



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





Strategic objective

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



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.



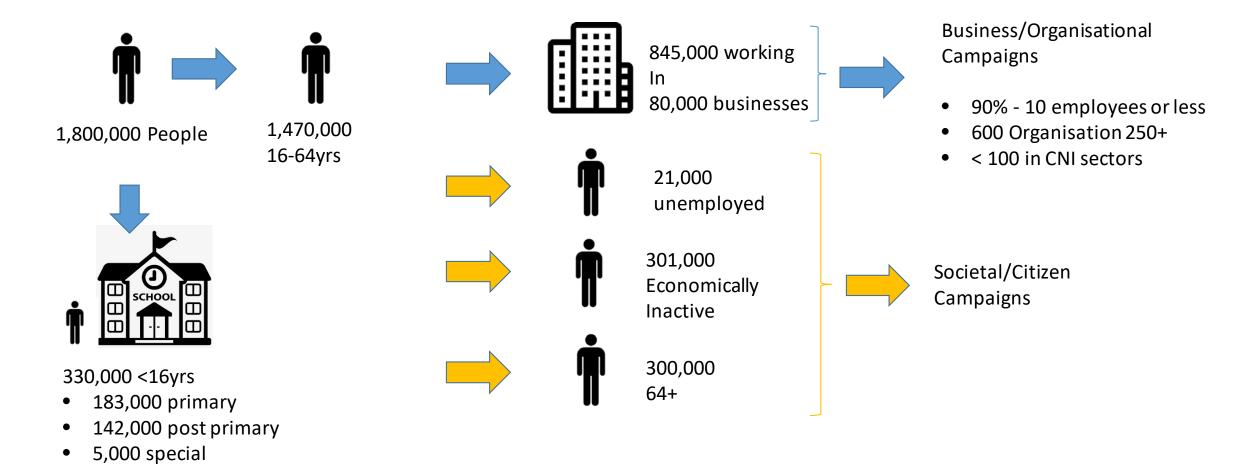


NI Cyber Security Defined

- 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.

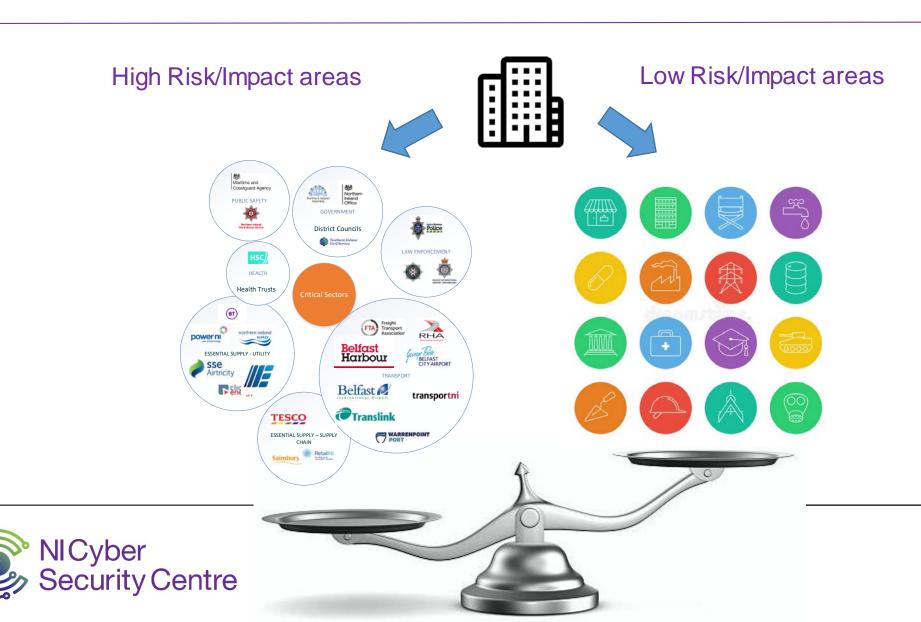


Northern Ireland Demography





Northern Ireland Risk Balance



NI Cyber Health – Messages



7 60

CORONAVIRUS (COVID-19)









record by M Collect Results





"Seculating" in SNEE plainting is social engineering about Largering various on their models phones. A floodulest text is sent to someone is

inferenties.

making phone, asting there to ribrication, call a number or otherwise

ect in a very that will lead to seasoners obtaining presental or financial













fe, secure and resilient for its citizens and

November 2019

Media

Likes

berSC · 23h

ghted a phishing attempt using a Penalty

ure about, forward it to the suspicious phishing.gov.uk for investigation.

> Penalty Charge Notice Number: YJ102837128833121



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.



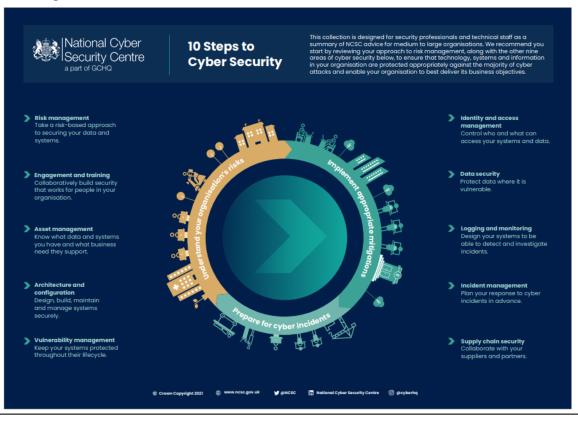
Take Steps to Manage Risks

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.







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







Threat landscape

Global Landscape

Integrated Review – launched 16th March

Original release date: April 15, 2021

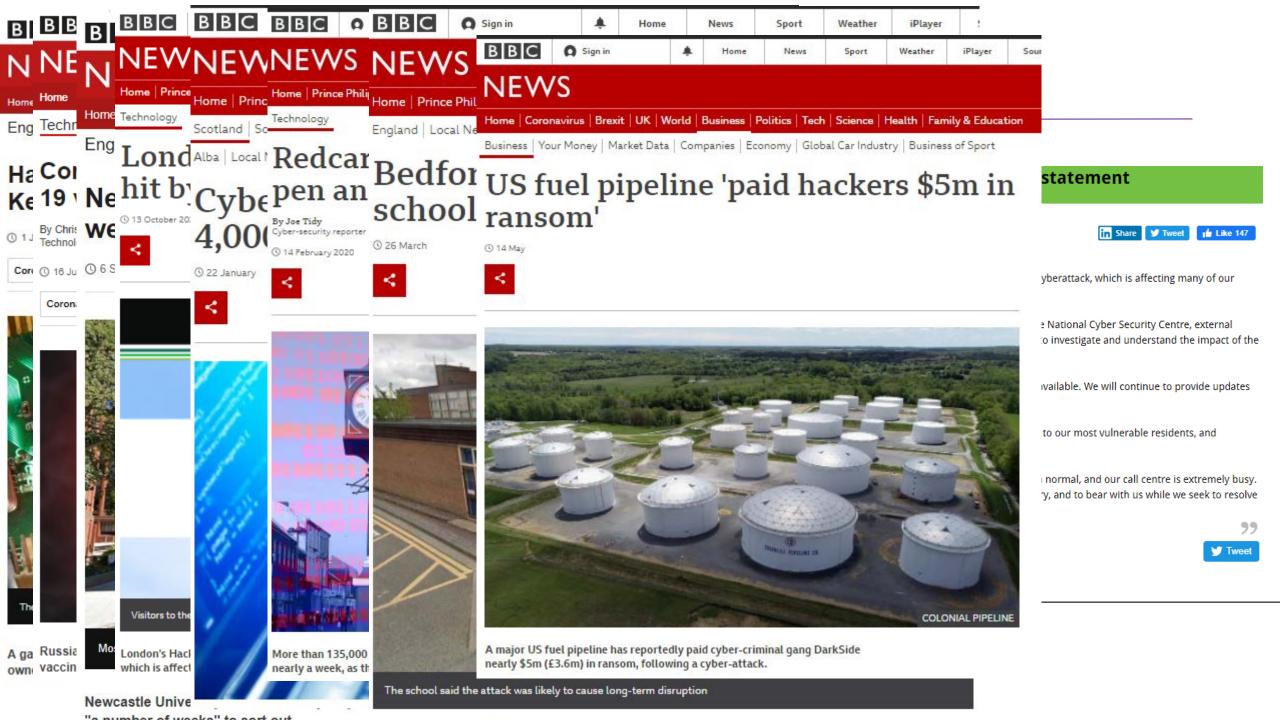
CISA, the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) have released a <u>Joint Cybersecurity Advisory (CSA)</u> on Russian Foreign Intelligence Service (SVR) actors scanning for and exploiting vulnerabilities to compromise U.S. and allied networks, including national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









Home | Prince Philip | Coronavirus | Bre Queen's Unive N. Ireland | N. Ireland Politics | Local Ne | precautions a Translink repeattempt to the police

By Robbie Meredith & Eve Rosato BBC News NI

() 5 March



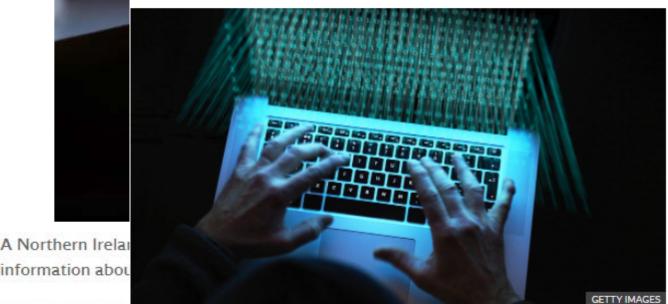
(§ 7 February 2020







Cyber attack 'most significant on Irish state'



vate

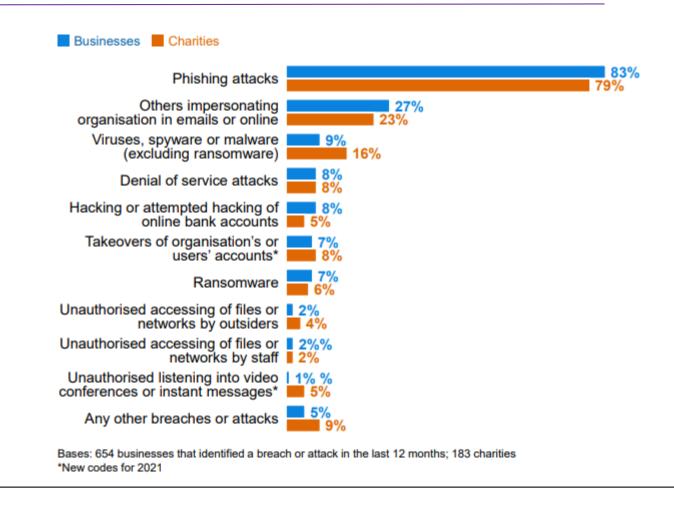
Michael Kenwoo

March 18 2021 07: Carober attack on Irish health service computer systems is "possibly the March 18 2021 07: Carobia significant cybercrime attack on the Irish state", a minister has said.



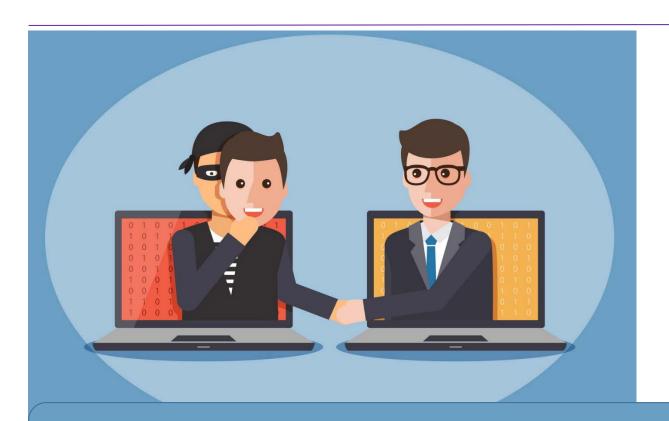
Top Cyber threats

- 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





Top Cyber threats – Social Engineering



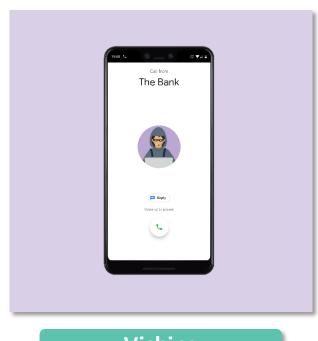


The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent or malicious intent.



Top Cyber threats – Social Engineering







Vishing

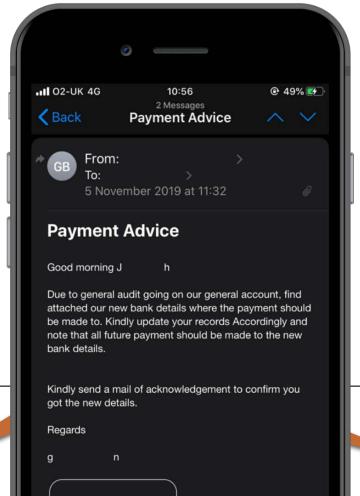
Smishing



Top Cyber threats – Invoice Re-direction/Mandate Fraud

Your Supplier

You



Criminal





Top Cyber threats – Invoice Re-direction/Mandate Fraud







Why do Cyber Security?





Threats – Who (know your enemy)

Nations









Hacktivists



Cyber Criminals



Hackers



Employees



Suppliers

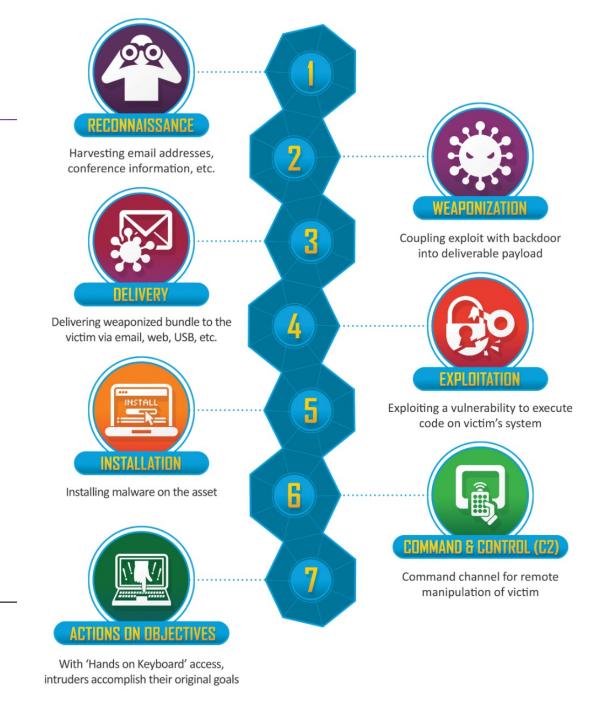




How cyber attacks work?

Cyber Kill Chain

7 Stages of a cyber attack





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.





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



Delivery

Breach

Affect



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.



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.



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

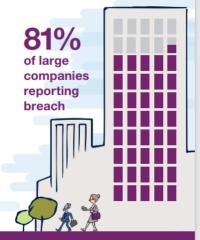
Devices within the internal gateway should be used to prevent unauthorised access to critical services or inherently insecure services that may still be required internally.



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.



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



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.



Average cost of security breach





Vulnerability – exposure to threats

Description Services Common Services Commo	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Determination Services Continue Application Continue Applicati	Drive-by Compromise	AppleScript	.bash_profile and .bashre	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Part	Automated Enfitration	Account Access Femovel
Terrent for Scholar Sc	Exploit Public-Pacing Application	CMSTP	Accessibility Features	Accessibility Postures	Sinary Padding	Sash History			Automated Collection		Deta Compressed	Data Ocstruction
Appel Court Appel Control Service Ministry of Control Serv	Extornal Remote Services	Command-Line Interface	Account Manipulation	AppCort DLLs	EFTS Jobs	Bruits Force			Clipboard Data		Delle Encryptod	Date Encrypted for Impact
Application From Promate Proma	Herdwere Additions	Compiled HTML File	AppCort DLLs	Appinit DUa	Bypass User Account Control	Crodontial Dumping					Data Transfer Size Limits	Defecement
Terminative College Co			Appinit DLLs	Application Shimming	Clear Command History							Disk Content Wipe
Starty-Bridge (Authorities Assemble (Authori			Application Shimming	Bypess User Account Control	CMSTP			Services				Disk Structure Wipe
Septimbly of the Company of Septimbly of the Company of Septimbly of the Company of Septimbly of			Authentication Package	DLL Scarch Order Hijacking	Code Signing			Internal Spearphishing				Endpoint Doniel of Service
Secretable Frame of Secret			5/T3.1ebs	Dylib Hijacking	Compile After Delivery			Logon Scripts		Data Encoding		Firmware Corruption
Supply does foreignment Well named by Company of the Company of Co	.,,		Sootkit	Elevated Execution with Prompt	Compiled HTML File			Pass the Hash		Data Obfuscation	Other Network Medium	inhibit System Resovery
Sould search of the control of the c			Browser Extensions	Emond	Component Firmwere			Pass the Ticket	Date Staged	Domain Fronting		Network Denial of Service
Wild Assert D Corporated Fromware Employed our or reference Employed and provides to Company or Clinic for Setting to From Setting F			Change Default File Association					Mometo Desktop Protocol	Email Collection			Resource Hijacking
Beyind our retirable Industrial Company of Special State (Industrial State Company of Special St	Velid Accounts		Companent Firmwere					Remate Nile Copy	Input Capture		Scheduled Transfer	Nurtime Data Manipulation
Hadded Market Ma		Graphical User Interface			Connection Proxy			Memote Services	Man in the Browser			Service Step
Lack Driver Lack		InstallUtil			Control Panol Items				Screen Capture			System Shutdown/Meboot
Load Driver Color Preserve Load Driver All Section Reports Services Water All Section Reports Services Water Reports Color Reports Services Reports Services Services Report Services Services Reports Services Services Services Reports Services		Launchetl			DCShadow				Video Capture			Stored Data Manipulation
March Device Marc		Local Job Schoduling	DLL Scarch Order Hijacking	Hooking						Multiband Communication		
The State of		LSASS Driver		Image File Execution Options						Multilayer Encryption		Manipulation
Person Find Dis. Person Find Dis. Person Find		Mahte	Emend	Injection	Disabling Security Tools	Network Sniffing				Port Knocking	[
Figure 1 Section		PowerShell	External Remote Services	Launch Decmon	DLL Search Order Hijacking	Password Filter DLL	Security Seltimens			Romotic Access Tools		
Merch Collegation Merch Collega		ficezes/ficesam		New Service	DLL Sido-Loeding	Private Keya	Discovery		1	Remote file Capy		
Audition of the processor of the process		Mossyr52		Parent PID Specifing	Execution Quardrails	Securityd Memory	Software Discovery					
the final field with Progression State of the Conference of the Co		fundisz		Path Interception	Exploitation for	Steel Web Session Cookie		management.	J			
Souther Service Part Described Copies For the Execution Copies For t		Scheduled Task		Plat Modification	Defense Evasion	Two-Pector Authoritication						
About texturine Expect Source Proc. Decoding Expect Source Proc.		Spripting				interesption						
Signet flow we have detaulied over this value and detaution. Signet flow we was the standard over the		Service Execution		PowerShell Profile			System Nictiverk	1		Uncommonly Used Port	1	
Signed Sorphirms Desiration Sorphirms Desiration Sorphirms Sorphir		Signal Sings Press Press for		Process Injection			Connections Discovery			Web Service	1	
The State State of St			Leunch Agent	Scheduled Task	File Deletion		System Owner/User Discovery				,	
Seement for Friences Authorities Control of					Nic Statem Logical Offsets		System Service Discovery					
This seek of Section 1. The Control of Secti		Source office following	Jauerhet				System Time Discovery					
These used and a she full register of the second se												
Trailed Developer Utilities Legin form Sude Hidden Learn Sude Hidden Learn Learn Learn Sude Hidden Learn Sude Hidden Minden						l	Evasion	l				
Liver broaden Legen Briefs Modern Windows Note Cashing Middlers Windows												
Sude Cathing												
		Windows Menegoment	LSASS Oriver	Sude Caching	HISTORIUS I							

MITRE ATT&CK° Enterprise Framework

attack.mitre.org

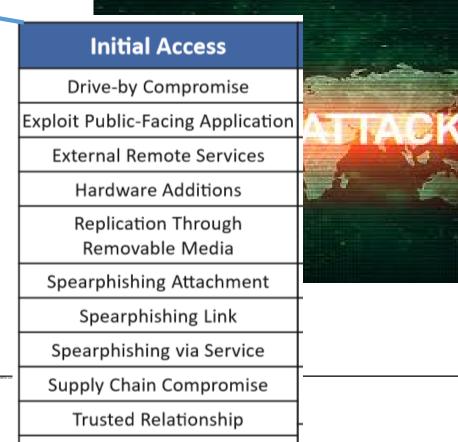


MITRE | SOLVING PROBLEMS



Vulnerability – exposure to threats

	•												
-	1	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact	
Drive-by Compromise		Interiot	.bash_profile and .bashre	Access Token Manipulation	Access Token Manipulation	Account Menipulation	Account Discovery	AppleScript	Audia Capture	Commonly Used PerC	Automated Exfiltration	Account Access Removal	
Exploit Public-Pacing Applicatio		CMSTF	termability features	Accessibility Postures	Sinary Padding	Seah History	Application Window	Application Deployment Software	Automated Collection	Communication Through	Data Compressed	Data Destruction	
External Remote Services			Account	AppCort Dilla	5173 Jobs	Bruite Force	Discovery Semuner Spekmark	Company Offices Model	Clipboard Data	Removable Media Connection Proxy	Deta Encrypted	Deta Encrypted for Impac	
Hardware Additions Replication Through	Compon		AppCort DLIa Appinit DLIa	Application Shimming	Sypess User Account Control	Credential Dumping Credentials from	Discovery	and Distributed CDM	Data from information Repositories	Custom Command	Data Transfer Size Limits Exfiltration Over	Defecement Disk Content Wise	
Removable Media	Company	Dis ributed CDM	Appinit DLIs Application Shimming	Sycess User Account Control	Command History	Web Srowsers	Domain Trust Discovery	Exploitation of Remote Services	Date from Local System	and Control Protocol	Alternative Protocol	Disk Structure Wise	
Spearphishing Attachment	Con	on rol Penci Itoma	Authentication Package	DU. Search Order Hijacking	Code Signing	The files	File and Directory Discovery	Internal Spearphishing	Data from Notwork	Custom Cryptographic Protocol	Editration Over Command	Endpoint Denial of Service	
Spearphishing Link	Dyna		SITS Jobs	Dylib Hijading	Compile After Delivery	Credentials in Region ,	Network Service Scanning	Logon Scripts	Shared Drive Data from	Data thooding	and Control Channel Militation Core	Firmware Corruption	
Spearphishing via Service		ccution through API	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Exploitation for Contential Access	Network Sniffing	Pass the Hash	Removable Media	Data Obfuscation	Other Network Medium	inhibit System Recovery	
Supply Chain Compromise	- 7	Medule Lead	Browser Extensions	Emond	Component firmwere	Perced Authoritication	Password Policy	7max	Date Staged	Domain Fronting	brillitation Over	Network Denial of Service	
Trusted Melationship Valid Accounts		Exploitation for	Change Default File Association	Exploitation for Privilege	Component Object	Hooking	Discovery	Romoto Desktop Protocol		Domain SchoreGon	Physical Medium Scheduled Transfer	Resource Hijecking	
1910 Accounts		Client Execution	Component Firmwere	Establish Esta Window Memory	Model Hijacking Connection Proxy	Input Capture	Peripheral Device Discovery	Remete File Copy	Input Capture	Algorithms	Softgales Irensier	Nurtime Data Manipulatio	
	Graph	phical User Interface	Companent Object Model Hijacking	Injection	Control Panel Items	Input Prompt	Permission Groups	Remote Services Replication Through	Man in the Browser	Multi-hea Presy		Service Step	
	1—	Installutil Launchsti	Create Account	File System Permissions Weakness	OCShedow	Kerberousling	Discovery	Repleation Through Removable Media	Screen Capture Video Capture	Multi-Stage Channels		System Shutdown/Reboo	
	Lee	cal Job Schoduling	DLL Search Order Hijacking	Hooking	Doobfuscate/Docode Files	Keychein	Process Discovery	Shared Webreet	Widea Capture	Multiband Communication	1	Transmitted seem	
		LSASS Driver	Dylib Hijecking	Image File Execution Options	or information	LLMNR/INST-NS Poisoning and Roley	Query Registry Remote System	33H Hijacking		Multilayer Eneryption]	Manipulation	
		Mahte	Emend	Injection	Disabling Security Tools	Network Sniffing	Mometo System Discovery	Taint Shared Content		Port Knocking]		
		PowerShell	External Remote Services	Launch Dacmon	DLL Scarch Order Hijacking	Password Filter DLL	Security Seftmere	Third-party Software		Romoto Access Tools			
		rcs/Rogsam	Mile System Permissions Weakness	New Service	DLL Side-Leading	Private Keys	Discovery	Windows Admin Shares Windows Remote		Remete File Capy	Į.		
		No. 152	Hidden Files and Directories	Parent PID Speefing	Execution Guardrails	Scounityd Momeny	Software Discovery System Information	Windows ficmolic Management		Standard Application Layor Protocol			
		Mundis	Hooking	Path interception	Exploitation for	Steel Web Session Cookie	Discovery		,	Standard Cryptographic Protocol	1		
	3	Scheduled Task	Hypervisor	Port Monitors	Defense Evesion Extre Window	Two-factor Authentication Interception	System Network			Standard Non-Application	1		
	<u> </u>	Soriating	Image file Execution Options	Powershell Profile	Memory Injection		Configuration Discovery			Layer Protocol	ļ		
		Service Execution	Korno dules and Extensions	Process Injection	File and Directory Permissions Medification		System Network Connections Discovery			Uncommonly Used Port Web Service	-		
		Sinary Proxy Execution Script Proxy Execution	Korne Tules and Excersions	Scheduled Task	Permissions Medification File Deletion		System Owner/User Discovery			Web Service	J		
	signes s	Source	Launch	Service Registry Permissions	File System Lagical Offsets		System Service Discovery						
	Soe	acc after filoname	Leunchot	Weakness Setuid and Setgid	Getckcoper Sypess		System Time Discovery						
		ird-party Software	LC_LDAD_DYLIS Additio	Schristery injection	Group Policy Modification		Virtualization/Sandbox Evasion						
		Trap	Local Job Scheduling	Startup Roma	Hidden Files and Directories		Evenion	ı					
	Trusto	ed Developer Utilities	Lagin Rem	Sude	Hidden Users								
		User Exception	Logon Scripts	So Caching	Hidden Window								
	Wind	ndows Management Instrumentation	LSASS Driver	Valid Au eta	HISTOONTROL								
	W	Windows Remote	Medify tristing Service Notah Helper DLL	Web Shelf	Image Nie Execution Options Injection								
		Management	Netsh Helper DLL New Service		Indicator Blocking								
	XSL	L Script Processing	Office Application Startup	1	cator ficmoval from Tools								
			Path interception	1	ins or ficmoval on Host								
			Plat Medification	1	Indirect L. nand Execution								
			Port Knocking	1	Install Root Officato								
			Port Monitors]	installuti								
			PowerShell Profile	1	Launchetl LC_MAIN Hisoking								
			Re-approx		Masquereding		IN.	AITO	г ат	T&C	®		
			Applications		Medify Registry		I\	(/II I I I Z	⊢ДІ	1 X/(_	K		
			Rodundant Access	1	Mahte			A 11 1 1 Z			I 🔪		
			Registry Run Reys /	1	Network Share Connection								
			Stertup Polder Schooluled Teak	-	Nomovel NTFS file Attributes			" I		- Г., -			
			Scheduled Task	1	Obfuscated Files or Information				erprise Frameworl				
							Г	-niei	mrise	→ FI(11 I I I	M/Ori	
			Security Support Provider	1	Perent PID Specifina			:niei	Prise	3 LIC	ai i iev	wori	
			Security Support Provider Server Software		Parent PID Speeding Plat Medification			:niei	prise	3 LIC		wori	
			Security Support Provider Server Softwere Companent					:niei	prise	3 LIC	ar nev	wori	
			Security Support Provider Server Software Component Service Registry		Plat Medification Port Knocking Process Doppelgänging			:niei	prise	3 FIC	arriev	worl	
			Security Support Provider Server Softwere Companent		Plat Modification Port Knocking Process Doppelganging Process Hollowing						ıme	wori	
			Security Support Provider Server Software Component Service Registry Permissions Weekiness Setuid and Setajid Shortout Modification		Plat Modification Port Mosking Process Doppelganging Process Hollowing Process Injection							wori	
			Security Support Provider Server Software Companient Server Registry Permissions Weekness Setuld and Setupid Shortest Modification SIP and Trust		Plat Medification Part Knacking Process Depptiganging Process Hollowing Process Injection Redundant Access							wori	
			Security Support Provider Server Software Component Service Registry Permissions Westness Setuid and Setgid Shortest Modification 31P and Trust Provider Highling		Plist Modification Port Knocking Process Doppelganging Process Hollowing Process Injection Redundant Access Regaves/Regasm				Prise		arrie	wori	
			Security Support Provider Server Software Component Service Registry Permasions Weakness Softsid and Setgid Shortext Medification 3P and Trust Provider Highsting Status Items Status Items Status Items		Plat Modification Perl Knocking Process Depotalizinging Process Injection Process Injection Redundent Access Respons/Regeom Regove22						ше	wori	
			Security Support Provider Server Servers Servers Companent Service Registry Permissions Westernes Setuid and Setaid Shortex Medification Sit and Trust Provider Highling Startup Items System Primare System Primare		Plat Modification Part Knocking Process Doppstjärnjing Process Hollowing Process Injection Modurdient Access Regova/Regeam Megovi2 Modifit Modifit						ш	worl	
			Security Support Provider Server Software Component Service Registry Permasions Weakness Sottod and Sotgid Shortest Weakness 19 P and Trust Provider Highestry Startup Items System Frimmere Systems Springer		Plat Modification Part Modification Part Modeling Process Popplishing Process Injection Redundent Assess Reports/Eagann Regunds:							worl	
			Security Support Provider Server Servers Servers Companent Service Registry Permissions Westernes Setuid and Setaid Shortex Medification Sit and Trust Provider Highling Startup Items System Primare System Primare		Plat Modification Part Modification Part Modeling Process Coppelganging Process Injection Modurdant Access Magnet						ш	worl	
			Security Support Provider Server Software Companent Service Registry Permaisers Vicelances Setvid and Setgid Shortect Modification 37 and Trust Provider Registry Software System Primasers System Primasers System Primasers		Plat Modification Part Modification Part Modeling Process Popplishing Process Injection Redundent Assess Reports/Eagann Regunds:							worl	
			Sexurity Support Provider Server Softwer Correspond Service Registry Permission Violenzas Setud and Setgel Shrotac Modification Sit and Trust Provider Rigistry Satrula (Italia) Satrula (Italia) Satrula (Italia) Satrula (Italia) Satrula (Italia) Satrula (Italia) System Fronzara Systemd Sarvice Time Providers Times		Plat Modification Part Modification Part Modification Process Depolarizing Process relationing Process injection Redundant Access Regional Region Regional Region Regional Region Regional Region Regi						arriev	wori	
			Security Support Provider Server Software Server Regulary Permaneners Vicelenze Service Regulary Permaneners Vicelenze Service Trans Providers Trans		Prior Medification Port Greeking Process Deportiginging Process Hollowing Regional Region Regional Region Regional Region Regional Region Regional Region Regional Region Regi						игте	wori	
			Security Support Provider Serve Serv		Pist Medification Part Growing Process Desprightaring Process Topprightaring Process Intellectual Process Intellec							wori	
			Security Support Provider Server Software Server Regulary Permaneners Vicelenze Service Regulary Permaneners Vicelenze Service Trans Providers Trans		Pist Medification Part Oreology Process Depolphyrip Region Process Region Regio						ше	wori	
			Security Support Provider Correspond Companies Correspond Service Regulary Permissions Vicaliness Bottud and Setupid Shortest Vicaliness Bottud and Setupid Shortest Vicaliness South and Setupid Shortest Vicaliness System France System France System Service Time Provider Time Provider Vicaliness V		Pilat Medification Partitionaling Process Depoplishment Process Periodishment Process Periodishment Process Periodishment Process Periodishment Redundent Assess Regence Process Periodishment Redundent Assess Regence Process Regence Process Reduction Samed Society Process Samed Society						ште	worl	
			Security Support Provider Correspond Companies Correspond Service Regulary Permissions Vicaliness Bottud and Setupid Shortest Vicaliness Bottud and Setupid Shortest Vicaliness South and Setupid Shortest Vicaliness System France System France System Service Time Provider Time Provider Vicaliness V		Piot Vasification Protein State State Protein State State Protein State State Protein Protein State Protein Pr						ште	worl	
			Security Support Provider Correspond Companies Correspond Service Regulary Permissions Vicaliness Bottud and Setupid Shortest Vicaliness Bottud and Setupid Shortest Vicaliness South and Setupid Shortest Vicaliness System France System France System Service Time Provider Time Provider Vicaliness V		Part Inspiration Part Inspiration Part Inspiration Presson Disput Injury Presson Inflation Presson Inflation Presson Inflation Report R						ште	wori	
			Security Support Provider Correspond Companies Correspond Service Regulary Permissions Vicaliness Bottud and Setupid Shortest Vicaliness Bottud and Setupid Shortest Vicaliness South and Setupid Shortest Vicaliness System France System France System Service Time Provider Time Provider Vicaliness V		Pist Intelligence Protocologie Protocologi							wori	
			Security Support Provider Correspond Companies Correspond Service Regulary Permissions Vicaliness Bottud and Setupid Shortest Vicaliness Bottud and Setupid Shortest Vicaliness South and Setupid Shortest Vicaliness System France System France System Service Time Provider Time Provider Vicaliness V		Mich Intelligation Part Consisting Process Depositioning Process Intelligency Process Intelligency Process Intelligency Process Intelligency Report Organia Majorited Assess Report Organia Majorited Assess Report Organia Majorited Assess Report Deposition Report							wori	
SOLVING PROD	BLEM:	S	Security Support Provider Correspond Companies Correspond Service Regulary Permissions Vicaliness Bottud and Setupid Shortest Vicaliness Bottud and Setupid Shortest Vicaliness South and Setupid Shortest Vicaliness System France System France System Service Time Provider Time Provider Vicaliness V		Pist Intelligence Protocologie Protocologi						ште	worl	



Valid Accounts





How cyber secure and resilient is NI

How do we measure cyber security?



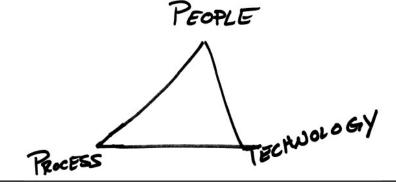


Minimum standard for NI?

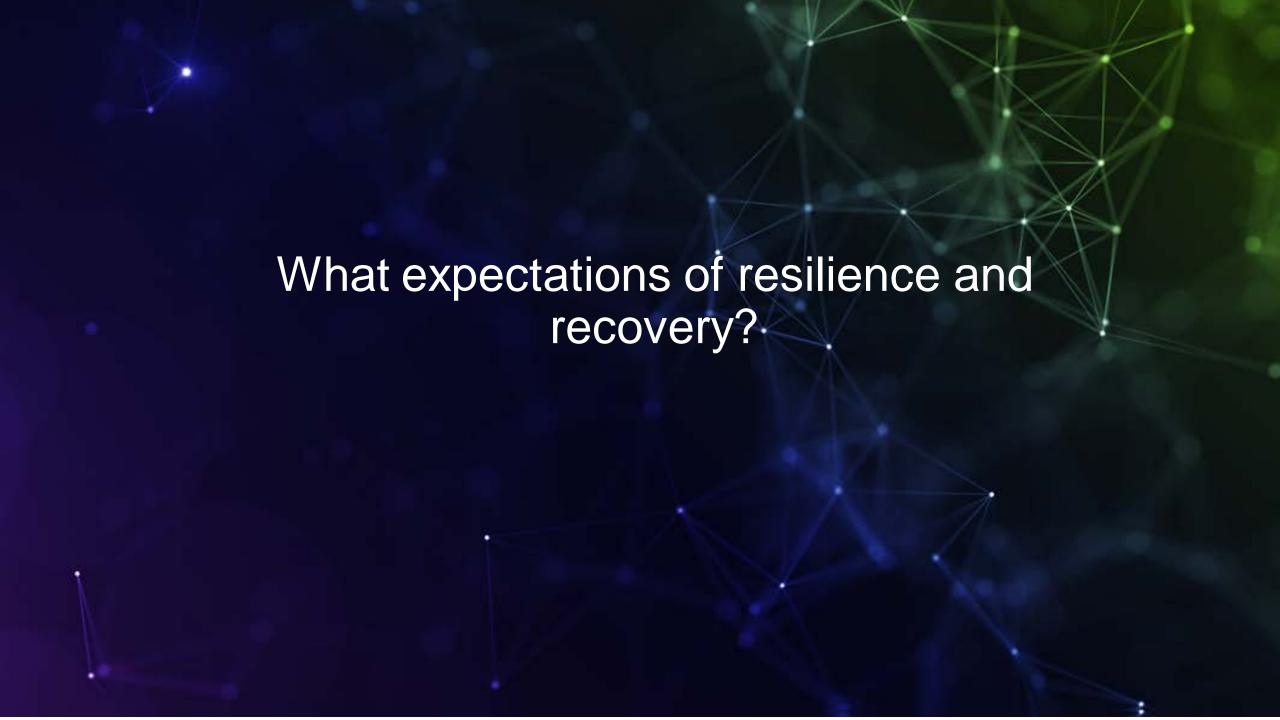


Compliance of standards are a visible demonstration of assurance and good practice

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

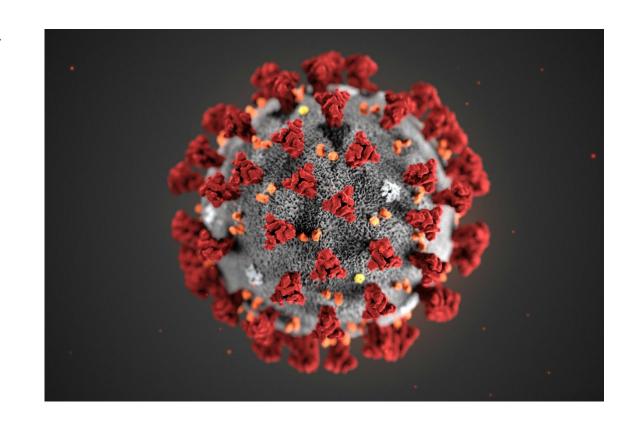






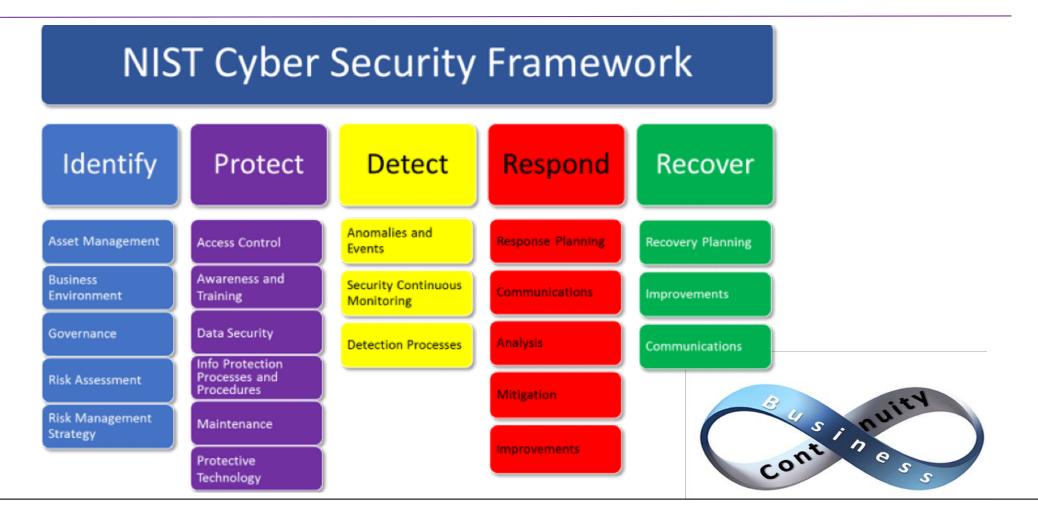
Cyber Resilience

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



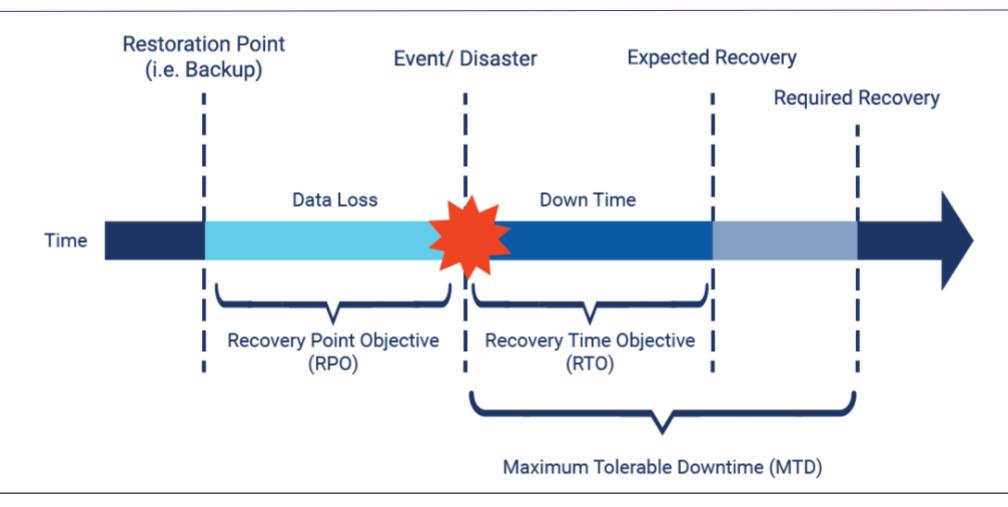


Cyber attack and recovery





Resilience and Recovery





Resilience and Recovery

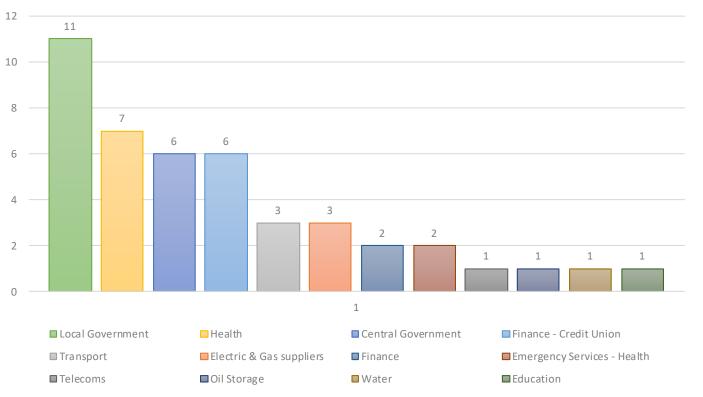
Who sets the levels?





Cyber Resilience – through testing





Good cross sector representation



66% public sector



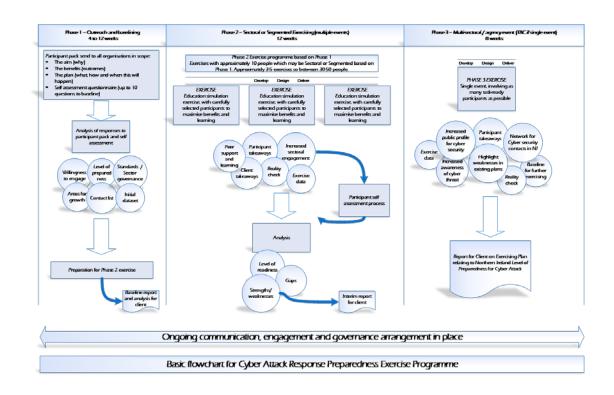
34% private sector



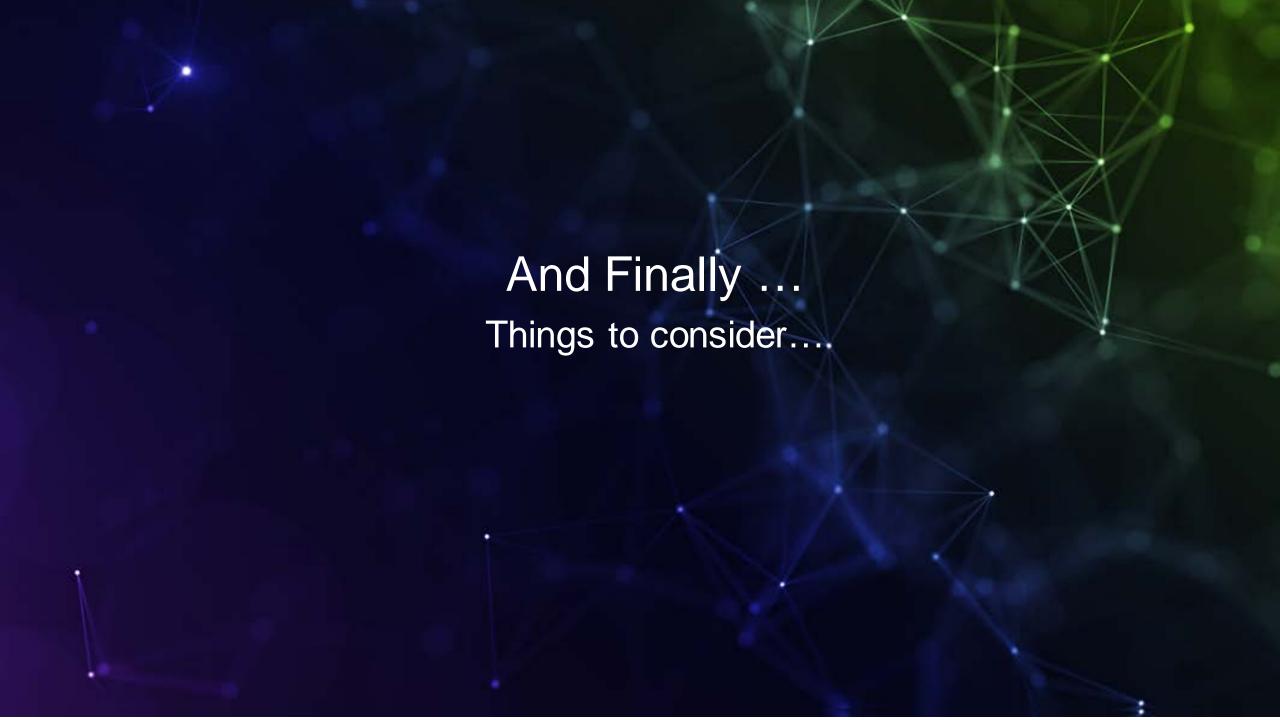


Current baselines

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







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





Website
Contact
Follow us

www.nicybersecruitycentre.gov.uk info@nicybersecuritycentre.gov.uk Twitter @NIcyberSC

#CyberSecureNI