sibos TORONTO 16 - 19 Oct 2017

SWIFT INSTITUTE

The cyber security ecosystem: Defining a taxonomy of existing, emerging and future cyber threats

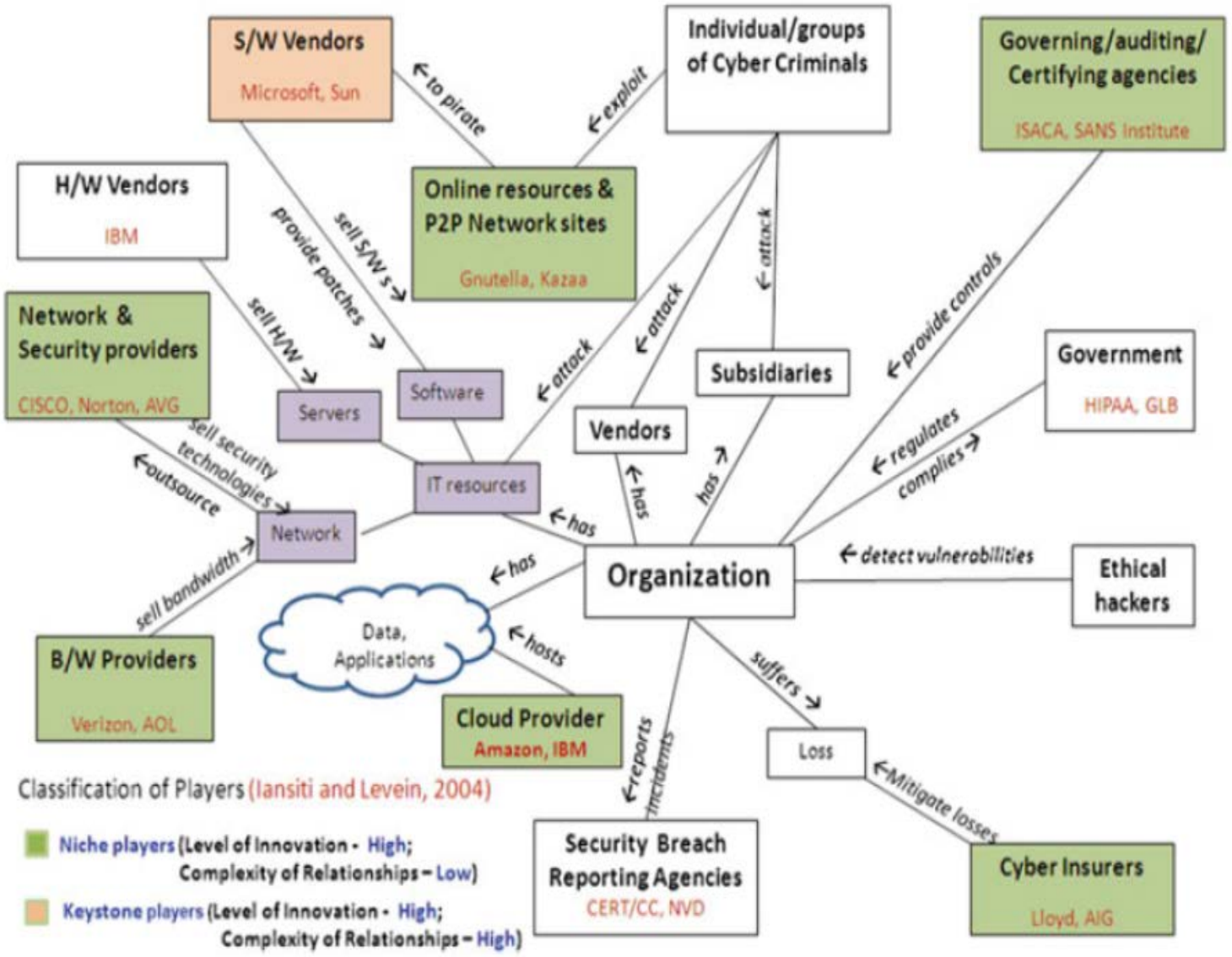
sibos TORONTO
16 - 19 Oct 2017

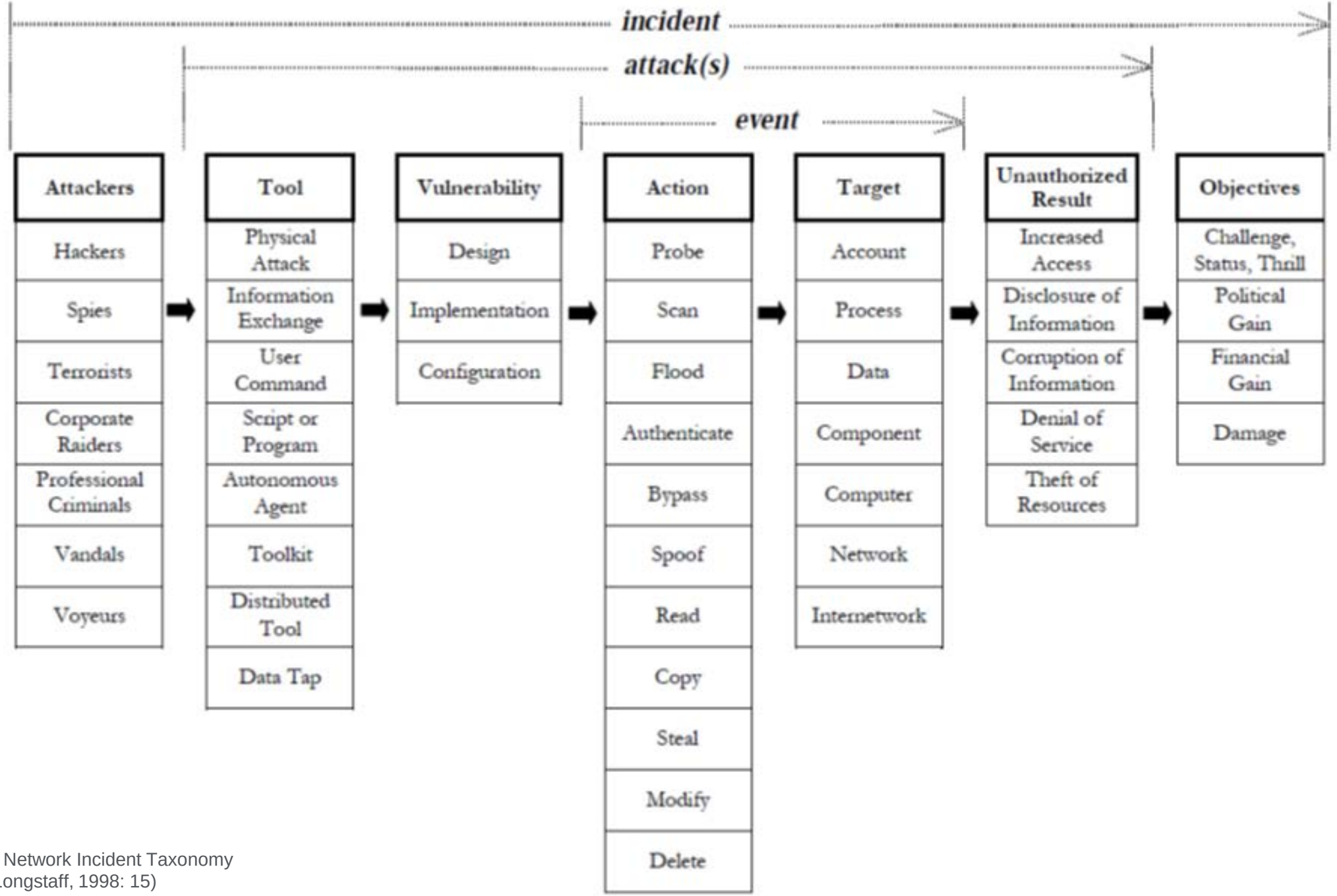
SWIFT INSTITUTE

Jason Ferdinand

Founder
IKSM Ltd

The cyber security ecosystem

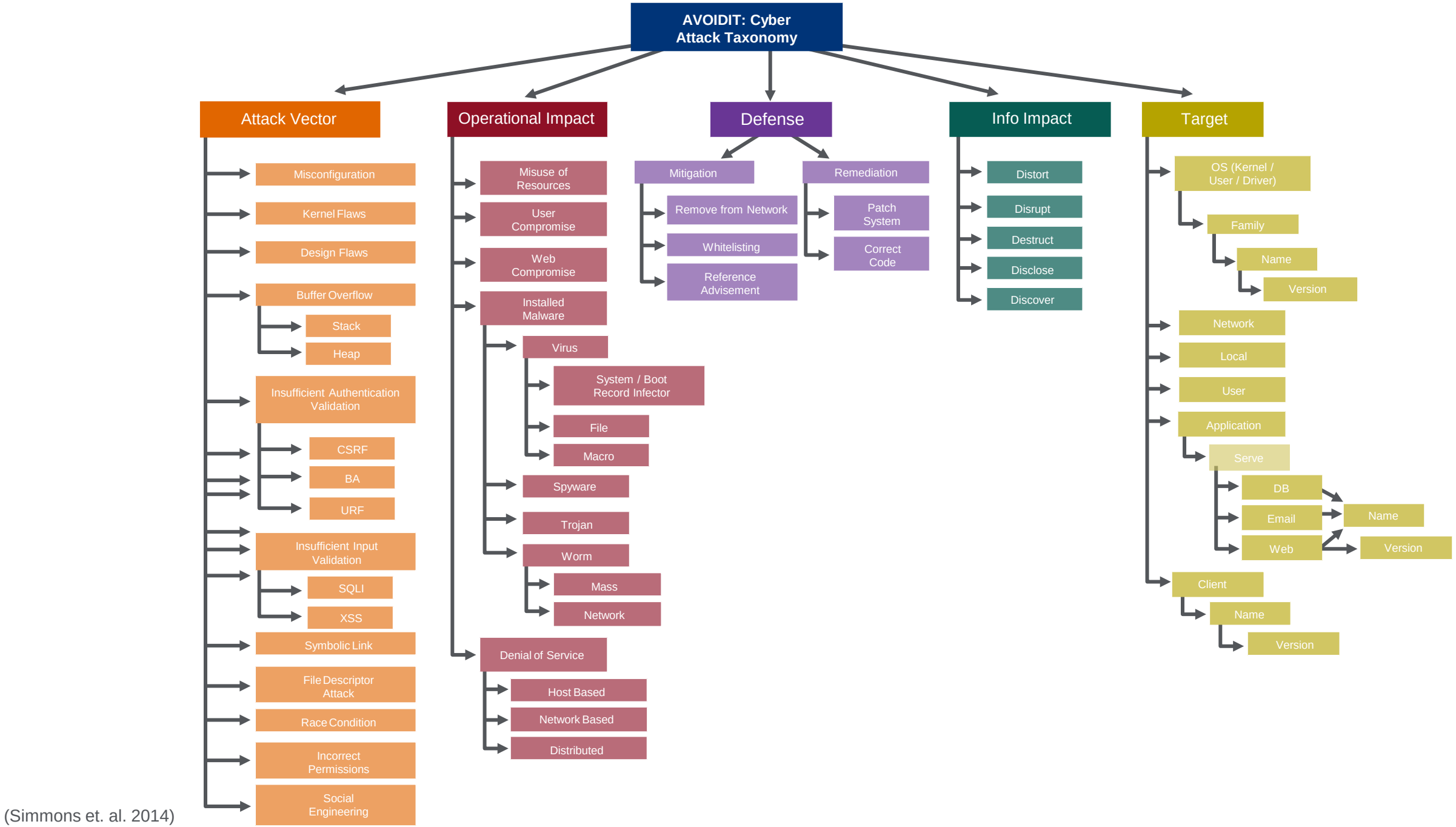




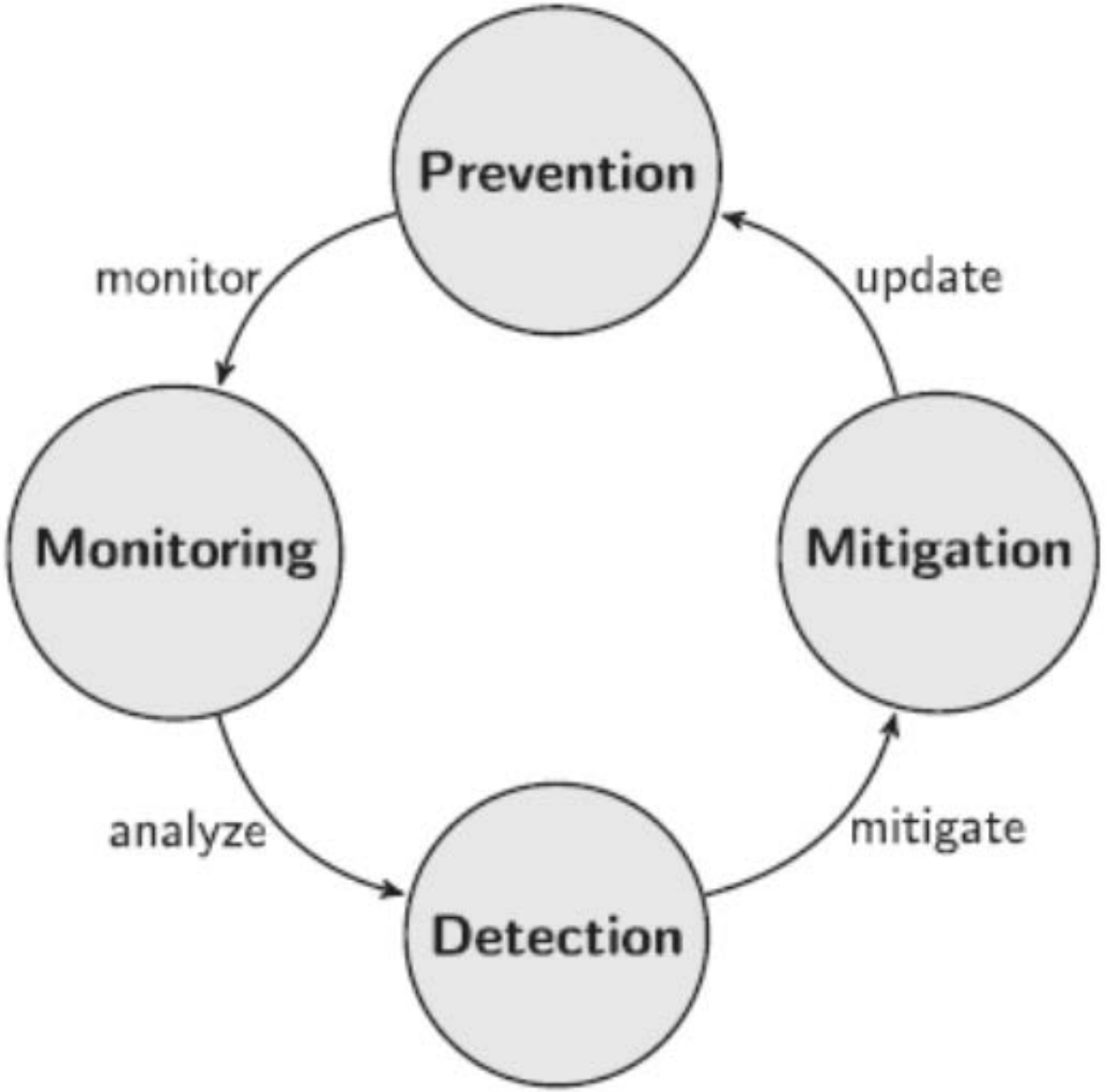
Computer and Network Incident Taxonomy
(Howard and Longstaff, 1998: 15)

New Categories	Old Categories
Script Kiddies	Novice
Cyber-Punks	Cyber-Punks, Virus Writers
Insiders	Internals
Petty thieves	Petty Thieves
Grey Hats	Old Guard Hackers
Professional Criminals	Professional Criminals, Information Warriors
Hacktivists	Political Activists
Nation states	N/A, Information Warriors

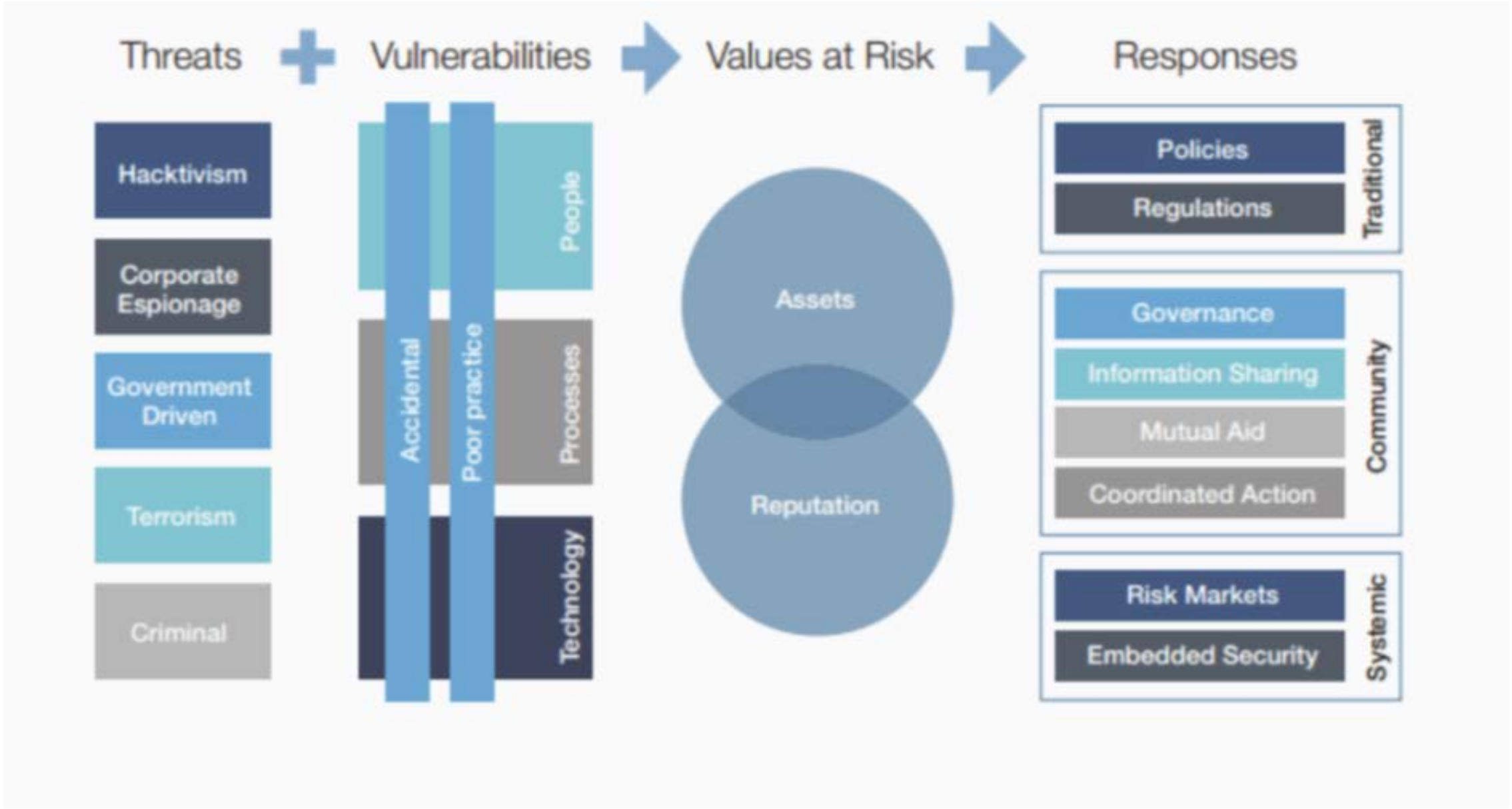
(Hald and Pederson, 2012: 83)



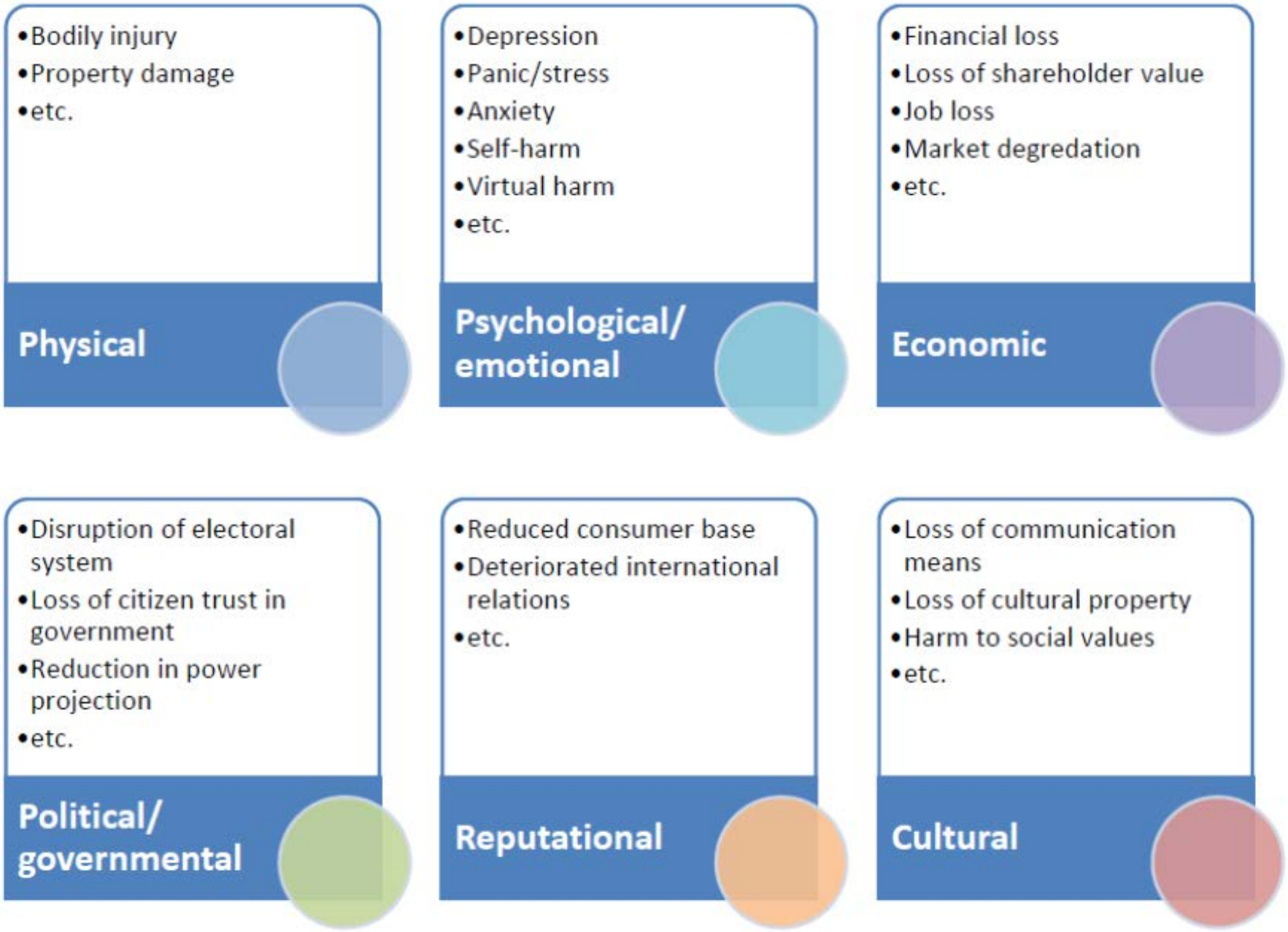
(Simmons et. al. 2014)



(Simmons et. al. 2014)



(Simmons et. al. 2014)



Types and examples of cyber harm
(Agrafiotis et. al., 2016:30)

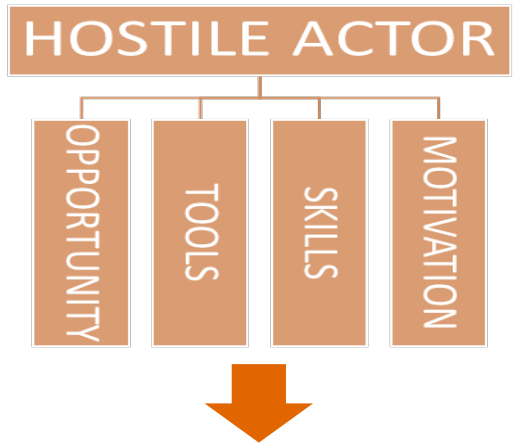
Summary Findings from the Focus Groups (cont.)

- The sample of 67 managers from a range of industries should not be taken as a representative sample, as the number is too small and the selection of participants was somewhat opportunistic. Our findings thus provide a ‘snapshot’ that suggests areas that need detailed further exploration:
- Wanting a more consistent approach to cyber threat to be presented in plain English to avoid confusion
- Respondents demonstrated a surprising lack of knowledge of cyber attacks, monitoring, reporting, and mitigation strategies and practices, which suggests a larger problem in cyber security
- The widespread adoption of cyber security practices themselves has yet to occur, and this proposition is very concerning for cyber security professionals.
- Identifiable bias towards IT and technology in general
- Cyber security as an IT issue

Summary Findings from the Focus Groups (cont.)

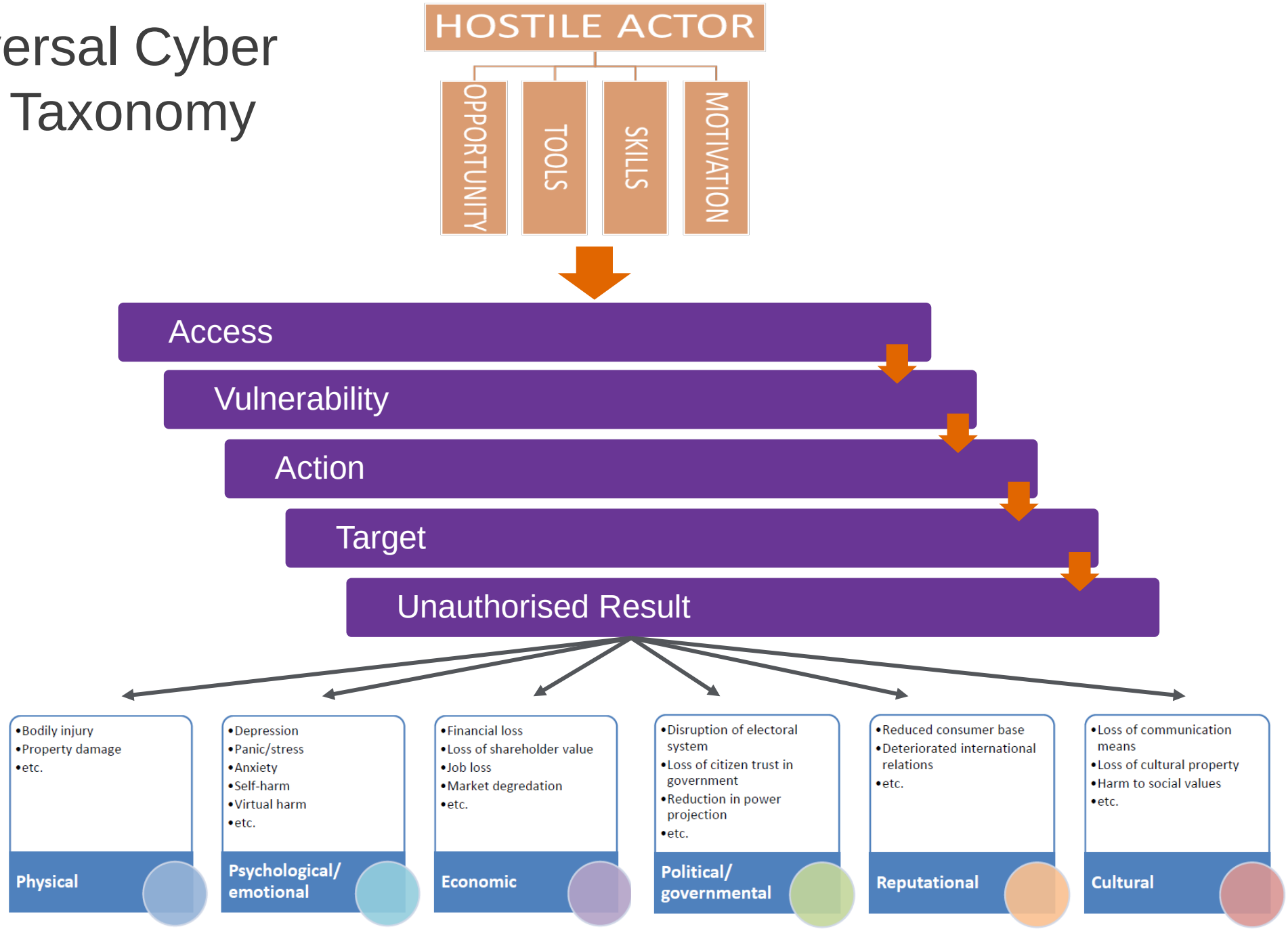
- Acknowledgement of the need to take personal responsibility, in action and communication, but a failure to do so
- Managers lacked knowledge and understanding despite induction courses, and in some cases cyber awareness schemes
- Feeling panic, the ‘awfulness’ of cyber breach, and a total lack of knowledge of what to do and who to report incidents to
- The value of knowledge sharing
- Straightforward and consistent approaches to cyber threats.
- Desire to know more about cyber threats and what they can do about them

A Universal Cyber Threat Taxonomy

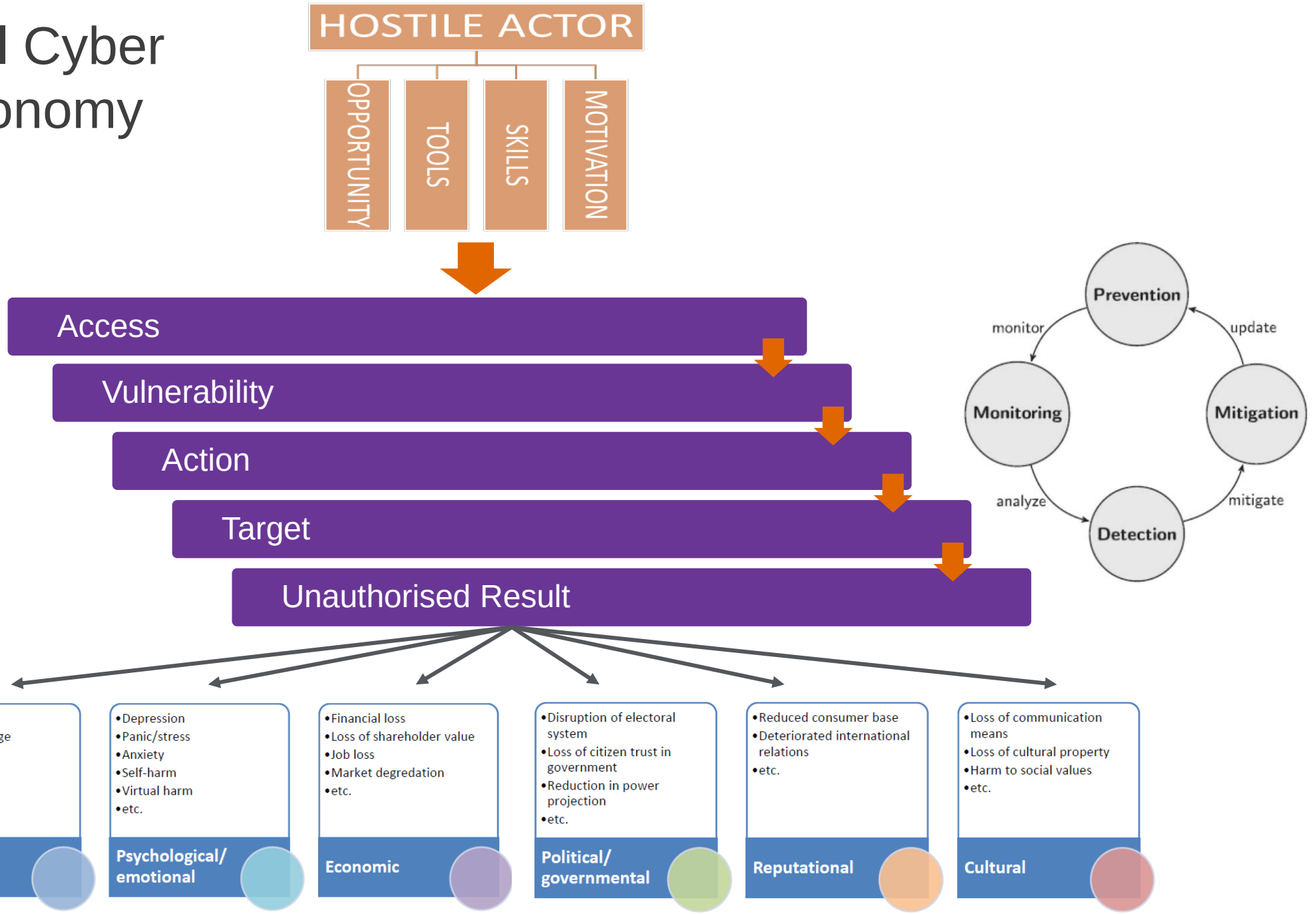


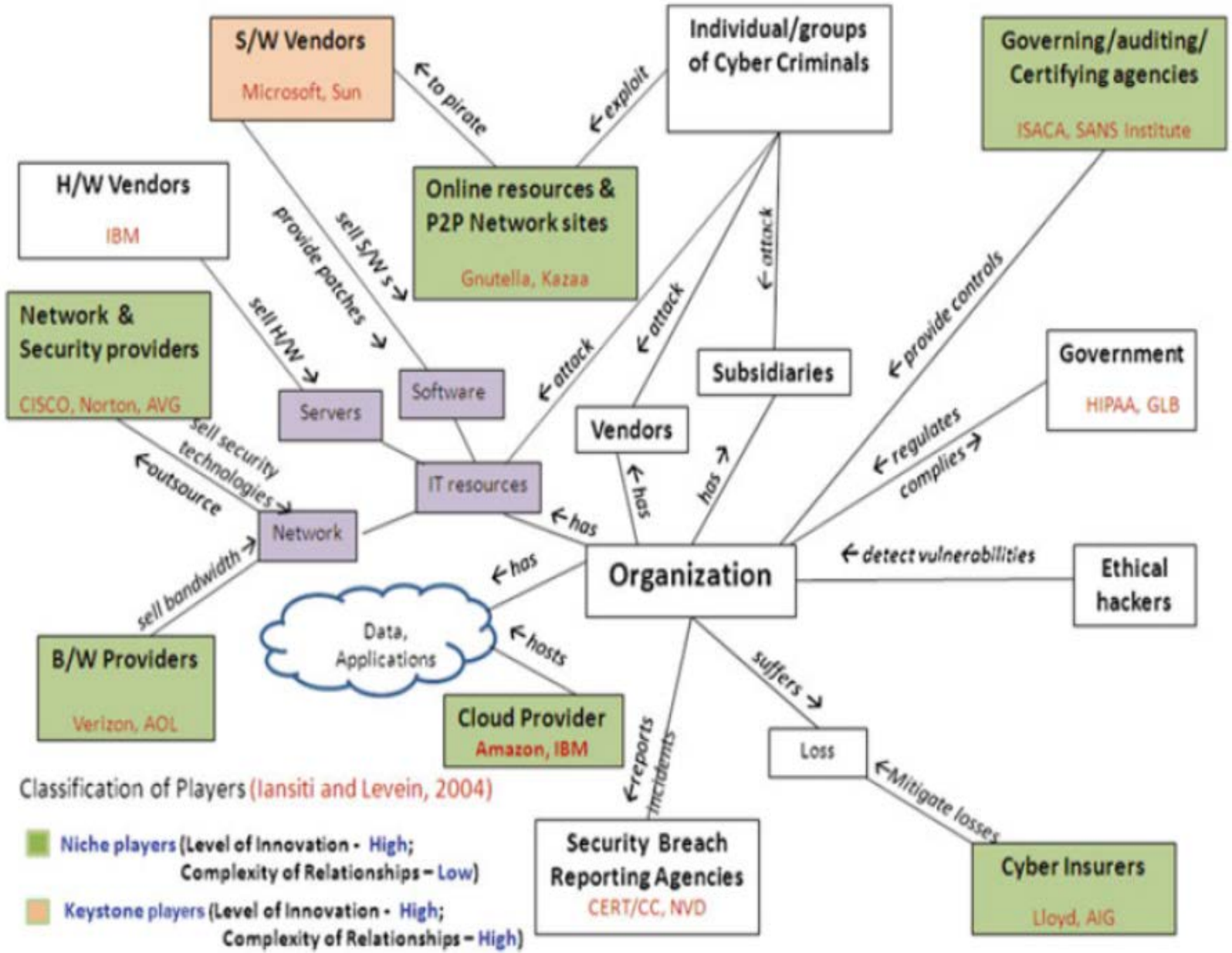
Physical	Psychological/ emotional	Economic	Political/ governmental	Reputational	Cultural
•Bodily injury •Property damage •etc.	•Depression •Panic/stress •Anxiety •Self-harm •Virtual harm •etc.	•Financial loss •Loss of shareholder value •Job loss •Market degredation •etc.	•Disruption of electoral system •Loss of citizen trust in government •Reduction in power projection •etc.	•Reduced consumer base •Deteriorated international relations •etc.	•Loss of communication means •Loss of cultural property •Harm to social values •etc.

A Universal Cyber Attack Taxonomy



A Universal Cyber Attack Taxonomy




S/W Vendors
Microsoft, Sun
to pirate
Individual/groups of Cyber Criminals
exploit
Governing/auditing/ Certifying agencies
ISACA, SANS Institute
H/W Vendors
IBM
Online resources & P2P Network sites
Gnutella, Kazaa
sell S/W s
provide patches
attack
attack
attack
provide controls
sell H/W
Network & Security providers
CISCO, Norton, AVG
Software
Servers
Subsidiaries
Government
HIPAA, GLB
sell security technologies
outsource
IT resources
Vendors
has
has
has
regulates
complies
Network
detect vulnerabilities
Organization
Ethical hackers
sell bandwidth
Data, Applications
hosts
B/W Providers
Verizon, AOL
Cloud Provider
Amazon, IBM
suffers
reports incidents
Loss
Mitigate losses
Security Breach Reporting Agencies
CERT/CC, NVD
Cyber Insurers
Lloyd, AIG
Classification of Players (Iansiti and Levein, 2004)
Niche players (Level of Innovation - High; Complexity of Relationships – Low)
Keystone players (Level of Innovation - High; Complexity of Relationships – High)

Knowledge-based Cyber Resilience Framework

Stage 1: Non-existent Cyber Resilience	Stage 2: Immature Cyber Resilience	Stage 3: Established Basic Cyber Resilience	Stage 4: Reactive Cyber Resilience	Stage 5: Fully Proactive and Reactive Cyber Resilience
Only Generic Capabilities associated with 'business as usual'	Generic capabilities	Generic capabilities	Generic Capabilities	Generic Capabilities
	Ordinary Defensive Capability	Ordinary Defensive Capability	Ordinary Defensive Capability	Ordinary Defensive Capability
		Internal Monitoring Capability	Internal Monitoring Capability	Internal Monitoring Capability
			External Monitoring Capability	External Monitoring Capability
			Extra-Ordinary Capability	Extra-Ordinary Capability
			Reactive Dynamic Capability	Reactive Dynamic Capability
				Proactive Dynamic Capability
				Future Proofing
				'Hacking Back'

Advice and Guidance

Access

- At the ‘Access’ step an organisation has to determine whether physical access and/or virtual access is possible to hostile actors
- This means reviewing the physical security measures in place to assess whether physical access can be obtained
- This will include policies and practices associated with security card limited access to sensitive areas, the use of USB devices, zip drives, the use of own devices whilst at work, and subcontracting arrangements
- In terms of virtual access the organisation should review policies and procedures in relation to their supply chain and information sharing, password protection, whitelisting, and authentication

Vulnerability

At the ‘Vulnerabilities’ step the organisation should seek to limit the vulnerabilities by considering the design, implementation and configuration of hard and soft systems, including IDS

Action

At the ‘Action’ step each of the alternatives should be examined in order to assess what limits and controls can be put in place to stop each of these actions

Target

At the ‘Target’ step the organisation should seek to reduce the potential availability of targets for a hostile actor.

The possibilities here are numerous, and should be tailored to the specific characteristics of the organisation in question

Unauthorised Results

If appropriate defensive measures are in place these results will be avoided and cyber harm should not occur

- The new Cyber Threat Taxonomy, Cyberattack Taxonomy, and Knowledge-based Cyber Resilience Framework presented here provide the foundational models for a common language in cyber security
- Managers can use these models to assess their own stage of development, the options available within the cyber security ecosystem, and thus make more informed decisions as to resource deployment and procurement to build cyber resilience
- It also allows a manager to review the organisation's cyber resilience in relation to the NIST IT Security Maturity Model in a more nuanced way by locating the policies, procedures, implementation, testing and integration levels of the NIST model within, and across, each of the five stages of the Cyber Resilience Framework
- This encourages a holistic understanding of cyber resilience that incorporates IT security, as the framework presented includes response by an organisation, through incorporating EOCs triggered when security controls have been proved to be ineffective
- Adopting these models across industries would enhance our understanding of cyber security and enable managers to improve communication, coordination, governance, and recovery when managing cyber security

Questions

sibos TORONTO 16 - 19 Oct 2017

SWIFT INSTITUTE

Research paper can be downloaded from:

www.swiftinstitute.org