CANSO Standard of Excellence in Cyber Security

canso
civil air navigation services organisation

ICAO Asia/Pacific Regional Cybersecurity Webinar – June 2021

Shayne Campbell

Safety Programme Manager

CANSO

Have we just been lucky so far…?

There have been security incidents that have affected aviation, but no truly disruptive cyber event.

Is that because we're "good", or because we've been "lucky"?

The "Good"

- We have a culture of care and attention to support safety
- Our systems generally operate in an isolated environment (but this is changing…)
- Our processes and procedures are naturally defensive & cautious
- We have checklists of checklists

What if…

- … our safety focus can be used to distract from other threats?
- … the systems we trust implicitly have been altered?
- … our caution stops us acting quickly when we need to?
- … our checklists & procedures make us predictable to an attacker?
- … a supplier we trust gets compromised?

canso

CASE STUDY: SolarWinds "SUNBURST" Attack

Probably the most publicised attack so far in 2021

In late 2020, SolarWinds discovered malicious code had been inserted into its Orion monitoring product.

The malicious code was distributed to customers around March 2020.

The attackers first accessed internal SolarWinds systems in Sept 2019.

Information taken from Microsoft Security's Deep Dive into Solorigate/SUNBURST[1]

Step 4 - Compromise

The code was designed to provide an entry point into end user organisations.

Even in isolated environments.

Step 3 - Deployment

The attackers deployed 4,000 lines of malicious code, packaged as a genuine part of Orion

Step 2 - Research

The attackers spent time researching the protections SolarWinds had in place and finding a way to use them maliciously.

Step 1 – Unauthorised Access

The attackers covertly found a way into SolarWinds' systems and established a persistent capability.

canso

[1] https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/

Establishing Cyber 'Policy" is a great place to start

But isn't security about technical protections, firewalls and keeping 10,000 unique passwords?

These technical protections need to build on a solid foundation:

Risk Management

Business is about **managing risk,** so this is about managing security in a way that is familiar and well understood.

Regulation

Aka **Governance –** independent oversight to help keep the right behaviours happening.

Maintenance

Protecting against **supply chain** attacks via maintenance partners

Comms Security

Protecting against **impersonation** and **being influenced** by anonymous attackers

Access Control

Both **physical** and **logical,** use of least privilege, etc.

Handling Incidents

Consider an incident might be an **intelligent attacker** rather than a statistical event.

Think about **Business Continuity**, maybe graceful degradation of service.

Also consider **Disaster Recovery** – how to rebuild from nothing.

Share knowledge and **work together** - even commercial competitors are on the same side against attackers.

New Systems

Design in **foundational security**, and make sure **procurement chains** are trustworthy and not compromised

Ops Security

Building good cyber into operational processes

Compliance

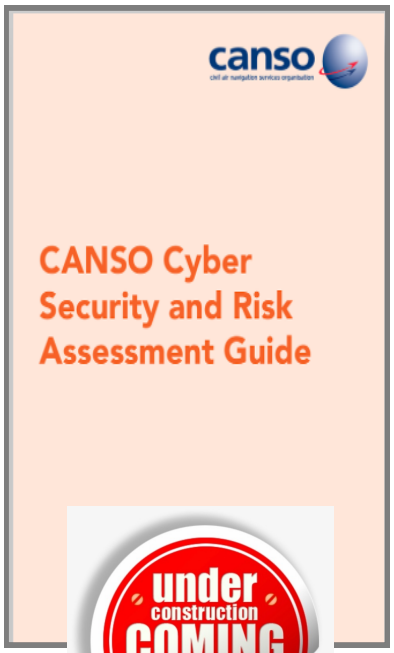
Maintaining **evidence packs** – a key part of Audit

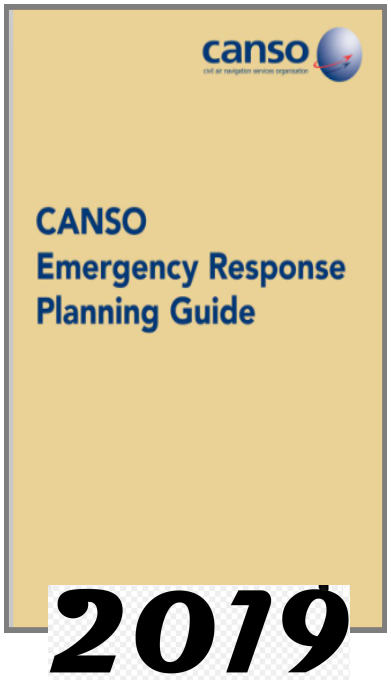
Asset Management

Knowing what you have, and what vulnerabilities you might be exposed to

Policy stands as the foundation of good technical protections

CANSO Cyber Toolkit

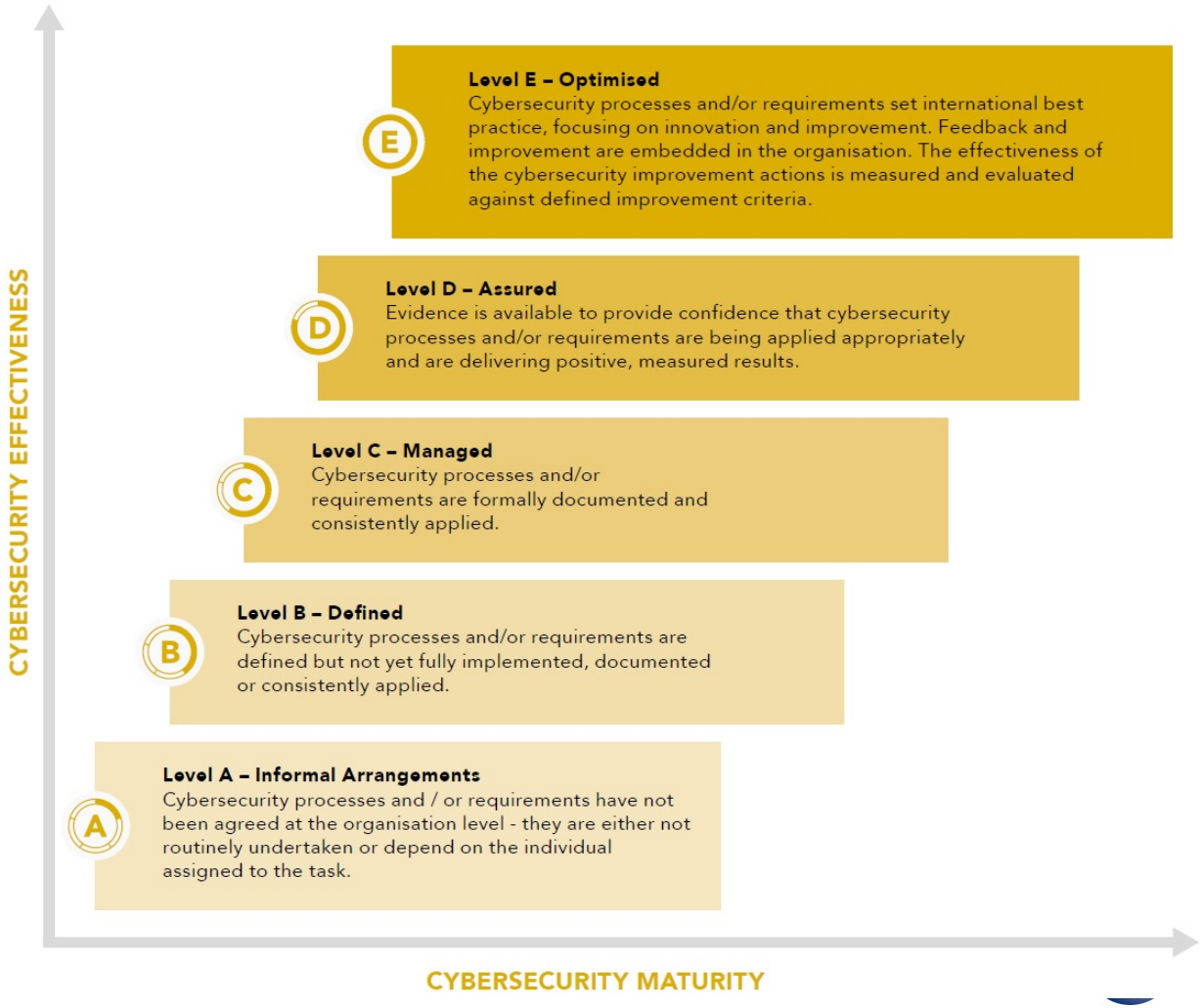




https://canso.org/publications/

SoE Maturity Levels

CANSO Standard of Excellence in Cybersecurity



Example: Information Sharing

Where are we currently?

			Maturity levels				
	Element	**Description**	**A Informal Arrangements**	**B Defined**	**C Managed**	**D Assured**	**E Optimised**
	Information sharing	The organisation obtains and shares threat intelligence, vulnerability and incident information activities, with internal and external parties	No, or very limited, cybersecurity information sharing	Using some threat intelligence and vulnerability information; Informal information sharing internally and externally where appropriate	Trends are identified; Internal and external sharing based on formal processes linked to risk assessment, vulnerability management, response and recovery processes; Relevant risk information is shared between safety and security functions	Threat intelligence and vulnerability information for all critical systems; Consistent, widespread and effective sharing between all relevant parties.	Information sharing is habitual and proactive; demonstrable leadership in improving industry-wide information sharing

Assessment is supported by probing questions for ANSPs and suppliers

SoE contains loads of advice and lessons learned

canso

Example Assessment Results

Function	Capability	ANSP	Supplier 1	Supplier 2	Supplier 3	Supplier 4	Supplier 5
Lead and Govern	Leadership and Governance	D	D	D	C	B	B
	Information Security Management System	C	D	C	C	C	B
Identify	Asset Management	E	E	D	C	C	B
	Risk Assessment	B	D	D	B	C	B
	Information Sharing	C	D	C	B	B	A
	Supply Chain Risk Management	C	D	D	C	B	A
Protect	Ident ity Management and Access Control	D	E	C	C	D	C
	Human - Centred Security	B	D	D	C	C	A
	Protective Technology	D	E	C	D	B	B
Detect	Anomalies and Events	D	C	C	C	C	A
Respond	Response Planning	C	D	D	D	A	A
	Mitigation	D	D	C	C	A	B
Recover	Recovery Planning	D	D	D	B	C	B

YAMM 🤦

Yet Another Maturity Model???

Yes, but

- it is *aimed at ATM* – so it is relevant for us (at least for many of us in ATC…)
- it aims to focus on security *in a safety-related context*
- it has already been and will likely be *used by our customers* to assess us
- it is very simple and a *self-assessment* should be possible in *less than a day*!

canso

What to do with the results of the SoE?

Profile and maturity		
	Current	Target
Lead and govern		
Identify		
Protect		
Detect		
Respond		
Recover		

Element	Gaps	Priority	Budget	Year 1 improvements	Year 2 improvements
1	Small	Low	€		✓
2	Large	High	€€	✓	✓
3	Medium	Moderate	€€€	✓	
...					
n	None	Low	–		


Visit us:
canso.org
canso