



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

ACCA7028

Data Security, Governance and Compliance

Week 2 :The need for Security

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk

Learning Objective(s) and Key Concepts

Learning Objective(s)

- Identify and describe the issues related to threats and vulnerabilities in an IT infrastructure.

Key Concepts

- Threats, and vulnerabilities
- IT and network infrastructures
- Malicious attacks
- Attack perpetrators and attack vectors
- The importance of countermeasures

Introduction

- IT enables the storage and transportation of information—often a company's most valuable resource—from one business unit to another
 - But what happens if the vehicle breaks down, even for a little while?
- Astute managers increasingly recognize the critical nature of information security as the vehicle by which the organisation's information assets are secured
- The emergence of executive-level InfoSec managers allows for the creation of professionally managed information security teams that have a primary objective to protect information assets, wherever—or whatever—they may be

Sun Tzu Wu's The Art of War

Therefore I say: One who knows the enemy and knows himself will not be in danger in a hundred battles

One who does not know the enemy but knows himself will sometimes win, sometimes lose. One who does not know the enemy and does not know himself will be in danger in every battle (Sun Tzu, 500 BC)

- To protect your organisation's information, you must:
 - know yourself; that is, be familiar with the information assets to be protected and the systems, mechanisms, and methods used to store, transport, process, and protect them; and
 - know your enemy; that is the threats your organisation faces

Key Concepts of Information Security: Threats and Attacks

- A threat represents a *potential* risk to an information asset, whereas an attack (or threat event) represents an ongoing act against the asset that could result in a loss
- Threat agents damage or steal an organisation's information or physical assets by using exploits to take advantage of a vulnerability where controls are not present or no longer effective
 - Attack: “an intentional or unintentional act that can damage or otherwise compromise information and the systems that support it”
 - Exploit: “a technique used to compromise a system... Threat agents may attempt to exploit a system or other information asset by using it illegally for their personal gain”
 - Vulnerability: “a potential weakness in an asset or its defensive control system(s)”

Forces of Nature

- Forces of nature can present some of the most dangerous threats because they usually occur with little warning and are beyond the control of people
- Because it is not possible to avoid these threats, organisations must implement controls to limit damage and prepare contingency plans for continued operations
- Force majeure, or “superior force,” includes forces of nature as well as civil disorder and acts of war
- Most forces of nature can only be mitigated through insurance, although careful facilities design and placement can reduce the likelihood of damage

Forces of Nature

Some typical force of nature attacks include the following:

- Fire
- Flood
- Earthquake
- Lightning
- Landslide or mudslide
- Tornados or severe windstorms
- Hurricanes, typhoons, and tropical depressions
- Tsunami
- Electrostatic discharge (ESD)
- Dust contamination

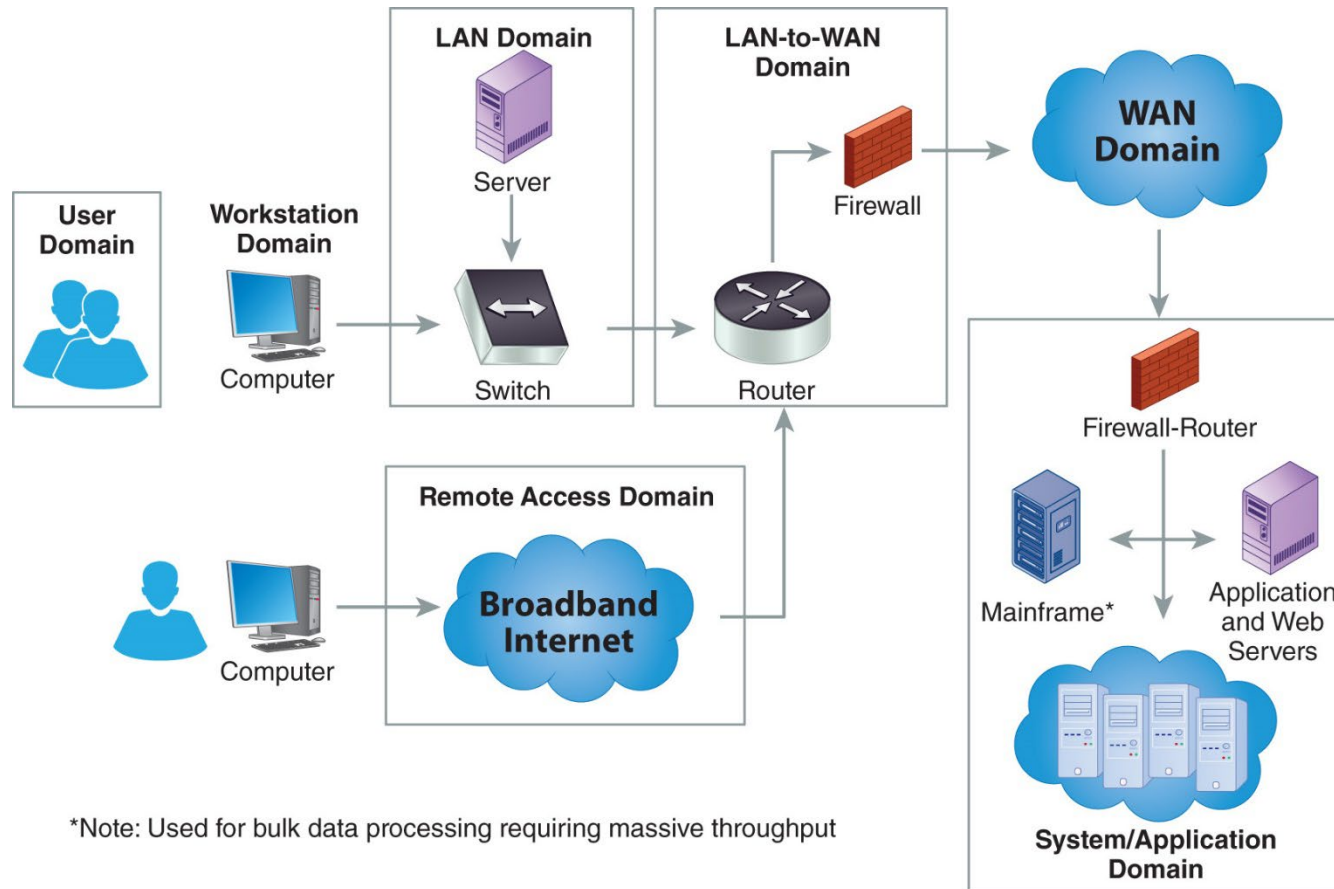
Protecting Physical Security

- Heating, ventilating, and air conditioning (HVAC)
- Fire suppression
- Electromagnetic interference (EMI) shielding
- Lighting
- Signs
- Fencing
- Barricades
- Biometrics
- Protected access (cabling)
- Alarms
- Guards
- Motion detectors
- Video surveillance
- Locks
- Mantraps
- Access lists
- Proximity readers
- Escape plan
- Escape routes
- Drills
- Control testing

Selecting Safeguards and Countermeasures

- Fix known exploitable software flaws
- Develop and enforce operational procedures and access controls (data and system)
- Provide encryption capability
- Improve physical security
- Disconnect unreliable networks

IT and Network Infrastructure



Intellectual Property

- The central asset of many organisations
 - Patents
 - Drug formulas
 - Engineering plans
 - Sales and marketing plans
 - Scientific formulas
 - Recipes
- Protecting intellectual property is a top-of-mind consideration for any organisation

Finances and Financial Data

- Financial assets are among highest-profile assets in any organisation
- Loss of financial assets due to malicious attacks is a worst-case scenario for all organisations
- Represents significant physical loss
- Can have long-term effects on a company's reputation and brand image

Service Availability and Productivity

- Critical services
 - Must be available for use when organisations need them
- Downtime
 - The time during which a service is not available due to failure or maintenance
- Unintentional downtime
 - The result of technical failure, human error, or attack
- Opportunity cost
 - The amount of money a company loses due to either intentional or unintentional downtime

Reputation

- Companies that suffer from security breaches and malicious attacks that expose assets are likely to face serious negative consequences in the public eye
 - Even if the company's response were swift and solved the problem effectively
- Negative public perception could lead to a decline in the organisation's revenue, net worth, and market capitalization

Who Are the Perpetrators?

- Black-hat hackers
 - Try to break IT security and gain access to systems with no authorization to prove technical prowess or potentially steal sensitive data
- White-hat (or ethical) hackers
 - Information systems security professionals who have authorization to identify vulnerabilities and perform penetration testing
- Gray-hat hackers
 - Hackers with average abilities who may one day become black-hat hackers but could also choose to become white-hat hackers
- Crackers
 - Have a hostile intent, possess sophisticated skills, may be interested in financial gain, and represent the greatest threat to networks and information resources

Threats, and Vulnerabilities in an IT Infrastructure

- End-User Licensing Agreement (EULA)
 - Transfers software companies' risk to its end users from having vulnerable software and being held liable for a software vulnerability
- Hackers continuously look for known software vulnerabilities as a means to find an exploitable weakness
- Vulnerability window
 - The gap in time between the announcement of a vulnerability and the application of a patch
- Zero day (in zero-day vulnerability)
 - A vulnerability window of zero days because there is no patch yet for a known software vulnerability

The Most Common IT Infrastructure Threats

- Malicious software
- Hardware or software failure
- Internal attacker
- Equipment theft
- External attacker
- Natural disaster
- Industrial espionage
- Terrorism

Threat Targets and Types

- Threat Targets
 - Identify where in the seven domains of an IT infrastructure threats are likely to occur
- Threat Types
 - Disclosure threats
 - Alteration threats
 - Denial or destruction threats

What Is a Malicious Attack?

- Four categories of attacks
 - Fabrications
 - Interceptions
 - Interruptions
 - Modifications

Types of Active Threats

- Birthday attacks
- Brute-force password attacks
- Credential harvesting and stuffing
- Dictionary password attacks
- Internet Protocol (IP) address spoofing
- Hijacking
- Replay attacks
- Man-in-the-middle attacks
- Masquerading
- Eavesdropping
- Social engineering
- Phreaking
- Phishing
- Pharming

What Are Common Attack Vectors?

- Attacks on availability
- Attacks on people
- Attacks on IT assets

Web Application Attacks

- Arbitrary/remote code execution
- Buffer overflow
- Client-side attack
- Cookies and attachments
- Cross-site scripting (XSS)
- Cross-site request forgery (CSRF)
- Directory traversal/command injection
- Header manipulation
- Integer overflow
- Lightweight Directory Access Protocol (LDAP) injection
- Local shared objects (LSO)
- Malicious add-on
- SQL injection
- Watering hole attack
- XML injection
- Zero day

Software and Web Application Attacks

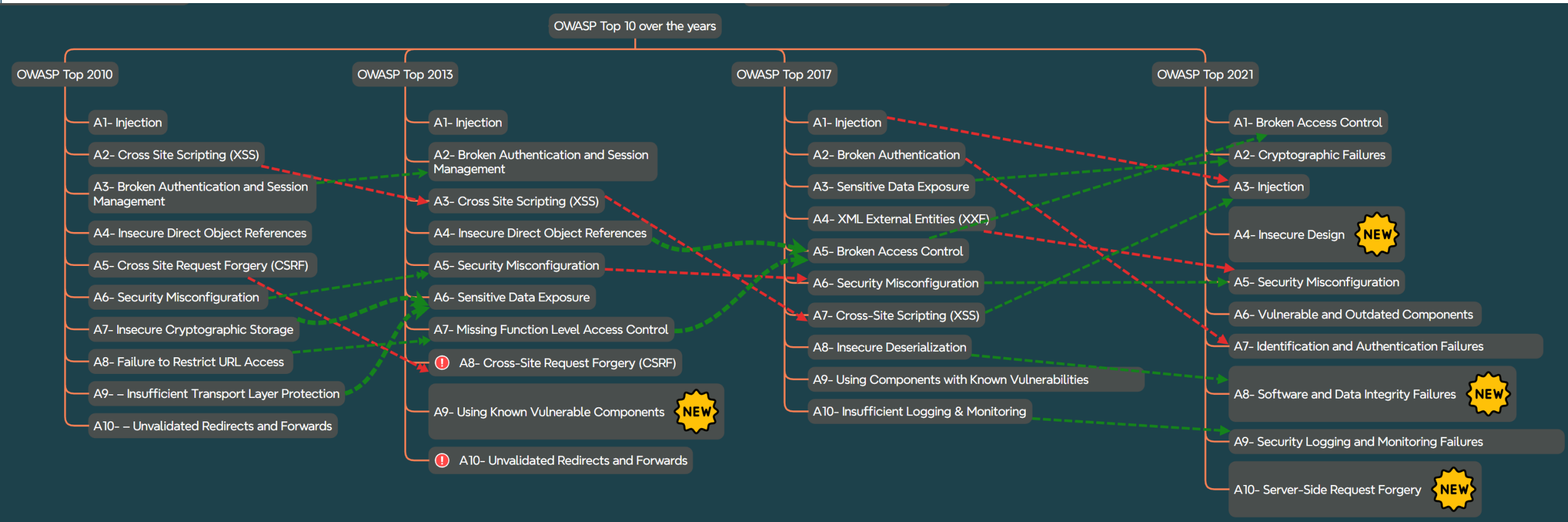
- Deliberate software attacks occur when an individual or a group designs and deploys software to attack a system
- This software can be used to overwhelm the processing capabilities of online systems or to gain access to protected systems by hidden means
 - Malware—viruses, worms, Trojan horses, polymorphic threats and hoaxes
 - Back doors, trap doors, and maintenance hooks
 - Denial-of-service (DoS) and distributed denial-of-service attacks (DDoS)
 - E-mail attacks—spam, mail bombs, and social engineering attacks
 - Communications interception attacks—packet sniffers, spoofing, pharming, and man-in-the-middle attacks

Technical Hardware Failures

- Technical hardware failures or errors occur when a manufacturer distributes equipment containing a known or an unknown flaw, which can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability
- In hardware terms, failures are measured in mean time between failure (MTBF) and mean time to failure (MTTF)
 - MTBF presumes that the item can be repaired or returned to service, MTTF presumes the item must be replaced
 - From a repair standpoint, $MTBF = MTTF + MTDD + MTTR$, where mean time to diagnose (MTDD) examines diagnosis time and mean time to repair (MTTR) calculates repair time

Technical Software Failures

- Large quantities of computer code are written, debugged, published, and sold before all their bugs are detected and resolved
- Sometimes, combinations of certain software and hardware reveal new failures that range from bugs to untested failure conditions
- Sometimes these bugs are not errors, but purposeful shortcuts left by programmers for benign or malign reasons, bypassing security checks to speed up software testing—known as trap doors
- Among the most popular bug documentation Web site is Bugtraq, hosted by Security Focus, which provides up-to-the-minute information on the latest security vulnerabilities as well as a thorough archive of past bugs



Technical Software Failures (Continued)

The Open Web Application Security Project (OWASP) list of “The Ten Most Critical Web Application Security Risks” for 2020:

Deadly Sins of Software Security

Web Application Sins

- SQL injection
- Web server-related vulnerabilities
- Web client-related vulnerabilities (XSS)
- Use of magic URLs, predictable cookies, and hidden form fields

Implementation Sins

- Buffer overflow
- Format string problems
- Integer overflows
- C++ catastrophes
- Catching exceptions
- Command injection
- Failure to handle errors correctly
- Information leakage
- Race conditions
- Poor usability
- Not updating easily
- Executing code with too much privilege
- Failure to protect stored data
- The sins of mobile code

Deadly Sins of Software Security

Cryptographic Sins

- Use of weak password-based systems
- Weak random numbers
- Using the wrong cryptography

Networking Sins

- Failure to protect network traffic
- Improper use of PKI, especially SSL
- Trusting network name resolution

Compromises to Intellectual Property

- Intellectual property (IP) can be trade secrets, copyrights, trademarks, and patents
- IP is protected by U.S. Copyright and other laws, carries the expectation of proper attribution or credit to its source, and potentially requires the acquisition of permission for its use, as specified in those laws
- The unauthorised appropriation of IP constitutes a threat to information security
- This category includes two primary areas:
 - Software piracy
 - Copyright protection and user registration

Deviations in Quality of Service

- An organisation's information system depends on the successful operation of many interdependent support systems, including power grids, data and telecommunications networks, parts suppliers, service vendors, and even janitorial staff and garbage haulers, any of which can be interrupted by severe weather, employee illnesses, or other unforeseen events
- Irregularities in Internet service, communications, and power supplies can dramatically affect the availability of information and systems
- Subcategories of this threat include the following:
 - Internet service issues
 - Communications and other service provider issues
 - Power irregularities

Espionage or Trespass

- When an unauthorised person gains access to information an organisation is trying to protect, the act is categorised as espionage or trespass
- When information gatherers employ techniques that cross a legal or ethical threshold, they are conducting industrial espionage
- In the real world, a hacker frequently spends long hours examining the types and structures of targeted systems and uses skill, guile, and/or fraud to attempt to bypass controls placed on information owned by someone else
- Once an attacker gains access to a system, the next step is to increase privileges (privilege escalation) to gain administrator- (or root-) level control

Espionage or Trespass

- Password attacks fall under the category of espionage or trespass just as lock-picking falls under breaking and entering
- Attempting to guess or reverse-calculate a password is often called cracking
- There are alternative approaches to password cracking:
 - Brute force attack
 - Dictionary password attack
 - Rainbow tables
 - Social engineering password attack

Social Engineering Attacks

- Authority
- Consensus/social proof
- Dumpster diving
- Familiarity/liking
- Hoaxes
- Impersonation
- Intimidation
- Scarcity
- Shoulder surfing
- Smishing
- Tailgating
- Trust
- Trusted users
- Urgency
- Vishing
- Whaling

Human Error or Failure

- This category includes acts performed without intent or malicious purpose or in ignorance by an authorised user
- When people use information systems, mistakes happen; similar errors happen when people fail to follow established policy
- Inexperience, improper training, and incorrect assumptions are just a few things that can cause human error or failure
- One of the greatest threats to an organisation's information security is its own employees, as they are the threat agents closest to the information
- Human error or failure often can be prevented with training, ongoing awareness activities, and controls

Human Error or Failure

- Some typical human error or failure attacks include the following:
 - Social engineering
 - Phishing
 - URL manipulation
 - Web site forgery
 - Spear phishing
 - Pretexting
 - Information extortion
 - Information extortion, also known as cyberextortion, is common in the theft of credit card numbers
- Recent information extortion attacks have involved specialised forms of malware known as ransomware that encrypt the user's data and offer to unlock it if the user pays the attacker



Figure 1-5 Ransomware notification screen

Source: Wikipedia Commons public-domain images (Securelist.com).

Sabotage or Vandalism

- This category of threat involves the deliberate sabotage of a computer system or business, or acts of vandalism to destroy an asset or damage the image of an organisation
- These acts can range from petty vandalism by employees to organised sabotage against an organisation
- Vandalism to a Web site can erode consumer confidence, diminishing an organisation's sales, net worth, and reputation
- Activism in the digital age:
 - Online activism
 - Cyberterrorism and cyberwarfare
 - Positive online activism

Technological Obsolescence

- Antiquated or outdated infrastructure can lead to unreliable and untrustworthy systems
- Management must recognize that when technology becomes outdated, there is a risk of losing data integrity from attacks
- Ideally, proper planning by management should prevent technology from becoming obsolete, but when obsolescence is clear, management must take immediate action
- Perhaps the most significant case of technology obsolescence in recent years is Microsoft's Windows XP

Theft

- The value of information is diminished when it is copied without the owner's knowledge
- Physical theft can be controlled easily using a wide variety of measures, from locked doors to trained security personnel and the installation of alarm systems
- Electronic theft, however, is a more complex problem to manage and control
- Theft is often an overlapping category with software attacks, espionage or trespass, information extortion, and compromises to intellectual property

Wireless Network Attacks

- Bluejacking
- Bluesnarfing
- Evil twin
- Initialization vector (IV) attack
- Jamming/ interference
- Near field communication attack
- Packet sniffing
- Replay attack
- Rogue access point
- War chalking
- War driving

References

- Lectures slides are devices from the recommended books resources.
 - Pearson Education 2014, Information Security: Principles and Practices, 2nd Edition
 - Fundamentals of Information Systems Security, by David Kim , and Michael G. Solomon



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk