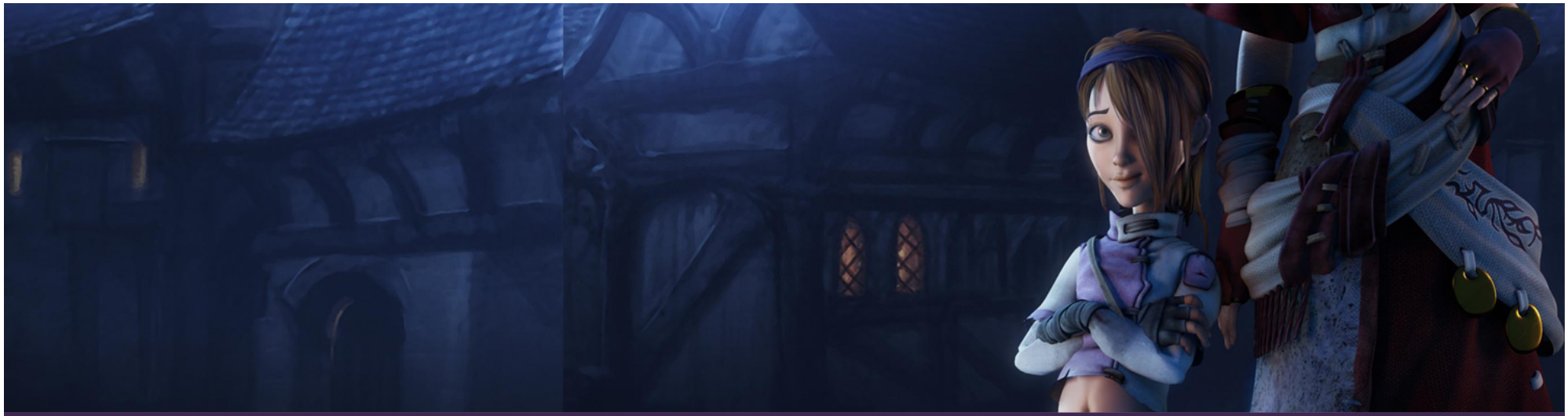


FALMOUTH
UNIVERSITY

Lecture 3: Controls and Legal frameworks for Cybersecurity

COMP280: Creative Computing
BSc(Hons) Computing for Games
BA(Hons) Game Development: Programming

FALMOUTH
UNIVERSITY

- Last time …
  - **Understand** how developments in social, technical, legal and economic spheres created an environment for cybersecurity
  - **Define** the term ‘cybersecurity’
  - **Identify** common hacking and phishing approaches

- Learning outcomes
  - **Define** the 3 types of control and 6 control strategies
  - **Understand** the application of GDPR and DMCA from the perspectives of individuals and organisations
  - **Identify** common software development issues using the OWASP as a framework

- Define the 3 types of control and 6 control strategies

- Types of control
  - As someone in charge of cybersecurity, what approaches can you use to:

protect the confidentiality, integrity & availability of an organisation's information assets from malicious actors and/or accidents.

- Types of control
  - As someone in charge of cybersecurity, what approaches can you use to:

    protect the confidentiality, integrity & availability of an organisation's information assets from malicious actors and/or accidents.

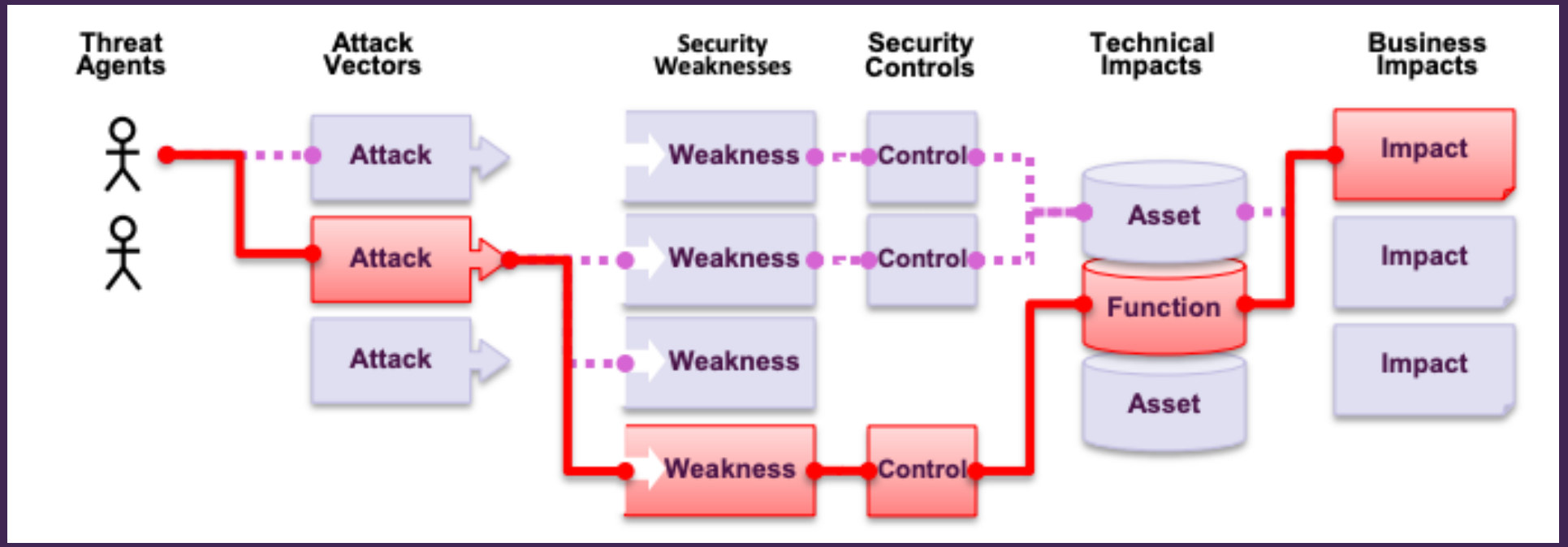
  - Normally, consider this as *'stopping bad things from happening'*
    - Let's make an impenetrable system
    - However, we know from our experiences with virus detection – *you are always one step behind the hackers*
    - This is the plot of every bad heist / hacking movie

- Types of control

'There are two types of companies: those that have been hacked and those that will be'

-Robert Mueller, FBI Director 2012

- Types of control



- Types of control
  - Preventative
  - Detective
  - Corrective

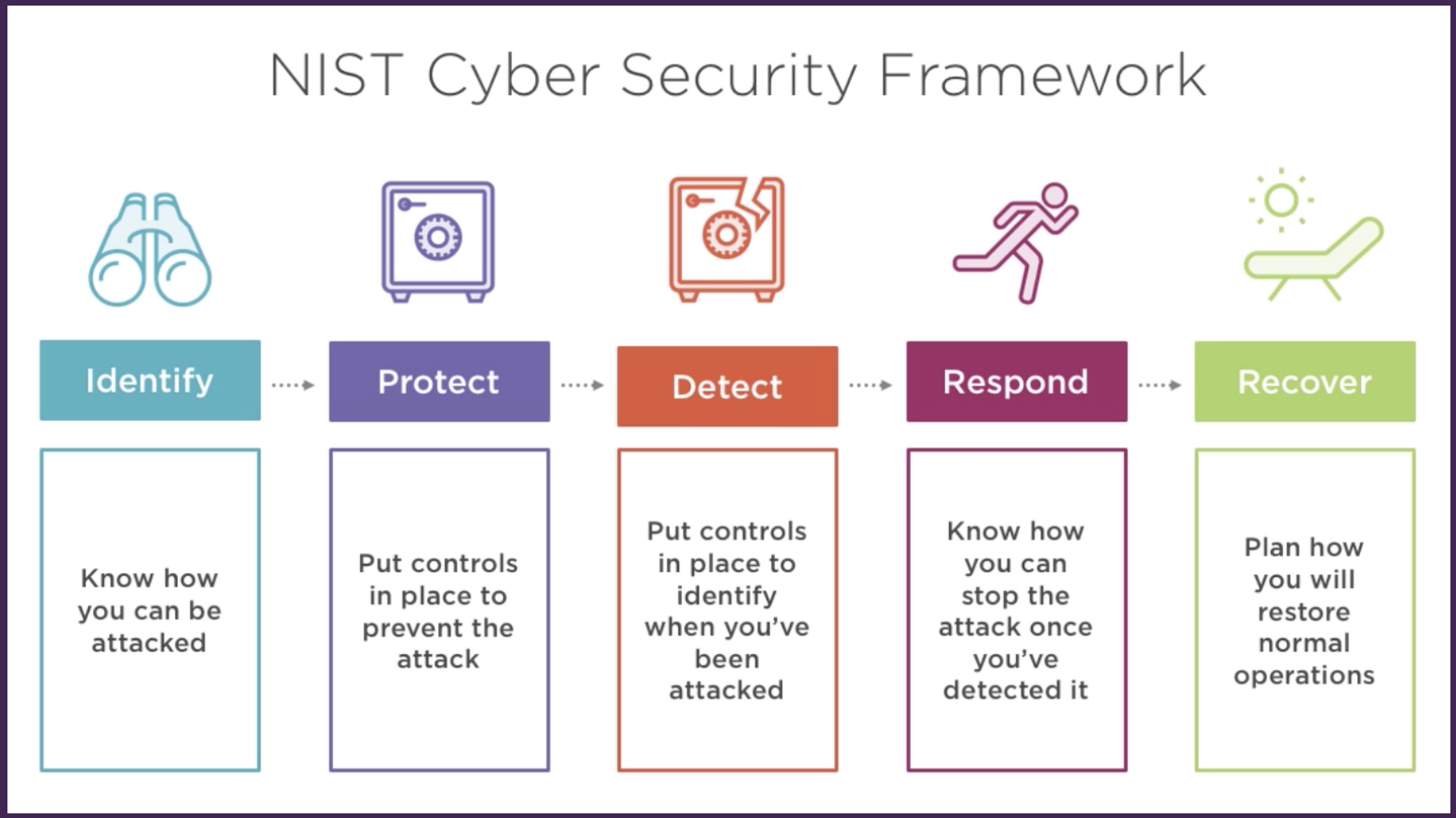
- Types of control
  - Preventative
    - We want to stop malicious activities where we can:
      - Passwords & usernames
      - Locking accounts (close accounts when people quit organisation, limit accounts to certain locations and levels of access)
      - Updating software to up to date versions
      - Training Users
      - Anti-virus / anti-malware applications
      - Firewalls
      - We can see this at play in the Academy as part of the IT policy
  - Detective
  - Corrective

- Types of control
  - Preventative
  - Detective
    - If we can't stop an attack with preventative measures, we want to monitor what's going on
      - Anti-virus / anti-malware reporting applications
      - Network logging systems
      - Log files
      - Again, these are all part of the Academy and University's IT Policies
  - Corrective

- Types of control
  - Preventative
  - Detective
  - Corrective
    - When bad things happen, we need to be able to recover lost assets & services quickly and efficiently
      - Incident report process
      - Forensic analysis
      - Back-ups
      - Redundant systems

- Control strategies
  - There are a lot of control strategies & frameworks:
    - ISO 27001
    - FFIEC Cyber Security assessment
    - Payment Card Industry Data Security Standard
    - Health Insurance Portability and Accountability Act (HIPAA)
    - CIS 20 Critical Controls
    - UK NCSC Cyber Essentials
    - Australian CSC Essential Eight
    - etc
    - These will often relate to industries, given that different kinds of industries will have different legal and ethical considerations to operate in
      - Remember cyber risk assessments from last week

- Control strategies
  - NIST Cybersecurity Framework
    - (US National Institute of Standards & Technology)



- Control strategies
  - 6 essential control strategies
    - Patch vulnerabilities
    - Application Whitelisting
    - System Hardening
    - Limit accounts
    - Two-factor authentication
    - Backup systems and data

- Control strategies
  - 6 essential control strategies
    - Patch vulnerabilities
      - Update O/S and S/W to address known vulnerabilities
      - This has become very common with internet-enabled devices
      - However, does open attack vectors for bogus updates ;)
    - Application Whitelisting
    - System Hardening
    - Limit accounts
    - Two-factor authentication
    - Backup systems and data

- Control strategies
  - 6 essential control strategies
    - Patch vulnerabilities
    - Application Whitelisting
      - Provide approved applications for users & update/patch to address vulnerabilities
    - System Hardening
    - Limit accounts
    - Two-factor authentication
    - Backup systems and data

- Control strategies
  - 6 essential control strategies
    - Patch vulnerabilities
    - Application Whitelisting
    - System Hardening
      - Hardening refers to removing things that aren't needed (or could cause issues)
      - Harden system security for machines & network infrastructure (e.g. closing ports to firewall)
      - Stop users from running their 'own' applications
      - This becomes an IT policy with things like 'no C drive' and no install privileges on user-level accounts.
    - Limit accounts
    - Two-factor authentication
    - Backup systems and data

- Control strategies
  - 6 essential control strategies
    - Patch vulnerabilities
    - Application Whitelisting
    - System Hardening
    - Limit accounts
      - Typically, O/S will provide ‘admin’ and ‘user’ level accounts
      - Look to limit number of admin accounts
      - Look to limit privilege and functionality of all accounts:
        - » Applications that can be run
        - » Access on network
    - Two-factor authentication
    - Backup systems and data

- Control strategies
  - 6 essential control strategies
    - Patch vulnerabilities
    - Application Whitelisting
    - System Hardening
    - Limit accounts
    - Two-factor authentication
      - Provide more than just name & password accounts
      - 2nd factor (mobile, email, app, device) can be very useful
      - Very frustrating in poor mobile environments
      - 2nd factor can be pointless if not properly considered
    - Backup systems and data

- Control strategies
  - 6 essential control strategies
    - Patch vulnerabilities
    - Application Whitelisting
    - System Hardening
    - Limit accounts
    - Two-factor authentication
    - Backup systems and data
      - Provide fast recovery for system failure & non-availability of systems and/or data (ransomware)
      - Back-up power …

- Control strategies
  - 6 essential control strategies
    - Patch vulnerabilities
    - Application Whitelisting
    - System Hardening
    - Limit accounts
    - Two-factor authentication
    - Backup systems and data
  - Control assurance
    - Put systems in place to make sure these strategies work
      - White hat hacking, disaster recovery
    - Keep strategies up to date

- Understand the application of GDPR and DMCA from the perspectives of individuals and organisations

- Legal frameworks
  - So far, cybersecurity sounds like the Wild West.
  - Part of STEP / PESTLE is L, Legal considerations
  - Law making tends to lag law breaking, particularly in ‘new’ areas
    - technology is a good example of this
    - Laws will often act as deterrent rather than detective measure
      - i.e. look to stop crime by making the downsides of crime larger than the upsides
    - Laws are often blunt

- Legal frameworks
  - UK
    - Computer Misuse Act (1990)
    - Serious Crime Act (2015)
    - Regulation of Investigatory Powers Act (2000)
  - US
    - Computer Fraud & Abuse Act (1986)
    - Digital Millennium Copyright Act (DMCA) (1998)
  - EU
    - General Data Protection Regulation (GDPR) (2018)

- Legal frameworks
  - Generally, these laws work to make unauthorised use of computers a criminal act
    - Blanket and vague enough to cover most cyber criminal attacks (hacking)
    - Can be problematic for social phishing crimes
      - Traditional fraud laws will generally cover them, but perpetrators are often in other countries
        - » Nigerian 419 scams
        - » Indian ‘help desk’ scams
      - For local crimes, US wire & mail fraud laws & UK fraud laws will apply

- GDPR (2018)
  - GDPR applies to all organisations operating within the European Union that process personal data and any companies in the world that process data about EU residents.
    - This makes it very wide ranging
  - Anyone or organisation that commits an offence under the GDPR can face fines of up to E20M or 4% of worldwide turnover for organisations
    - This makes it (potentially) very costly

- GDPR (2018)
  - GDPR covers all personal data relating to identifiable living individuals, that is help or indented to be be held in a computer or structured filing system.
-

- GDPR (2018)
  - As a collector / store of data you have clear responsibilities
  - As a data subject you have rights:
    - Right to be informed about your data
    - Right of access
    - Right of rectification
    - Right to erasure
    - Right to restrict processing
    - Right to data portability
    - Right to object
    - Right to challenge automated decisions
  - Exceptions to this are:
    - Data is necessary for protecting life or providing medical treatment
    - Clear legal requirement or strong public interest

- DCMA (1998)
  - US copyright law concerning circumvention of DRM
  - Often referred to in games as ‘DCMA takedowns’
    - To remove unflattering game commentary on Steam, Youtube et al
      - See jimquisition
  - Remember, *information assets* covers digital content
    - Content creators rightly have significant issues with content sharing, particularly if they aren’t being paid for it

- Identify common software development issues using the OWASP as a framework

- Creating secure applications
  - OWASP (Open Web Application Security Project)
    - Open community to share good practice
    - Produces a yearly top-10 of issues
      - https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
    - Can be used by developers to build better systems
      - Input for ‘types of control’
      - ‘Identify’ as part of NIST framework
      - ‘Overarching’ control strategy

- Creating secure applications
  - OWASP (Open Web Application Security Project)
    - A10: Insufficient Logging and Monitoring
    - A9: Using components with known vulnerabilities
    - A8: Insecure Deserialisation
    - A7: Cross-site scripting (XSS)
    - A6: Security misconfiguration
    - A5: Broken Access Control
    - A4: XML External Entities
    - A3: Sensitive Data Exposure
    - A2: Broken Authentication
    - A1: Injections (SQL, LDAP)

- Wrap-up
  - Significant resources exist for cybersecurity
    - Though you are always vulnerable to novelty
    - Expect to be hacked at some point and work out
      - 1. how to detect anomalous situations
      - 2. how to recover from them with back-ups and redundant systems
      - 3. how to stop them from happening in the future
  - Legal protection exists world-wide
    - Not all of it is for organisations (GDPR)
    - Will be scant reward seeing hackers sent to prison if your company has lost IP, reputation, finance etc

- Wrap-up
  - **Define** the 3 types of control and 6 control strategies
    - Control types:
      - Stop things from happening
      - Detect when bad things happen
      - Recover from whatever has happened
    - Control strategies
      - Patch vulnerabilities
      - Application Whitelisting
      - System Hardening
      - Limit accounts
      - Two-factor authentication
      - Backup systems and data

- Wrap-up
  - **Understand** the application of GDPR and DMCA from the perspectives of individuals and organisations
    - GDPR exists to protect living individuals
    - DMCA exists to protect copyright holders

- Wrap-up
  - **Identify** common software development issues using the OWASP as a framework
    - We have the OWASP top ten
      - https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

A10: Insufficient Logging and Monitoring
A9: Using components with known vulnerabilities
A8: Insecure Deserialisation
A7: Cross-site scripting (XSS)
A6: Security misconfiguration
A5: Broken Access Control
A4: XML External Entities
A3: Sensitive Data Exposure
A2: Broken Authentication
A1: Injections (SQL, LDAP)

      - These are all defined in OWASP report

- Questions