UNIVERSITY OF LEEDS

Leeds University: A Case Study

Making Yourself Unimportant

By **Neil Favager**, IT Risk & Assurance Manager and **Filipe Baldin**, InfoSec Risk & Compliance Analyst

Introduction

UNIVERSITY OF LEEDS

Neil

- I am not technical, but I do work in IT
- People
- Trust no one
  - Especially Dave who put us on after a BAFTA award winner

Filipe

- New to IT but is technical
- People focussed too – teaching, customer service
- Likes people but is learning not to trust them

Who are we

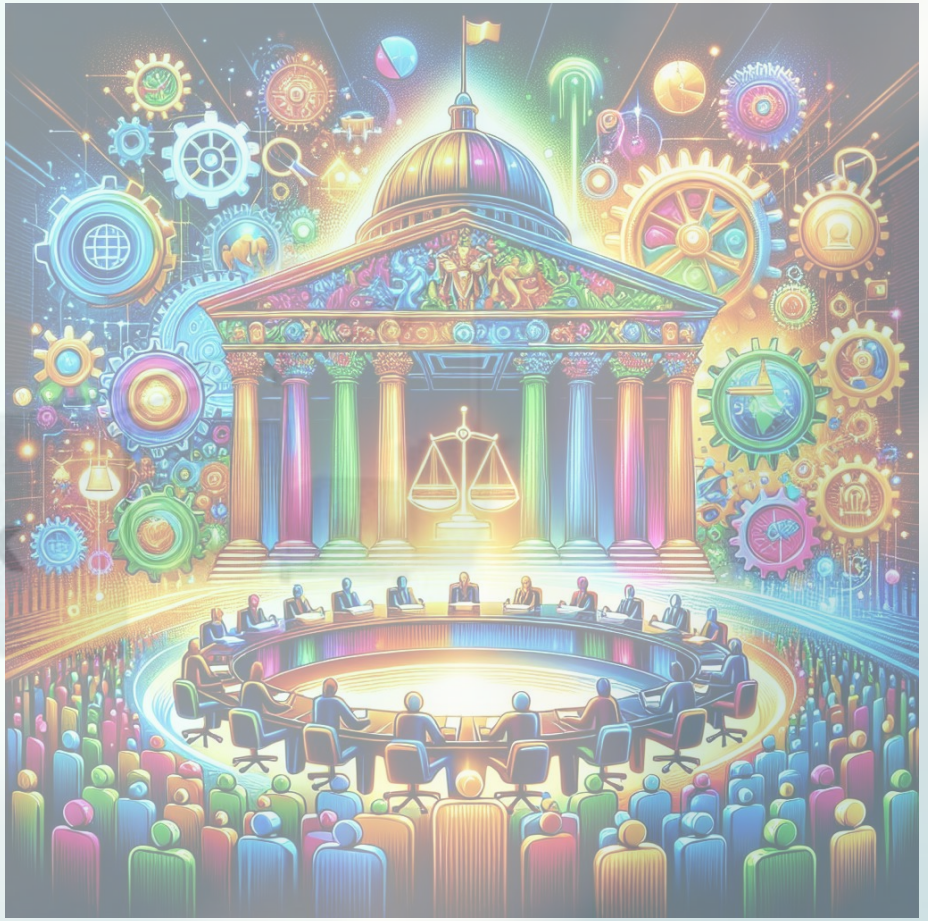
UNIVERSITY OF LEEDS

- How old is Leeds?
  - Established in 1904 King Edward VII granted charter but dating back to 1831 School of Medicine
- Currently 39000 students with some well-known alumni – including the current PM and Captain Kirk
- Approximately 12500 staff
- Famous staff include J.R.R. Tolkien
- University estate 1230 acres, main campus 98 acres in the centre of Leeds

Governance at UOL

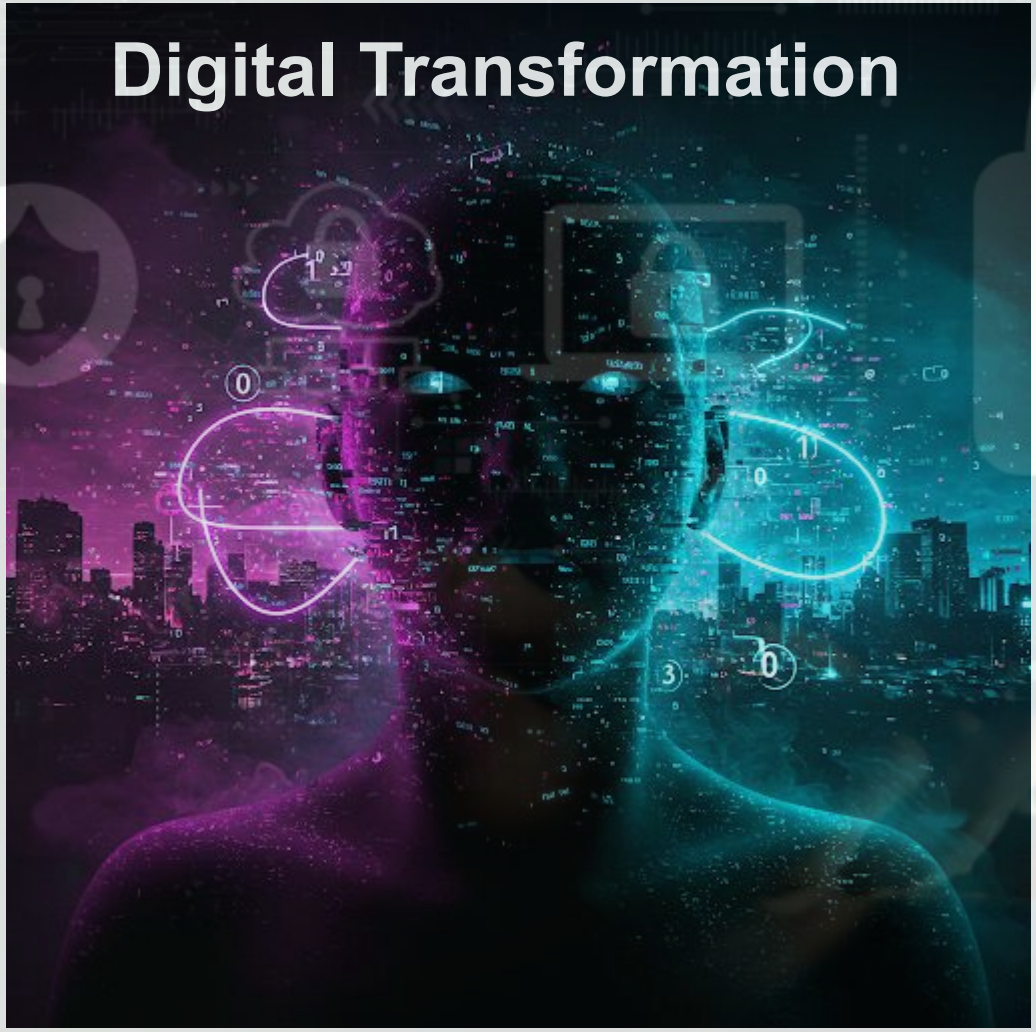
UNIVERSITY OF LEEDS

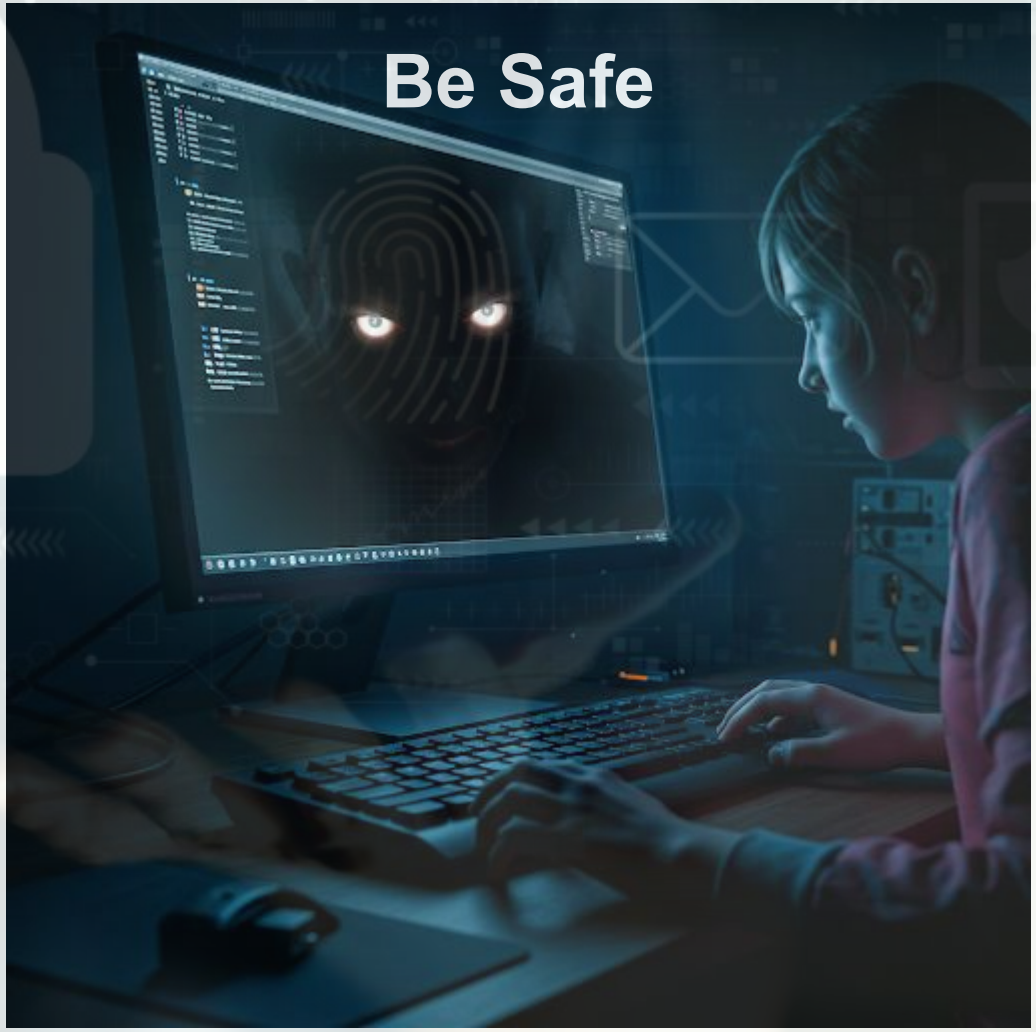
- University Strategy
  - IT/Finance Strategy
- Audit and Risk Committee
- Information Governance Oversight Group (IGOG)
- IT Design Authority
- CAB
- CISC
- Secretariat
- University Policies including PCI Policy
- The LAW



Keeping up with the Times

UNIVERSITY OF LEEDS





Where are we Today

UNIVERSITY OF LEEDS

- Compliant for 10 years
- Over 900,000 card payments under UoL Merchant IDs
- 90.5% payments are card present P2PE
- 3% (Approx 29,000 transactions) through e-commerce (on-prem) migrated to flywire SaaS and Merchant Of Record
  - Equating to just over 50% of monetary value of card transactions in the previous PCI cycle
- SaaS e-commerce applications (Store, Conferences, Library, PCB, Parking)
- Two on premise e-commerce applications (Print and Sport)
- Also, payments via Stripe (Ticketing, Student Supplies, merchandise and Hubbub (Alumni)

The Team

UNIVERSITY OF LEEDS

- Programme Manager: Finance Governance, Risk and Compliance Manager
- Core Team (2 x IT, 3 x Finance)
- Includes 3 ISAs (Finance and IT)
- Many stakeholders across the University
- Flywire as part of Payment Security Implementation Programme

Payment Security Implementation Programme

UNIVERSITY OF LEEDS

- In the 4th year – after six previous years of compliance
- Access to QSA and industry knowledge - Dave Neild with Mike Vale as backup
- Phil Watson as implementation Consultant
- Meet every two weeks with additional meetings on-site and virtual as required

The PSMS helps with

- Documentation
- Risk management
- Sense checking
- Embedding into BAU
- Flywire keep it up to date with changes to the standard

Leeds approach

- Meet internally once a week and monthly on campus
- Auditing based on expected testing
- Key stakeholders with knowledge in PCI DSS are accountable also via CICs..
- Report quarterly to CFO and CISO. Sign off by CFO.

Reducing Risk

UNIVERSITY OF LEEDS

- Only physical devices that are P2PE and compliant
- Ecommerce (Mostly SaaS, only two in scope on prem)
- Approach is to de-scope as much as possible (SaaS first, MOR)
- Trusted suppliers – Due Diligence – tools such as Black Kite
- Advancement are using 3rd parties as MOR
- Majority of tuition and accommodation payments are via Flywire – who are fully PCI compliant (ROC / AOC), PCI board member, WPM QSA, registered with the FCA

What's Next?

UNIVERSITY OF LEEDS

- Get remaining on-prem ecommerce payment channels to SaaS (Print and Sport)
- Bringing in new corporate system SAP HANA - Working in advance to implement Flywire recurring card payments API on the go live
- Continual improvement
  - We can't stand still
  - Always looking to improve security posture
  - Reduce scope further – how much further can we go?
- Technology is always updating and threat landscape changes
- One more ISA (2 IT x 2 Finance)

Summary

UNIVERSITY OF LEEDS

- Descope, Descope, Descope
- Use 3rd parties as MOR so we can focus on core activities
- Must do diligence on trusted third parties – continued monitoring not just a point in time
- Staying current

Thank you for Listening

UNIVERSITY OF LEEDS

Questions?

n.favager@leeds.ac.uk
f.baldin@leeds.ac.uk