Information security in practice: Challenges in the public sector

The Royal Academy of Engineering funded a Visiting Professorship in Practical Cybersecurity Insights at Northumbria University, 2019–2022. These slides are a slightly modified version of those delivered, intended to be available after the project has ended

Web `https://green-pike.co.uk/nvp`
Email p.brooke@northumbria.ac.uk (until it stops working. . .)
phil@green-pike.co.uk

Who am I?

An "information security professional" with experience in academia, the public sector, consultancy...
Generalist computer scientist and software engineer

What am I going to talk about?

How we usually teach you — undergraduates — about infosec
The horrors of real business requirements and limited resources

Why?

To argue why it's important for *all* IT professionals to understand infosec regardless of specialism
Illustrate possible career paths in infosec

Outline

- Introduction to information security (infosec)
- Business environments
- Public sector
- Career paths
- Where next?

What is information security about?

What comes to mind when we mention infosec?

Phil Brooke
A *Royal Academy of Engineering Visiting Professor* in Practical Cybersecurity Insights
Northumbria University

- Hackers?

- “Red-teaming” and pen-testing
- A cost on the business

The north east has suffered high-profile attacks:

- February 2020 — Redcar and Cleveland Borough Council — c. £8.6m
- University of Newcastle — September 2020
- University of Northumbria... (August 2020)

Ransomware attacks, including exfiltration of data, are increasing...

"90% of people wanting to get into #infosec want to do red team work.
10% of the most senior people are qualified to do that work.
>90% of #infosec jobs are doing compliance, architecture, policy, management, monitoring, analysis, threat intel, blue team and "other duties" work."

`https://twitter.com/TProphet/status/1172233844759678978`, last checked 20 Sep 2019

Typical introduction to security properties

A starting point: what are we trying to achieve?

Confidentiality disclosure of information and unauthorised reads (*e.g.*, medical records)

Integrity unauthorised writes or destruction (*e.g.*, modifying a payment instruction from 'pay £20' to 'pay £2000')

Availability access to information systems when it is required (*e.g.*, DoS)

Why do we care?

- Confidentiality
- Integrity
- Availability

Failure in one or more of these areas has an *impact*

That impact may be economic, cause physical harm to people or damage property, damage reputation or cause embarrassment

Contractual and regulatory requirements

There are scenarios in the public sector where this impact can include death

More motivations for studying security

Protecting customer privacy

- Important from the customer's viewpoint
- Not always from an organisation's (*cf.* Schneier's concept of 'externality')
- GDPR in 2018 put reputational harm on the executive agenda

Profits!

- Cheating in games is often security-related. If not dealt with, are players going to spend money?
- E-commerce: risk of fraud reduces customer confidence $\Rightarrow$ reduced sales

A functioning society

Vote-counting, ID cards, freedom of speech, "chilling effects"...

Classical risk assessment and treatment

Risk (probability of loss) $\times$ (value of the loss) $=$ *expected loss*

- calculate the probability (likelihood) of it occurring
- calculate the damage caused by its occurrence

Treatments:

Avoidance	eliminate, withdraw from or not become involved
Reduction	optimize, mitigate
Sharing	transfer the risk — outsource(!) or insure
Retention	accept the risks (budget for it)

Example: Health records

Confidentiality

Does it matter if *your* health records are published?
Who should see them? (Should you?)

Integrity

What harm could occur due to errors/omissions?

Availability

Does it matter if the records are off-line?

- for a minute?
- for an hour?
- for a day?
- for a week?

Business concerns

The purpose of most companies is to make money for their shareholders

GDPR and Snowden put privacy and surveillance (corporate, state) in the public eye — much larger factor than previously

"Schrems II" has created more uncertainty relating to data transfers out of Europe, with post-Brexit changes adding more (*e.g.*, adequacy decisions)

Notable points:

- Protecting assets from intruders (*e.g.*, state-sponsored theft of aircraft or CPU designs)
- Preventing disaffected employees stealing information

Business concerns

- Large businesses typically have multiple operating systems
  . . . huge amounts of software in use
  . . . many configurations and different sites
- Smaller businesses are often challenged by limited staff resource – might not even have full-time ICT support

Maintaining assets (hardware, software, information) can be a major headache!
An environment of *continual change*

Public sector

- May be large employers (NHS!), with all the challenges of huge environments
- *Much* greater transparency — Freedom of Information; media interest
- Chronically underfunded in many cases, with greater impact on back-office functions
- Inhibited by procurement regulations
- Subject to central direction, *e.g.*, "cloud first" ideology
- Statutory requirement to provide services

So very limited ability to maintain business-as-usual, let alone react to change, *e.g.*, "evergreen" Windows or DevOps

Career paths

Assertion

There is no conventional career path for infosec professionals

(but this could change. . .)

(*cf.* national Cyber Skills Strategy, CIISec, UK Cyber Security Council)

Characteristics of good infosec staff

- experience they can apply
- understanding business requirements
- communicate up/down and across the business
- know their limitations and consult other specialists

Where does this leave you?

Getting experience is hard!

Suggestions:

- Try lots of software, operating systems, languages and devices
- Read broadly — not just computing!
- Take opportunities for visits, industrial placements, *etc.*
- Don't believe everything. . .

More options

There are *many* bodies, courses, certifications and standards relating to information security

- Chartered Institute of Information Security (CIISec)
- British Computer Society (BCS)
- Certified Information Security Manager (CISM)
- Certified Ethical Hacker (CEH)
- ISO27001
- NIST Cyber Security framework
- Vendor specific, e.g., Cisco, MS, AWS

Royal Academy of Engineering

The Royal Academy of Engineering is paying for me to visit Northumbria (thank you!)

- Provide more specialist lectures
- Project ideas
- Mentoring

Final thoughts

There are lots of fun (or scary) problems to consider — much more interesting when constrained by real circumstances

- incident management, including handling major malware attacks (ransomware, data exfiltration, loss of systems)
- removable media (a perpetual nightmare of need vs. potential loss & malware)
- maintenance and evolution of systems and environments (*cf.* cloud)
- video conference (are MS Teams and Zoom the answer to everything?)
- sharing across organisational boundaries
- human resources — handling "joiners, movers and leavers"
- user education
- social interaction — Facebook/Twitter/WhatsApp/..., privacy

The end

Web	`https://green-pike.co.uk/nvp`
Email	p.brooke@northumbria.ac.uk (until it stops working. . .)
	phil@green-pike.co.uk

Phil Brooke
A *Royal Academy of Engineering Visiting Professor* in Practical Cybersecurity Insights
Northumbria University