University of Kent | Kent Interdisciplinary Research Centre in Cyber Security (KirCCS)

University of Oxford

CYBER SECURITY OXFORD

Interdisciplinary Approaches to Cyber Security for Organisations

Dr Jason R.C. Nurse

Asst. Prof. in Cybersecurity, School of Computing, University of Kent

Visiting Academic in Cybersecurity, University of Oxford

Visiting Fellow in Defence & Security, Cranfield University

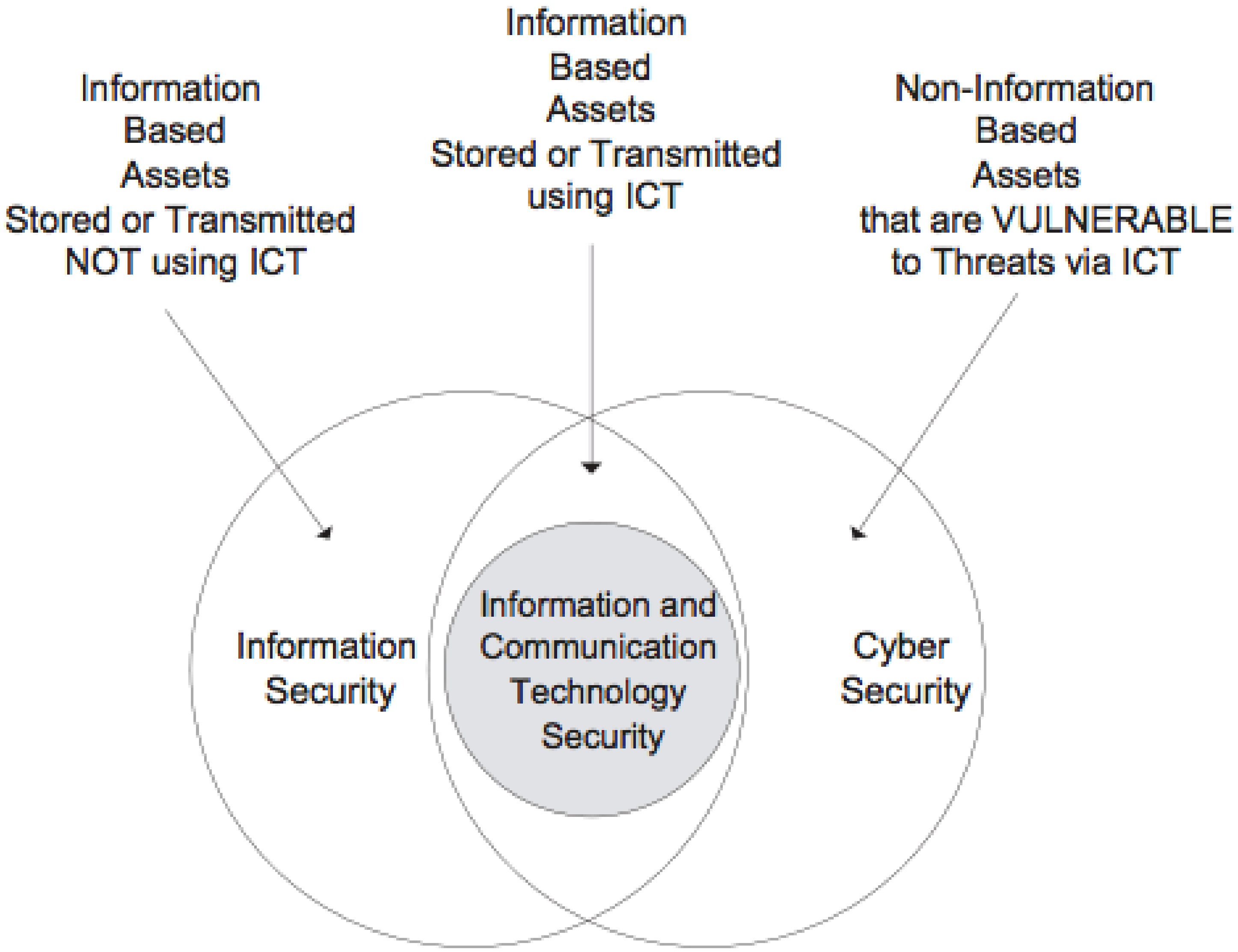
✉ j.r.c.nurse@kent.ac.uk

🐦 @jasonnurse

"I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."

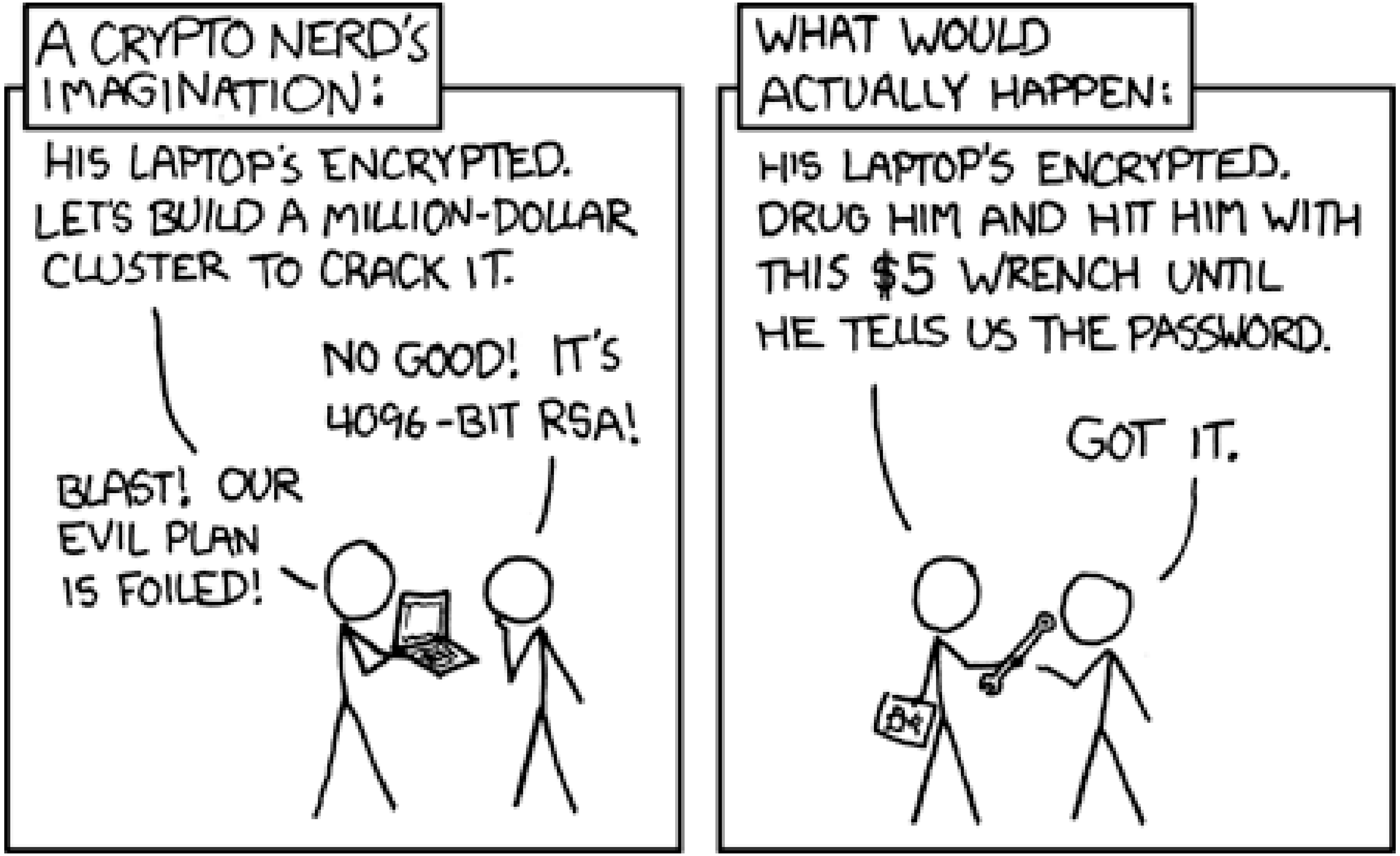
Robert Mueller, Former Director of the FBI

The uniqueness of cyber security and cyber risk


Information Based Assets Stored or Transmitted NOT using ICT
Information Based Assets Stored or Transmitted using ICT
Non-Information Based Assets that are VULNERABLE to Threats via ICT
Information Security
Information and Communication Technology Security
Cyber Security

Von Solms, R. and Van Niekerk, J., 2013. From information security to cyber security. *computers & security*, *38*, pp.97-102.

Cyber criminals are thinking beyond technology


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

https://xkcd.com/538/

Tackling future cyber risk requires collaboration and engagement beyond ‘just’ technology as well…

Case 1: Insider Threat

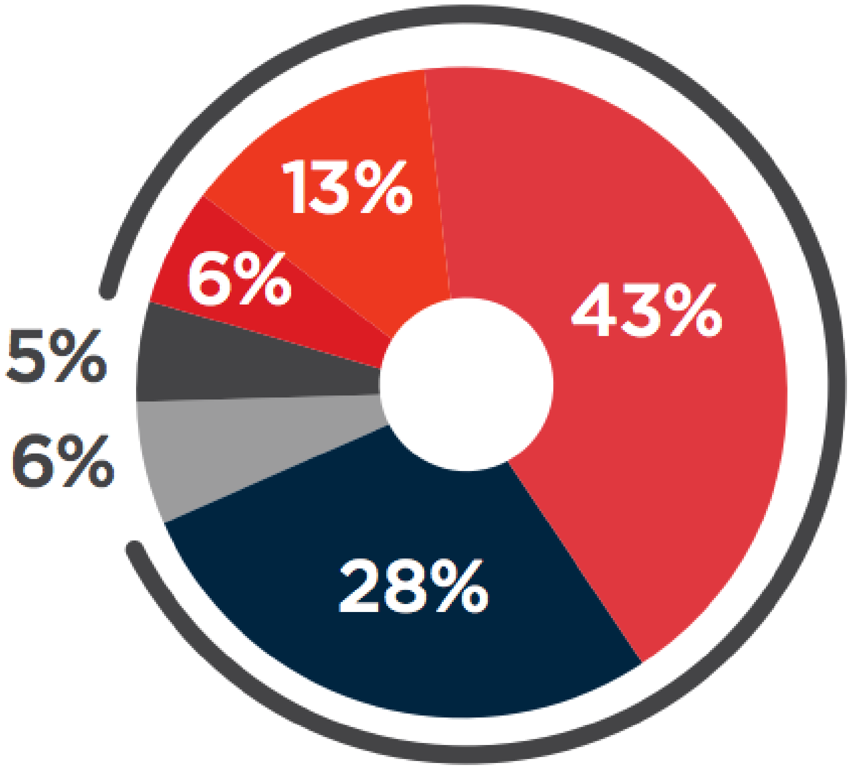
Case 2: Security Awareness

Case 3: Cyber-harm

Case 1: Insider threat

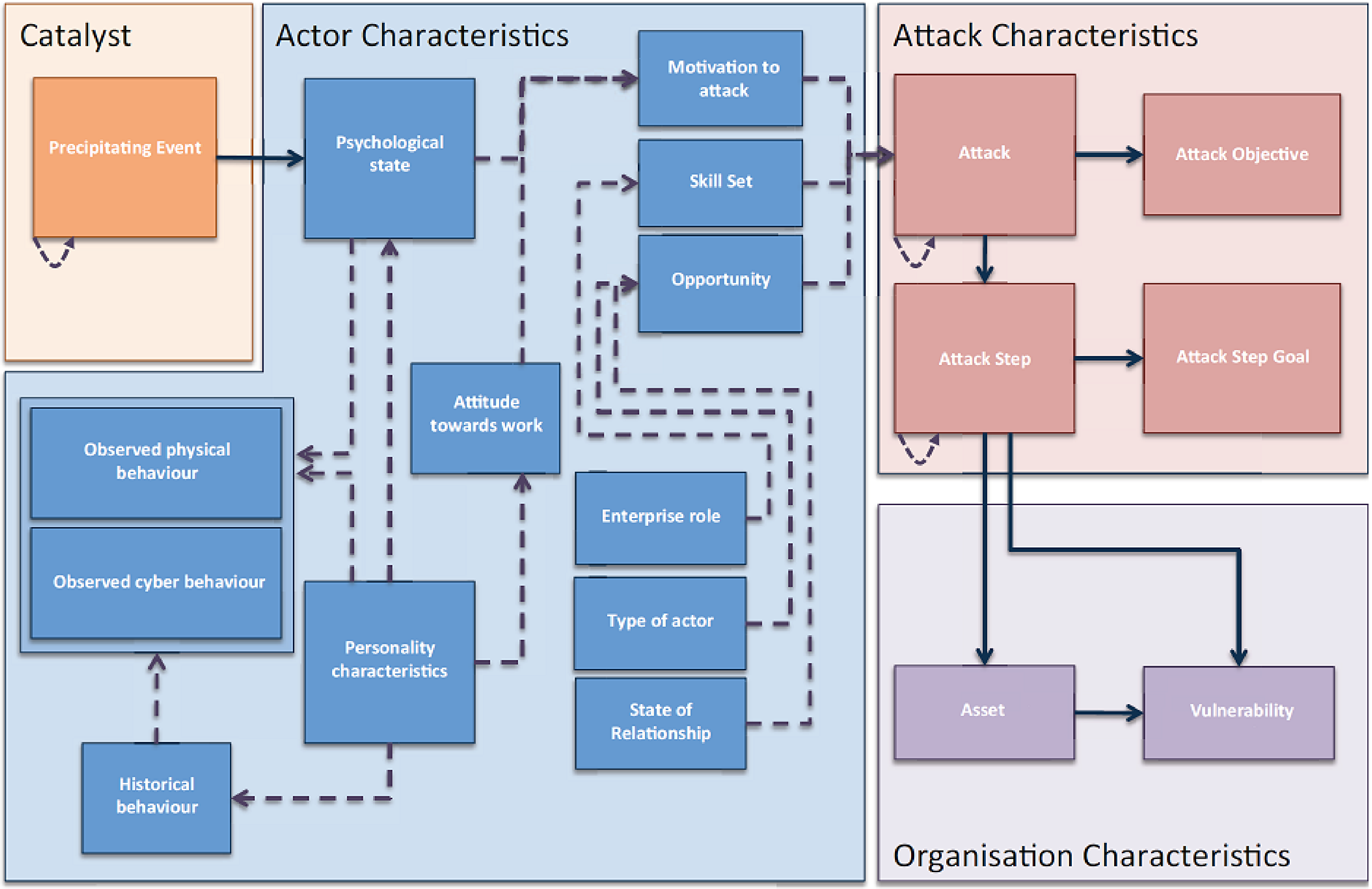
Corporate insider threat

How vulnerable is your organization to insider threats?



90% feel vulnerable to insider threats

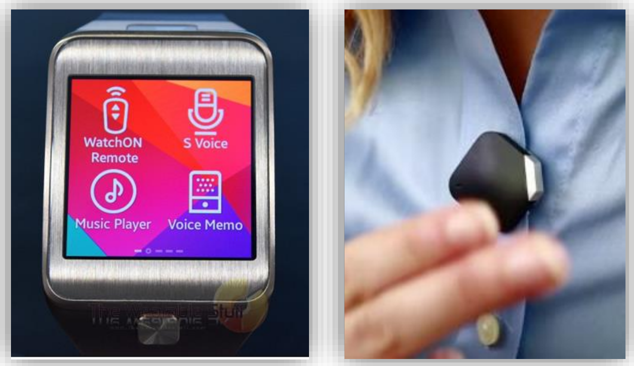
Framework for insider threat analysis, detection and prevention



Nurse et al. “Understanding insider threat: A framework for characterising attacks”. In *IEEE Security and Privacy Workshops.*

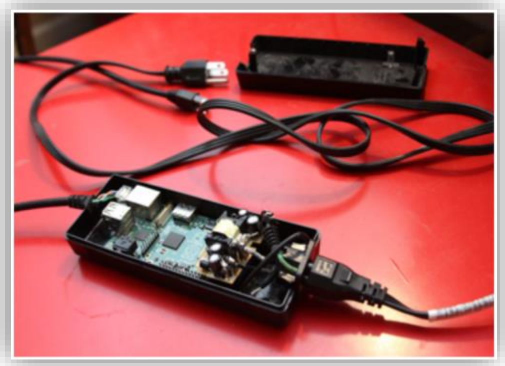
The ‘*new*’ cyber risk present with insiders using smart tech

- New technologies (e.g., smart devices, wearables, personal IoT) create several new ways to attack organisations



Discrete audio recording (e.g., in private meetings) & leaking that information

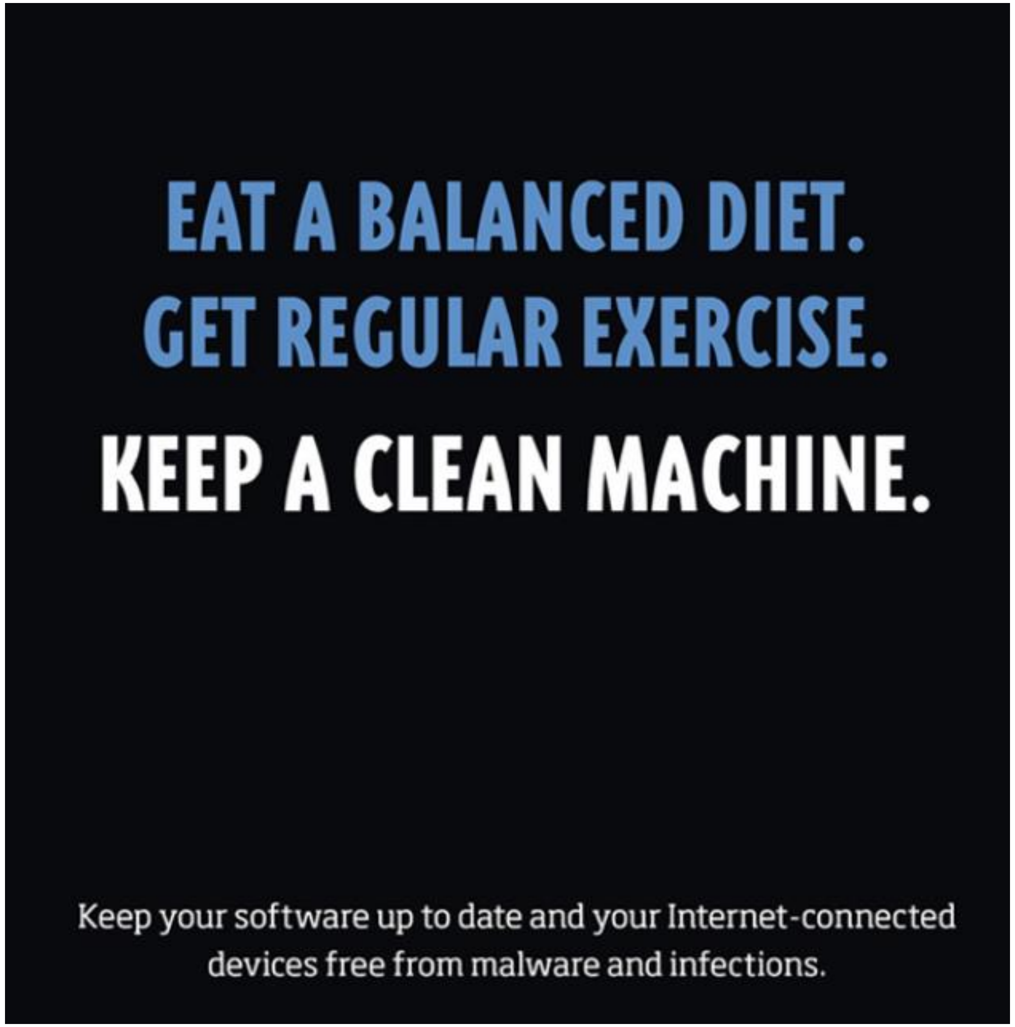
Discrete video recording allowing password theft



Raspberry pi disguised and left to allow remote access

Nurse et al., “Smart Insiders: Exploring the Threat from Insiders using the Internet-of-Things”. In Workshop on Secure Internet of Things at ESORICS.

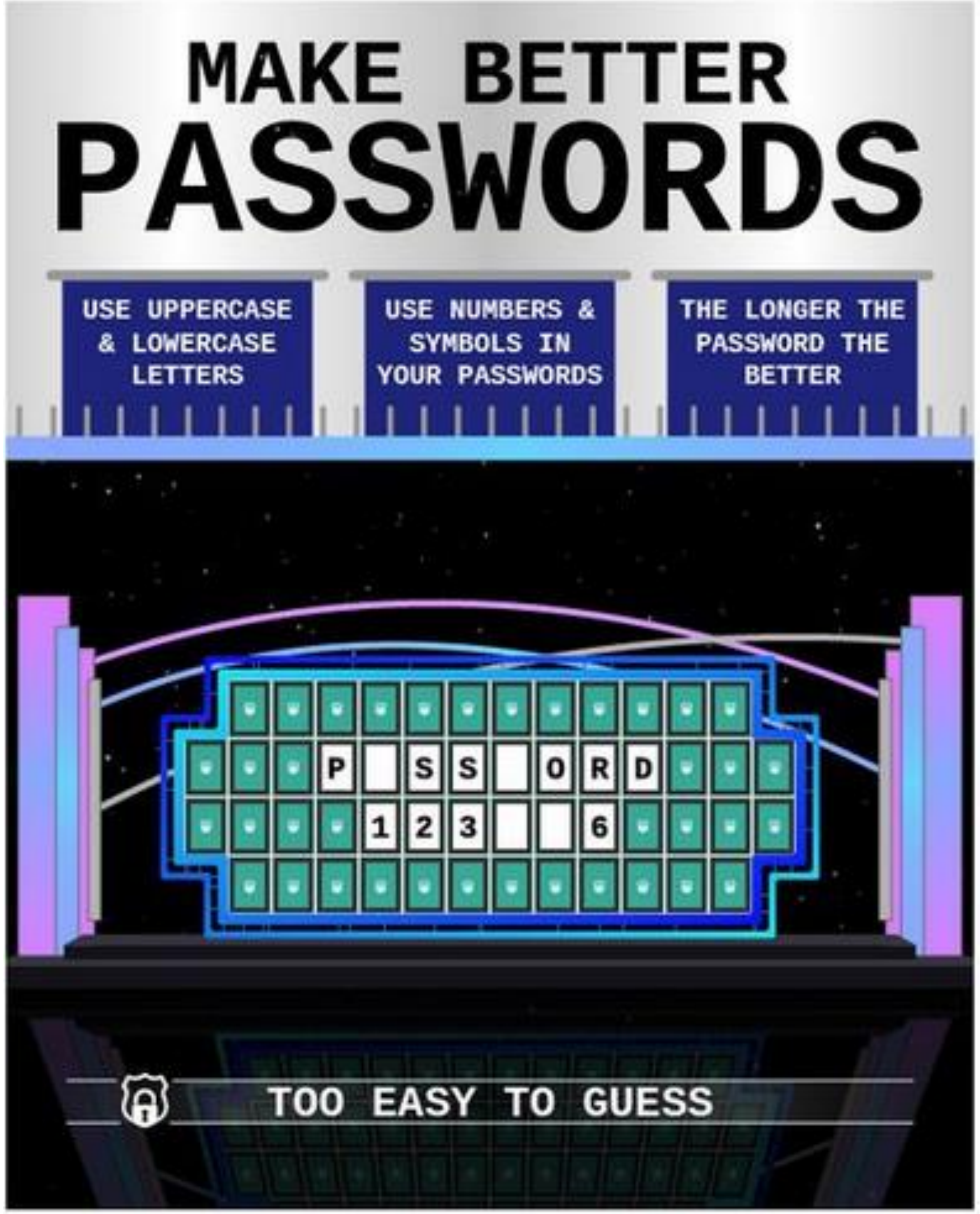
Case 2: Security Awareness



EAT A BALANCED DIET.
GET REGULAR EXERCISE.
KEEP A CLEAN MACHINE.

Keep your software up to date and your Internet-connected devices free from malware and infections.

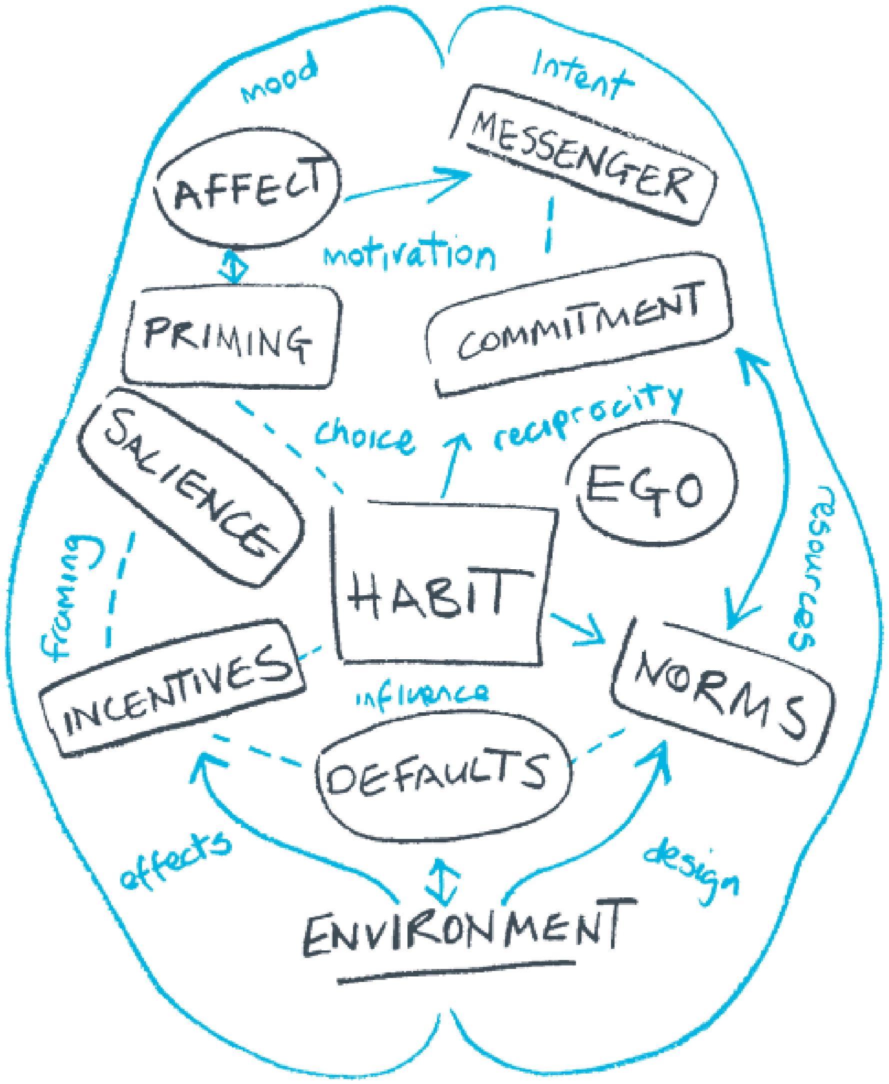
https://stopthinkconnect.org.ag/campaigns/details/?id=266


MAKE BETTER
PASSWORDS
USE UPPERCASE & LOWERCASE LETTERS
USE NUMBERS & SYMBOLS IN YOUR PASSWORDS
THE LONGER THE PASSWORD THE BETTER
P SS ORD
123 6
TOO EASY TO GUESS

https://www.pinterest.co.uk/pin/502292164690414631

MINDSPACE

To change future security behaviour and create a security aware culture, we need to *really* understand people

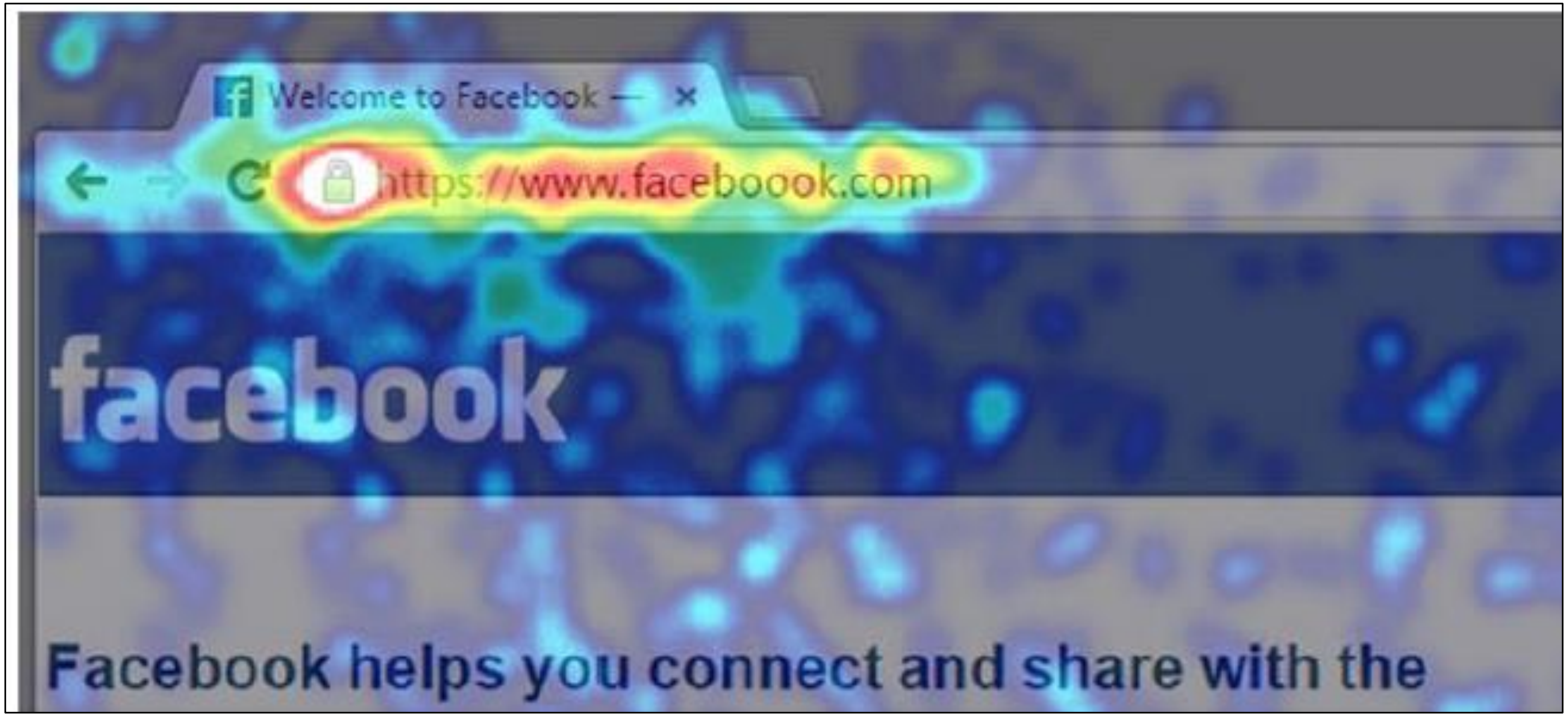


- Combine **several different approaches** (training sessions, awareness material, supportive technologies, etc.)
- Be carefully **planned** and **tailored** to the organisation
- Use **simple consistent rules** of behaviour that people can follow
- Use **engaging** and appropriate materials
- Arrange **multiple training exercises** – option of offering general training and specific sessions
- **Assess/measure/refine** the awareness programmes

https://www.instituteforgovernment.org.uk/sites/default/files/publications/MINDSPACE.pdf

Bada et al. “Cyber Security Awareness Campaigns: Why do they fail to change behaviour?” In CSSS Conference.

Approaches to cyber risk constantly need to be updated and refined based on the environment and context

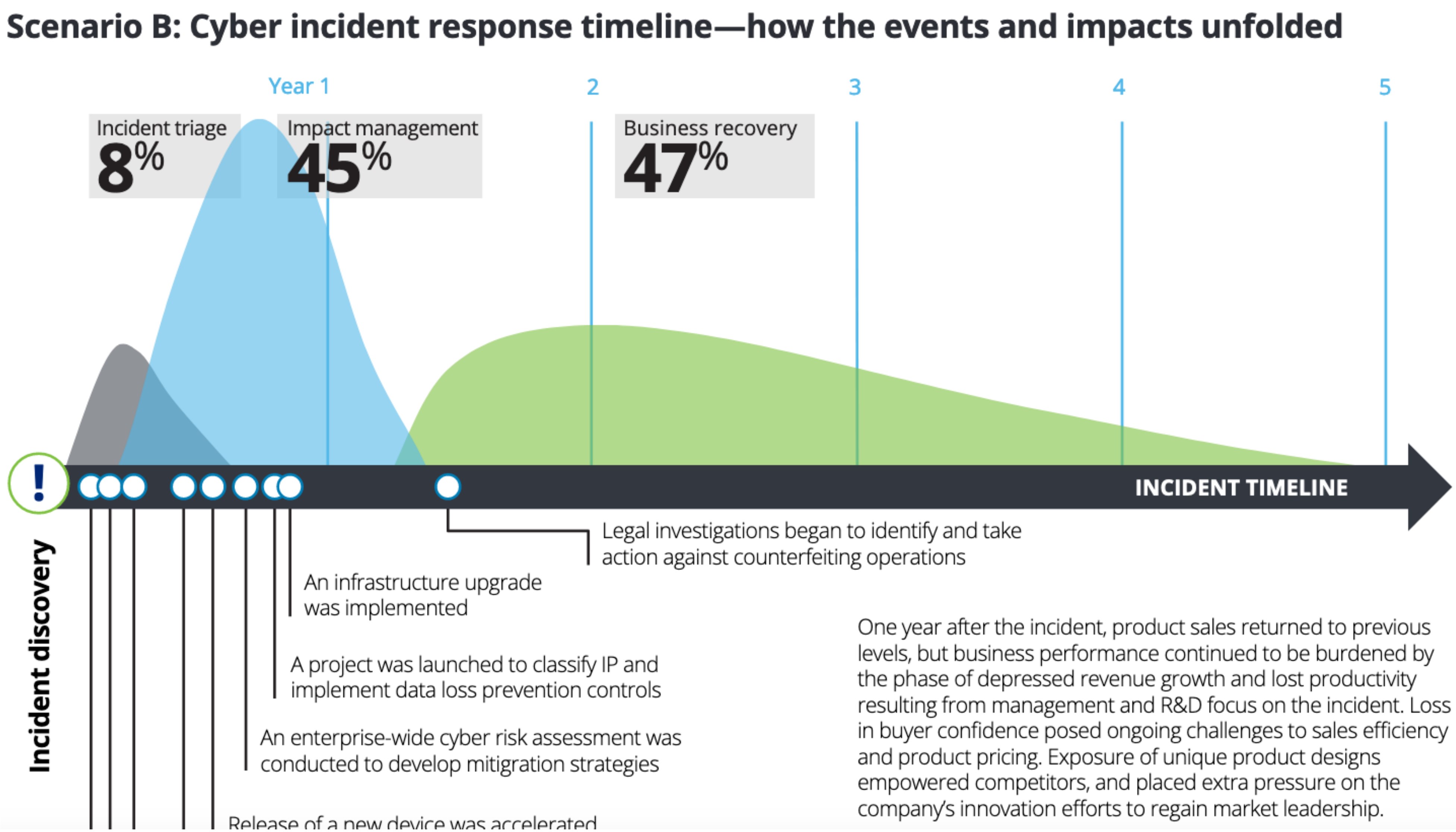

Welcome to Facebook
https://www.facebooook.com
facebook
Facebook helps you connect and share with the

In our study, we found that training people to listen to the padlock only has meant that cybercriminals now know exactly how to deceive people.

Iuga, et al. “Baiting the hook: factors impacting susceptibility to phishing attacks”. Human-centric Computing and Information Sciences, 6(1), pp.1-20.

Case 3: Cyber-harm

Cyber attacks have a much larger impact than many companies realise, and this impact is often not considered in risk assessments



Scenario B: Cyber incident response timeline—how the events and impacts unfolded

Legal investigations began to identify and take action against counterfeiting operations

An infrastructure upgrade was implemented

A project was launched to classify IP and implement data loss prevention controls

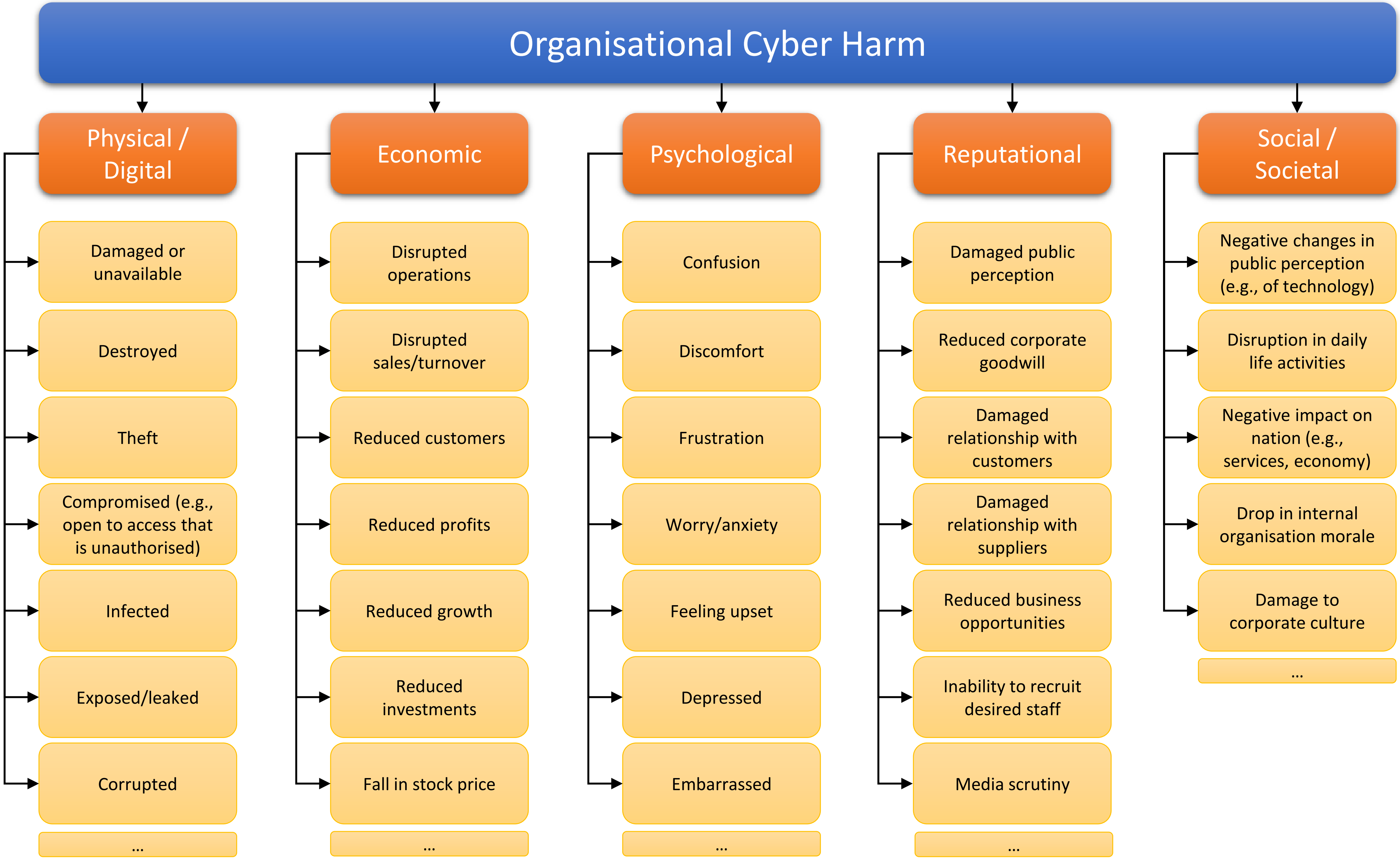
An enterprise-wide cyber risk assessment was conducted to develop mitigation strategies

Release of a new device was accelerated

One year after the incident, product sales returned to previous levels, but business performance continued to be burdened by the phase of depressed revenue growth and lost productivity resulting from management and R&D focus on the incident. Loss in buyer confidence posed ongoing challenges to sales efficiency and product pricing. Exposure of unique product designs empowered competitors, and placed extra pressure on the company's innovation efforts to regain market leadership.

Deloitte. Beneath the surface of a cyberattack: A deeper look at business impacts

Cyber-harm can be used to emphasise the wider spectrum of harms that can result from a cyber-attack

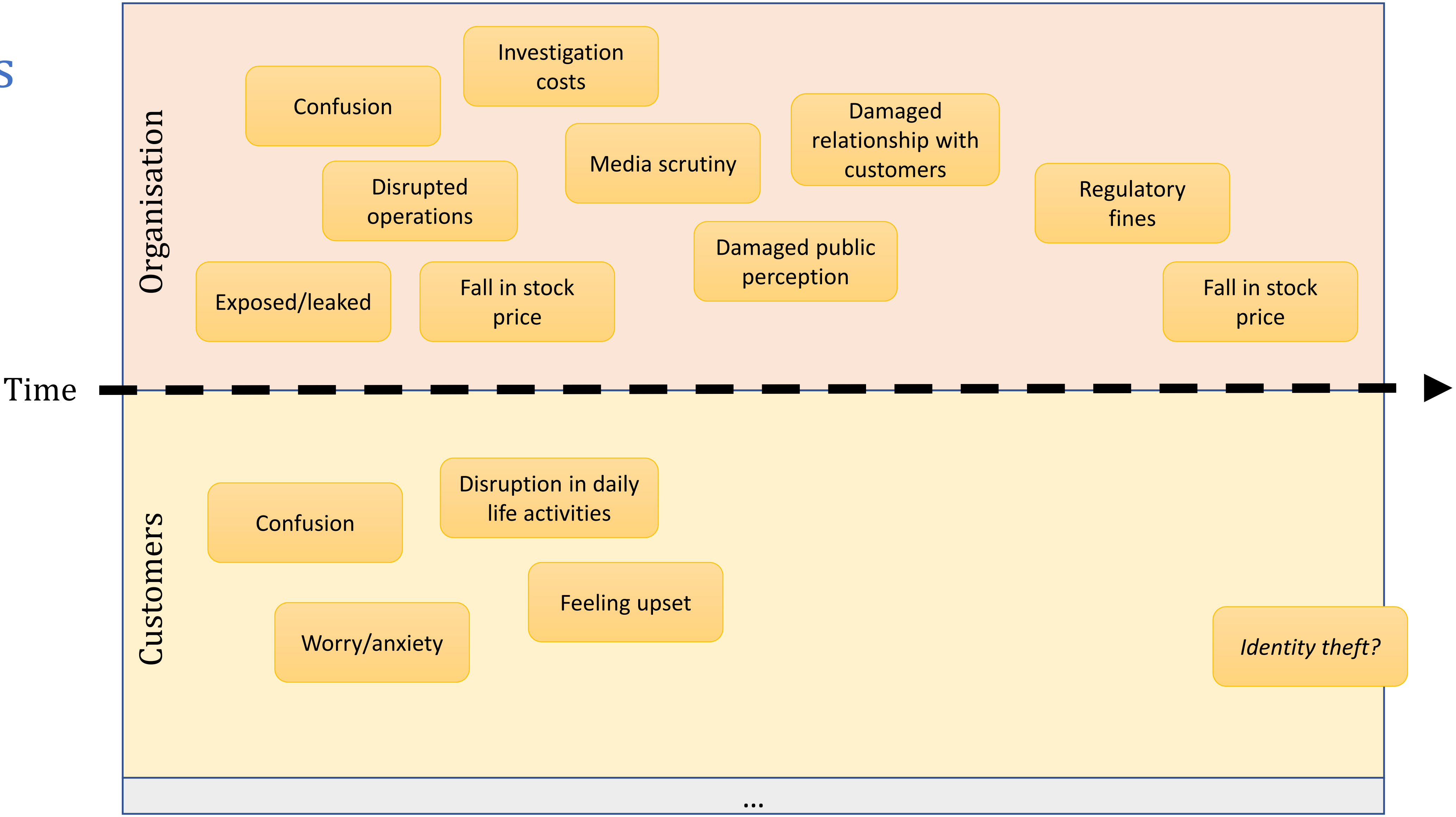


Organisational Cyber Harm

Physical / Digital	Economic	Psychological	Reputational	Social / Societal
Damaged or unavailable	Disrupted operations	Confusion	Damaged public perception	Negative changes in public perception (e.g., of technology)
Destroyed	Disrupted sales/turnover	Discomfort	Reduced corporate goodwill	Disruption in daily life activities
Theft	Reduced customers	Frustration	Damaged relationship with customers	Negative impact on nation (e.g., services, economy)
Compromised (e.g., open to access that is unauthorised)	Reduced profits	Worry/anxiety	Damaged relationship with suppliers	Drop in internal organisation morale
Infected	Reduced growth	Feeling upset	Reduced business opportunities	Damage to corporate culture
Exposed/leaked	Reduced investments	Depressed	Inability to recruit desired staff	…
Corrupted	Fall in stock price	Embarrassed	Media scrutiny	
…	…	…	…	

Agrafiotis et al. "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate." *Journal of Cybersecurity.*

Modelling cyber-harms resulting from the BA data breach in 2018



Agrafiotis et al. "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate." *Journal of Cybersecurity.*

To tackle future cyber risk, an inter-disciplinary approach is required…

Computer Science

Education and awareness

Finance

International relations

Sociology

Enterprise Operations Management

Psychology

War studies

Criminology

Business

Economics

Psychological profiling

Visual analytics

Organisational culture

Data science

Dr Jason R.C. Nurse

j.r.c.nurse@kent.ac.uk

@jasonnurse