COS80013 Internet Security

Week 1

Presented by Dr Rory Coulter

3 March 2025

SWINBURNE UNIVERSITY OF TECHNOLOGY

Acknowledgement of Country

We respectfully acknowledge the Wurundjeri People of the Kulin Nation, who are the Traditional Owners of the land on which Swinburne's Australian campuses are located in Melbourne's east and outer-east, and pay our respect to their Elders past, present and emerging.

We are honoured to recognise our connection to Wurundjeri Country, history, culture, and spirituality through these locations, and strive to ensure that we operate in a manner that respects and honours the Elders and Ancestors of these lands.

We also respectfully acknowledge Swinburne's Aboriginal and Torres Strait Islander staff, students, alumni, partners and visitors.

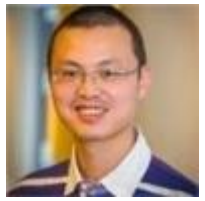
We also acknowledge and respect the Traditional Owners of lands across Australia, their Elders, Ancestors, cultures, and heritage, and recognise the continuing sovereignties of all Aboriginal and Torres Strait Islander Nations.

Unit Overview

SWINBURNE UNIVERSITY OF TECHNOLOGY

Meet the Team

Who are we



Prof Jun Zhang, convenor

Head of the Swinburne Cyber Security Lab

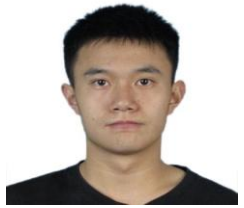
Dr Rory Coulter, lecturer

Academic and industry professional: Incident response, threat detection and response, cyber security exercising, threat intelligence

Mr Yasas Akurudda Liyanage Don, tutor

PhD candidate, a cybersecurity researcher at Swinburne, collaborates with CSIRO on AI privacy and has industry experience.

Mr Hao Jiang (Kevin)



PhD student at Swinburne. Research interests: system resilience, efficient learning

SWINBURNE UNIVERSITY OF TECHNOLOGY

Unit Usuals

Common Questions or Requests

- Lectures are recorded
- Lecture slides are to be available before the lecture
- Weekly announcements identifying what is going on, your responsibilities
- We have made a focus to enable you across the semester to complete your assessment. Labs are highly focused
- A significant portion will be required to achieve well in the unit

- Swinburne email for correspondence
- Raise any concerns with Yasas as your first point of call
- OneDrive, Office 365, back up your work
- Lab machines and Library devices

- Swinburne's extension policy is clear, please adhere to it: https://www.swinburne.edu.au/life-at-swinburne/student-support-services/special-consideration-assistance/

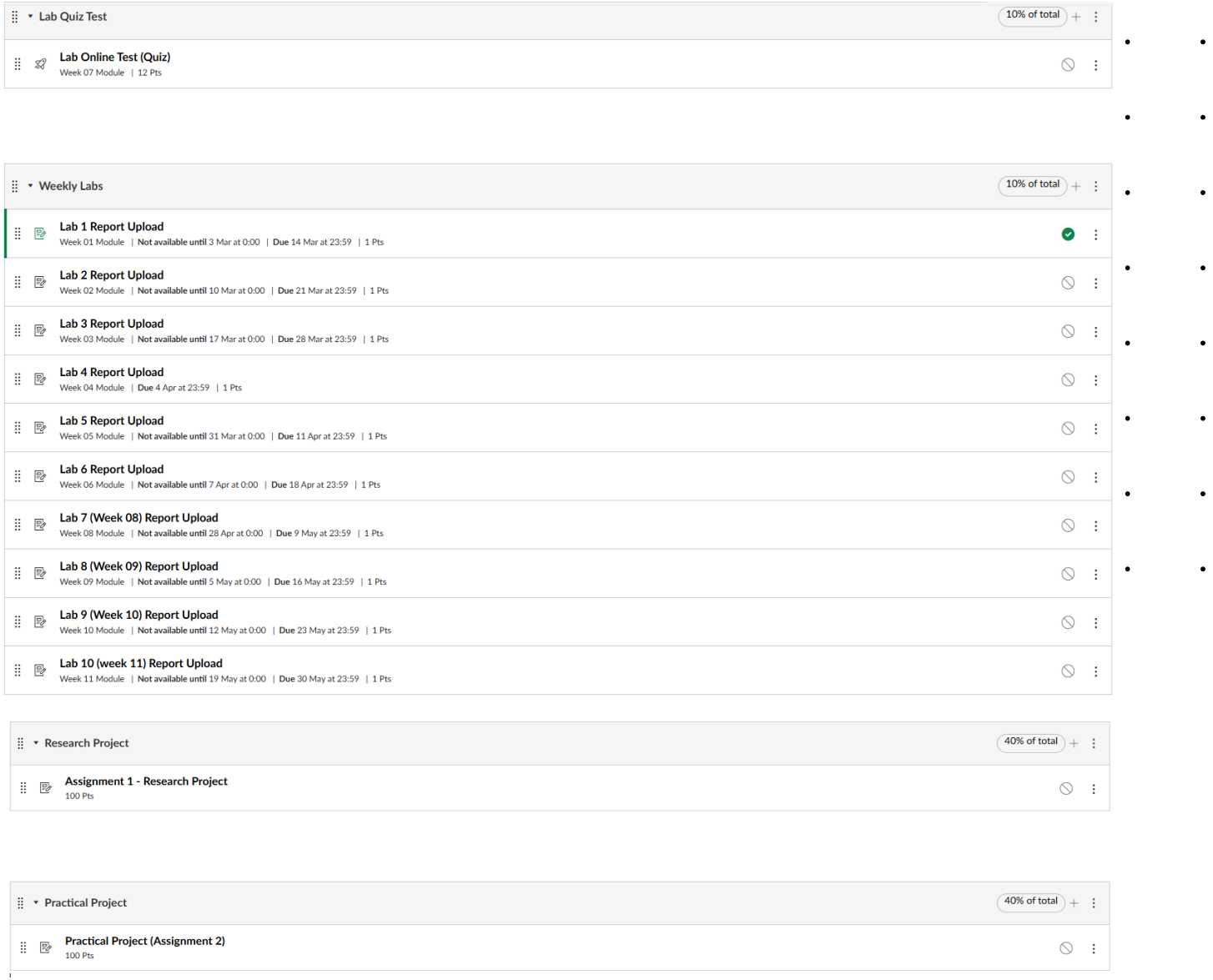
SWINBURNE UNIVERSITY OF TECHNOLOGY

Navigating the Unit

What, When, Expectations

All the usuals

- 12 weeks
- Mid-Semester break week 17 – 23 April
- 3 assessment types:
  - Released week 2 - Assignment 1: A comparative research review
  - Week 7 - Quiz (weeks 1 – 6)
  - Released end of week 6 - Assignment 2: Practical exercise, digital forensic analysis of artefacts, review evidence and perform open source intelligence to respond to a cyber incident
- Range of speakers from industry



Navigating the Unit

What, When, Expectations

What

- 12 Weeks engaging a wide range of cyber security topics
- 4 assessment types:
  - Assignment 1: Technical Review
  - Quiz (weeks 1 – 6)
  - Assignment 2: Practical Exercise
  - Lab Reports
- Lectures online, tutorials in EN207
- Variety of guest speakers from industry
- Yasas and myself will be sharing some content, diversity of knowledge and style is good
- Consultation available upon request

Navigating the Unit

What, When, Expectations

When

- 12 weeks from 3 March 2025 – 2 June 2025
- Mid-Semester break Thursday,17 April - Wednesday, 23 April
- 4 assessment types:
  - Released Week 2 - Assignment 1: Technical Review
  - Week 7 - Quiz (weeks 1 – 6)
  - Released end of week 6 - Assignment 2: Practical Exercise
  - Due following Friday - Lab Reports (weeks 1 – 10)

SWINBURNE UNIVERSITY OF TECHNOLOGY

Navigating the Unit

What, When, Expectations

Expectations

- Regular attendance, both lectures and tutorials
- We are Masters students, you know how to *student* by now, time management exists
- Disappear or prioritise another unit or work, extensions here don't count
- Check weekly modules
- Communicate with your tutor, use discussion board
- Don't spend more time getting around plagiarism controls
- There are usually 3 types of students
  - Those who are enthusiastic
  - Those who participate and get the job done
  - Those who disappear week 1, see above
- Communication
  - Yasas
    - Consultation when requested, TBA
    - Email, 1 - 2 days
- You can expect the following
  - Lectures update you on key tasks
  - Lectures provide guidance on how to do assessments
  - Lectures alert you to responsibilities
  - Tutorials give you a chance to get feedback
  - Weekly communication including those above
  - Consultation

Please see Discussion posts: *Navigating the Unit* and *Extension Policy*

SWINBURNE UNIVERSITY OF TECHNOLOGY

Twelve Weeks

Cyber Security unit, our focus is Cyber Security

What we're trying to do

- Introduce you to a wide range of ideas, concepts, and knowledge
- Some areas we get technical/in depth, others we just scratch the surface
- Provide some theoretical ideas, do some practical tasks
- Practical tasks are academic only, consider the ethics of what you might learn
- Not learning every "attack" type, we actually cover very few
- Do not perform any activities on live systems, laws exist

- Please consult the Syllabus
- There is additional content each week to watch and read
- Note: any assessment that does not follow the specification will receive an instant 0
  - We have seen people use live systems as a part of their assessment
  - This will be an instant 0

SWINBURNE UNIVERSITY OF TECHNOLOGY

Why No Cool Hacks?

We will come to learn Tactics, Techniques and Procedures (TTPs) over cool hacks, but some resources to get started

Knowing TTPs is more beneficial than cool “hacks”, the underlying avenues stay the same

- https://www.asd.gov.au/cyber-security
- https://www.cyber.gov.au/
- https://www.cisa.gov/
- https://www.blackhat.com/
- https://attack.mitre.org/

SWINBURNE UNIVERSITY OF TECHNOLOGY

Core Concepts

Definitions

Principles

Cyber Security Frameworks

Risk

SWINBURNE UNIVERSITY OF TECHNOLOGY

Security Paradigms

Confidentiality, Integrity, Availability (CIA), Information Security, ICT Security, Cyber Security

Confidentiality

- Only those entitled to access the information can see it
- Authorise, encrypt, access control, authenticate, restrict physical access

Integrity

- Information cannot be altered and changes are immediately detectable
- Backup, checksum, hash, correction code

Availability

- Information is available (to read, write) to those who need it without interruption or onerous access restrictions
- Redundant systems, data recovery, disaster planning, UPS, backup power systems, redundant network connections

SWINBURNE UNIVERSITY OF TECHNOLOGY

Security Paradigms

Confidentiality, Integrity, Availability (CIA), Information Security, ICT Security, Cyber Security

Confidentiality

- Only those entitled to access the information can see it
- Authorise, encrypt, access control, authenticate, restrict physical access

Integrity

- Information cannot be altered and changes are immediately detectable
- Backup, checksum, hash, correction code

Availability

- Information is available (to read, write) to those who need it without interruption or onerous access restrictions
- Redundant systems, data recovery, disaster planning, UPS, backup power systems, redundant network connections

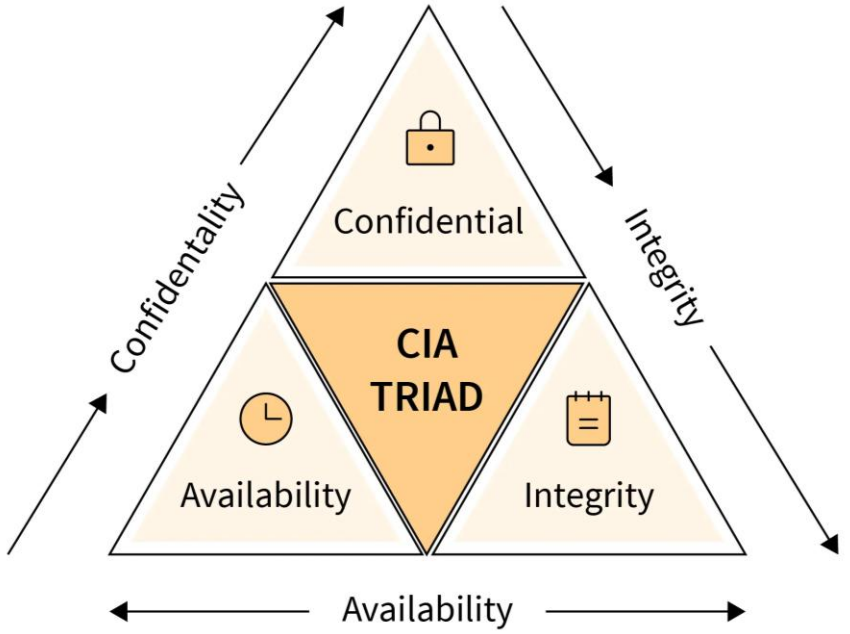
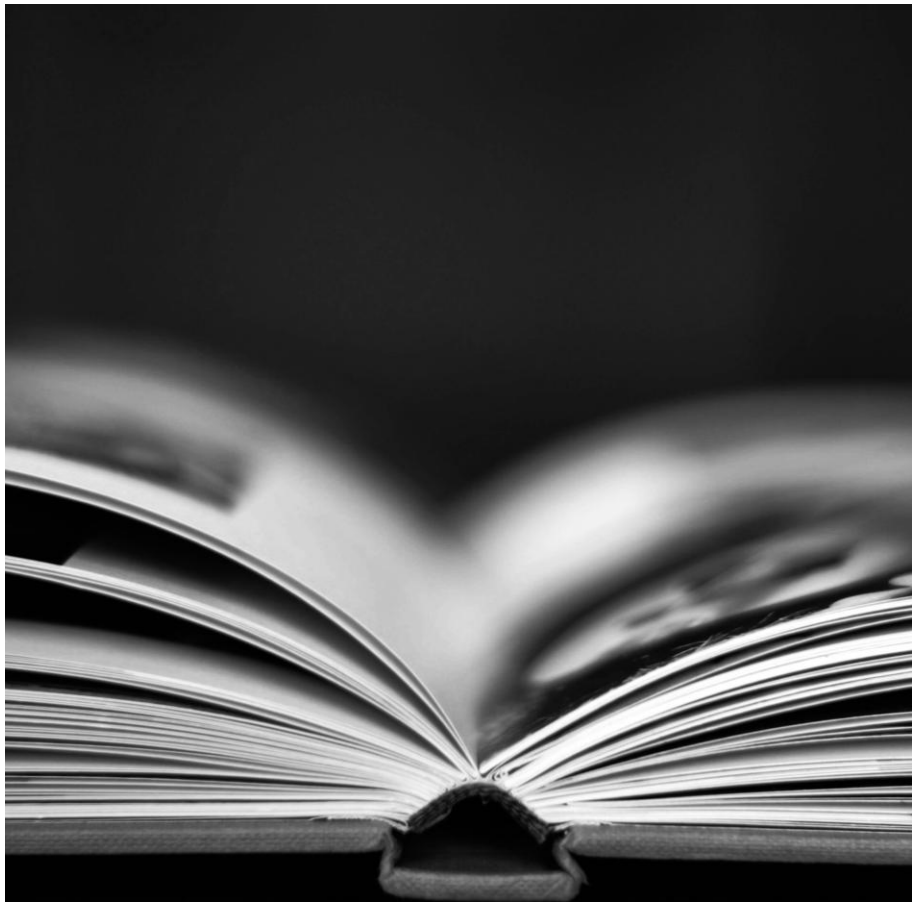


IMAGE SOURCE: https://www.scaler.com/topics/cyber-security/cia-triad/

Security Paradigms



Confidentiality, Integrity, Availability (CIA), Information Security, ICT Security, Cyber Security

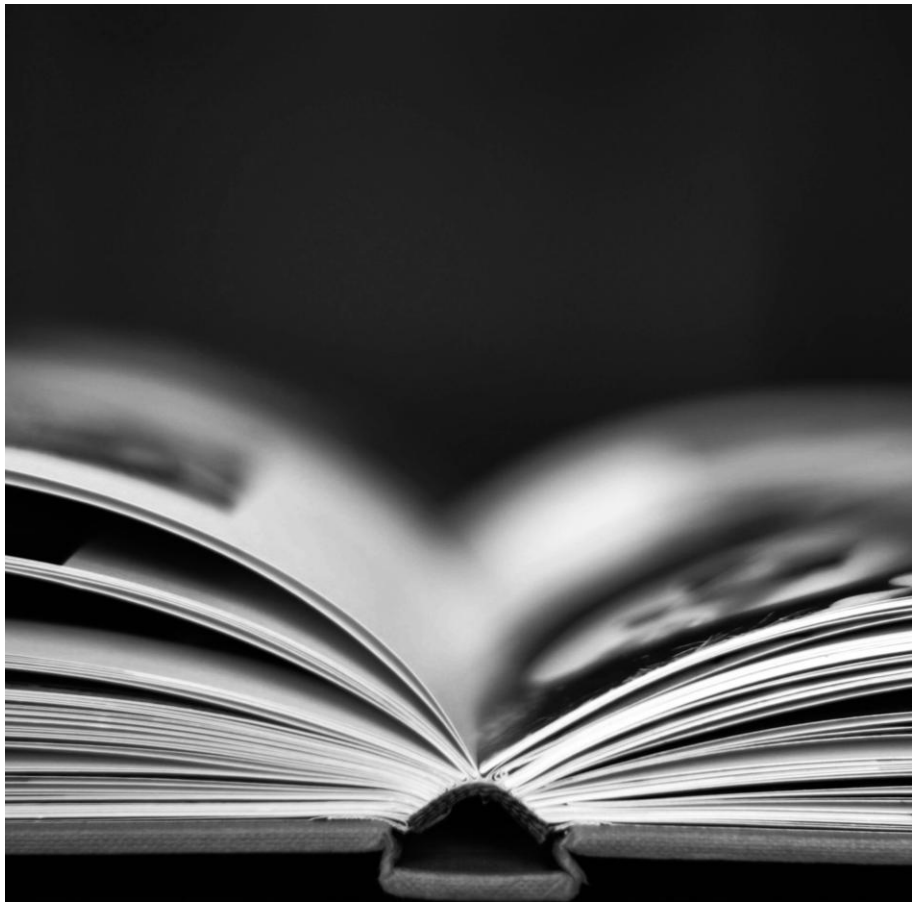
Information Security

Practices to keep data secure, defined in properties data should have CIA

"*The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability*."

SWINBURNE UNIVERSITY OF TECHNOLOGY

Security Paradigms



Confidentiality, Integrity, Availability (CIA), Information Security, ICT Security, Cyber Security

Information Security

Policy:

- What data needs to be protected and in what way
- Password Conditions
- Roles and responsibilities
- Access controls Required

Measures:

- Technical (hardware or software – e.g. encryption/firewall)
- Organisation (staff, team responsibilities)
- Human (training)
- Physical (Access control)

Security Paradigms

Confidentiality, Integrity, Availability (CIA), Information Security, ICT Security, Cyber Security

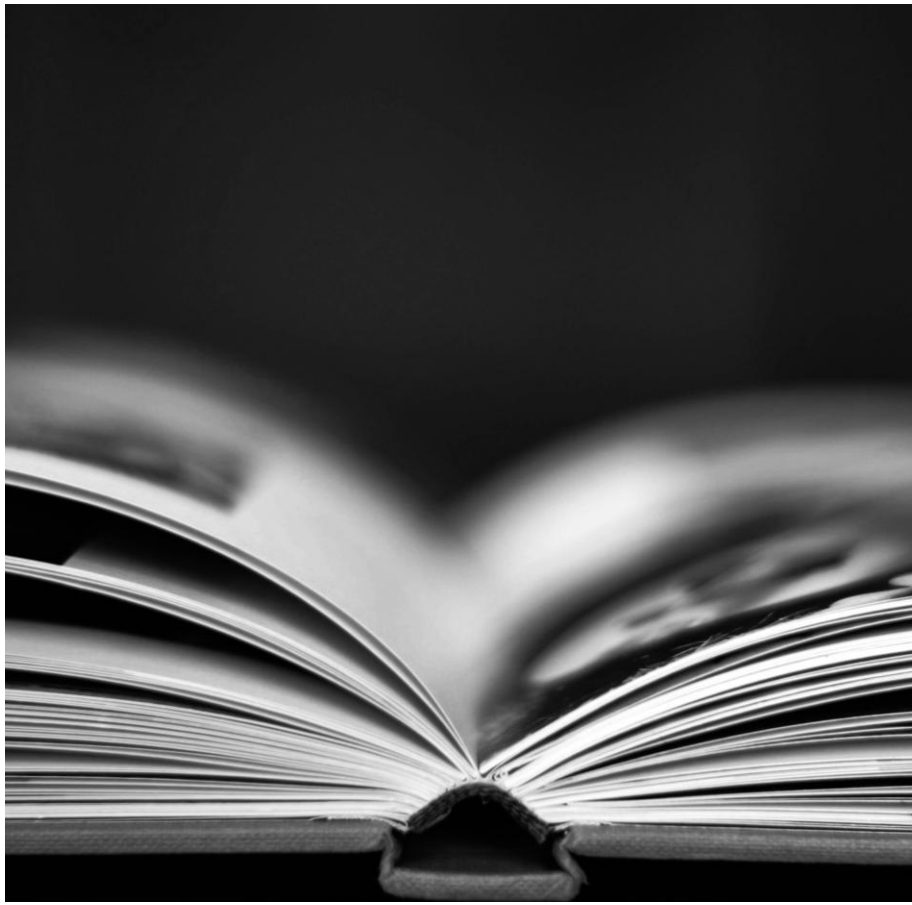
Information Communication Technology (ICT)

ICT:

- Unified communication using telecommunication and computer technology
- Software, storage, AV
- Enable users to access, store, transmit and manipulate information

Security:

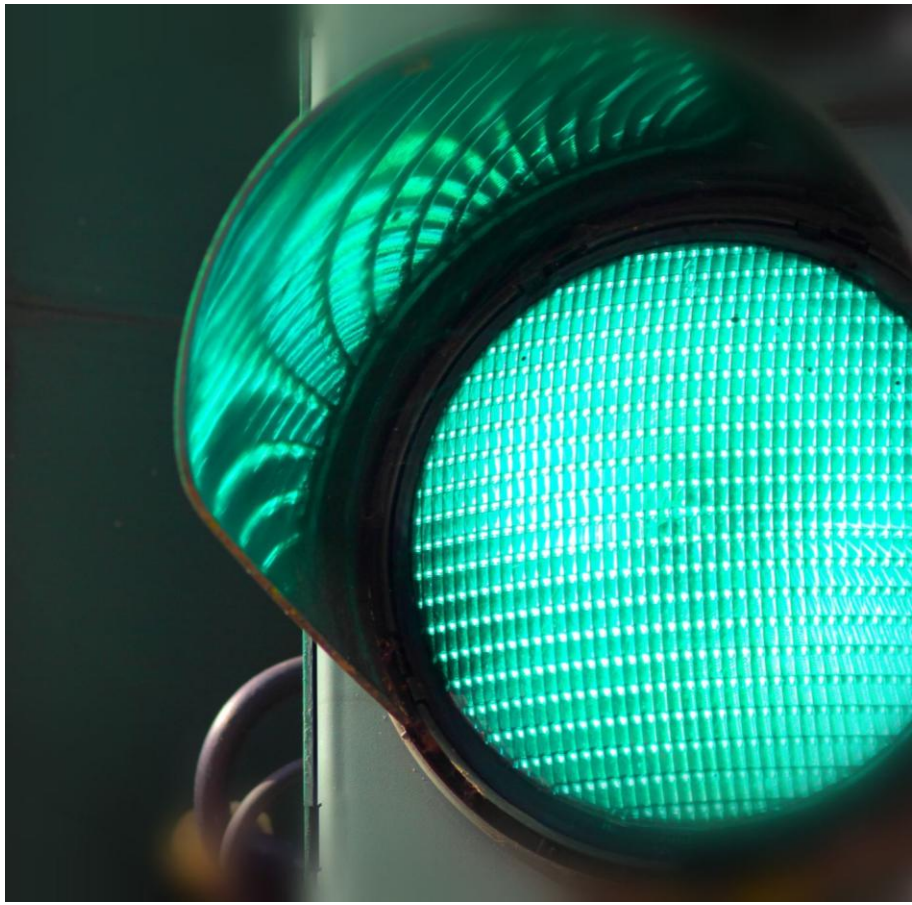
- Protect confidential information from unauthorised use, modification, loss or release
- Monitoring and controlling access
- Safe transmission
- Secure storage and disposal



https://www.cyber.gov.au/acsc/view-all-content/glossary
https://statisticaldataintegration.abs.gov.au/topics/secure-data-management/information-and-communication-technology-security

SWINBURNE UNIVERSITY OF TECHNOLOGY

Security Paradigms



Confidentiality, Integrity, Availability (CIA), Information Security, ICT Security, Cyber Security

Cyber Security

- Information assets:
- Non-information based assets
- Real work assets

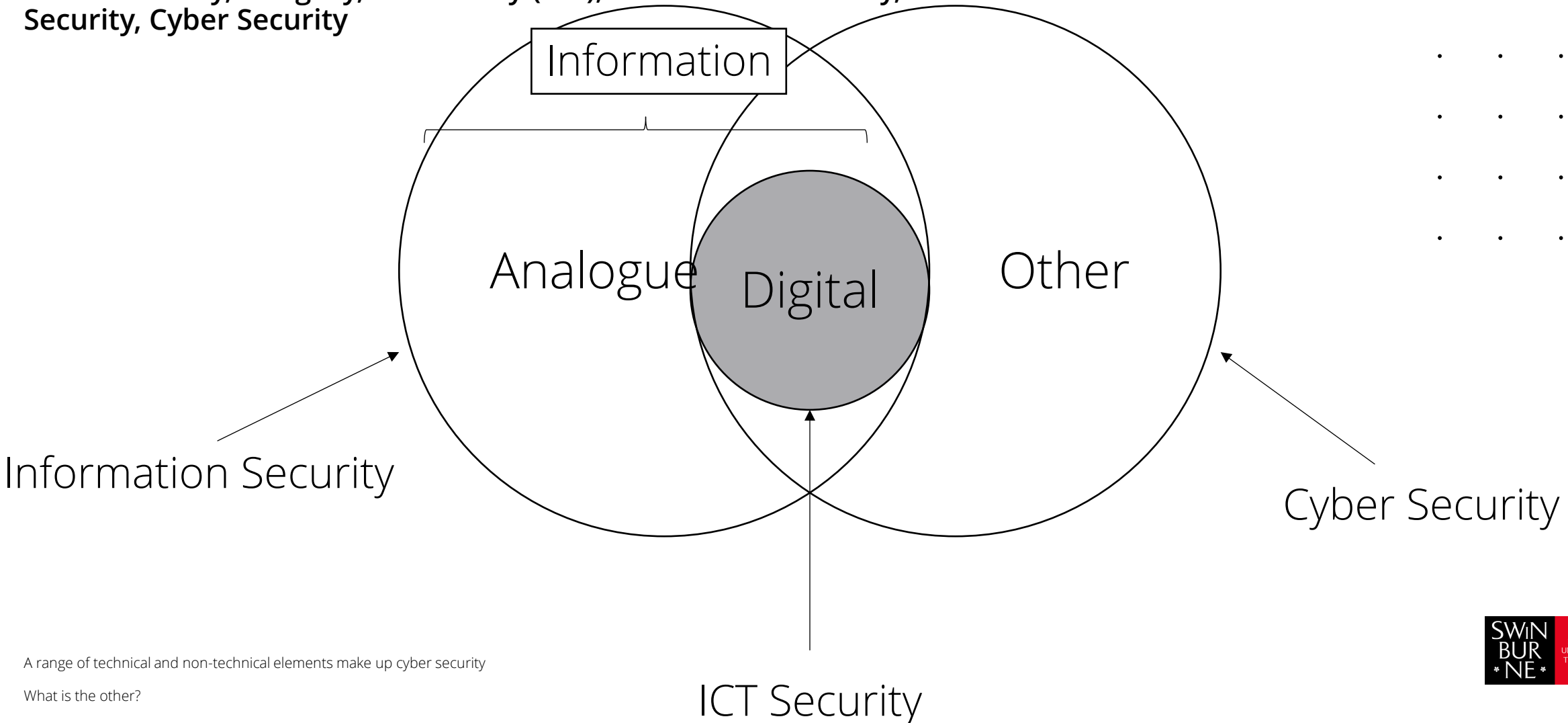
Protect CIA of systems, devices, information

https://www.cyber.gov.au/acsc/view-all-content/glossary
https://statisticaldataintegration.abs.gov.au/topics/secure-data-management/information-and-communication-technology-security

SWINBURNE UNIVERSITY OF TECHNOLOGY

Security Paradigms

Confidentiality, Integrity, Availability (CIA), Information Security, ICT Security, Cyber Security



A range of technical and non-technical elements make up cyber security

What is the other?

Cyber Security Complicates things

Security doesn’t play well with useability

Increased Complexity: Introducing cyber security measures adds layers of complexity to IT systems, making them harder to manage and maintain

Integration Issues: Cyber security solutions may not seamlessly integrate with existing IT infrastructure, leading to compatibility challenges

Resource Intensive: Implementing robust cyber security often requires additional resources, such as skilled personnel and advanced technology, increasing operational costs

User Resistance: Users may resist new security protocols and find them cumbersome, leading to potential non-compliance and security gaps

Training Needs: IT staff and end-users require specialised training to understand and follow cyber security best practices effectively

Balancing Usability and Security: Striking the right balance between usability and security can be challenging, as stringent security measures may impede productivity

Constant Updates: Cyber threats evolve rapidly, necessitating regular updates and adjustments to maintain effective security measures

Core Concepts

Definitions

Principles

Cyber Security Frameworks

Risk

Threat Landscape

A high-level look at actors

Threats	Objectives	Skill	Attack Span
Nation/States	Geopolitical/Espionage, profit	High	Long
Cyber Criminals/Gangs	Profit	Medium - High	Long - Short
Terrorist Groups	Ideology, profit	Medium	Somewhat Short
Hacktivists	Ideology	Medium	Somewhat Short
Insider Threats	Disgruntled, profit, corporate espionage	Medium - Low	Long to short
Script Kiddies	Satisfaction or notoriety	Low	Short

Skill and Span subject to change, variables

Threat Landscape

Common cyber threats

Not a complete list by any means

Threats	Objectives
Cryptomining	Often stealing processing power to mine crypto currency
Data Spill	Data leakage, exfiltration, breach
Denial of Service	Service or Resource is made unavailable (CIA?), Distributed DOS
Hacking	Unauthorised access to a computer system (CIA?)
Identity Theft	Stealing of personal information often for benefits
Malicious insiders	Employees, contractors for example with access, may steal, destroy and sabotage data, service or resources
Malware	Malicious software
Phishing	Steal confidential information
Ransomware	Type of malware which encrypts files for fee
Webshell Malware	Enable remote access to compromised device (think Trojan)

SWINBURNE UNIVERSITY OF TECHNOLOGY

Know your Extorsion

An example of how security is an ever changing game

We've heard of ransomware, lets understand the demands

Extorsion Type	Characteristic
Single	Encrypt, demand a ransom
Double	Threaten to release the data to encourage payment
Triple	Deny service to key systems (DoS)
Quadruple	Extort third parties and victims of incident to encourage payment

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti

Core Concepts
Definitions
Principles
Cyber Security Frameworks
Risk

SWINBURNE UNIVERSITY OF TECHNOLOGY

Cyber Security Principles

Principles provide strategic aims to protect information and operation technology assets

GOVERN: A strong cyber security culture is developed (executive, risk management, audit data and applications)

IDENTIFY: Identify assets and associated security risks (criticality is assessed and documented, CIA assessed for systems, applications and data and documented, risks assessed for systems, applications and data and documented)

PROTECT: Implement controls to manage security risks (systems and applications design, deploy, maintained, decommissioned considering CIA, trusted suppliers, administer securely, manage vulnerabilities, encrypt data, backup, minimum access, identity controls, physical access)*

DETECT: Detect and analyse cyber security events to identify cyber security incidents (event logs collect and are analysed/security events are collected and analysed in a timely manner)

RESPOND: Respond to and recover from cyber security incidents (cyber incidents are reported timely internally/externally, incidents are analysed, contained, eradicated and recovered in a timely manner, incident response, business continuity and disaster recovery plans properly support returning to normal operations)

SOURCE: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-principles

*Not all

Core Concepts
Definitions
Principles
Cyber Security Frameworks
Risk

SWINBURNE UNIVERSITY OF TECHNOLOGY

MITRE ATT&CK Tactics, Techniques and Procedures

Understanding attackers and attacks

"The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique"

- 14 Tactics
  - Consider as technical objective
- 240+ techniques and 370+ sub-techniques for enterprise
  - Way an adversary may achieve an objective
- Procedures as technique method and process

https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures

NIST SP 800-150 Tactics, Techniques, and Procedures (TTPs)

SWINBURNE UNIVERSITY OF TECHNOLOGY

TTPs

A method to categorise actions, behaviours, aims and objectives

MITRE ATT&CK: https://attack.mitre.org/

- We can observe a wide range of attackers, motivations and a diverse set of technologies (both attacker and defender)
- How may we standardise the attacks, actions, and technologies?
- De facto framework
- Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	CMSTP	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Password Policy Discovery	Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking	Hooking	Permission Groups Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Control Panel Items	Input Capture	Process Discovery	Remote Services	Input Capture		Multi-hop Proxy
	Launchctl	Component Firmware	File System Permissions Weakness	DCShadow	Input Prompt	Query Registry	Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information	Kerberoasting	Remote System Discovery	Shared Webroot	Screen Capture		Multiband Communication
	LSASS Driver	Create Account	Image File Execution Options Injection	Disabling Security Tools	Keychain	Security Software Discovery	SSH Hijacking	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon	DLL Search Order Hijacking	LLMNR/NBT-NS Poisoning	System Information Discovery	Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	DLL Side-Loading	Network Sniffing	System Network Configuration Discovery	Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion	Password Filter DLL	System Network Connections Discovery	Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection	Private Keys	System Owner/User Discovery	Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Port Monitors	File Deletion	Replication Through Removable Media	System Service Discovery				Standard Cryptographic Protocol
	Scheduled Task	Hooking	Process Injection	File System Logical Offsets	Securityd Memory					Standard Non-Application Layer Protocol
	Scripting	Hypervisor	Scheduled Task	Gatekeeper Bypass	Two-Factor Authentication Interception					Uncommonly Used Port
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Hidden Files and Directories						Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	Hidden Users						
	Signed Script Proxy Execution	Launch Agent		Hidden Window						
	Source			HISTCONTROL						
	Space after Filename			Image File Execution Options Injection						

Extra viewing: https://www.youtube.com/watch?v=Yxv1suJYMI8&embeds_euri=https%3A%2F%2Fwww.mitre.org%2F&feature=emb_imp_woyt

https://www.rapid7.com/fundamentals/mitre-attack/

SWINBURNE UNIVERSITY OF TECHNOLOGY

An Example – Impact [T1486]

Impact

The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes. Techniques used for impact can include destroying or tampering with data. In some cases, business processes can look fine, but may have been altered to benefit the adversaries' goals. These techniques might be used by adversaries to follow through on their end goal or to provide cover for a confidentiality breach.

ID: TA0040
Created: 14 March 2019
Last Modified: 25 July 2019

Version Permalink

Techniques

Techniques: 13

ID	Name	Description
T1531	Account Access Removal	Adversaries may interrupt availability of system and network resources by inhibiting access to accounts utilized by legitimate users. Accounts may be deleted, locked, or manipulated (ex: changed credentials) to remove access to accounts. Adversaries may also subsequently log off and/or perform a System Shutdown/Reboot to set malicious changes into place.
T1485	Data Destruction	Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources. Data destruction is likely to render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives. Common operating system file deletion commands such as `del` and `rm` often only remove pointers to files without wiping the contents of the files themselves, making the files recoverable by proper forensic methodology. This behavior is distinct from Disk Content Wipe and Disk Structure Wipe because individual files are destroyed rather than sections of a storage disk or the disk's logical structure.
T1486	Data Encrypted for Impact	Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.

Mitigations

ID	Mitigation	Description
M1040	Behavior Prevention on Endpoint	On Windows 10, enable cloud-delivered protection and Attack Surface Reduction (ASR) rules to block the execution of files that resemble ransomware. [95]
M1053	Data Backup	Consider implementing IT disaster recovery plans that contain procedures for regularly taking and testing data backups that can be used to restore organizational data.[96] Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery. Consider enabling versioning in cloud environments to maintain backup copies of storage objects.[97]

Detection

ID	Data Source	Data Component	Detects
DS0010	Cloud Storage	Cloud Storage Modification	Monitor for changes made in cloud environments for events that indicate storage objects have been anomalously modified.
DS0017	Command	Command Execution	Monitor executed commands and arguments for actions involved in data destruction activity, such as vssadmin, wbadmin, and bcdedit
DS0022	File	File Creation	Monitor for newly constructed files in user directories.
		File Modification	Monitor for changes made to files in user directories.
DS0033	Network Share	Network Share Access	Monitor for unexpected network shares being accessed on target systems or on large numbers of systems.
DS0009	Process	Process Creation	Monitor for newly constructed processes and/or command-lines involved in data destruction activity, such as vssadmin, wbadmin, and bcdedit.

Data Encrypted for Impact

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.[1][2][3][4]

In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as File and Directory Permissions Modification or System Shutdown/Reboot, in order to unlock and/or gain access to manipulate these files.[5] In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.[3]

To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like Valid Accounts, OS Credential Dumping, and SMB/Windows Admin Shares.[2][3] Encryption malware may also leverage Internal Defacement, such as changing victim wallpapers, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").[6]

In cloud environments, storage objects within compromised accounts may also be encrypted.[7]

ID: T1486
Sub-techniques: No sub-techniques
Tactic: Impact
Platforms: IaaS, Linux, Windows, macOS
Impact Type: Availability
Contributors: ExtraHop; Harshal Tupsamudre, Qualys; Mayuresh Dani, Qualys; Oleg Kolesnikov, Securonix; Travis Smith, Qualys
Version: 1.4
Created: 15 March 2019
Last Modified: 16 June 2022

Version Permalink

Procedure Examples

ID	Name	Description
G0082	APT38	APT38 has used Hermes ransomware to encrypt files with AES256.[8]
G0096	APT41	APT41 used a ransomware called Encryptor RaaS to encrypt files on the targeted systems and provide a ransom note to the user.[9]

SWINBURNE UNIVERSITY OF TECHNOLOGY

Application of TTPs

TTPs contribute to many areas of cyber security

For example

- Threat Intelligence: Security teams leverage ATT&CK to enhance their threat intelligence by mapping and understanding the techniques and procedures used by various threat actors
- Incident Response: During incident response, ATT&CK provides a common language and framework for analysing and describing the actions of adversaries, aiding in effective incident handling and mitigation, remediation to combat TTPs
- Red Teaming: Organisations use ATT&CK in red teaming exercises to simulate real-world cyberattacks, test defences, and identify potential vulnerabilities.
- Defensive Strategies: Develop proactive defensive strategies by helping security professionals prioritise security measures based on known adversary behaviours
- Tool Selection: Security teams can use ATT&CK to evaluate and select cyber security tools that align with the specific techniques and tactics most relevant to their organisation's threat landscape

MITRE has lots more than TTPs, I would encourage you to explore Actors and Software too

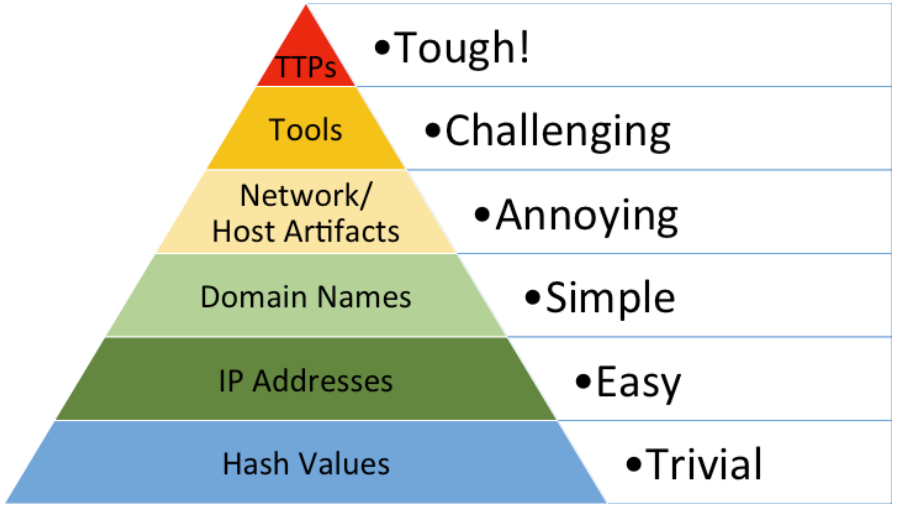
SWINBURNE UNIVERSITY OF TECHNOLOGY

Threat Detection or Incident Response

TTPs are the end game

Attacker artefacts which might contribute to TTPs

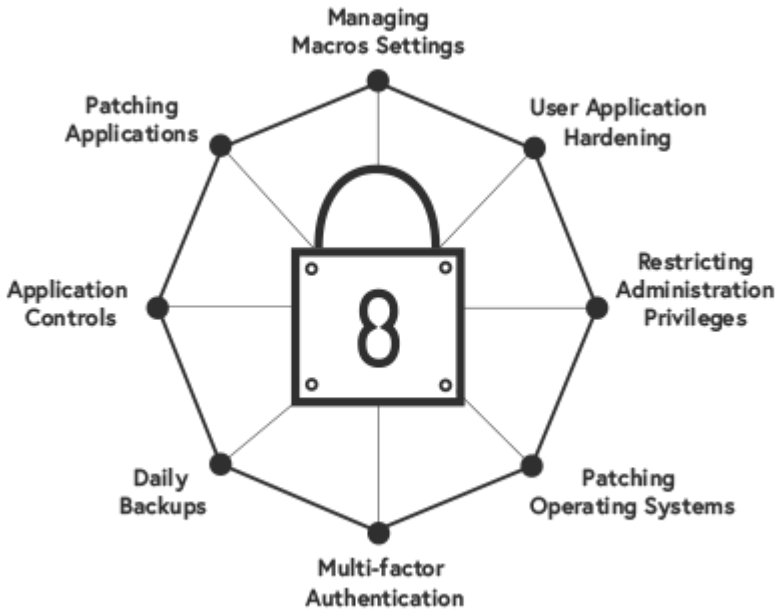
- Hash values: Signature of artefact, e.g., SHA-1 and MD5. Could be software or string
- IP addresses: Destination device
- Domain names: Attacker domain or compromised domain
- Network artifacts/host artifacts: Result of activity
- Tools: Attacker tools
- Tactics, techniques, and procedures (TTPs): Attacker behaviour or modus operandi which helps identify



Bianco, D. (2013). The pyramid of pain. Enterprise Detection & Response. https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

ASD - ACSC Essential 8

Covering 8 most essential areas from repeat analysis of threat landscape



- A set of mitigation strategies (8 in total)
- Administering application controls
- Patching vulnerable applications
- Managing macros setting
- User application hardening
- Restricting administrative privileges
- Patching operating systems
- Implementing and strengthening multi-factor authentication
- Initiate daily backups

IMAGE SOURCE: https://www.itstrategic.com.au/

1. APPLICATION CONTROL

To prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Hosts, Powershell and HTA) and installer.

2. APPLICATION PATCHING

Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.

3. CONFIGURE MICROSOFT OFFICE MACRO SETTINGS

Block macros from the internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.

4. USER APPLICATION HARDENING

Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet.
Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.

5. RESTRICT ADMINISTRATIVE PRIVILEGES

Restrict Administrative Privileges
Restrict administrative privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.

6. PATCH OPERATING SYSTEMS

Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.

7. MULTI-FACTOR AUTHENTICATION

Implement multi-factor authentication (MFA) for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.

8. DAILY BACKUPS

Maintain a daily backup of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.

IMAGE SOURCE: https://acurus.com.au/what-is-the-essential-8-and-why-should-you-be-interested/

SWINBURNE UNIVERSITY OF TECHNOLOGY

An Example

Appendix A: Maturity Level One

Mitigation Strategy	Description
Patch applications	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.
	A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.
	Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.

Appendix B: Maturity Level Two

Mitigation Strategy	Description
Patch applications	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.
	A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.
	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.

IMAGE SOURCE: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model

SWINBURNE UNIVERSITY OF TECHNOLOGY

An Example (cont.)

Appendix B: Maturity Level Two

Mitigation Strategy	Description
Patch applications	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.
	A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.
	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.

Appendix C: Maturity Level Three

Mitigation Strategy	Description
Patch applications	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.
	Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
	Patches, updates or other vendor mitigations for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release.
	Online services that are no longer supported by vendors are removed.

IMAGE SOURCE: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model

SWINBURNE UNIVERSITY OF TECHNOLOGY

Mapping the ASD Essential 8 to the Mitre ATTACK™ framework

ASD Essential 8	MITRE ATT&CK™ Tactics	MITRE ATT&CK™ Techniques	Description
Application Whitelisting	Execution	T1204: User Execution	Prevents execution of unauthorized software.
		T1059: Command and Scripting Interpreter	
Patch Applications	Exploitation for Client Execution	T1203: Exploitation for Client Execution	Protects against exploitation of software vulnerabilities.
Configure Microsoft Office Macro Settings	Defense Evasion	T1027: Obfuscated Files or Information	Limits macro execution to prevent evasion techniques.
Multi-factor Authentication	Credential Access	T1110: Brute Force	Enhances security by requiring multiple forms of verification.
Daily Backup of Important Data	Impact	T1486: Data Encrypted for Impact	Ensures data recovery, mitigating ransomware impact.

SOURCE: https://www.reliaquest.com/blog/mapping-the-asd-essential-8-to-the-mitre-attck-framework/

SWINBURNE UNIVERSITY OF TECHNOLOGY

NIST Cyber Security Framework

- **Identify:** To protect against cyber attacks, the cyber security team needs a thorough understanding of the organisation's most important assets and resources

- **Protect:** The protect function covers much of the technical and physical security controls for developing and implementing appropriate safeguards and protecting critical infrastructure

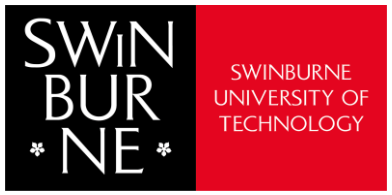
- **Detect:** The detect function implements measures that alert an organisation to cyber attacks. Detect categories include anomalies and events, security, continuous monitoring and detection processes

- **Respond:** The respond function categories ensure the appropriate response to cyber attacks and other cybersecurity events

- **Recover:** Recovery activities implement plans for cyber resilience and ensure business continuity in the event of a cyber attack, security breach or other cybersecurity event

IMAGE SOURCE: https://www.cisco.com/c/en/us/products/security/what-is-nist-csf.html

Risk



Cyber Risk

Risk is a driving factor across multiple cyber viewpoints

Let's consider two perspectives on risk

- Risk itself can be considered exposure to danger, harm, loss, negative impact
- Loss of confidentiality, integrity, or availability of information, data, or information (or control) systems
  - potential adverse impacts to organisational operations and assets, individuals, other organizations, and the Nation
- Potential Impact of Threat x Attack Likelihood = Cyber Risk
- The existence of risk requires it to be framed, assessed, respond and monitored
  - Components of Risk management
  - Multitiered Risk Management

https://csrc.nist.gov/glossary/term/cybersecurity_risk

https://www.tenable.com/principles/cyber-risk-principles#chapter-2

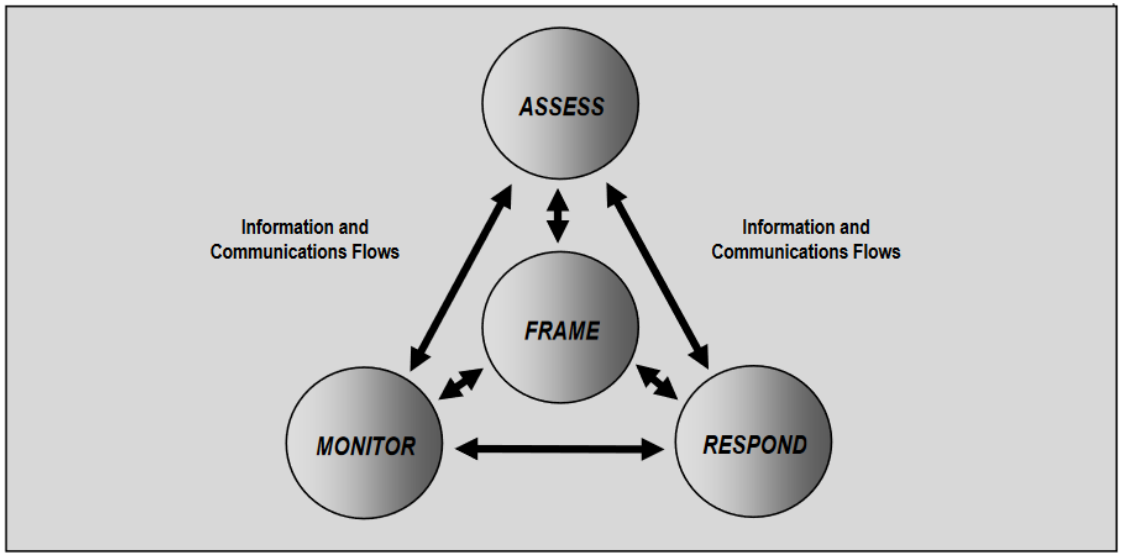
SWINBURNE UNIVERSITY OF TECHNOLOGY

Risk Management

Components

Let's consider two perspectives on risk

- Frame or "describing the environment in which risk-based decisions are made"
  - Assumptions, constraints, tolerance, priorities
- Assess
  - Assess given framing context
- Respond
  - Develop to implement risk response
- Monitor
  - Verify, ongoing effectiveness, changes



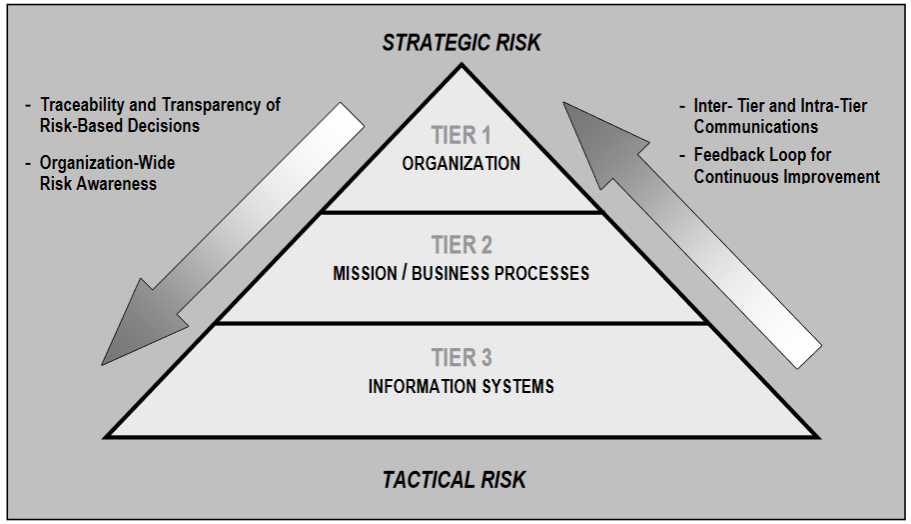
https://csrc.nist.gov/glossary/term/cybersecurity_risk

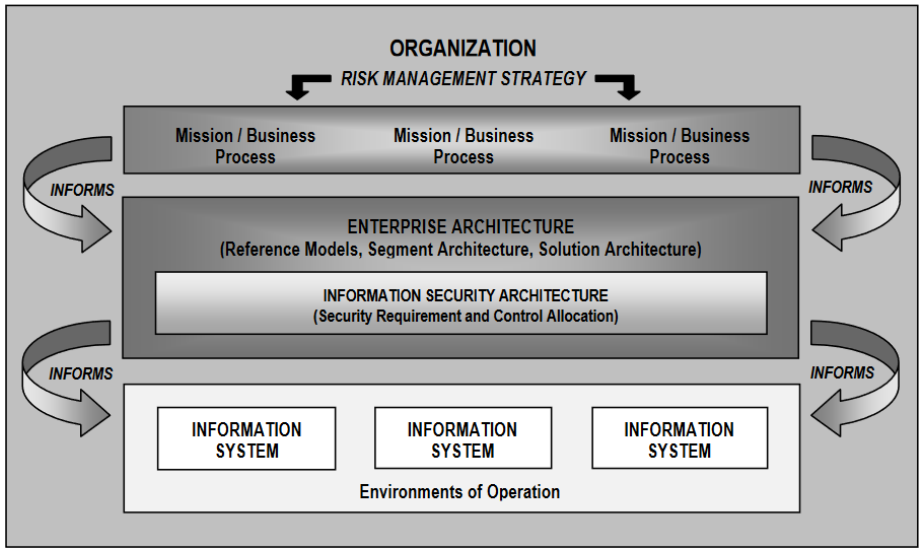
Risk Management

Multitiered Risk Management

Three level approach

- Tier 1
  - Organisation risk, Framing
- Tier 2
  - Risk associated with business/mission processes
  - Information/Information security of business
  - Enterprise architecture
- Tier 3
  - Risk associated for information system
  - Controls aligned to architecture
  - Managing and monitoring





https://csrc.nist.gov/glossary/term/cybersecurity_risk

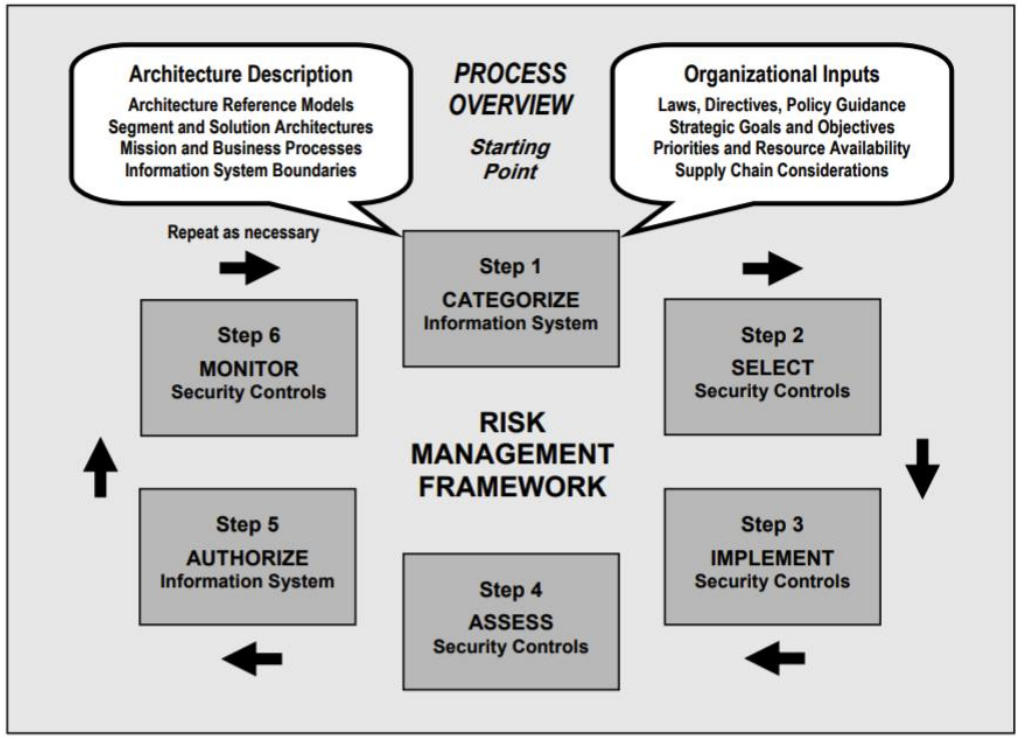
SWINBURNE UNIVERSITY OF TECHNOLOGY

Risk Management Framework

NIST

Cyclical Approach

- Categorise
- Select
- Implement
- Assess
- Authorise
- Monitor



https://csrc.nist.gov/glossary/term/cybersecurity_risk

Risk Management

Categorising issues

Consequence Rating	Sample Interpretation
Insignificant	Little disruption Managed through standard business operations, broad stakeholders Minor effort required for technology in use
Minor	Minor disruption Availability of service is restricted Receiving key stakeholder, management attention
Moderate	Some inconvenience Availability of service is compromised severely Moderate effort required for alternative solution implementation Activities or service receiving public criticism from key stakeholders
Major	Noticeable user impact Some core services unavailable Potential for serious distress or minor injury Sustainability of current operations receives sustained criticism from majority portion of key stakeholders
Catastrophic	Community unable to function without significant support Key technologies no longer available and no viable alternative exists Potential for major injury or fatalities Irreparable damage to relationships with key stakeholders and potential for organisation to cease operating in current form

SWINBURNE UNIVERSITY OF TECHNOLOGY

Risk Management

Likelihood

Recall impact and likelihood?

Likelihood Rating	Example Interpretation
Almost certain	The event is expected to occur. (e.g., 1 incident every month)
Likely	The event will probably occur. (e.g., 1 incident every 6 months)
Possible	The event should occur at some time. (e.g., 1 incident every year)
Unlikely	The event could occur at some time. (e.g., 1 incident every 2 years)
Rare	The event may occur only in exceptional circumstances. (e.g., 1 incident every 5 or more years)

Cyber Risk Matrix

Potential Impact of Threat x Attack Likelihood = Cyber Risk

	Rare	Unlikely	Possible	Likely	Almost Certain
Insignificant	Very Low	Very Low	Very Low	Low	Low
Minor	Very Low	Low	Low	Low	Low
Moderate	Low	Medium	Medium	Medium	Medium
Major	Medium	Medium	High	High	High
Catastrophic	High	High	Extreme	Extreme	Extreme

SWINBURNE UNIVERSITY OF TECHNOLOGY

Cyber Risk Governance and Compliance

Importance of Cyber Risk Governance

- Aligns cybersecurity strategies with business objectives
- Ensures accountability for cyber risk management
- Supports a proactive approach to risk mitigation

Key Cybersecurity Regulations and Frameworks

- GDPR (General Data Protection Regulation)
- CCPA (California Consumer Privacy Act)
- NIS Directive (EU)
- Australia's Essential Eight Framework

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

SWINBURNE UNIVERSITY OF TECHNOLOGY

Cyber Insurance

Any breach, theft, or compromise of electronic data can have detrimental effects on your business. It may lead to loss of customer trust, damaging your company's reputation, or result in significant financial expenses required to recover from the incident. Cyber insurance can help mitigate these financial risks, preventing your business from bearing the full cost of recovery.

Cyber insurance can assist in covering:

- Legal expenses
- Costs associated with restoring the identities of affected customers
- Expenses for recovering compromised data, such as in ransomware attacks
- Overall repair costs for damaged computer systems
- Financial obligations related to notifying customers about potential data breaches

The cyber insurance industry creates jobs in a variety of roles, including underwriting, cyber security analysis, and risk management.

What Is Cyber Insurance? | Trend Micro (AU)

SWINBURNE UNIVERSITY OF TECHNOLOGY

Emerging Trends in Cyber Risk

- AI and machine learning in cyber risk assessment
- Quantum computing threats to cryptography
- Growing impact of nation-state cyber warfare
- The rise of ransomware-as-a-service (RaaS)
- Zero Trust Architecture (ZTA)

SWINBURNE UNIVERSITY OF TECHNOLOGY

Notable cyber risk incidents

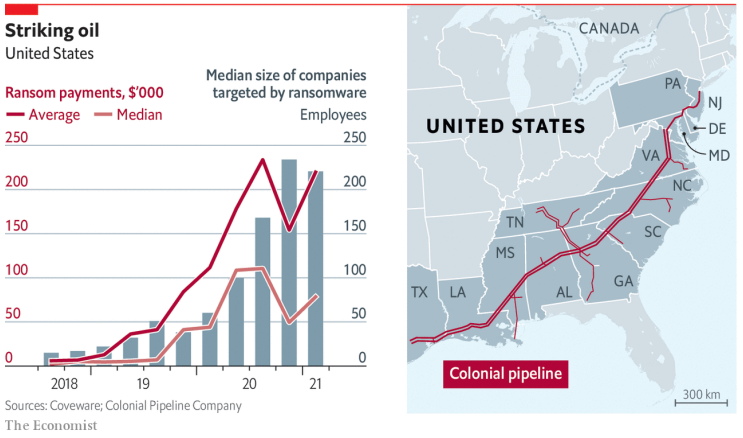
Equifax Data Breach (2017)

- The affected portal had the username and password set to “admin”, making it extremely easy to breach.
- The vulnerability exploited was known for two months before the attack, and a patch was available but not applied.
- Equifax’s official Twitter accidentally linked users to a fake phishing site instead of their security help page.
- Senior executives sold $1.8 million in stock before publicly announcing the breach.
- Equifax promised $125 per affected person, but due to high demand, many people got less than $5.

Economist.com

Colonial Pipeline Ransomware Attack (2021)

- The hackers gained access through an unused employee VPN account that had no multi-factor authentication.
- Panic buying caused massive gas shortages along the East Coast, with people filling plastic bags, laundry baskets, and even kiddie pools with gasoline.
- The ransomware group DarkSide tried to act professional, claiming they only wanted money and did not intend to cause social disruption.
- Colonial Pipeline paid $4.4 million in Bitcoin to DarkSide. But, thanks to FBI cyber experts, $2.3 million of the ransom was later recovered, proving that sometimes crime doesn't pay (at least, not fully).
- Shortly after the attack, DarkSide's servers were seized by law enforcement, and they lost access to their own ransom payments.



Introduction to MITRE ATT&CK

Agenda

- Introduction to the MITRE ATT&CK Matrix.
- Key concepts: Tactics, Techniques, and Procedures (TTPs).
- Using the ATT&CK Navigator for threat actor analysis.
- Practical exercise and case studies.

Goals

- Gain a solid understanding of the MITRE ATT&CK framework.
- Learn to use the ATT&CK Navigator for analyzing cyber threats.
- Apply knowledge to real-world scenarios and case studies.

What is the MITRE ATT&CK Matrix?

Definition

•MITRE ATT&CK Matrix stands for Adversarial Tactics, Techniques, and Common Knowledge.

•A framework developed by MITRE to categorize and understand the tactics, techniques, and procedures (TTPs) used by attackers.

Purpose

•Provides a common language and framework for cybersecurity professionals.

•Helps identify and respond to cyber threats.

•Used by security analysts, incident responders, and cybersecurity professionals to develop effective defense strategies.

Components:

•**Tactics**: The goals or objectives of an attacker.

•**Techniques**: The specific methods attackers use to achieve their goals.

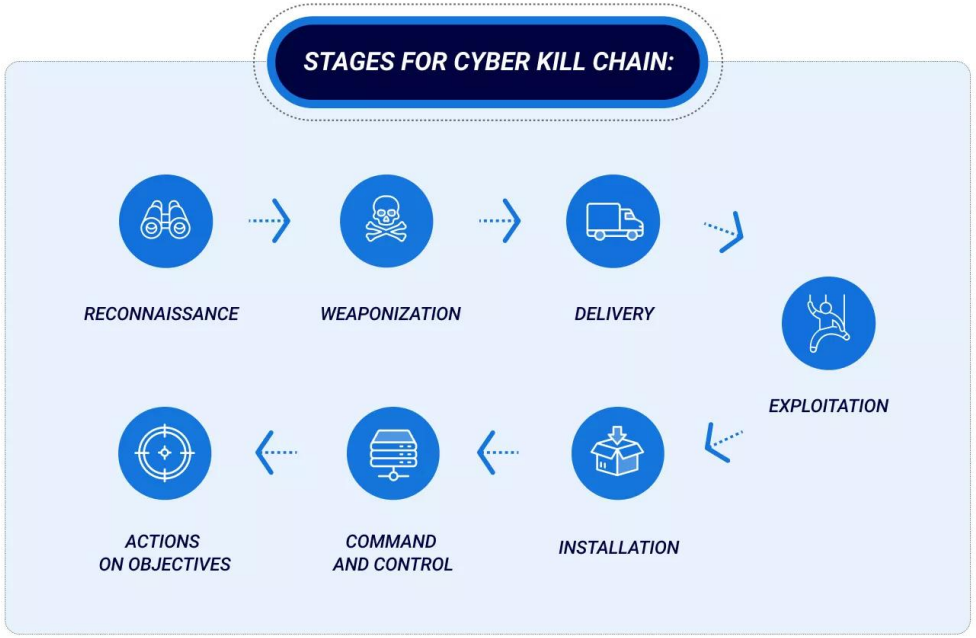
•**Procedures**: Detailed, practical examples of how techniques are executed.

Components of the ATT&CK Matrix

Tactics

High-level goals that attackers aim to achieve.

There are 11 tactics in the ATT&CK framework



- **Initial Access**
  Techniques to gain access to a target system or network.
- **Execution**
  Techniques to run malicious code on a target system.
- **Persistence**
  Techniques to maintain a foothold on a system.
- **Privilege Escalation**
  Techniques to gain higher access levels.
- **Defense Evasion**
  Techniques to avoid detection by security tools.
- **Credential Access**
  Techniques to steal credentials.
- **Discovery**
  Techniques to gather information about a system or network.
- **Lateral Movement**
  Techniques to move through a network.
- **Collection**
  Techniques to gather data from a system.
- **Exfiltration**
  Techniques to steal data from a system.
- **Command and Control**
  Techniques to communicate with compromised systems.

SWINBURNE UNIVERSITY OF TECHNOLOGY

Techniques

Specific methods used to achieve the tactics.
Each tactic includes multiple techniques.
•Examples:
•**Initial Access**
Phishing, Exploit Public-Facing Application.
•**Execution:** PowerShell, Scripting.
•**Persistence:** Registry Run Keys, Scheduled Task.

Procedures

Detailed descriptions and examples of techniques.
•Real-world implementations by adversaries.
•Example: Using PowerShell to inject into lsass.exe to dump credentials.

Difference Between ATT&CK Matrix and Framework

ATT&CK Framework	ATT&CK Matrix
• Contains detailed information on tactics, techniques, and procedures (TTPs) used by attackers.. • Categorizes TTPs based on the stage of a cyber attack (e.g., Initial Access, Execution, Persistence). • Helps organizations understand the steps attackers take during a cyber attack. • Serves as a common language for describing attacker behavior. • Enables organizations to assess their defenses against known attack methods.	• Condenses the information in the ATT&CK framework into a matrix format. • Lists tactics along the top and techniques along the side. • Each cell represents a specific technique within a specific tactic. • Provides a clear and concise view of attacker TTPs. • Helps security professionals quickly identify and map out attacker methods.

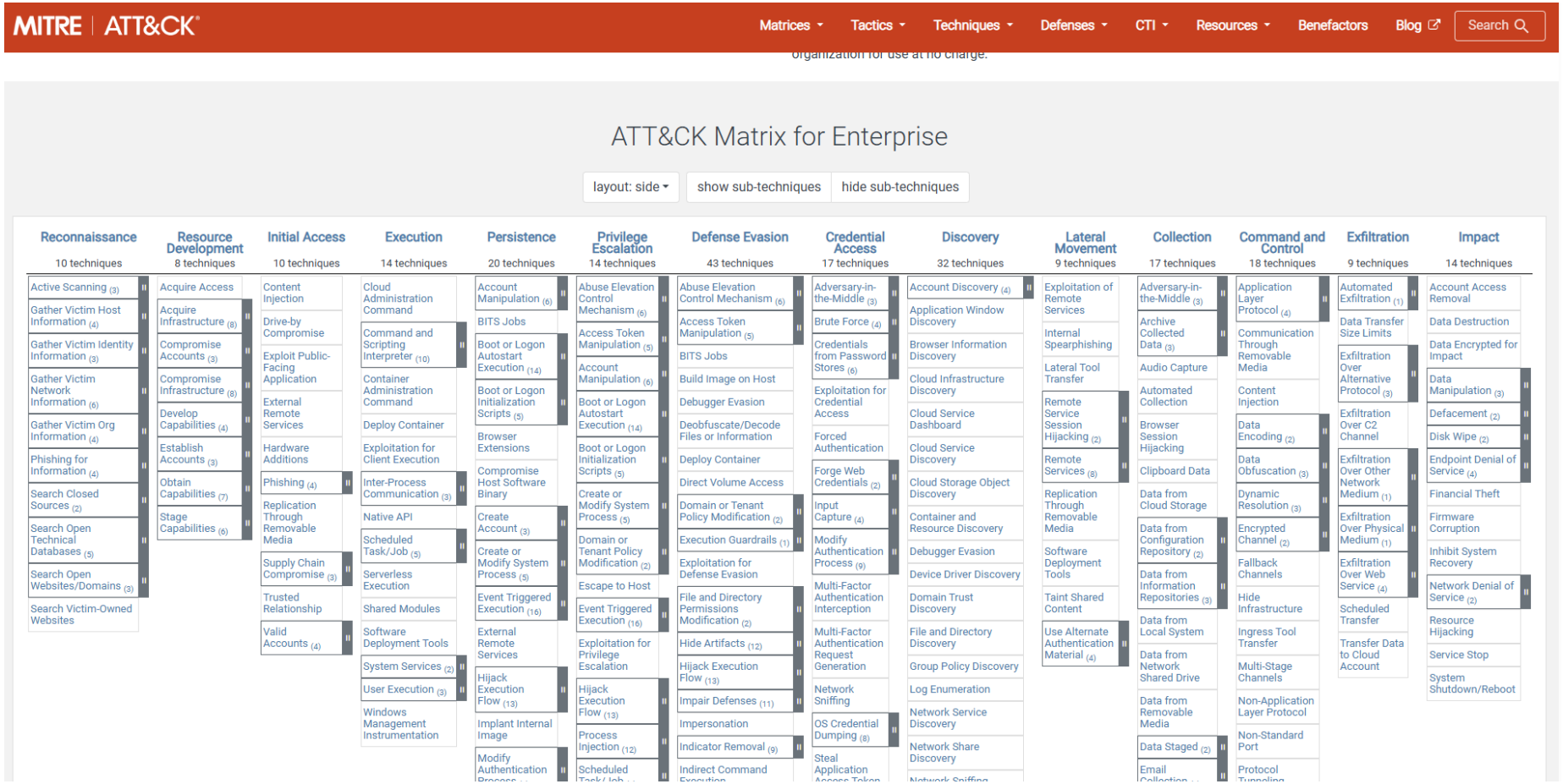
SWINBURNE UNIVERSITY OF TECHNOLOGY

Key Differences:

- **Framework =** Comprehensive and detailed while **Matrix =** Condensed and visual.
- **Framework =** Understanding and describing attacker behavior while **Matrix =** Quick reference and mapping of attacker techniques.

Using ATT&CK Navigator

- **ATT&CK Navigator:** A tool for visualizing and manipulating the ATT&CK framework data. Helps in creating, exploring, and sharing customized views of the ATT&CK knowledge base.



SWINBURNE UNIVERSITY OF TECHNOLOGY

Steps to Use ATT&CK Navigator

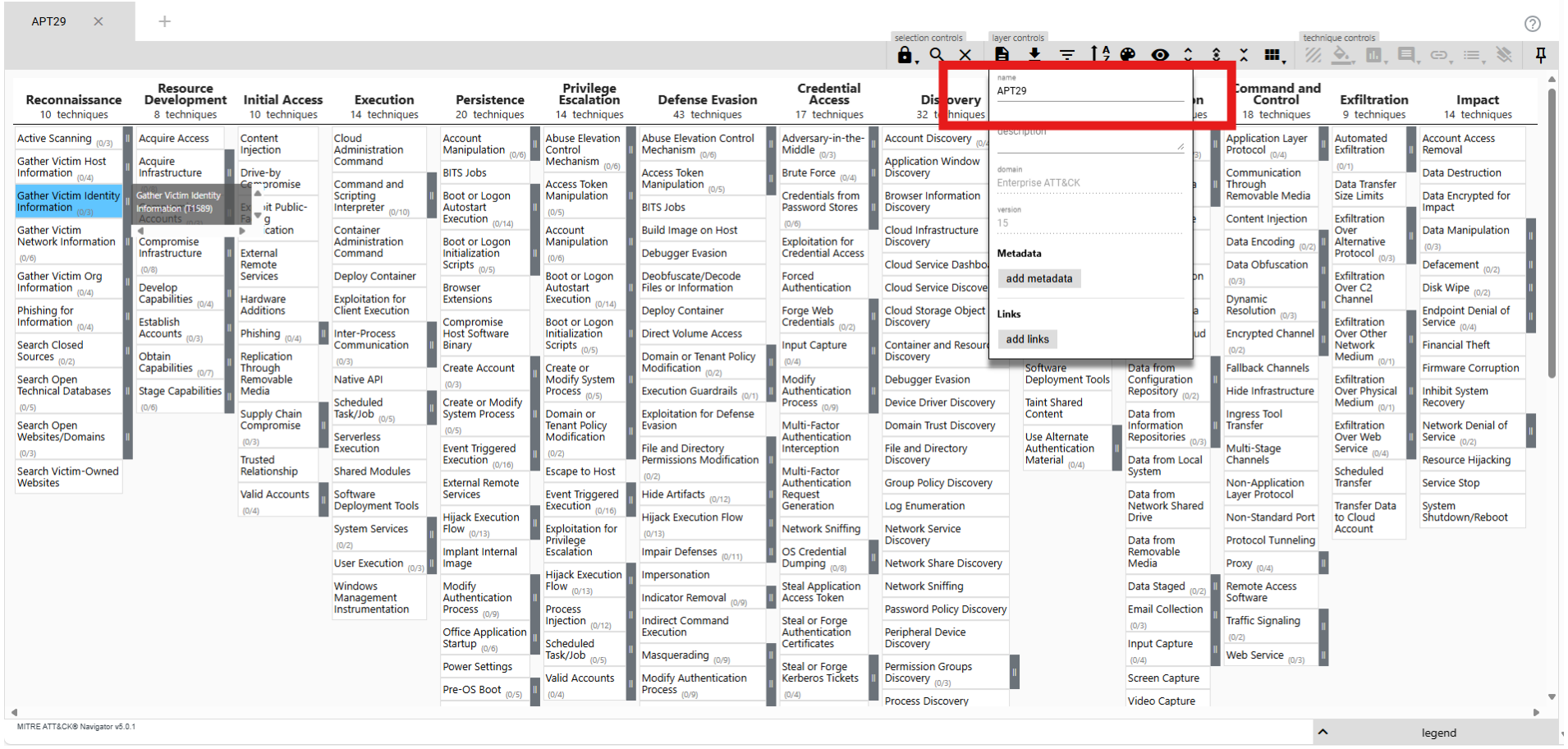
Find Threat Actor Page

- Visit the cyber actor page for a specific threat actor (e.g., APT29).
- Obtain the table of MITRE ATT&CK Tactics and Techniques involved in the case.

Tactic	ID	Technique	Procedure
Credential Access	T1110	Brute forcing	The SVR use password spraying and brute forcing as an initial infection vector.
Initial Access	T1078.004	Valid Accounts: Cloud Accounts	The SVR use compromised credentials to gain access to accounts for cloud services, including system and dormant accounts.
Credential Access	T1528	Steal Application Access Token	The SVR use stolen access tokens to login to accounts without the need for passwords.
Credential Access	T1621	Multi-Factor Authentication Request Generation	The SVR repeatedly push MFA requests to a victim's device until the victim accepts the notification, providing SVR access to the account.
Command and Control	T1090.002	Proxy: External Proxy	The SVR use open proxies in residential IP ranges to blend in with expected IP address pools in access logs.
Persistence	T1098.005	Account Manipulation: Device Registration	The SVR attempt to register their own device on the cloud tenant after acquiring access to accounts.

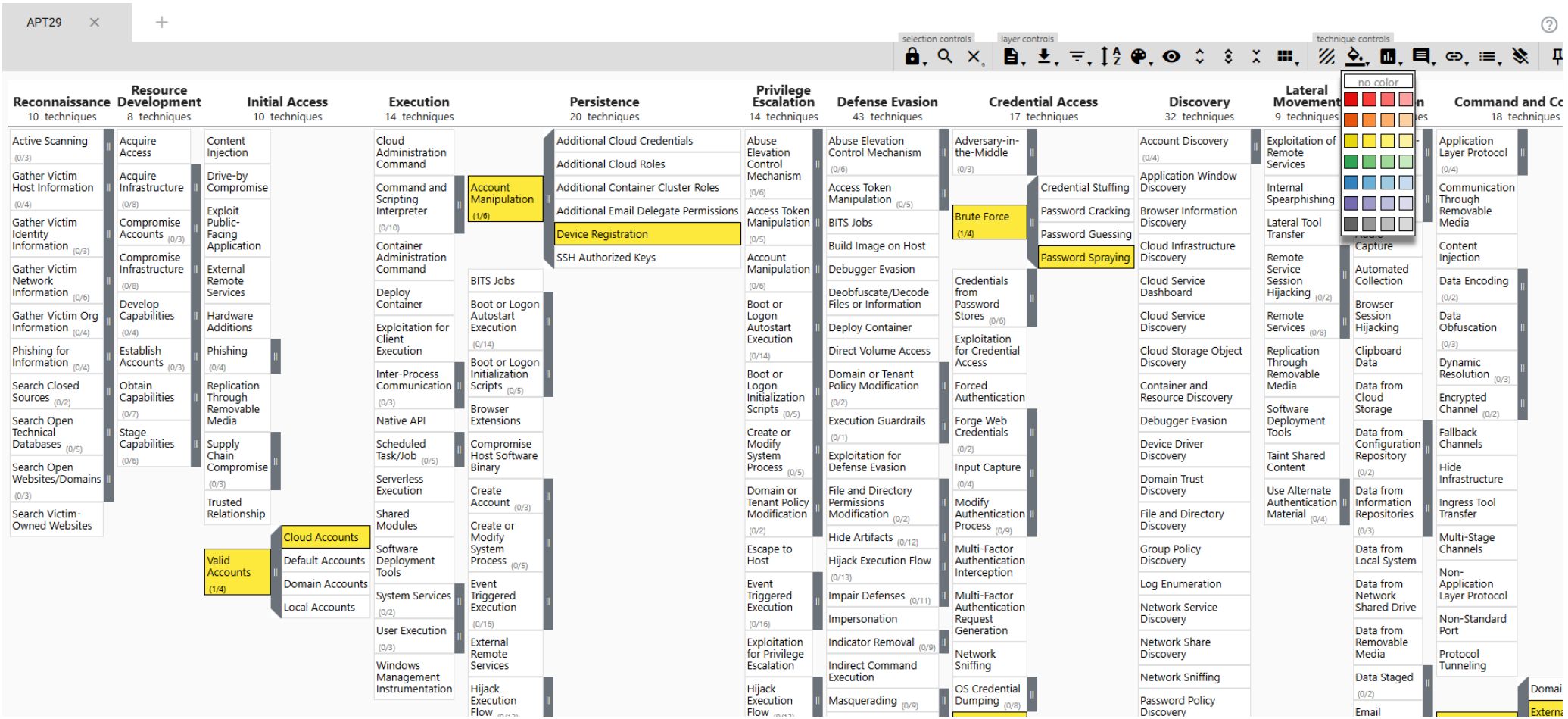
Create a Layer

- Go to the ATT&CK Navigator website.
- By default, Navigator starts with a new layer called “layer.”
- Rename the layer to the threat actor's name (e.g., "APT29").



Assign Scores to Techniques

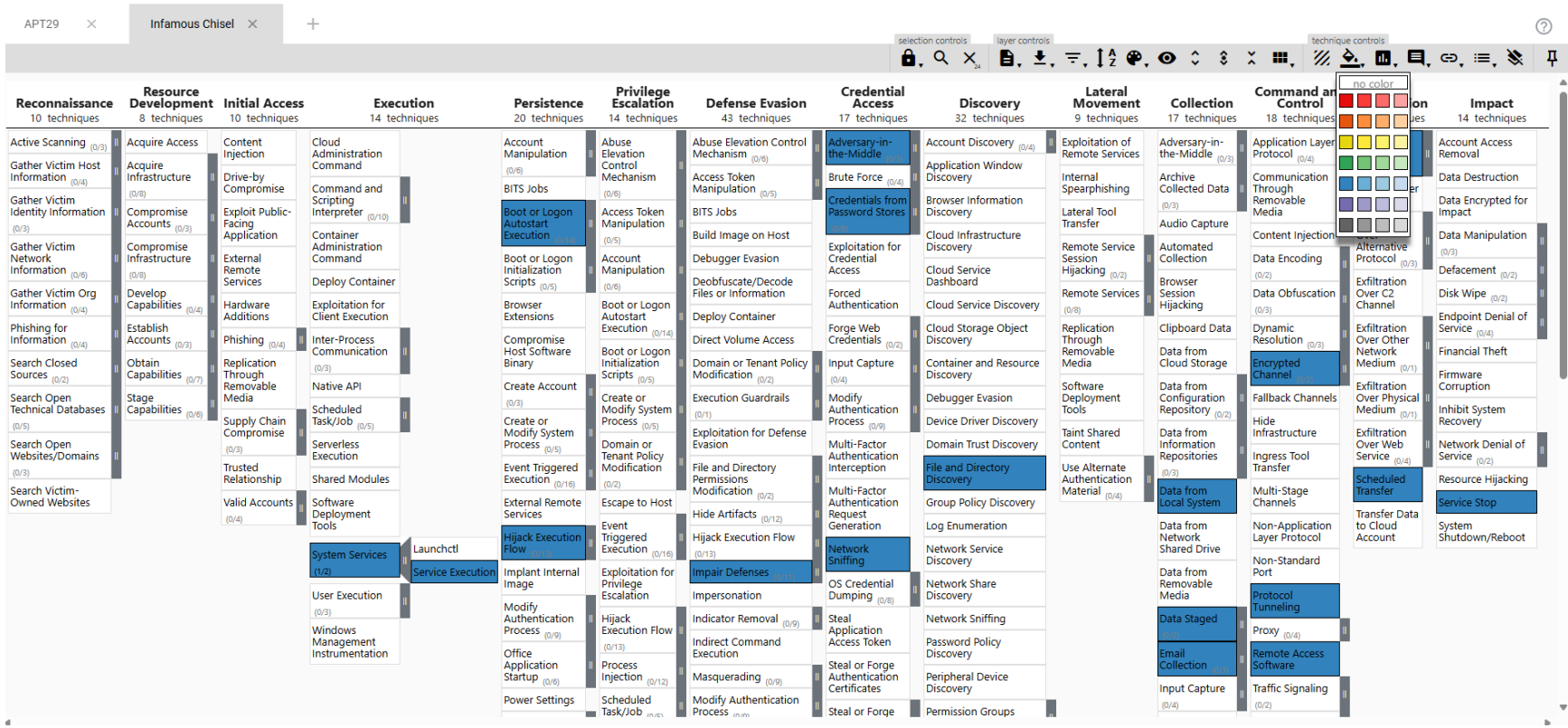
- Manually select techniques used by the threat actor.
- Assign a score (e.g., 1) to each selected technique.
- Optionally, color-code the techniques for better visualization.



Create Layers for Other Threat Actors

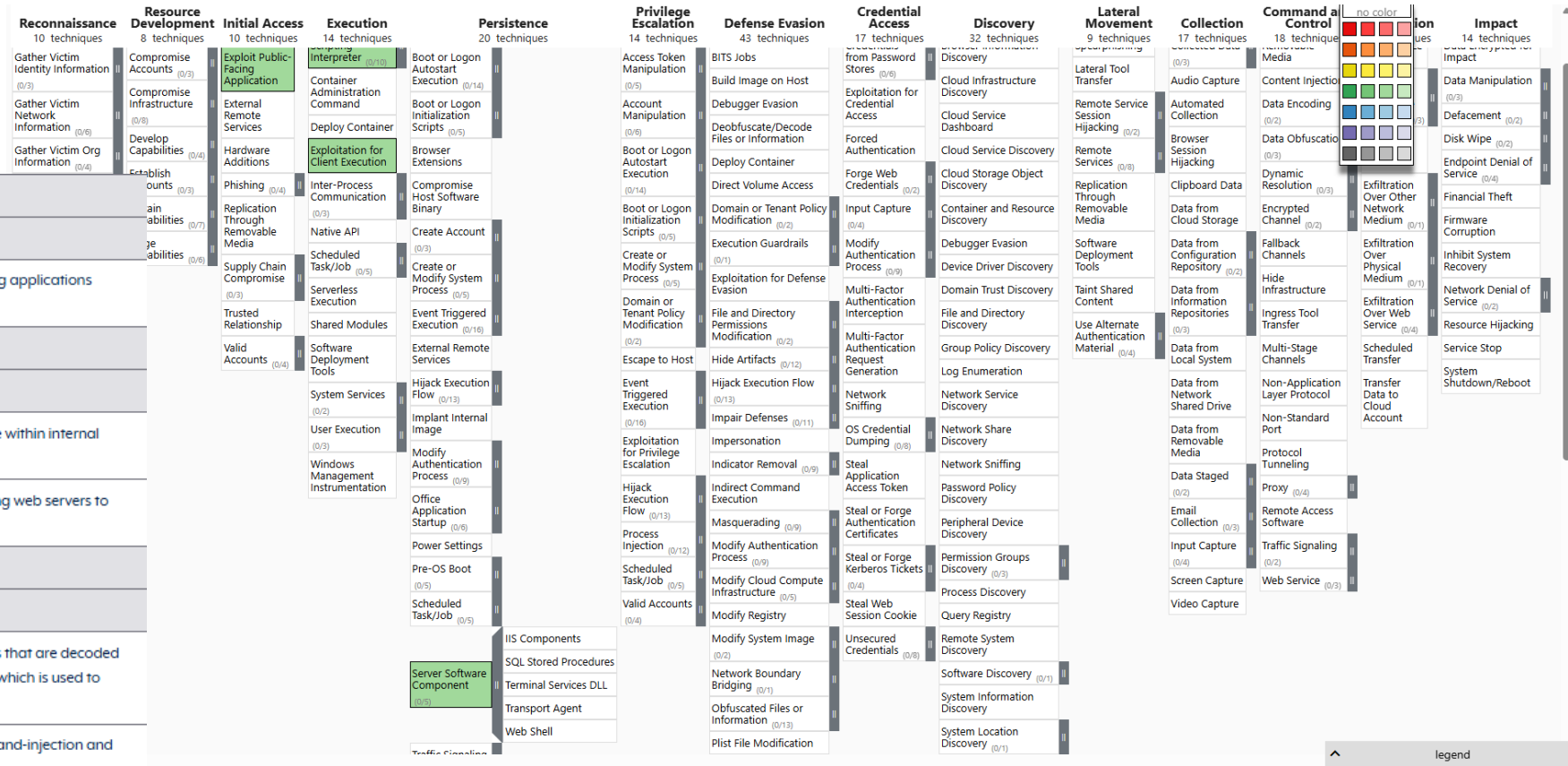
- Repeat the steps to create layers for additional threat actors (e.g., Ivanti, Infamous Chisel).
- Assign different scores to techniques used by each actor.

Discovery	T1420 (Mobile)	File and Directory Discovery	Infamous Chisel - `netd` enumerates multiple data directories to discover files of interest.
	T1430 (Mobile)	Location Tracking	Infamous Chisel - `netd` collects GPS information.
	T1418 (Mobile)	Software Discovery	Infamous Chisel - `netd` collects a list of installed packages.
	T1426 (Mobile)	System Information Discovery	Infamous Chisel - `netd` collects various system information such as the Android ID and other hardware information.
	T1422 (Mobile)	System Network Configuration Discovery	Infamous Chisel - `netd` collects IP interface configuration information.
	T1421 (Mobile)	System Network Connections Discovery	Infamous Chisel - `netd` performs IP scanning of the local network to discover other devices.
Collection	T1533 (Mobile)	Data from Local System	Infamous Chisel - `netd` automatically collects files from the local system based on a predefined list of file extensions.
	T1074.001	Data Staged: Local Data Staging	Infamous Chisel - `netd` creates multiple temporary files in the system to hold collected information.
	T1114.001	Email Collection: Local Email Collection	Infamous Chisel - `netd` exfiltrates files from application and data directories containing communication data.
Command and Control	T1437 (Mobile)	Application Layer Protocol	Infamous Chisel - `db` provides SCP functionality.
	T1521 (Mobile)	Encrypted Channel	Infamous Chisel - `td` is deployed alongside this malware providing a Tor hidden service relaying connections to SSH program.
	T1572	Protocol Tunnelling	Infamous Chisel - `td` is deployed alongside this malware providing a local Socks connection for db.
	T1219	Remote Access Software	Infamous Chisel - `db` provides a SSH server and client.
Exfiltration	T1020	Automated Exfiltration	Infamous Chisel - `netd` automatically exfiltrates files at regular intervals.
	T1029	Scheduled Transfer	Infamous Chisel - `netd` automatically exfiltrates files at regular intervals.
Impact	T1489	Service Stop	Infamous Chisel - `netd` replaces the legitimate `netd`.



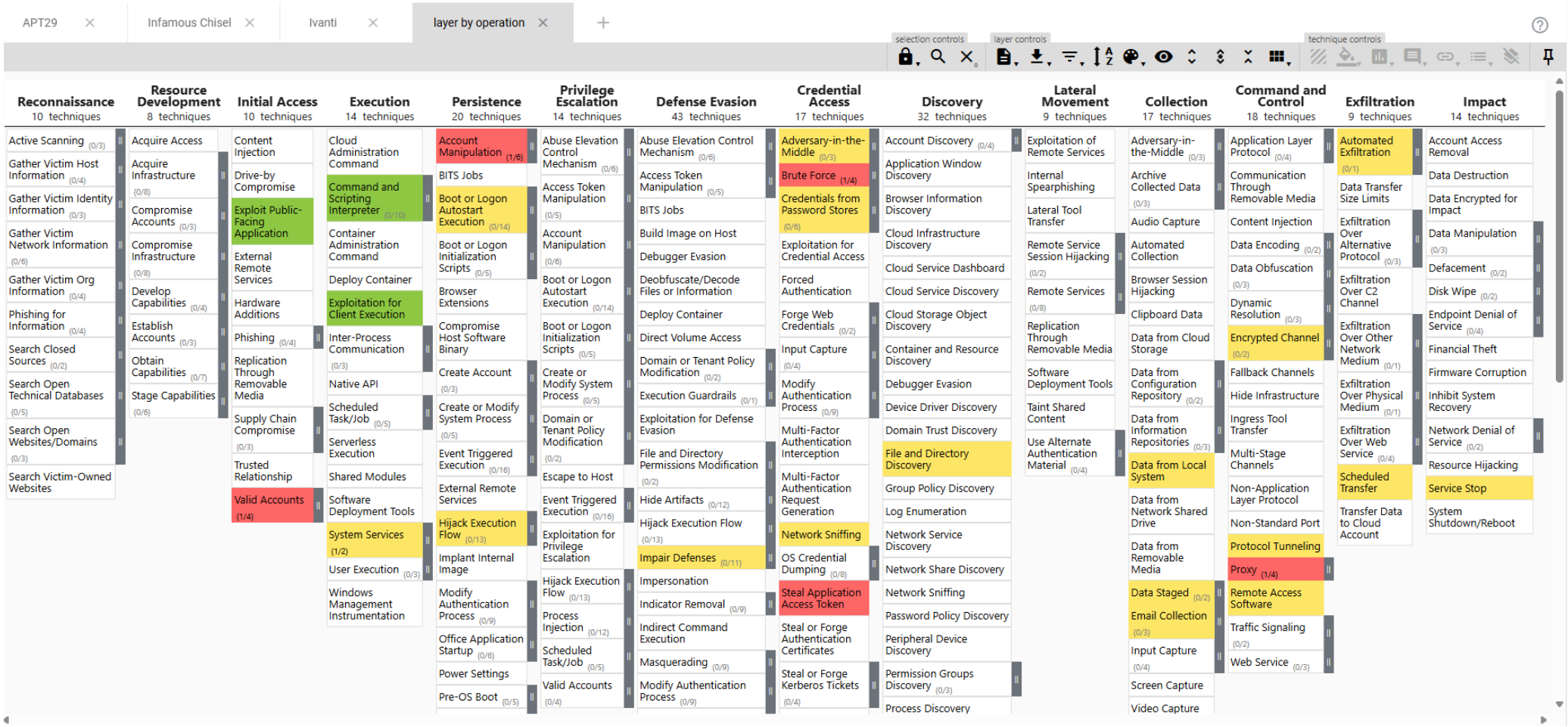
Ivanti

Initial Access		
Technique Title	**ID**	**Use**
Exploit Public-Facing Applications	T1190	Cyber actors will use custom web shells planted on public facing applications which allows persistence in victims' environment.
Persistence		
Technique Title	**ID**	**Use**
Valid Accounts	T1078	Cyber actors leverage compromised accounts to laterally move within internal systems via RDP, SBD, and SSH.
Server Software Component: Web Shell	T1505.003	Cyber actors may use web shells on internal- and external-facing web servers to establish persistent access to systems.
Execution		
Technique Title	**ID**	**Use**
Command and Scripting Interpreter: PowerShell	T1059.001	Cyber actors leverage code execution from request parameters that are decoded from hex to base64 decoded, then passed to Assembly.Load() which is used to execute arbitrary PowerShell commands.
Exploitation for Client Execution	T1203	Cyber actors will exploit software vulnerabilities such as command-injection and achieve unauthenticated remote code execution (RCE).



Combine Layers

- Use the “Create Layer from other layers” feature.
- Combine layers using expressions like “a + b + c.”
- Adjust color settings for combined layers to represent different scores.



Export the Layer

- Export the combined layer in the desired format (e.g., Excel, JSON, SVG).
- Choose the export format based on your needs (e.g., analysis, presentation).

Reconnaissance	Resource Development	Initial Access		Execution	Persistence		Privilege Escalation	Defense Evasion
Active Scanning	Acquire Access	Content Injection		Cloud Administration Command	Account Manipulation	Additional Cloud Credentials	Abuse Elevation Control Mechani	Abuse Elevation Control Mecha
Gather Victim Host Information	Acquire Infrastructure	Drive-by Compromise		Command and Scripting Interpret		Additional Cloud Roles	Access Token Manipulation	Access Token Manipulation
Gather Victim Identity Informatio	Compromise Accounts	Exploit Public-Facing Application		Container Administration Comma		Additional Container Cluster Role	Account Manipulation	BITS Jobs
Gather Victim Network Informatic	Compromise Infrastructure	External Remote Services		Deploy Container		Additional Email Delegate Permis	Boot or Logon Autostart Executior	Build Image on Host
Gather Victim Org Information	Develop Capabilities	Hardware Additions		Exploitation for Client Execution		Device Registration	Boot or Logon Initialization Script	Debugger Evasion
Phishing for Information	Establish Accounts	Phishing		Inter-Process Communication		SSH Authorized Keys	Create or Modify System Process	Deobfuscate/Decode Files or Ir
Search Closed Sources	Obtain Capabilities	Replication Through Removable Media		Native API	BITS Jobs		Domain or Tenant Policy Modifica	Deploy Container
Search Open Technical Databases	Stage Capabilities	Supply Chain Compromise		Scheduled Task/Job	Boot or Logon Autostart Execution		Escape to Host	Direct Volume Access
Search Open Websites/Domains		Trusted Relationship		Serverless Execution	Boot or Logon Initialization Scripts		Event Triggered Execution	Domain or Tenant Policy Modif
Search Victim-Owned Websites		Valid Accounts	Cloud Accounts	Shared Modules	Browser Extensions		Exploitation for Privilege Escalatic	Execution Guardrails
			Default Accounts	Software Deployment Tools	Compromise Host Software Binary		Hijack Execution Flow	Exploitation for Defense Evasic
			Domain Accounts	System Services	Create Account		Process Injection	File and Directory Permissions
			Local Accounts	User Execution	Create or Modify System Process		Scheduled Task/Job	Hide Artifacts
				Windows Management Instrumer	Event Triggered Execution		Valid Accounts	Hijack Execution Flow
					External Remote Services			Impair Defenses
					Hijack Execution Flow			Impersonation
					Implant Internal Image			Indicator Removal
					Modify Authentication Process			Indirect Command Execution
					Office Application Startup			Masquerading
					Power Settings			Modify Authentication Process
					Pre-OS Boot			Modify Cloud Compute Infrastr
					Scheduled Task/Job			Modify Registry
					Server Software Component			Modify System Image
					Traffic Signaling			Network Boundary Bridging
					Valid Accounts			Obfuscated Files or Informatio
								Plist File Modification
								Pre-OS Boot
								Process Injection
								Reflective Code Loading
								Rogue Domain Controller
								Rootkit
								Subvert Trust Controls
								System Binary Proxy Execution
								System Script Proxy Execution
								Template Injection
								Traffic Signaling
								Trusted Developer Utilities Pro
								Unused/Unsupported Cloud Re
								Use Alternate Authentication M

Enterprise ATT&CK v15 (APT29-0) | Enterprise ATT&CK v15 (Infamous | Enterprise ATT&CK v15 (Ivanti-2 | Enterprise ATT&CK v15 (layer by

SWINBURNE UNIVERSITY OF TECHNOLOGY

Thank You

Thank you

COS80013 Internet Security

Lecture Week 1A

A Reference

**Rossouw von Solms, Johan van Niekerk,
From information security to cyber security,
Computers & Security,
Volume 38,
2013,
Pages 97-102,
(https://www.sciencedirect.com/science/article/pii/S0167404813000801)**

&

**https://www.cyber.gov.au/acsc/view-all-content/glossary
https://www.itgovernance.co.uk/what-is-cybersecurity**

COMPUTERS & SECURITY 38 (2013) 97–102

Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

ELSEVIER

From information security to cyber security

Rossouw von Solms, Johan van Niekerk*

School of ICT, Nelson Mandela Metropolitan University, Port Elizabeth 6031, South Africa

ARTICLE INFO

Article history:
Received 26 November 2012
Received in revised form
10 April 2013
Accepted 11 April 2013

Keywords:
Information security
Cyber security
Cybersecurity
Cyber-Security
Computer security
Risk
Threat
Vulnerability

ABSTRACT

The term *cyber security* is often used interchangeably with the term *information security*. This paper argues that, although there is a substantial overlap between cyber security and information security, these two concepts are not totally analogous. Moreover, the paper posits that cyber security goes beyond the boundaries of traditional information security to include not only the protection of information resources, but also that of other assets, including the person him/herself. In information security, reference to the human factor usually relates to the role(s) of humans in the security process. In cyber security this factor has an additional dimension, namely, the humans as potential targets of cyber attacks or even unknowingly participating in a cyber attack. This additional dimension has ethical implications for society as a whole, since the protection of certain vulnerable groups, for example children, could be seen as a societal responsibility.

SWINBURNE UNIVERSITY OF TECHNOLOGY

Definitions

Information Security

Practices to keep data secure, defined in properties data should have

CIA per data

ICT Security

Monitor and control access to information

Safeguard transmission

Secure storage and data disposal

Cyber security?

The same computer?

A blend

Magic?

https://csrc.nist.gov/glossary/term/information_security
https://statisticaldataintegration.abs.gov.au/topics/secure-data-management/information-and-communication-technology-security

Confidentiality, Integrity, Availability (CIA)

CIA comes from the information systems industry

Confidentiality

Only those entitled to access the information can see it

Authorise, encrypt, access control, authenticate, restrict physical access

Integrity

Information cannot be altered and changes are immediately detectable.

Backup, checksum, hash, correction code

CIA...

Availability

Information is available (to read, write) to those who need it without interruption or onerous access restrictions.

Redundant systems, data recovery, disaster planning, UPS, backup power systems, redundant network connections.

e.g. “Fail open” authentication systems have been DDOSed (loss at availability) to allow attackers to bypass access restrictions (break confidentiality)

Repudiation

Authenticity

Enforcing commitments, contracts, agreements.

The internet has no fundamental way of managing this.

Not designed for commerce, access control (paywalls) or even uploads.

Information Security Measures

Policy

What data needs to be protected and in what way

Password

Roles and responsibilities

Access controls

Measures

Technical (hardware or software – e.g. encryption/firewall)

Organisation (staff, team responsibilities)

Human (training)

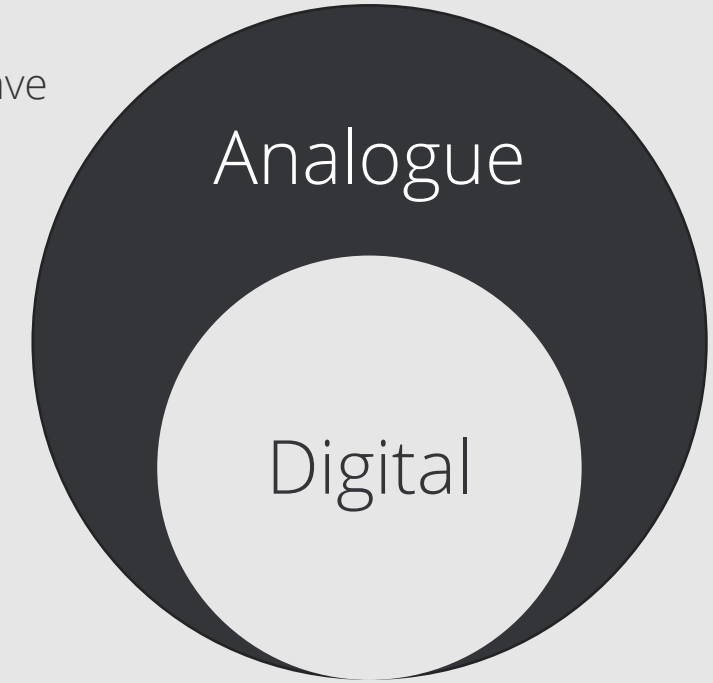
Physical (Access control)

Information Security

Information Security

Practices to keep data secure, defined in properties data should have CIA

"The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability."



Information and Communications Technology

From our government definition and a little extra

Information and communications technology (ICT)

An extensible term for information technology that stresses the role of unified communications and the integration of telecommunications and computers, as well as related enterprise software, middleware, storage and audio-visual systems, that enable users to access, store, transmit and manipulate information.

Information and communications technology (ICT) equipment

Any device that can process, store or communicate electronic information—for example, computers, multifunction devices and copiers, landline and mobile phones, digital cameras, electronic storage media and other radio devices.

Information and communication technology security

Information and communication technology (ICT) security measures are necessary to protect confidential information from unauthorised use, modification, loss or release.

The three key elements of an effective ICT security system include:

- Monitoring and controlling access to confidential information
- Safe transmission of data
- Secure storage and disposal of data

https://www.cyber.gov.au/acsc/view-all-content/glossary
https://statisticaldataintegration.abs.gov.au/topics/secure-data-management/information-and-communication-technology-security

SWINBURNE UNIVERSITY OF TECHNOLOGY

What's Vulnerable

Through the use of ICT

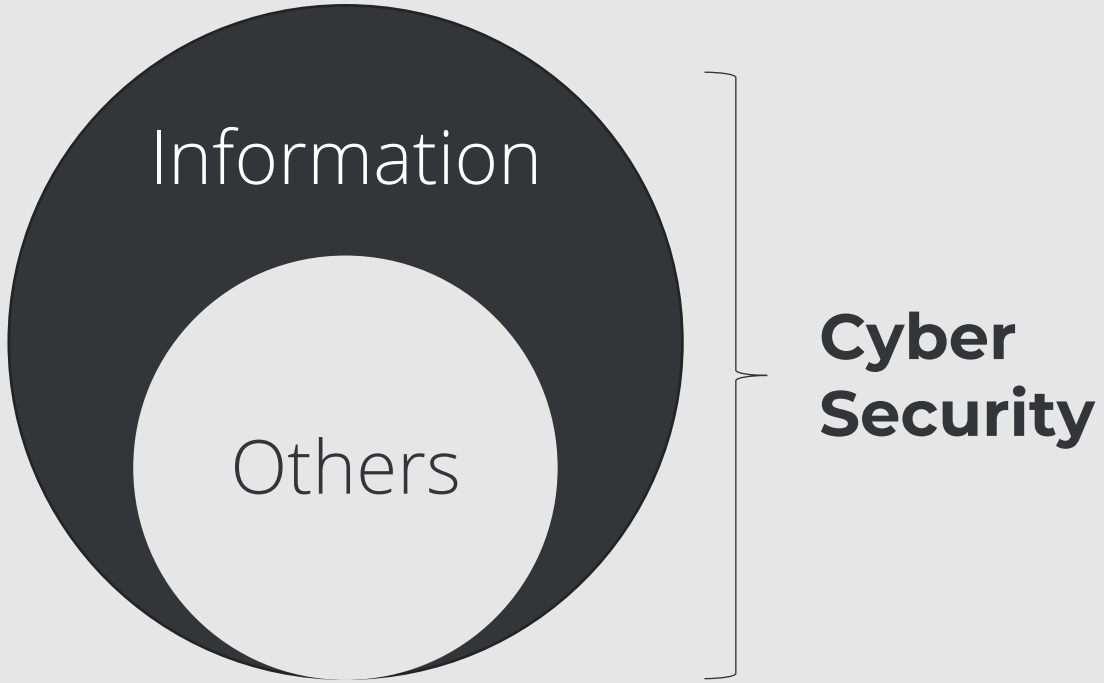
Information assets

Non-Information based assets

Remember ICT is processes, storage or communication of electronic information which can be edited, manipulated, displayed

What could others mean here?

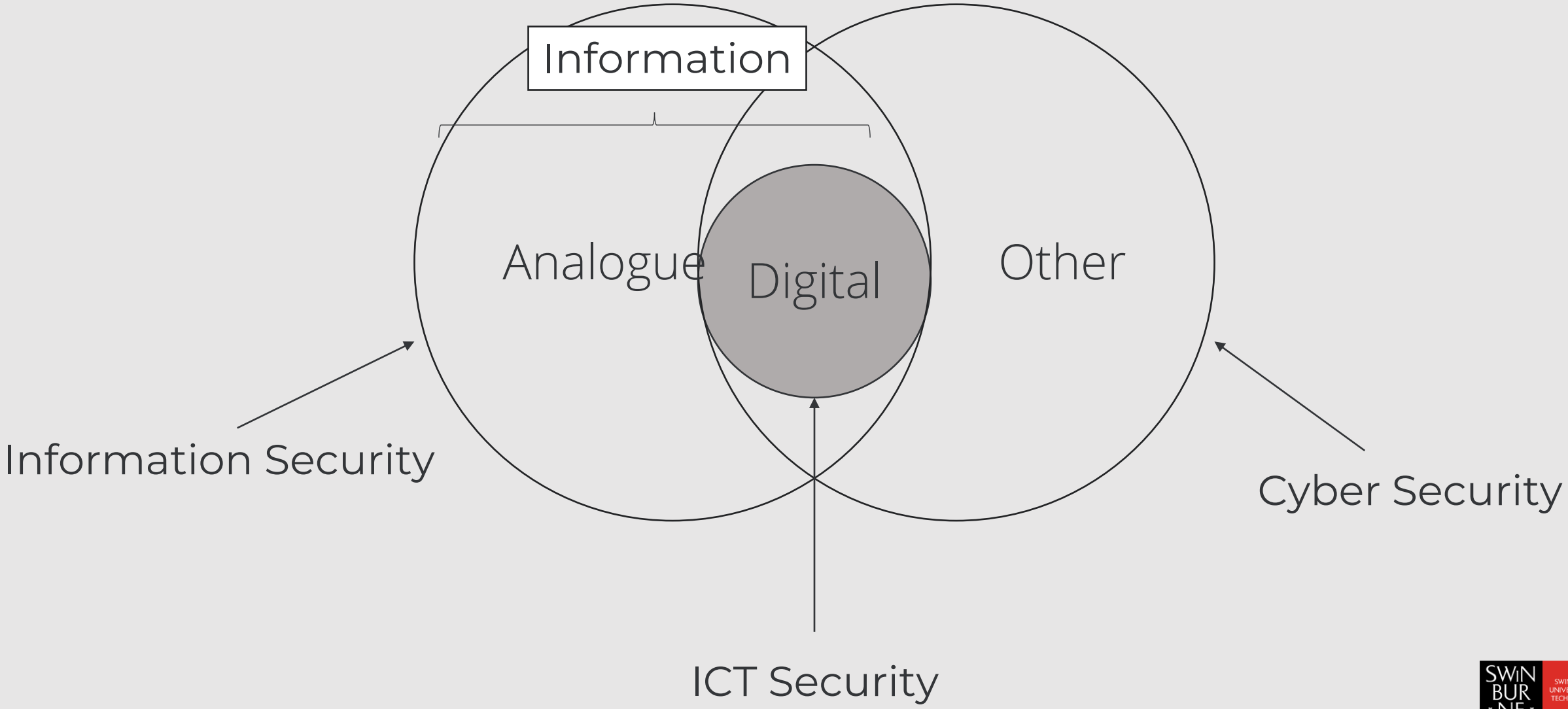
- Inspecting webpages for a phishing attempt
- Malware detection
- Inspecting traffic for known indicators
- …



https://www.cyber.gov.au/acsc/view-all-content/glossary
https://www.itgovernance.co.uk/what-is-cybersecurity

SWINBURNE UNIVERSITY OF TECHNOLOGY

All Together



* Security

Information Security

Information assets (stored or transmitted) ≠ using ICT

Computer Security / ICT Security

Monitor and control access to information

Safeguard transmission

Secure storage and data disposal

Cyber security?

Non-Information based assets = using ICT [vulnerable]

Information based assets

Definitions

Cyber security?

Information Security, ICT Security?

A blend?

Magic?

Aus Gov Glossary

Measures used to protect the confidentiality, integrity and availability of systems, devices and the information residing on them.

Industry

Cyber security is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks.

It aims to reduce the risk of cyber attacks and protect against the unauthorised exploitation of systems, networks and technologies.

https://www.cyber.gov.au/acsc/view-all-content/glossary
https://www.itgovernance.co.uk/what-is-cybersecurity

Security paradigms

- **Probabilistic Risk Analysis**
  - Assess the probability and severity of known* attacks against targets.
  - Risk factor = pr(Risk) * pr(Severity) for each target.
  - Allocate protection budget to highest risk factor target.
- **Doesn't work because:**
  - Criminals change the risk probabilities by studying the protection schemes and attack (many of) the least protected/probable targets.

Impact →	1	2	3	4	5
Probability ↓	Negligible	Minor	Moderate	Significant	Severe
(81-100)%	Low Risk	Moderate Risk	High Risk	Extreme Risk	Extreme Risk
(61-80)%	Minimum Risk	Low Risk	Moderate Risk	High Risk	Extreme Risk
(41-60)%	Minimum Risk	Low Risk	Moderate Risk	High Risk	High Risk
(21-40)%	Minimum Risk	Low Risk	Low Risk	Moderate Risk	High Risk
(1-20)%	Minimum Risk	Minimum Risk	Low Risk	Moderate Risk	High Risk

SWINBURNE UNIVERSITY OF TECHNOLOGY

Security paradigms

- **Perimeter security**
  - Encase the LAN with firewall / IDS / IPS to prevent any nasty stuff from getting in.
  - Referred to as "M&M security"
  - Hard outer shell, soft middle.

- **Doesn't work because:**
  - If malware gets past perimeter, all computers become compromised. e.g. US drones
  - phishing attacks, social engineering, insiders, XSS, VPNs
  - managers who are “too important” to follow procedure/policy.

Security paradigms

- **Security policy**
  - Accidental damage or vulnerabilities may be introduced by insiders, management, visitors.
  - To reduce the chances of your network users compromising the network, tell them what they are allowed to do!
  - Make sure that they understand what they are not allowed to do.

  - https://www.swinburne.edu.au/about/leadership-governance/policies-regulations/procedures-guidelines/acceptable-use-guidelines/

Security paradigms

- **Access control / User Rights Management (ACLs)**
  - Both Windows and Linux support this complicated method of enforcing security.
  - Individual files / directories are tagged to allow/disallow file execution, reading, writing for different user groups.
  - Users are groups according to their roles / normal activities and privileges.

User	accounts	web page	policy docs
user 1	rwa-	r--x	rw--
user 2	----	rw-x	r---
user 3	r---	r--x	rwa-

Security paradigms

- **Reactive security / Black listing**

default allow

- ➢Used for default installations of Windows (including Vista) and Linux assume there is only one user who is the system administrator.
- ➢All activities (and types of network traffic) are allowed.
- ➢Rules are added / ports are closed when a problem / incursion occurs.
- ➢Black-listing of known threats

- **Doesn't work because:**

- ➢ 0-day attacks are not known; not on black list.

Security paradigms

- **Proactive security / White listing**

  default deny

  - All unknown activities / ports / software are blocked until an administrator allows them.
  - Allowed activities / ports / software are white-listed

- **Hard to implement:**

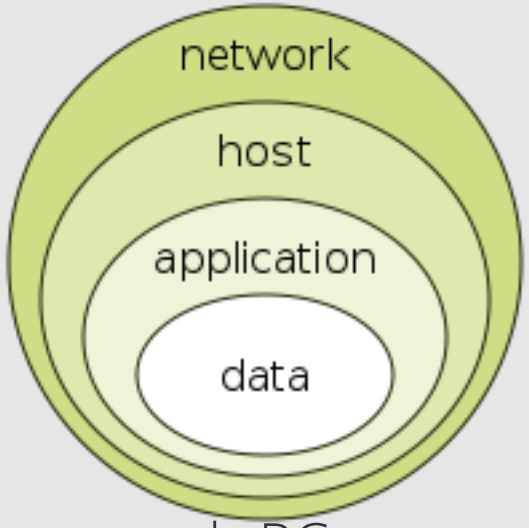
  - push-back from users, managers, CEO.
  - Requires open-minded, responsive and agile ISOs

Security paradigms

- **In Practice…**
  - Some blacklisted things
  - Some whitelisted things
  - Unknown threats slip through undetected.
  - Different policies for different resources (segmentation)
  - High-value targets are default deny, ACL;
  - Low value targets are default allow, daily re-image of SOE to minimise threat from 0-day attacks.
    - Persistent malware can defeat this
  - Need Defence in Depth because no single control is effective.

Security paradigms

- **Defence in Depth – can be based on ISO/OSI layers**
  - Sanitise input data, filter output data
  - ACLs, restricted rights to prevent unauthorised insiders / intruders.
  - AV / AntiMalware on all boxes
  - IPS, DMZ, network firewall, subnet firewalls, software firewalls on each PC.
  - Physical security + screening of employees



COS80013 Internet Security

Lecture Week 1B

Cyber Threats

Actors & Drivers Traditional

Nation/States	Profit
Cyber Criminals/Gangs	Disgruntled
Terrorist Groups	Satisfaction
Hacktivists	Geopolitical/Espionage
Insider Threats	Ideological
Script Kiddies	

SWINBURNE UNIVERSITY OF TECHNOLOGY

Actors & Drivers Expanded

Nation/States

Cyber Criminals/Gangs

Terrorist Groups

Hacktivists

Insider Threats

Script Kiddies

Profit

Disgruntled

Satisfaction

Geopolitical/Espionage

Ideological

Skills

Nation/States	High
Cyber Criminals/Gangs	Med-High
Terrorist Groups	Medium
Hacktivists	Med-Low
Insider Threats	Low
Script Kiddies	

SWINBURNE UNIVERSITY OF TECHNOLOGY

Tools

Nation/States

Cyber Criminals/Gangs

Terrorist Groups

Hacktivists

Insider Threats

Script Kiddies

Custom/Complex

SaaS

Developed Further

Online

Off The Shelf

Easy

Moderate

Complex

SWINBURNE UNIVERSITY OF TECHNOLOGY

Attack Span

Nation/States

Cyber Criminals/Gangs

Terrorist Groups

Hacktivists

Insider Threats

Script Kiddies

Quick/Short

Sustained/Brief

Long

Refresh your understanding

https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors
https://www.cyber.gov.au/acsc/view-all-content/glossary