Making the Leap from Training to Culture Change

Believe - Learn - Achieve

Who Am I? – Tim Harwood

Founder and CEO – Siker Limited

Certified Security trainer/author with over 40 years security experience

Full member and former member of the Board of Directors of the Institute of Information Security Professionals (IISP)

Security Capability Lead at BP for over 8 years

Certified Security Leader and Fellow of the Chartered Management Institute (FCMI)

Member of the GICSP Steering Committee, including setting GICSP exam questions

Developed skills and competencies framework for use in process control

SIKER

Managing Cyber Risks in OT

- Cyber Skills Poverty
- Threats and Vulnerability
- Organisational inter-dependencies
- Technical Complexity
- Digital Transformation
- New, cyber-focused regulations

SIKER

Practical Challenges for Cyber Transformation

(lessons learned from safety critical industry sectors)

- Understanding and quantifying risk
- Leadership and Governance
- Culture – Integration of cyber into the business
- Technical Capability development
- Basic Cyber Hygiene
- Cyber Resilience and Protection

SIKER

A Governance Framework

- Framework established to ensure risks are identified and dealt with in a consistent way
- Risks are set against business requirements
- Framework will set out
  - Clear roles and responsibilities
  - Up to date strategy
  - Provision of assurance

SIKER

Culture and Behavioural Change

- Enforces and supports innovation
- Historically resists standardisation
- Incorrect behaviour undermines security management
- Derived from Senior Leadership with input from business
- Benefits to business fully identified and understood

SIKER

What does good Culture look like?

- Staff know how to report any concerns and, more importantly, feel empowered to do so
- Staff don’t fear reprisals if they do
- Staff feel able to question anything and their input helps to shape security policy
- Staff understand the importance of cyber security and what it means to the organisation

SIKER

Do you encourage it?

- Properly resourced awareness
- Staff input to policy and system design
- Sharing of security metrics (make sure they pass the ‘So What’ test)
- Senior Leadership support
- Train those who need it – it’s a team sport so break the silo’s
- Security is not the mission (but a vital part of it)
- Cyber is a trajectory – not an end-state
- Assurance – authoritative, credible, independent assessment

SIKER

Secure the People

- Screened for role
- Background checks or vetting?
- Trained – check the certs!
- Role specific certifications not generic – GICSP versus CISSP

Look for the Anomaly

- Presence of the Abnormal
- Absence of the Normal

SIKER

Generic Levels

Knowledge Specifications

There are four levels defined for each skill or knowledge area – an Awareness tier plus three Competence tiers.

Awareness:

Has a basic perception of a skill or knowledge requirement and drivers setting the demand

Level 1:

Has acquired and can demonstrate basic knowledge associated with the skill, e.g. through training or self-tuition. Has a basic understanding of the knowledge requirement.

Level 2:

Understands the skill and applies it to basic tasks with some supervision. Has a demonstrated understanding of the knowledge item and can apply it independently to practical situations.

Level 3:

Understands!!

Within each tier there may be several skill requirement statements. During any competence assessment of an individual, the intention is that each statement is tested. The statement may be identified as not relevant to the role the individual holds. The tiers are progressive however, so failure to meet all the requirements of one tier may make it harder to evidence support for skills at a higher tier when progressing.

SIKER

Knowledge Level Descriptors

B1 - Control of Work	**Defines, implements or uses risk identification methods and applies risk-reduction controls to ensure work to OT systems is executed with as little risk to OT system cyber-security as reasonably possible.**	**Awareness**	**Can explain the need to consider the content of work to OT Systems and the methods of delivery to ensure cyber-security of OT systems always remains effective.**
		Level 1	Prepares for and delivers work to OT systems in accordance with process. Can explain to third-party engineers how and why the organisation's processes are structured as they are, and what actions are required to ensure security is always maintained. Can oversee work by third-party engineers and ensure that no activities are out with those approved within the Control of Work system in use.
		Level 2	Can assess the controls proposed for delivery of work to live OT systems, and technical approve on behalf of offshore management on request. Can recommend additional controls where needed Can recommend changes to standard controls, in order to improve the Control of Work system.
		Level 3	Can provide assurance that assessment of work and required risk controls is suitable, including check of supplementary controls recommended by others. Can technically approve recommendations to change the Control of Work standard controls as SME for the business.

SIKER

Example – Senior Maintenance Technician

Governance	
A1 - Governance	1
A2 - Policy	1
A3 - Standards (External)	1
A4 - Standards (Internal)	1
A5 - Process and Procedures	1
A6 - Security Strategy	1
A7 - Legal and Regulatory	2
A8 - Threat Intelligence Sourcing, Assessment and Management	1
A9 - Vulnerability Intelligence, Assessment and Management	1
A10 - Risk Assessment	1
A11 - Documenting the System under Control	2
Security Delivery	
B1 - Control of Work	2
B2 - Security Behaviours Improvement	2
B3 - Third Party Management	1
B4 - Incident Response	1
B5 - Business Continuity planning	1
B6 - Cyber Security Impacts to Functional Safety	1
Networking Skills	
C1 - Operational Technology Security Architecture	1
C2 - Operational Technology Network Architecture	1
C3 - Operational Technology Systems Inter-Networking	1
C4 - Operational Technology Local Networking	1
C5 - Network Security Design	1
Endpoint Security	
D1 - Endpoint Hardware	1
D2 - Anti-virus/Anti-Malware application management	1
D3 - Endpoint Hardening	1
D4 - Patching and Patch Management	1

SIKER

Example - The Siker Industrial Control Security Curriculum

Awareness/Foundational
Skill Level 1/2

ICS110
ICS Managers Security

ICS201
Networking Essentials for ICS staff

ICS202
Incident Response Fundamentals

ICS203
ICS Practitioners Security

ICS204
ICS Basics for IT staff

Core Skills
Skill Level 2/3

ICS301
Wireless Security for ICS

ICS305
ICS Pen Testing ****NEW****

ACT201
Introduction to OSINT

ACT310
Penetration Testing Fundamentals

ISS201
Python Basics ****NEW****

Specialised
Skill Level 3/4

ICS405
Securing ICS: Becoming a Global Industrial Cyber Security Professional

ACT401
Incident Handling: Becoming a Certified Incident Handler

Trusted by…

https://sikercyber.com/cyber-learning/

Are there any questions?

Thank you
Tim Harwood
tim_harwood@sikercyber.com

SIKER