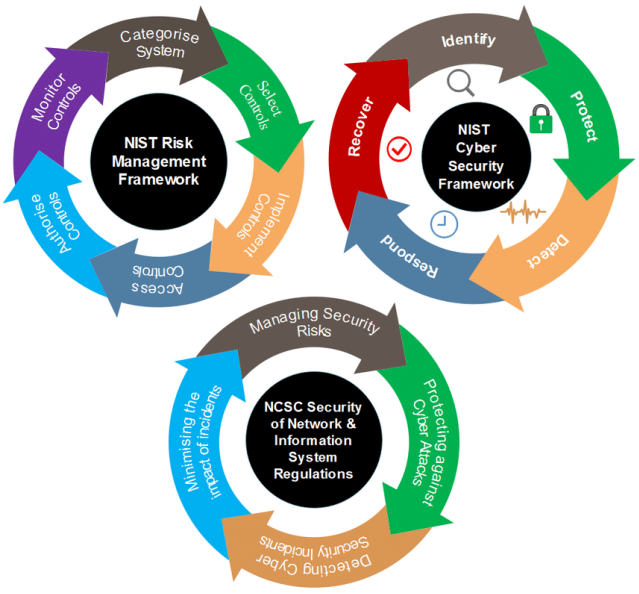
FOUNDATIONS IN IT SECURITY: CORE SECURITY PRINCIPLES

COMPUTER SYSTEMS SECURITY

TODAY ….

Today we will look at Core Security Principles, which includes:

- Keeping Information Safe
- Managing Risk
- Scam Artists
- Attack Surfaces
- Modelling Threats



COMPUTER SYSTEMS SECURITY

CORE SECURITY PRINCIPLES: KEEPING INFORMATION SAFE

GORDON | REYNOLDS (2018)

KEEPING INFORMATION SAFE

- A basic principle of providing a secure system is:
  - Manage Risk
  - Protect sensitive information
  - Keep data private, unchanged and available
  - CIA triad: a widely recognised information assurance model

GORDON | REYNOLDS (2019)

PRIVATE INFORMATION

- Private Information Includes:
  - Personally identifiable information
    - PPSN, credit card or bank account numbers
  - Business information
    - Data, employee records and trade secrets

GORDON | REYNOLDS (2019)

PRIVATE INFORMATION

- The Challenge
  - Nearly everyone, including companies, social media, hospitals and many others collect, store and share our information

GORDON | REYNOLDS (2019)

PRIVATE INFORMATION

- Confidentiality
  - The promise of keeping private information private by preventing unauthorised access.
- Violations of Confidentiality
  - Includes, someone other than your doctor's office reading your medical file

GORDON | REYNOLDS (2019)

PRIVATE INFORMATION

- Integrity
  - Protecting data from unauthorised changes
  - Both from intentional and unintentional changes
- Violation of Integrity
  - Data integrity can be compromised when information has been altered or destroyed, either maliciously or accidentally.
  - E.g. A student goes into a gradebook and changes their (or someone else's) subject grade(s).

GORDON | REYNOLDS (2019)

PRIVATE INFORMATION

- Availability
  - Ensuring data and services are available only to authorised users when needed
- Preventing Access to Data
  - One threat against availability is a distributed denial-of-service attack or DDoS.
  - Such an attack interrupts or suspends services to legitimate users.

GORDON | REYNOLDS (2019)

PRIVATE INFORMATION

- DDoS and Botnets
  - At a predefined time, armies of Botnets will launch an attack by sending multiple requests to a system and lockout legitimate users.

GORDON | REYNOLDS (2019)

PRIVATE INFORMATION

- Keep Data Private
  - Provide access to private data only to authorised individuals.
  - Verify a users identity in some way. Methods include:
    - Password or Pin
    - Smart Card
    - Fingerprint
  - Permissions allow access to data only to authorised users and no one else.

GORDON | REYNOLDS (2019)

PRIVATE INFORMATION

- Keep Data Private
  - Encryption
    - Scrambles and conceals the data in a format where the only way you can see the data is if you have a key.

GORDON | REYNOLDS (2019)

PRIVATE INFORMATION

- Prevent Unauthorised Changes
  - Use specialised software that monitors for suspicious activity and notify someone if there are unauthorised changes to the data.
- Prevent a Denial of Service
  - Tune devices to monitor for DDoS attacks
  - Keep Systems current
  - Backup and store in an offsite location
  - Backup your own personal data as well

GORDON | REYNOLDS (2019)

EXERCISE

- In-class video (DDoS)

- Website:
  - www.digitalattackmap.com

GORDON | REYNOLDS (2019)

COMPUTER SYSTEMS SECURITY

CORE SECURITY PRINCIPLES: MANAGING RISK

GORDON | REYNOLDS (2018)

MANAGING RISK

- Risk
  - When a person, place or thing is open or exposed to harm, which can result in injury, death or destruction

GORDON | REYNOLDS (2018)

MANAGING RISK

- Risk Analysis
  - Consider potential threats
    - Such as a cyberattack
  - Evaluate system weakness
    - Such as a missing password

GORDON | REYNOLDS (2019)

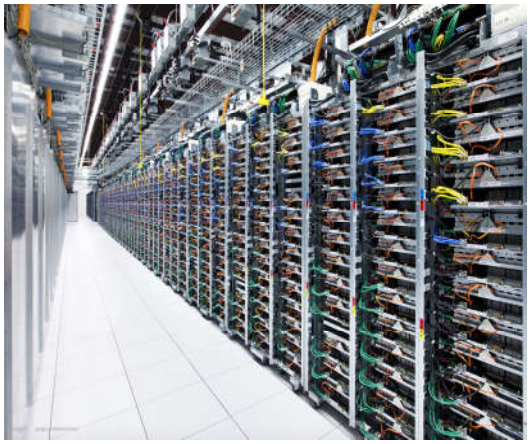
MANAGING RISK

- Manage Risk
  - Implement methods to manage risks and reduce potential for harm
  - Managing risk is an important exercise for a company / business
- Reduce Risk
  - The goal is to protect assets which are both tangible and intangible items that can be assigned a value.

GORDON | REYNOLDS (2019)

MANAGING RISK

- Assets
  - Tangible
    - Printers, Computers, Servers
  - Intangible
    - Databases, Trade Secrets, Company Records



GORDON | REYNOLDS (2019)

MANAGING RISK

Risk is a function of a threat exploiting a weakness or vulnerability

RISK = Threats x Vulnerabilities

GORDON | REYNOLDS (2019)

MANAGING RISK

- Defining risk:
  - Threats may exist but if there is no vulnerability, there will be no risk
  - Also, if there is a vulnerability but no threat, then there is no risk.

  - Risk includes:
    - Business disruption
    - Financial loss
    - Loss of Life

GORDON | REYNOLDS (2019)

MANAGING RISK

- Defining Threat:
  - Anything that can exploit a vulnerability (intentionally or accidentally) and obtain, damage or destroy an asset.
  - Something that might happen and are difficult to control. (employee mistakes to natural disasters).

GORDON | REYNOLDS (2019)

MANAGING RISK

- Threat Assessment
  - Determine the best approach to securing a system

GORDON | REYNOLDS (2019)

MANAGING RISK

- Identifying Vulnerabilities:
  - A security flaw or weakness in a system that can be exploited by threats to gain unauthorised access to an asset.
  - Connecting a system to the internet can represent a vulnerability if the system is unpatched.
  - Other vulnerabilities can include:
    - Unpatched systems
    - Human error
    - Software flaws

GORDON | REYNOLDS (2019)

MANAGING RISK

- Remember,

RISK = Threats x Vulnerabilities

- Therefore, in order to understand the risk to assets, we need to identify the possible threats and vulnerabilities.

GORDON | REYNOLDS (2019)

MANAGING RISK

- The Three Little Pigs

Scenario	Risk		Threat		Vulnerability
Straw House	90%	=	100%	X	90%
Stick House	40%	=	100%	X	40%
Brick House	0%	=	100%	X	0%

GORDON | REYNOLDS (2019)

MANAGING RISK

- The Moral of the Story
  - We can't do anything about the threats
  - In most cases, a vulnerability can be fixed
  - Test and address vulnerabilities on an ongoing basis
  - Remember,

GORDON | REYNOLDS (2019)

COMPUTER SYSTEMS SECURITY

CORE SECURITY PRINCIPLES: AVOIDING SCAM ARTISTS

GORDON | REYNOLDS (2018)

AVOIDING SCAM ARTISTS

- Social Engineering (SE)
  - A process used by Cybercriminals to trick us into doing something
  - To obtain information so they can launch an attack
  - SE is accomplished in many ways:
    - Telephone, online, dumpster diving
    - Shoulder surfing and simple persuasion

GORDON | REYNOLDS (2018)

AVOIDING SCAM ARTISTS

- Social Engineering (SE)
  - Anyone can use Social Engineering
    - Scam Artists
    - Sales people
    - Ordinary individuals
  - The goal is to trick you into completing a task you might not otherwise do in normal circumstances.

GORDON | REYNOLDS (2018)

AVOIDING SCAM ARTISTS

- Social Engineering (SE)
  - SE is one of the hardest attacks to protect against and is now one of the most prevalent
  - A malicious actor doesn't need technical skills
  - Instead, it uses persuasion to gain access into a system

GORDON | REYNOLDS (2018)

AVOIDING SCAM ARTISTS

- Several methods are used in Social Engineering
  - Some are simple
  - Some are sophisticated
  - Many don't appear malicious

GORDON | REYNOLDS (2018)

VIDEO

- Social Engineering Example

GORDON | REYNOLDS (2019)

AVOIDING SCAM ARTISTS

- Many other methods exist
  - Phishing using email
  - Vishing using the telephone
  - IM (instant messaging)

GORDON | REYNOLDS (2018)

AVOIDING SCAM ARTISTS

- Scareware
  - A message is presented to the user
  - Tricks them into clicking a malicious link
  - Exercise: https://haveibeenpwned.com/

GORDON | REYNOLDS (2018)

AVOIDING SCAM ARTISTS

- Best Practices
  - Be aware of people that want too much information
  - Don't trust individuals you meet on the web
    - Avoid answering typical security questions
  - Use caution when providing credit card details
  - Don't allow push notifications

GORDON | REYNOLDS (2018)

AVOIDING SCAM ARTISTS

- Social Engineering is effective because people can be the weakest link.
  - Be vigilant, stop a social engineering attack before it begins.
  - Be a human firewall

GORDON | REYNOLDS (2018)

COMPUTER SYSTEMS SECURITY

CORE SECURITY PRINCIPLES: ANALYSING THE ATTACK SURFACE

GORDON | REYNOLDS (2018)

ANALYSING THE ATTACK SURFACE

- Attack Surface
  - Known or potential vulnerabilities across different areas that might be exposed
  - Example:
    - Hardware
    - Software
    - Networks
    - Users

GORDON | REYNOLDS (2018)

ANALYSING THE ATTACK SURFACE

- Vulnerability
  - A flaw in a system that can be exploited by threats to launch an attack and gain unauthorised access to an asset.
  - When we reduce the vulnerabilities in each attack surface, we can reduce the overall risk.
- Cyberattacks
  - Anything that can compromise the security of a system

GORDON | REYNOLDS (2018)

ANALYSING THE ATTACK SURFACE

- Types of Cyberattacks
  - Passive
    - Non-invasive, such as monitoring transmissions
    - Capturing passwords or data files
  - Active
    - Tries to break into secured systems
    - Steal, modify information, introduce malicious code

GORDON | REYNOLDS (2018)

ANALYSING THE ATTACK SURFACE

- There are many attack surfaces, each has a potential for an attack

GORDON | REYNOLDS (2018)

ANALYSING THE ATTACK SURFACE

- Software
  - Largest attack surface
  - There are a multitude of applications available
    - Applications (Word), Browsers (Safari), Mobile Apps (Pandora)
  - It also includes everything in the background
    - Software Code & Libraries

GORDON | REYNOLDS (2018)

ANALYSING THE ATTACK SURFACE

- Software Vulnerabilities
  - Theses are common and are found in all types of software and OS and are not limited to a specific vendor
  - When using software, you may or may notice the vulnerabilities, which appear as a flaw or glitch
  - Vulnerabilities can lead to an attack:
    - Can cause anything from minor annoyance to a system crash

GORDON | REYNOLDS (2018)

ANALYSING THE ATTACK SURFACE

- Hardware Attack Surface
  - Hardware provides an avenue for attack.
  - As simple as stealing your phone or cutting a cable
  - Generally, physical access to the device is required

GORDON | REYNOLDS (2018)

ANALYSING THE ATTACK SURFACE

- Network Attack Surface
  - Exposure to bogus networks
    - Looks normal
    - Gets you to join so they can capture information
  - Someone gaining access to a network
    - Using default passwords
    - Not using a strong enough password
  - Exercise: https://howsecureismypassword.net/

GORDON | REYNOLDS (2018)

ANALYSING THE ATTACK SURFACE

- User Attack Surface
  - Typically the weakest link
  - Can introduce malicious behaviour into the network
    - Both accidently or deliberately
  - Typically, it's a lack of education/training on the users behalf that can lead to a breach.
    - E.g. Social Engineering, where one click can lead to an attack

GORDON | REYNOLDS (2018)

ANALYSING THE ATTACK SURFACE

- Security Education Training and Awareness
  - Typically, an organisation will train their users in respect to security policies and best practices
  - This ensures employees are in tune with common security issues:
    - Report unusual activity
    - Delete emails requesting sensitive information
    - Keep all devices updated with malware protection

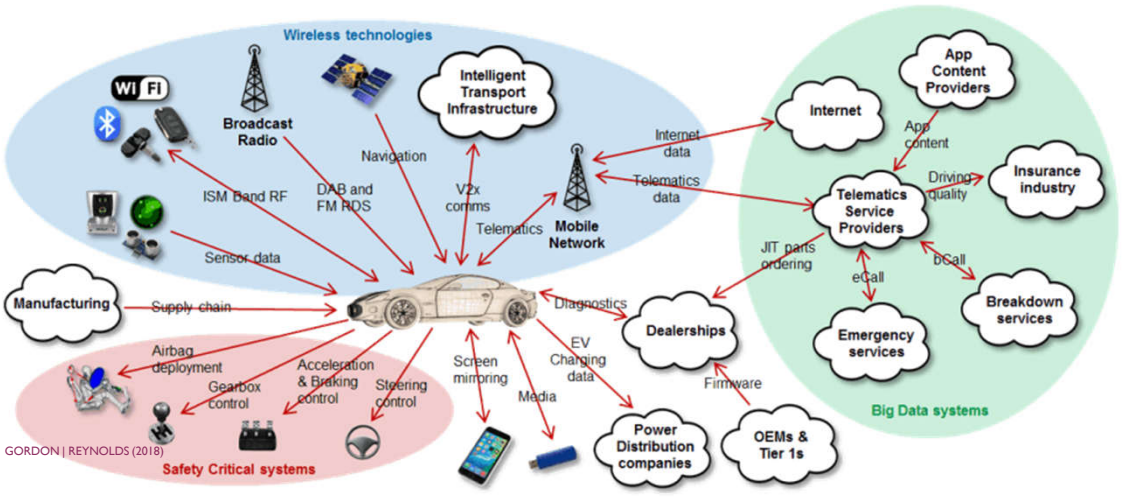
GORDON | REYNOLDS (2018)

ANALYSING THE ATTACK SURFACE

- Internet of Things (IoT)
  - A collection of devices attached to the internet
  - Collect and exchange data using nodes and controllers
  - IoT creates unique challenges in managing data as all systems become interconnected.
  - All attack surfaces must be considered

GORDON | REYNOLDS (2018)

ANALYSING THE ATTACK SURFACE



GORDON | REYNOLDS (2018)

ANALYSING THE ATTACK SURFACE

- Reduce Risk
  - Although we have many attack surfaces, the best way to reduce risk is by reducing the vulnerabilities
- Protect Systems
  - Update systems with the latest security patches
  - Enact software restriction policies
  - Remove unnecessary software and services

GORDON | REYNOLDS (2018)

ANALYSING THE ATTACK SURFACE

- Minimise the attack surface
  - Only enable the necessary features
  - Close unnecessary ports
  - Limit available resources (especially to untrusted users)
  - Implement IDS and firewalls
  - User education
    - Best practices for securing systems
    - Safe computing guidelines

GORDON | REYNOLDS (2018)

COMPUTER SYSTEMS SECURITY

CORE SECURITY PRINCIPLES: THREAT MODELLING

THREAT MODELLING

- Threat Modelling
  - Identifies possible weaknesses along with ways cybercriminals can use the information, across entry points such as software, hardware, network and users
  - Becoming more important due to multiple security threats.

THREAT MODELLING

- Multiple Security Threats
  - ***Ransomware*** – holding data hostage
  - ***Supply chain attacks*** – penetrates through a third-party vendor
  - ***Formjacking*** – theft of information from ecommerce forms
  - ***Cryptojacking*** – using a system to mine cryptocurrency

GORDON | REYNOLDS (2018)

THREAT MODELLING

- There a number of exercises that can help reduce risk:
  - ***Vulnerability analysis:*** analysing potential weaknesses for access vectors
  - ***Threat assessment:*** determine the best approach to securing a system against a threat
  - ***Threat modelling:*** looks at the external attack vectors and how the attacks are delivered

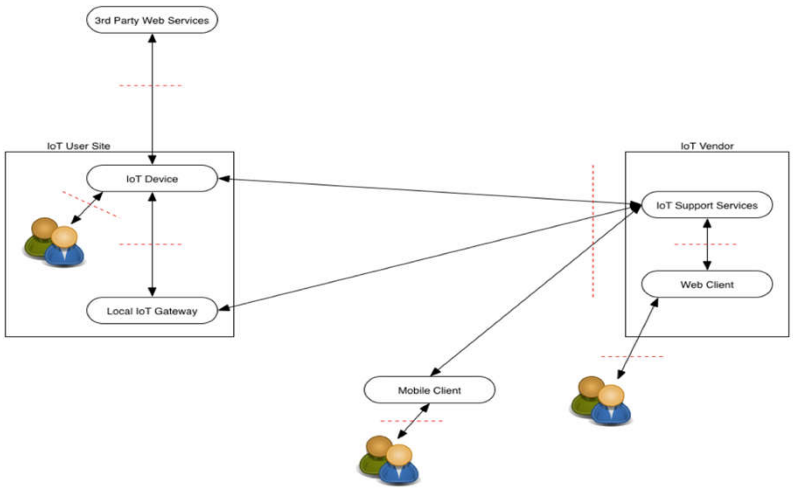
GORDON | REYNOLDS (2018)

THREAT MODELLING

- Threat modelling methods
  - Used to create a visualisation of the entire system along with potential entry points and a list of possible attacks.
  - The goal is to reduce overall risk

GORDON | REYNOLDS (2018)

THREAT MODELLING



GORDON | REYNOLDS (2018)

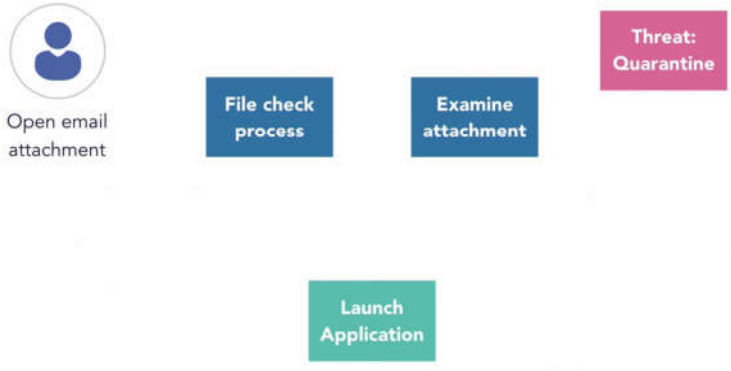
THREAT MODELLING

Threat Assessment

GORDON | REYNOLDS (2018)

THREAT MODELLING

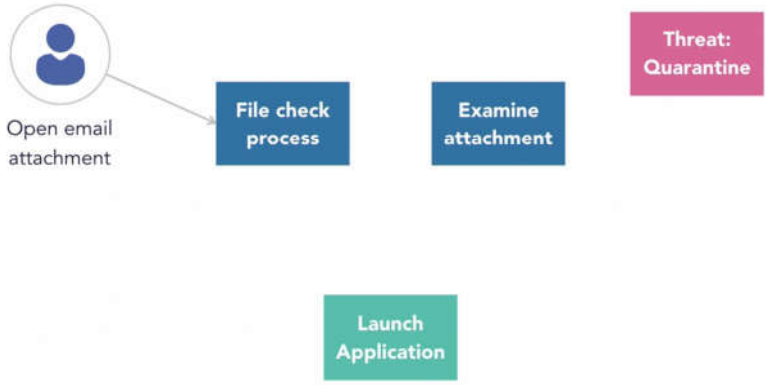
Address the Vulnerabilities



GORDON | REYNOLDS (2018)

THREAT MODELLING

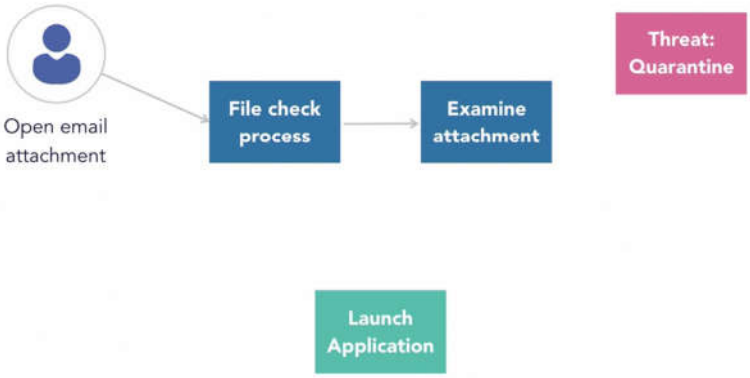
Address the Vulnerabilities



GORDON | REYNOLDS (2018)

THREAT MODELLING

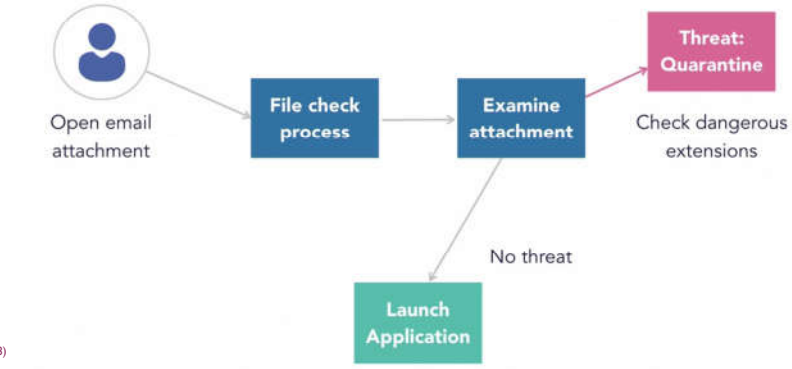
Address the Vulnerabilities



GORDON | REYNOLDS (2018)

THREAT MODELLING

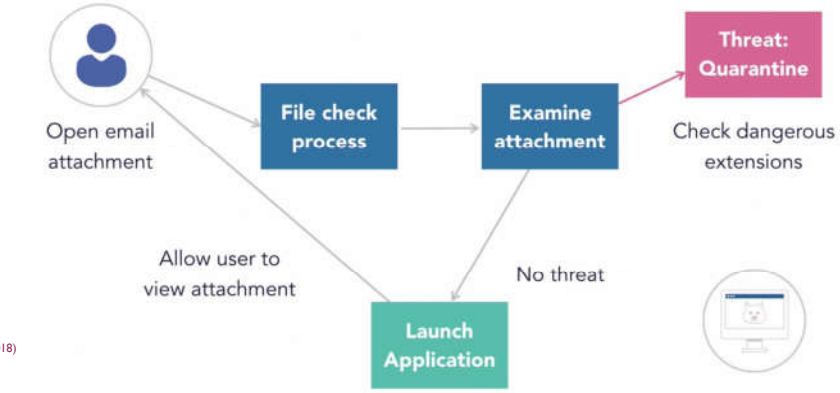
Address the Vulnerabilities



GORDON | REYNOLDS (2018)

THREAT MODELLING

Address the Vulnerabilities



GORDON | REYNOLDS (2018)

THREAT MODELLING

- Due to the increase in attack surfaces, data breaches are becoming more common. Check this with the following website:
  - https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

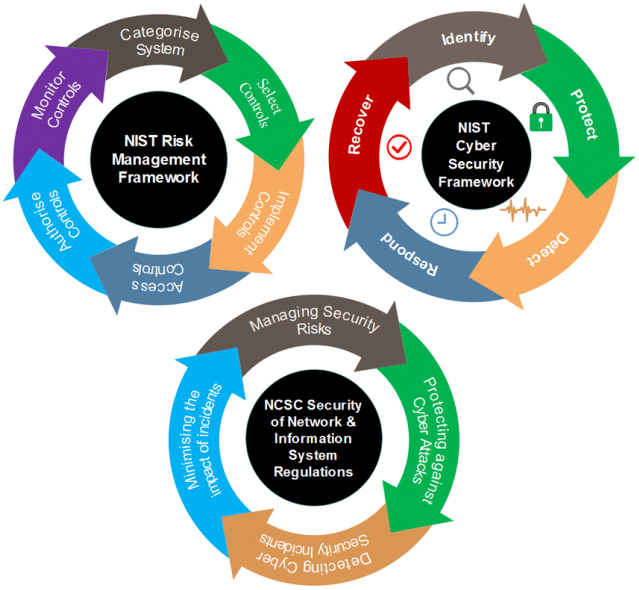
THREAT MODELLING

- Visualise Vulnerabilities
  - Prevent an attack that may result in data loss, business disruption, or even loss of life

SUMMARY ….

Today we looked at Core Security Principles, which includes:

- Keeping Information Safe
- Managing Risk
- Scam Artists
- Attack Surfaces
- Modelling Threats



GORDON | REYNOLDS (2019)