Equipping security teams to deal with changing technology

Piers Wilson

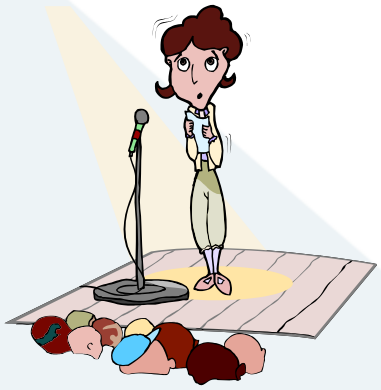
Director – IISP
Head of Product Management – Tier-3

The Institute of Information Security Professionals

Tier-3

HUNTSMAN®

What I Intend to Cover …



- Dealing with emerging technologies
  - Mobile, Cloud, Virtualisation
- Changing security exposures
  - Spear phishing, Trojans/APTs, Social media
- The role of security technologists
- Compliance and Governance – A visibility and communication problem
- Professionalisation, business focus and service maturity

Dealing with emerging technologies

- The technology landscape is changing all the time – this affects how we protect our information and secure our systems
- Examples:
  - **Virtualisation** changed where systems are located, forensics processes, how patching needs to work, network access control and filtering
  - **Smartphones** and apps completely changed the remote user/client/browser environment and interaction model
  - **Cloud** service provision meant that we moved away from technology we could control, to services that we consumed

Security teams – and the policies, standards, toolsets and operational processes - have had to, or are having to, evolve to cope with this

Changing security exposures

- The risk has changed, as has the visibility
- More awareness outside “the security function”
  - Higher levels of management
  - The press
  - Regulators
  - Public
- If “Cyber security” has achieved one thing, it is that it has raised the profile
  - Examples:
    - “Awareness-resistant” Spear phishing attacks
    - APTs and Trojans that circumvent “standard” controls,
    - Social media has become universally accessible (in or out of work)

So security teams are under increased scrutiny and faced with a more sophisticated adversary

Cyber risk: **Technology** OR **People**?

	Thieves	Organised crime		
Customers	Mobile	Internet	Hackers	
	Carriers	Network	Gov’ts	
	Developers	Apps	Security teams	
	Admins	Systems	Data	Owners
	3rd Parties	Cloud	Other Customers	
		Audit/Compliance		

The role of security technologists

- Business Owners make **good or bad** decisions
- Users behave **securely or insecurely**
- Security managers make **sound or flawed** risk judgements
- Developers create **secure or exploitable** code
- Administrators run **tight or loose** environments
- Security operators **spot or miss** potential incidents
- Companies hire **smart or cheap** security teams
- Investigators **are or aren't** able to diagnose / resolve incidents
- People **do or don't** have the right tools

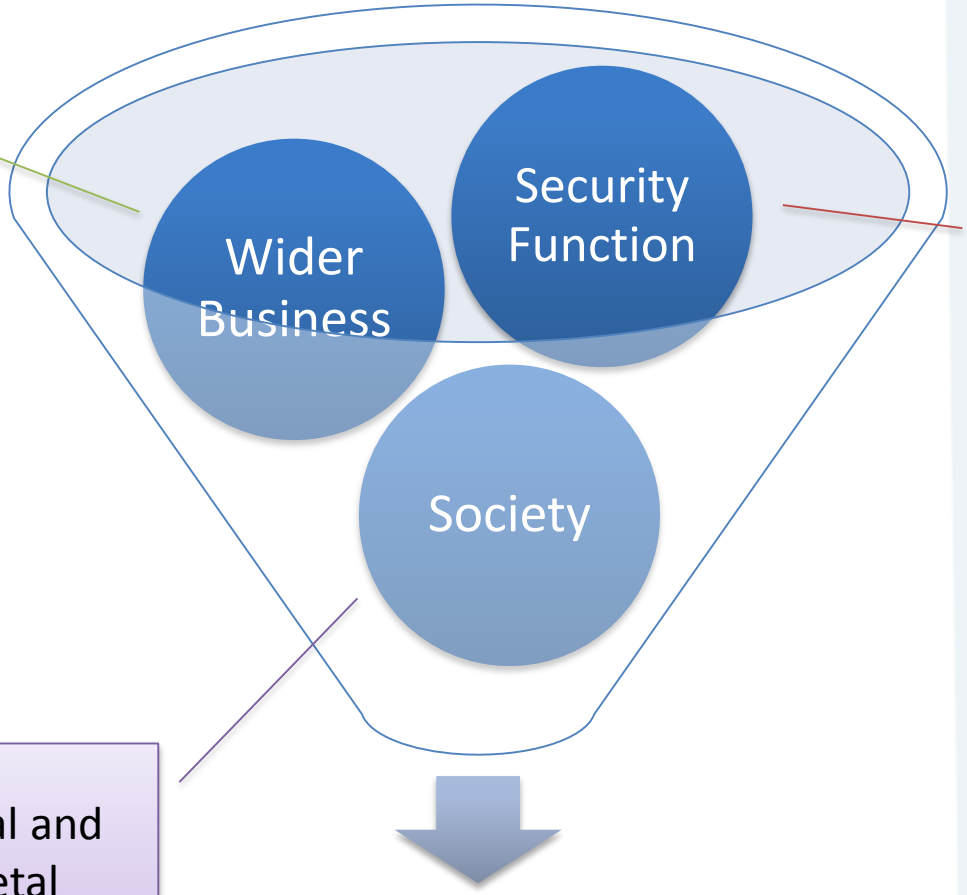
We are all security technologists

The quality of security technologists

Better risk ownership and understanding

Recognition of IT and non-IT aspects

Strategic integration



Assessable skills

Verified experience

Availability of training

Business experience

Career paths

More transparency, visibility and communication

Cultural and societal contribution

Reduced risk

Changing technology

Remember the disruptive technologies

- Virtualisation
- Cloud
- Mobility
- Collaboration
- …

Remember the more complex threat landscape

- Cyber threats
- Spear phishing
- APT
- Social media
- …

It means being more technologically agile – dealing with both a change of pace and a loss of direct control

It means having good, skilled, professional people; but also equipping them with tools that utilise the skills, rather than bogging them down in operational handle turning

Compliance and Governance
A visibility and communication problem

2000's problem:

"Why can't we get Security on the Board's agenda?"

2010's problem:

"Help! The Board want to understand and get involved in our cyber security defence"

Well, we got our wish...

Now we need to present security business cases, status reports, risk management and issues in a language that non-security people will understand

Compliance and Governance
A visibility and communication problem

- Business cases are more than a comparison between a hypothetical impact scenario and a solution cost
  - We need to help business/service owners understand risks better
- Being “incident free for 341 days” is of limited value where **detection** is as difficult as **defence**
- Security processes have outputs; we must be better at measuring these in a way that makes the “business benefits” evident
  - Policy definition and publication
  - Security monitoring operations
  - Incident handling
  - Secure design and development
- Patch deployments/Penetration test results are not good statistics to use for this

Professionalisation, business focus and service maturity – IISP's role

- IISP aims to improve standards, recognition & professionalism
  - We live in the same complex business and technical environment
- Membership based on reportable experience and interview
  - a jury of your peers
- Broad spectrum of skills – technical, business, soft
- Provides a career structure and a level of trust in security professionals and teams

IISP Goals

- **IISP Aims to assess, develop, foster and improve the overall security professional**

Outcomes for businesses:

- Effective security control environments based on reasoned judgement rather than news stories and sales hyperbole
- Organisations can understand the advice they are being given and trust it
- Processes designed around controls, real threats and business risks to deliver an efficient service to the business and users
- Visibility of control status, process outcomes, successes and failures
- Well chosen tool sets that support processes and support this – rather than having been blindly bought from salesmen

Thank You and Questions

Please contact the IISP/me with questions

- IISP Office
  - office@iisp.org
  - +44 (0) 2033 840 399
  - www.iisp.org
  - @IISPmedia
- Piers Wilson
  - piers.wilson@tier-3.com
  - 07800 508517
  - @Tier3Huntsman