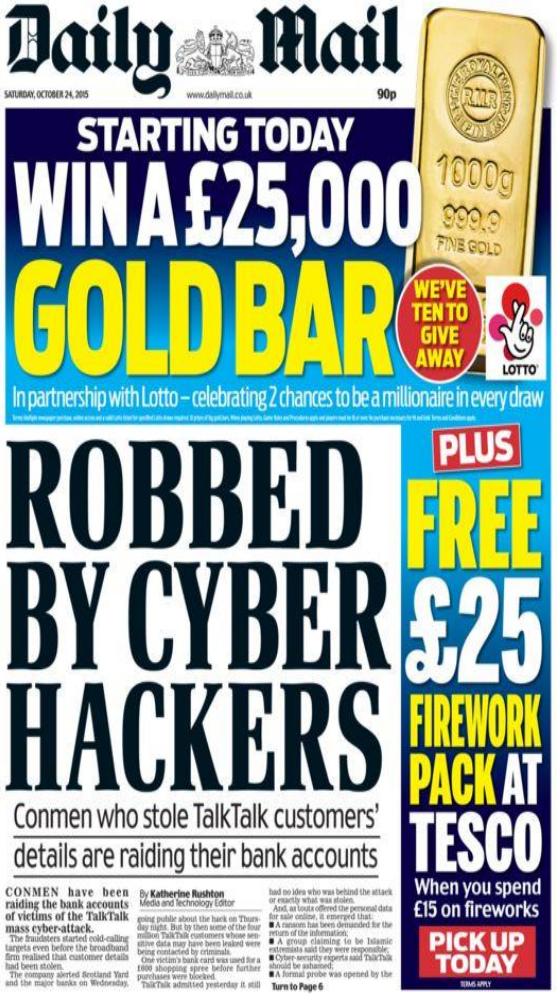
Welcome

The National Cyber Management Centre®

Dr Jason Ferdinand

Prof Richard Benham



Agenda

The National Cyber Management Centre®

Corporate Customers – your weakest digital link?

The content presented in this research presentation is solely the views of the authors and do not represent those of the SWIFT Institute or SWIFT

Agenda

The National Cyber Management Centre®

The Institute of Director Cyber survey 2017

Benham

Our research and findings

Ferdinand

What does this mean for banks?

Benham

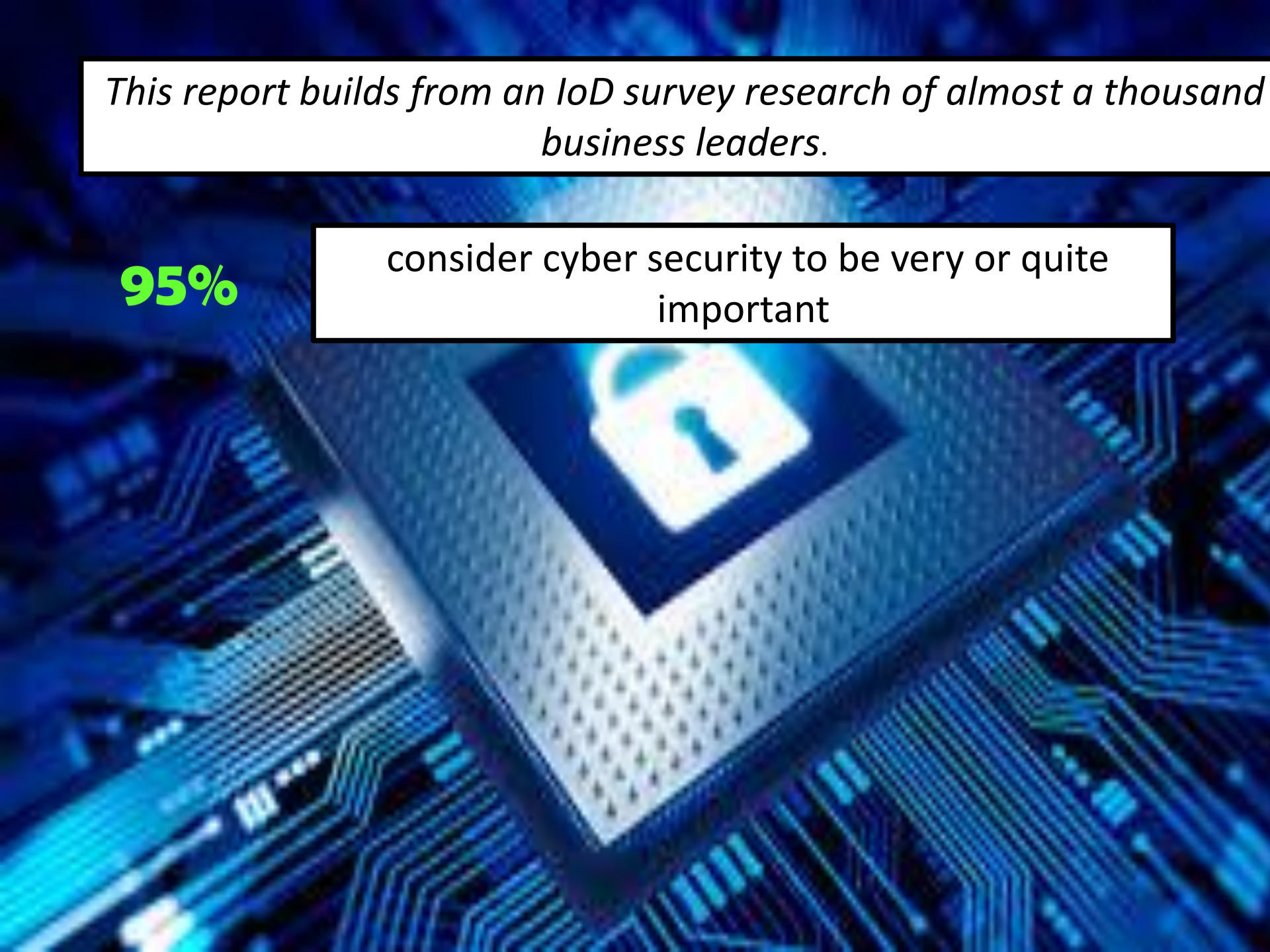
Open questions and answers

Ferdinand/Benham

This report builds from an IoD survey research of almost a thousand business leaders.

95%

consider cyber security to be very or quite important



This report builds from an IoD survey research of almost a thousand business leaders.

95% consider cyber security to be very or quite important

45% do not have a formal cyber security strategy

This report builds from an IoD survey research of almost a thousand business leaders.

95% consider cyber security to be very or quite important

45% do not have a formal cyber security strategy

40% do not who to contact or report an incident to if attacked

This report builds from an IoD survey research of almost a thousand business leaders.

95%	consider cyber security to be very or quite important
45%	do not have a formal cyber security strategy
40%	do not who to contact or report an incident to if attacked
27%	have no process to check the legitimacy of invoices

Further support from Government

A check list for business

Prepare for GDPR – understand what it means for your business and how you can prepare.

Ensure your **directors and board members** are trained on the business risks of cyber security.

Run an **attack simulation** with senior management to ensure your processes are suitably robust in the case of an attack.

Ensure all your staff have **regular cyber awareness training**, building it into induction processes and ensure your people are a robust and secure first line of defence.

Regularly **scrutinise** your cloud and server suppliers to ensure their processes are up to date.

Investigate whether you need cyber insurance, and whether it is already covered by any IT disruption policy.

Incentivise employees to spot false invoices or emails, and encourage honesty when human error has been made

Further support from Government

Clearer Guidance on GDPR

A check list for business

Prepare for GDPR – understand what it means for your business and how you can prepare.

Ensure your **directors and board members** are trained on the business risks of cyber security.

Run an **attack simulation** with senior management to ensure your processes are suitably robust in the case of an attack.

Ensure all your staff have **regular cyber awareness training**, building it into induction processes and ensure your people are a robust and secure first line of defence.

Regularly **scrutinise** your cloud and server suppliers to ensure their processes are up to date.

Investigate whether you need cyber insurance, and whether it is already covered by any IT disruption policy.

Incentivise employees to spot false invoices or emails, and encourage honesty when human error has been made

A check list for business

Prepare for GDPR – understand what it means for your business and how you can prepare.

Ensure your **directors and board members** are trained on the business risks of cyber security.

Run an **attack simulation** with senior management to ensure your processes are suitably robust in the case of an attack.

Ensure all your staff have **regular cyber awareness training**, building it into induction processes and ensure your people are a robust and secure first line of defence.

Regularly **scrutinise** your cloud and server suppliers to ensure their processes are up to date.

Investigate whether you need cyber insurance, and whether it is already covered by any IT disruption policy.

Incentivise employees to spot false invoices or emails, and encourage honesty when human error has been made

Further support from Government

Clearer Guidance on GDPR

Encourage Directors to treat Cyber as a Busir Risk

A check list for business

Prepare for GDPR – understand what it means for your business and how you can prepare.

Ensure your **directors and board members** are trained on the business risks of cyber security.

Run an **attack simulation** with senior management to ensure your processes are suitably robust in the case of an attack.

Ensure all your staff have **regular cyber awareness training**, building it into induction processes and ensure your people are a robust and secure first line of defence.

Regularly **scrutinise** your cloud and server suppliers to ensure their processes are up to date.

Investigate whether you need cyber insurance, and whether it is already covered by any IT disruption policy.

Incentivise employees to spot false invoices or emails, and encourage honesty when human error has been made

Further support from Government

Clearer Guidance on GDPR

Encourage Directors to treat Cyber as a Busir Risk

Incentives e.g tax relief on Insurance and Awareness Training

Our research and findings

The National Cyber Management Centre®

Sli.do

The National Cyber Management Centre®

Who do you think is responsible for education your corporate customers on digital safety?

A. Governments
B. Non profit forums
C. Banks
D. No one

Our research and findings

The National Cyber Management Centre®

"We are conducting research on cyber threats to create a taxonomy of threats, and responses to attacks, that we hope will become the industry standard for banking and finance.

All responses will be recorded for analysis so please state if you want anything kept 'off the record'.

The questions will fall into three interconnected subjects – cyber threat taxonomy, cyber threat and lastly responses to threats and attacks"

Our thanks to…

The National Cyber Management Centre®

Insurance

Manufacturing

IT Providers

Law Enforcement

Schools

Retail

Our research base

The National Cyber Management Centre®

Sector	Specific	Number of People
Public	Policing	5
	Local Government	1
	National Government (MP)	1
Charity	Various	3
Financial Services	Banking	5
	Insurance	2
	Brokers	3
IT	Web Services	7
	Cyber and IS	10
	Data Management	2
Schools	Private	1
	State	1
Engineering	National Infrastructure	2
	Manufacturing	2
Utilities	Electricity	2
	Water	5
	Gas	1
Sports Clubs	Premier League	10
	Rugby	2
	Tennis	1
Entertainment	Media	1
Marketing and Comms	Various	3
Retail	Clothing	1
	Electrical	1
Training	Technical	1
TOTAL		67

Our research

The National Cyber Management Centre®

“Do you know about or use any cyber threat taxonomy?”

Sample Responses

“Yes we use classification to help us identify what may attack us”

“We don’t understand what the threats are”

Observations

Once probed many felt they use cyber threat taxonomy instinctively. For example the threats they felt at home were different to those at work. Personal banking was seen as requiring more care as it was a personal responsibility.

Our research

The National Cyber Management Centre®

Analysis

- 70% felt they behaved differently to the types of cyber threats
- 84% said they didn't classify cyber threats consciously
- 100% agreed more publicity was needed for businesses and citizens
- 100% said that human error was a key factor particularly on emails.

Conclusion

There is a human instinctiveness in understanding that a cyber threat can be at work or home, on-line or on the phone and that different ways of dealing with them are needed. Generally it is felt no one (providers / Government etc) has classified these

Our research

The National Cyber Management Centre®

What cyber threats are you aware of?

Sample Responses

“ransomware”

“My staff who do silly things”

“Viruses and bugs”

“Dodgy emails asking for money”

Observations

An overall awareness that the threat is real however most still thought it an IT problem. They perceived there were fewer issues at home and less risk although they weren’t sure why.

Our research

The National Cyber Management Centre®

Analysis

- 100% knew of the threat of Viruses and suspicious emails
- 12% understood phishing but only 2% knew what Vishing was
- 50% confirmed they hoped it would happen to them
- 100% recognised people were a weak link

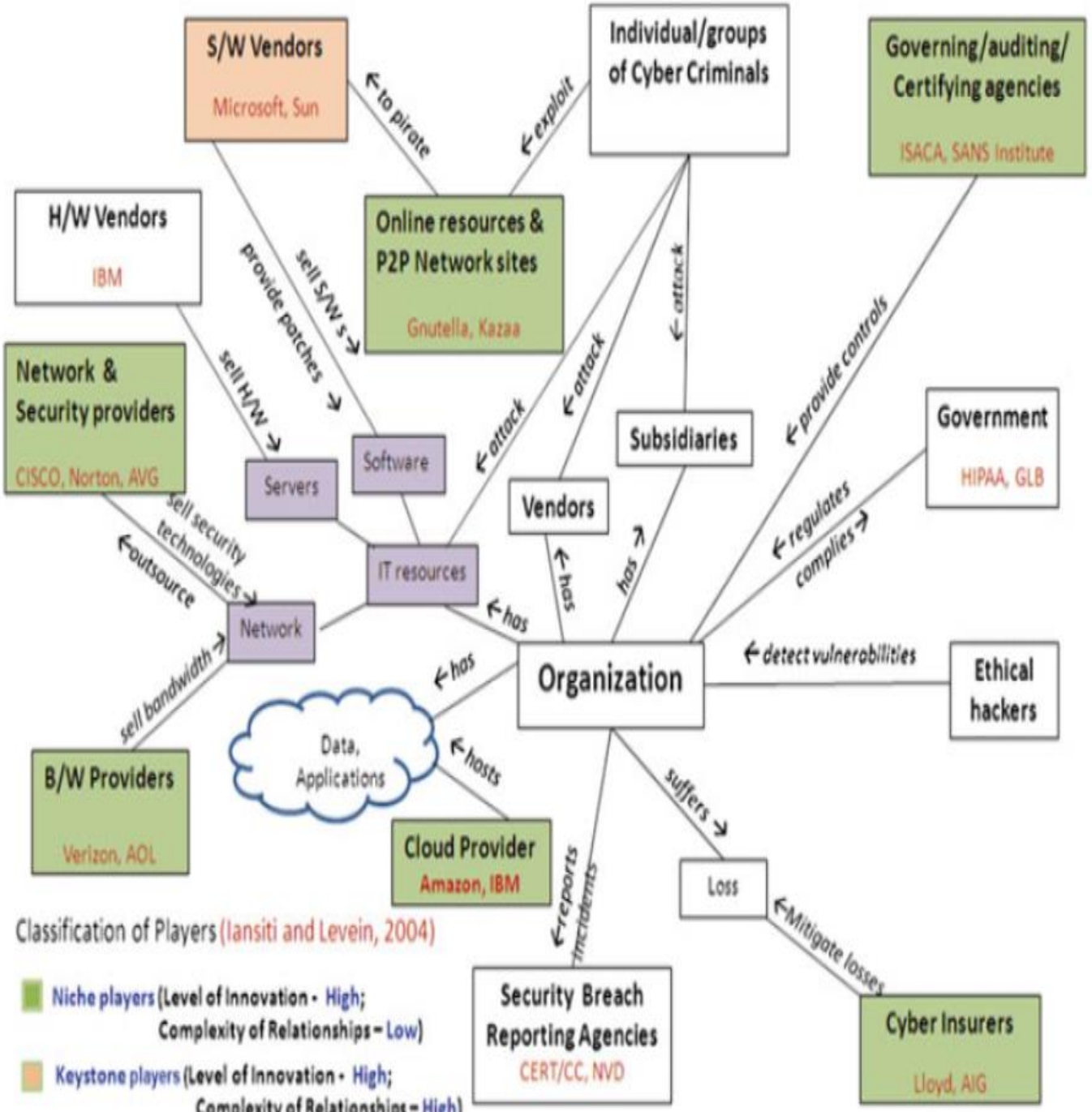
Conclusion

At the highest level everyone knew of cyber threats and examples. Beyond this there was a “head in the sand” mentality which is surprising. This is felt to be down to a lack of understanding of what cyber threats actually are and how to deal with them.

Agenda

The National Cyber Management Centre®

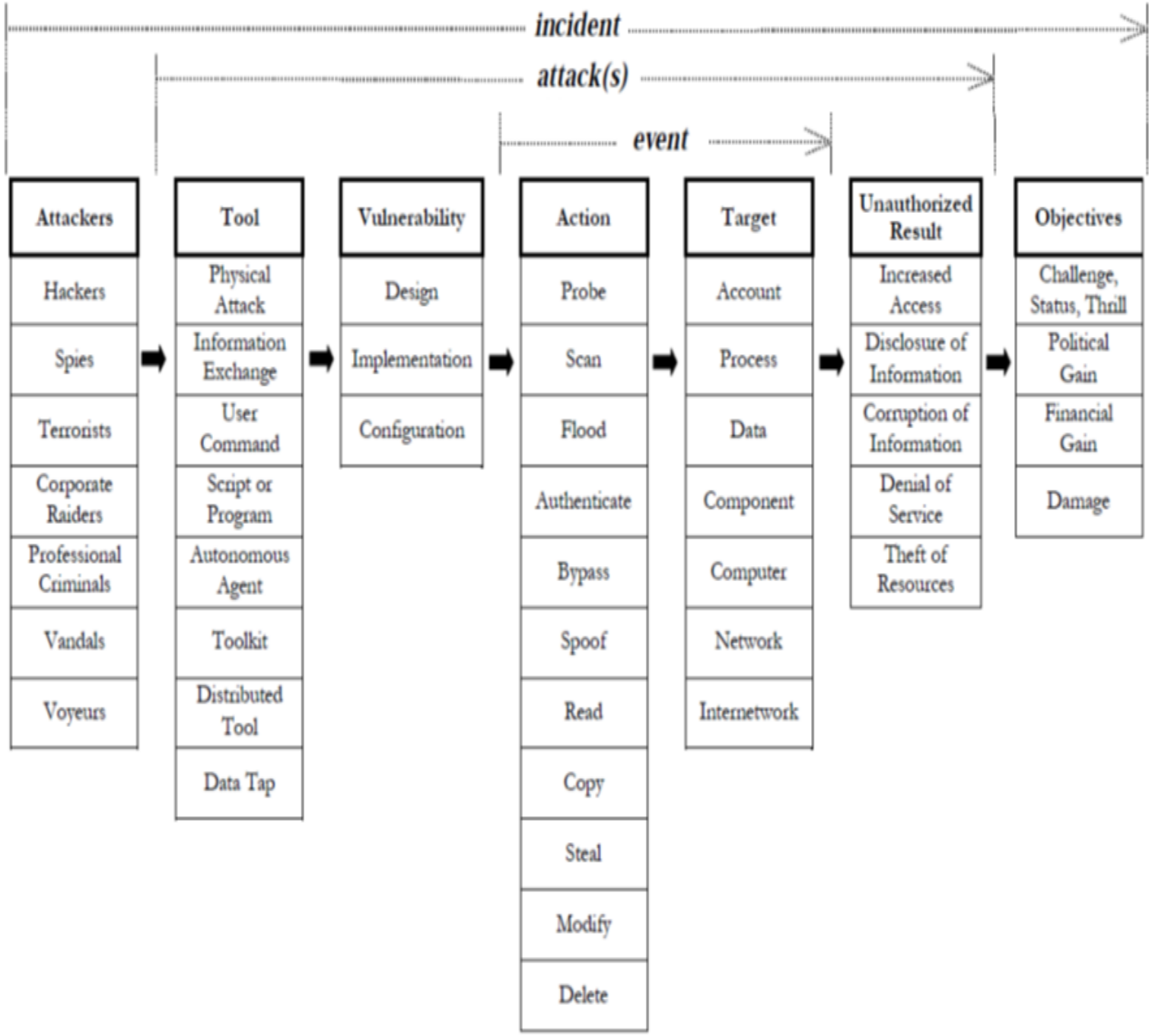
How Organisations Can Develop Cyber Resilience Capabilities



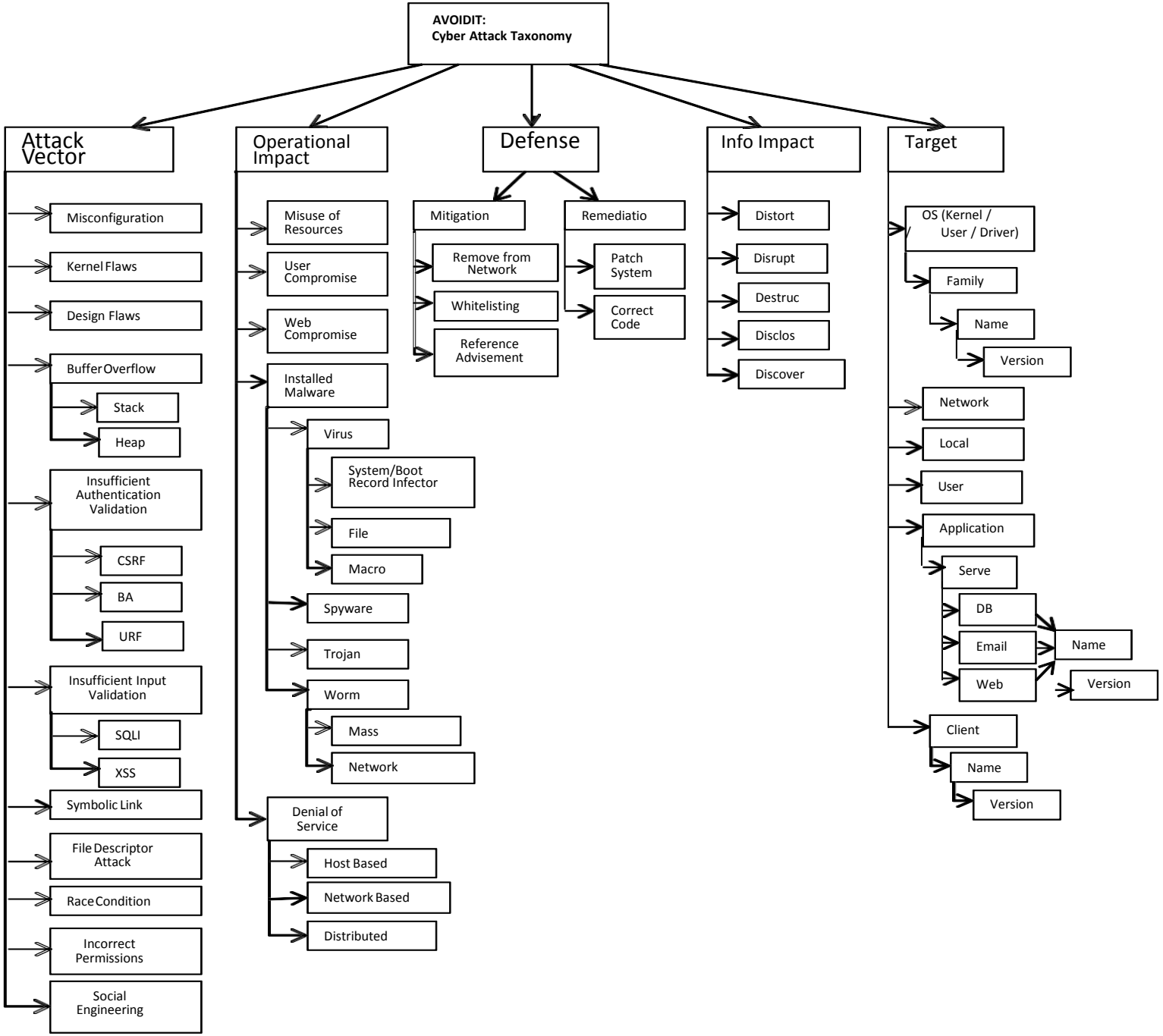
Classification of Players (Iansiti and Levein, 2004)

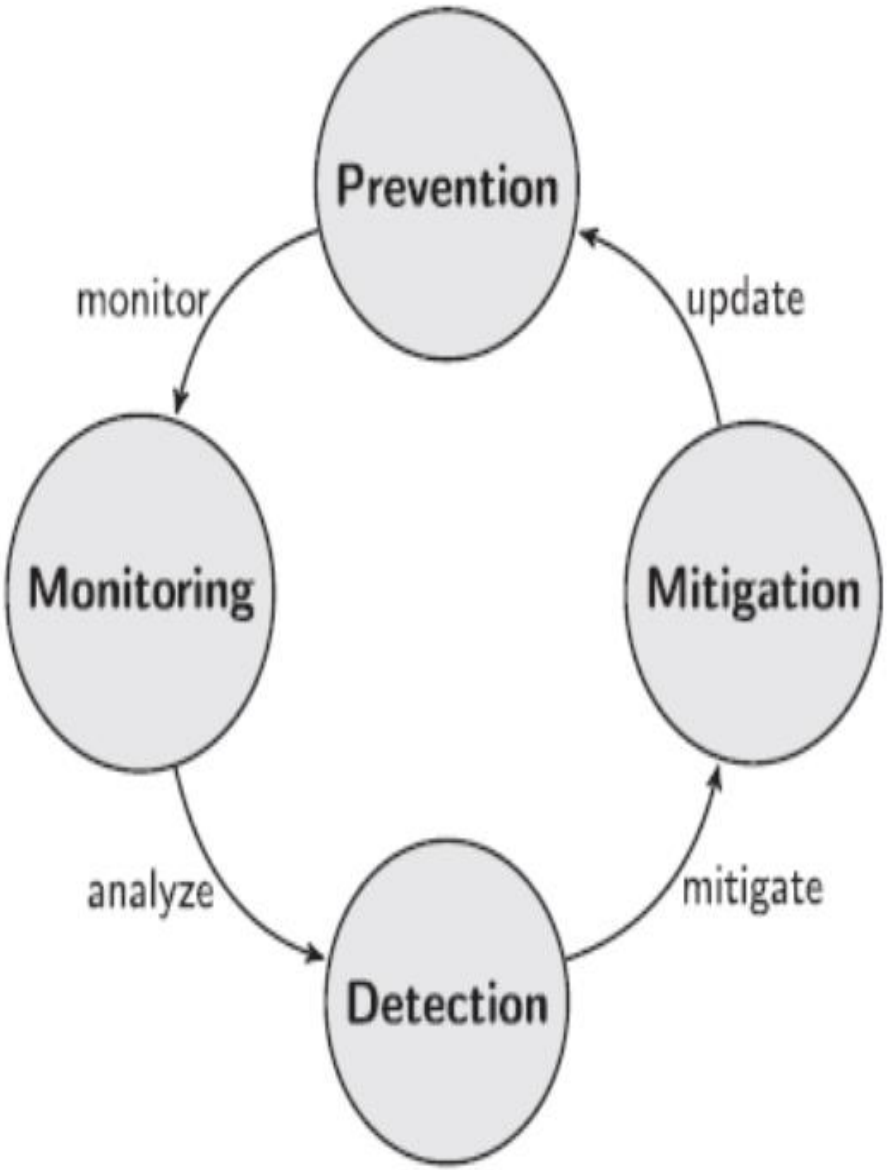
Niche players (Level of Innovation - High; Complexity of Relationships - Low)

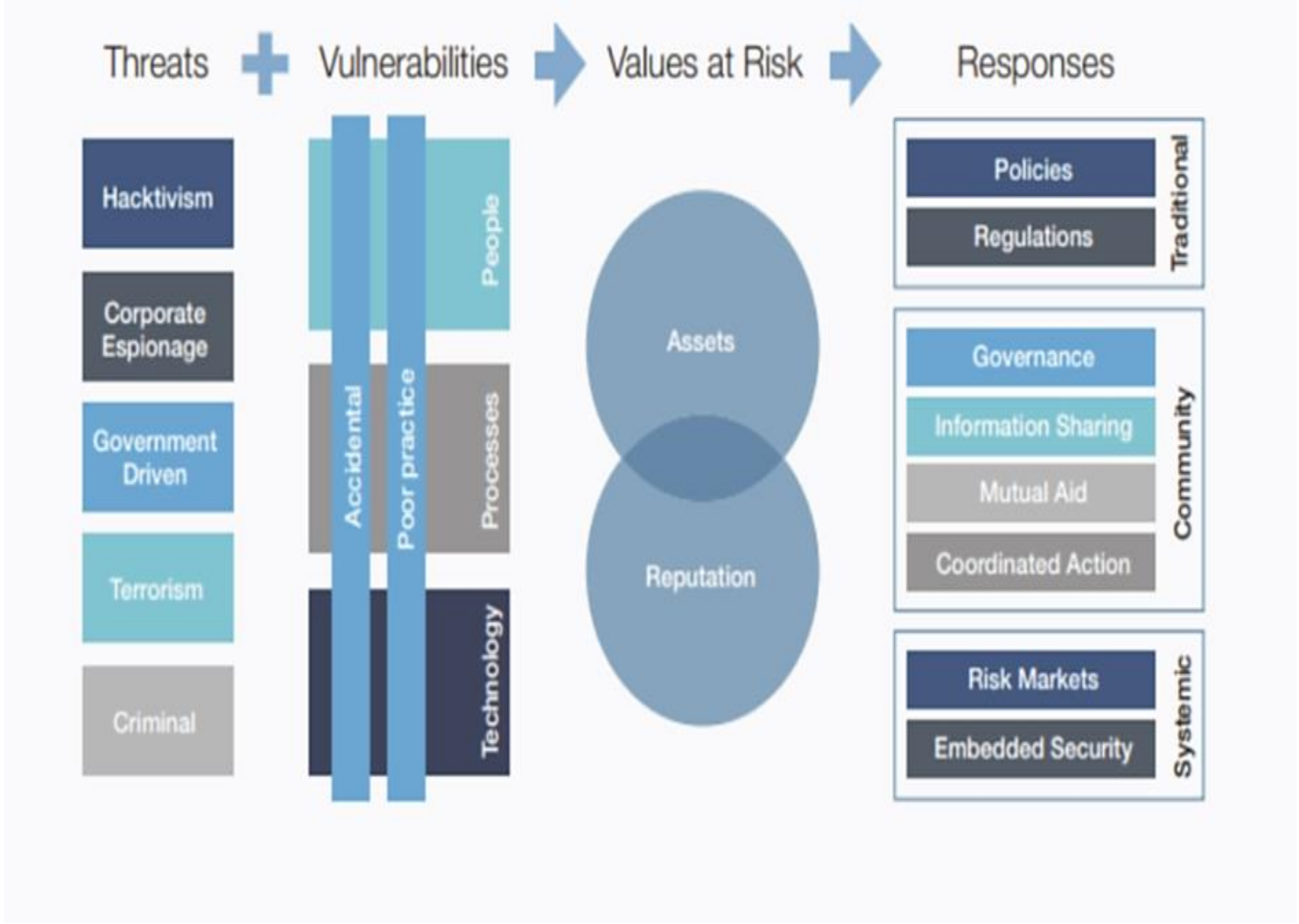
Keystone players (Level of Innovation - High; Complexity of Relationships - High)

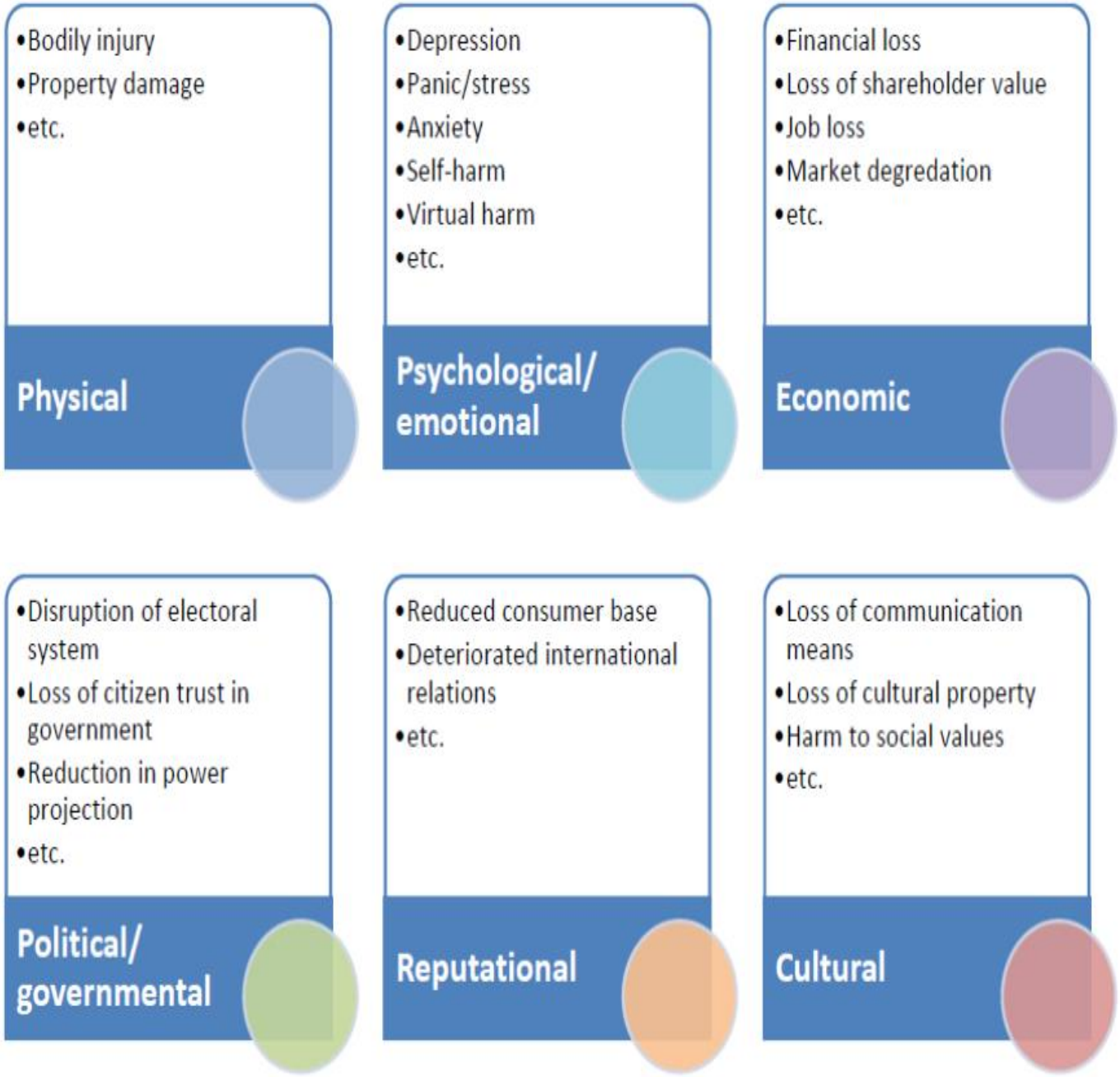

incident
attack(s)
event
Attackers
Hackers
Spies
Terrorists
Corporate Raiders
Professional Criminals
Vandals
Voyeurs
Tool
Physical Attack
Information Exchange
User Command
Script or Program
Autonomous Agent
Toolkit
Distributed Tool
Data Tap
Vulnerability
Design
Implementation
Configuration
Action
Probe
Scan
Flood
Authenticate
Bypass
Spoof
Read
Copy
Steal
Modify
Delete
Target
Account
Process
Data
Component
Computer
Network
Internetwork
Unauthorized Result
Increased Access
Disclosure of Information
Corruption of Information
Denial of Service
Theft of Resources
Objectives
Challenge, Status, Thrill
Political Gain
Financial Gain
Damage

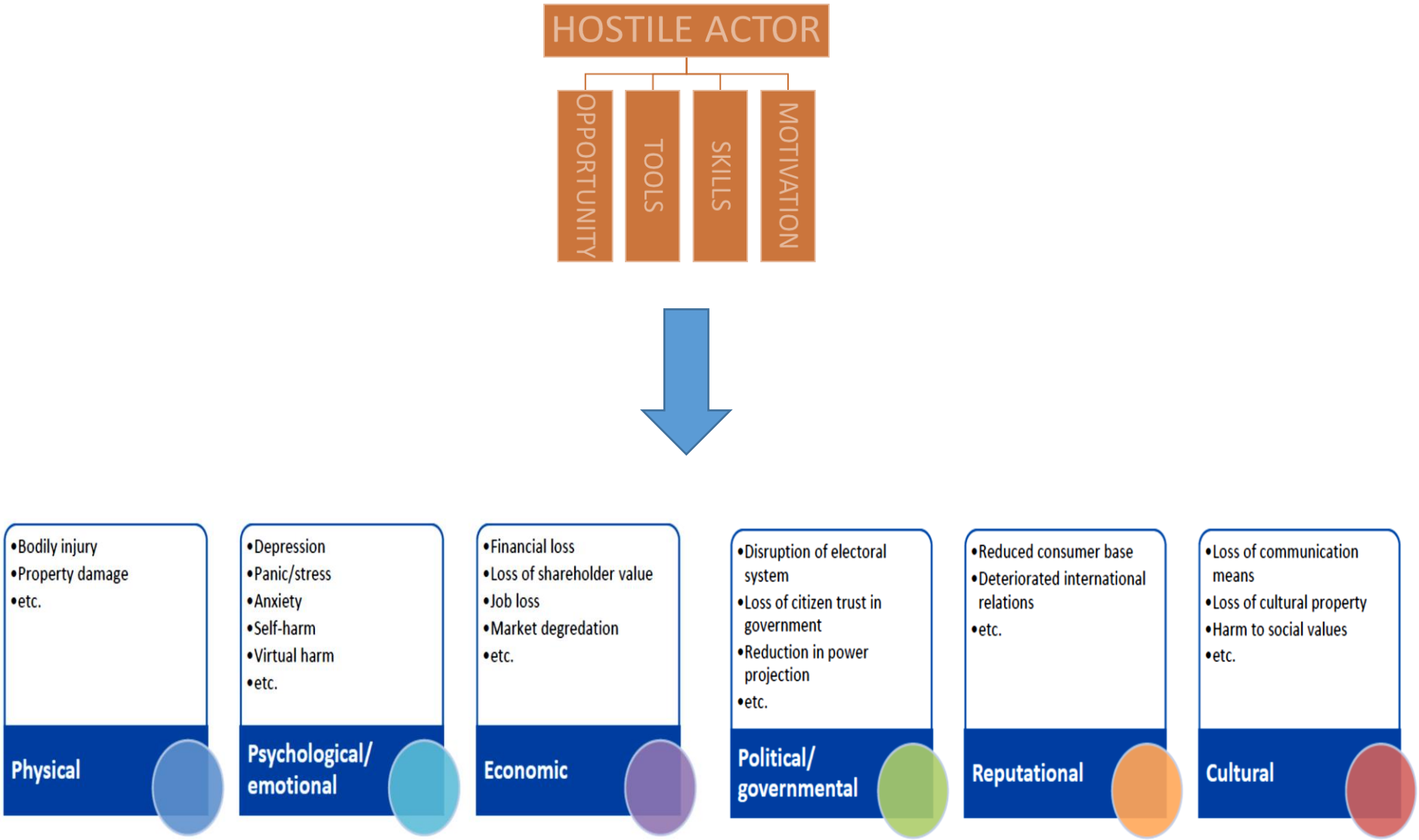
New Categories	Old Categories
Script Kiddies	Novice
Cyber-Punks	Cyber-Punks, Virus Writers
Insiders	Internals
Petty thieves	Petty Thieves
Grey Hats	Old Guard Hackers
Professional Criminals	Professional Criminals, Information Warriors
Hacktivists	Political Activists
Nation states	N/A, Information Warriors

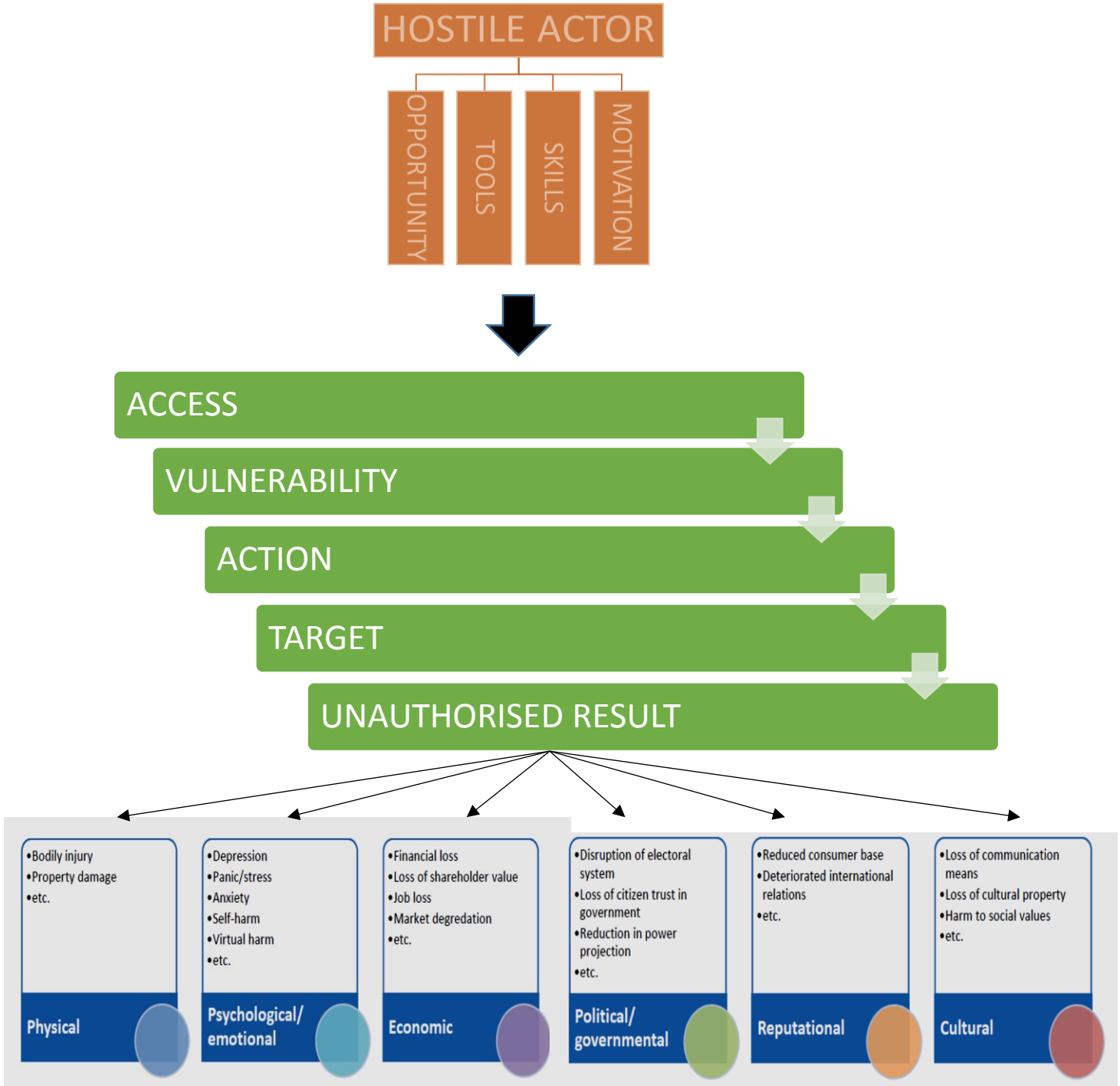

AVOIDIT:
Cyber Attack Taxonomy
Attack Vector
Misconfiguration
Kernel Flaws
Design Flaws
Buffer Overflow
Stack
Heap
Insufficient Authentication Validation
CSRF
BA
URF
Insufficient Input Validation
SQLI
XSS
Symbolic Link
File Descriptor Attack
Race Condition
Incorrect Permissions
Social Engineering
Operational Impact
Misuse of Resources
User Compromise
Web Compromise
Installed Malware
Virus
System/Boot Record Infector
File
Macro
Spyware
Trojan
Worm
Mass
Network
Denial of Service
Host Based
Network Based
Distributed
Defense
Mitigation
Remove from Network
Whitelisting
Reference Advisement
Remediatio
Patch System
Correct Code
Info Impact
Distort
Disrupt
Destruc
Disclos
Discover
Target
OS (Kernel / User / Driver)
Family
Name
Version
Network
Local
User
Application
Serve
DB
Email
Web
Name
Version
Client
Name
Version

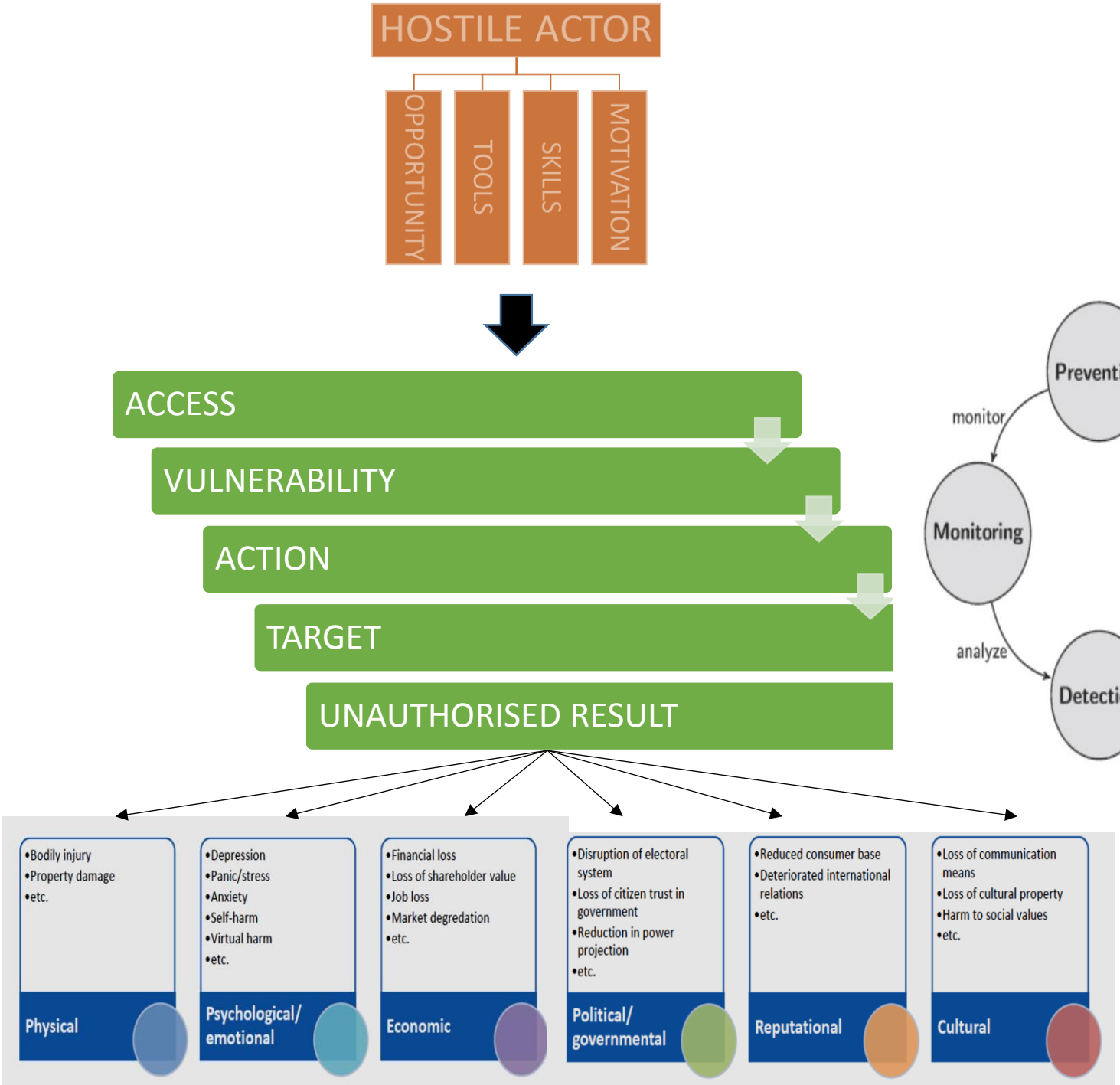

Prevention
monitor
update
Monitoring
Mitigation
analyze
mitigate
Detection

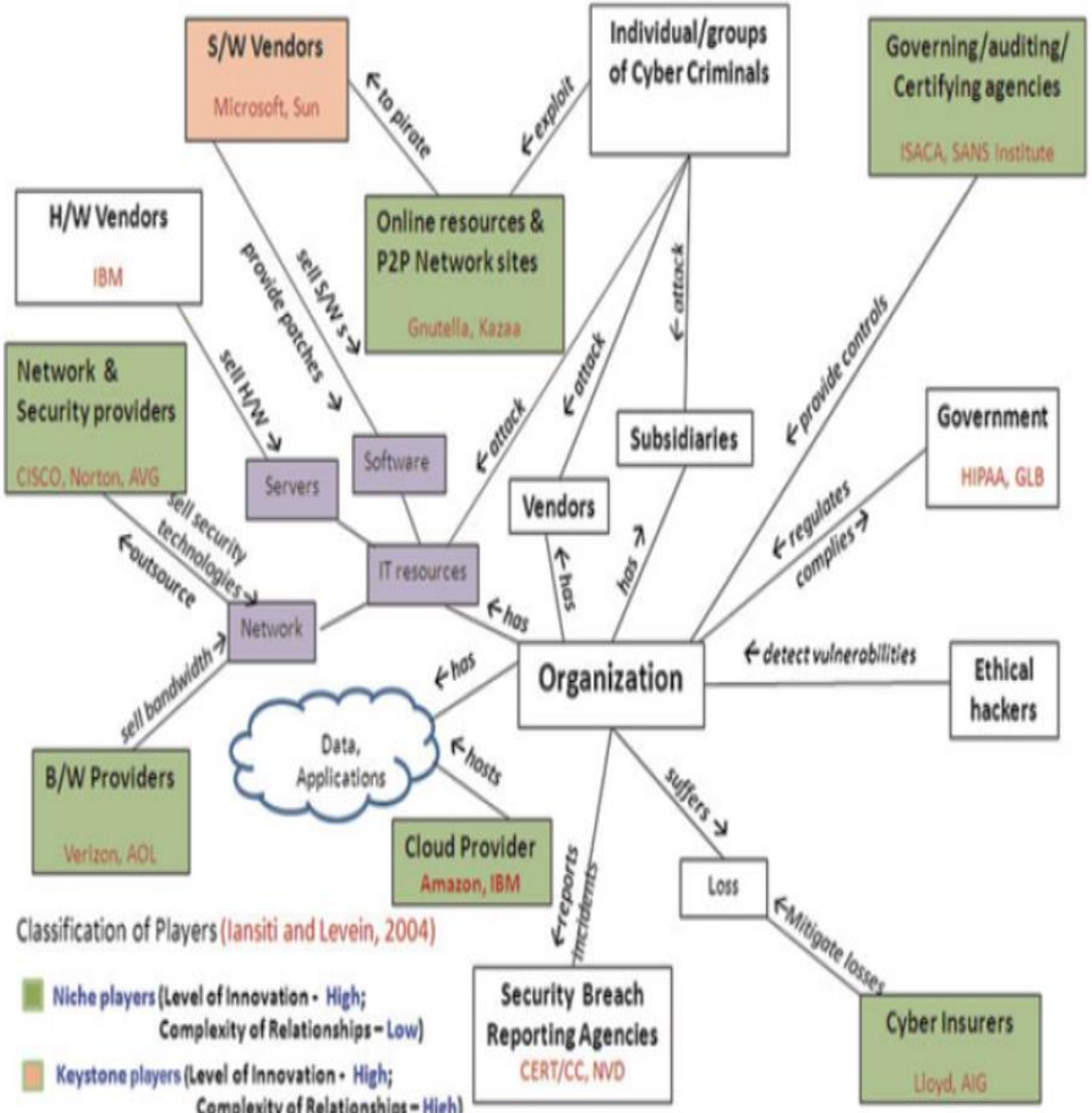

Threats
Vulnerabilities
Values at Risk
Responses
Hacktivism
Corporate Espionage
Government Driven
Terrorism
Criminal
People
Processes
Technology
Accidental
Poor practice
Assets
Reputation
Policies
Regulations
Traditional
Governance
Information Sharing
Mutual Aid
Coordinated Action
Community
Risk Markets
Embedded Security
Systemic


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


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


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


HOSTILE ACTOR
OPPORTUNITY
TOOLS
SKILLS
MOTIVATION
ACCESS
VULNERABILITY
ACTION
TARGET
UNAUTHORISED RESULT
Prevention
monitor
update
Monitoring
Mitigation
analyze
mitigate
Detection
•Bodily injury
•Property damage
•etc.
Physical
•Depression
•Panic/stress
•Anxiety
•Self-harm
•Virtual harm
•etc.
Psychological/ emotional
•Financial loss
•Loss of shareholder value
•Job loss
•Market degredation
•etc.
Economic
•Disruption of electoral system
•Loss of citizen trust in government
•Reduction in power projection
•etc.
Political/ governmental
•Reduced consumer base
•Deteriorated international relations
•etc.
Reputational
•Loss of communication means
•Loss of cultural property
•Harm to social values
•etc.
Cultural



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)

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'

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.

Endsleigh has been part of the Zurich Group since 2008 and is the UK's largest insurer in the student market. Contributor was a Senior IT Officer responsible for Cyber Security.

A British engineering and manufacturer operating across all major global markets through a network of key distributors for Tungum Tubing. Finance Director contributed.

Family run web building and hosting firm with the Chief Executive and an apprentice contributing.

Gloucestershire Safer Cyber Forum is a partnership between Gloucestershire Police, local business and its citizens. Regional Co-ordinator contributed.

Dean Close School is an Independent School based in Cheltenham with over 1000 pupils. Contributor was Director of Operations.

Severnside Software Ltd. (SSL) have been providing IT solutions to businesses for over 26 years. Their clients are all over the world including Spain, Portugal, Holland, USA, Colombia and Germany. CEO contributed.

What does this mean for banks?

The National Cyber Management Centre®

Who do you think is responsible for educating your corporate customers on digital safety?

A. Governments
B. Non profit forums
C. Banks
D. No one

What does this mean for banks?

The National Cyber Management Centre®

Who do you think is responsible for educating your corporate customers on digital safety?

A. Governments
B. Non profit forums
C. Banks
D. No one

What does this mean for banks?

The National Cyber Management Centre®

Who do you think is responsible for educating your corporate customers on digital safety?

A. Governments ✓
B. Non profit forums
C. Banks ✓
D. No one

What does this mean for banks?

The National Cyber Management Centre®

Who do you think is responsible for educating your corporate customers on digital safety?

A. Governments ✓
B. Non profit forums ✓
C. Banks ✓
D. No one

What does this mean for banks?

The National Cyber Management Centre®

Who do you think is responsible for educating your corporate customers on digital safety?

A. Governments ✓
B. Non profit forums ✓
C. Banks ✓
D. No one

Three big questions..

The National Cyber Management Centre®

Where is the legal and moral point at which customers ignorance is a bank's responsibility in the event of a cyber loss?

What is the legal and moral obligation on a bank to mitigate this lack of understanding?

Who is a trusted global partner who can ensure cyber standards and intelligence sharing work?

Open questions and answers

The National Cyber Management Centre®