Archwilydd Cyffredinol Cymru
Auditor General for Wales

WALES AUDIT OFFICE
SWYDDFA ARCHWILIO CYMRU

Wales Audit Office - Cyber Security

Our audit approach

April 2018

Paul Cunningham

Wales Audit Office

Our approach to:

- risk assessment
- awareness raising
- reviewing of audited bodies arrangements for ensuring they have sound cyber security controls in place

Cyber Security

The protection of internet connected systems,

the data on them and

the services they provide

from unauthorised access, harm or misuse

More about people and management processes attitude and approach than technical IT solutions (IMHO)

Current approach

- IT risk assessment at each audited body
- Currently part way through programme:
  - National Health Service (completed)
  - Local Government (part completed)
  - Welsh Government (later in 2018)
  - Others (later in 2019)

Section 8 of risk assessment

Inadequate arrangements for IM&T and cyber security potentially places the Council's key information assets and service continuity at significant risk.

	Risk considerations:	Stop	Think	Go
8a	Are there up-to-date and agreed IM&T security policies, procedures and training programmes in place (e.g. for IT security and information confidentiality)?			
Issue			✓	
8b	Has the Council risk assessed and identified its key potential IM&T and cyber security threats, and put in place specific plans and arrangements to address them (to protect its IT and information assets)?			
Issue				✓
8c	Does the Council carry out regular IT health checks (both external and internal penetration testing) to identify potential vulnerabilities (are they PSN code of connection/ accredited to other cyber/security standards?)?			
Issue				✓
8d	Are incident plans in place to respond to a 'successful' cyber attack (to isolate, contain and manage threats, and restore systems)?			
Issue			✓	

Summary issue	Stop	Think	Go
		✓	

Stop- Definitely a risk, propose further digital work
Think- Potential risk, needs further consideration
Go- No obvious risk identified

Section 8 key questions:

- Are there up-to-date and agreed IT security policies, procedures and training programmes?
- Has the organisation risk assessed and identified its key cyber security threats, and put in place specific plans and arrangements to address them?
- Does the organisation carry out regular IT health checks, external and internal penetration testing?
- Are plans in place to respond to a 'successful' cyber attack to isolate, contain and manage threats, and restore systems?

Advantages of this approach

- Simpler and less resource intensive than traditional audit work
- Can be followed up with traditional audit work if needed
- Easy to highlight issues
- Easy to compare issues across organisations:
  - Workshops
  - More focused audit work
  - Summary reports for auditors and audited bodies

Our findings
Key Cyber Security Issues - 2003

National Health Service

- Low levels of staff training
- Unclear responsibility for data sets
- Weak information access controls

Local Government

- Inaccurate asset management/records
- Incomplete risk registers

Source:
WAO Caldicott Review and
WAO E-Govt review

Our findings
Key Cyber Security Issues - 2011

NHS

- Inconsistent disaster recovery and business continuity arrangements
- Data quality problems (major and long standing)

LG

- Political challenges of working with neighbours
- Much reduced budgets
- Missed opportunities to use IT to do more with less

Source: WAO risk assessment summaries

Our findings
Key Cyber Security issues - Today

NHS

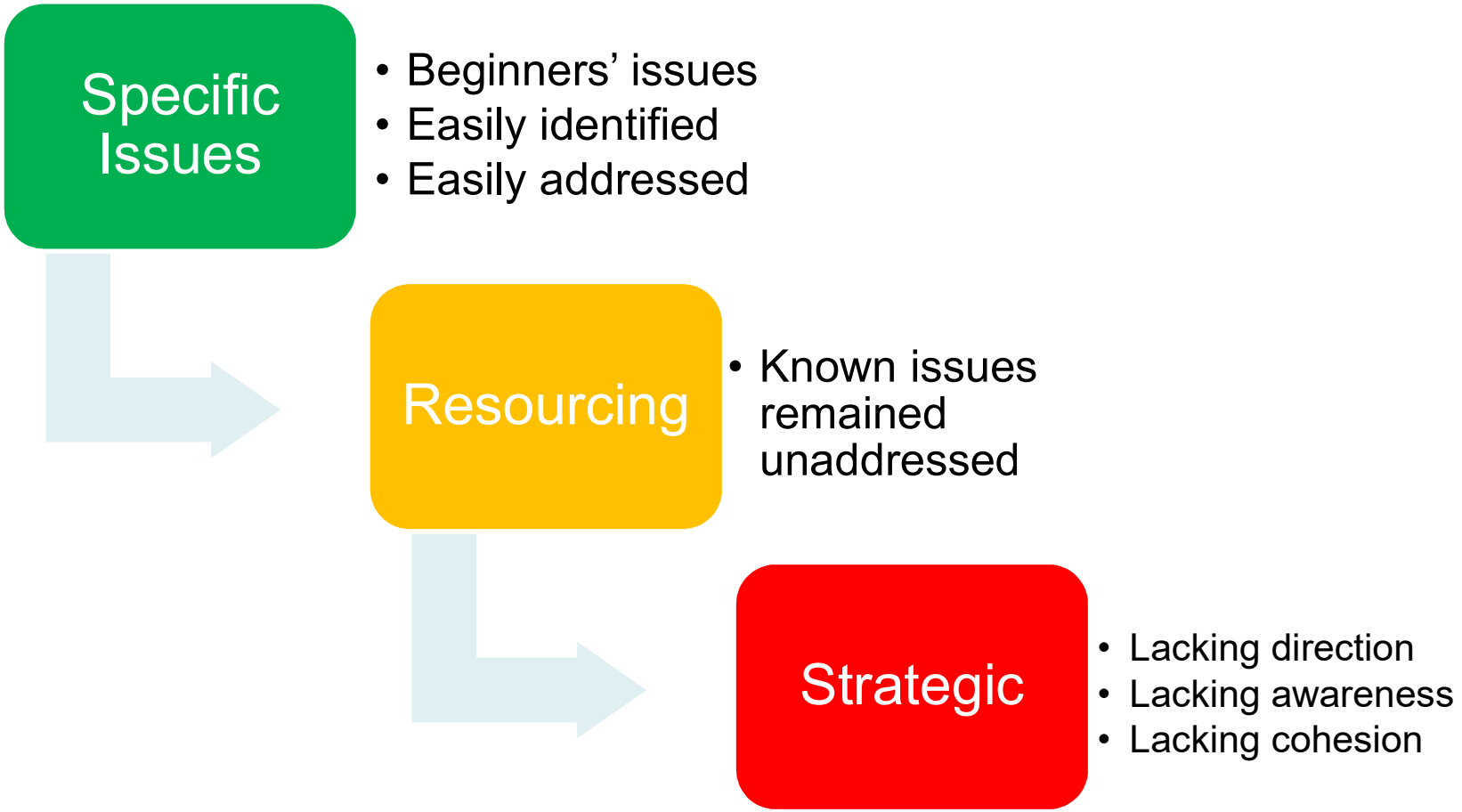
- Several organisations each striving with limited resources to address a range of common issues
  - Risk management
  - Service delivery model
  - Staffing levels

LG

- Difficulty producing or updating strategy
- Lack of awareness of attack scale

Source:
WAO risk assessment summaries

Journey of audited bodies



Past 5 years

NHS

- Constant low profile attacks (DDoS etc)
- Occasional high profile attacks (Wannacry)
- also generally Amazon Web Services, Facebook…

LG

- 98M Cyber attacks on UK local authorities in past 5 years (real figure likely much higher)

Source: Big Brother Watch 2018

How do we make a difference?

- Risk assessments highlight key issues
- May lead to reports with recommendations
- Organise events to raise awareness, for example:
  - Central Government body A&RAC Chairs
  - NHS IT Security Forum
  - NHS IT Risk Summary report

- All positively received

Case Study – Audit and Risk Committee Chairs

In 2017 we invited Audit Committee chairs and key officers to attend an awareness raising workshop:

- Overview of current cyber risks
- The role of the audit committees in addressing these
- Recent cyber incidents
- Potential models for addressing cyber security
- Demonstrated how easy it is to breach security of mobile phones

- Very positive feedback, particularly on the last point!

Moving forward

- Some exciting work in the pipeline on data analytics
- Next version of ISAs (from 2020 onwards)
- Revolutionise approach to audit
- More to report on next time.

Thank you

Paul Cunningham

paul.cunningham@audit.wales

+44 777 1505 802