Conference Presentations

Technology Ireland ICT Skillnet

Technology Ireland ICT Skillnet is co-funded by Skillnet Ireland and member companies. Skillnet Ireland is funded from the National Training Fund through the Department of Education and Skills.

An Roinn Oideachais agus Scileanna
Department of Education and Skills

Skillnet IRELAND

Technology Ireland Software Skillnet

Carmel Somers

Talent Manager, IBM Ireland Lab

Chair, Cybersecurity Skills Initiative

Technology Ireland ICT Skillnet

Technology Ireland Software Skillnet


IDA Ireland


ENTERPRISE
IRELAND
where innovation means business


Skillnet
IRELAND


MAXOL
At the heart of it


Deloitte.


IBM

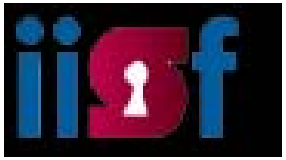

Technology
Ireland
Ibec


ICS
CELEBRATING
50 YEARS


NATIONAL CYBER SECURITY CENTRE
NCSC


IRISS
Irish Reporting and
Information Security Service


ISI
infosecurity
ireland


iisf


etbi


UCD
DUBLIN


itb
Institute of Technology
Blanchardstown
Institiúid Teicneolaíochta
Baile Bhlainséir

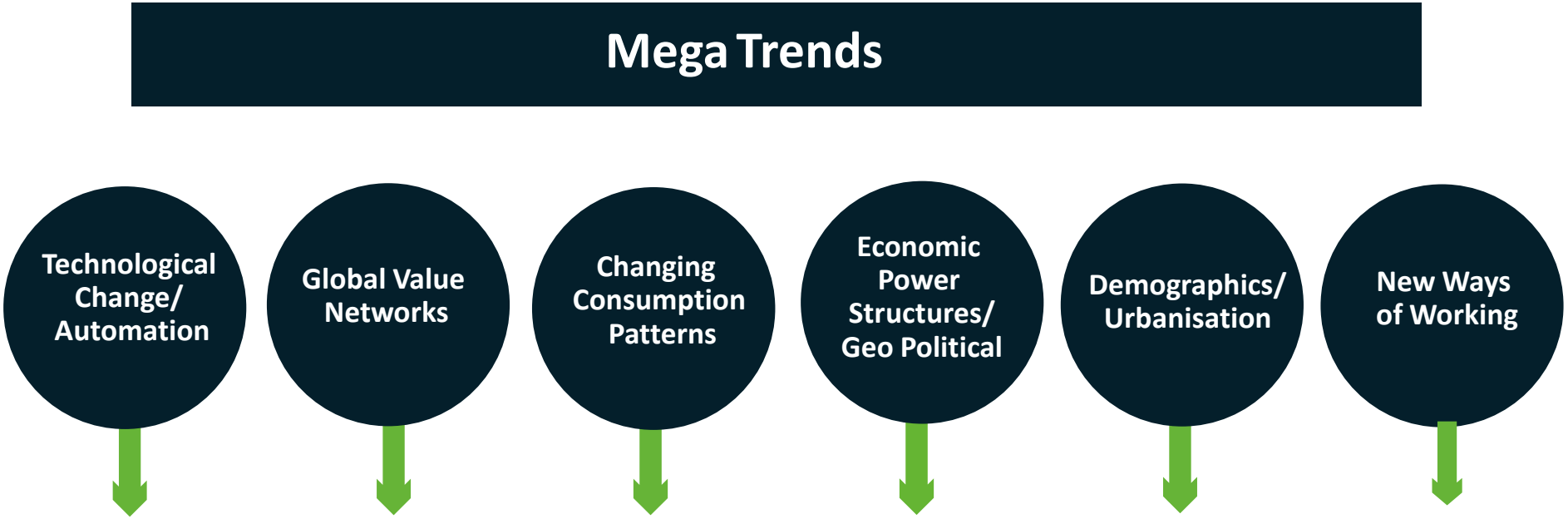
The Road to Excellence


1
2
3
4
5
Awareness
Attract People into Cybersecurity
Preparedness
Enhance Cybersecurity capability
Resilience
Cybersecurity Skills and Expertise
Standards
Standards and Competencies
Automation
Uptake of automation and AI

Paul Healy

Chief Executive
Skillnet Ireland

The Big Picture……..



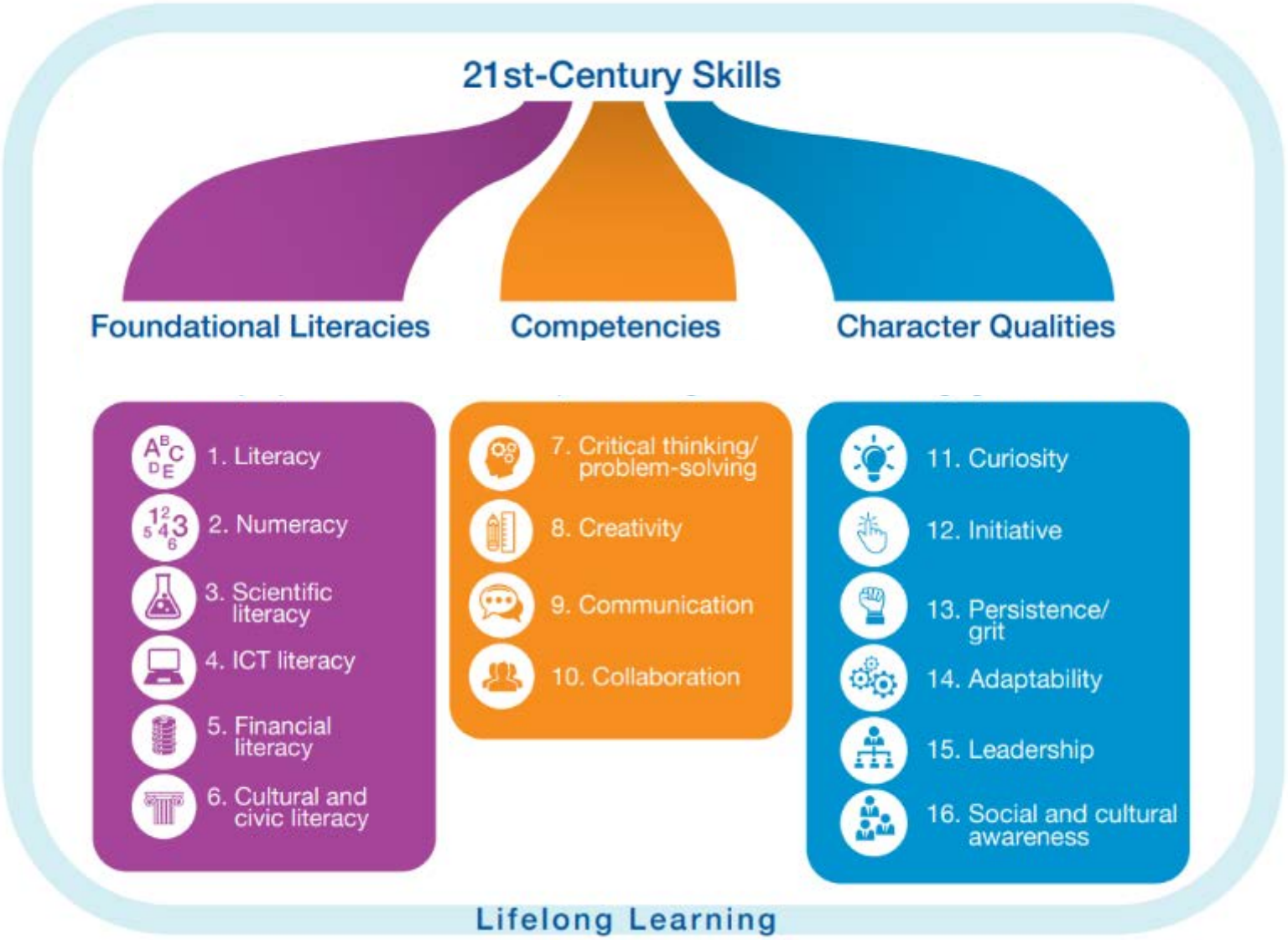
Major Implications for Skills & Talent in Ireland

The Big Picture…..

Meaning…..

Opportunities for Skills Development in Ireland

21st Century Skills…..

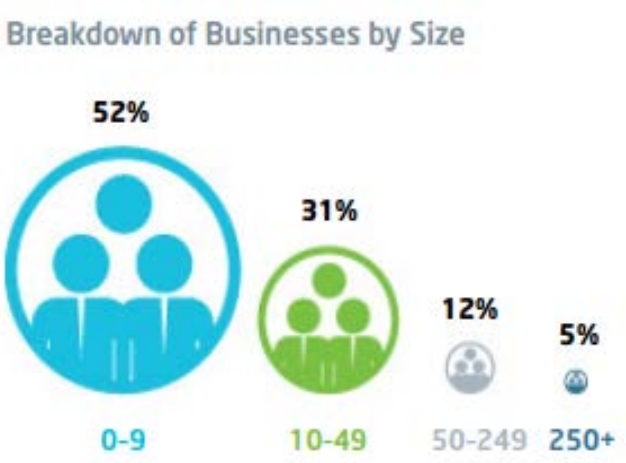


Source: World Economic Forum / Boston Consulting Group (2016)

Building Digital Intelligence….

Source: Yuhyun Park, IZ Foundation 2017

Supporting
15,000 firms & 50,000 learners annually



Recent Evaluations

Skillnet Ireland selected as an international best-practice case study to guide policymakers on designing and implementing funding schemes for SME training.

"The Skillnet decentralised model generates highly specialised knowledge on employment and training related issues, resulting in better alignment between labour market needs and the supply of skills"

- 89% employers: Skiilnet had a positive impact on addressing skills gaps
- 78% employers: Skillnet had a positive impact on enhanced service/product quality.
- 76% employers: Skillnet a positive impact on the long-term performance of their business.
- 73% employers: Skillnet a positive impact on increased staff engagement.
- Every **€1million** of State funding via Skillnets attracts **€1.16 million** in investment from employers.

"Financial Incentives for Steering Education and Training, Getting Skills Right"": OECD, Oct 2017, p. 90-91
"Evaluation of Skillnets Training Networks Programme" Indecon International Economic Consultants, Sept 2017, p.9
"Upskilling SMEs" : International Labour Organization, Oct 2017, p. 3

BH Consulting

Where's the Risk? Examining the Threat Landscape

Brian Honan October 2018

@brianhonan

Brian Honan

BH Consulting


INDEPENDENT.IE
NEWS
OPINION
BUSINESS
SPORT
LIFE
STYLE
Brexit | Irish | World | Technology | Personal Finance | Small Business | FarmIreland
Monday 16 October 2017
Business Newsletter
Business Irish
SuperValu, Centra and Daybreak stores targeted in cyber attack


THE IRISH TIMES
Wed, Sep 13, 2017
NEWS
SPORT
BUSINESS
OPINION
LIFE & STYLE
CULTURE
Ireland › Irish News
AIB employee loses banking details of 500 customers
Bank notifies Data Protection Commissioner and customers after details are mislaid


Irish Examiner
NEWS
SPORT
BUSINESS
VIEWS
LIFE
EXAMVIRAL
PROPERTY
MOTORS
LATEST
IRELAND TODAY
BUSINESS
FARMING
WORLD
DEATHS
HOT TOPICS:
FORD 100
GARDA COMMISSIONER
CORK NOW AND THEN
HOME
»
TODAY'S STORIES
Concerns over alleged data breaches in Kerry
2
Wednesday, September 13, 2017

ISME Crime Survey 2018

- **26%** experienced computer related crime in the last 12 months
- **12%** of businesses employed an IT manager responsible for security,
- **33%** employed an IT supplier responsible for security
- **98%** would like to see the establishment of a Central/National E-crime body to deal specifically with E-crime

Institute of Directors in Ireland

- **33%** of organisations experienced a cyber breach in the past 2 years with **44%** of organisations selling online have experienced a cyber breach

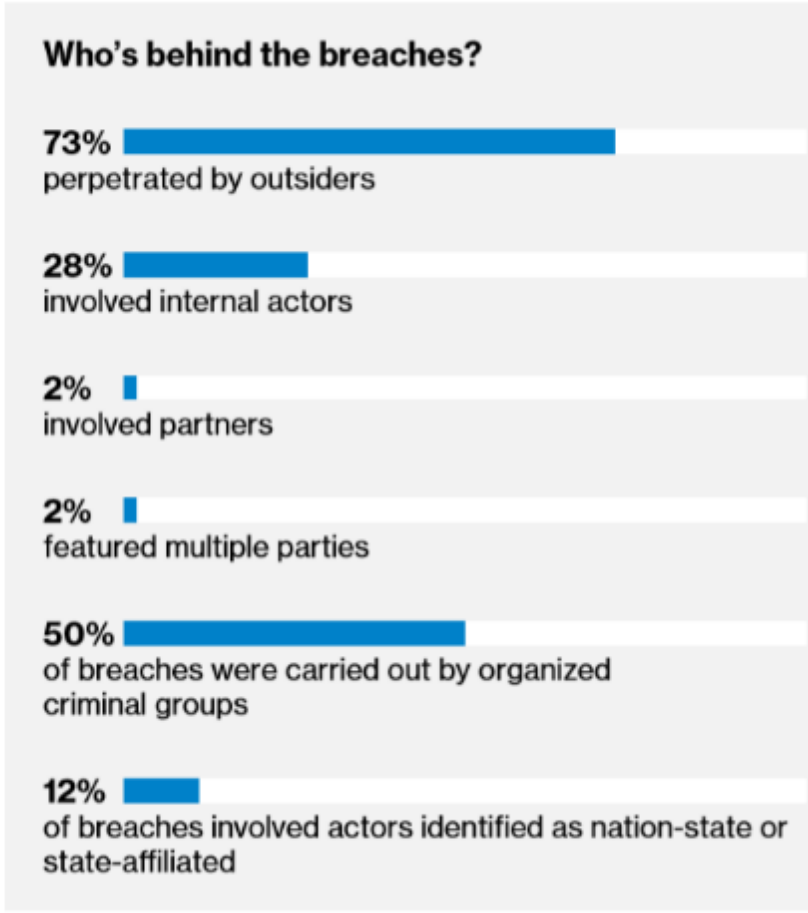
- **84%** of directors say their organisation will increase spending on cyber security measures over the next 3 years

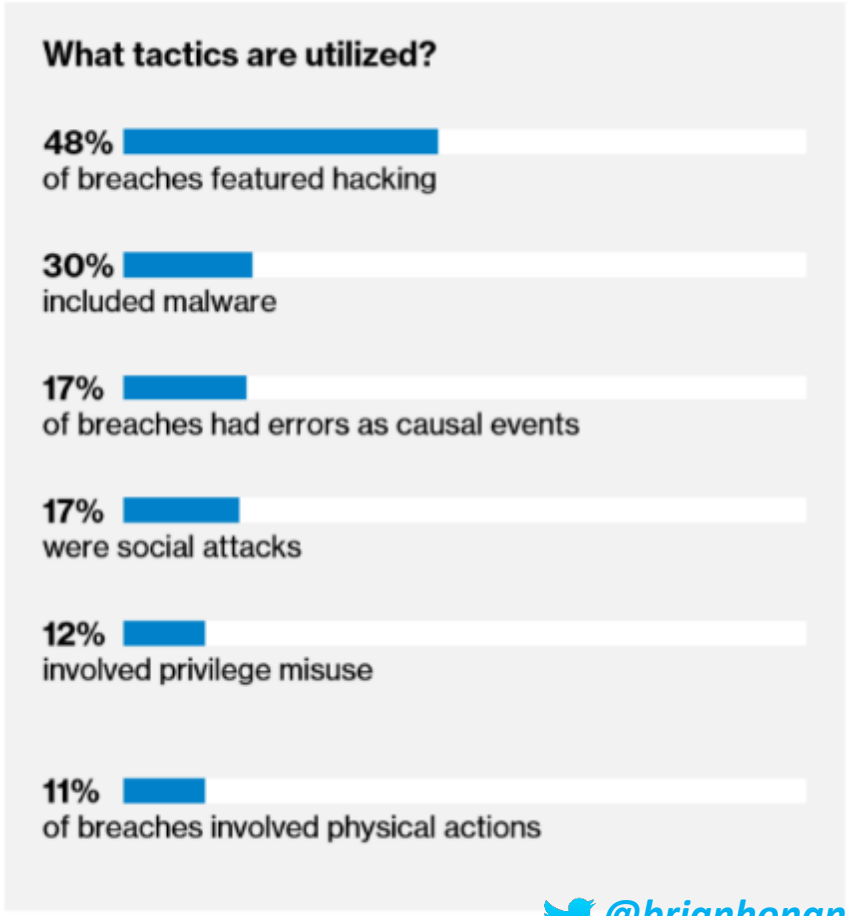
- **69%** of directors claim their organisation is prepared or very prepared for a cyber breach

- **40%** of organisations have **no** formal cyber security strategy

verizon

Summary of findings





@brianhonan

verizon

Summary of findings

Who's behind the breaches?

73% perpetrated by outsiders

2% featured multiple parties

50% of breaches were carried out by organized criminal groups

12% of breaches involved actors identified as nation-state or state-affiliated

What tactics are utilized?

17% were social attacks

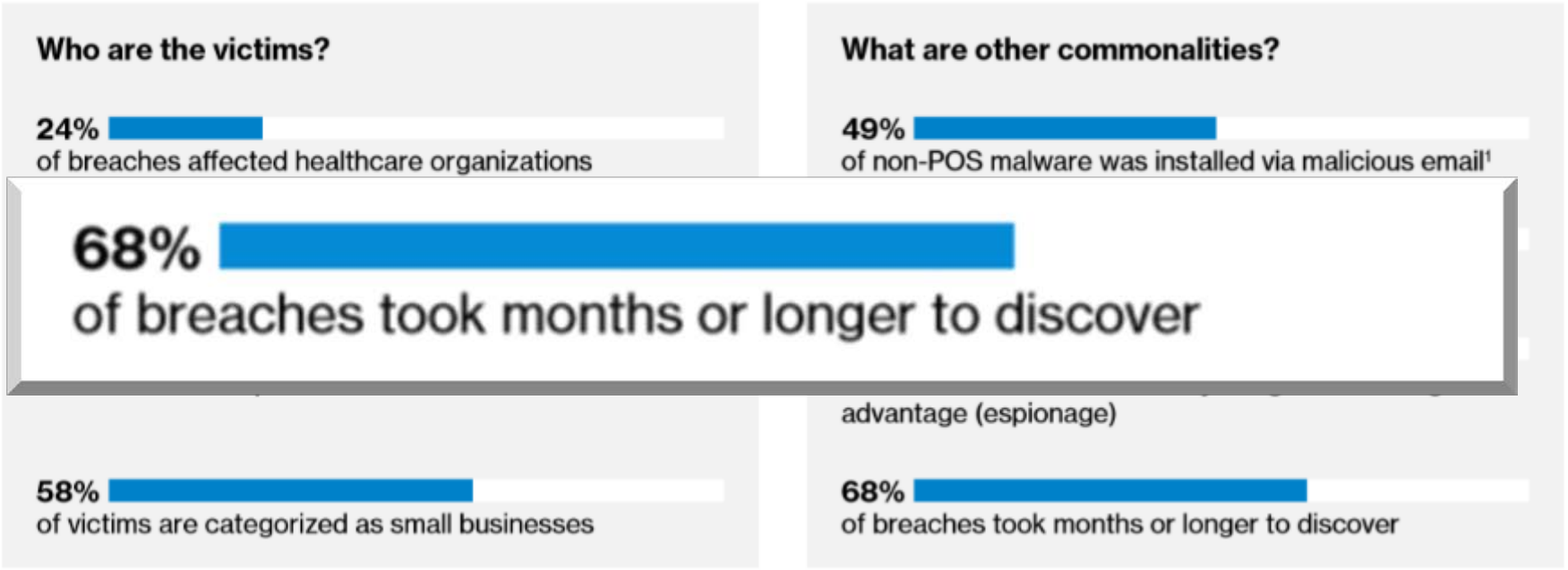
12% involved privilege misuse

11% of breaches involved physical actions

@brianhonan

verizon

Summary of findings



@brianhonan

Root Causes

- Poor Passwords
  - Web Based Email Attacks
- Missing Patches
- Vulnerabilities
  - Web Platforms
  - Out of date software (Windows XP)
- Out of Date Anti-Virus Software
- Lack of Monitoring

@BrianHonan
Brian.honan@bhconsulting.ie
www.bhconsulting.ie

Cybersecurity Skills Initiative (CSI)

Detective Superintendent Michael Gubbins

Garda National Cyber Crime Bureau

Technology Ireland ICT Skillnet

Technology Ireland Software Skillnet

Garda National Cyber Crime Bureau

- Forensic Examinations
- Cyber Crime Investigation
- Cyber Intelligence
- Cyber Crime Prevention
- Cyber Crime Training
- Public awareness
- National & International Liaison
- Industry & Academic Liaison

Cybercrime: Enabled –v- Dependent

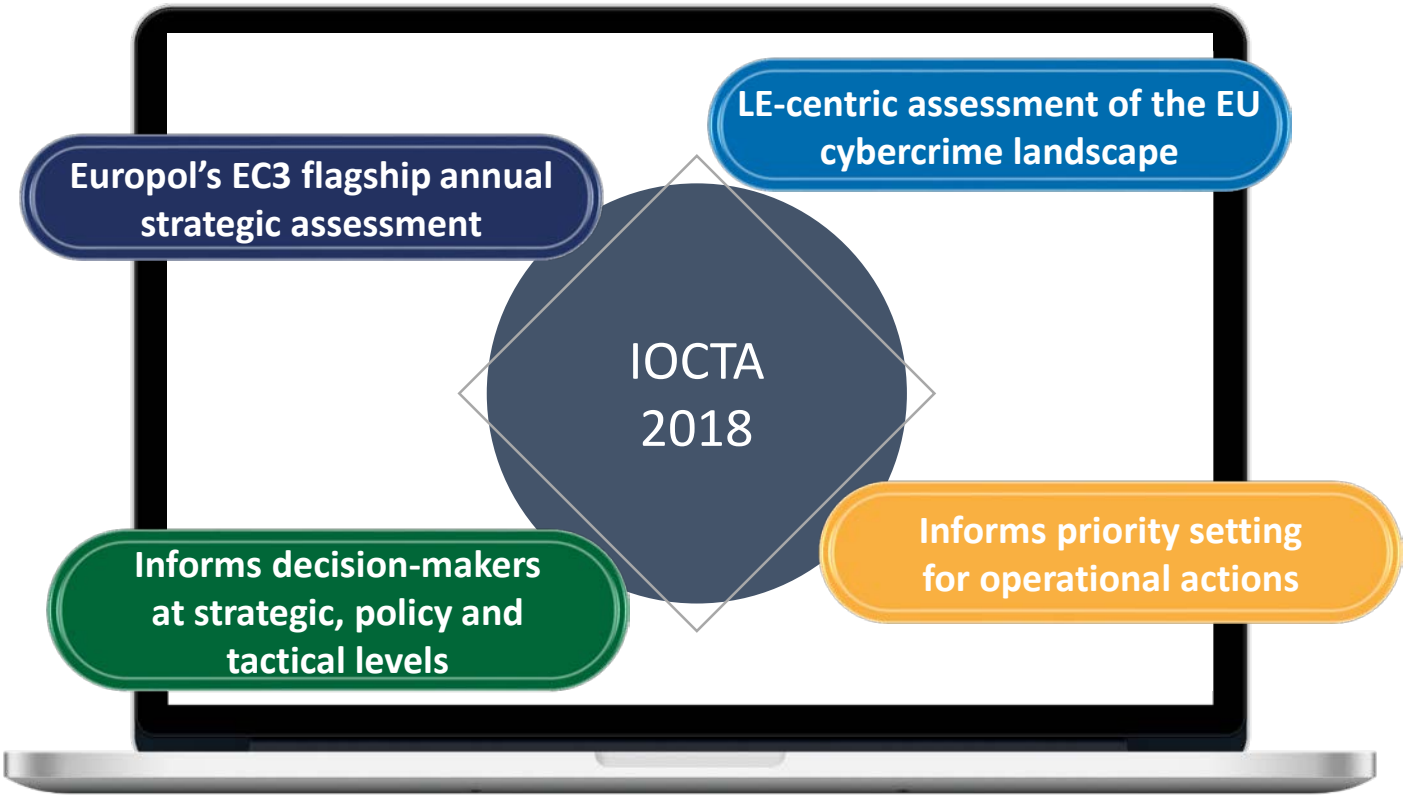
Cyber-Enabled

- Existing types of crime which are perpetrated through the use of the internet
- Email scams, theft of credit card details, CEO fraud, invoice re-direction, distribution of illegal material
- GNCCB assist/support

Cyber-Dependent

- Crimes which can only be committed through the use of a computer, mobile device, computer network/system or other form of ICT infrastructure
- Hacking, DDoS, ransomware
- GNCCB assist/support or investigate

Internet Organised Crime Threat Assessment



IOCTA 2018 – How was it put together?

- Member States Surveys
- Third Parties Surveys
- Advisory Groups Surveys
- Open Source Research

IOCTA 2018 – Topic Areas

IOCTA 2018 – Key Trends & Threats

Ransomware retains its dominance

DDoS continues to plague public and private organisations

Card-not-present fraud dominates payment fraud, but skimming continues

Cryptocurrency users and exchangers are becoming targets

Cryptojacking

Social engineering still the engine of many cybercrimes

Darknet markets still facilitates illegal business

Production of CSEM continues

IOCTA 2018 – Key findings

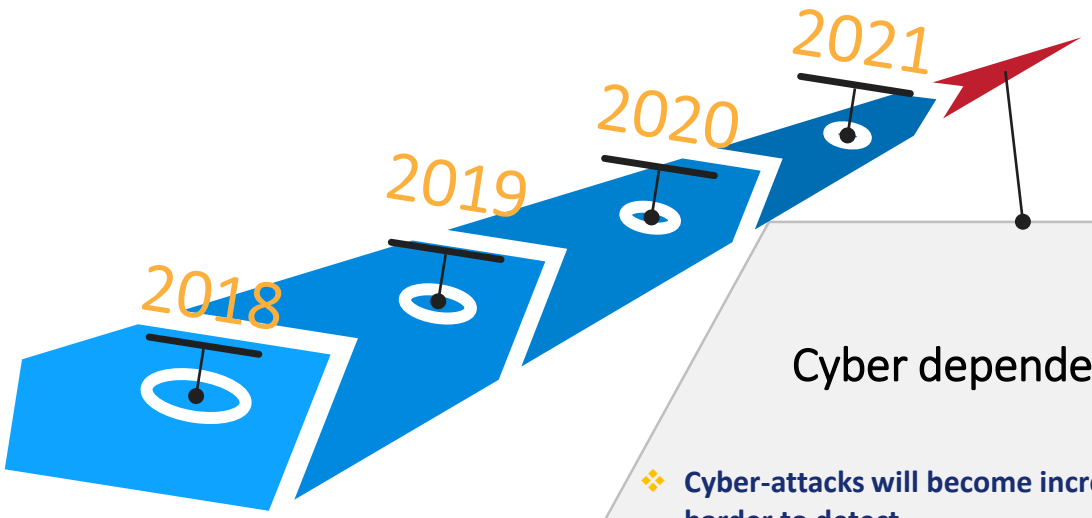
Cyber-dependent crime

- Ransomware remains a key threat
- Spam, social engineering and other methods are evolving
- Cryptomining malware gradually becomes a regular, low-risk revenue stream for cybercriminals

Payment Fraud

- Card-not-Present Fraud expected to increase as EMV compliance spreads
- New forms of PoS terminals abuse: from device manipulation to fraudulent acquisition of new terminals
- Telecommunication fraud as a new challenge for law enforcement

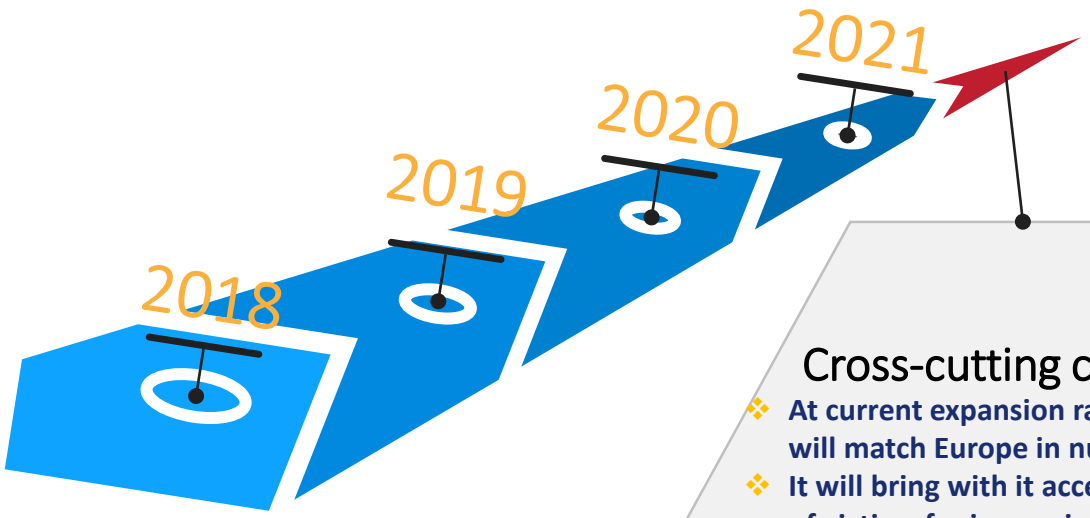
IOCTA 2018 – Flashforward



Cyber dependent crime

- **Cyber-attacks will become increasingly stealthy and harder to detect.**
- **Attacks using fileless malware will become a standard component of the crime-as-a-service industry.**

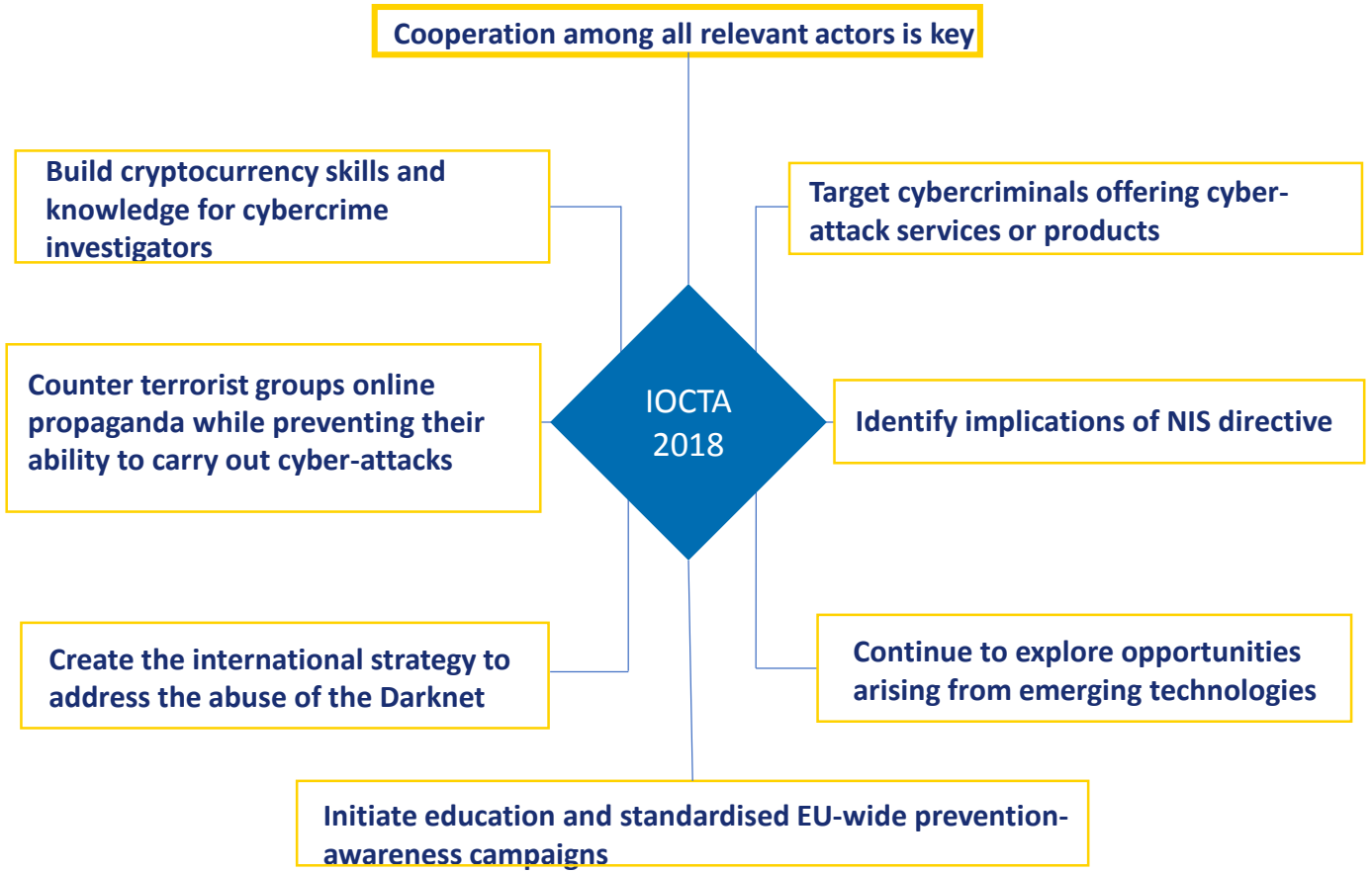
IOCTA 2018 – Flashforward



Cross-cutting crime factors

- At current expansion rates, it is likely that Africa will match Europe in numbers of internet users.
- It will bring with it access to a global assemblage of victims for increasingly sophisticated and tech-savvy cybercriminals and a more significant role for West African OCGs within the EU.
- Phishing continues to increase and remains the primary form of social engineering. Although only a small proportion of victims click on the bait, one successful attempt can be enough to compromise a whole organisation.

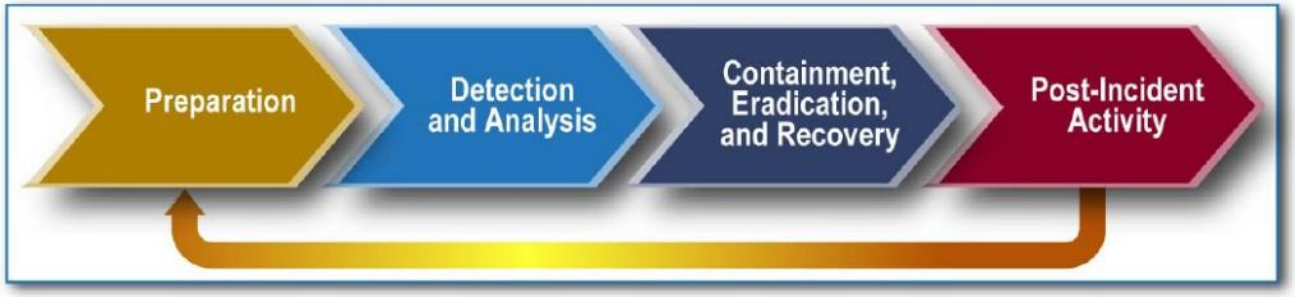
IOCTA 2018 – Key Recommendations



Reported to Gardaí

- Snapchat account hacked
- DDOS attack
- Data Breach
- Facebook account ha
- Ransomware
- PABX Fraud
- Instagram Account hacke
- Phone Hacked
- PC hacked
- Email account compromised

Incident Response



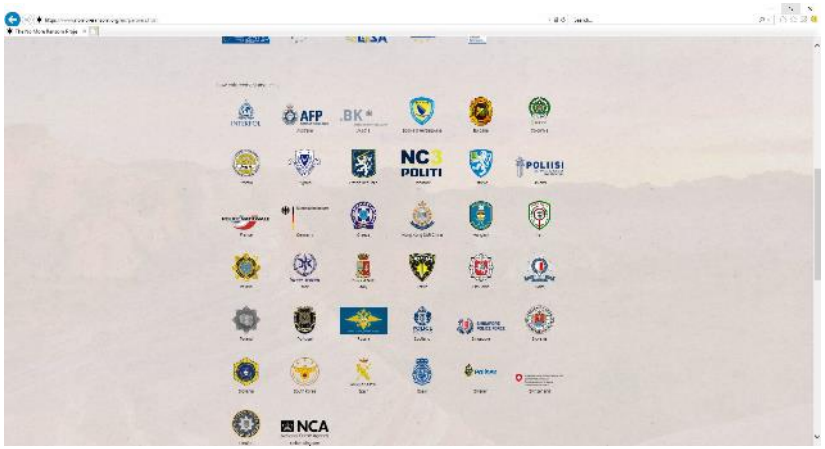
How do I report a crime?

- Local Garda Station
- Garda National Cyber Crime Bureau

High-Tech Crime Forum

- BPFI membership
- AGS
- PSNI
- UCD
- ISPAI
- Invited guests

www.nomoreransom.org



Responsibilities

"He who defends everything, defends nothing."

Frederick the Great

Board Level Considerations

- What are your organisations most valuable assets?
- What are the things you have to protect?
- What can you not do without?
- Who are the people involved?
  - High risk targets
- Monitoring, education & training of employees

Board Level Considerations

- Need to acquire own level of expertise internally
- Need to identify your own threat landscape
- Vulnerability management (Programmes, Networks)
  - Business needs
  - Rapid remediation
- Regular external review

Board Level Considerations

- Not everything is critical
- What happens if there is a business outage?
- How do you get back on line?
- How do you define controls?
- Situational awareness
  - Intelligence feeds
  - Analyse
  - Identify Threats and vulnerabilities

Board Level Considerations

- Data leakage prevention programme
- Insider/Employee risks
- “Inspect not expect”
- How do you define controls
- Aim is to be best in class
- Whatever you are spending on cyber security is not enough!
  - *“Clients are investing in security to provide them with a competitive advantage.”*

Filling the Cybersecurity Skills Gap

Detective Superintendent Michael Gubbins,
Garda National Cyber Crime Bureau,
Harcourt Square,
Harcourt Street,
Dublin 2,
D02 DH42

Tel: +353 1 6663708

Email: gccb.districtoffice@garda.ie

Cybersecurity Skills Initiative (CSI)

James B Alvilhiera

World Wide Sales Leader & Cyber Security Expert, IBM Watson Talent

Technology Ireland ICT Skillnet

Technology Ireland Software Skillnet

Future-proofing Cyber Talent Strategy

Three forces are culminating in unprecedented disruption

- Rapid advancement of digital technologies
- Fundamental disruption of industry value chains and business and operating models
- Increased globalization, social commentary and engagement

This disruption is impacting global skills in three ways

- Demand for and types of skills required by industry are changing
- Availability of skills in labor markets is uncertain
- Quality of skills is being challenged

Leadership in addressing skills challenge has not yet emerged

- Governments have been overwhelmed by the extent and depth of the challenge
- Educational institutions struggle to adapt to changing needs of industry
- Private sector has been underinvesting in necessary engagement and training

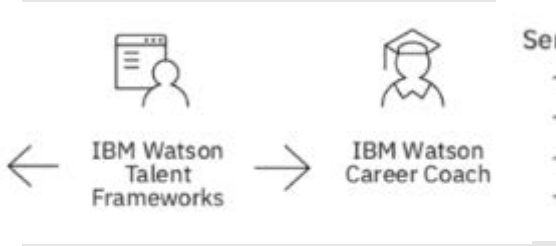
Create a Future-proof Cyber Talent Strategy

- **Find new talent**
- AI-powered recruiting processes can help candidates find you and their fit;
  you find candidates faster, with greater precision

- **Upskill existing talent**
- AI-powered solutions push personalized learning and skills to your people - so they can reinvent fast and continuously

- **Listen and communicate**
- Engagement and sentiment analysis helps you listen and respond to what your people are thinking

Cyber Workforce Strategy

	ATTRACT	ENGAGE	OPTIMIZE	
Critical Skills Shortage				Excess Capacity
High Turn Over				Longevity
Education not keeping pace				Responsive Education
Future of Work	INTEL	OPS	IR	TECH	Future-proof Workforce

Technology Ireland ICT

Skillnet

Challenges for the Higher Education Sector in delivering on the Cyber Security Skills Agenda

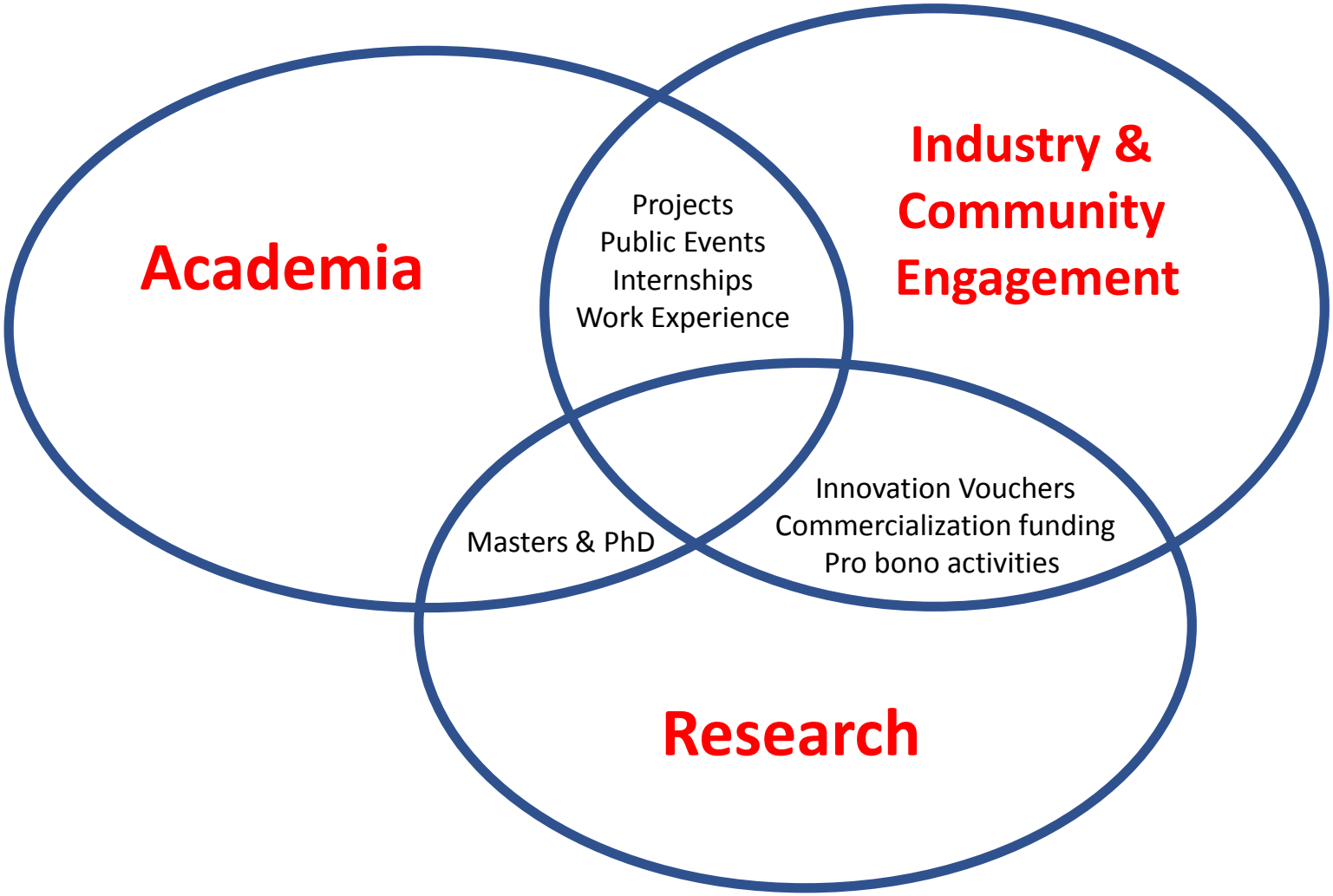
Dr Anthony Keane,

Head of School Informatics and Engineering,

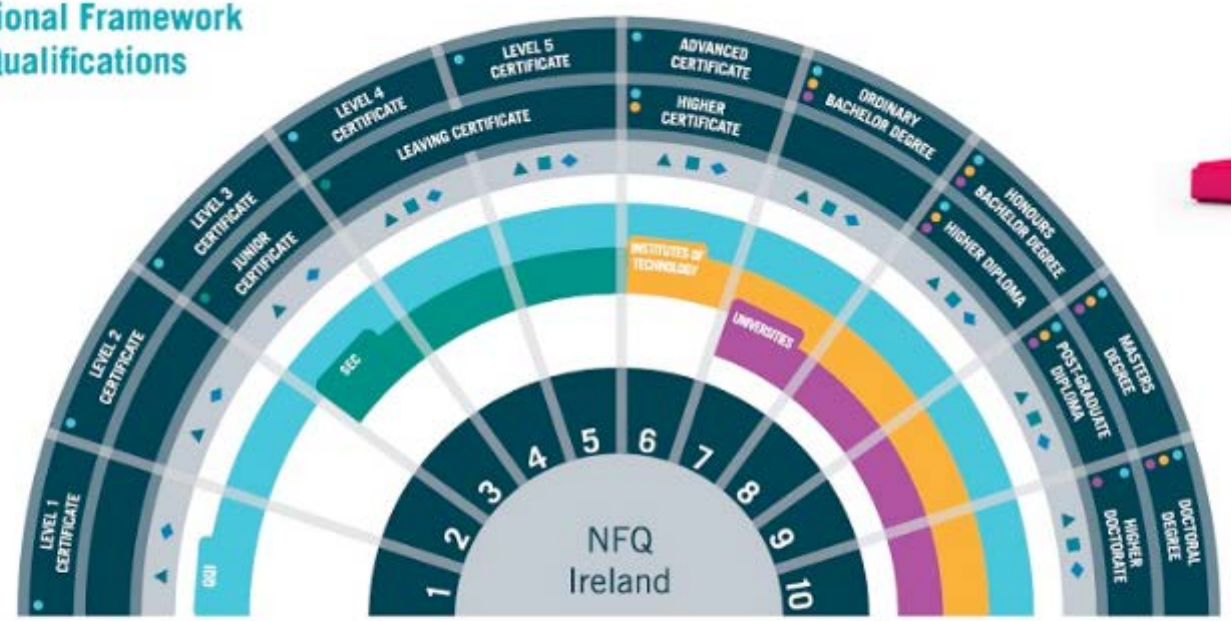
Institute of Technology Blanchardstown

itb Institute of Technology Blanchardstown
Institiúid Teicneolaíochta Baile Bhlainséir


Education is the
key to success


Academia
Industry & Community Engagement
Research
Projects
Public Events
Internships
Work Experience
Masters & PhD
Innovation Vouchers
Commercialization funding
Pro bono activities

National Framework of Qualifications



AWARDING BODIES

- **Quality and Qualifications Ireland** (QQI) makes awards in further and higher education and training
- **SEC - State Examinations Commission** *(Department of Education and Skills)*
- **Institutes of Technology**
- **Universities**

AWARDS IN THE FRAMEWORK

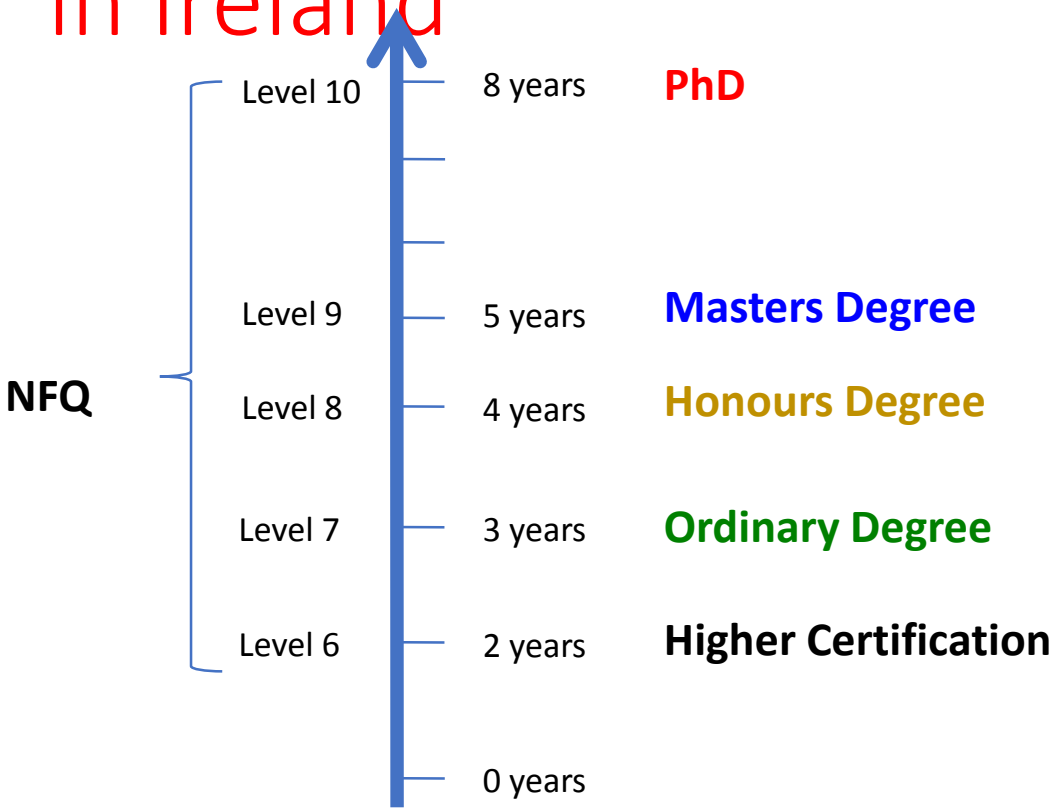
There are four classes of award in the National Framework of Qualifications:

- **Major Awards:** named in the outer rings, are the principal class of awards made at a level
- **Minor Awards:** are for partial completion of the outcomes for a Major Award
- **Supplemental Awards:** are for learning that is additional to a Major Award
- **Special Purpose Awards:** are for relatively narrow or purpose-specific achievement

European Qualifications Framework

For further Information consult: www.nfq.ie www.QQI.ie

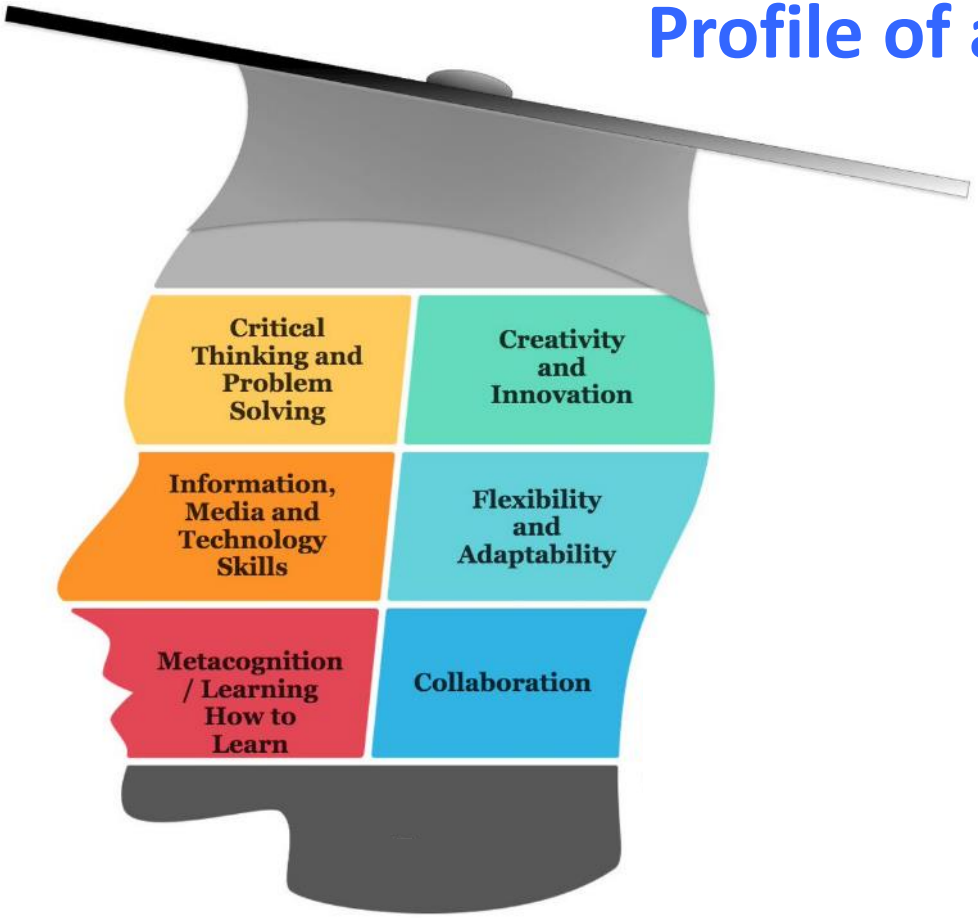
3rd Level Education Structure in Ireland



Types of Degrees and Training

- **Higher Education ICT Courses**
  - Computer Science (level 8)
  - Computer Engineering (level 8)
  - Applied Computer Science
    - Certification Level Courses (level 6)
    - Ordinary Degree Level Courses (level 7
- Awarding Bodies
  - Universities (7)
  - Dublin Institute of Technology (DIT) -> *Technological University Dublin (8th)*
  - Quality & Qualifications Ireland (QQI)
- **Industry Certification Courses**
  - Short, intensive, narrow, shallow, material focused

Profile of a Graduate



Core Computer Technical Skills
level 6

Sample Content

- Computer & Network Infrastructure
- Software Development
- Web & Mobile Technologies
- Personal & Professional Development

Cyber Security Ordinary Degree
Level 7

- Digital Forensics
- Secure Communication
- Penetration Testing
- Network Security

+ Group Project

Cyber Security Honours Degree
Level 8

- Business Continuity Management
- Cloud Security
- Threat Intelligence & Incident Response
- Secure Coding

+ Individual Project

Cyber Security Master's Degree
Level 9

Risk Assessment & Management
Security Intelligence
Application Security
Advanced Network Security Analytics

+ Research Project

What is the Problem?

Cybersecurity is considered an interdisciplinary domain.

"cybersecurity is not a clearly demarcated field of academic study that lends itself readily to scientific investigation. Rather, ***cybersecurity combines a multiplicity of disciplines*** *from the technical to behavioural and cultural. Scientific study is further complicated by the* ***rapidly evolving nature of threats****, the difficulty to undertake controlled experiments and the* ***pace of technical change and innovation****. In short, cybersecurity is much more than a science"*

High Level Advisory Group of the EC Scientific Advice Mechanism 2017

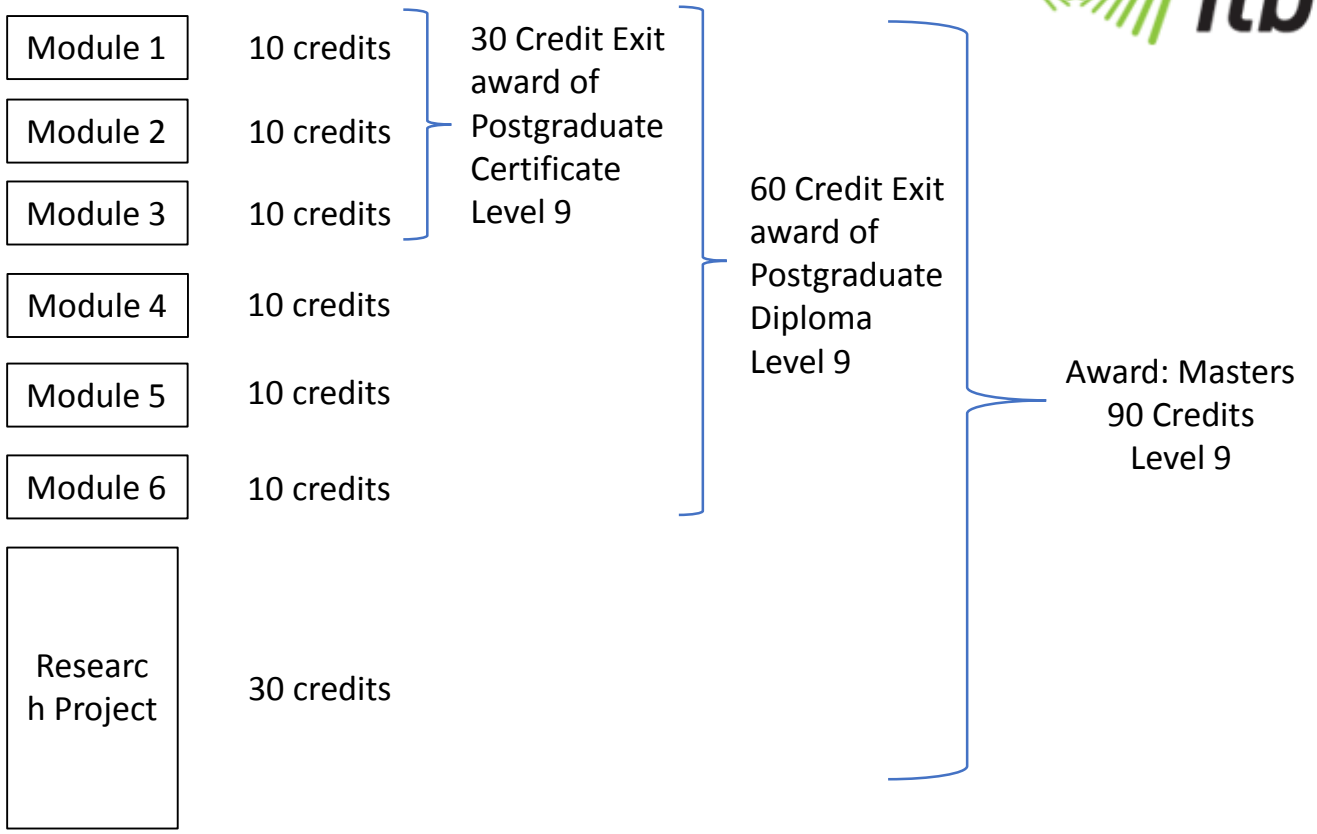
Technology Ireland ICT Skillnet - MSc in Applied Cyber Security

- Engagement with Industry on Course Design and Delivery
- **Conversion Masters**: For graduate computing or related discipline bu Cyber Security knowledge.
  - Digital Forensics
  - Secure Communications & Cryptography
  - Network Secu
  - Cyber Crime I...
  - Business Continuity Management
  - Research Skills & Ethics

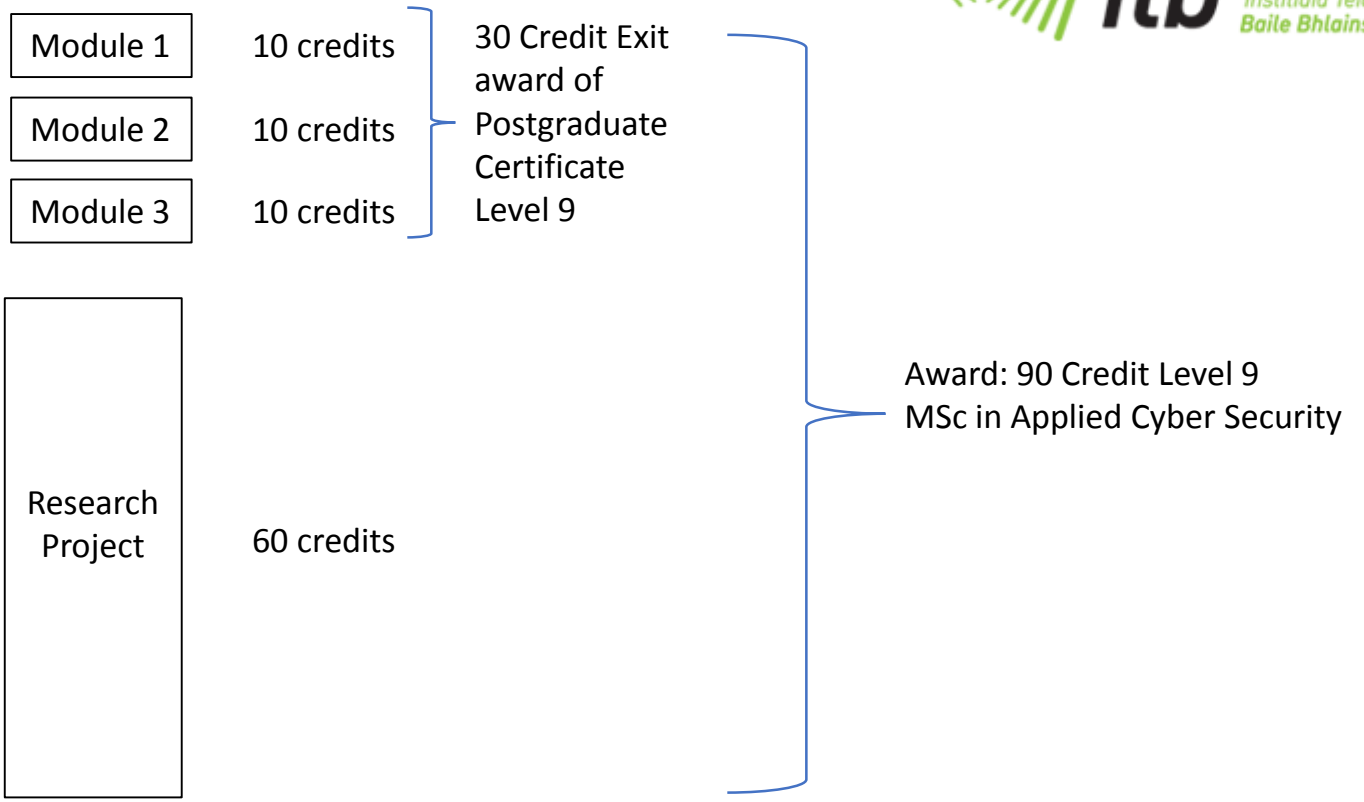
Technology Ireland ICT Skillnet

itb Institute of Technology Blanchardstown Institiúid Teicneolaíochta Baile Bhlainséir

Structure1 of Masters (60/30 model)



Structure2 of Masters (30/60 model)



Students can select from the following list of modules:

- Network Security
- Cyber Crime Malware
- Business Continuity Management
- Secure Communications & Cryptography
- Digital Forensics
- Biometrics
- Secure Programming
- Financial Fraud
- Application Security
- Security Intelligence
- Research Skills & Ethics

Challenges for HEIs

- Preserving that quality and integrity of academic processes
- Managing expectations
- Close working partnership with industry on needs
- Courses for the non-ICT technical as well as ICT-technical
- Single subject awards and minor awards as well as major awards
- Rapid validation of new courses and update of content on existing courses
- Integration of industry recognized certifications and CPD points
- Access - Recognition of Prior Learning

Deloitte.

Cybersecurity Primer for CEOs

What to know so you know what to do

Liam O'Connor

Contents

What this workshop will cover

- Why cybersecurity is a business issue not just an IT issue
- Necessity of investing in security awareness training
- What cybersecurity technologies to deploy
- Cost-benefit analysis of investing in cybersecurity prevention measures
- Outsource or build in-house capability
- Encouraging vulnerability reporting by staff at every level
- How to manage recovery after an attack and adapt future processes
- Risk of being too slow to detect and respond

Why cybersecurity is a business issue …

… Not just an IT issue

Current events and the **cyber threat landscape**

Cybercrime is "the **greatest threat** to every profession, every industry, every company in the world"

(Source: CLO, IBM Corp)

Equifax announced that **143 million** US-based users had their personal information **compromised** this year.

(Source: The Verge)

Global annual cybercrime costs will grow from $3 trillion in 2015 to $6 trillion annually by 2021, which includes damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

(source: Cybersecurity Ventures)

Worldwide businesses will **spend $101.6 billion on cybersecurity in 2020**, a 38% increase from the estimated $73.7 billion spend in 2016 with the banking sector spending the most.

(source: International Data Corp.)

The average **cost** of a data breach in 2020 will exceed **$150 million by 2020**, as more business infrastructure gets connected.

(source: Juniper Research)

Why cybersecurity is a business issue …

… Not just an IT issue

Political

Political interference

Encryption

Into the wild – Powerful technical exploits

Offensive capability

Legal

Wave of regulation

GDPR (General Data Protection Regulation)

NIS Directive (Directive on security of network and information systems)

Privacy Shield

Economic

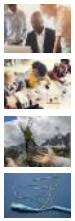
Trust is priceless

Attacks become destructive

Cyber risk remains difficult to price

Cybercrime as a Service

Social



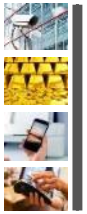
People still matter

Diversity is needed

Trust is essential

Perceptions of privacy

Technological

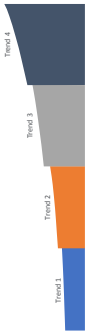


Attack of the things

Ransomware is lucrative

Smartphones become ubiquitous

Fintech spreads



These trends are evolving at the same time as cross-sector demand is growing for security advisory, delivery and managed services capabilities. While some demands are common to all industry sectors, others vary widely between sectors, geographies, and regulatory regimes.

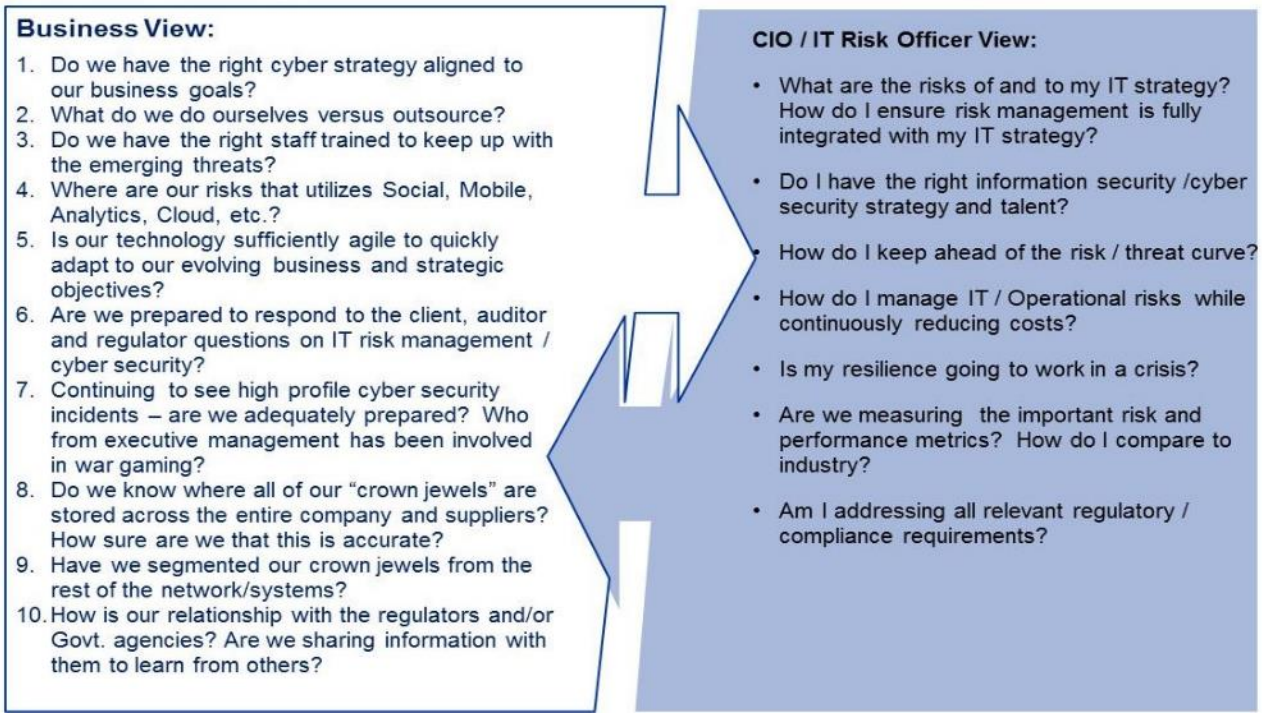
Leading organisations are responding by investing in cyber transformation programmes, talent acquisition and retention, and security innovation – with particular emphasis on threat intelligence, security operations and red-teaming.

Source: Navigating Cyber Risk – Executive Briefing, December 2017

Why cybersecurity is a business issue …

… Not just an IT issue

Maturity of risk management practices should be proportionate to the risks present based on the business, industry, size and complexity of an organisation



Why cybersecurity is a business issue …

… Not just an IT issue

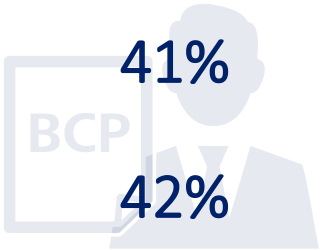
Cyber criminals focusing on business disruption

$450B — Estimates on cost of cybercrime to global economy in 2016 [1]

$4B — Estimates on cost of WannaCry ransomware variant alone [1]

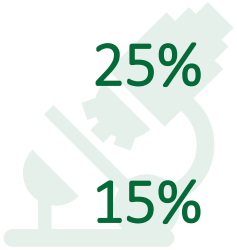
50% — Through 2020, more than 50% of ransomware will specifically target businesses and focus on the disruption of business, rather than the encryption of data [2]

100% — By 2019, despite increasing effectiveness of countermeasures, successful ransomware attacks will double in frequency year over year, up from 2 to 3 million in 2016. [3]



41% — of firms do not have external business partners participate in their BC / DR exercises and tests [4]

42% — of respondents reported not addressing a cybersecurity incident in their BC plan [4]



25% — By 2018, lack of digital IT competence will cause 25% of healthcare payers to lose competitive ranking. [6]

15% — of all consumer-level digital businesses, by 2020, will fail due to inadequate protection against unplanned end-to-end transaction downtime. [5]

[1] Hiscox [2] Gartner "Simple Lessons You Must Learn from WannaCry" 29 June 2017 [3] Gartner "Predicts 2017: Business Continuity Management and IT Service Continuity Management" 15 November 2016 [4] Forrester "The State Of Business Continuity 2015: Planning, Maintenance, And Exercises" – October 2015 [5] Gartner "Predicts 2015: Business Continuity Management and IT Disaster Recovery Management" 26 November 2014 [6] Gartner "New Digital Business Skills Required to Leverage Modern Healthcare Payer Core Administrative Technologies" 9 June 2017

Necessity of investing in security awareness training

Top 5 reasons

- 1. Weak Link – the human element
- With a number of cyber defences being implemented by companies, the human element is often left exposed.
- Many cyber threats look to exploit this especially through social engineering attacks.
- Investing in a security awareness training not only shows the employees the Dos and Don’ts of IT security such as identifying phishing mail, but also shows them how to safeguard against more advanced attacks such as social engineering.
- Security awareness training also makes employees more aware about their surroundings and enforces that cybersecurity is everyone’s responsibility.

Necessity of investing in security awareness training

Top 5 reasons

- 2. Better Culture – more accountability
- Being better informed creates a better workplace culture.
- By establishing cybersecurity as a priority, employees can help keep each other accountable for best practices and support each other in safe technology use.
- Employees will feel more responsible when interacting with technology and will in turn be conscious of the attacks that could happen.

Necessity of investing in security awareness training

Top 5 reasons

- 3. Compliance
- Legislation such as Sarbanes-Oxley 404, EU General Data Protection Regulation, PCI-DSS, etc. requires security awareness training to be implemented for organisations in scope.
- Also, organisations aiming to get certified with industry standards such as ISO 27001, COBIT, NIST 800 or CIS, need to establish a security awareness program.

Necessity of investing in security awareness training

Top 5 reasons

- 4. Cost effective
- Combining well informed employees with a cybersecurity-conducive culture will be cost effective.
- Data breaches can be expensive and having a team that is prepared to prevent them is key.
- Security awareness training is an investment as any cost incurred as part of the training can prevent much larger costs down the line.

Necessity of investing in security awareness training

Top 5 reasons

- 5. Save Time
- Having security-aware users does not always mean less incidents, but since they would know what constitutes a security incident and how to report it, detection times could significantly reduce.
- A significant number of incidents could be prevented with increased awareness and even the ones that occur would have a better response.

Which cybersecurity technologies to deploy?

End Point Security

Endpoint security or endpoint protection is an approach to the protection of computer networks that are remotely bridged to client devices. The connection of laptops, tablets, mobile phones and other wireless devices to corporate networks creates attack paths for security threats.
Endpoint security attempts to ensure that such devices follow a definite level of compliance to standards.

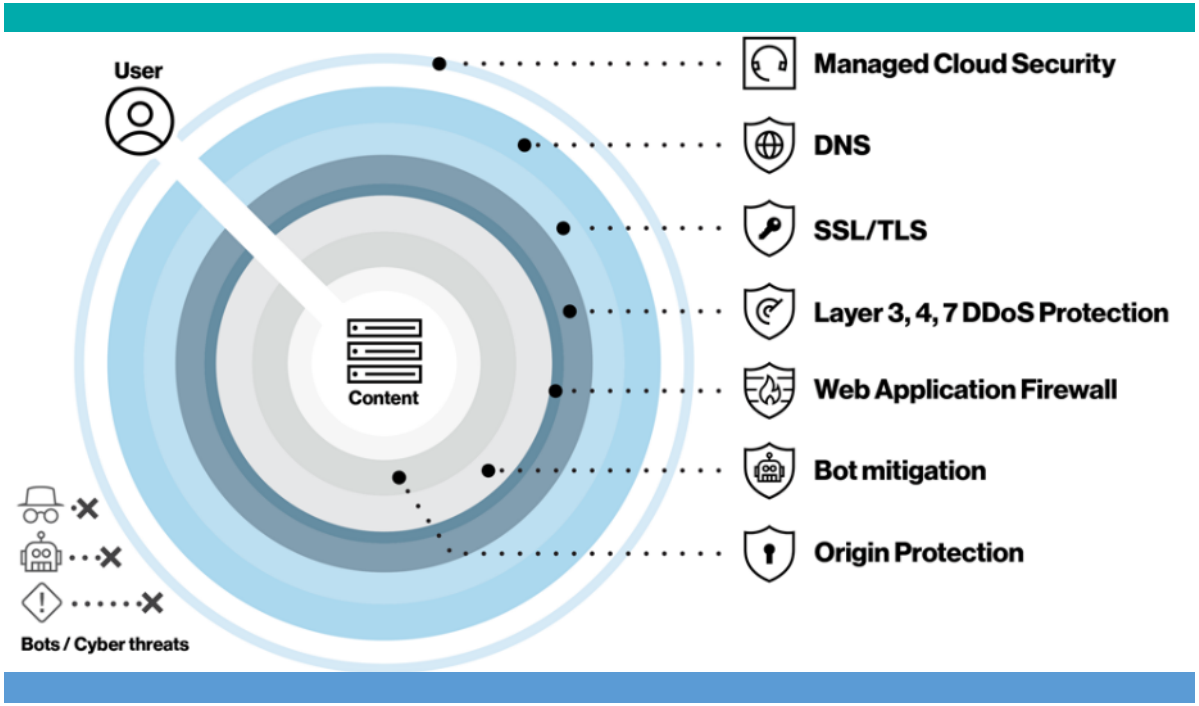
Data loss prevention	• **Data loss prevention** (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what **data** end users can transfer.
Web filtering	• A **Web filter** is a program that can screen an incoming **Web** page to determine whether some or all of it should not be displayed to the user. The **filter** checks the origin or content of a **Web** page against a set of rules provided by company or person who has installed the **Web filter**.
Anti virus solution	• **Antivirus software**, or anti-virus software (abbreviated to AV), also known as anti-malware, is a computer program used to prevent, detect, and remove malware. • These solutions are installed on every endpoints (laptops, desktops, mobile devices) and cater to the detection and prevention of threats.
Mobile device management	• **Mobile device management (MDM)** is an industry term for the administration of mobile devices, such as smartphones, tablet computers, laptops and desktop computers. MDM is usually implemented with the use of a third party product that has management features for particular vendors of mobile devices.
Encryption - Bitlocker	• **Encryption** is the process of encoding a message or information in such a way that only authorised parties can access it and those who are not authorised cannot. Encryption does not itself prevent interference, but denies the intelligible content to a would-be interceptor. For endpoints, Bitlocker must be installed.

Which cybersecurity technologies to deploy?

Cloud Security - Defence in Depth

Cloud computing security is a fast-growing service that provides many of the same functionalities as traditional IT security. This includes protecting critical information from theft, data leakage and deletion.

Cloud computing and storage provides users with capabilities to store and process their data in third-party data centers. Organizations use the cloud in a variety of different service models (with acronyms such as SaaS, PaaS, and IaaS) and deployment models (private, public, hybrid, and community). Security concerns associated with cloud computing fall into two broad categories: security issues faced by cloud providers and security issues faced by their customers (organizations who host applications or store data on the cloud).



Which cybersecurity technologies to deploy?

Security Information Event Management (SIEM)

A SIEM (Security Information and Event Management) is the key tool which provides the security team with an overview of the organisations security solution.

SIEM	Benefits
Real-time incident response	• Aggregated information from multiple systems provides an overview of organisation security on an easy-to-use dashboard • Ultimately means security teams can handle issues quicker and speeds containment reducing the damage that security breaches will cause
Streamlined compliance reporting	• Systems from across the organisation which require information requisite for compliance reporting provide logs and incident reports to the SIEM which creates a single rich and customisable report • Built in support for common compliance requirements such as HIPAA, PCI DSS and GDPR
Detect the undetected	• SIEM systems will detect issues that traditional security systems may miss, they have built in detection capabilities along with the ability to analyse the logs created by security incidents. • Reduces the likelihood of data breaches and helps the security team gain insight into the cause and mitigating solution after incidents occur

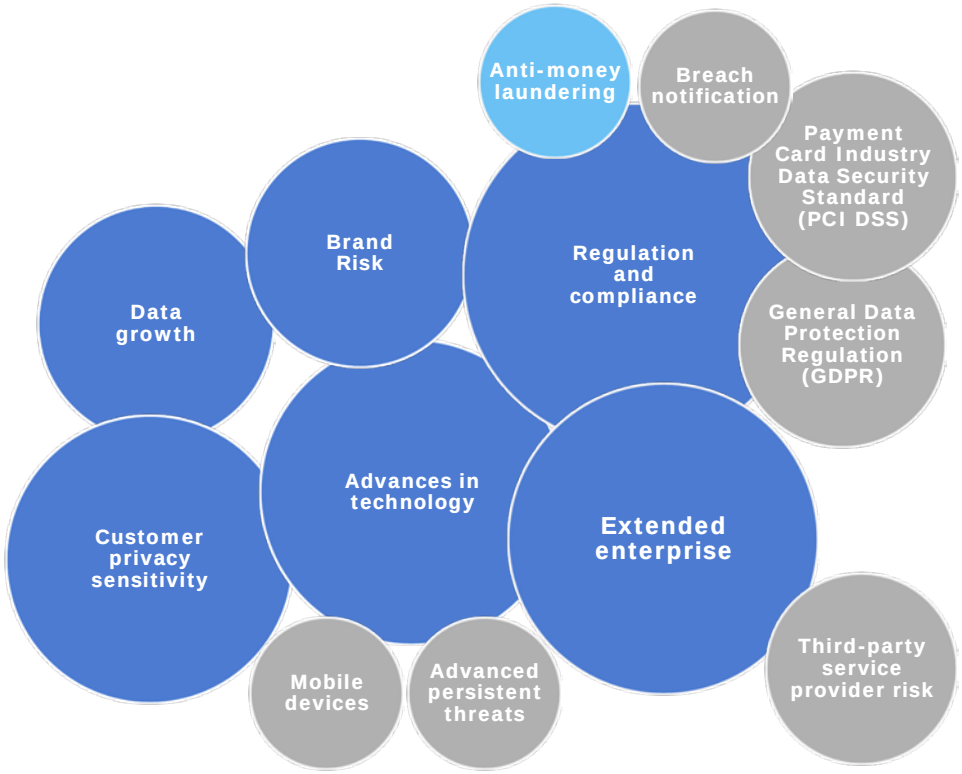
Which cybersecurity technologies to deploy?

Data Loss Prevention (DLP)

Data loss prevention software detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring, detecting and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage).

Quick wins of implementing a DLP solution:

- Ensure compliance
- Maintain integrity of data
- Secure data transfer
- Data protection



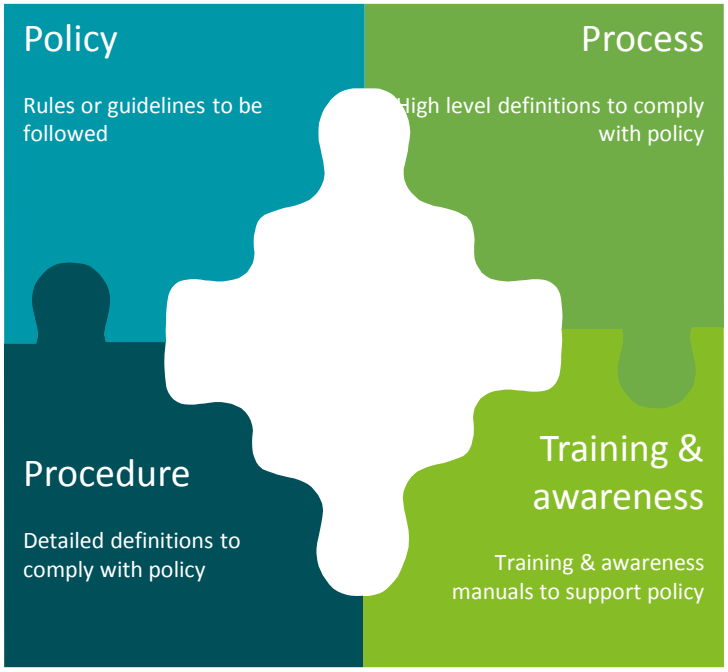
Cost-benefit analysis of investing in cybersecurity prevention measures

Defence in Depth

Technology Tool/ Service	Cost Estimate	Benefits
Data Encryption		
Data Backup		
Data Loss Prevention		
Remote Access		
Firewalls		
Network Access Control		
Intrusion Prevention System (IPS)		
Intrusion Detection System (IDS)		
Anti-virus		
Penetration Testing		
Vulnerability Scanning Tool		
Patch Management Tool		
Privileged User Access Management/ Identity Access Management		
Managed SOC		
Credential Vault		
Physical Security		
Security Incident and Event Management Tool		
Asset Management Tool		
Cloud Security		

Cost-benefit analysis of investing in cybersecurity prevention measures

Policies, processes, procedures and training and awareness programmes for employees help create an internal control framework within an organisation. Management uses this internal control framework to rely upon and ensure that the organisation's objectives are being met.

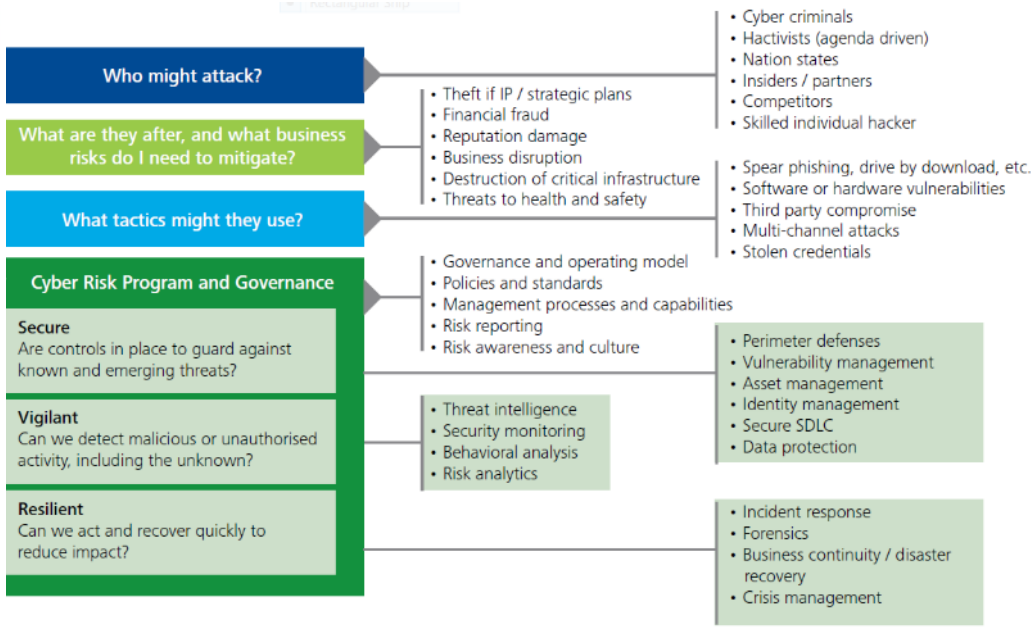


Cost-benefit analysis of investing in cybersecurity prevention measures

There are many different facets to understanding the role of the Board in defending the organisation from a cyber threat. Two of these facets are presented below.

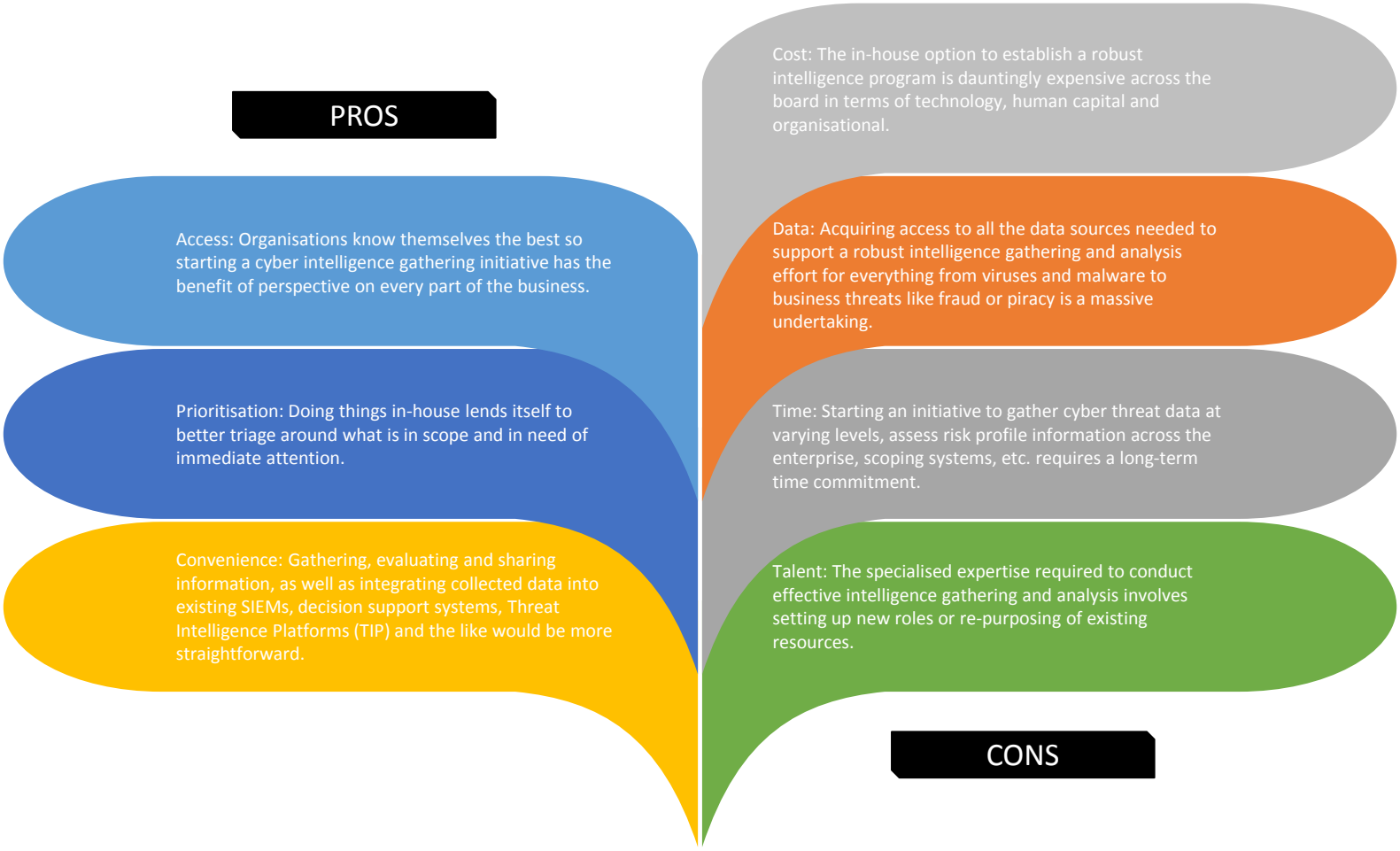
3 lines of defence

Cybersecurity plan



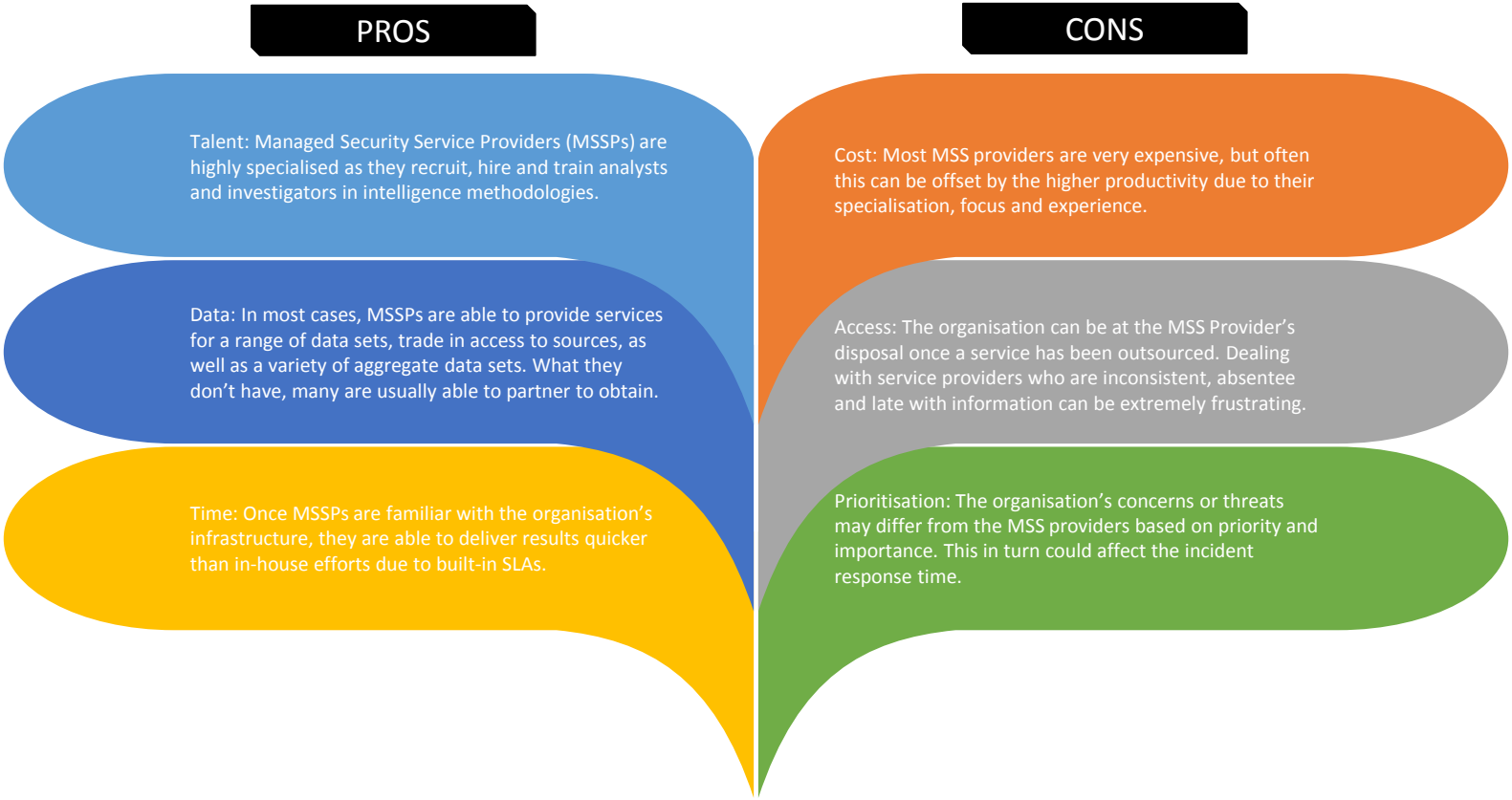
Outsource or build in-house capability

In-House



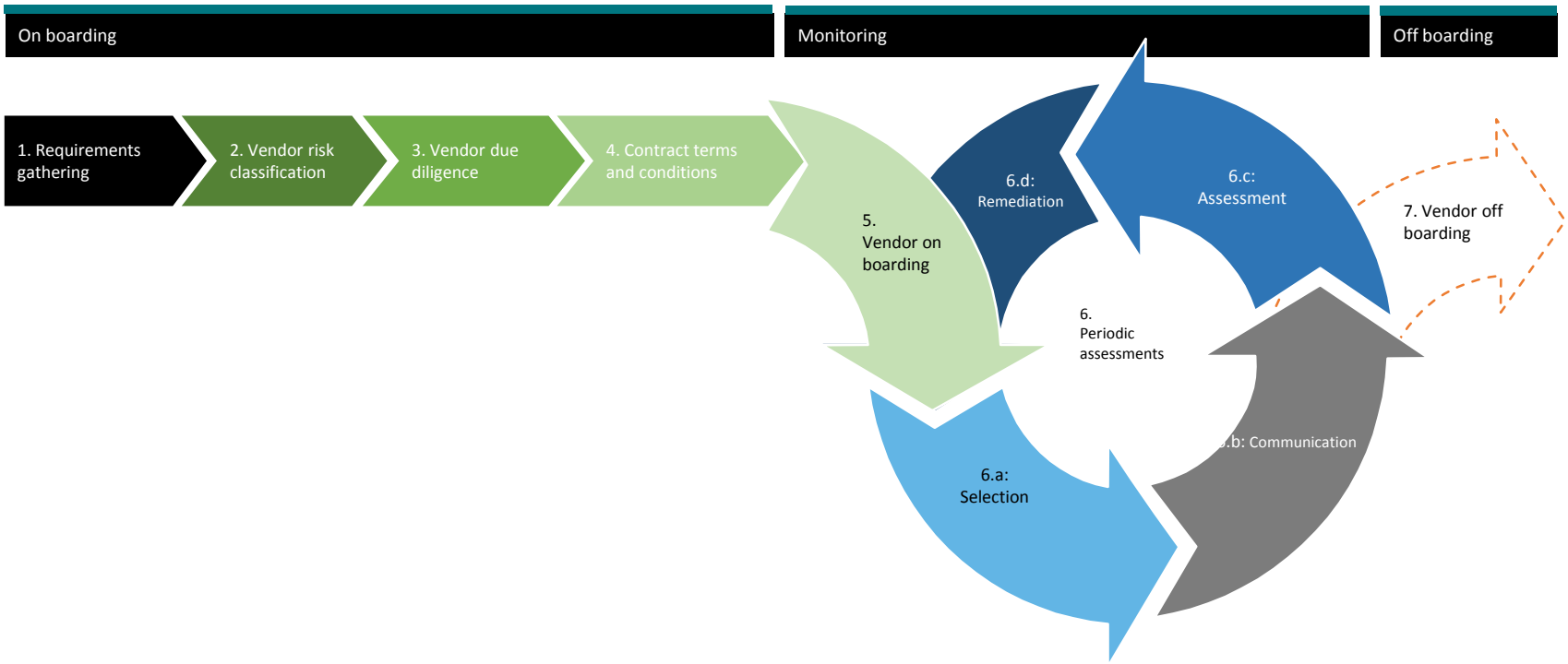
Outsource or build in-house capability

Outsourced



Outsource or build in-house capability

Outsourcing – an effectively managed approach



Encouraging vulnerability reporting by staff at every level

Cyber risk discussions take place at the board and C-suite level

Described and operationalise roles and responsibilities across the cyber risk program

Cyber leader should have the right mix of technical and business acumen to understand how the organisation operates, to engage with the business, and to know where to prioritise efforts

Compensation and total reward programs are in-line with industry and risk profile/ importance to the organisation

Teams of passionate and energised staff stay up-to-date on the latest cyber trends, threats, and implications for their business

Key risk and performance indicators exist, and processes are in place to escalate breaches of limits and thresholds to senior management for significant or critical cyber incidents

Encouraging vulnerability reporting by staff at every level

Strong tone at the top. The board and C-suite promote a strong risk culture and sustainable risk/return thinking

People's individual interests, values, and ethics are aligned with the organisation's cyber risk strategy, appetite, tolerance, and approach

Executives are comfortable talking openly and honestly about cyber risk using a common vocabulary that promotes shared understanding

Company-wide education and awareness campaign established around cyber risk (all employees, third parties, contractors, etc.)

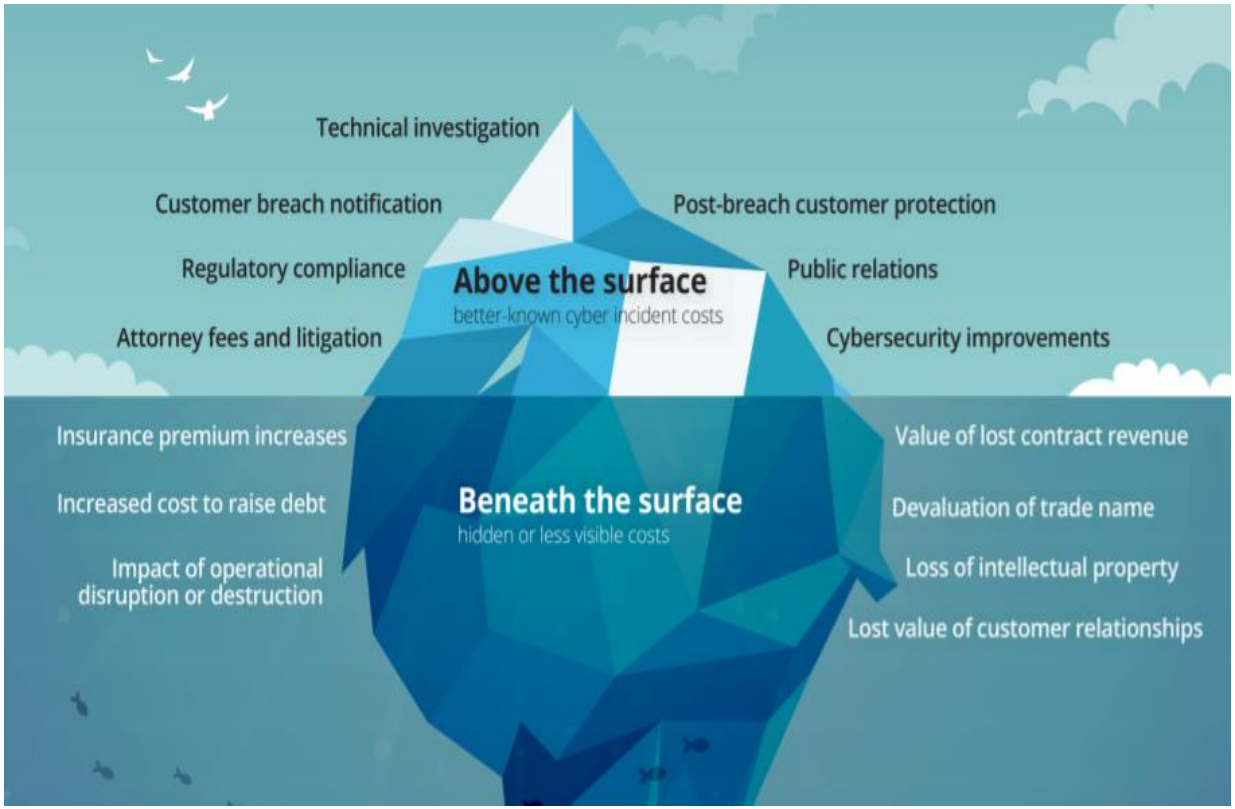
Awareness and training specific to individual job descriptions helps staff understand their cyber responsibilities

People take personal responsibility for the management of risk and proactively seek to involve others when needed

How to manage recovery after an attack and adapt future processes

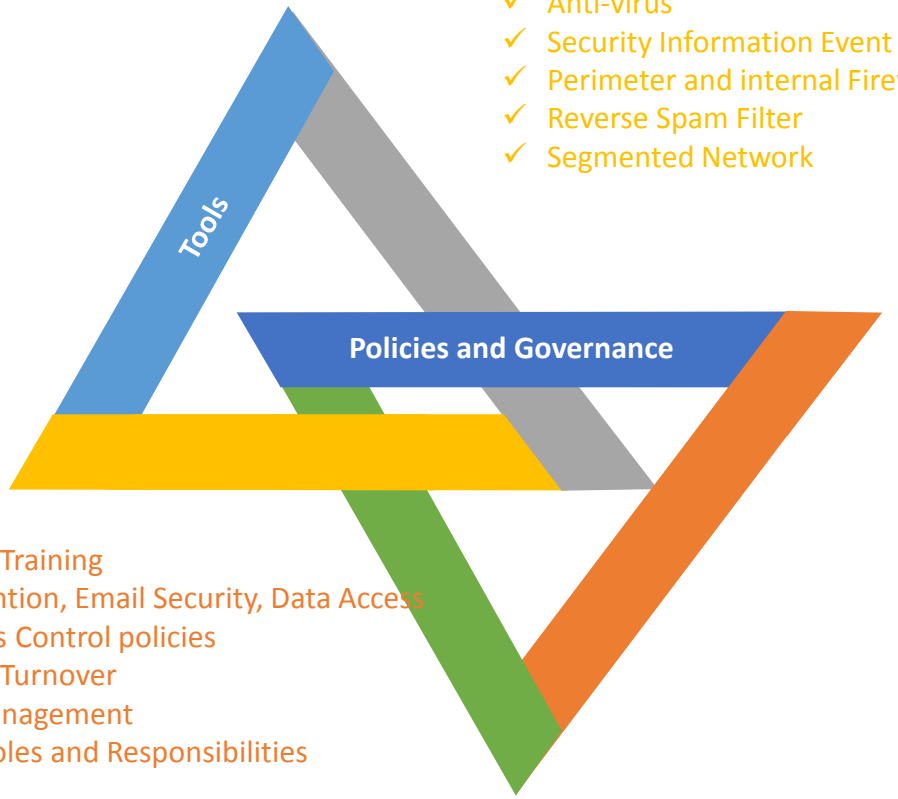
Impact of Incidents

- Loss of client data
- Loss of Intellectual Property
- Reputational damage
- Loss of business
- Time lost to rebuild/ repair affected systems



Mitigation Strategies

How to manage recovery after an attack and adapt future processes



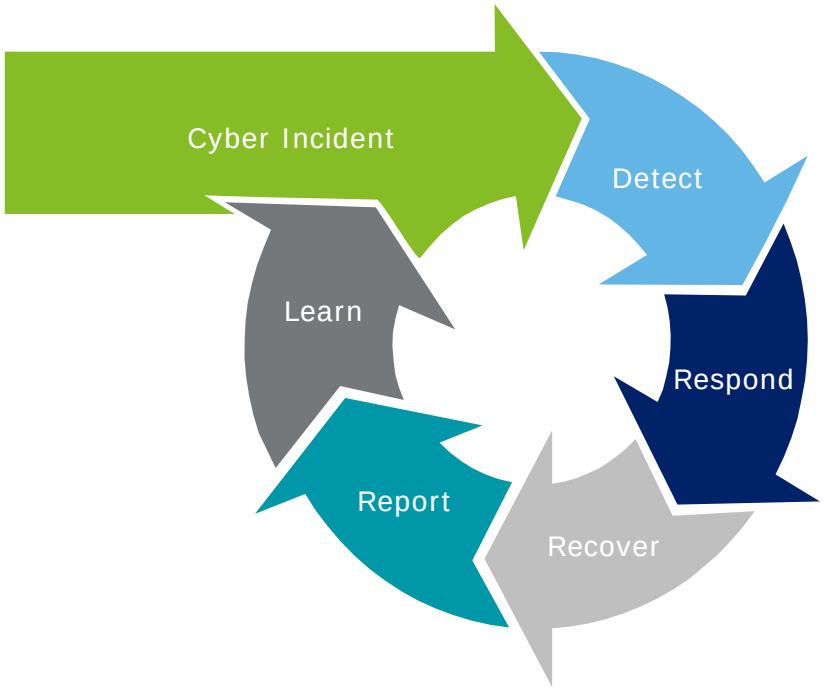
- ✓ Anti-virus
- ✓ Security Information Event Manager (SIEM)
- ✓ Perimeter and internal Firewalls
- ✓ Reverse Spam Filter
- ✓ Segmented Network

- ✓ Employee Training
- ✓ Data Retention, Email Security, Data Access and Access Control policies
- ✓ Employee Turnover
- ✓ Device Management
- ✓ Defined Roles and Responsibilities

How to protect the data

How to manage recovery after an attack and adapt future processes

- Convene the right team.
- Manual/Automated detection.
- Invoke Disaster recovery/ alternate processing.
- Cleanse systems.
- Restore and recover (could take days or months depending on nature of attack).
- Establish communication channels.
- Redefine “readiness” and build incident response plans that facilitate faster and more effective recovery.
- Prepare and practice for the next incident.



Risk of being too slow to detect and respond

In December 2013, Target disclosed that it was victim to the world-largest data breach which affected more than 100M customers

One of Target's 3rd parties breached via phishing email – credentials stolen to procurement application

Attackers used credentials to breach network, infect Target's POSs & commit largest data breach to date

Vulnerabilities identified – attack detected early enough to avoid breach – risks were neither articulated nor managed appropriately by executive management

Intense & prolific media coverage exposing breach

Loss of consumer confidence & sales; Brand reputation & market confidence damaged

Target's CEO, CIO & Security Officer resign

>90 lawsuits filed against Target by customers & banks - >$61m spent within 3 mos to increase security capabilities

BY THE NUMBERS*

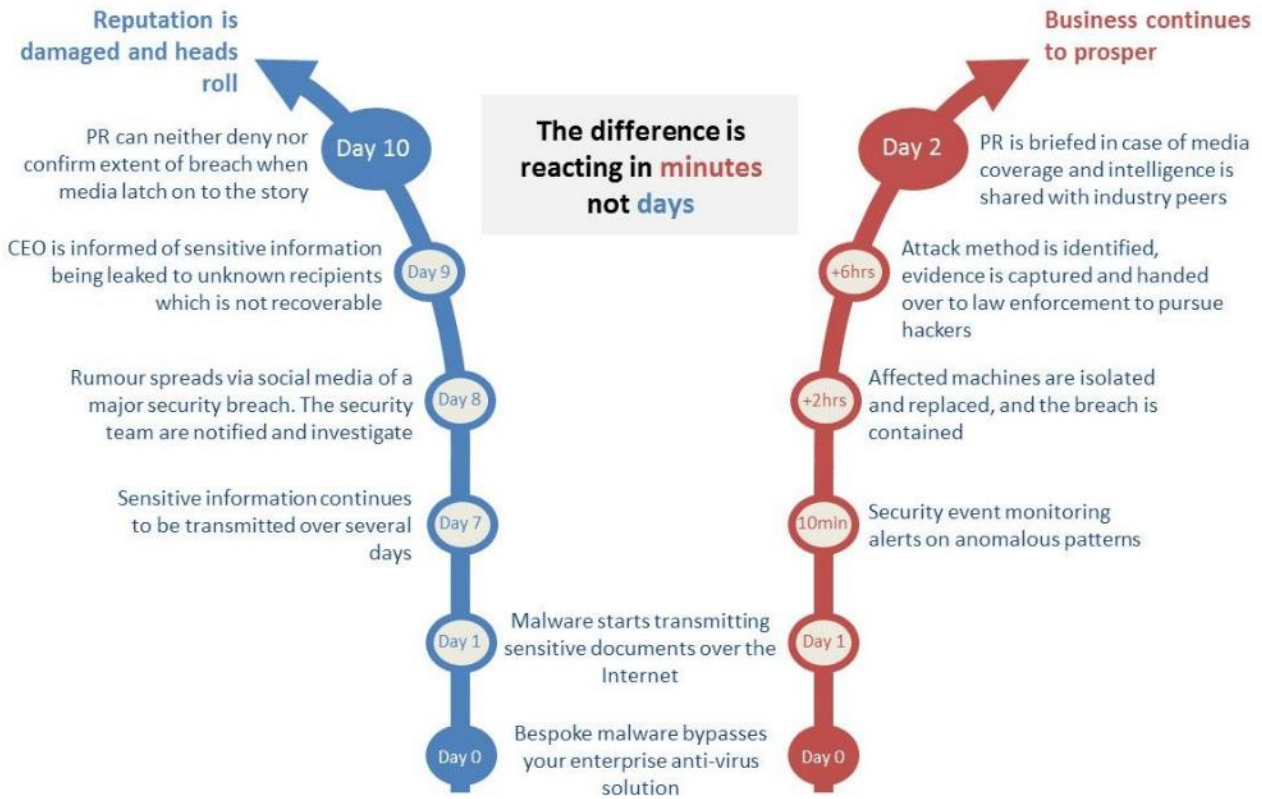
70M	Number of credit card numbers affected
$148M	Current cost of Target's data breach
$0.78	Drop in earnings reflecting more cautious consumer spending
1 Year	Time Target will provide free credit screening services to any customers affected
$1B	Forrester Research's forecasted total cost to Target resulting from breach

ESSENTIAL TRUTHS

The Target breach reiterated several realities:

- No industry is immune & all will be compromised
- Security damages go well beyond dollars
- The speed of attacks are increasing while response times are decreasing
- Monitoring helps to detect and respond faster
- A secure, vigilant & resilient program requires strong governance & risk management

Risk of being too slow to detect and respond



Key Takeaways

Recurring themes across incidents

- Better MONITORING will help detect attacks earlier, or prevent them entirely.
- Adherence to BASIC SECURITY PRINCIPALS can help limit the impact. Weak passwords are often a factor in a breach.
- Stricter VETTING OF THIRD PARTY COMPANIES is necessary to ensure a high standard of security.
- Poor DATA GOVERNANCE is often an issue. Confidential documents or systems should be restricted by ACCESS RIGHTS or ENCRYPTION.
- A culture of minimum adherence to risk mitigation – check box security.
- All alerting information should be thoroughly INVESTIGATED. This can include FORENSIC ANALYSIS of a potentially compromised system.

Risk Assessment For Companies

Brian Honan October 2018

@brianhonan


INDEPENDENT.IE NEWS OPINION BUSINESS SPORT LIFE STYLE ENTERTAIN

Brexit | Irish | World | Technology | Personal Finance | Small Business | FarmIreland | Job

Monday 16 October 2017

Business Newsletter

Business Irish

SuperValu, Centra and Daybreak stores targeted in cyber attack


THE IRISH TIMES

Wed, Sep 13, 2017

NEWS SPORT BUSINESS OPINION LIFE & STYLE CULTURE

Ireland › Irish News

AIB employee loses banking details of 500 customers

Bank notifies Data Protection Commissioner and customers after details are mislaid


Irish Examiner

NEWS SPORT BUSINESS VIEWS LIFE EXAMVIRAL PROPERTY MOTORS

LATEST IRELAND TODAY BUSINESS FARMING WORLD DEATHS W

HOT TOPICS: FORD 100 GARDA COMMISSIONER CORK NOW AND THEN

HOME » TODAY'S STORIES

Concerns over alleged data breaches in Kerry

2

Wednesday, September 13, 2017

ISME Crime Survey 2018

- **26%** experienced computer related crime in the last 12 months
- **12%** of businesses employed an IT manager responsible for security,
- **33%** employed an IT supplier responsible for security
- **98%** would like to see the establishment of a Central/National E-crime body to deal specifically with E-crime

Institute of Directors in Ireland

- **33%** of organisations experienced a cyber breach in the past 2 years with **44%** of organisations selling online have experienced a cyber breach

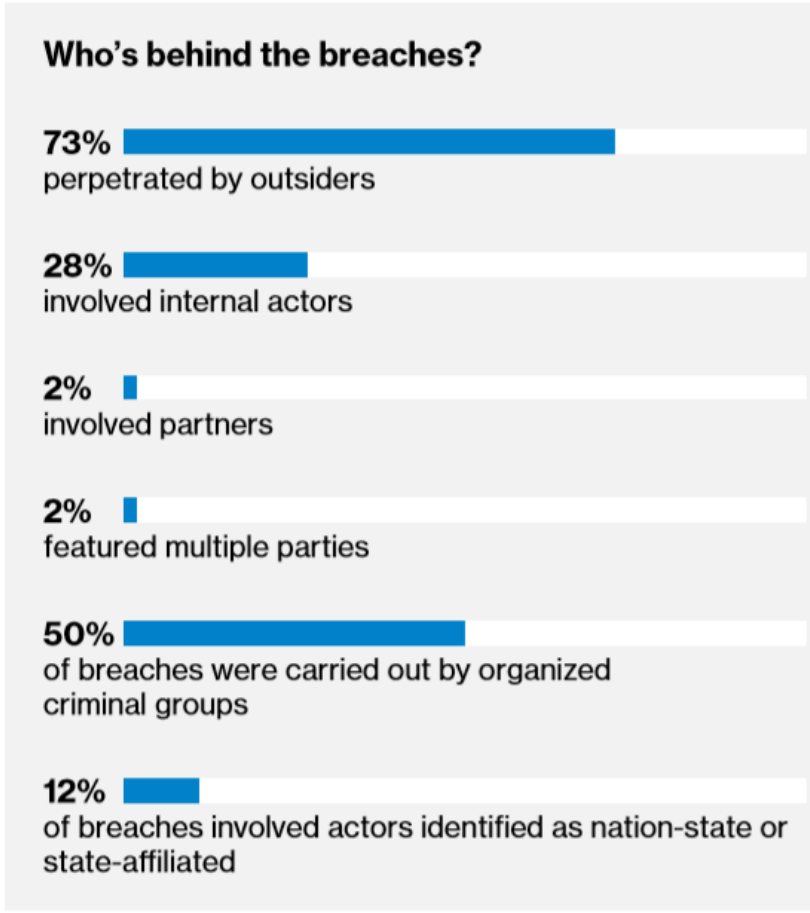
- **84%** of directors say their organisation will increase spending on cyber security measures over the next 3 years

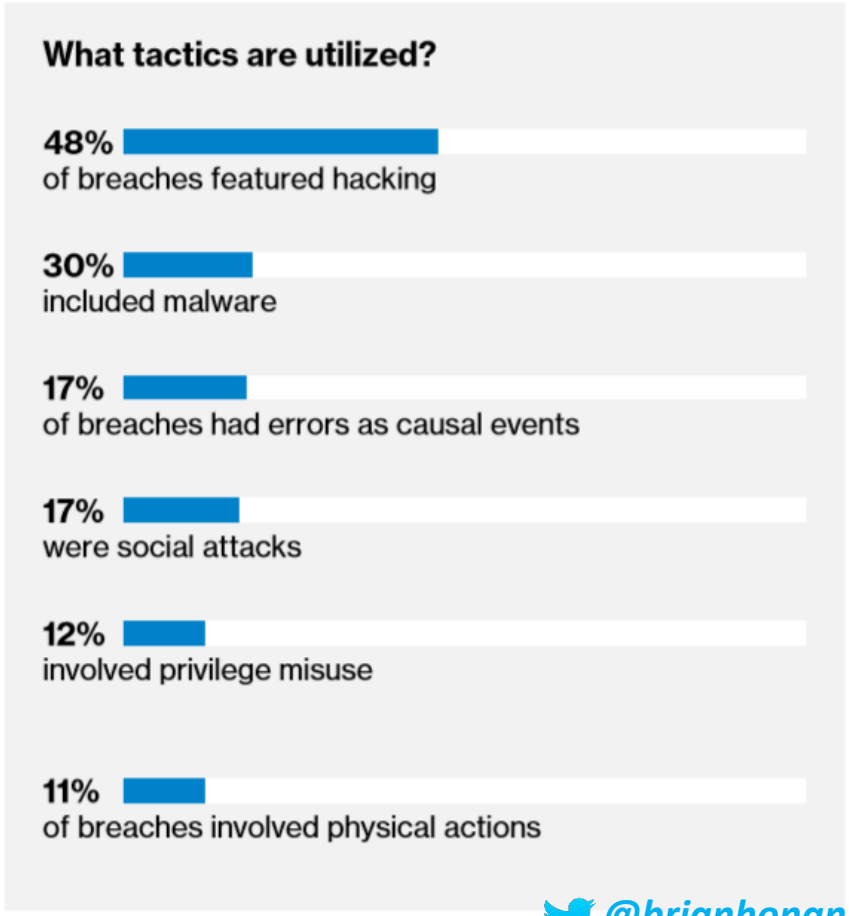
- **69%** of directors claim their organisation is prepared or very prepared for a cyber breach

- **40%** of organisations have **no** formal cyber security strategy

verizon

Summary of findings



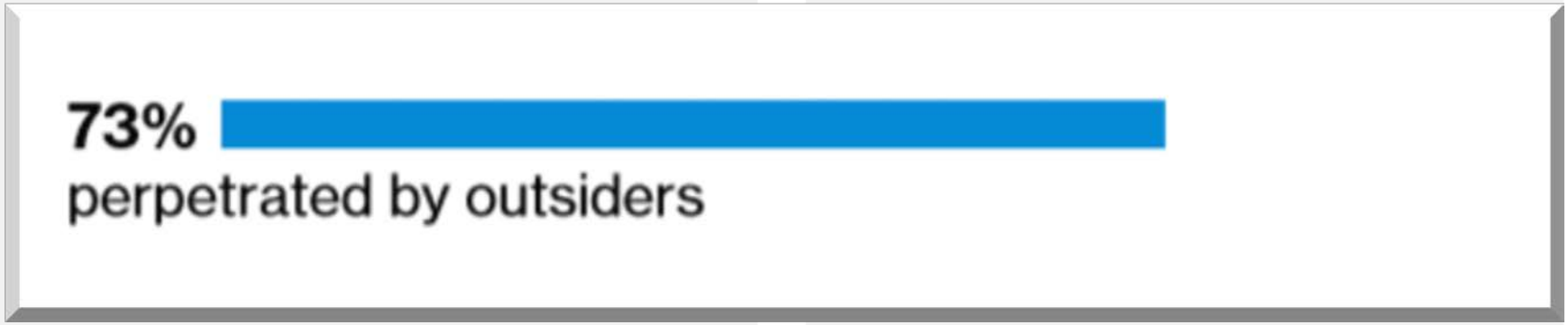


@brianhonan

verizon

Summary of findings

Who's behind the breaches?



2% featured multiple parties

50% of breaches were carried out by organized criminal groups

12% of breaches involved actors identified as nation-state or state-affiliated

What tactics are utilized?

17% were social attacks

12% involved privilege misuse

11% of breaches involved physical actions

@brianhonan

verizon

Summary of findings

Who are the victims?

24%
of breaches affected healthcare organizations

58%
of victims are categorized as small businesses

What are other commonalities?

49%
of non-POS malware was installed via malicious email[1]

advantage (espionage)

68%
of breaches took months or longer to discover

68%
of breaches took months or longer to discover

Root Causes

- Poor Passwords
  - Web Based Email Attacks
- Missing Patches
- Vulnerabilities
  - Web Platforms
  - Out of date software (Windows XP)
- Out of Date Anti-Virus Software
- Lack of Monitoring

@BrianHonan
Brian.honan@bhconsulting.ie
www.bhconsulting.ie

Tommy Barlow
Director Commercial
Sales EMEA, Pluralsight

Richard Harpur
Information Security
Professional, CISM
& Pluralsight Author

Technology Ireland ICT Skillnet

Technology Ireland Software Skillnet

Using the Power of eLearning

Creative Ways To Fill The Skills Gap

Presenters

Tommy Barlow, Pluralsight

Director Commercial Sales EMEA

Richard Harpur, @rharpur

Information Security Professional, CISM & Pluralsight Author

Pluralsight

Who are Pluralsight?

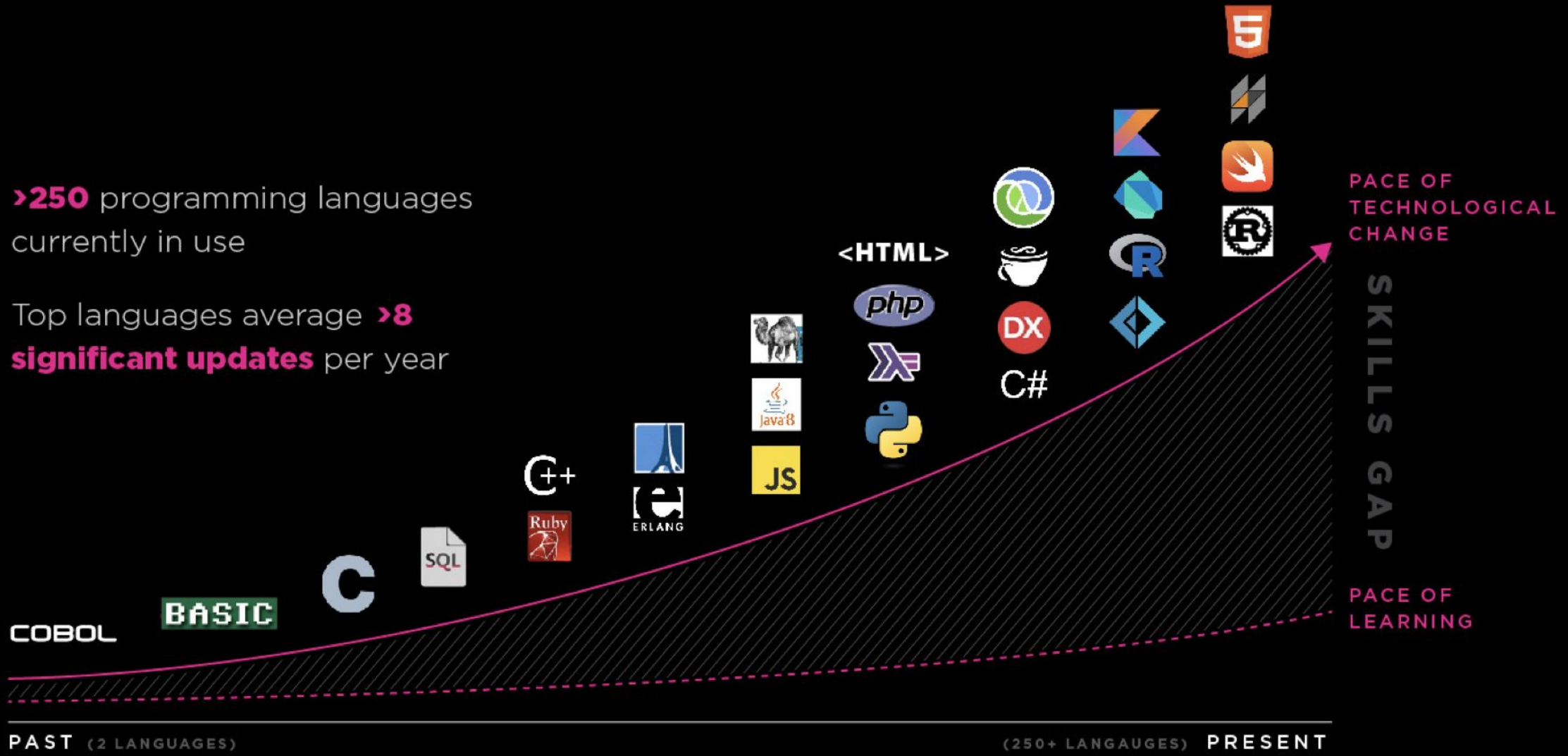
Technology Learning Platform

- Assessment of Skills
- Scale
- Bringing the experts to you (when you need them)

Businesses face a massive **technology skills gap**

>250 programming languages currently in use

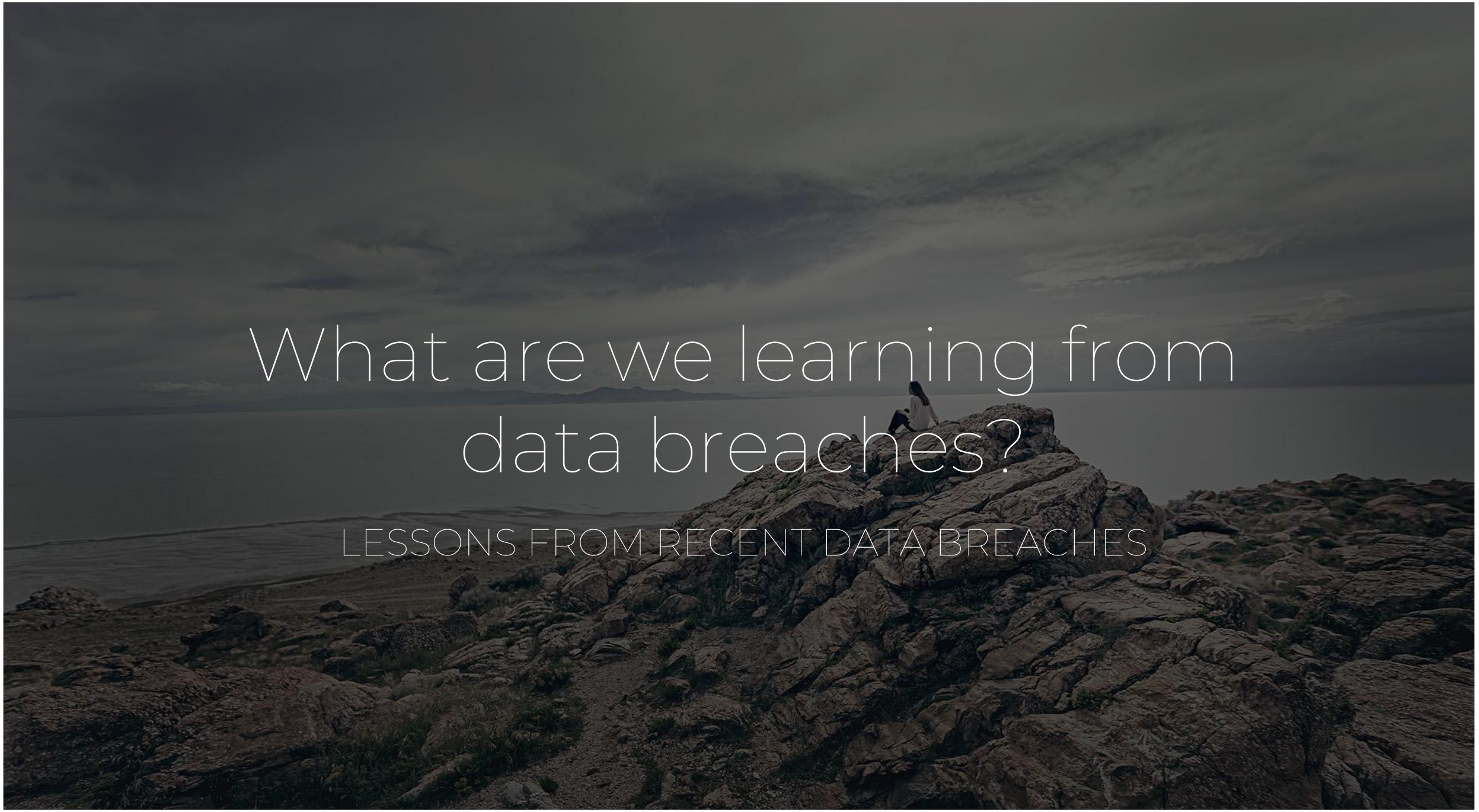
Top languages average **>8 significant updates** per year




Developing technology
skills at scale is the
superpower of the future


Your technology strategy
shouldn’t come from a classroom


1,390+ authors
~10% acceptance rate for new authors
~18 years of professional experience per author
~80 new courses published each month

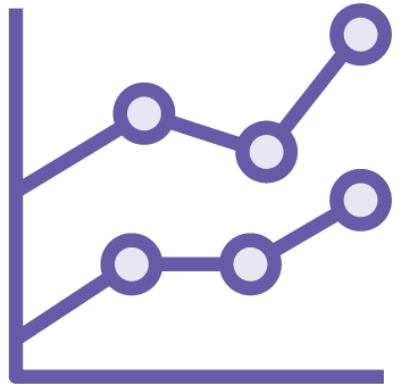

What are we learning from data breaches?
LESSONS FROM RECENT DATA BREACHES

Take Stock

How is cybersecurity evolving

History Books

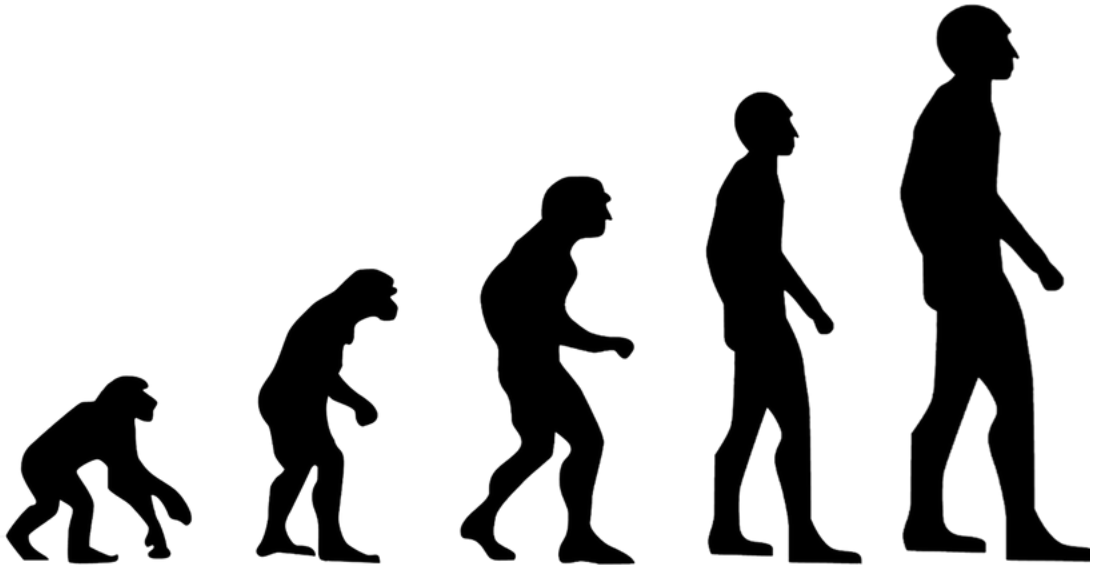
What can we learn from previous experience



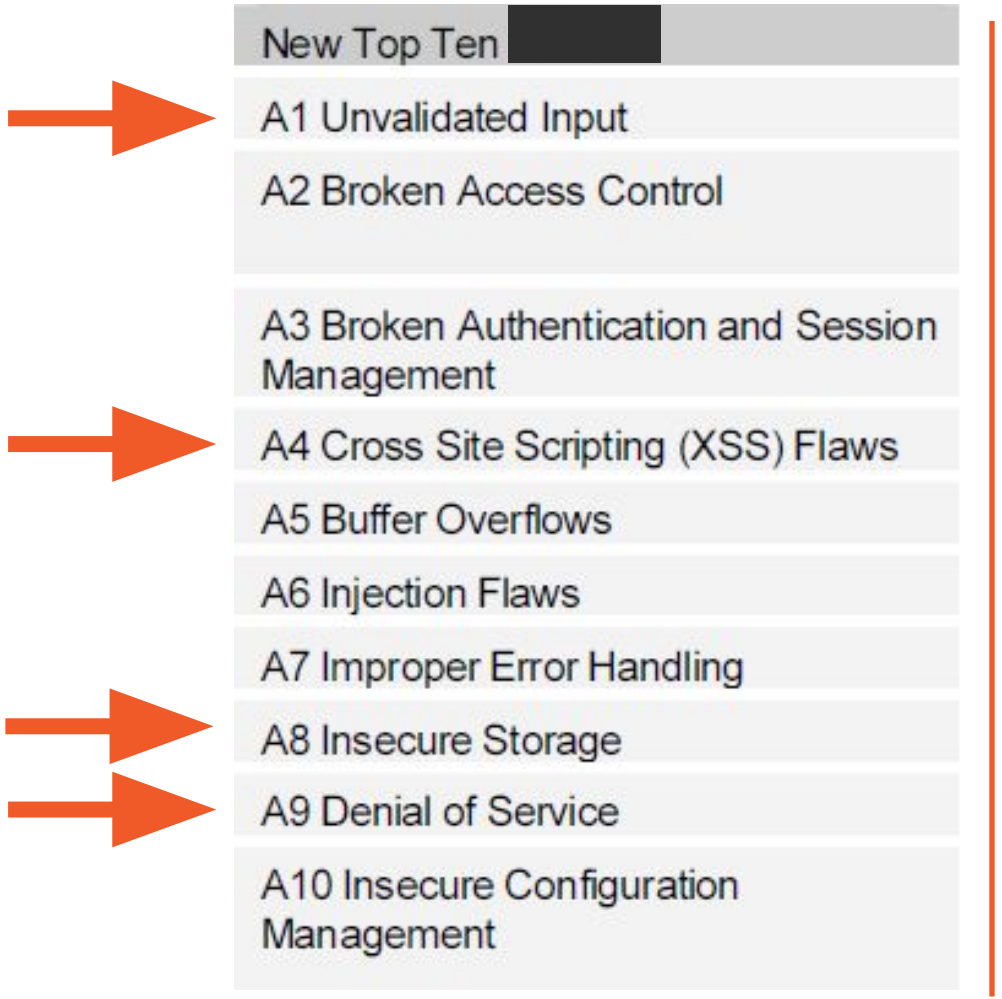
Going Forward

Techniques to lock-in gains and improve skills going forward

So How Well is Cybersecurity Evolving?



OWASP Top 10


New Top Ten
A1 Unvalidated Input
A2 Broken Access Control
A3 Broken Authentication and Session Management
A4 Cross Site Scripting (XSS) Flaws
A5 Buffer Overflows
A6 Injection Flaws
A7 Improper Error Handling
A8 Insecure Storage
A9 Denial of Service
A10 Insecure Configuration Management

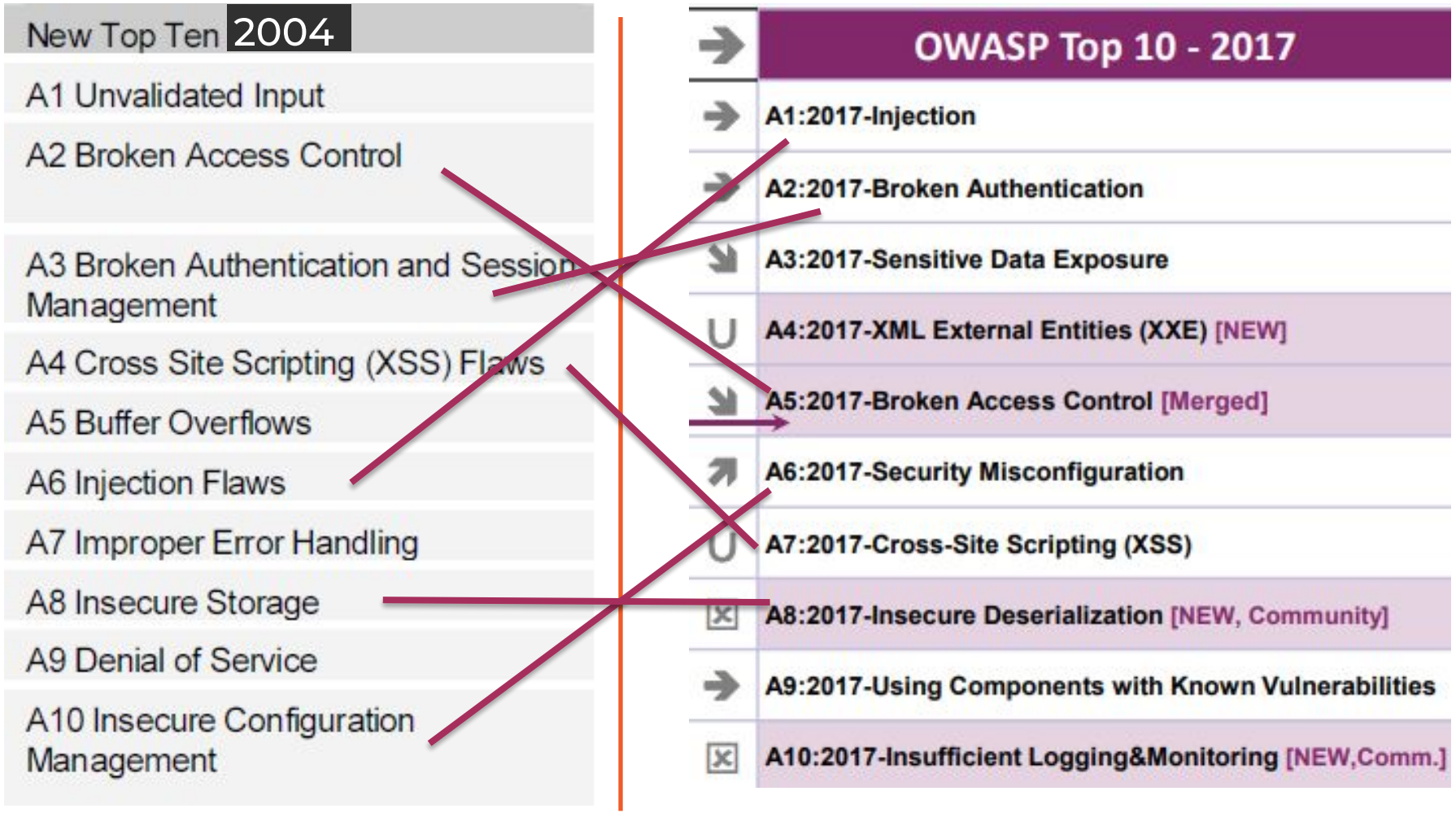
OWASP Top 10

New Top Ten 2004
A1 Unvalidated Input
A2 Broken Access Control
A3 Broken Authentication and Session Management
A4 Cross Site Scripting (XSS) Flaws
A5 Buffer Overflows
A6 Injection Flaws
A7 Improper Error Handling
A8 Insecure Storage
A9 Denial of Service
A10 Insecure Configuration Management

2004 2005 2006 2007

OWASP Top 10

6 of top 10 issues remain after 13 years

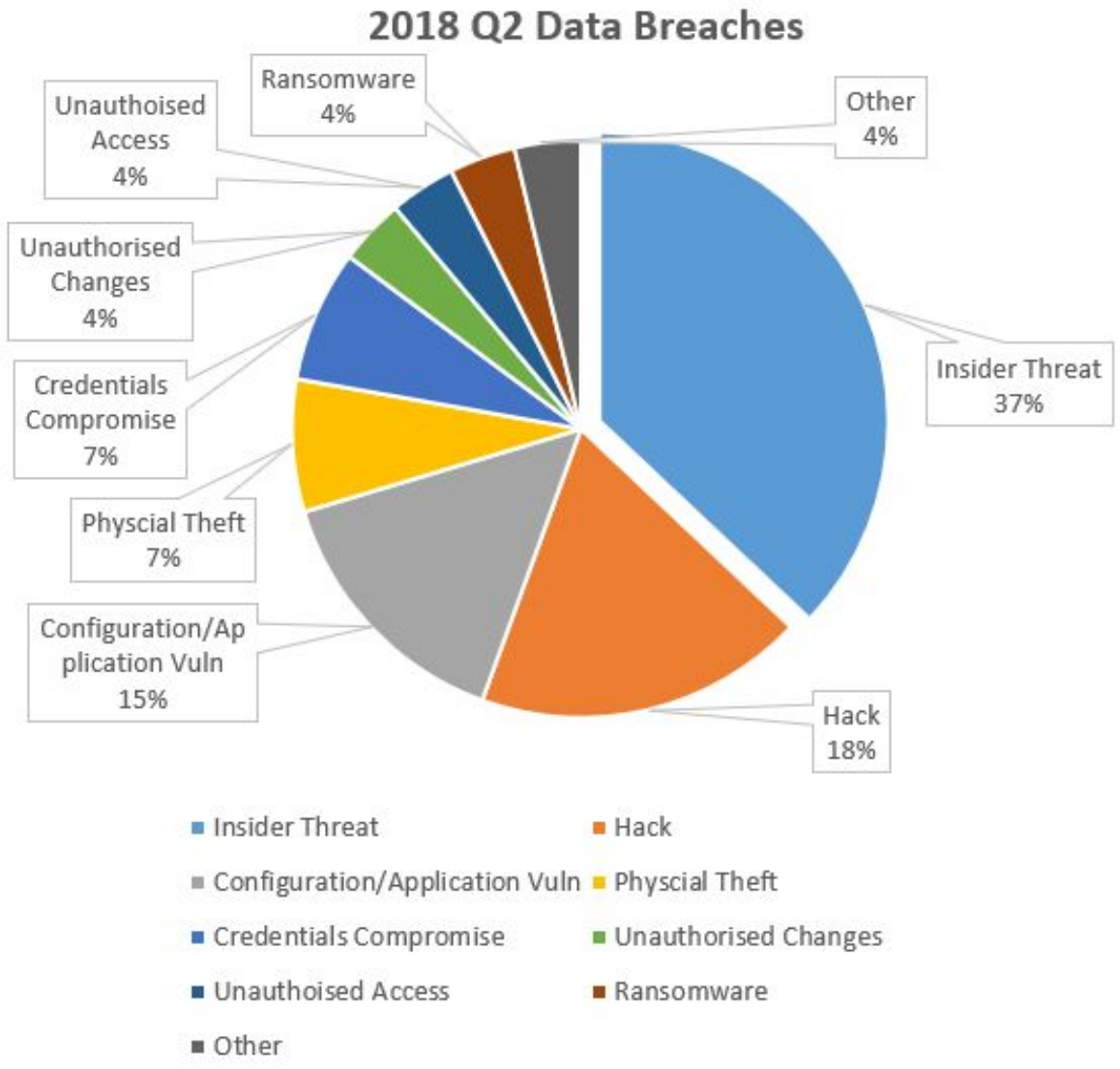


Can We Learn From Other Mature Industries?

Learning From Incidents

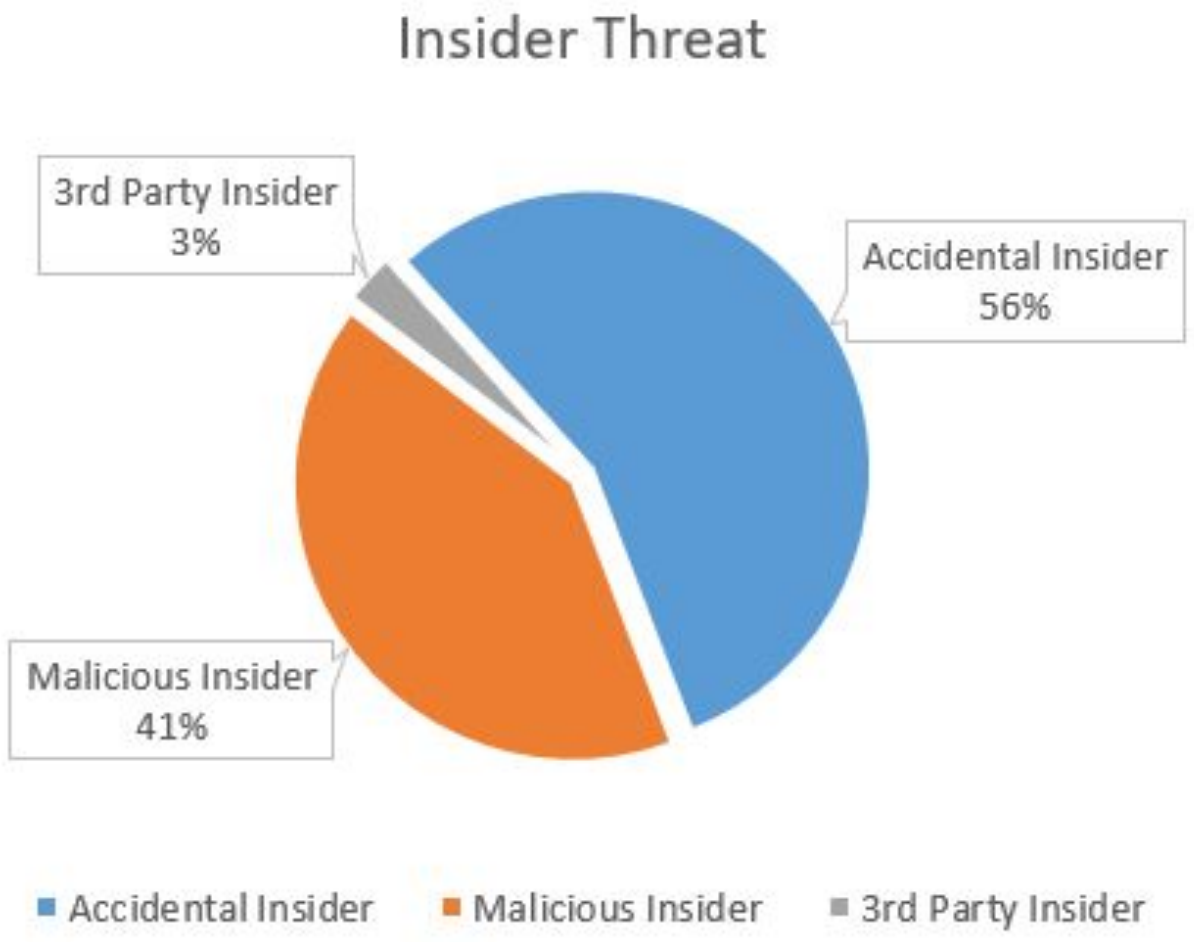
Learning From Incidents

CyberFailures.com Report May-Jun 2018

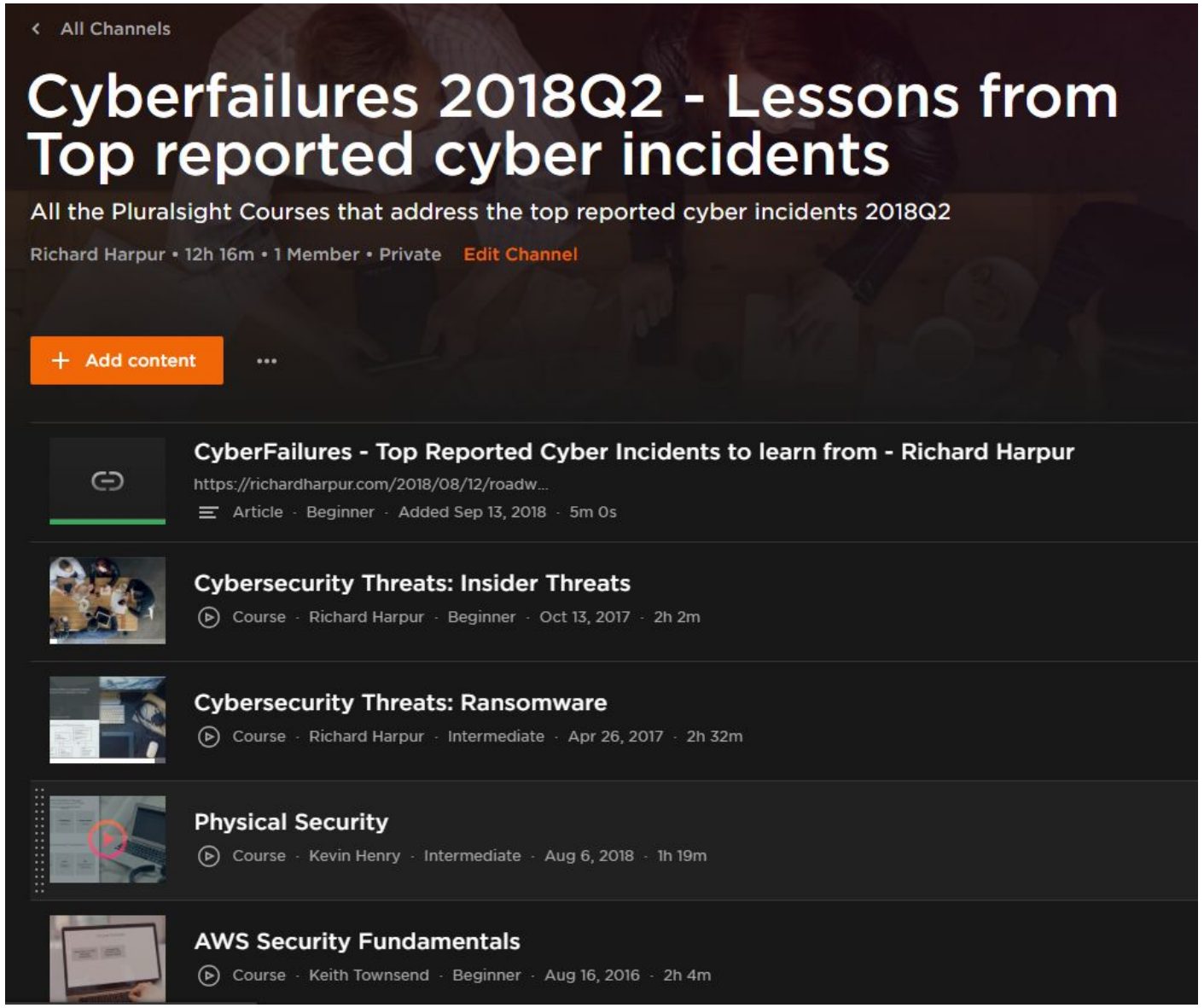


Source: https://RichardHarpur.com

CyberFailures.com Report May-Jun 2018



Call to Action - Pluralsight Channel

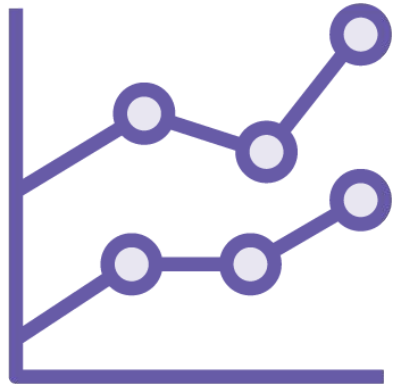


Take Stock

How is cybersecurity evolving

History Books

What can we learn from previous experience



Going Forward

Techniques to lock-in gains and improve skills going forward