INVESTIGATING THE CYBERSECURITY POSTURE OF HIGHER EDUCATION INSTITUTIONS IN IRELAND. *AN IT PROFESSIONAL STAKEHOLDER PERSPECTIVE*

JOHN DUNNE, DR. JAMES EGAN
School of Computing, South East Technological University, Ireland

85%
Higher education organisations identified breaches or attacks in past year

31days+
Average recovery time Higher Education sector slowest recovery time following an attack

€3.5 million
Average cost of Data Breach in Higher Education

49%
Higher education say the level of cybersecurity they need to qualify for cyber insurance is now higher

1. Introduction

- Several high-profile cyber attacks on Irish HEIs in recent years causing substantial damage and cost.
- Targeted attacks of this nature are common and can completely paralyse or significantly disrupt HEIs operations and delivery of services.
- Cyber attacks can expose HEIs to wide reaching financial, Legal and regulatory consequences.
- This study sets out to explore the current state of the art of Cybersecurity In HEIs through the lens of IT Subject Matter experts working in the Sector.

What are some common types of cyberattacks?
HEIs have key assets, such as funds, resources and valuable data, that cybercriminals seek to exploit. Here are some of their most common tactics used to access HEIs systems.

Ransomware Attack
Paralysing systems and threatening to steal, block or publish University data unless a ransom is paid.

Hacking
Identifying weaknesses in a system or a network to gain access to data. Often involves using a password-cracking algorithm or purchasing passwords leaked to the Dark Web to break into HEI network to extract resources.

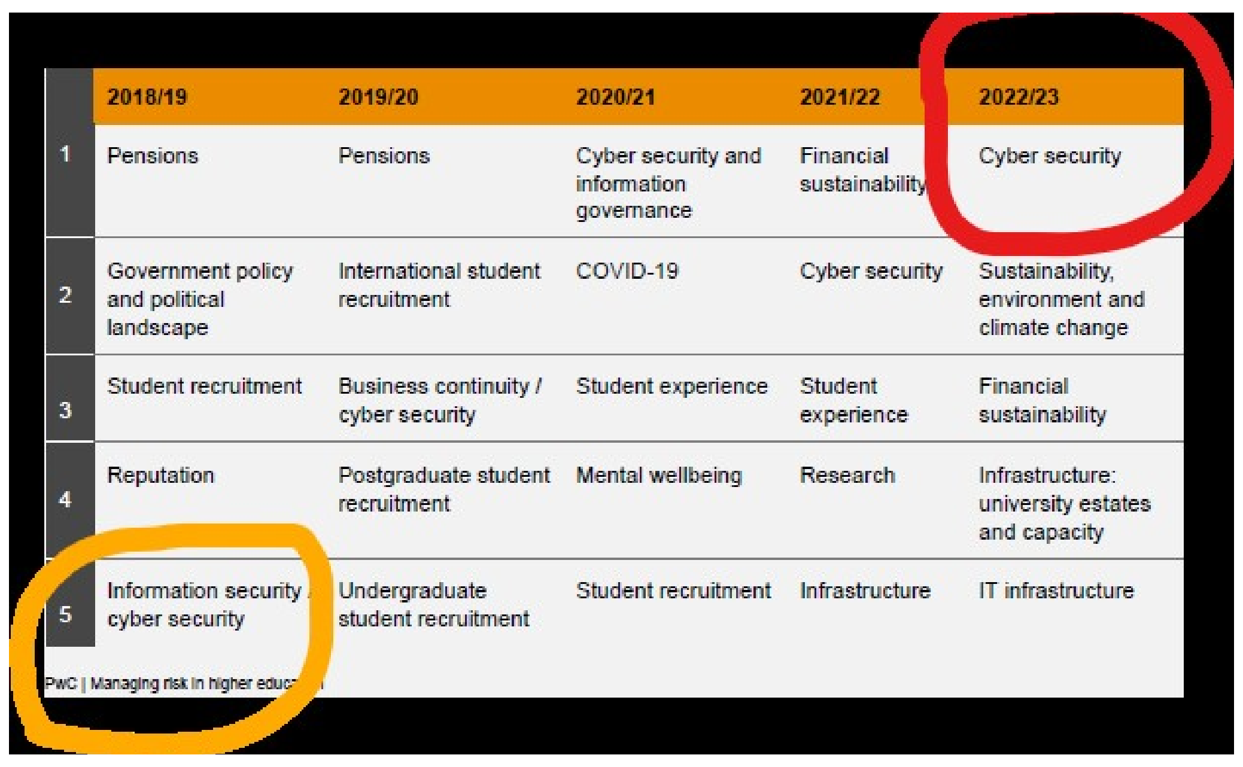
Phishing
Using electronic communications to deceive and take advantage of users, often beginning with an email attempting to obtain sensitive information by persuading a user to click on a malicious link or download an infected attachment.

Spear Phishing
Infiltrate the organisation to steal sensitive information through a targeted type of phishing. Attackers will often gather personal information about employees from HEIs websites and social media profiles to write emails with more authentic context.

Social-Engineering
Tactic to influence or deceive a victim to get them to freely provide sensitive information or download software in order to compromise HEI organisational security.

2. LIT Review

- HEIs are Lucrative targets for Cybercriminals (Valuable Data Stores).
- Heterogeneous technological nature of Higher Educational institutions pose system-wide security challenges.
- According to the literature Ransomware attacks are the most common malware infection in Higher Education.
- Cybersecurity Framework adoption varies with no Perfect "Fit"
- Cybersecurity has become a significant concern to the Higher Education sector in Ireland featuring high on Risk Registers.



	2018/19	2019/20	2020/21	2021/22	2022/23
1	Pensions	Pensions	Cyber security and information governance	Financial sustainability	Cyber security
2	Government policy and political landscape	International student recruitment	COVID-19	Cyber security	Sustainability, environment and climate change
3	Student recruitment	Business continuity / cyber security	Student experience	Student experience	Financial sustainability
4	Reputation	Postgraduate student recruitment	Mental wellbeing	Research	Infrastructure: university estates and capacity
5	Information security / cyber security	Undergraduate student recruitment	Student recruitment	Infrastructure	IT infrastructure

PwC | Managing risk in higher educ

Fig 2: Managing Risk in Higher Education

3. Research Questions

1. According to HEI professionals what is the current posture state of cybersecurity across Irish HEIs?
2. According to HEI professionals what are common cyber threats facing HEIs?
3. Can an improved cybersecurity posture be proposed in HEIs based on findings from this research?

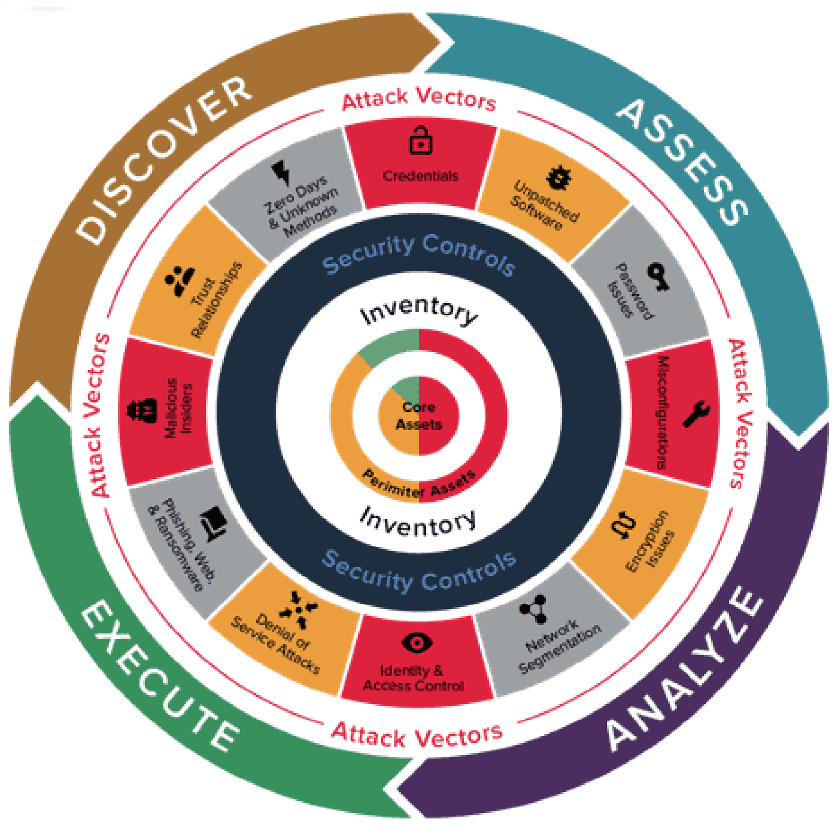


Fig 1: Conceptual diagram of security posture

4. Research Methodology

- Participant led data-driven inductive research approach.
- Interpretivist Philosophical Stance.
- Purposeful sampling.
- Cross-secional Time Horizon.

Data Collection & Analysis

- Qualatative Semi-Structured Interviews with IT Subject Matter Experts. working within HE Sector (Recording/Transcription MS Teams).
- Grounded Theory - Data Analysis using Nvivo Software.

5. Early Findings

- Lack of research on the state of cybersecurity across Higher Education Institutions.
- Strained IT resources and funding has led to slower development of cybersecurity measures than expected.
- Lack of Dedicated Cybersecurity Roles in HEIs.
- Partnerships Collaboration and Shared threat Intelligence is not optimised across the sector.
- Gov spotlighting Cybersecurity – 3.5 Million Initiative sectorwide - HEAnet SoC/SIEM - NCSC (PSB).
- NIS2 Critical Sectors (Education Institutions Optional for Member States)

Contacts

John Dunne
Tel: (+353) 59 9175695
e-mail: C00234454@setu.ie

References

- Fig 1: Conceptual diagram of security posture
  Balbix.. (2024). Conceptual diagram of security posture. [Online]. Balbix. Available at https://www.balbix.com/insights/what-is-cyber-security-posture

- Fig 2: Risk Register Findings (PwC)
  PricewaterhouseCoopers. (2023). Managing risk in Higher Education: Higher Education sector risk profile
  2023 - PwC [online]. Available from: https://www.pwc.co.uk/industries/government-public-sector/education/managing-risk-in-higher-education.html

- Statistic Bubbles
  "Cyber Security Breaches Survey 2023: Education Institutions Annex." GOV.UK, GOV.UK, 19 Apr. 2023, www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023-edu[1,2]
  IBM Security, 2023. IBM Cost of Data Breach Report 2023, New York: IBM[3]
  The State of Ransomware in Education 2022, white paper, (Abingdon, UK: Sophos, July 2022)[4]