Security

Week 6 – Information Governance (CIS3005-N)

Vicky Rushin-Chape

Schedule – Week 6

Week	Date	Lecture, IT Lab & Weekly Feedback on Progress
1	23rd Jan 2025	Welcome, **Introduction & Case Studies**
2	30th Jan 2025	Principles of information governance, **ICA Released, Q&A**
3	6th Feb 2025	Risk Management, **ICA Development**
4	13th Feb 2025	Social engineering 1, **ICA Development**
5	20th Feb 2025	Social engineering 2, **ICA Development**
6	27th Feb 2025	Security, **ICA Development, Review & Feedback 1**
7	6th Mar 2025	ISO 27k 1, **ICA Development, ICA Development, Review & Feedback 2**
8	13th Mar 2025	Managing change, **ICA Development, Review & Feedback 3**
9	20th Mar 2025	ISO 27k 2, **ICA Development, Review & Feedback 4**
10	27th Mar 2025	Compliance and legal issues, **ICA Development, Review & Feedback 5**
11	3rd April 2025	Business Continuity and Disaster recovery planning, **ICA Development, Review & Feedback 6**
Spring Break (3 weeks)		
12	1st May 2025	ICA Q&A, **ICA Development, Review & Feedback 7**
ICA Hand-in – Friday 2nd May 2025, 4pm via Blackboard		

Recap & introduction

Last week – Social Engineering 2 with Chidimma
This week looking at Security -> feeds into:

- Several module learning outcomes/KSBs; ties in to ISO27K which you'll look at next week with Chidimma
- Assessment: you will need to: identify risks and mitigation relating to security; show your understanding of ISO standards in relation to security

Classification/Types of Information Security

Can you name any *specific* types of information security?
If I asked you to classify types of security what might they be?

Classification/Types of Information Security

Physical Security

Endpoint Security

Application Security

Network Security

- Cloud Security
- Internet Security
- Mobile Security

As a business, which of these security groups does the University need to consider? Why?

Tools and Techniques - Cybersecurity

What tools and techniques can be employed to aid information security?

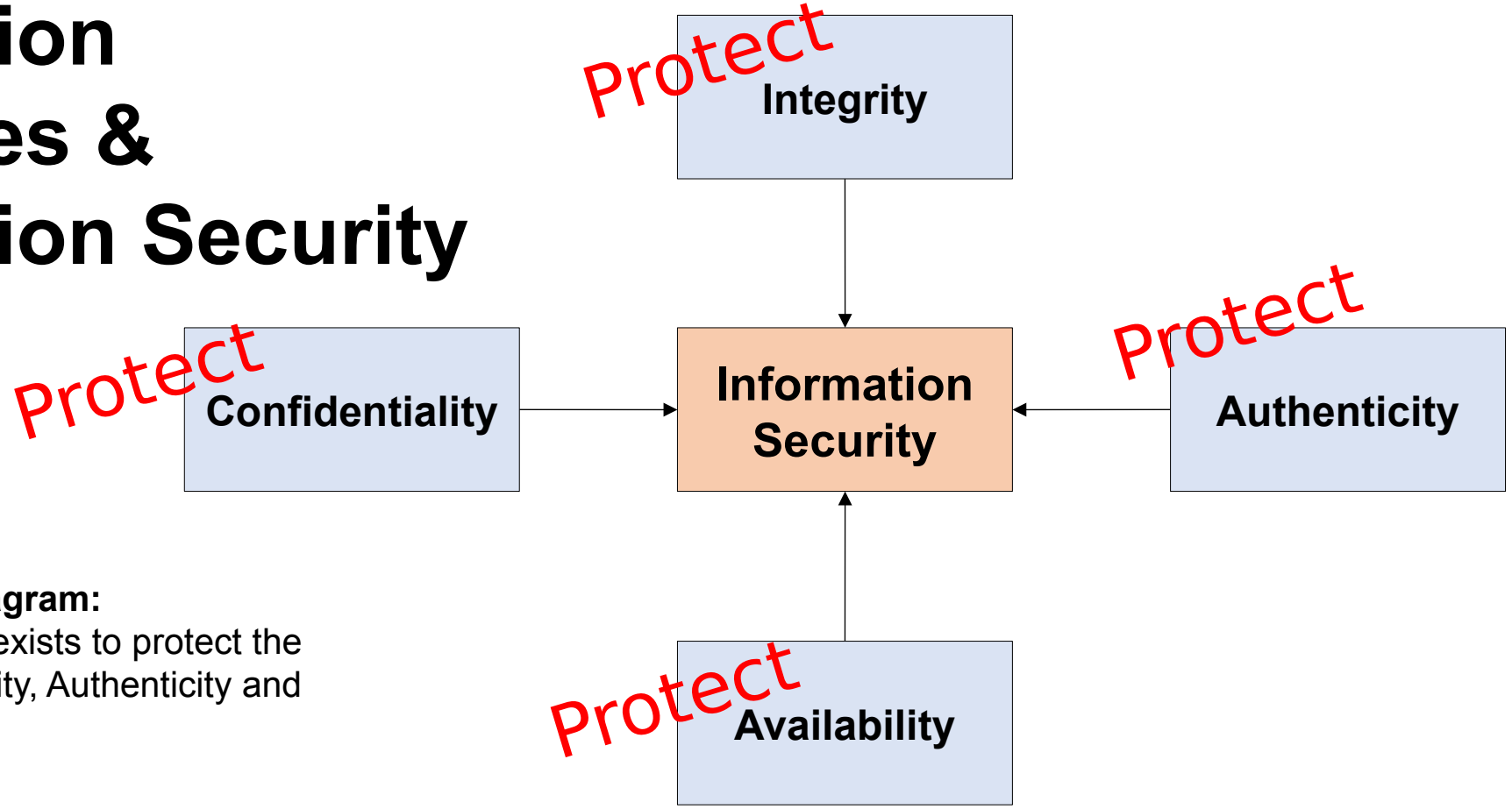
Tools and Techniques - Cybersecurity

- Authentication
  - Knowledge Factors (e.g. password)
  - Possession Factors (e.g. RFID card)
  - Inheritance Factors (biometric)
- Encryption
- Firewall
- Antivirus
- Digital Signature

- Anti-spam
  - Word (simple) / heuristic (algorithmic scoring) / Bayesian filters (+AI)
  - Blacklist / greylist / whitelist
- DNS Filtering
- Secure web gateway

Which of these tools and techniques do you think the University do/should employ?

Information Properties & Information Security



How to read this diagram:
Information Security exists to protect the Integrity, Confidentiality, Authenticity and Availability of data

Adapted from Shimeall, T; 2014

Protecting Integrity

- Why does data need to be reliable?
- How do you ensure data integrity?
- Prevent unauthorised or undesirable access/changes to maintain organisational control

  - What type of organisation would identify data integrity as a main priority for information security? Why? (2 mins)
  - Key examples from the University
  - What is the potential outcome for organisations?

SECURITY CASE STUDY: AUTOTOTE INSIDER CASE—COMPROMISE OF DATA INTEGRITY

In early October 2002 [4], Glenn DaSilva placed a "pick four" bet on a local horserace via a phone call to an off-track betting facility operated by Autotote Systems, Inc. His bet was of a form where he picked two specific horses in the first two races, then the field (any horse at all) in the last two races. While this is ordinarily a very poor strategy, Glenn knew his bet would win, whether or not the horses he had marked won. His fraternity brother, Christopher Harn, a senior programmer at Autotote, would make sure of that.

Christopher had learned that, to avoid overloading the track computers, Autotote did not send the off-track bets to the track until 20 minutes after the second race in a four-race exacta, or after the fourth race in a six-race exacta. With Christopher's level of access, that gave him plenty of time. On the day of the race, Christopher arranged to be working. He monitored the races Glenn had bet on, and right after the second race, he ran a program that changed the bet so that the first two actual winners replaced the horses Glenn had bet on. That gave Glenn a guaranteed win, yielding over $100,000 in winnings, which Glenn split with Christopher.

Since no one noticed, the guys grew bolder. Christopher contacted Derrick Davis, another fraternity brother, and in October 2002, Derrick opened an account with Autotote and placed six bets on the Breeder's Cup, a very large national race. Since this was a six-race exacta, Derrick bet on four specific horses in the first four races, then the field on the last two. On the day of the race, Christopher ran his program again after the fourth race, changing the first four bets to reflect the actual winners.

Shortly after that is where things fell apart. The next race was won by a long shot—a horse almost nobody bet on. This was the third long-shot win in the exacta, which gave Derrick the only winning tickets. When the race officials examined the bets, they realized (due to the odd form of the bets, and that the same horses were bet on repeatedly) there was some form of irregularity and started an investigation, which quickly led to the arrest of Christopher, Derrick, and Glenn. Instead of the more than three million–dollar payoff from the bet, they each ended up serving time in prison [5].

Protecting Authenticity

- Important to audit individual activity to ensure authenticity
- Systems have authorised users and processes/policies in place to maintain authenticity

  - Can you think of an example in the University where authenticity ***could*** be compromised?
  - What type or organisation would identify authenticity as a key priority for information security?
  - What is the potential outcome for organisations?

Protecting Availability

- Why protect availability?
  - Can you think of an example where availability could be compromised?
  - What type of organisation would identify availability as a key priority for information security?
  - What is the potential outcome for organisations?

Aeroplane system redundancy – no single points of failure

Protecting Confidentiality

- User access controls
- Credentials
- Policies and processes
- Auditing
  - All addressed in ITIL
  - Covered by Chidimma in ISO standards

Implementing Best Practice

- System Security
- Policy development and implementation
  - Internet/email policy
  - Data policy
- Training
- How do you think Teesside University deals with it?

Security in your ICA

- If you were an information security manager in the ICA case study, what vulnerabilities would you be most concerned about?
- How would you rank the information security priorities?
  - Integrity
  - Authenticity
  - Availability
  - Confidentiality

Security Exercises in Industry

- A commonly used tool designed to keep teams prepared for issues
- Similar to undertaking a fire drill, testing the response of people
  - Tabletop (see document on Blackboard)
    - Discussion based, talking through different scenarios
  - Functional
    - Operations-based and test organisational processes and responses
  - Hybrid
    - A combination of the two where senior managers undertake a tabletop exercise and other staff complete a functional exercise

Industry Case Studies

- Endpoint detection and response to increase plastic manufacturer's cy ber posture
- GDPR assessment and US data privacy laws action plan for a global p harmaceutical company

Homework: Can you spot the Security and Compliance Issues?

- What happened:
- https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/
- How it was fixed:
- https://www.wired.com/2012/08/mat-honan-data-recovery/