KF4011 Systems Analysis
An infosec perspective on systems analysis

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

Why this lecture?

. . . because I spend a lot of my time dealing with projects
There are lots of problems. . .

Why me?

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

Fundamentals

What needs building by *who* for *which* end-users. . .
. . . and *who* is paying for it; *who* is responsible?

A project / system *needs* a "senior responsible owner" (SRO)

Common problems

Disinterested SRO
Changes of SRO (too common)

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

Project management

A separate specialism...
Lots of options for software/system lifecycles

- "classic" waterfall
- iterative
- agile, including XP
- PRINCE2

Regardless of method, typical steps include requirements capture, analysis, design, implementation and testing

Some form of iteration is valuable, as are prototypes to confirm the specification

Who should be consulted?

Assuming we have an engaged SRO...

- Project manager
- Finance
- Contractors, software suppliers
- ICT (!)
- **End-users**

End-users. . .

Common problem

. . . are often forgotten about in this process

- They have to use the system!
- A poor UX is a potential disaster
- Forcing a work process inconsistent with existing practices (business change management?)

GDPR

Imposes duties for

- Data protection by design
- Data Protection Impact Assessments (DPIAs)

DPIA

"You must do a DPIA for processing that is likely to result in a high risk to individuals. This includes some specified types of processing. You can use our screening checklists to help you decide when to do a DPIA.
"It is also good practice to do a DPIA for any other major project which requires the processing of personal data."

ICO, last checked 24 Jan 2020

Common problems

Still frequently misunderstood
No case law for guidance. . . yet
Infosec and data protection staff approached towards the end of the project *(cont'd)*

Email to ISO and DPO

> *"Project (name) is rolling out a new system tomorrow and the boss is preparing a message to all staff asking them to start using it from midday. Do we need to do anything for final sign-off?"*

(Polite!) reply:

> *"What is (project name)? Where is the DPIA?*
> *From your very unhappy infosec officer."*

Most projects deal with personal data!
Even if they don't, are there unaddressed ethical issues?

Changes in data protection

- Moving data around the EU *could* become more "exciting" as UK is now a "third country" (in EU terms). Depends on EU assessment of "adequacy"
  [Remark, Jul 2022: In June 2021, the EU published two adequacy decisions, see
  `https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-and-the-eu-in-detail/adequacy/`]
- Data protection agreements/contacts (DPA/DPC) and supply chain security is receiving more focus

Requirements capture

Common problem

Project requirements *evolve*

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

Authentication and SSO

Single sign-on is great from a user perspective *e.g.*, Active Directory, LDAP, SAML, Kerberos

Federated SSO becomes more challenging. "Do I trust the other organisation?"

Decommissioning

At the start of projects, I now ask project teams *how* the system will be decommissioned

Why?

Common problem

Huge costs for decommissioning — or even just impossible!

Cloud

Even more fun when combined with SSO federation...

- Where is it stored?
- Where *could* it be stored?
- How do we destroy it? (*cf.* DPA requirement for "storage limitation")

Resource limits and infrastructure

"Gucci" projects are more fun than maintenance (usually)

Common problems

Inadequate/inconsistent development, test and operational platforms

Sometimes need training platforms too

Creaky, aging or just broken existing infrastructure

Poor development processes

Too few staff to go round

Unrealistic time demands

Last: bugs and other horrors

Common problem

Some bugs are security critical

Examples:

- Leaking credentials
- Badly configured firewalls
- Mistaken assumptions
- Concurrency and race conditions

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