www.pwc.com

How Aviation Security can benefit from policies, standards and best practices in other domains.

5 November 2014

marc.sel@be.pwc.com

Agenda

1. Aviation Security
2. Best Practices in other domains
3. Best of both worlds

Aviation Security

1

Aviation Security

What

ICAO: « *Safeguarding civil aviation against acts of unlawful interference* »

Viewpoints:

- People (trained and licensed aviation professionals – aircrew, airtraffic, meteorologic, airport, …)
- Process (multiple supply chains – aircraft, airport, control, maintenance)
- Technology

Who are the actors?

Which levels should be involved?

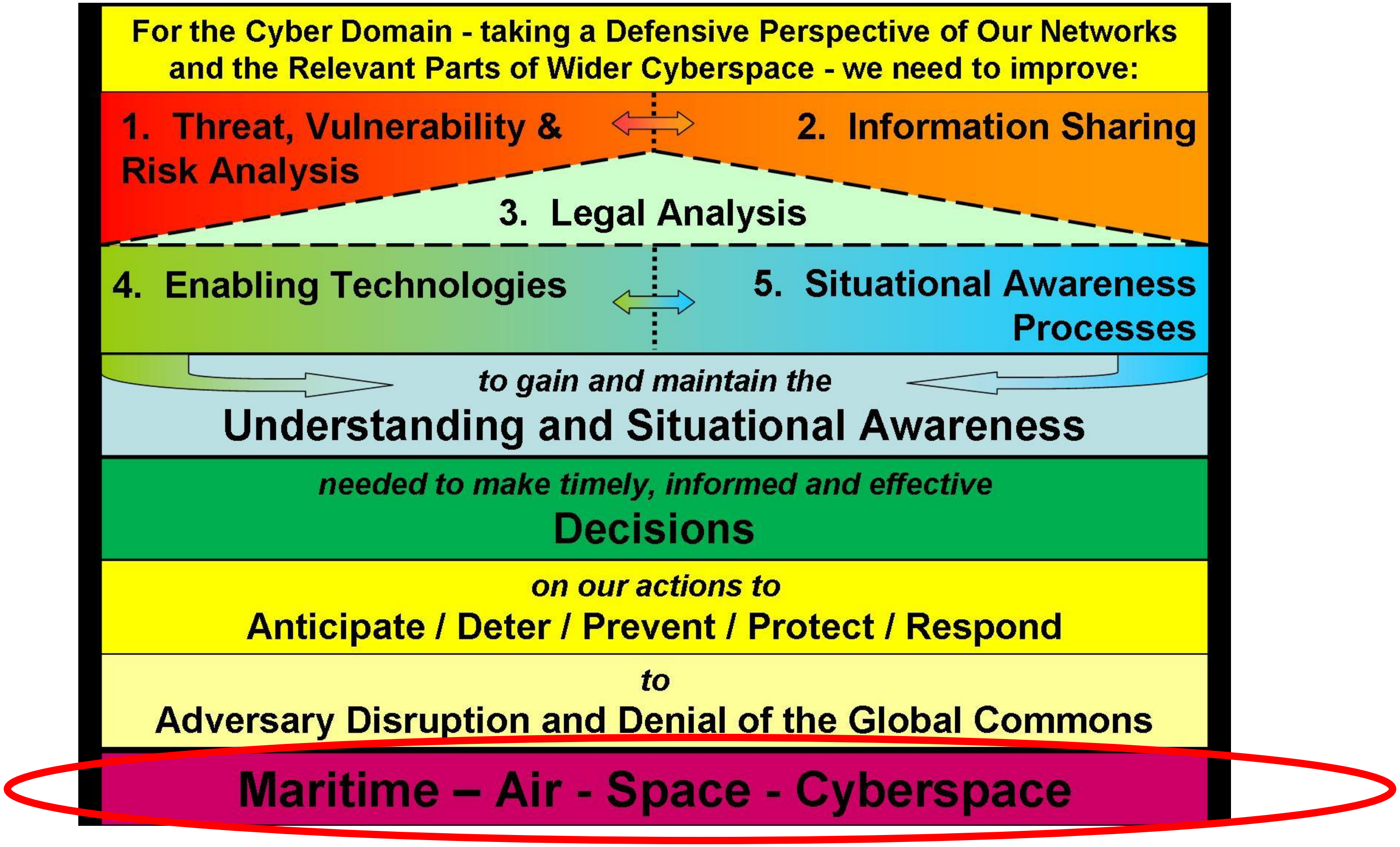
Which actions should be taken, in what order?

Best practices in other domains

2

NATO Multi National Experiment 7

January 2011 – December 2012 ⇨ Access to the Global Commons



For the Cyber Domain - taking a Defensive Perspective of Our Networks and the Relevant Parts of Wider Cyberspace - we need to improve:

1. Threat, Vulnerability & Risk Analysis

2. Information Sharing

3. Legal Analysis

4. Enabling Technologies

5. Situational Awareness Processes

to gain and maintain the

Understanding and Situational Awareness

needed to make timely, informed and effective

Decisions

on our actions to

Anticipate / Deter / Prevent / Protect / Respond

to

Adversary Disruption and Denial of the Global Commons

Maritime – Air - Space - Cyberspace

Identify all relevant stakeholders

E.g. in the cyber landscape

EC – EP – Council – Cybersec/CIP regulation

US - DC3

Europol - EC3

SOCTA

NATO Cooperative Cyber Defence Centre of Excellence

EDA

ENISA

Eurocontrol

Police

Justice

Security Information Exchange Schemes

Public sources - CERTs
Bugtraq, Arbor, Team Cymru,
Shadowserver,
Spamhaus, Clean MX, Conficker
WG, ZeuS Tracker, …
CIRCL datafeeds (AS's)
Botfrei.de – DE-cleaner
FR SignalSpam

Commercial sources
Microsoft
IBM Xforce
Symantec
Intel/McAfee
Verizon

IRC, twitter, anonops, ...

Your MSS contracts (if any)
Your own sensor data (SIEM, IDS, logs, …)

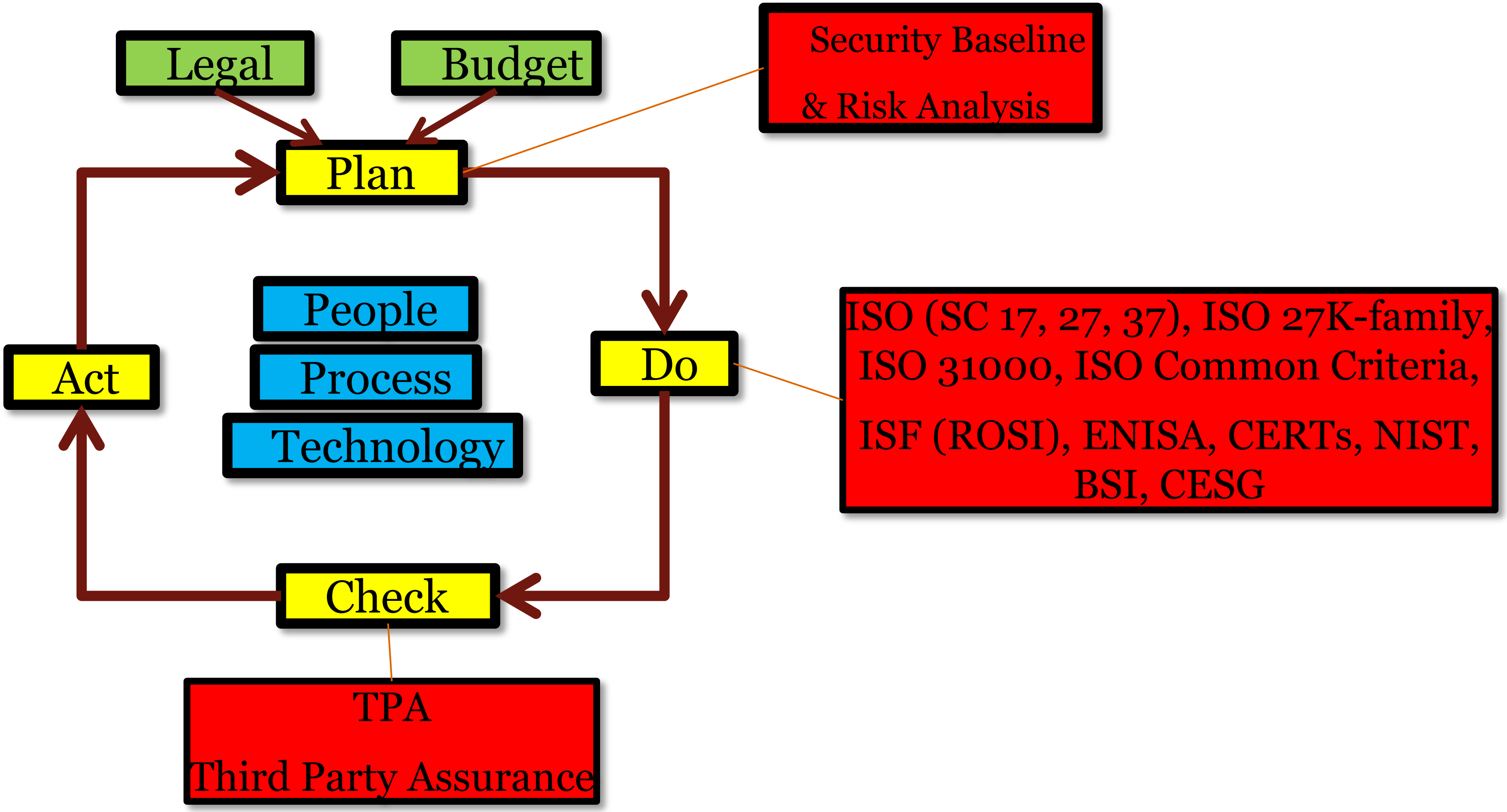
Regular markets – Black markets – Grey markets

Enterprises – SME – Public Sector

Infrastructure – Critical Infrastructure

Suggested Approach

Conceptual



Legal

Budget

Plan

Security Baseline & Risk Analysis

People

Process

Technology

Do

ISO (SC 17, 27, 37), ISO 27K-family, ISO 31000, ISO Common Criteria,

ISF (ROSI), ENISA, CERTs, NIST, BSI, CESG

Act

Check

TPA

Third Party Assurance

Security Baseline

1. Install a management cycle with accountability and budget
2. Implement user education and awareness, and integrate in evaluation cycle
3. Inventory of authorised devices & software
4. Create a layered information security architecture
5. Address security in software development and acquisition
6. Configure systems securely, patched and up to date, and deploy anti-virus (laptop/desktop/server/mobile/routers/access points)
7. Protect information physically wherever it resides
8. Manage the lifecycle of accounts, apply “need to know” in granting logical access, and control the use of administrative privileges
9. Use strong passwords and keep them safe (better: use hardware tokens or biometrics)
10. Generate and analyse logs
11. Prepare incident management
12. Prepare business continuity
13. Perform penetration testing

Selecting your 'above baseline' safeguards

AS-IS

Confidentiality	C.1	Sniffing	2	3	6
	C.2	Acc. Disclosure	2	2	4
	C.3	Traffic analysis	3	3	9
	C.4	Rerouting	1	1	1
	C.5	Software bugs	3	4	12
	C.6	Pass-through	3	2	6
Integrity	I.1	Transmission errors	1	3	3
	I.2	Intentional modification	2	3	6
	I.3	Replay attack	3	4	12
	I.4	TCP/IP weaknesses	2	3	6
	I.5	Credential guessing	3	4	12
	I.6	Software bugs	3	4	12
	I.7	Priviledge escalation	3	4	12
	I.8	Active code	3	4	12
	I.9	Pass-through	3	2	6
Availability	A.1	Ext. physical accident	4	2	8
	A.2	Ext. logical accident	4	3	12
	A.3	Int. physical accident	4	2	8
	A.4	Int. logical accident	4	3	12
	A.5	DOS	4	2	8
	A.6	pass-through	3	2	6
	A.7	facilities	3	2	6
	A.8	int. staff problems	1	1	1
	A.9	ext. staff problems	1	1	1
	A.10	Sabotage, terrorism, theft	2	2	4

TO-BE

Confidentiality	C.1	Sniffing	2	3	6
	C.2	Acc. Disclosure	2	2	4
	C.3	Traffic analysis	3	3	9
	C.4	Rerouting	1	1	1
	C.5	Software bugs	3	2	6
	C.6	Pass-through	3	2	6
Integrity	I.1	Transmission errors	1	3	3
	I.2	Intentional modification	2	3	6
	I.3	Replay attack	3	3	9
	I.4	TCP/IP weaknesses	2	3	6
	I.5	Credential guessing	3	2	6
	I.6	Software bugs	3	2	6
	I.7	Priviledge escalation	3	2	6
	I.8	Active code	3	2	6
	I.9	Pass-through	3	2	6
Availability	A.1	Ext. physical accident	4	2	8
	A.2	Ext. logical accident	4	2	8
	A.3	Int. physical accident	4	2	8
	A.4	Int. logical accident	4	2	8
	A.5	DOS	4	2	8
	A.6	pass-through	3	2	6
	A.7	facilities	3	2	6
	A.8	int. staff problems	1	1	1
	A.9	ext. staff problems	1	1	1
	A.10	Sabotage, terrorism, theft	2	2	4

Best of both worlds

3

Best of both worlds

Aviation is continuously transforming, increasingly by integrating more ICT

Physical checks/cargo screening must be complemented by logical checks, also upstream in the supply chain

Internet of Things, ConnectedCars/ConnectedPlanes will only increase importance of logical checks

Increasing role of:

- Secure SDLC (software development lifecycle)
- Cryptography (authentication, integrity, encryption)
- Biometrics (Smart Borders, ABC-gates)

Risk management applications as per ISO 31K and Information Security Management Systems (ISMS) as per ISO 27K can help to balance increasing ICT risk

Further references

- **Aviation Security Engineering, a holistic approach**, by Rainer Kölle, Garik Markarian and Alex Tarter, ISBN-13: 978-1-60807-072-5, Artech House
- ETSI on security - annual free conference: www.etsi.org/securityworkshop
- ACDC - http://www.acdc-project.eu/
- BSI (DE) - https://www.bsi.bund.de/
- EC3 (within Europol, NL) - https://www.europol.europa.eu/ec3/
- EDA (EU) - http://www.eda.europa.eu/
- ENISA (EU) - http://www.enisa.europa.eu/
- IDC Herzliya (IL) - http://www.ict.org.il/
- NATO - http://www.ccdcoe.org/
- NIST - http://www.nist.gov/cyberframework/

AVIATION SECURITY ENGINEERING
A HOLISTIC APPROACH
AVIATION SECURITY ENGINEERING A HOLISTIC APPROACH

Thank you for your attention