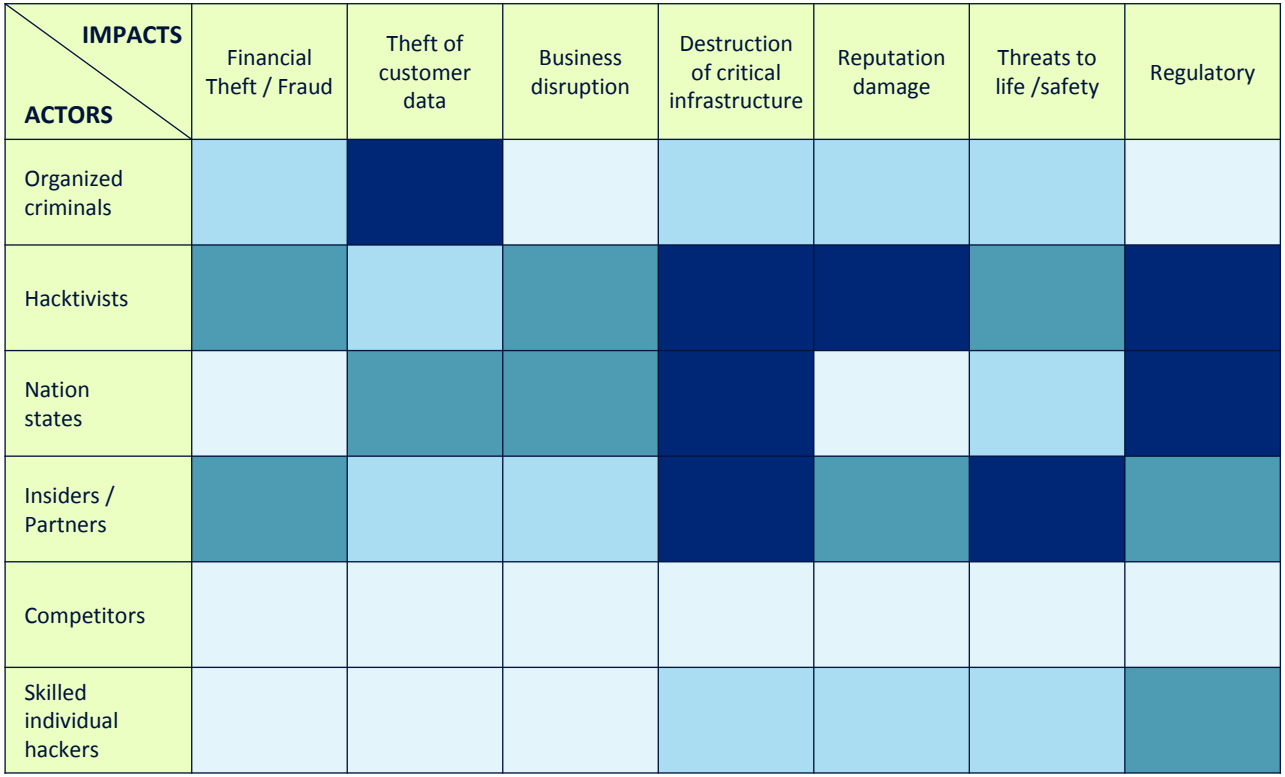
Copyright © 2014 Deloitte Development LLC. All rights reserved.

Threat actors and their motives vary by industry and organization

A typical cyber risk heat map for the Power & Utilities sector

Notable insights:

- There is financial risk tied to failure to comply with North American Electric Reliability Control Critical Infrastructure Protection (NERC CIP) version 5, and other regulations, but greater concern is loss of rate payer and board confidence should systems be breached.
- Hacktivists and nation-state actors could be behind the increase of publicized and unpublicized attacks on Industrial Control Systems (ICS), which are also vulnerable to accidental or intentional damage by business partners and insiders. While vendors have improved software security, fear of destabilizing the infrastructure leads many organizations to lag in keeping software up to date, magnifying the risk level.
- Metering and accounting systems may be vulnerable to tampering, resulting in financial loss.



Cyber attacks are increasing, but defenses lag.

- *From Oct. 1, 2012 to Apr. 30, 2013, ICS-CERT responded to over 200 incidents across all critical infrastructure sectors, more than had been reported the entire previous year.* (ICS-CERT Monitor, *April-June 2013)*
- *In 2012, a researcher identified over 20,000 ICS-related devices directly IP addressable and vulnerable to exploitation through weak or default authentication.* (ICS-CERT Monitor *Oct.-Dec. 2012)*

Copyright © 2014 Deloitte Development LLC. All rights reserved.

Executive sponsorship is the key to success

Every leader has a distinct role to play in driving alignment

Board & CEO

Tone at the top, establish senior management accountability and a cyber-aware culture

CYBER RISK GOVERNANCE

Senior Management (COO, CAO, CRO)	IT Leadership (CIO)	IT Risk Leadership (CISO / CITRO)	Line of Business Leaders
Define the organization's cyber risk appetite and be accountable for cyber risk management. Empower the extended leadership team.	Lead (not delegate) in defining and executing the strategy to become *secure, vigilant, and resilient*. Establish an effective interaction model with CISO and IT risk officer.	Define the right balance between threat-centric vs. compliance-centric programs. Be a business enabler, without shying away from the role of risk custodian.	Support integration of cyber risk management into business growth and development activities. Appoint line-of-business risk officers.

IT DOMAINS

Execute on strategy

Manage and report on risks

Architecture & Engineering	Infrastructure	Application Development	Security Operations	*Other functions…*

Fully integrate cyber risk management into IT disciplines – design for Six Sigma, not quality control. Integrate current technologies to address the latest threats

Copyright © 2014 Deloitte Development LLC. All rights reserved.

Top actions and questions for executives

Key actions you need to own

- **Put a senior executive at the helm.**
  He or she must be able to lead in a crisis, and also guide the program and enlist collaboration across diverse functions.
- **Map threats to the business assets that matter.**
  Set direction, purpose, and risk appetite for the program. Establish priorities, and ensure funding and resourcing.
- **Drive early "wins."**
  Establish momentum by focusing on pilot initiatives that measurably impact business success. Use these to plant the seeds of long-term cultural change.
- **Accelerate behavior change.**
  Create active learning scenarios that instill awareness of the impact of daily activity on cyber risk. Embed cyber risk management goals into evaluation of Top 100 executives.
- **Trust but verify.**
  Conduct monthly or quarterly reviews about key risks and risk metrics, and address roadblocks.

Key questions you need to ask

- **Are we focused on the right things?**
  Often said, but hard to execute. Understand how value is created in your organization, where your critical assets are, how they are vulnerable to key threats. Practice defense-in-depth.
- **Do we have the right talent?**
  Quality over quantity. There is not enough talent to do everything in-house, so take a strategic approach to sourcing decisions.
- **Are we proactive or reactive?**
  Retrofitting for security is very expensive. Build it upfront in your management processes, applications and infrastructure.
- **Are we incentivizing openness and collaboration?**
  Build strong relationships with partners, law enforcement, regulators, and vendors. Foster internal cooperation across groups and functions, and ensure that people aren't hiding risks to protect themselves.
- **Are we adapting to change?**
  Policy reviews, assessments, and rehearsals of crisis response processes must be regularized to establish a culture of perpetual adaptation to the threat and risk landscape.

Copyright © 2014 Deloitte Development LLC. All rights reserved.

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

Copyright © 2014 Deloitte Development LLC. All rights reserved.
Member of Deloitte Touche Tohmatsu Limited