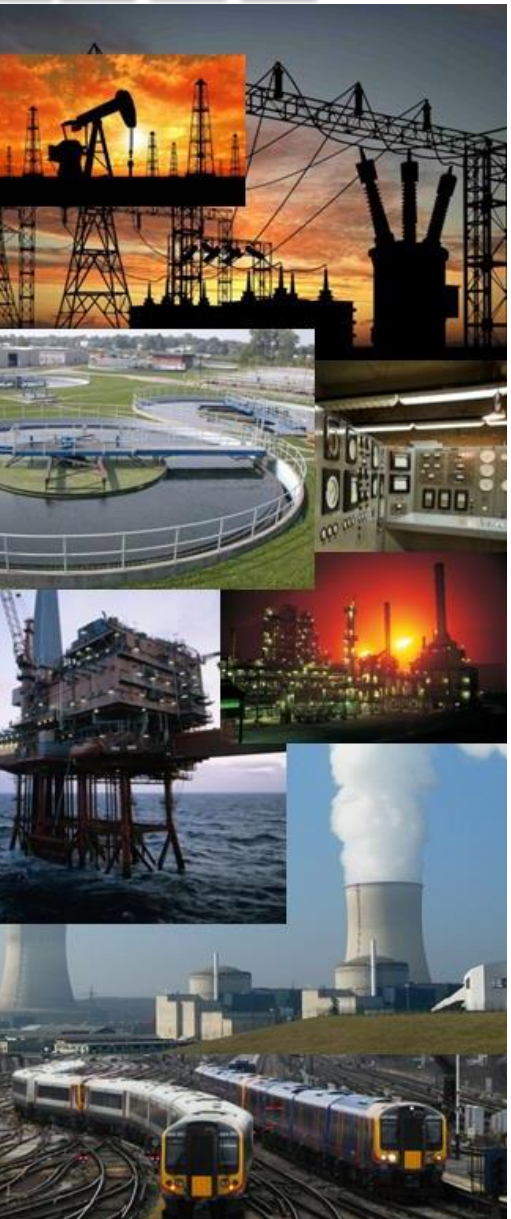


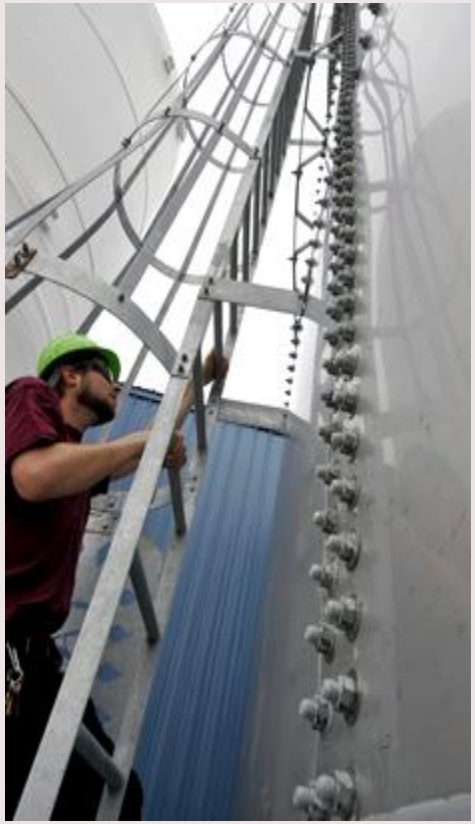
ICS Security Skills and Certifications

Certification Challenges

What is the Problem?

- **Individuals and Organisations struggle** to identify appropriate certifications and skills that demonstrate their ability to effectively mitigate ICS security-related risk

- **A lot of Certifications are targeted** at demonstrating and documenting compliance**.**

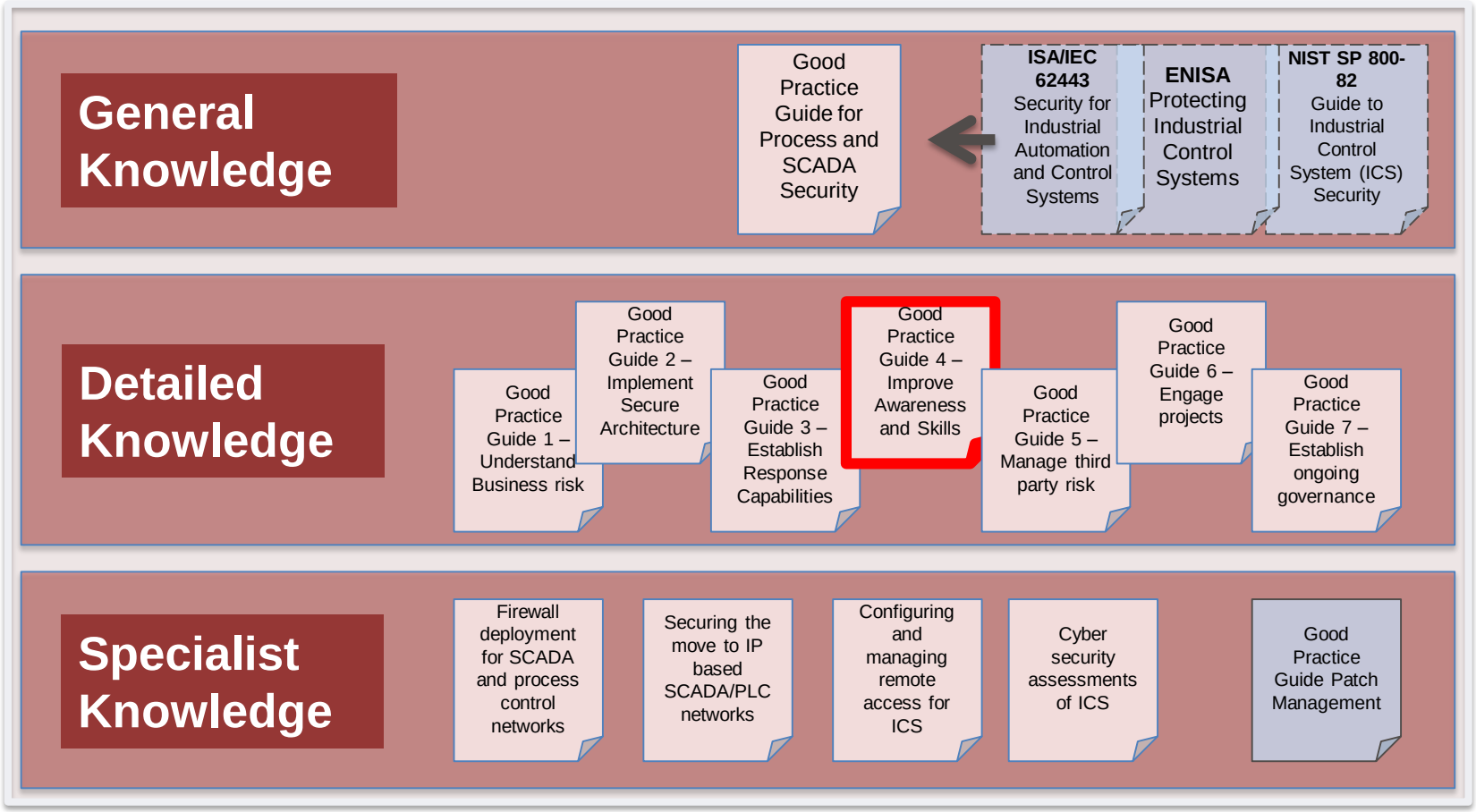


What Does the Business Want?

- **A Workforce capable of** identifying anomalous behaviour that may indicate when their ICS environment is under attack

- **Teams who are able to respond** to an identified incident in a timely and efficient way in order to best protect the business

CPNI Good Practice Framework



Many Names For the Same Thing

What is an ICS?

According to the ISA/IEC 62443 glossary, an ICS (or IACS) can be defined as:

*'A collection of **personnel**, hardware, software and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation'*

Why Are We Bothering?

Harwood Security and Training Consultancy

Trends

Business Changes Can Introduce Security Risk

- Increased **outsourcing**
- Social Media and **Gen Y** entering workforce
- **Changing skill set** demands not being met by Academia
- Strong safety but **weak security**

+

Technologies

Security Through Obscurity No Longer An Option

- **Legacy** equipment
- Using more **IT technologies** without including IT security
- Bridging **IP connectivity**
- Lack of formal **patching**
- Limited **security monitoring**

+

Threats

Number of Threats & Sophistication Increasing

- Use of **Cyber as a Weapon**
- Nation states, espionage and **hacktivists**
- Untrained **contractors and staff** in security
- **Viruses & malware** sophistication
- Accidents and Human **errors**

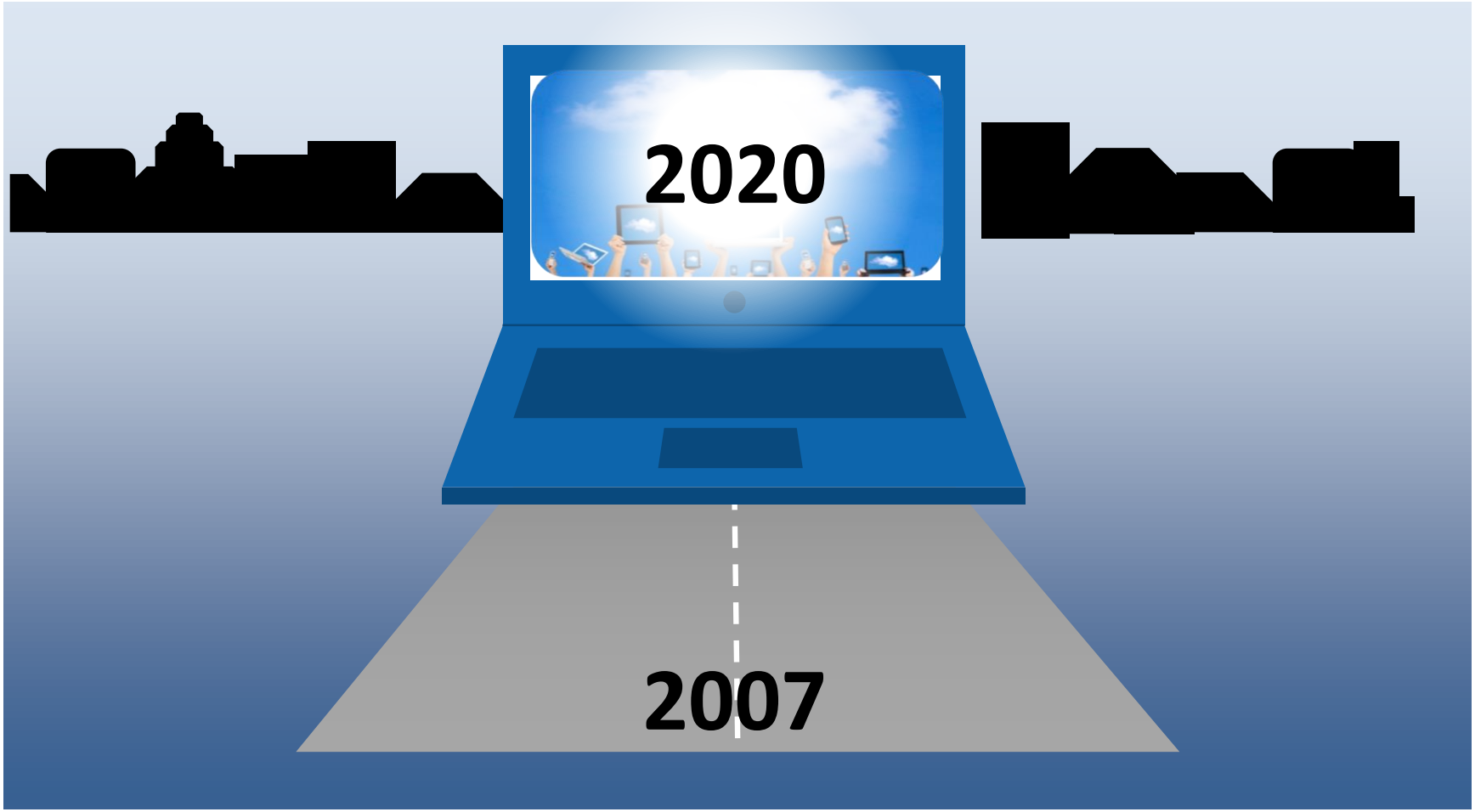
Rising

Risk

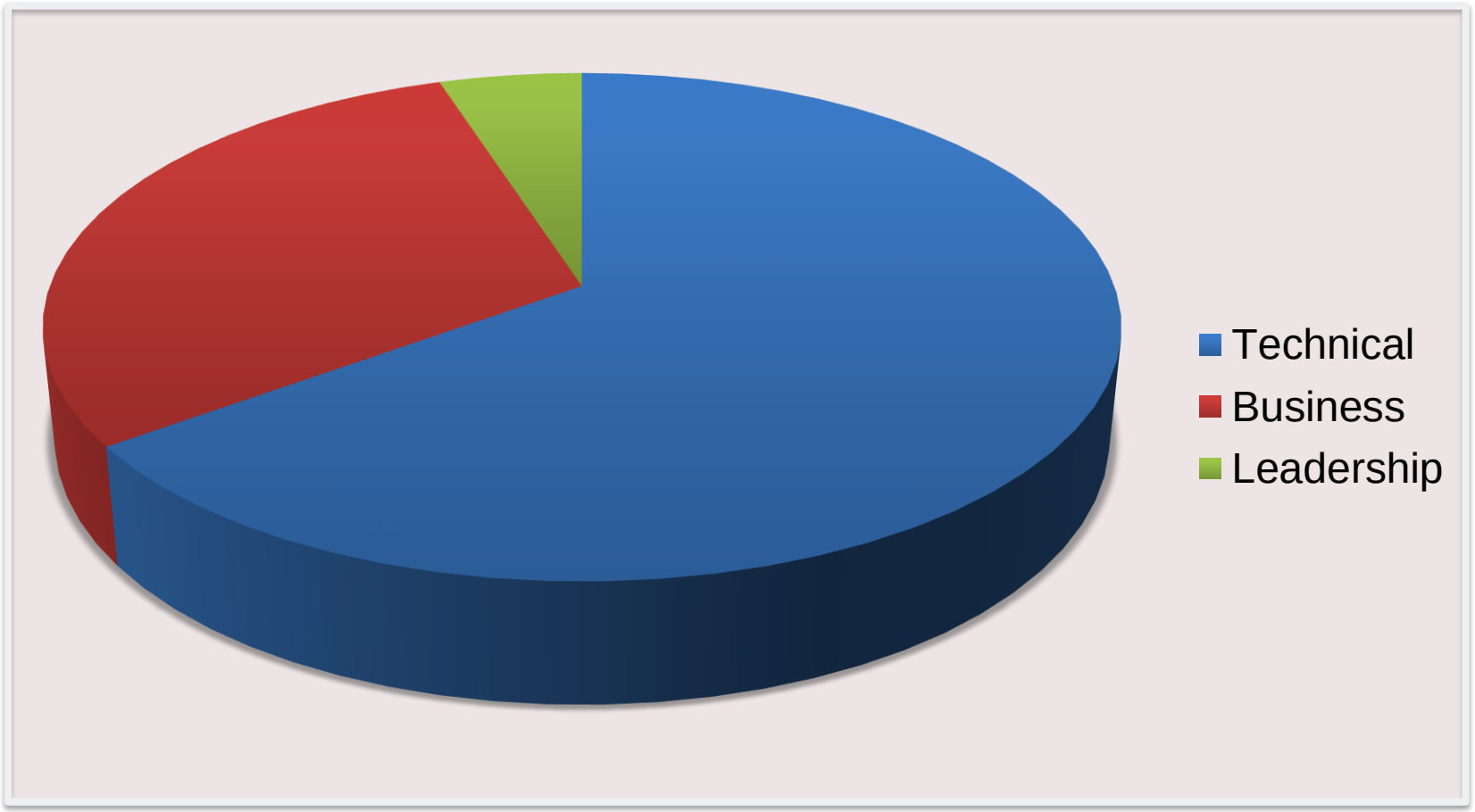
Risk

Failures Can be Catastrophic

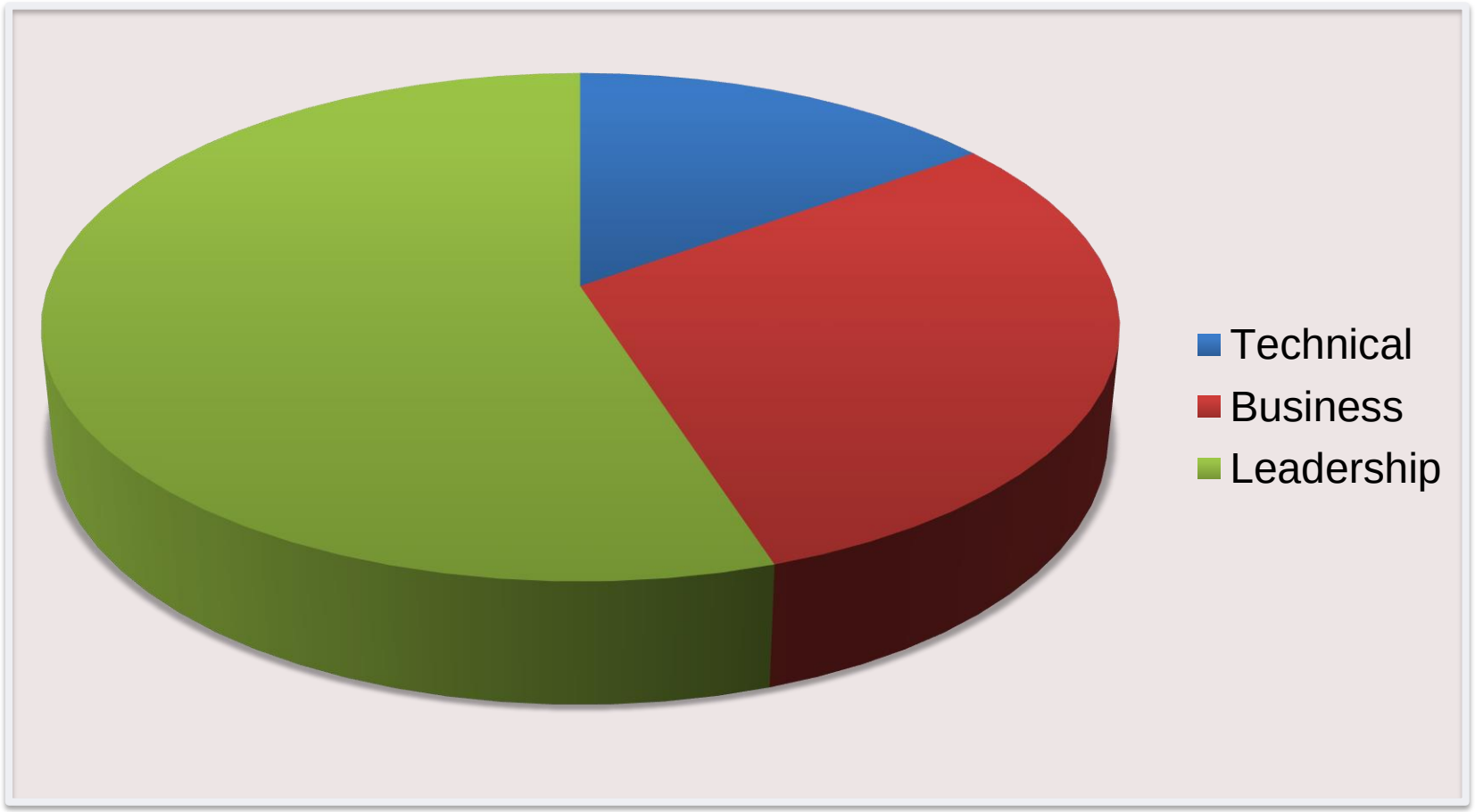
Skills Requirement



Skills Mix at Beginning of Career

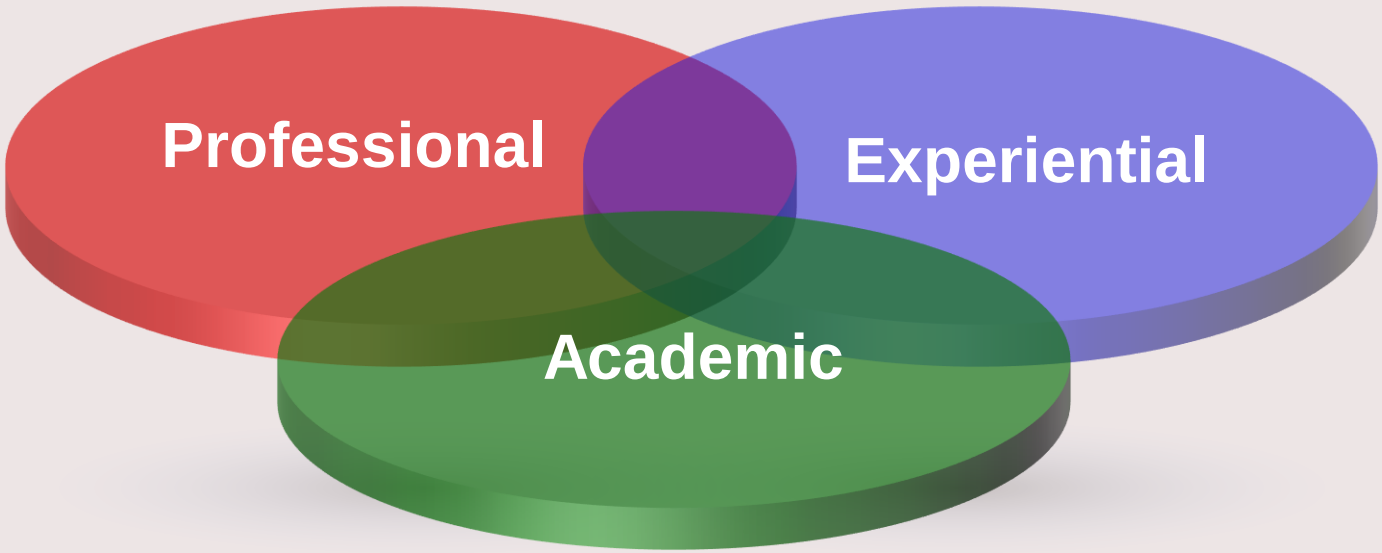


Skills Mix When in Senior Position



Relevant Skills

There is a need to drive cultural and behavioural change as incorrect behaviours can undermine cyber security defences.
Three main areas to consider are:



Why Are We Bothering?

Harwood Security and Training Consultancy

Trends

Business Changes Can Introduce Security Risk

- Increased **outsourcing**
- Social Media and **Gen Y** entering workforce
- **Changing skill set** demands not being met by Academia
- Strong safety but **weak security**

+

Technologies

Security Through Obscurity No Longer An Option

- **Legacy** equipment
- Using more **IT technologies** without including IT security
- Bridging **IP connectivity**
- Lack of formal **patching**
- Limited **security monitoring**

+

Threats

Number of Threats & Sophistication Increasing

- Use of **Cyber as a Weapon**
- Nation states, espionage and **hacktivists**
- Untrained **contractors and staff** in security
- **Viruses & malware** sophistication
- Accidents and Human **errors**

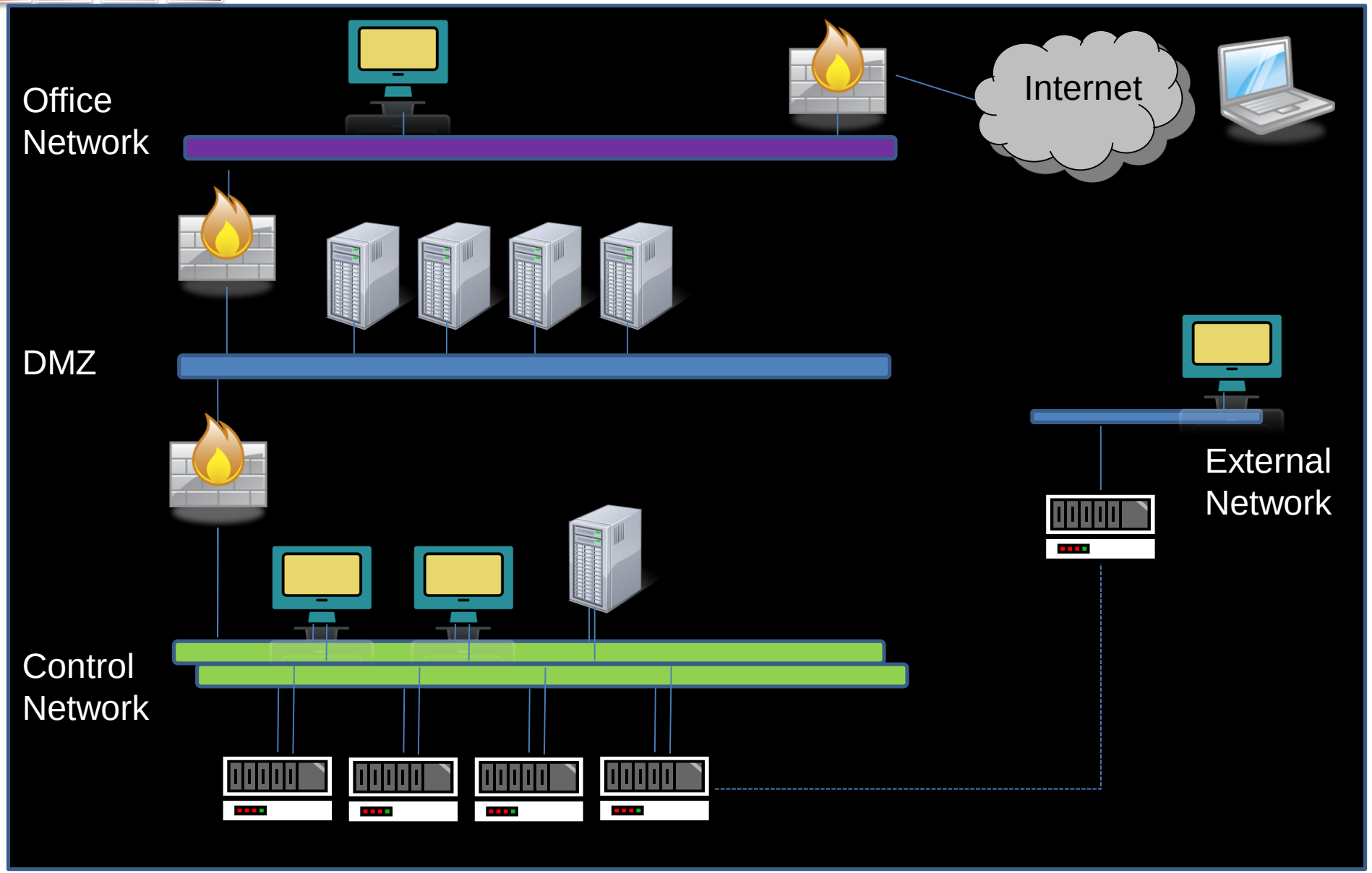
Rising

Risk

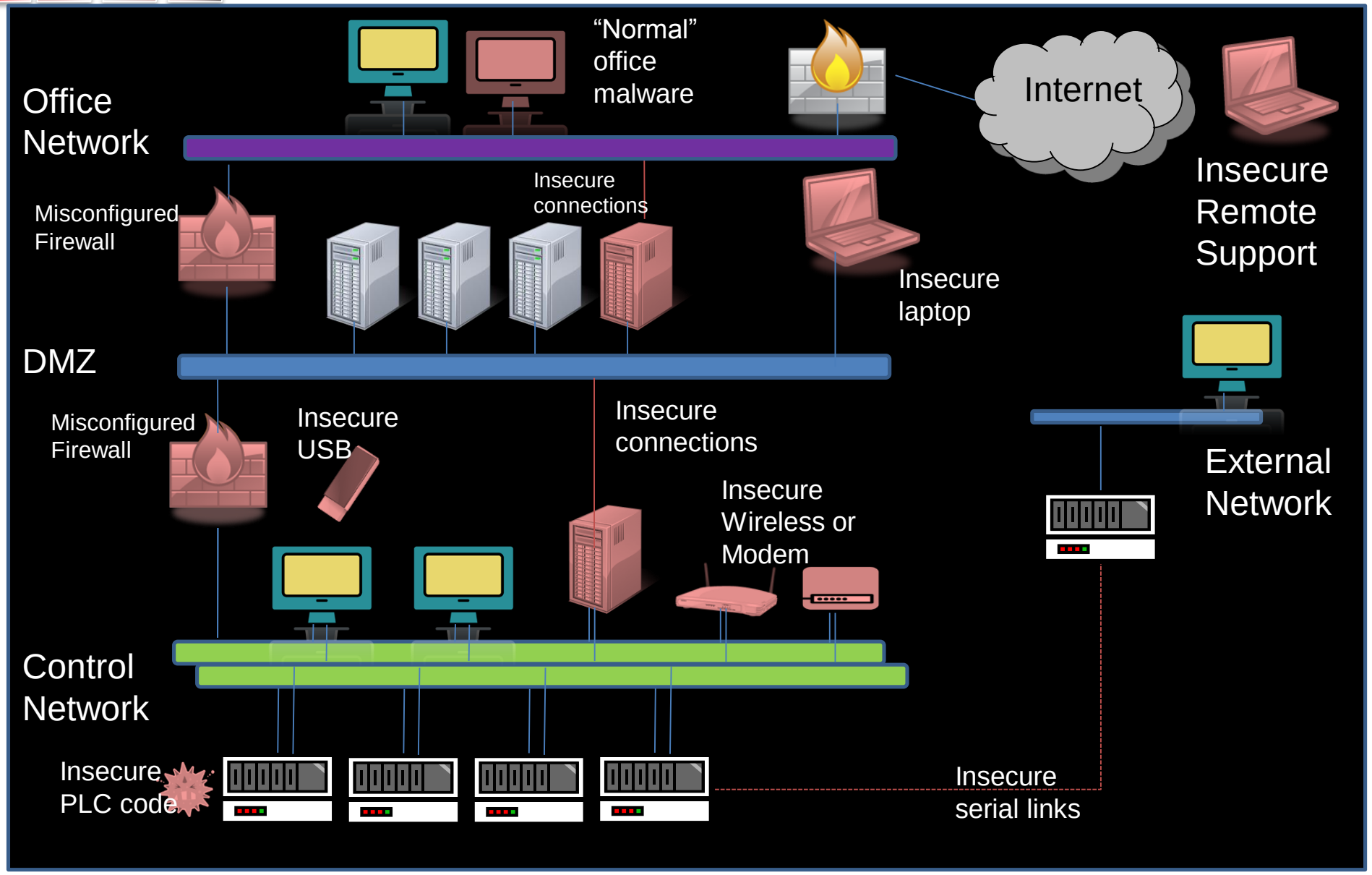
Risk

Failures Can be Catastrophic

3-Tier Architecture



IT and ICS Vulnerabilities



Why Are We Bothering?

Harwood Security and Training Consultancy

Trends

Business Changes Can Introduce Security Risk

- Increased **outsourcing**
- Social Media and **Gen Y** entering workforce
- **Changing skill set** demands not being met by Academia
- Strong safety but **weak security**

+

Technologies

Security Through Obscurity No Longer An Option

- **Legacy** equipment
- Using more **IT technologies** without including IT security
- Bridging **IP connectivity**
- Lack of formal **patching**
- Limited **security monitoring**

+

Threats

Number of Threats & Sophistication Increasing

- Use of **Cyber as a Weapon**
- Nation states, espionage and **hacktivists**
- Untrained **contractors and staff** in security
- **Viruses & malware** sophistication
- Accidents and Human **errors**

Rising

Risk

Risk

Failures Can be Catastrophic

The Three Weaknesses

There are **three main avenues of weakness** that an attacker can exploit (although most modern attacks exploit a combination of all three) i.e.

- **People** (social engineering, default/weak passwords, etc.)
- **Process** (poor Joiners/Movers/Leavers (JML) process, Access control, etc.)
- **Technology** (out of date patching, weak architecture, etc.)

The 2012 Verizon DBIR illustrated that **97%** of breaches analysed could have been prevented by either simple or intermediate controls.

Why Are We Bothering?

Harwood Security and Training Consultancy

Trends

Business Changes Can Introduce Security Risk

- Increased **outsourcing**
- Social Media and **Gen Y** entering workforce
- **Changing skill set** demands not being met by Academia
- Strong safety but **weak security**

+

Technologies

Security Through Obscurity No Longer An Option

- **Legacy** equipment
- Using more **IT technologies** without including IT security
- Bridging **IP connectivity**
- Lack of formal **patching**
- Limited **security monitoring**

+

Threats

Number of Threats & Sophistication Increasing

- Use of **Cyber as a Weapon**
- Nation states, espionage and **hacktivists**
- Untrained **contractors and staff** in security
- **Viruses & malware** sophistication
- Accidents and Human **errors**

Rising

Risk

Risk

Failures Can be Catastrophic

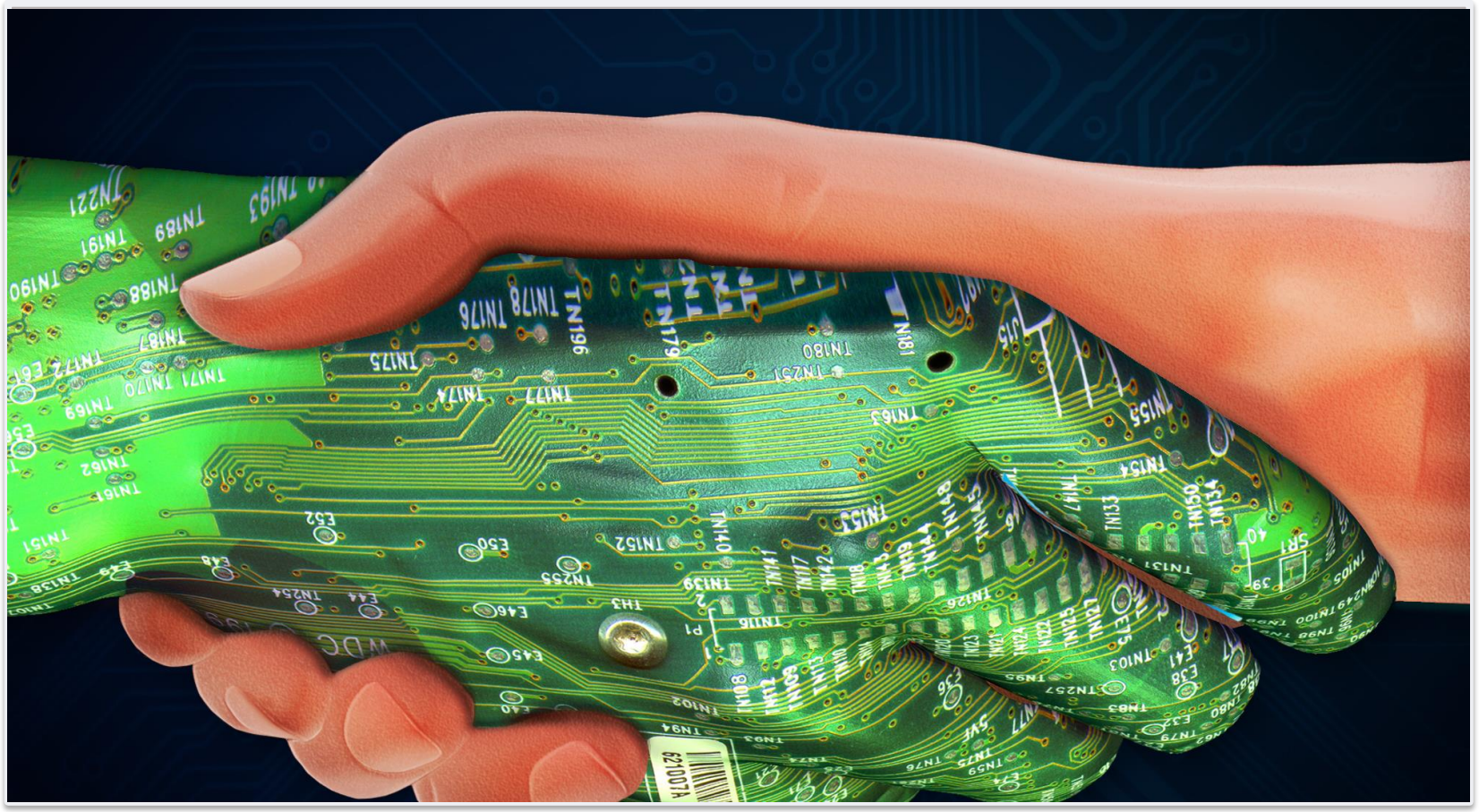
Question Writing

WRITE THE QUESTION AND ANSWER

NOW WRITE THREE DETRACTORS

LASTLY, WRITE THE EXPLANATION

And The Answer Is…



Summary

The aim is not to make staff Security Professionals but to make them professionally secure

"In times of change, Performers inherit the earth… while the learned find themselves beautifully equipped to work in a world that no longer exists."

Eric Hofer, 1932

Are there any questions?

Thank You!

Tim Harwood
Managing Director, HS and TC
tim_harwood@hsandtc.com