3 Lines of Defence

Understanding the different roles in protecting our data and assets

Jethro Perkins

Information Security Manager

LSE

Overview

- Problem landscape
- What we've got (and how that works)
- The 3 lines model
  - Operations
    - Embed as BAU
  - Internal governance (me)
    - Minimum Standards
    - Risk appetite
    - Policy
    - User awareness
  - Internal audit
    - Independent verification

Problem landscape

- It should become clear later why I'm going through this…
- In no particular order…
- Malware
  - Drive-by
  - Delivery via phishing
  - Admin risks
  - Unpatched browsers / flash etc.
- Hacking
  - Bad config / lack of hardening
  - Lax firewall rules
  - Patching / EOL OS, applications

Problem landscape II

- Phishing
  - Any old account
  - Political (dissidents/hacktivism/integrity)
  - Whaling (usually financial)
  - Deep attack
    - IP theft
    - Staging post
    - Political (again)
- BYOD / Remote working
  - Ancient OS
  - No AV
  - Trivial login
  - BitTorrent / Freeware
  - “Bring your own malware”

Problem landscape III

- Boundaries
  - Which boundary?
  - External firewall
  - DMZ
  - Internal zone-DMZ
  - Application boundaries
  - Private Cloud-Internal
  - Public Cloud-Internal
  - Private Cloud-Public Cloud
  - Site-Site

Problem landscape IV

- Cloud
  - Ad hoc commissioning
  - Casual use (Google Docs, Dropbox)
  - Where’s my data…?
  - Contracts?
  - Data flows?
  - Any service assessment?
  - Any IaaS? How’s that configured?
- Network
  - Hey – what’s going on? Visibility
  - Bad traffic
  - Tricky architectures – capacity, speed, zoning, availability, accessibility, wireless

Problem landscape V (nearly there!)

- Patching / Maintenance
  - Hardware
  - OS
  - Applications
  - Software
  - Things (that cannot be patched)
- User education
  - Phishing again
  - Accidental leak
  - Personal devices
  - Unrealistic expectations
  - “Consumer grade” understanding and approach

Problem landscape VI

- Physical
  - Boundaries (workplaces, offices)
  - Multiple sites
  - Visitors / Staff / Others
  - Access to:
    - Computers
    - Wireless
    - Network sockets
    - “The network”
  - Comms Rooms
  - Datacentres

Regulatory and Contractual requirements

- Regulatory
  - GDPR
    - Anyone not aware of what that entails?
  - PCI DSS
    - If you're taking card payments
  - Various Terrorism Acts
  - RIPA and the IPA
- Contractual (often connected to research data)
  - ISO27001
  - Cyber essentials
  - Data Location (e.g. within EEA)
  - Breach reporting (may be <72hrs)
  - Access Controls
  - Risk assessments
  - User awareness

What we've got

- We tend to boil all these problems together…
- …and then lump them under the term "information security"
- We treat it as a separate function, or maybe part of someone's function
- (always radically underfunded)
- (and often, weirdly, as part of *infrastructure*)
- That is supposed to understand and handle all of these problems
- Despite often having no real remit to do so
- …and being overwhelmed by simultaneously handling e.g. the firewall *and* information security policy

A better split: the ‘3 lines of defence’ model

Three lines of defence			
Lines	Role of Director IMT	Role of all Business Units	Role of the Security Leader
First Line *“The Operation”*	Risk Management of the Operation Apply Internal Controls Monitoring and reporting Incident Management Business Case for Investment in Security Technology	Risk Management of their part of the Operation including technology supporting their function Apply Internal Controls Monitoring and reporting Incident Management	Review threat external landscape and vectors Support incident management with expert investigation
Second Line *“Risk & Compliance”*	Provide organisational context to Security Leader Support the recommendations of Security Leader Sponsor the Security Leader Advocate and guide other C-Level execs on their role and the standards they maintain	Feedback and contribute to policy setting Set risk appetite Take part in and sponsor awareness and education initiatives	Oversee and Challenge cyber security response and risk management Provide guidance and direction Develop policy and frameworks (based on context) Awareness campaigns and education
Third Line *“Audit”*	Provide clear, actionable management response to audit reports Guide other business units on the importance and value of audit reports	Provide clear, actionable management response to audit reports	Review 1st and 2nd Lines for compliance with policy Provide an independent perspective Challenge Objective and offer assurance to executive leadership

First line: Ops

- Implement policy and minimum standards
- As set by second line
- And informed by risk appetite
  - Contractual consideration if using Cloud suppliers
  - Question them on their provision
- Manage incidents
- Monitor and report up to second line
- Supported by
  - Information Security lead amending policy and control standards to respond to threat landscape
  - IT head making the case for appropriate security provision up to C-Level
  - C-Level understanding risk landscape and setting risk acceptance levels

Second line: risk and compliance

- That’s me!
- Policy, frameworks and standards
- Awareness and education
- Responsibility for cyber response
- Set standards for Ops,
- review existing provision,
- challenge where it doesn’t seem to meet the risk
  - OR, if it’s too risk averse
  - (a large, but unacknowledged problem)

Second line II

- Supported by…
- Head of IT
  - Provides the organisation context: “what the business needs”
  - Advocate and sponsor for cyber security measures
  - Broker requirement with C-level
- Ops
  - Feedback
  - Sponsorship of awareness programmes

Third line: Audit

- Review the actions of 1st line (the doing)…
- …and second line (policy, risk management, understanding of threat)
- Auditors are your friends!
- They are powerful advocates for change
- BUT you need the right structures around audit review
  - E.g. strong, independent audit committee
  - Independent audit function with the capacity for deep dives if required
  - Good working relationship with second line
  - Open approach from Ops (not hiding things under the carpet)
  - Constructive, problem-solving culture…
  - …which means breaking down silos

Getting the most value out of audits

- An audit is only as useful as your response to it
- The management response needs to be:
  - A coherent strategic narrative
  - Joined up (not a piecemeal, siloed approach)
  - Cascading from risk, to policy, to Ops
  - Driven by the head of IT
  - Achievable by Ops
  - Supported by C-level
  - Backed by resources

“Are we there yet”?

- Not quite!
- Better embedding of risk at executive, management, project and operational level
- Operations need to be broken into service lines
- Clearer transmission of policy and minimum standards
- Information security is currently partly an operational unit
  - …with expectations of functional responsibility
  - Conflict of interest!
- Presentation of management responses to audit have encouraged a piecemeal approach
  - Seeing every action as a distinct problem, rather than a continuum
- Audit reports tend not to be as sensitive to organisational context and risk appetite as they should be
  - i.e. a ‘cookie cutter’ approach to audit reports, with much meaning QA’d out of them

Any questions?