Transitioning Cyber Security to a Mission Risk Mindset
(aka, why the new ISM is better)

Iain Dickson
@wan0net

What will I be covering?

- Definitions
- What is the ISM?
- What changed with the ISM?
- Why is a risk management approach better?**?
  - An allegory

** In my opinion

What's my experience with Cyber?

- 8 years in Cyber Security, 11 (inclusive) in IT
- Currently the Cyber Technical Lead for Australia at Leidos
- Previous Positions
  - Cyber Security Research Engineer
  - Assistant Director Cyber Threat Intelligence Technical Capability
  - Security Operations Centre Lead
- Relevant Qualifications:
  - GIAC Certified Industrial Control Systems Professional (GICSP)
  - GIAC Certified Penetration Tester (GPEN)
  - GIAC Certified Continuous Monitoring Analyst (GMON)
- ComfyCon AU Founder

Definitions #1

Threat

Any circumstance or event with the potential to adversely impact organizational operations, assets, or individuals.

×

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered.

→

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event.

Definitions #2

Risk Management: Using an understanding of risk, based on threat and vulnerability, to determine what actions to take. NIST RMF is an example of a Cyber Risk Management Approach

Risk Owner: Someone who is responsible / accountable should a given risk be realised.

CISO: An official position in the Information Security Manual

Accreditation: The process of achieving approval to use a network. Also known as “Authority to Operate”

Threat Actor Tiers

Resources

Volume

Tier VI
Nations, Global 25

Tier V
Nations, Global 150, State Sponsored

Tier IV
Organised Crime, Cyber Mercenaries

Tier III
Crime Groups, Hacktivists

Tier II
Criminals, Disgruntled Workers. Programmers

Tier I
Script Kiddies, Non Malicious Actors

Creates Vulnerabilities using Full Spectrum

Discovers Unknown Vulnerabilities

Exploits pre-existing, known vulnerabilities

https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf

BLUF | TL;DR

The new ISM allows **resourced** organisations who exercise **mature** risk management approaches to enable their business operations through **careful selection** of security controls.

What is the ISM?

Australian Government Information Security Manual

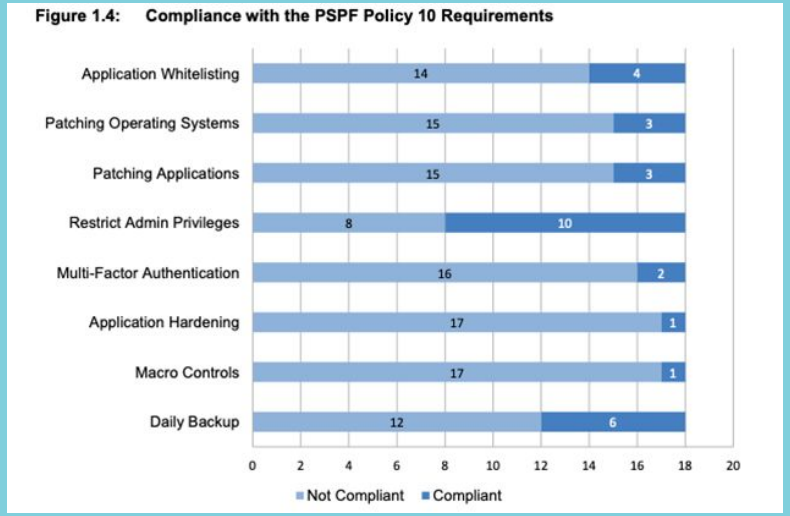
It contains….

- Information on suggested controls for Australian Government networks of the OFFICIAL DLM, PROTECTED, SECRET and TOP SECRET classifications
- Forms the basis for the development of security controls against these environments, which are then assessed for accreditation of the system by a member of the Information Security Registered Assessors Program.
- The accreditation authority / risk owner of the organisation** (generally the CISO) then holds accountability if they accept the resulting risk of the networks, and therefore accrediting.

** unless it’s a TOP SECRET network then this is held by DG ASD

It also contains… The Essential 8

- The Essential 8 provides a baseline of controls ***based on a set of threats that ASD/ACSC have deemed likely*** - They may not be your threats, or they may not be relevant to your vulnerabilities.
- The E8 is a reporting requirement for Federal Agencies, but has become a pseudo compliance requirement.
    - Arguably, it's not proven to not be working, or provide a false sense of security ------>



https://www.itnews.com.au/news/fed-agencies-cop-mass-fail-in-core-systems-cyber-review-548738

What changed with the ISM?

November 2019 (past)

Security Control: 1341; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
A HIPS is implemented on workstations.

Security Control: 1034; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
A HIPS is implemented on high value servers such as authentication servers, Domain Name System (DNS) servers, web servers, file servers and email servers.

June 2020 (present)

Security Control: 1341; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
A HIPS is implemented on workstations.

Security Control: 1034; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS
A HIPS is implemented on high value servers such as authentication servers, Domain Name System (DNS) servers, web servers, file servers and email servers.

November 2019

Risk management considerations

This document is not a compliance-based standard. Rather, organisations are encouraged to consider security risks discussed in this document and apply security controls where appropriate within a risk management framework in accordance with their business requirements and threat environment.

Security Control: 1341; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
A HIPS is implemented on workstations.

Security Control: 1034; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
A HIPS is implemented on high value servers such as authentication servers, Domain Name System (DNS) servers, web servers, file servers and email servers.

June 2020

Using a risk management framework

The risk management framework used by the ISM draws from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Rev. 2, ***Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy***. Within this risk management framework, the identification of security risks and selection of security controls can be undertaken using a variety of risk management standards, such as International Organization for Standardization (ISO) 31000:2018, ***Risk management – Guidelines***. Broadly, the risk management framework used by the ISM has six steps: define the system, select security controls, implement security controls, assess security controls, authorise the system and monitor the system.

Security Control: 1341; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS

A HIPS is implemented on workstations.

Security Control: 1034; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS

A HIPS is implemented on high value servers such as authentication servers, Domain Name System (DNS) servers, web servers, file servers and email servers.

Does this mean that Government Agencies can now ignore the ISM?

No.

The new ISM…

- Understands that system owners are the ONLY people who can adequately identify the risks (and prior to those, the threats and vulnerabilities), that their system has.
- Rather than a blanket approach to systems security it puts the onus on the government agencies to identify what is relevant to them.
- Allows the selection of specific controls for specific use cases, while not using controls where they are too onerous.

So why is a risk management approach better?

Risk Management is the Language of Executives

Allegory


D-8053

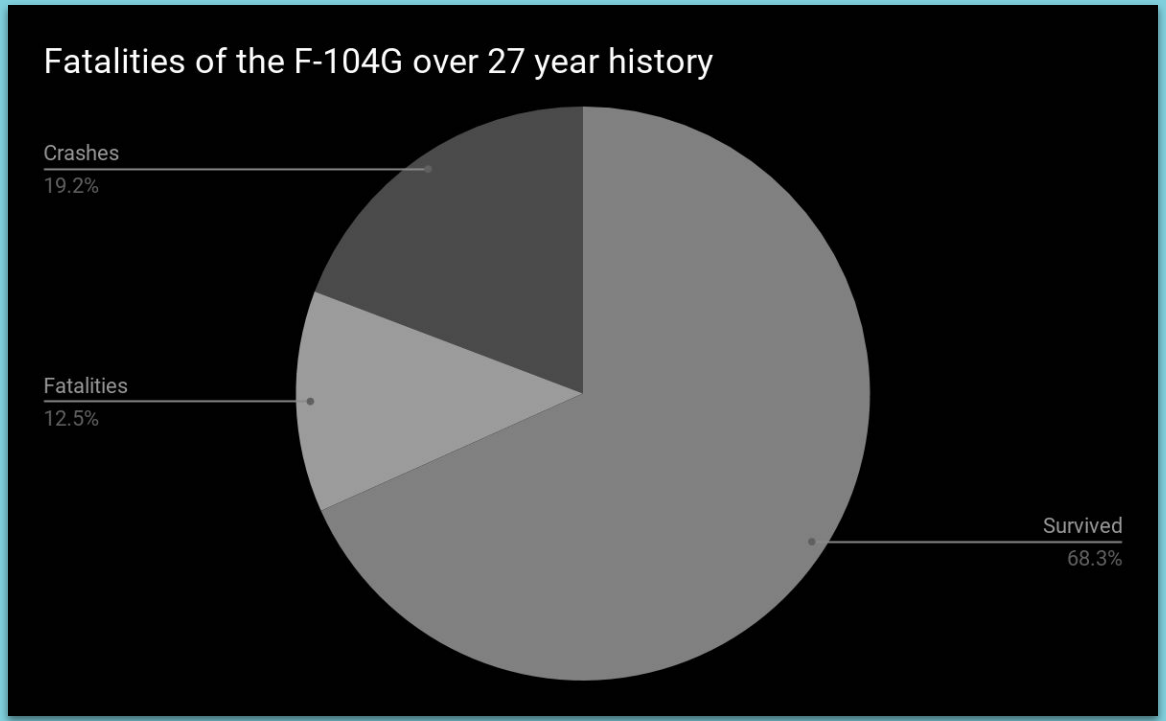

Captain Lockheed
and the Starfighters
by Robert Calvert

Salesman. Yes. It's the finest fairweather fighter on the market. You won't find a better one at the price. Or any price for that matter

Strauss: Yes, it's very nice. But we need a plane for bombing, straffing, assault and battery, interception, ground support and reconnaissance. Not just a fairweather fighter!

Salesman: Well, that's ok. We can make some modifications. It'll cost a little extra, but it's worth it.


Bavaria


Fatalities of the F-104G over 27 year history
Crashes
19.2%
Fatalities
12.5%
Survived
68.3%

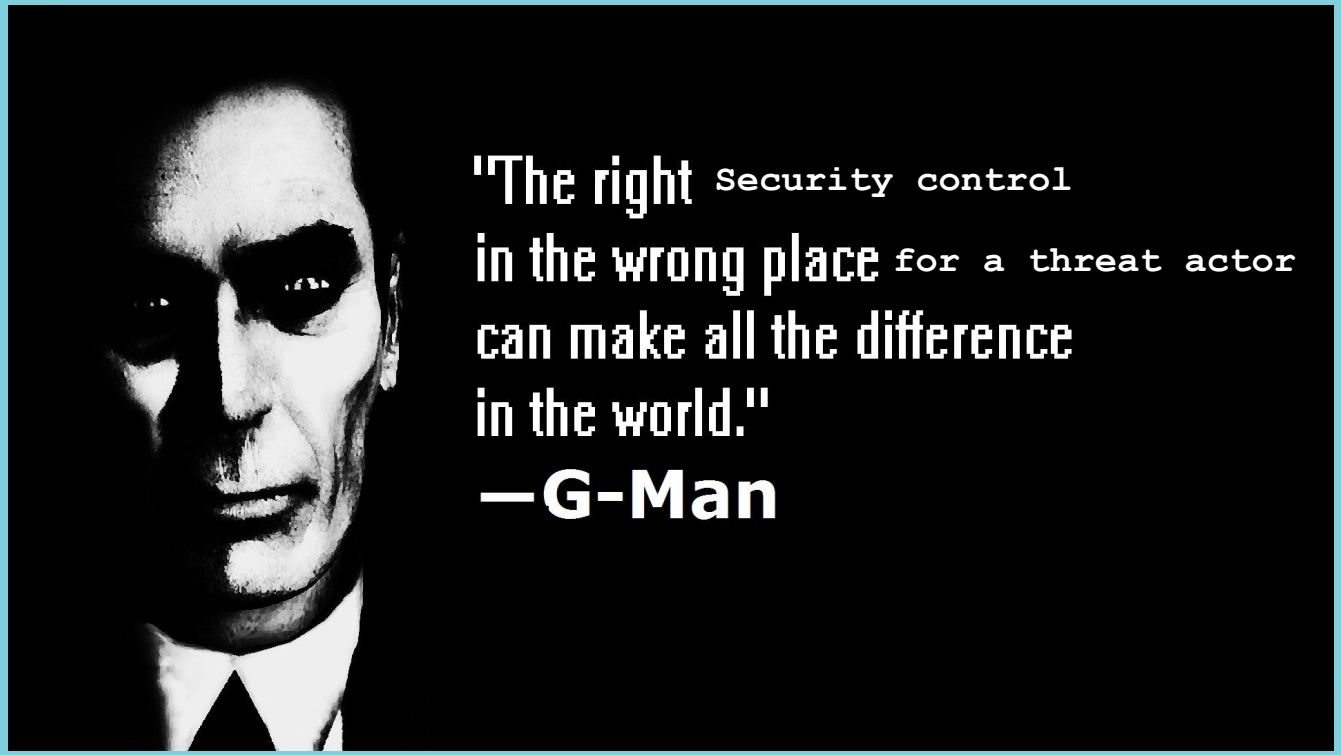
Systems should not, and can not, be designed to counter every threat imaginable without impacting usability.

Cyber security is there to enable a business to do it’s work securely. Not to inhibit it.

A risk approach takes into account the relevant threats, and vulnerabilities, AND the business context of which they sit, do determine appropriate controls to implement.

Mature risk management approaches provide better security outcomes and business outcomes.

In essence


"The right Security control
in the wrong place for a threat actor
can make all the difference
in the world."
—G-Man

A few examples where blanket rules of controls don’t work...

- Operating system patches to Industrial Control Systems (in fact anything ICS, controls go out the window)
- Application Whitelisting for Software Developers
- Macros for Finance Personnel
- AV if you are a penetration tester

Whats the next step?

- Understanding that risk is dependent on a number of factors. Your risk changes constantly, and a mature model adapts to this.

- Integrated Risk Management with other elements of business risk

- See Military Risk Management models, Mission risk!

Thanks!