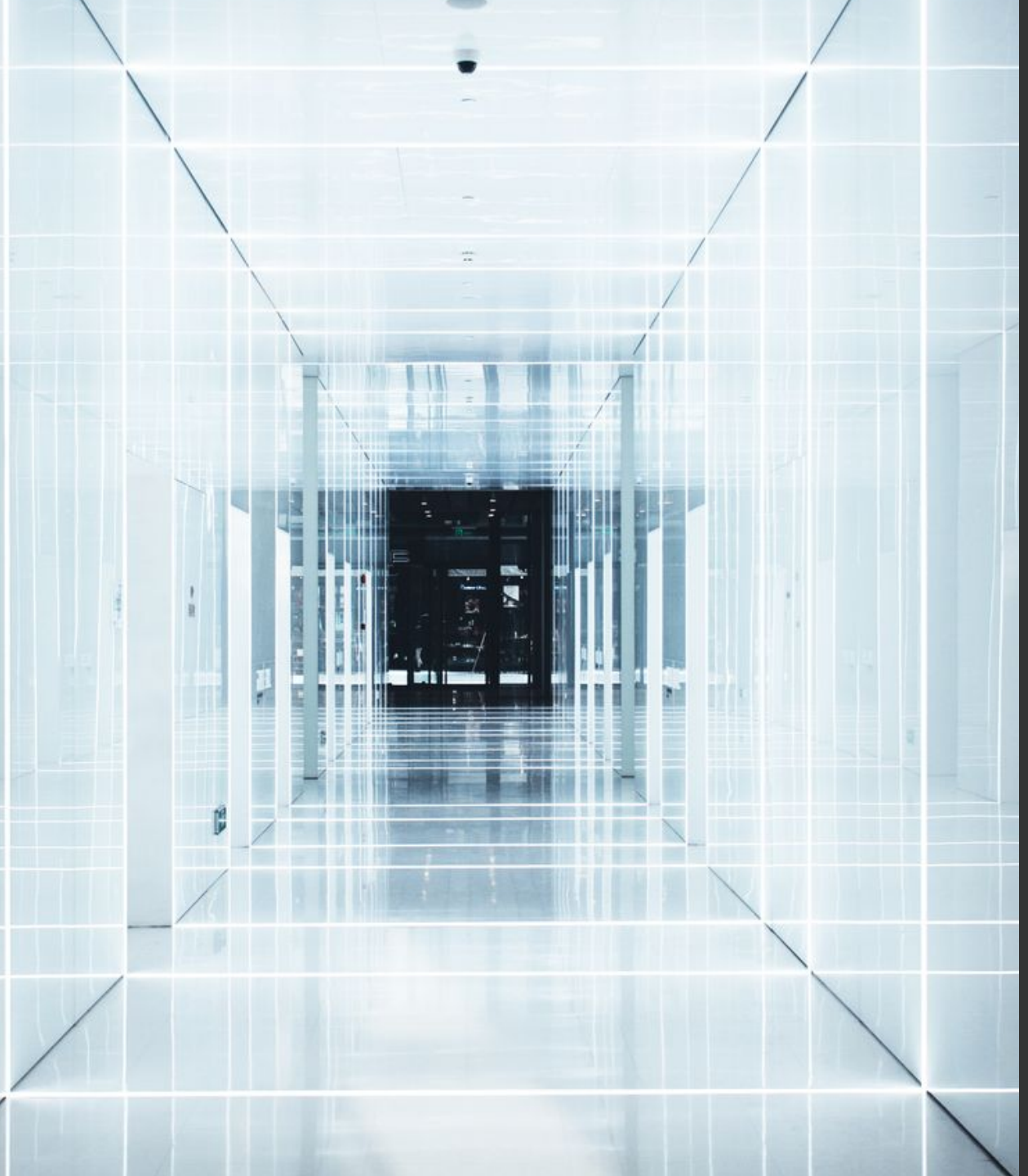
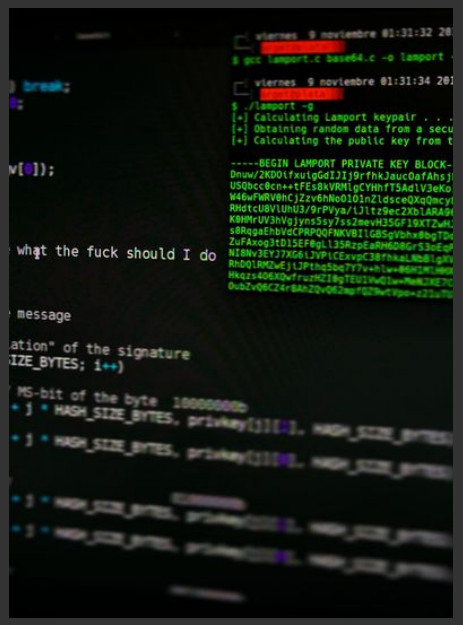


The Poor Person's Guide To Security

Who Am I?



The Agenda

1. GRC
2. The Boring Bits
3. Next Steps

GRC

Security Is A Balancing Act

- You Need To Do Your Job
- We Don't Have Any More Money
- You Need A Strategy
- You Can't Have Anymore Resources
- Make Everything More Secure
- They Take Your Stapler
- We Need This Yesterday

The Boring Bits

Keeping It Simple

Develop A Strategy

The Strategy Should Tell The Story Of What, Why & How

Choose A Framework

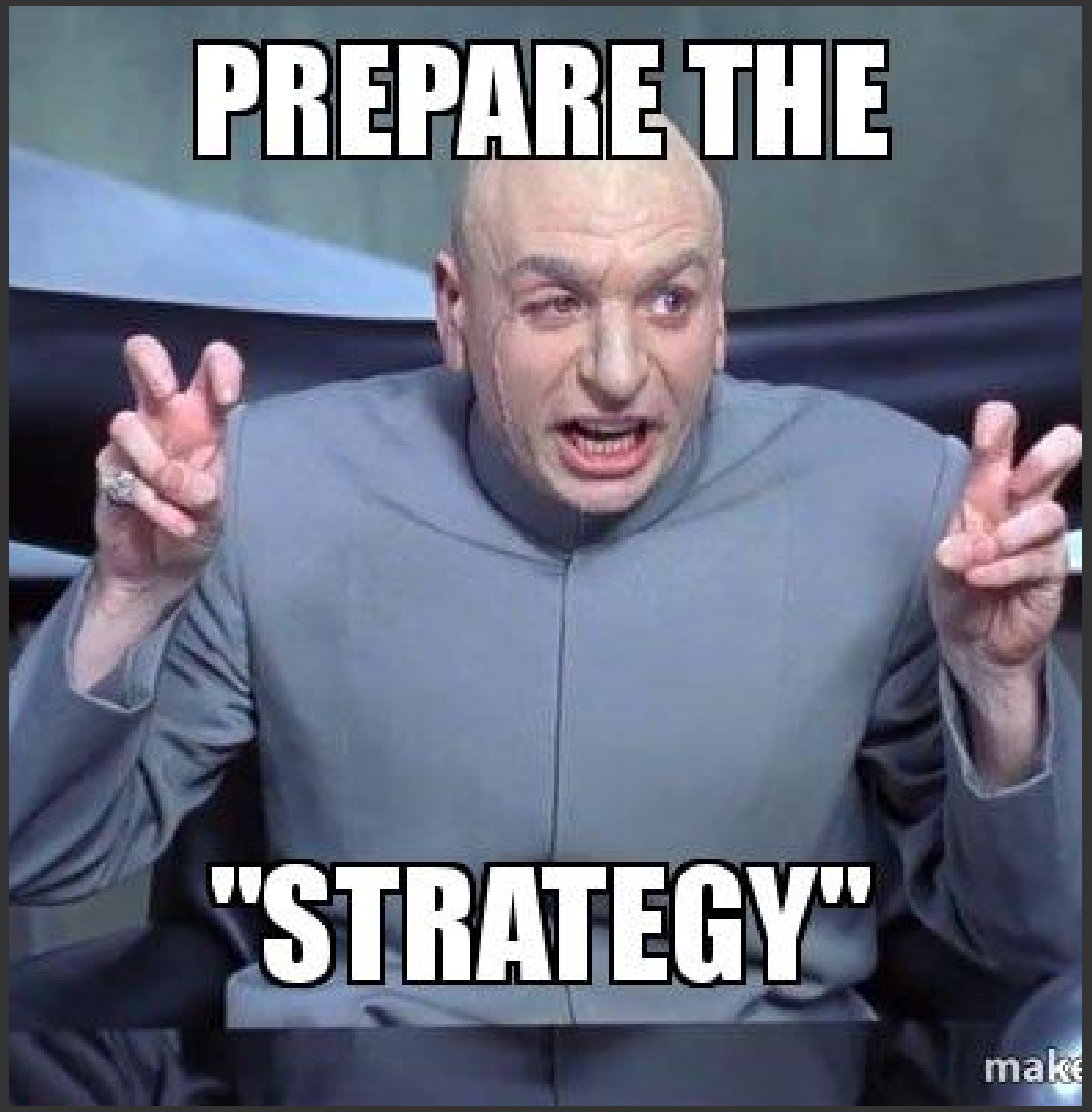
CIS Controls - Practical, Straight Forward & Well Documented

Perform A Gap Analysis

Simple & Straight Forward Approach To Work Out Where You Stand

Develop A Roadmap

The Outcome From The Gap Analysis Will Drive The Roadmap



Developing A Strategy

- Why There Is A Need For A Security Strategy?
- What Are You Going To Do?
- How Does The Strategy Align To The Business?
- What Are The Risks?
- How Long Will It Take To Achieve?
- How Will The Strategy Be Measured?

The Language Of Risk

1. **Identify The Risk**
   What Assets Are Critical To The Business?
2. **Assess The Risk**
   What Are The Threats & Consequences?
3. **Mitigate The Risk**
   Can The Risk Be Reduced Or Transferred?
4. **Accept The Risk**
   Is The Risk At An Acceptable Level?

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

CIS CONTROLS

An IG1 organisation is small to medium-sized with limited cybersecurity expertise to dedicate toward protecting IT assets and personnel. Sub-Controls selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks.

Inventory and Control of Hardware Assets

- Control 1.4

  Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all assets, whether connected to the organisation's network or not.

- Control 1.6

  Ensure that unauthorised assets are either **removed** from the network, quarantined or the inventory is updated in a timely manner.

Inventory and Control of Software Assets

- Control 2.1

  Maintain an up-to-date list of all authorised software that is required in the enterprise for any business purpose on any business system.

- Control 2.6

  Ensure that unauthorised software is either **removed** or the inventory is updated in a timely manner.

- Control 2.2

  Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to the organisation's authorised software inventory. Unsupported software should be tagged as unsupported in the inventory system.

- Control 2.9

  The organisation's application **whitelisting software must ensure that only authorised, digitally signed scripts** (such as *.ps1,*.py, macros, etc.) **are allowed** to run on a system.

Continuous Vulnerability Management

- Control 3.4

  Deploy automated software update tools in order **to ensure that the operating systems are running the most recent security updates** provided by the software vendor.

- Control 3.5

  Deploy automated software update tools in order **to ensure that third-party software** on all systems **is running the most recent security updates** provided by the software vendor.

Controlled Use Of Administrative Privileges

- Control 4.2

  Before deploying any new asset, **change all default passwords** to have values consistent with administrative level accounts.

- Control 4.3

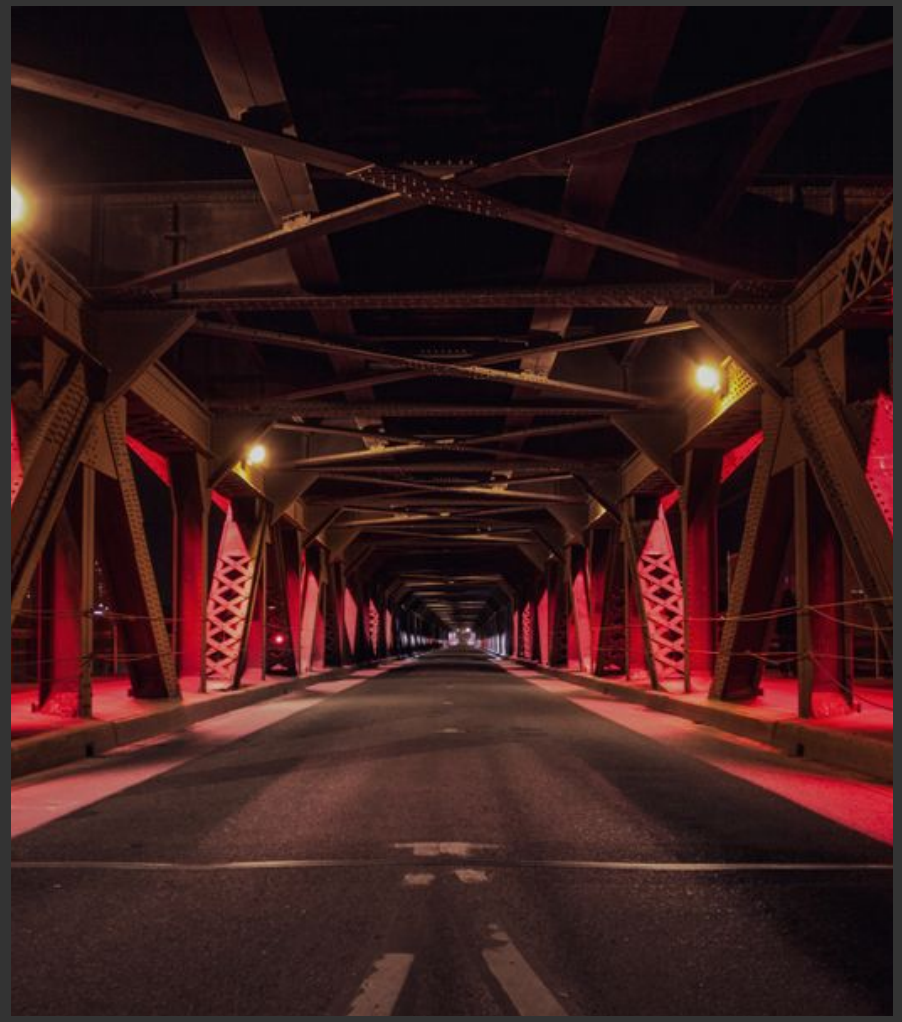
  Ensure that **all users with administrative account** access **use a** dedicated or **secondary account for elevated activities**. This account should only be used for administrative activities and not Internet browsing, email, or similar activities.

Secure Configuration For Hardware and Software On Mobile Devices, Laptops, Workstations and Servers

- Control 5.1

  Maintain documented **security configuration standards for** all authorised **operating systems and software**.

Maintenance, Monitoring and Analysis of Audit Logs



- Control 6.2

  Ensure that local **logging has been enabled** on all systems and networking devices.

Australian Privacy

- Control 21.1

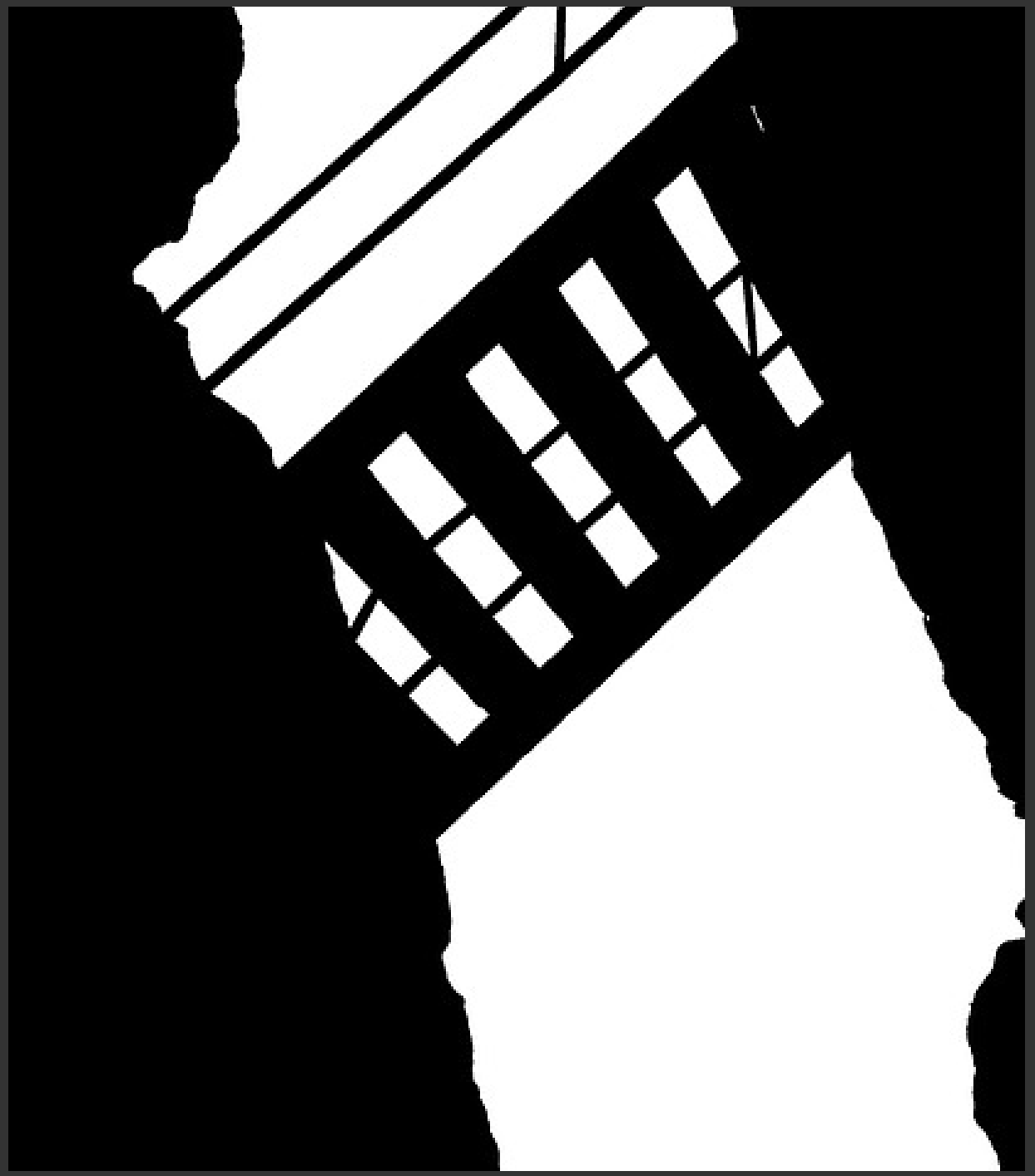
  Privacy requirements applicable to the organisation **have been identified**

- Control 21.2

  The organisation has defined what it considers **personal information in the context of its business activities**

- Control 21.3

  There is a point of contact (person or role) to whom privacy issues could be reported



Performing A Gap Analysis

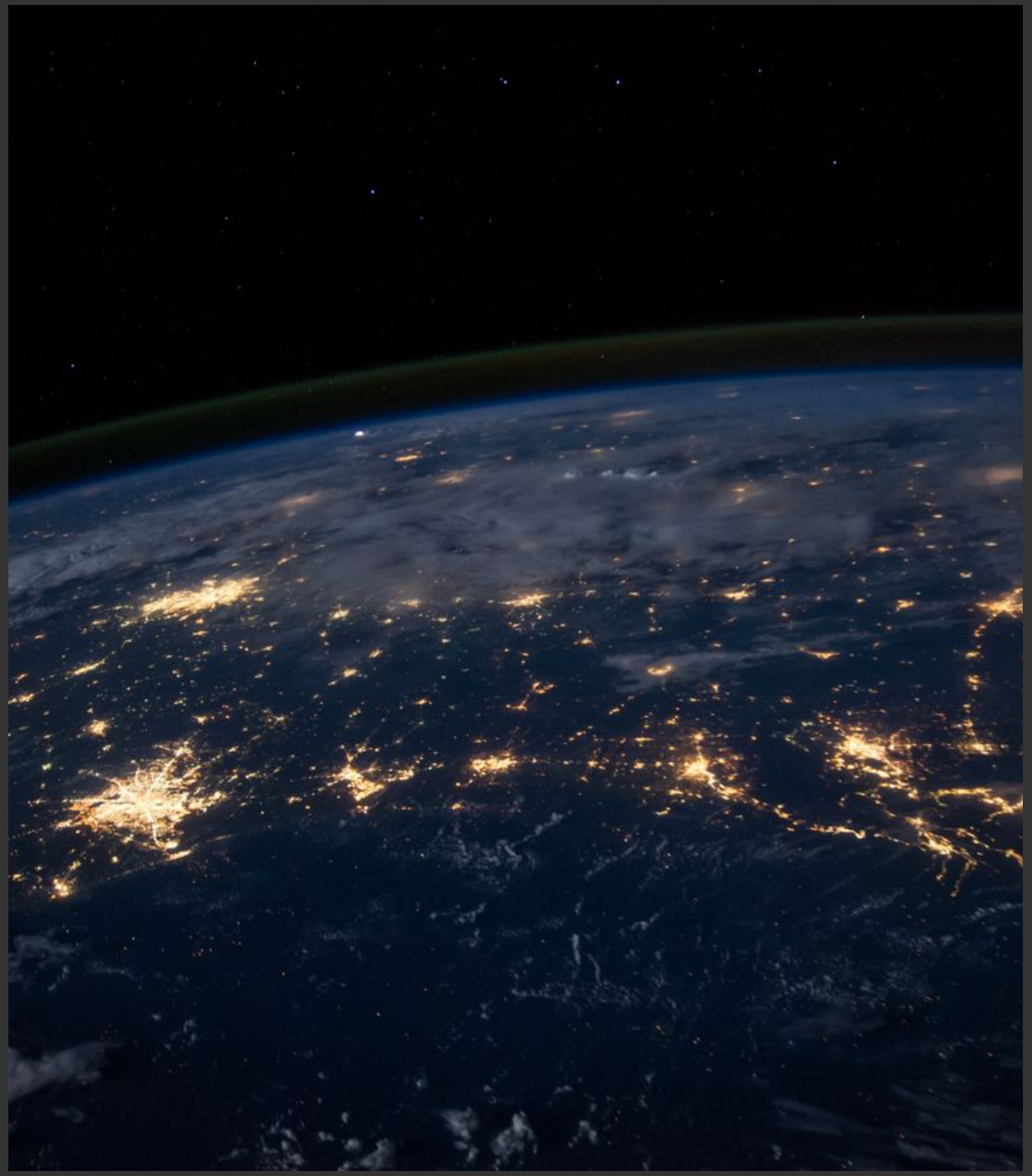
- Be Honest - It doesn't matter if the results are bad. It is NOT a reflection on YOU
- Keep It Evidenced Based - If it isn't documented it isn't happening
- Measuring Stick - Use the gap analysis to measure your progress
- This Is Just The Start - The gap analysis will help drive the roadmap

Developing A Roadmap

- Keep It Simple & Realistic
- Don't Take On More Than You Can Handle
- Take Your Time
- Prioritise What Is Most Important

Security Awareness - Users Are Your Friends

- Find A Topic That Resonates With Them
- Talk To Them On A Human Level
- Listen First To Understand
- Make Security Fun



Embrace OpenSource

- NMap (Network Scanner)
- Wazuh (SIEM)
- GoPhish (Phishing Framework)
- pfSense (Firewall)
- OpenVAS (Vulnerability Scanner)
- OPSI (OS / Patch Management)
- Security Onion (All In One)
- OSSIM (A Bit Of Everything)
- OpenCanary - (Honeypot)

Key Takeaways

- Slow & Steady Wins The Race
- Keep It Simple
- Don't Re-Invent The Wheel
- Doing Something Is Better Than Doing Nothing


TAKING THE
NEXT STEP

github.com/panz05/securityinabox

- Modified CIS Initial Assessment Tool For IG1
- Cyber Security Strategy Template
- Cyber Security Roadmap & Project Plan Template
- Security Risk Management Template
- Risk Register Template
- IT Asset Management Policy Template
- Vulnerability & Patch Management Policy Template
- Audit & Logging Plan Template
- Australian Privacy Policy Template
- Asset Security Hardening Policy Template
- Acceptable Use Policy Template
- Privileged Access Policy Template

“The Way To Get Started Is To Quit Talking And Begin Doing.” – Walt Disney

Thank You