Chief Executives Forum

8th June 2021

NI Cyber Security Centre

The NI Cyber Security Centre

Joe Dolan – Head of NI Cyber Security Centre

Outline

1. NICSC role
2. Board level responsibilities
3. Threat Landscape, Global, UK and NI
4. How attacks happen – examples
5. Cyber Assurance.
6. Expectations of resilience and recovery
7. Next steps

NI Cyber Security Centre’s role

Strategic objective

“We aim to make Northern Ireland cyber safe, secure and resilient for its citizens and businesses”

NI Cyber Security Centre

NICSC Principles

- **Cyber Advocacy**

The NICSC will be an authoritative and credible voice for the need for good cyber security in Northern Ireland.

- **Trusted source of advice and guidance**

To become the a single source of related cyber safety, security and resilience advice and guidance for Northern Ireland citizens, families, organisations.

- **Cyber Health promotion role**

Provide support and constructive challenge NI Public, Private and 3rd Sectors in the level of cyber safety, security and resilience to improve the overall cyber health of the region.

- **Facilitator not provider role**

The NICSC will help stimulate and promote take up of good cyber activities across Northern Ireland sectors and with the citizen but conscious not to become part of the delivery dependency ensuring that Northern Ireland ecosystems are self sustaining in maintaining good cyber health.

NI Cyber Health

Burning question – How cyber secure is Northern Ireland from an attack?

Are we cyber healthy?

Challenge

How to measure cyber health of the province?

Solution:-

- Define Northern Ireland scope
- Define a minimum level of good cyber safety & security
- Define expectations of resilience and recovery

Baseline:-

Measure current levels of cyber health – the level of knowledge, protective actions and levels of preparedness.

Plan to improve.

Understand the support/ interventions/ programs needed to achieve good cyber health.

NI Cyber Security Centre

NI Cyber Security Defined

- Northern Ireland - defined by its citizens, businesses and economy.
- Cyber Safety – having knowledge of the cyber threat landscape and how it applies to your sector, organisation, area.
- Cyber Security is the ability to apply good practice to protect against the cyber threat
- Cyber Resilience the ability to quickly recover from a cyber attack.

Northern Ireland Demography

1,800,000 People

1,470,000
16-64yrs

330,000 <16yrs

- 183,000 primary
- 142,000 post primary
- 5,000 special

845,000 working
In
80,000 businesses

Business/Organisational Campaigns

- 90% - 10 employees or less
- 600 Organisation 250+
- < 100 in CNI sectors

21,000
unemployed

301,000
Economically
Inactive

300,000
64+

Societal/Citizen Campaigns

Economically Inactive – looking after a home or retired<64+

NI Cyber Security Centre

Northern Ireland Risk Balance

High Risk/Impact areas

Low Risk/Impact areas

NI Cyber Security Centre

NI Cyber Health – Messages

NI Cyber Security Centre

Board level responsibilities

What is Cyber Security?

- Cyber - anything relating to computers
- Security - being free from danger or threat

Cyber Security – anything relating to computers being free from danger or threat.

- Threat - a <u>person</u> or <u>thing</u> likely to cause damage or danger
- Vulnerability – exposure to a threat.
- Risk – Likelihood a vulnerability will be exploited causing loss or damage

What is Cyber Security?

Cyber Security = Risk management

Cyber risk management definition:

managing the vulnerability of an organisation's computers and computer systems to cyber threats to reduce the likelihood or impact to the organisation's ability to operate and function.

Board Level Responsibilities

Getting the environment right		
Embedding cyber security in your organisation Growing cyber security expertise Developing a positive cyber security culture		
1. Get the information you need to make well informed decisions on the risks you face. Establishing your baseline and identifying what you care about most Understanding the cyber security threat	**2. Use this information to evaluate and prioritise your risks.** Risk management for cyber security	**3. Take steps to manage those risks.** Implementing effective cyber security measures Collaborating with suppliers and partners Planning your response to cyber incidents

Getting the Environment Right

Embed Cyber Security into Organisation

Integrate cyber security into your organisation's objectives and risks

Cyber security impacts on every aspect of your organisation. Therefore to manage it properly it must be integrated into organisational risk management and decision making.

Reflect this in your structure

Cyber security is the responsibility of the entire Board

Engage with your experts

Consider the communication between experts and members

Getting the Environment Right

Grow Cyber Security Expertise

Baseline your current skills

The Board should have an understanding of what cyber expertise there is in the organisation and what you need. Do you have a CISO? An information security team? Incident managers? If not, should you?

Getting the Environment Right

Develop Positive Cyber Security Culture

Lead by example

You set the tone when it comes to cyber security. Lead by example and champion cyber security within your organisation.

If policies don't work for you as a Board member (that is, if you find yourself doing something different to get your job done more easily), then there is a good chance they aren't working for others either. If it seems that the policy is having a detrimental effect on the organisation, work with policy makers to adapt it.

Culture takes time and concerted effort to evolve. Don't assume that because the Board has endorsed a security posture that it will automatically cascade down throughout the organisation.

Get Information to Inform Risk Decisions

Establish your baseline – what's important

Boards should understand what is most important to make the business work and reach its goals

Boards should consider what is of most value to the organisation. The 'crown jewels'

It is critical that this is an active and ongoing discussion between Boards and their experts:

- communicated the business goals and crown jewels to the technical teams so that they can prioritise protecting these.
- Boards will have business insight that technical teams may not have (such as which particular partner relationship must be to be prioritised)
- technical teams will have insight into the enablers for key objectives (such as which networks or systems do particular partners rely upon)

Get Information to Inform Risk Decisions

Understand the threat

Get an understanding of the threat.

Collaborate on security.

Assess the threat.

Working with suppliers and partners.

Evaluate and Prioritise Risk

Manage the Cyber Security Risk

Integrate cyber security into organisational risk management processes

Dealing with cyber security risk as a standalone topic (or considering it simply in terms of 'IT risk') will make it hard for you to recognise the wider implications of those cyber security risks.

Don't make reducing risk levels the measure of success

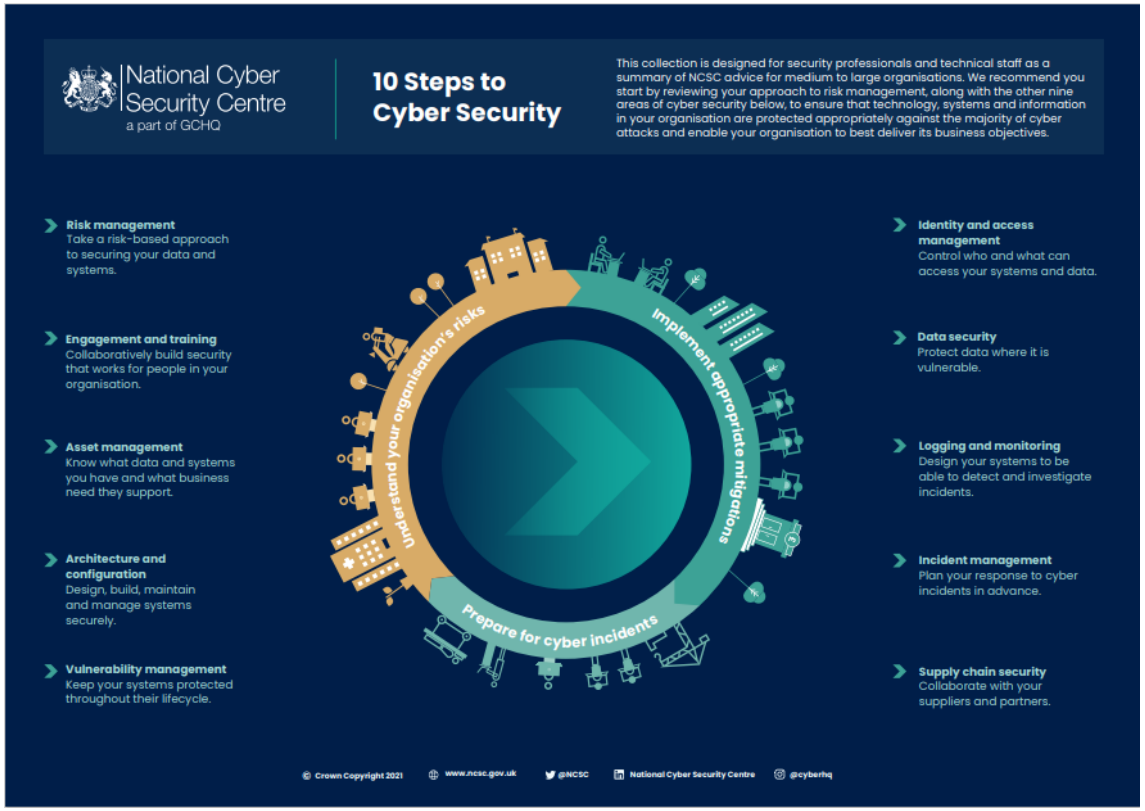
It can be difficult to measure the success of your organisation's cyber security efforts. A typical output of good cyber security is the absence of a failure, which can be hard to measure or It is common for risk assessments to deliver some kind of assessment level, be that high medium low, or a number, and so it could be tempting to use this as a performance metric for your cyber security efforts.

Take Steps to Manage Risks

Implement Effective Cyber Security Measures

Get a little bit technical

Having a basic understanding of cyber security can help you to ask the right questions to seek assurance about your organisation's cyber resilience -just as you would need to have a certain level of understanding of finance to assess the financial health of your organisation.



NI Cyber Security Centre

Take Steps to Manage Risks

Collaborate with Suppliers and Partners

Build cyber security into every decision

Cyber security risk should be a key consideration in any decision on new relationships or collaborations. This includes decisions on suppliers, providers, mergers, acquisitions and partners.

Ensure:

1. That this access doesn't provide a route for an attacker to gain access to your organisation, either through deliberate action or unintentional consequence.

2. That any partner or supplier is handling any sensitive data appropriately and securely.

3. That any product or service you buy has the appropriate security built in.

Take Steps to Manage Risks

Plan Your Response to Cyber Attacks

Ensure you have a plan

Understand your role in incident management

Get involved in exercises

Drive a 'no blame' culture

Current Cyber Threat Landscape

Threat landscape

Global Landscape

- Integrated Review – launched 16th March

Original release date: April 15, 2021

CISA, the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) have released a Joint Cybersecurity Advisory (CSA) on Russian Foreign Intelligence Service (SVR) actors scanning for and exploiting vulnerabilities to compromise U.S. and allied networks, including national security and government-related systems.

Specifically, SVR actors are targeting and exploiting the following vulnerabilities:

- CVE-2018-13379 Fortinet FortiGate VPN
- CVE-2019-9670 Synacor Zimbra Collaboration Suite
- CVE-2019-11510 Pulse Secure Pulse Connect Secure VPN
- CVE-2019-19781 Citrix Application Delivery Controller and Gateway
- CVE-2020-4006 VMware Workspace ONE Access

US fuel pipeline 'paid hackers $5m in ransom'

14 May

A major US fuel pipeline has reportedly paid cyber-criminal gang DarkSide nearly $5m (£3.6m) in ransom, following a cyber-attack.

statement

Share Tweet Like 147

yberattack, which is affecting many of our

e National Cyber Security Centre, external
o investigate and understand the impact of the

vailable. We will continue to provide updates

to our most vulnerable residents, and

normal, and our call centre is extremely busy.
y, and to bear with us while we seek to resolve

Tweet

Bedfor school

26 March

The school said the attack was likely to cause long-term disruption

Redcar pen an

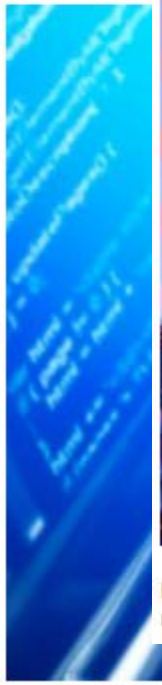
By Joe Tidy
Cyber-security reporter

14 February 2020

More than 135,000 nearly a week, as th

Cybe 4,000

22 January



Lond hit b

13 October 20

Visitors to the

London's Hacl which is affect

Ne we

6 S

Mo

Co 19

By Chris
Technol

16 Ju

Coron

Russia vaccin

Ha Ke

1 J

Cor

The

A ga own

Newcastle Unive
"a number of weeks" to sort out

Threat

BBC | Sign in

NEWS

Home | Prince Philip | Coronavirus | Bre

N. Ireland | N. Ireland Politics | Local Ne

Translink rep to the police

7 February 2020

Bus and train operator Translink has rep internal IT systems to the police, the BB

BBC | Sign in

NEWS

Home | Prince Philip | Coronavirus | Bre

N. Ireland | N. Ireland Politics | Local Ne

Queen's Unive 'precautions' a attempt

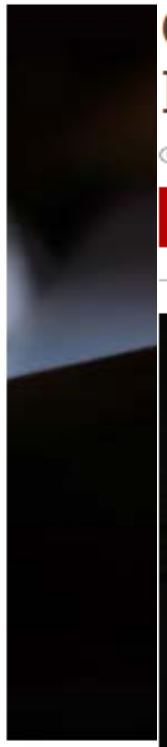
By Robbie Meredith & Eve Rosato
BBC News NI

5 March

Queen's University in Belfast (QUB) has had to suspend access to "a number of university systems" as a precaution following an attempted cyber-attack.

Belfast Tele

Personal Council t



A Northern Irela information abou

Michael Kenwoc

March 18 2021 07:0

BBC | Sign in | Home | News | Sport | Weather | iPlayer

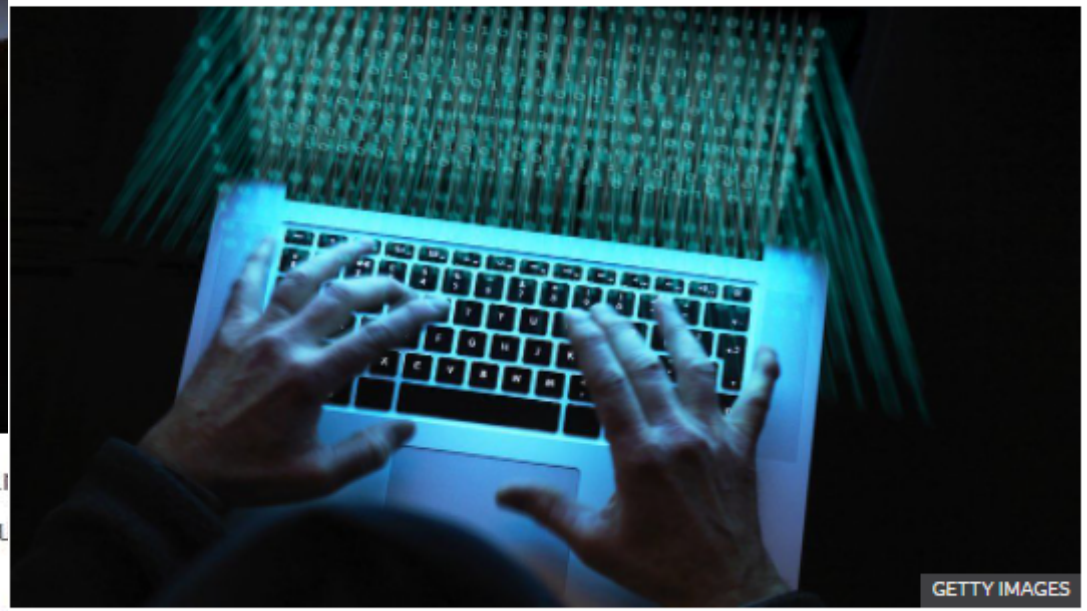
NEWS

Home | Coronavirus | Brexit | UK | World | Business | Politics | Tech | Science | Health | Family & Education

World | Africa | Asia | Australia | Europe | Latin America | Middle East | US & Canada

Cyber attack 'most significant on Irish state'

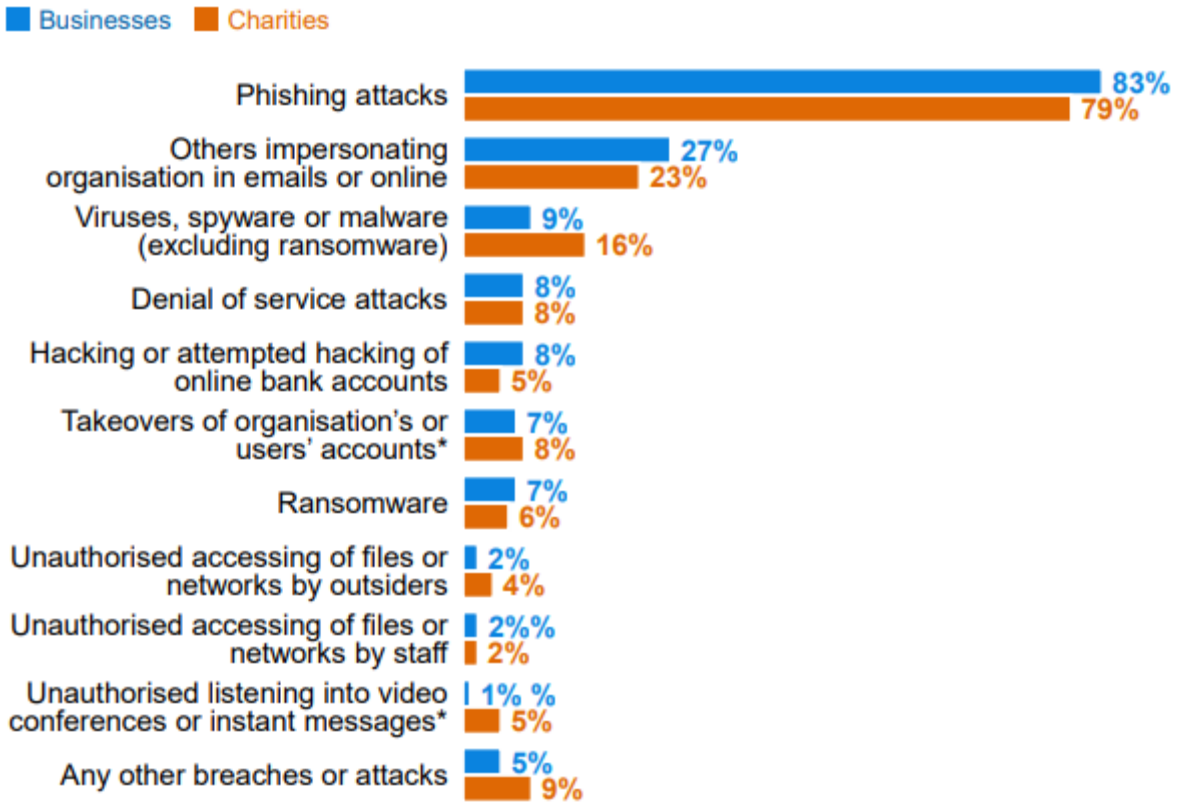
14 May



A cyber attack on Irish health service computer systems is "possibly the most significant cybercrime attack on the Irish state", a minister has said.

Top Cyber threats

- Many of the top attacks can be prevented with good education and cyber hygiene practices.
  - Education for end users and at risk personnel
  - Strong password and 2FA policy
  - Timely patching and updates
  - AV and/or end point security
  - Secure configuration



Bases: 654 businesses that identified a breach or attack in the last 12 months; 183 charities
*New codes for 2021

NI Cyber Security Centre

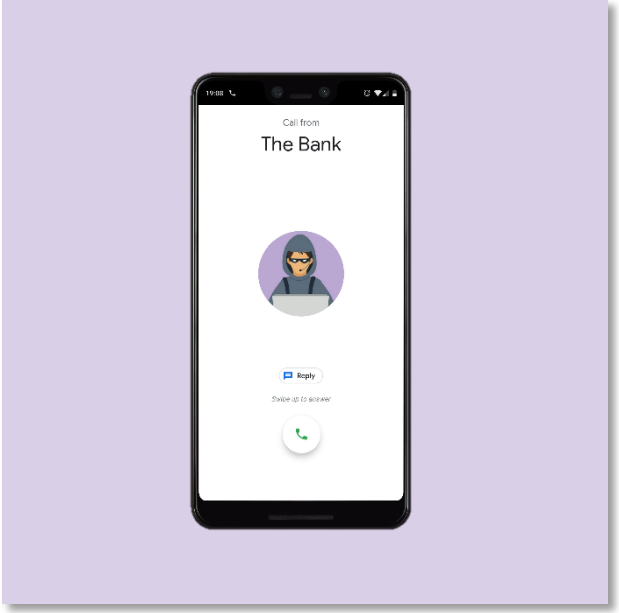
Top Cyber threats – Social Engineering

The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent or malicious intent.

NI Cyber Security Centre

Top Cyber threats – Social Engineering

Phishing



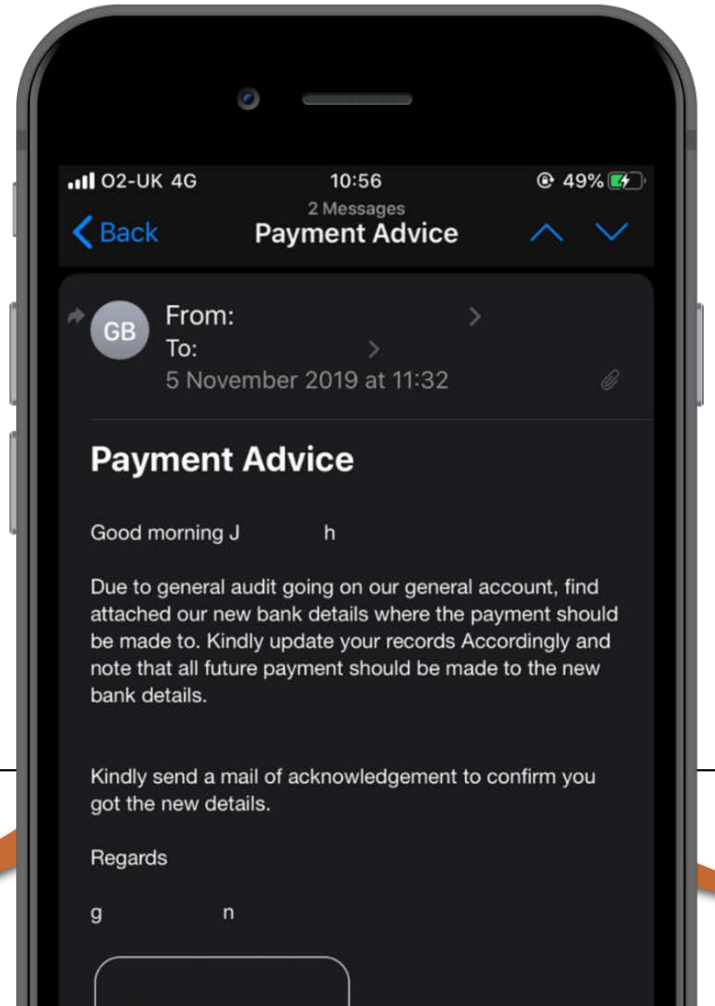
Vishing

Smishing

Top Cyber threats – Invoice Re-direction/Mandate Fraud

You

Your Supplier



Criminal

NI Cyber Security Centre

Top Cyber threats – Invoice Re-direction/Mandate Fraud

Hi 15°C | Lo 13°C Belfast | WEATHER

Belfast Telegraph DIGITAL

HOME NEWS SPORT BUSINESS ENTERTAINMENT LIFE CARS OPINION ARCHIVE

Northern Ireland | UK | Republic of Ireland | World | Politics | Brexit | Health | Sunday Life

Home › News › Northern Ireland

Email scams totalling almost £800,000 reported to PSNI in July

Chief Superintendent Simon Walls has warned that scammers will go to great lengths to trick their victims.

Simon Walls

scamwiseNI PARTNERSHIP POST OFFICE

£45.6 million

Lost during H1 2020 to Invoice Re-Direction Scams

Ireland › Irish News

Warning as Irish firms lose millions in sophisticated invoice scams

Two firms lost €650,000 recently in the so-called invoice redirection fraud

Mon, Nov 11, 2019,

Ronan McGreevy

THE IRISH TIMES

Mon, Sep 2, 2019

NEWS SPORT BUSINESS OPINION LIFE & STYLE CULTURE

Crime & Law | Brexit | Ireland | World | Politics | Social Affairs | Health | Education

We use cookies to personalise content, target and report on ads, to provide social medi

For more information see our Cookie Policy.

Dublin Zoo victim of €500,000 internet-based fraud by organised gang

Zoo tricked into paying invoices into bank account controlled by fraudsters

Belfast Telegraph

News Opinion Business Sport Life Entertainment Travel Sunday Life ≡ Sections

and UK Republic of Ireland World Politics Brexit Health Education Courts Obituaries Archive

Irish firm sent 65,000 euro to fraudulent account in bid to buy PPE machine

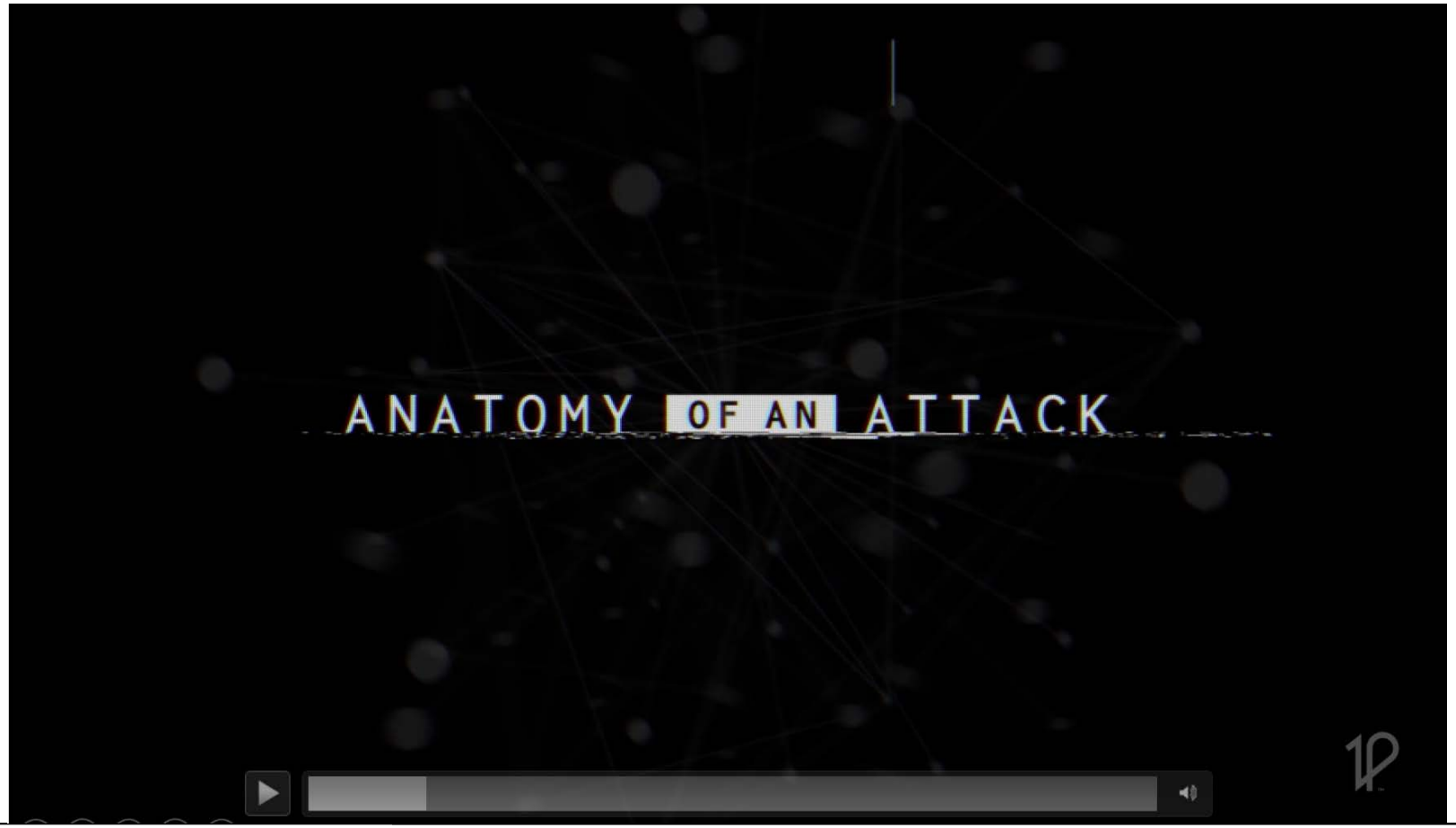
Gardai in Waterford are investigating the scam with assistance from the Garda National Economic Crime Bureau.

IRISH BUSINESS REPORTS LOSSES OF €4.4M DUE TO INVOICE REDIRECT FRAUD

NI Cyber Security Centre

How attacks happen

Why do Cyber Security?



NI Cyber Security Centre

Threats – Who (know your enemy)

Nations

Cyber Criminals

Employees

Hacktivists

Hackers

Suppliers

NI Cyber Security Centre

How cyber attacks work?

Cyber Kill Chain

7 Stages of a cyber attack

NI Cyber Security Centre

How cyber attacks work?

NCSC distil these down into 4 stages:

- **Survey -** investigating and analysing available information about the target in order to identify potential vulnerabilities.
- **Delivery -** getting to the point in a system where you have an initial foothold in the system.
- **Breach -** exploiting the vulnerability(ies) to gain some form of unauthorised access.
- **Affect -** carrying out activities within a system that achieve the attacker's goal.

National Cyber Security Centre

What you can do to combat cyber attacks

Reducing The Impact

Most cyber attacks are composed of four stages: **Survey, Delivery, Breach and Affect.** The following **security controls,** applied at each stage of an attack, can reduce your organisation's exposure to a successful cyber attack.

Survey

User Education

Train all users to consider what they include in publicly available documents and web content. Users should also be aware of the risks from discussing work-related topics on social media, and the potential of being targeted by phishing attacks.

Who might be attacking you?

Cyber Criminals interested in making money through fraud or from the sale of valuable information.

Industrial competitors and foreign intelligence services interested in gaining an economic advantage for their companies or countries.

Hackers who find interfering with computer systems an enjoyable challenge.

Hacktivists who wish to attack companies for political or ideological motives.

Employees, or those who have legitimate access, either by accidental or deliberate misuse.

Delivery

Network Perimeter Defences

Can block insecure or unnecessary services, or only allow permitted websites to be accessed.

Malware Protection

Can block malicious emails and prevent mailware being downloaded from websites.

Password Policy

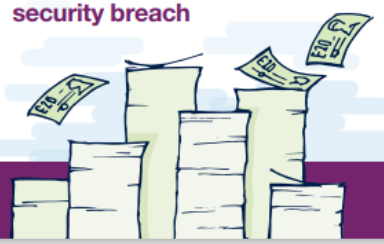
Can prevent users from selecting easily guessed passwords and locks accounts after a low number of failed attempts.

Secure Configuration

Restrict system functionality to the minimum needed for business operation, systematically apply to every device that is used to conduct business.

£600K-£1.15m

Average cost of security breach



Breach

Patch Management

Apply patches at the earliest possibility to limit exposure to known software vulnerabilities.

Monitoring

Monitor and analyse all network activity to identify any malicious or unusual activity.

Malware Protection

Malware protection within the internet gateway can detect malicious code in an important item.

Secure Configuration

Remove unnecessary software and default user accounts. Ensure default passwords are changed, and that automatic features that could activate malware are turned off.

User Access

Well maintained user access controls can restrict the applications, privileges and data that users can access.

User Training

User training is extremely valuable in reducing the likelihood of successful social engineering attacks.

Device Controls

Devices within the internal gateway should be used to prevent unauthorised access to critical services or inherently insecure services that may still be required internally.

Affect

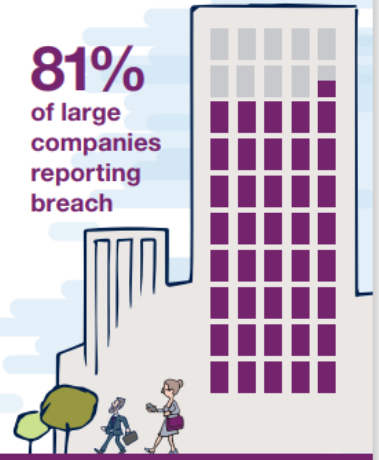
Controls For The Affect Stage

Once an attacker has achieved full access, it's much harder to detect their actions and eradicate their presence. This is where a more in-depth, holistic approach to cyber security can help.

10 Steps To Cyber Security outlines many of the features of a complete cyber risk management regime.

81%

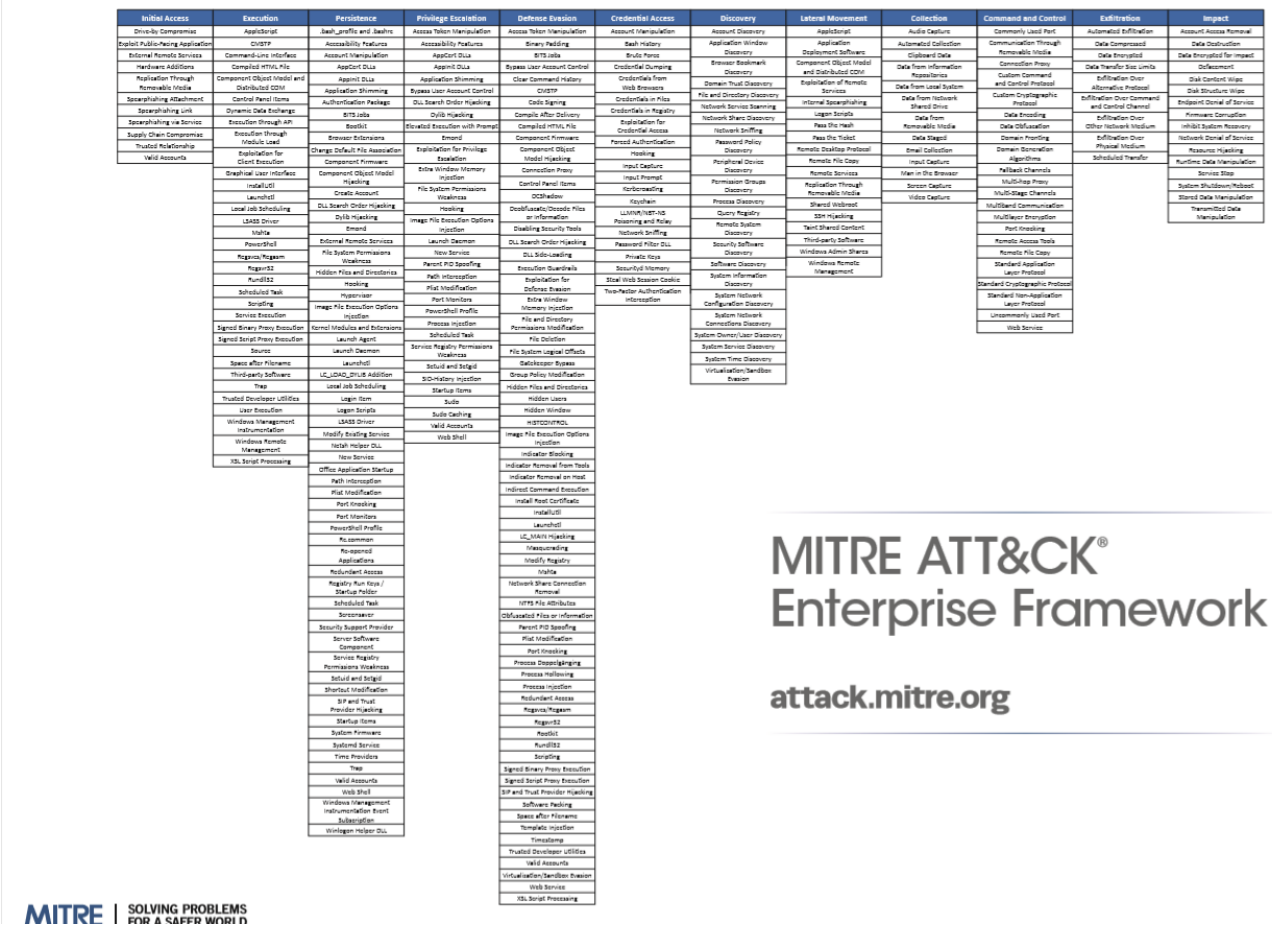
of large companies reporting breach



For more information go to www.ncsc.gov.uk @ncsc

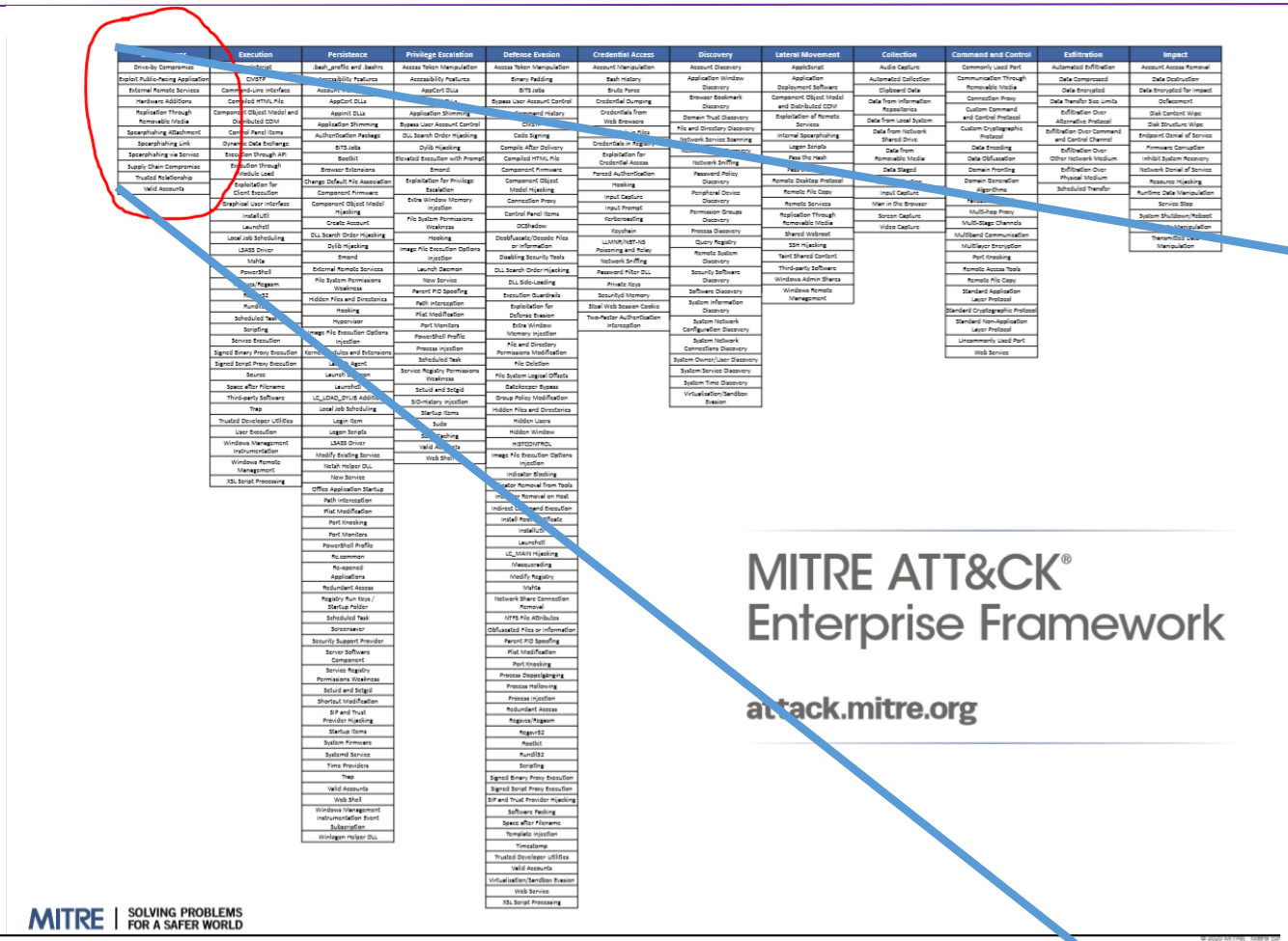
NI Cyber Security Centre

Vulnerability – exposure to threats

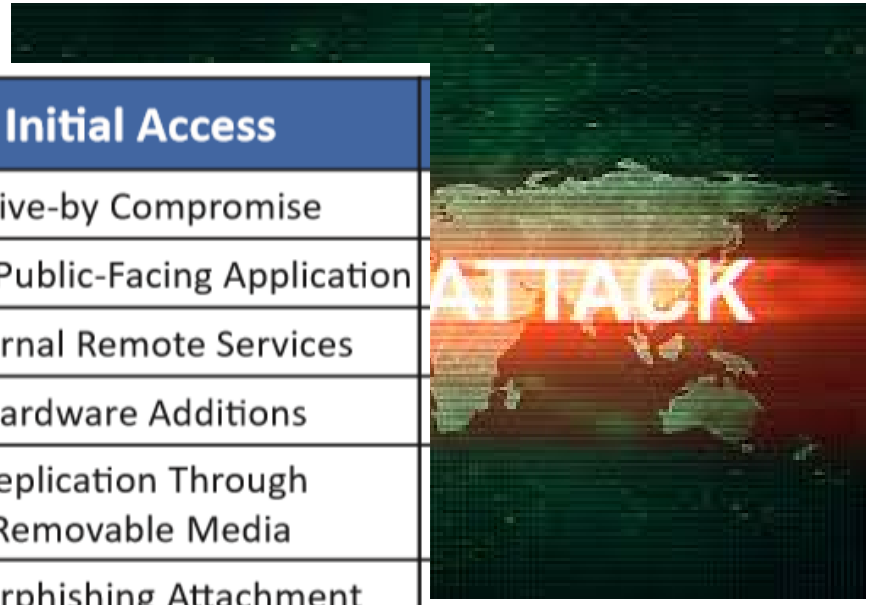


NI Cyber Security Centre

Vulnerability – exposure to threats



Initial Access
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Replication Through Removable Media
Spearphishing Attachment
Spearphishing Link
Spearphishing via Service
Supply Chain Compromise
Trusted Relationship
Valid Accounts



NI Cyber Security Centre

Cyber Assurance

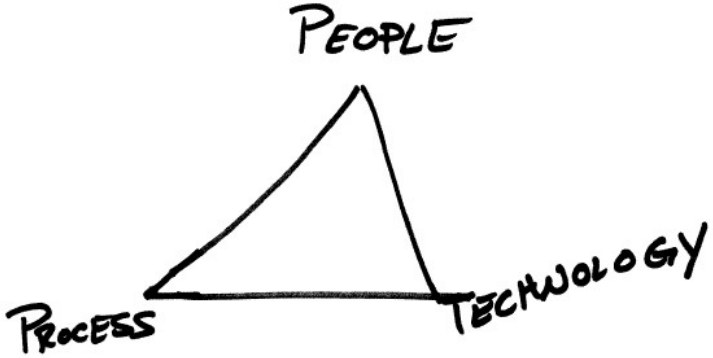
How cyber secure and resilient is NI

How do we measure cyber security?

Minimum standard for NI?

Compliance of standards are a visible demonstration of assurance and good practice

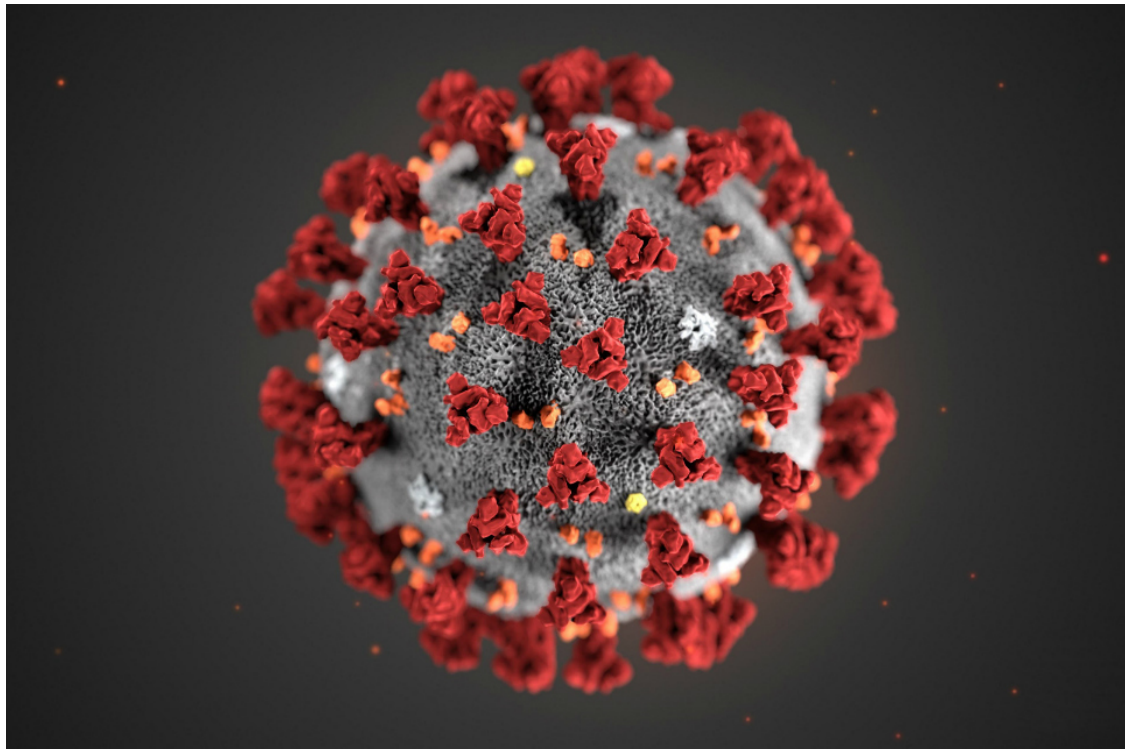
- How do you get assurance of you organisational cyber resilience?
- Does it test your people and processes or just technology?



What expectations of resilience and recovery?

Cyber Resilience

- Different than DR or Redundancy
- Think about treating an infection
- Can you:-
  - detect and isolate
  - Investigate, remediate and
  - Safely recover

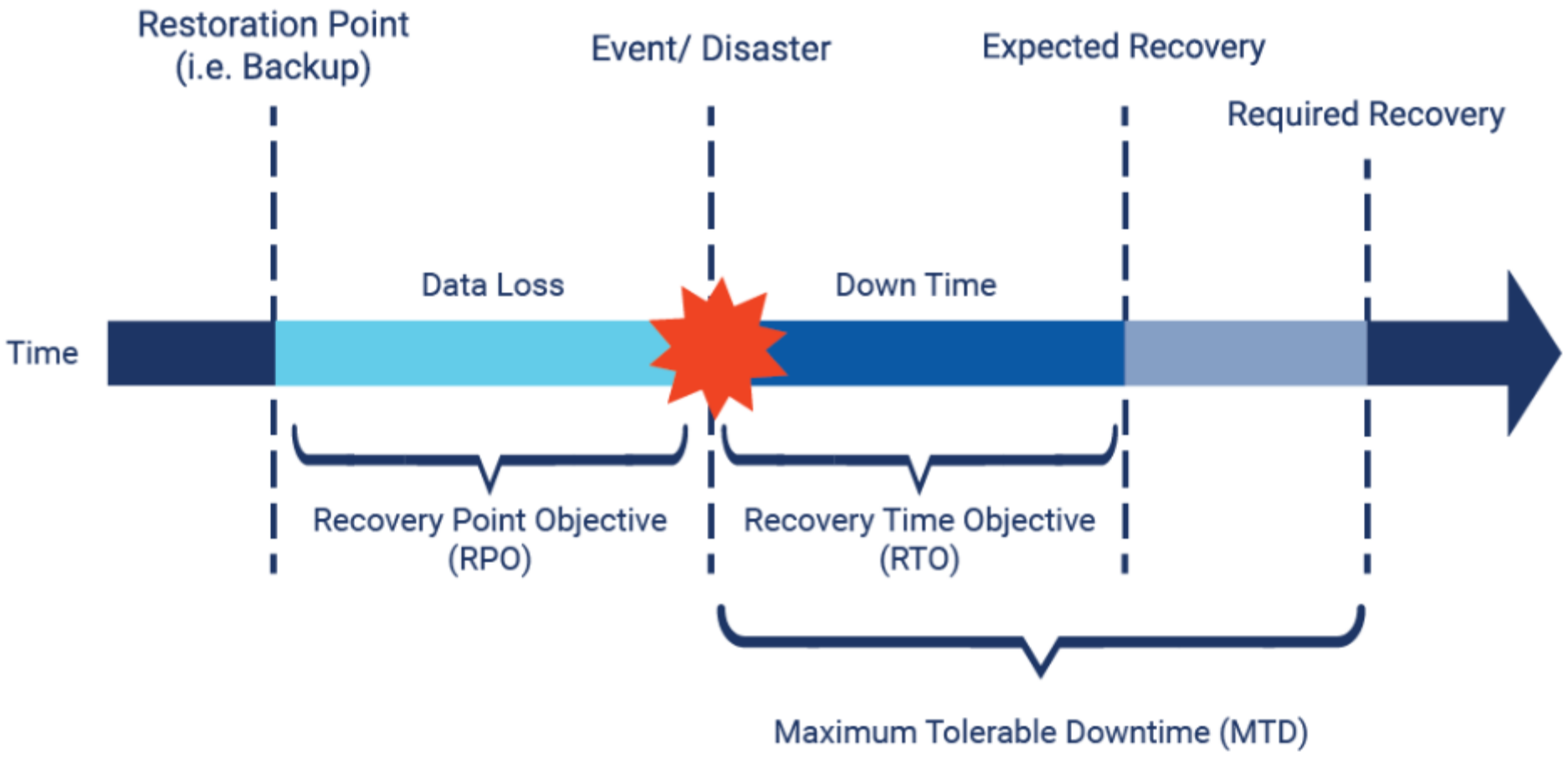


Cyber attack and recovery

NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

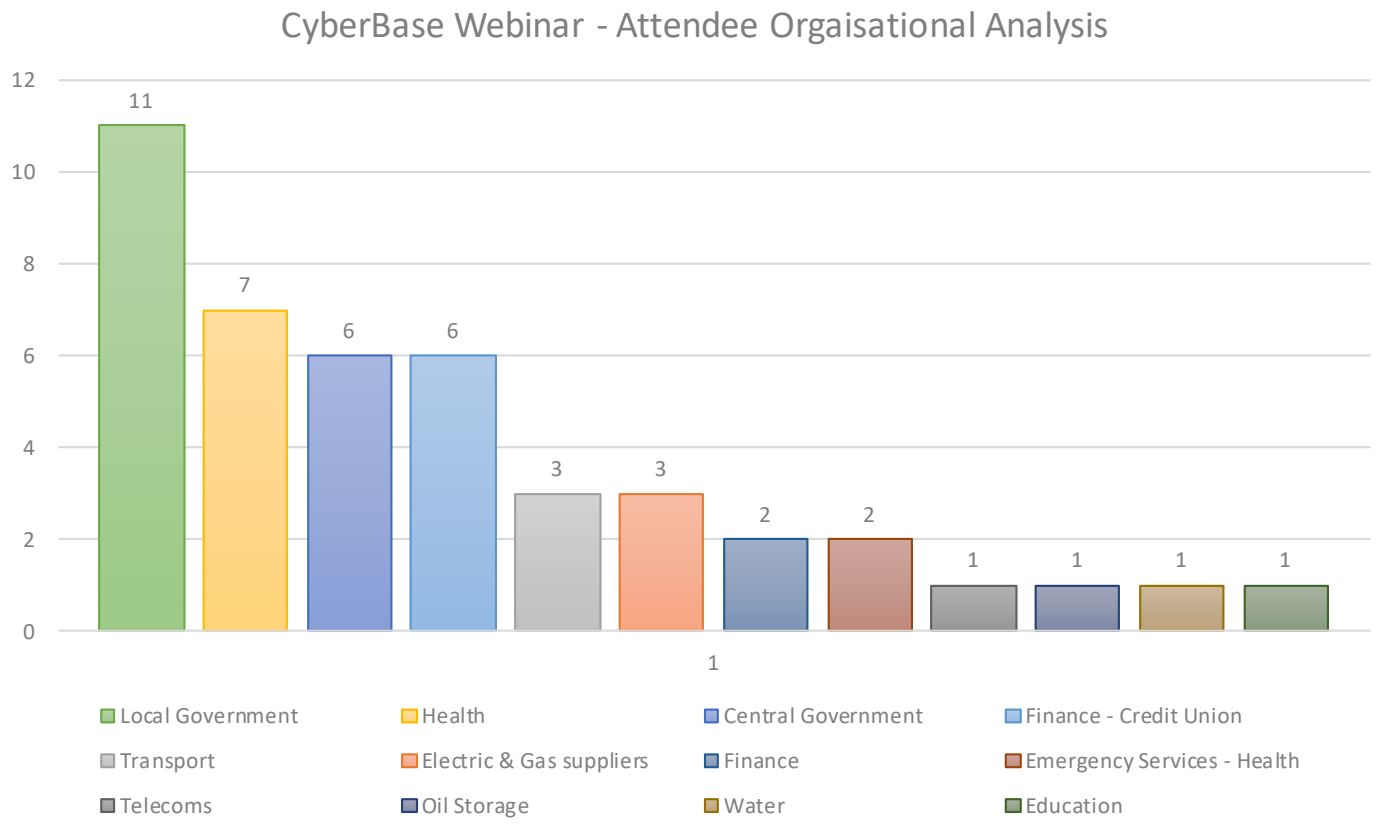
Resilience and Recovery



Resilience and Recovery

Who sets the levels?

Cyber Resilience – through testing



Good cross sector representation

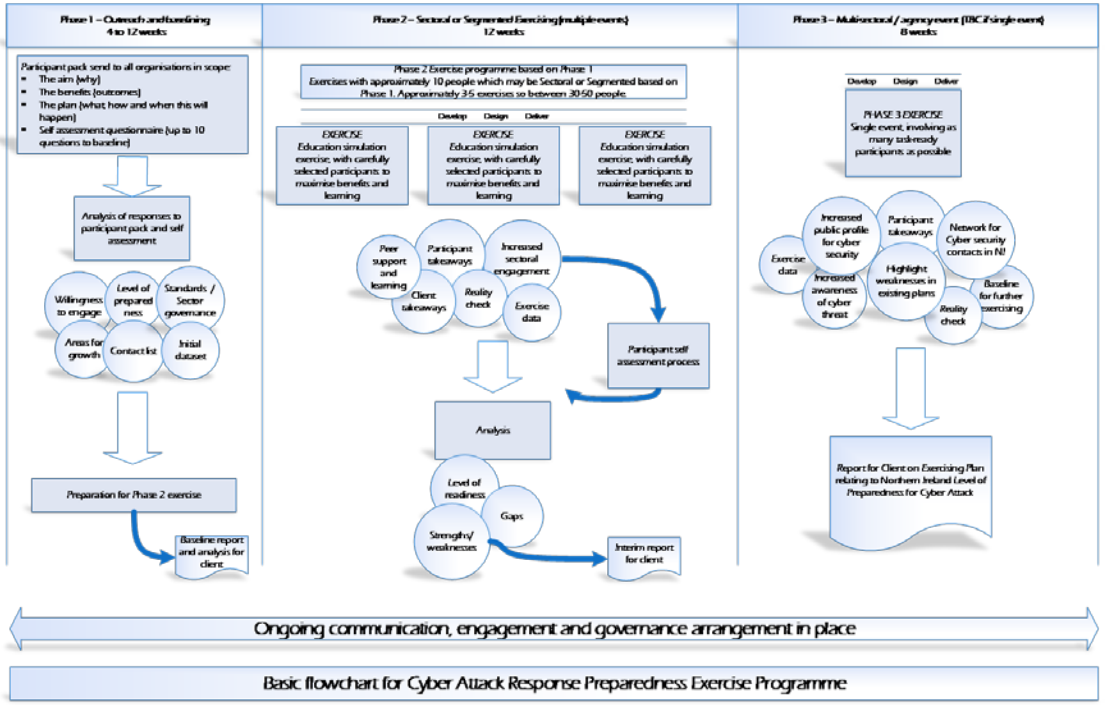
66% public sector

34% private sector

NI Cyber Security Centre

Current baselines

- Most organisations have BCP
- 60% have some cyber element
- 40% have a CIRP



NI Cyber Security Centre

And Finally …

Things to consider….

Takeaways – Have a healthy dose of scepticism

1. Do you know your priority business functions and do your technical teams?
2. Do you know how long these can be out of action before it becomes critical?
3. Do you know the people, processes and IT applications that underpin these?
4. Do you have a level of assurance that these services are protected, trust but verify?
5. Have you a cyber incident plan and tested it?
6. Have you good board level representation and communication with the technical teams?
7. Do you know your critical suppliers (internal as well as external)?
8. Have you tested or validated how they might impact on your security?
9. How are you protecting access to your critical systems?, invest in MFA.
10. Understand your enemy. – do you understand your threat landscape?

Ask from NICSC

1. Be demonstrable in your level of security – independent verification to a recognise standard
2. Know you are prepared – develop a CIRP and test it.
3. Recover – plan your recovery from worst case.
4. Engage with us to develop these

NI Cyber Security Centre

Website	www.nicybersecruitycentre.gov.uk
Contact	info@nicybersecuritycentre.gov.uk
Follow us	Twitter @NIcyberSC

#CyberSecureNI