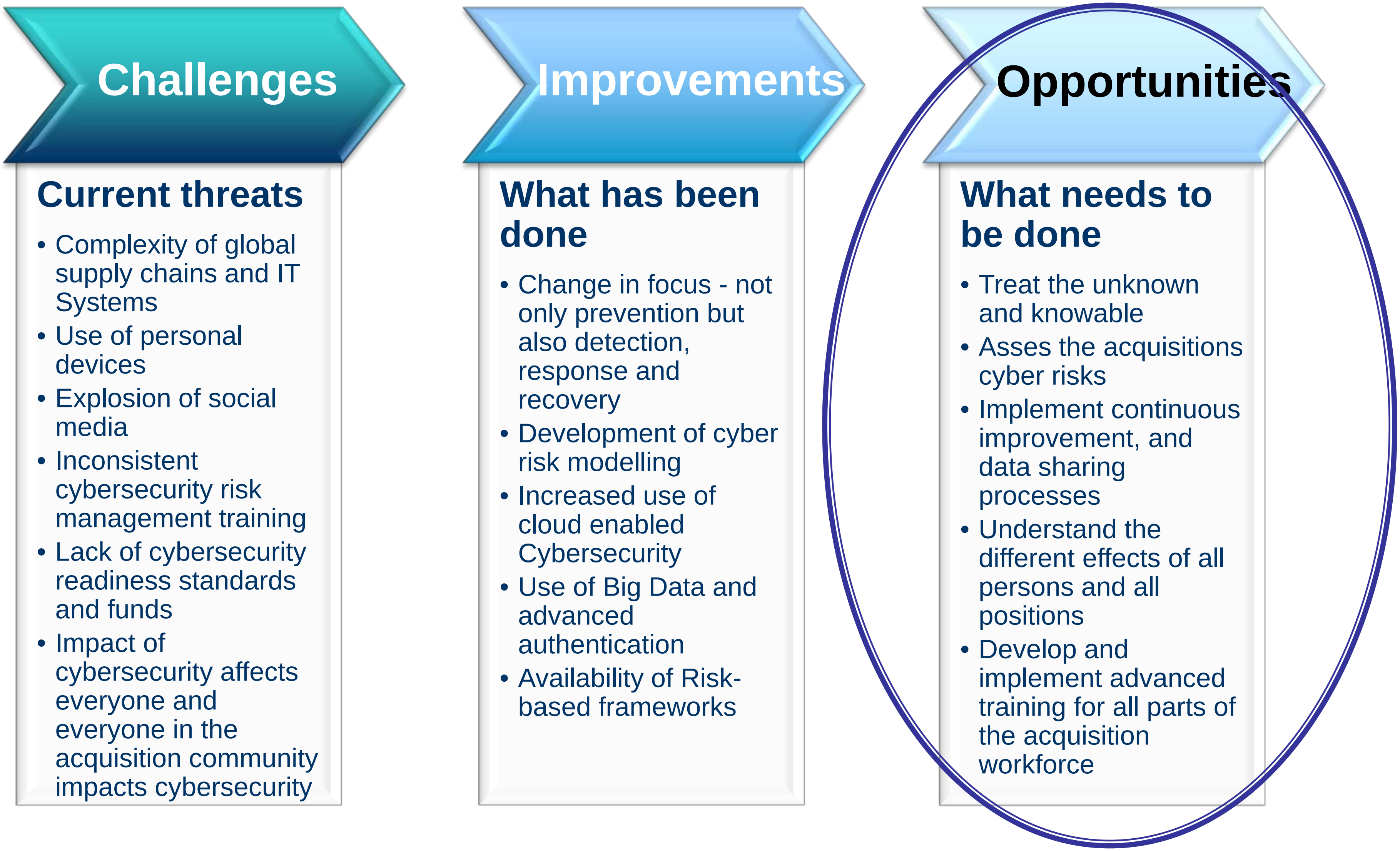
Cybersecurity Challenges in Acquisition

May 4, 2016

Sonia Kaestner, Craig Arndt, and Robin Dillon-Merrill

Georgetown University
McDonough School of Business

Cybersecurity Challenges in Acquisition Roadmap



Challenges

Current threats

- Complexity of global supply chains and IT Systems
- Use of personal devices
- Explosion of social media
- Inconsistent cybersecurity risk management training
- Lack of cybersecurity readiness standards and funds
- Impact of cybersecurity affects everyone and everyone in the acquisition community impacts cybersecurity

Improvements

What has been done

- Change in focus - not only prevention but also detection, response and recovery
- Development of cyber risk modelling
- Increased use of cloud enabled Cybersecurity
- Use of Big Data and advanced authentication
- Availability of Risk-based frameworks

Opportunities

What needs to be done

- Treat the unknown and knowable
- Asses the acquisitions cyber risks
- Implement continuous improvement, and data sharing processes
- Understand the different effects of all persons and all positions
- Develop and implement advanced training for all parts of the acquisition workforce

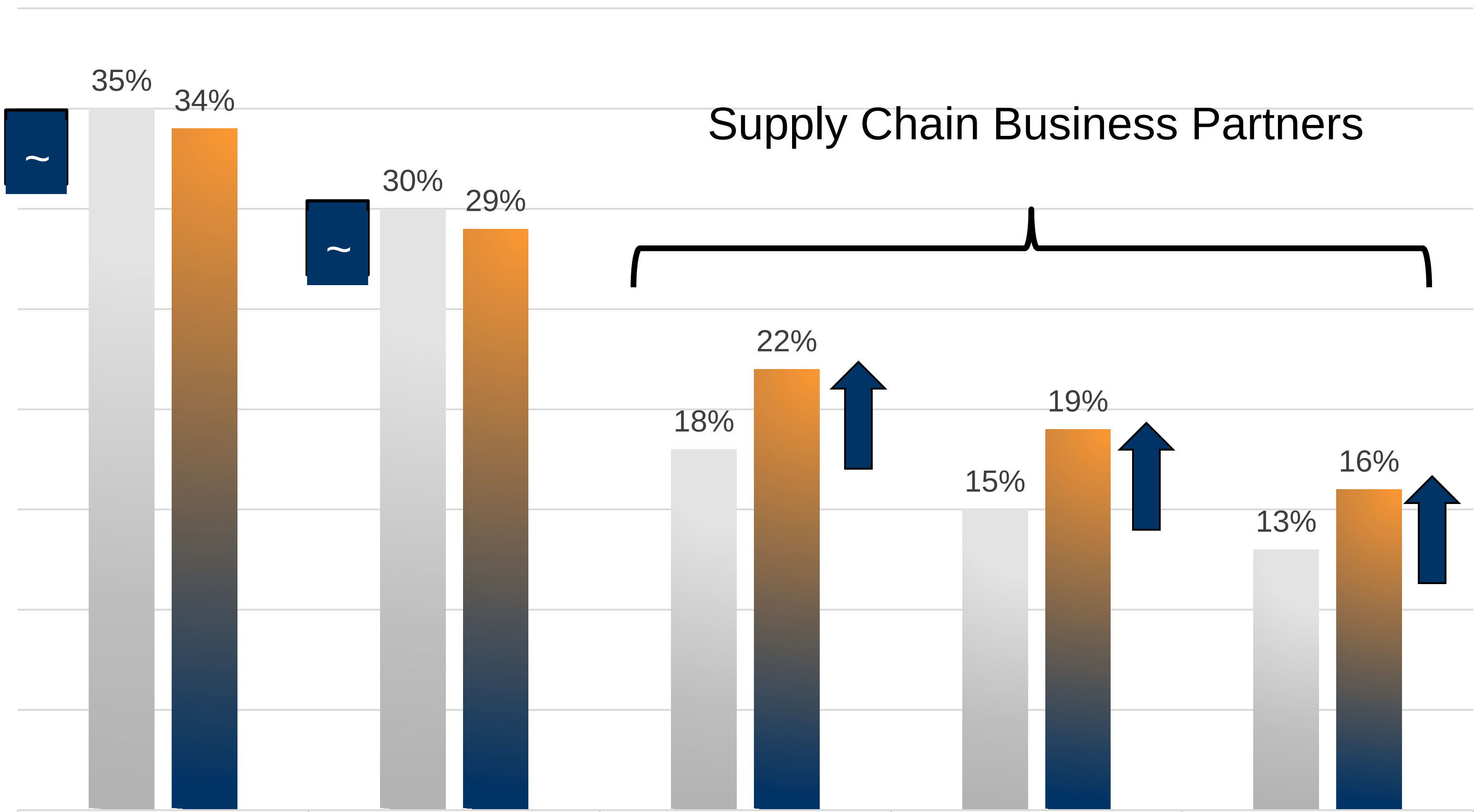
93% of Cybersecurity Breaches Are Caused by Human Error

- Inadequate and/or inconsistent security technology implementation
- User lack of cybersecurity knowledge proper to their role and responsibilities
- Incomplete requirements are created by people who do not understand the cyber technology or the cyber threats
- Poor design by people that do not understand the latest cyber security methods
- Poor testing, by people that do not fully understand the threats, produces unreliable results

The Risk of Insider Threats Is Underestimated

- Cybersecurity external attacks get plenty of attention
- Insider (i.e., connected companies, direct employees) attacks posse a more pernicious threat
  - Easier access to systems
  - Much greater window of opportunity
  - Less information available
- Most organization do not give the priority level insider threats deserve

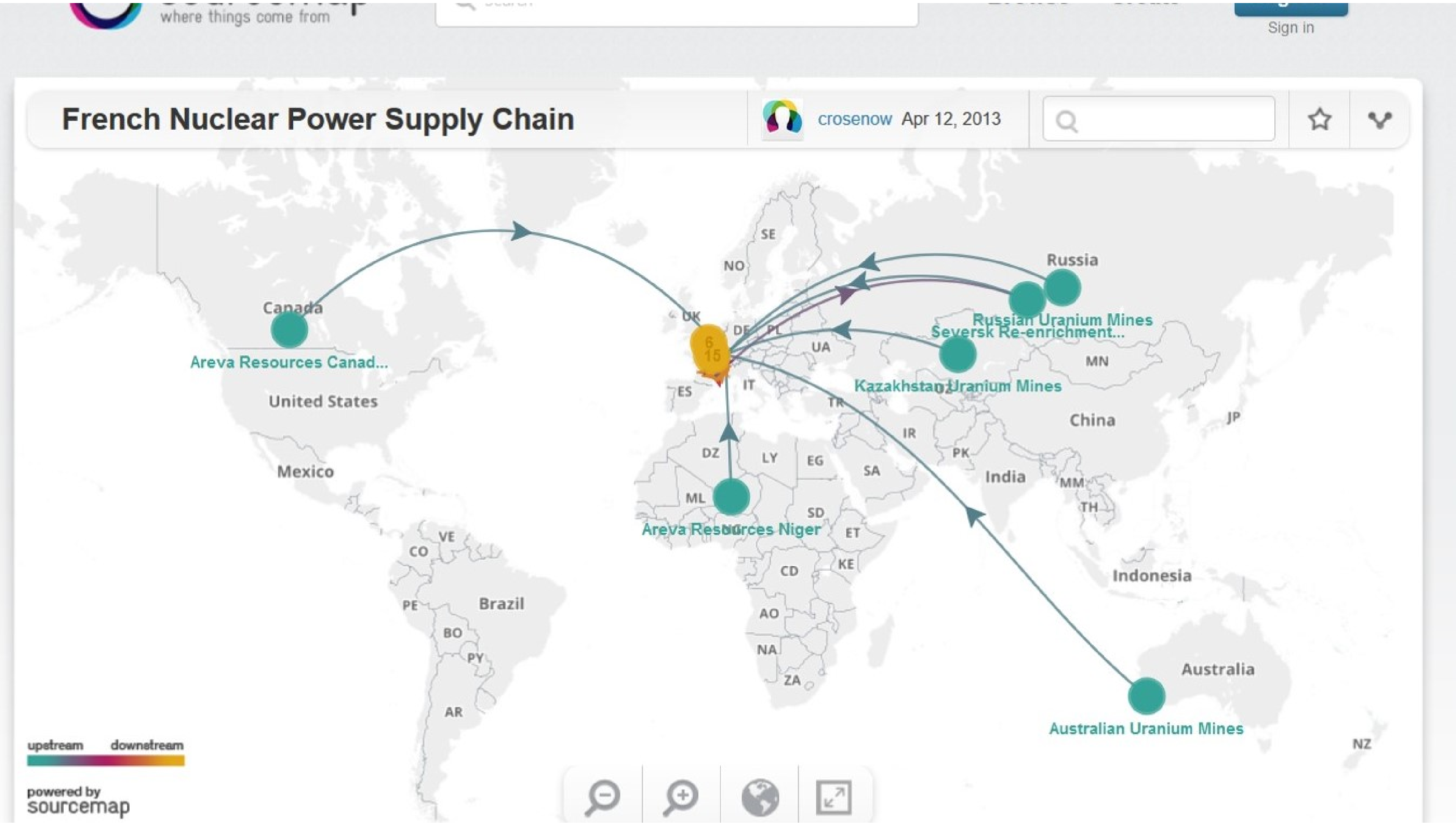
Incidents Related to Business Partners Increased in 2015*



	Current Employees	Former Employees	Current Service Providers Consultants/Contractors	Former Service Providers Consultants/ Contractors	Suppliers/ Partners
□ 2014	35%	30%	18%	15%	13%
■ 2015	34%	29%	22%	19%	16%

* Adapted from the PwC *The Global State of Information Security® Survey 2016,*

Global Nature of Most Supply Chains Adds an additional Layer of Complexity



Cost Benefit Analyses Underestimate the Importance of Cybersecurity RM

Financial Impact

- Losses are so small compared to the revenue for large organizations
- SEC reporting requirements are not fully complied and/or enforced

Accounting Perspective

- Treated as an expense
- Absorption costing is not used (include IT and cybersecurity spending into supply chain management cost)

Human Mentality

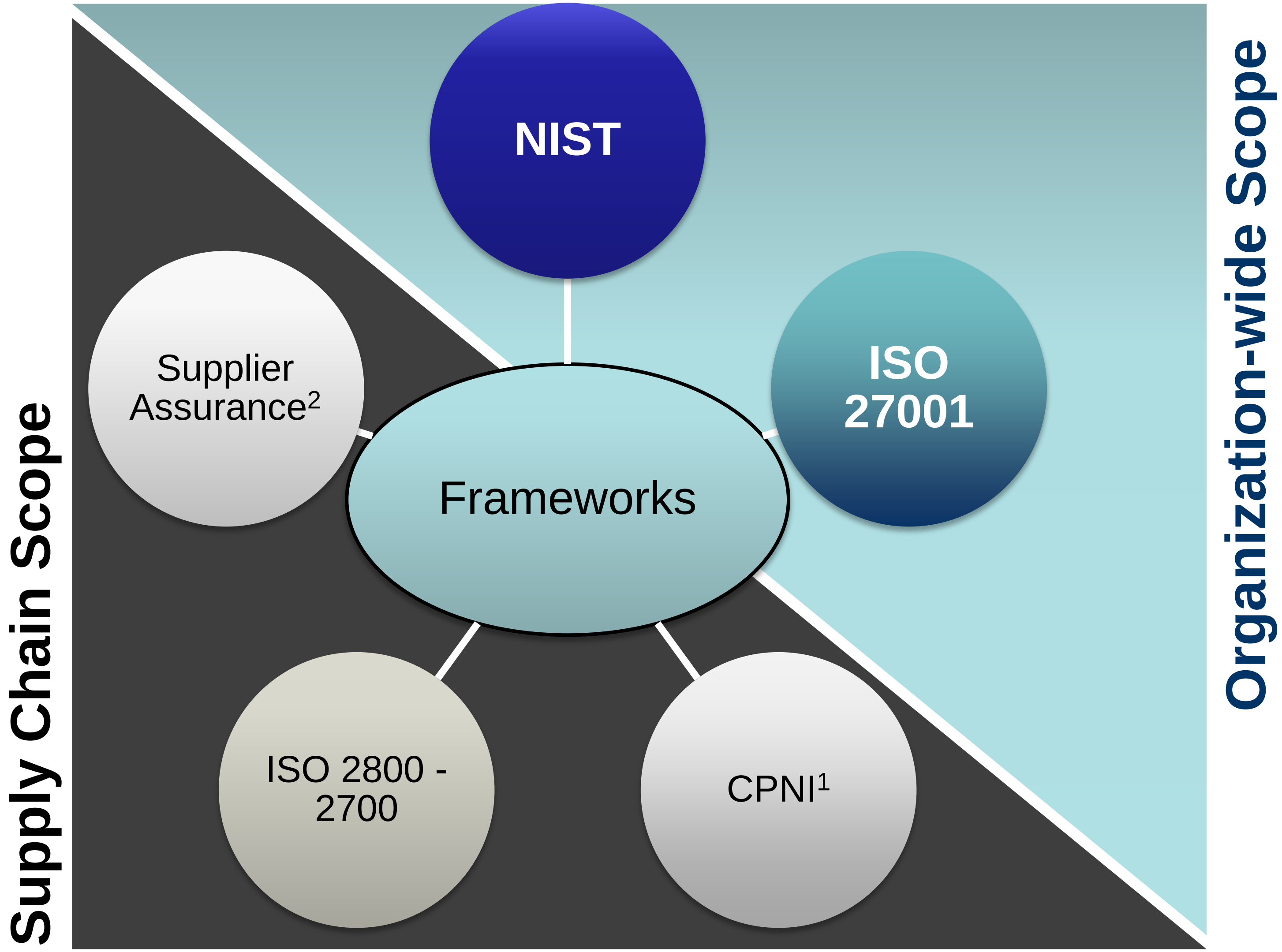
- Communicated as abstract and complex potential event
- Is not perceived as an intentional moral transgression
- Is deemed to be an uncertain event

Political Perspective

- Government subsidies
- Corporate responsibility

Cybersecurity Risk Management Practices

Risk-Based Cybersecurity Frameworks

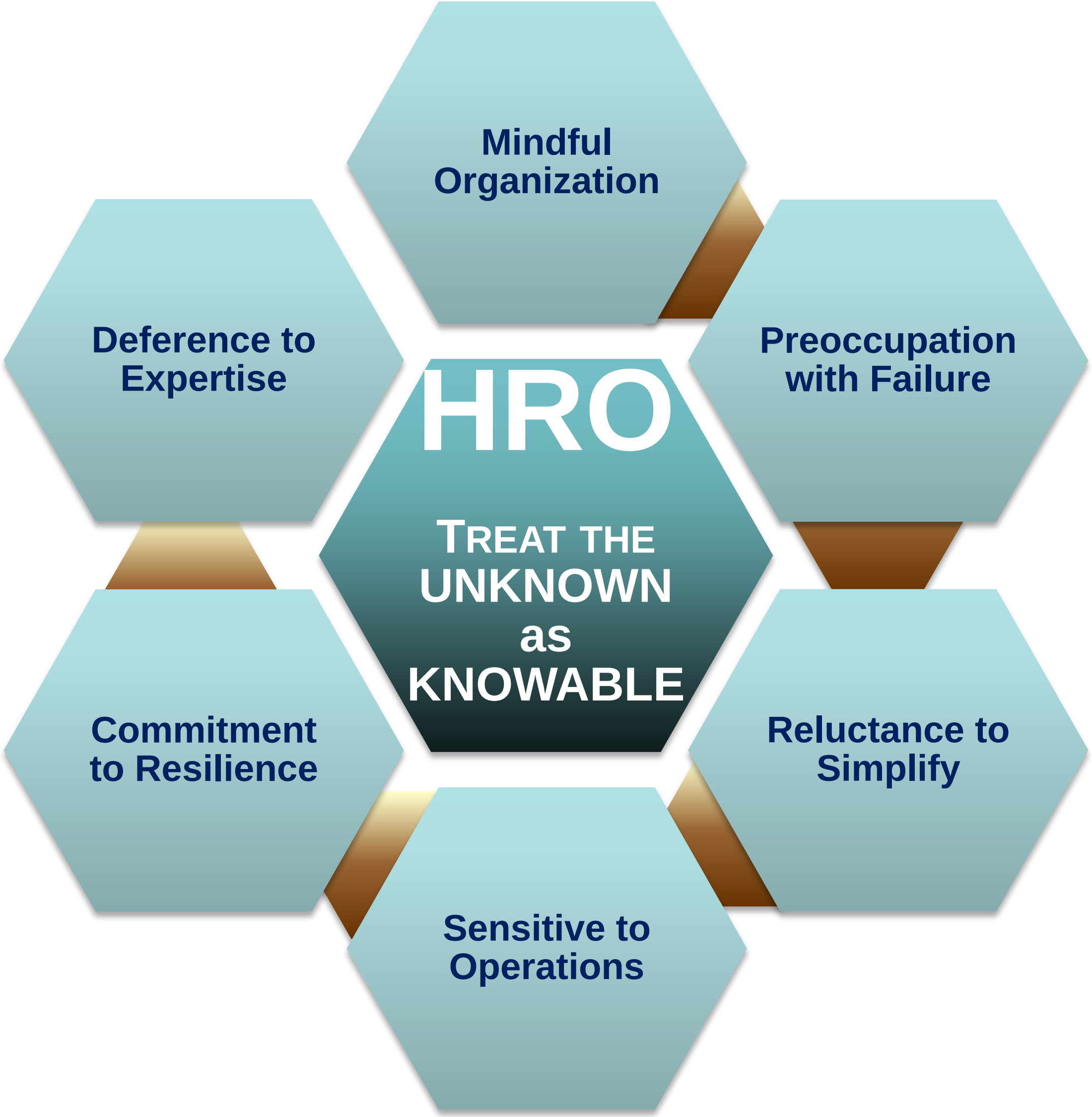


[1] Centre for the Protection of National Infrastructure

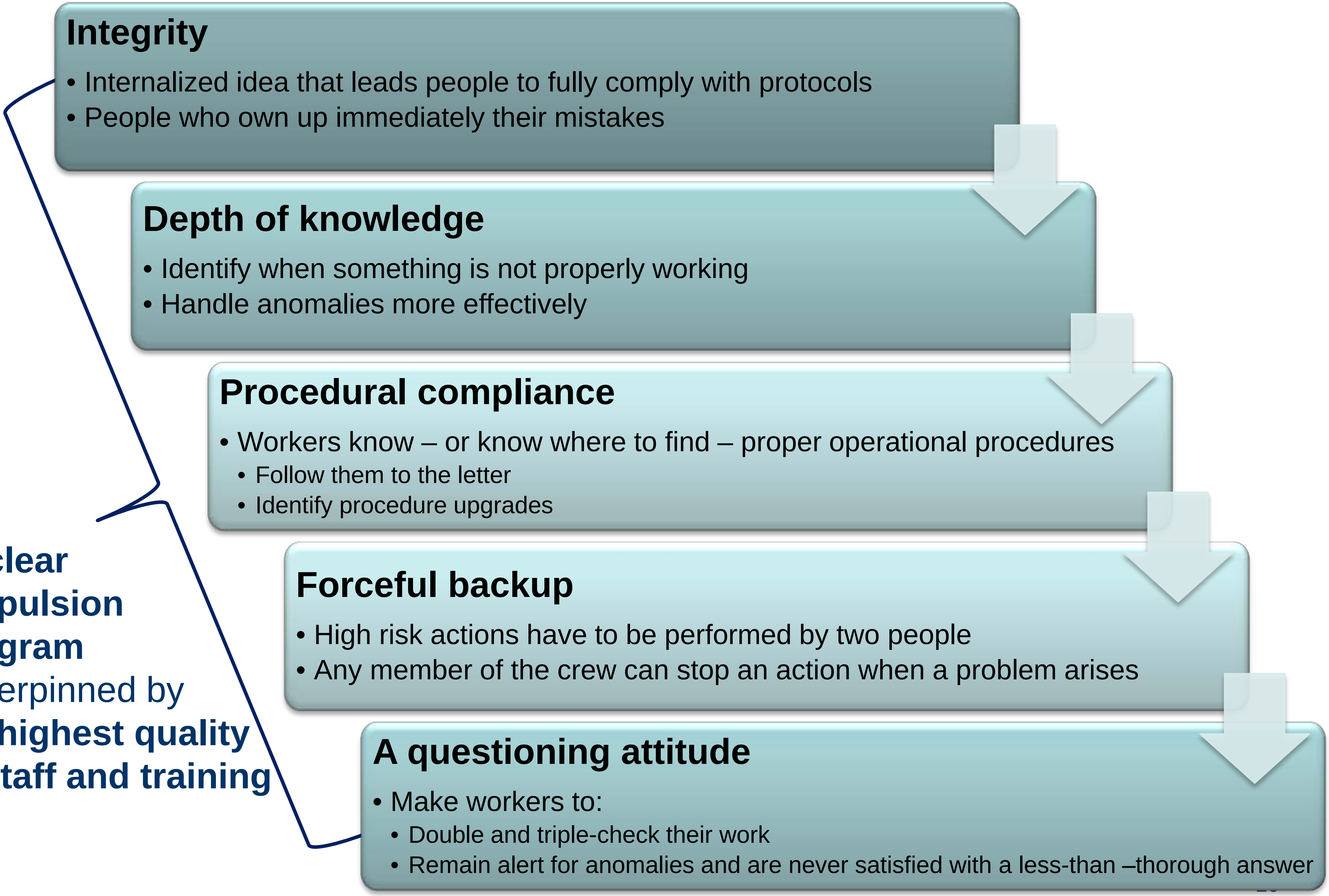
[2] UK Cabinet Office

High-Reliability Organization
An Alternative Approach to Cybersecurity

Georgetown University
McDonough School of Business



High-Reliability Organizations
U.S. Navy’s Nuclear Propulsion Program



Integrity

- Internalized idea that leads people to fully comply with protocols
- People who own up immediately their mistakes

Depth of knowledge

- Identify when something is not properly working
- Handle anomalies more effectively

Procedural compliance

- Workers know – or know where to find – proper operational procedures
  - Follow them to the letter
  - Identify procedure upgrades

Forceful backup

- High risk actions have to be performed by two people
- Any member of the crew can stop an action when a problem arises

A questioning attitude

- Make workers to:
  - Double and triple-check their work
  - Remain alert for anomalies and are never satisfied with a less-than –thorough answer

Nuclear Propulsion Program underpinned by the **highest quality of staff and training**

Recommendations & Research Path Forward

- Asses cybersecurity risks from an acquisition perspective
- Use insurance for commercially developed systems
- Implement KPIs to monitor cybersecurity progress as a whole and acquisition specific
- Complete cybersecurity knowledge gap research