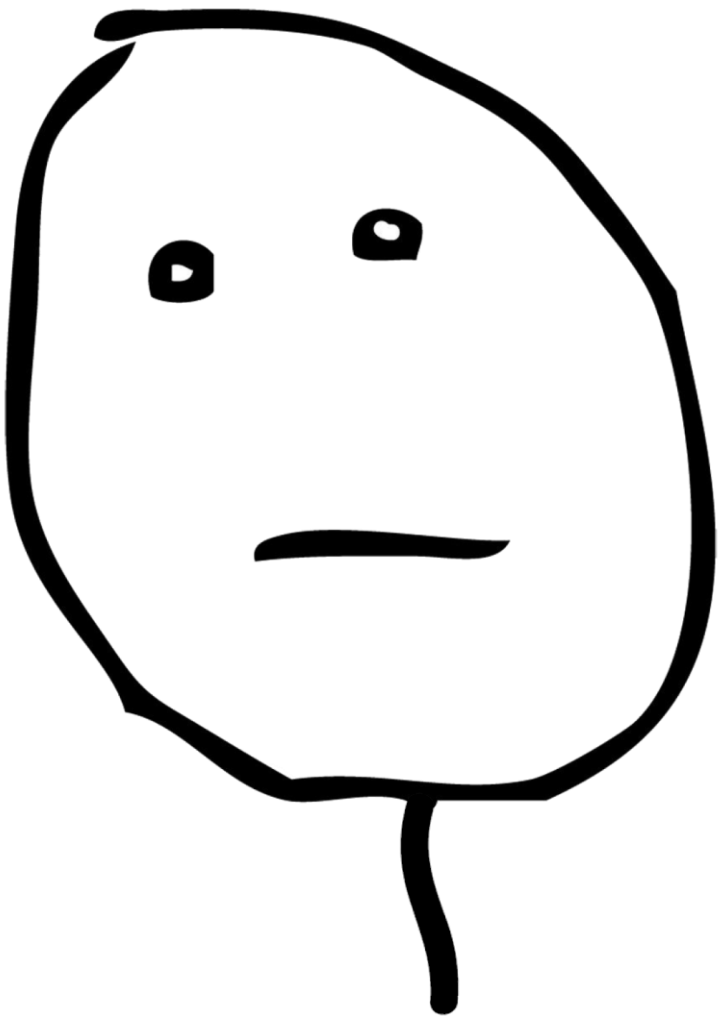
Exposing the Weak Links

A No-Holds-Barred Look at Cybersecurity Governance

You unexpectedly find yourself in the role of CISO at a new company.

Your CEO says:
“Congratulations on your new role. Now go make my company cyber secure.”

What do you do?



Who am I?

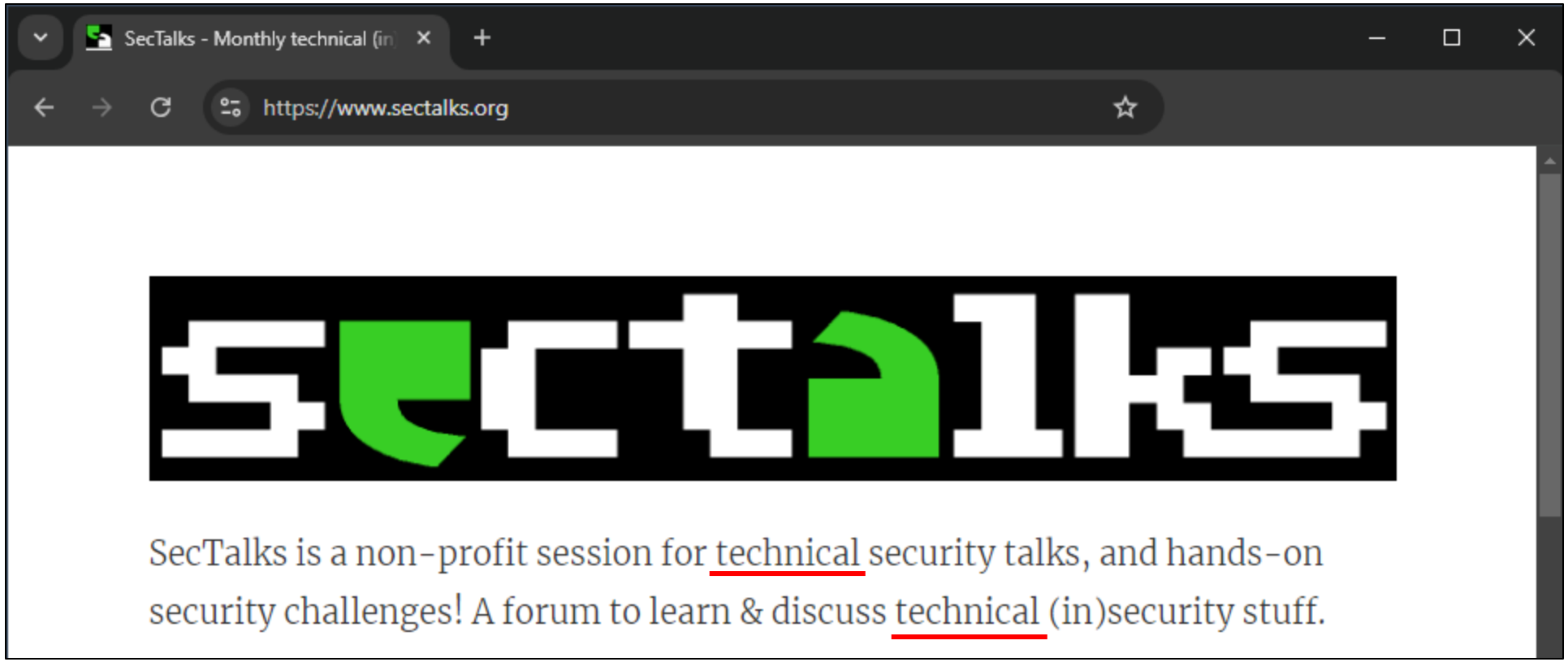
- Dylan Holloway
- Full time InfoSec Lead @ Avant
- Part time gym junkie
- All-time boardgames enthusiast
- I prefer beef burgers over chicken and I've never met a dog I didn't like

Who am I?

- Dylan Holloway
- Information Security Lead @ Avant
- Cyber consultant @ EY
- Various IT roles @ Macquarie Uni
- Hobby developer
- CISSP, CCSP
- Bachelor Arts / Commerce

Who am I?

- Dylan Holloway
- Information Security Lead @ Avant
- Cyber consultant @ EY
  - Policy & Standards @ Big 4 Bank
  - Cyber Hubs design @ Fed Gov
  - Cyber Strategy @ Superannuation
  - Threat & Risk Ass. @ various
  - Cyber Maturity Ass. @ various



Details

👉 *In this session we are going to host a rather different topic. We are looking to get your feedback. This will help the SecTalks review board in their future talk selection.*

Cyber governance in the news

PRESS RELEASE

Copy Link

SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures

Complaint alleges software company misled investors about its cybersecurity practices and known risks

https://www.sec.gov/newsroom/press-releases/2023-227

PRESS RELEASE

Former Chief Security Officer Of Uber Sentenced To Three Years' Probation For Covering Up Data Breach Involving Millions Of Uber User Records

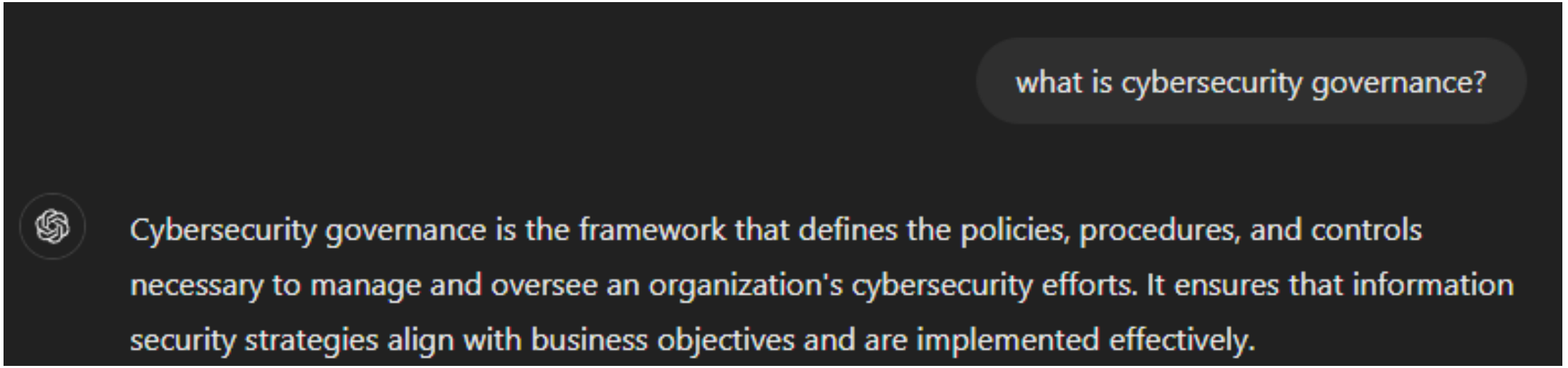
https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-sentenced-three-years-probation-covering-data

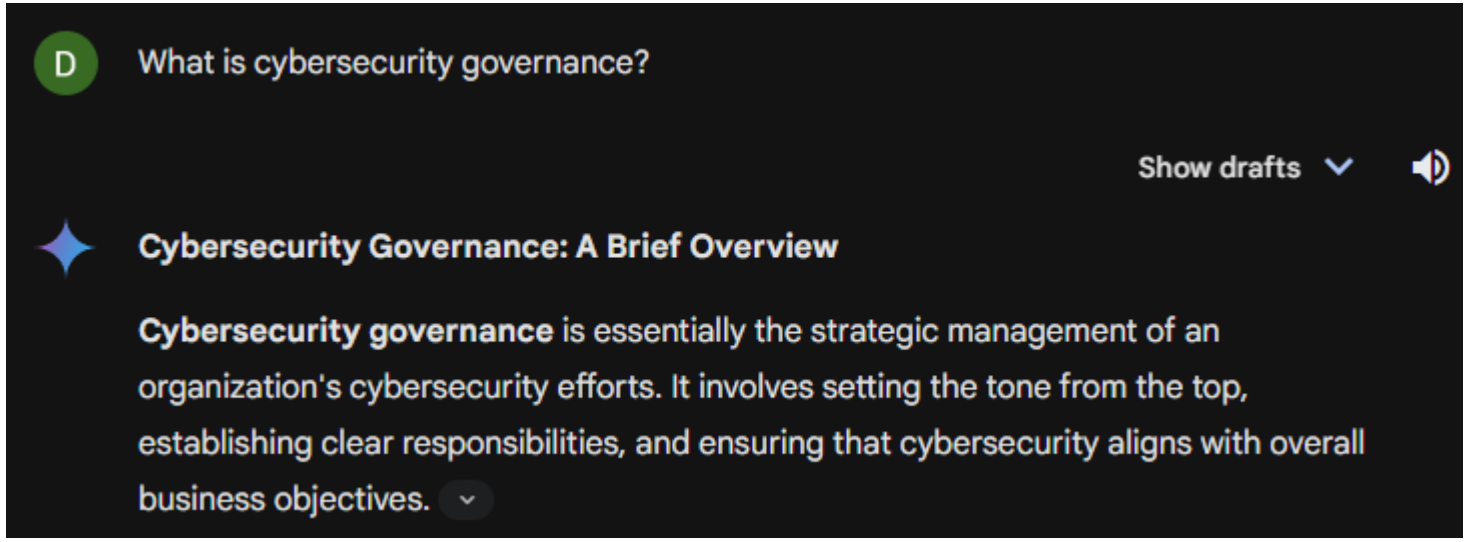
2018

2024

“I have literally no idea what it is”

What is cyber governance?





What is cyber governance?

Cybersecurity governance is the alignment of security to business requirements.

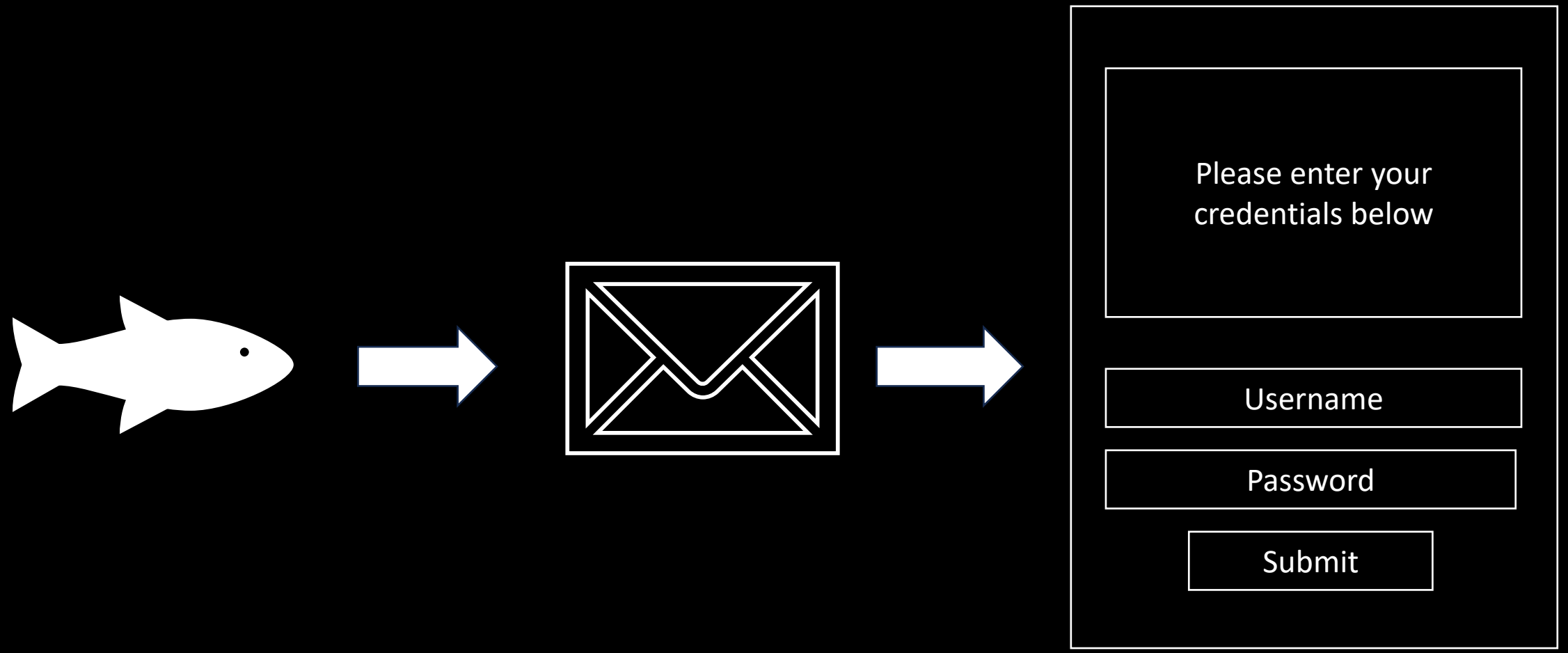
Why do we need cyber governance?

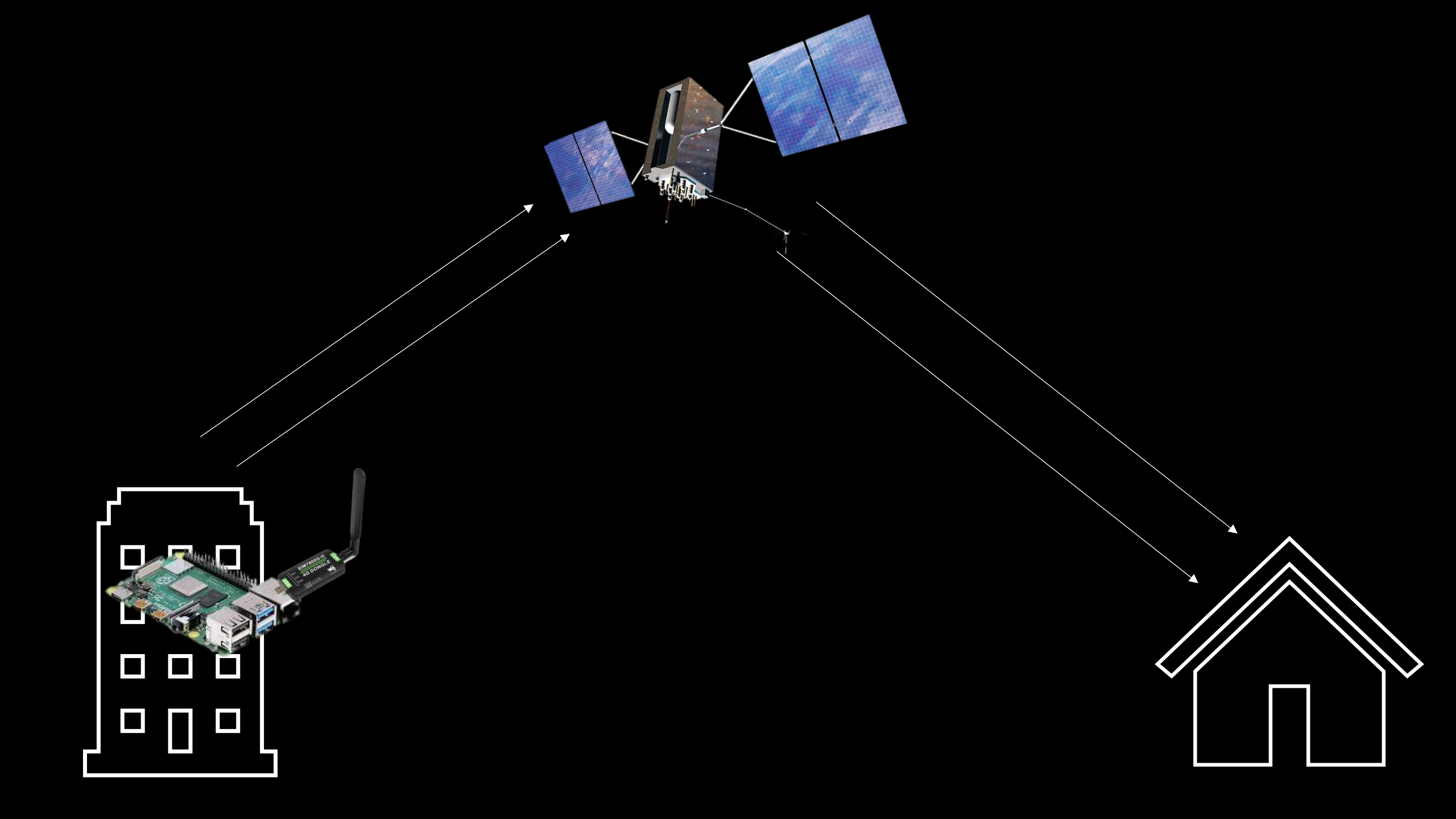
I’m a pentester. All I want are root shells and Domain Admin. Why should I care about GRC?

I’m a SOC analyst. Just give me the log files and stay out of my way. Why should I care about GRC?

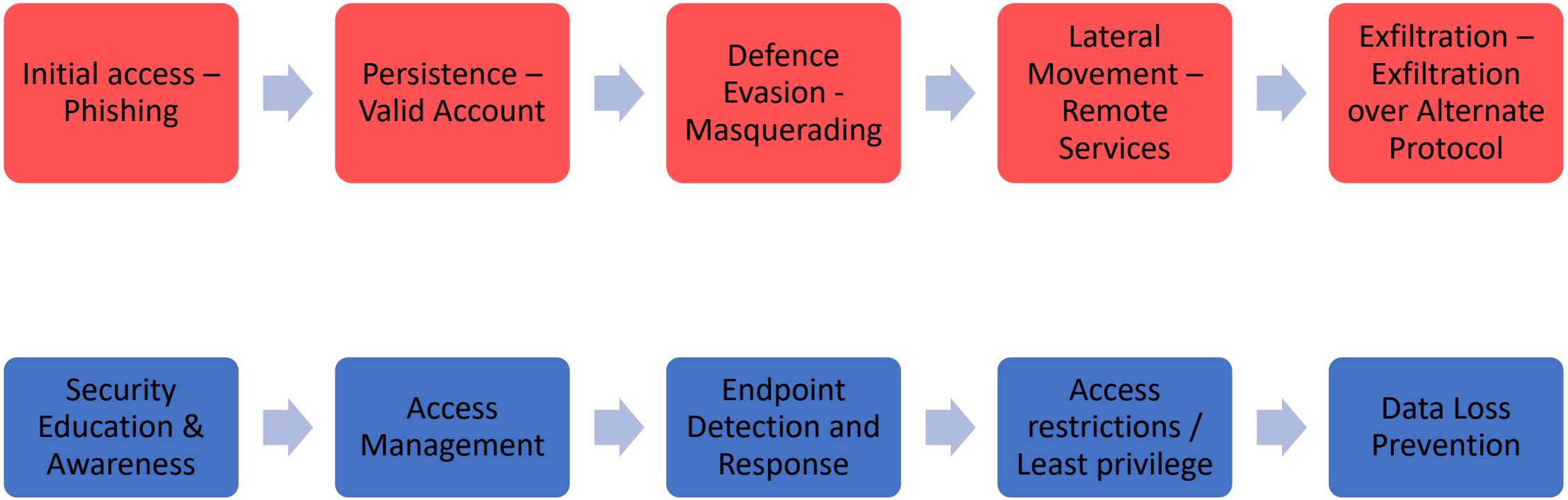
I’m a CISO. My job is to protect an organisation from every possible security threat. Why should I care about root shell, or your log files?

Case study – Targeted red team attack




SIM7600G-H
4G DONGLE

Mitre ATT&CK Framework



Cybersecurity's role in an organisation

- Companies exist to make money.
- They do this in 2 ways:

1. Maximise growth opportunities
2. Minimise risk

"If I give $1 million to Marketing, they will generate $10 million dollars in sales for us. If I give it to IT Security…I won't get hacked?"

"Maybe. Might still get hacked."

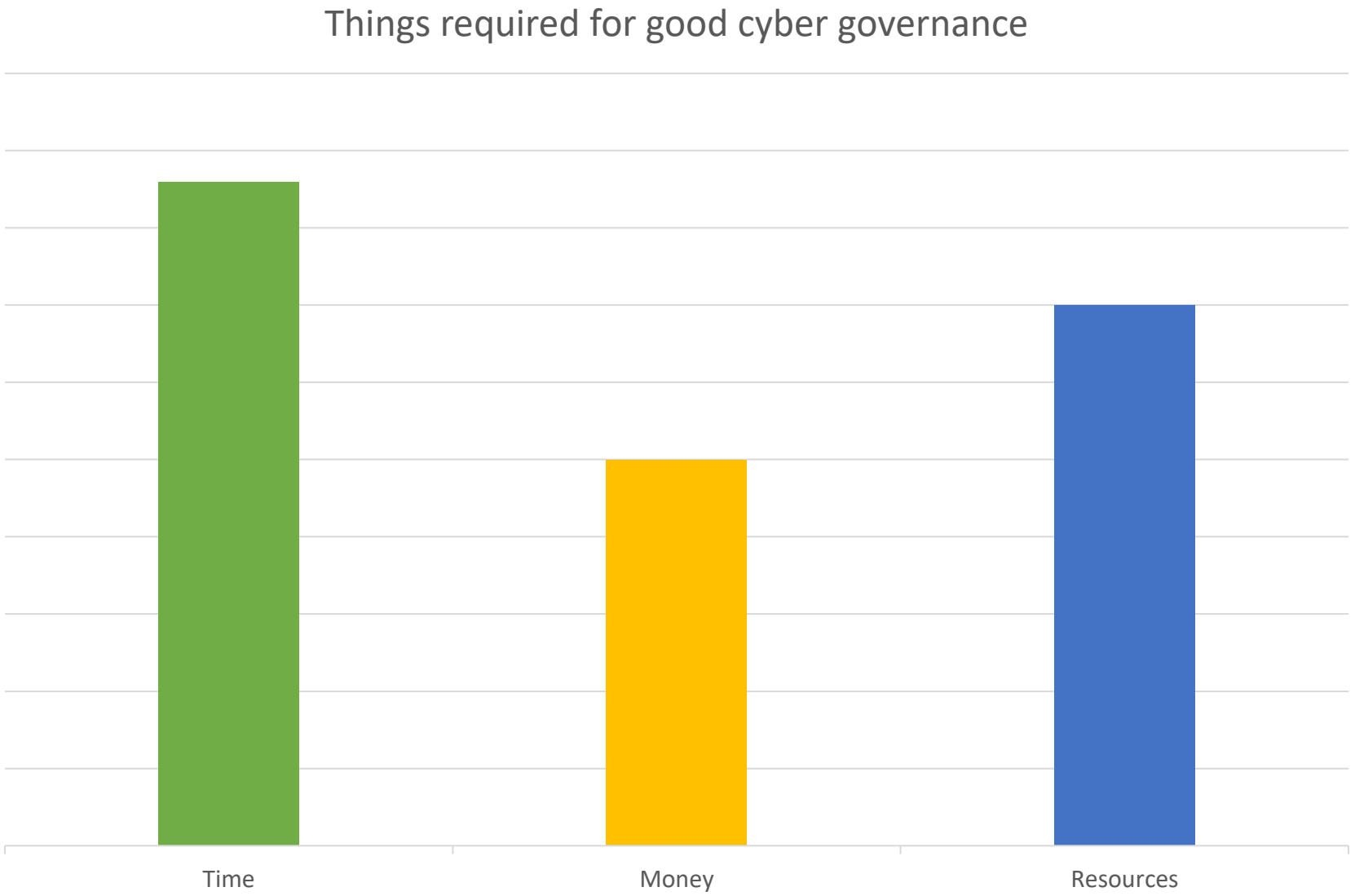
"And what if I don't give it to you? I'll definitely get hacked?"

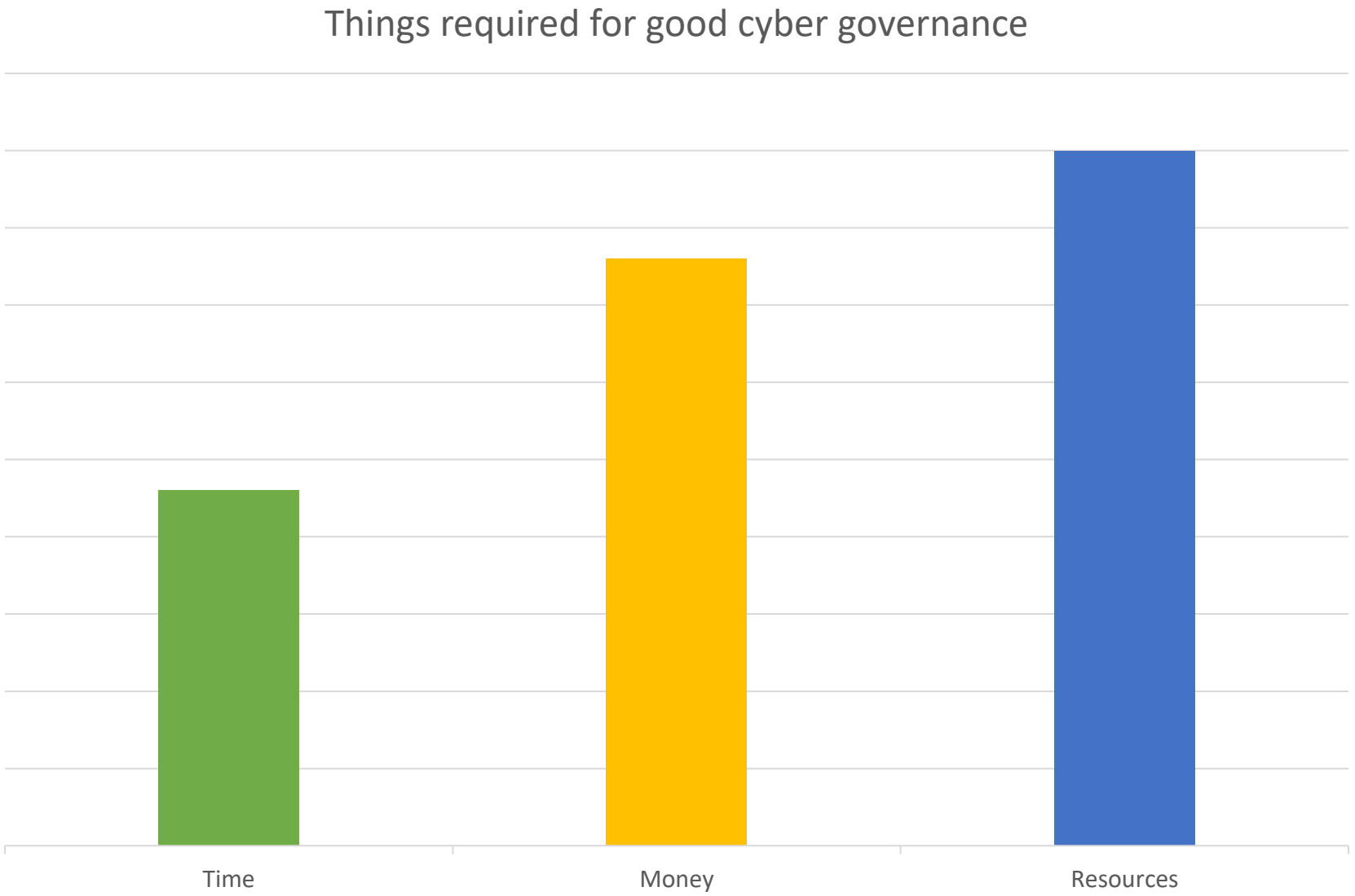
"Maybe. Might not get hacked."

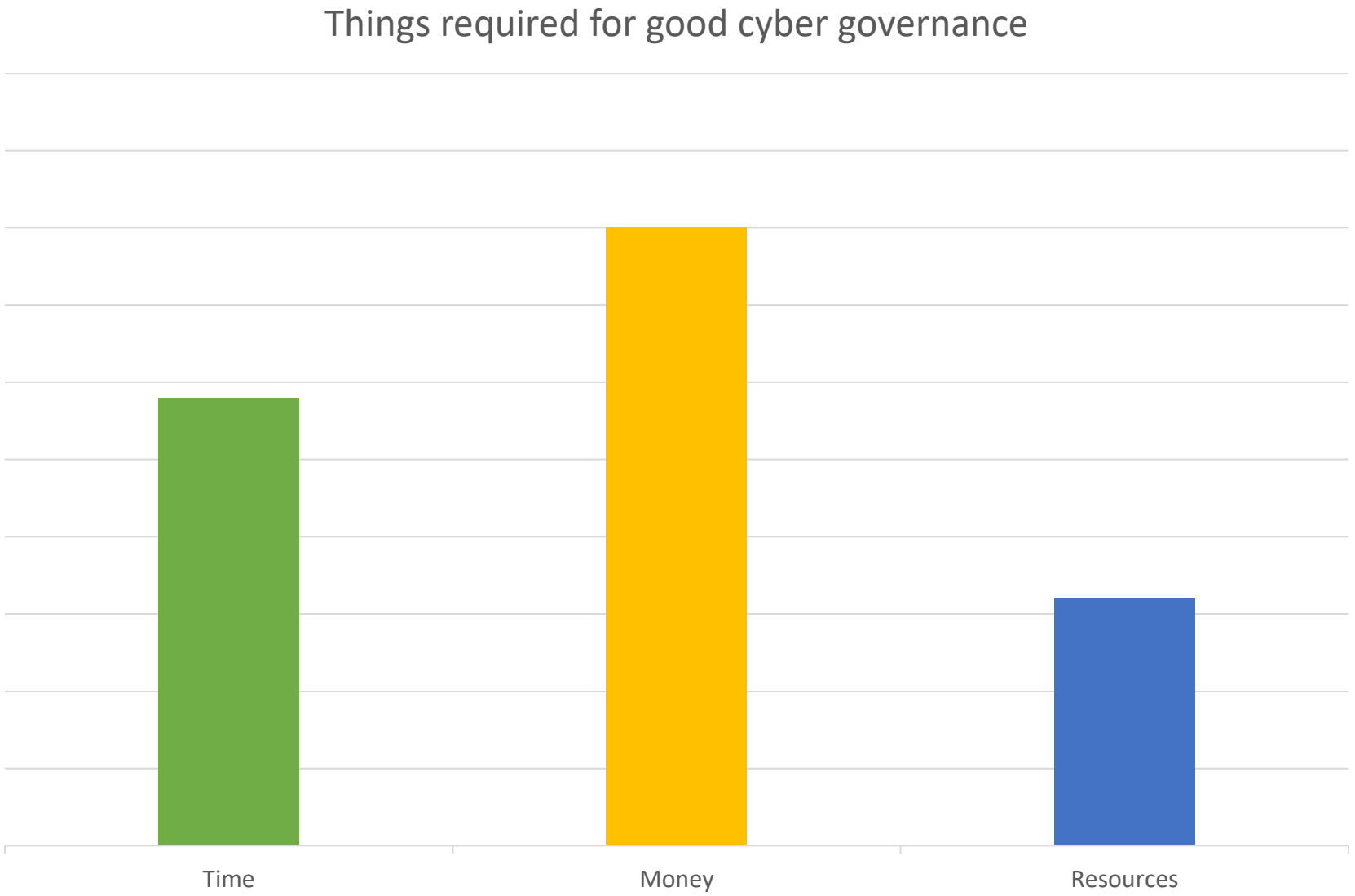
"So you're saying you have no idea whether we're going to get hacked or not?"

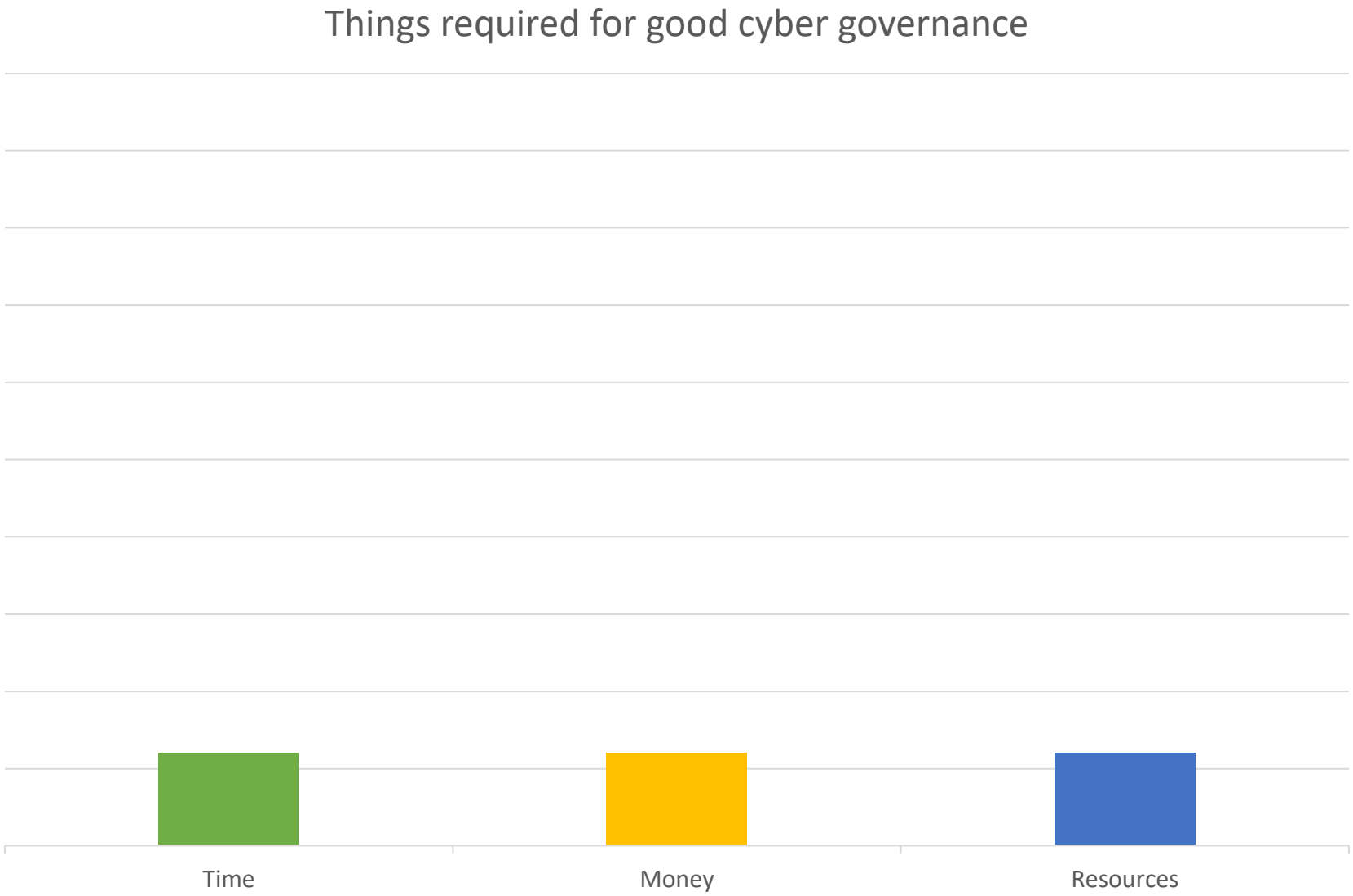
"Yes."

"So why should I give you $1 million?"


Things required for good cyber governance
Time
Money
Resources


Things required for good cyber governance
Time
Money
Resources


Things required for good cyber governance
Time
Money
Resources


Things required for good cyber governance
Time
Money
Resources

Defining cyber requirements

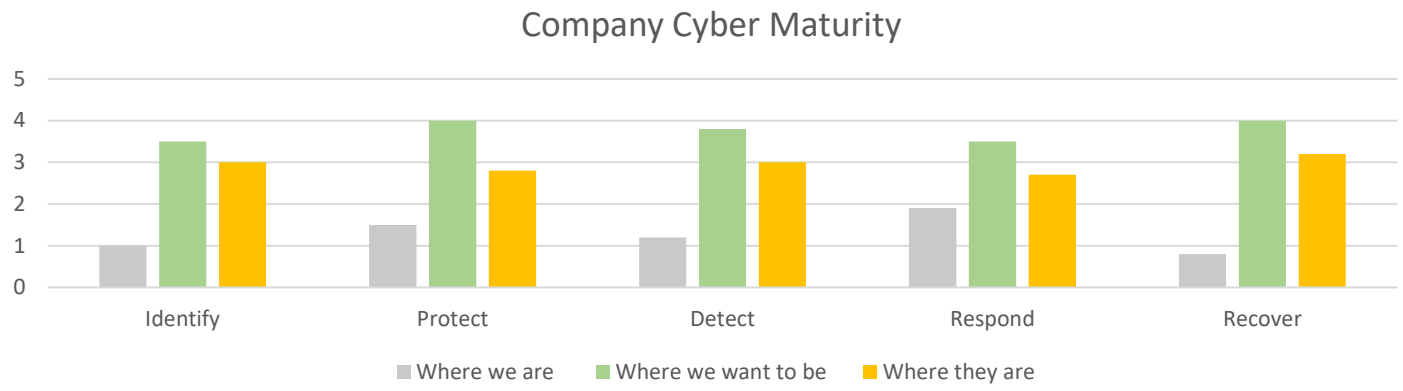
Business Profile

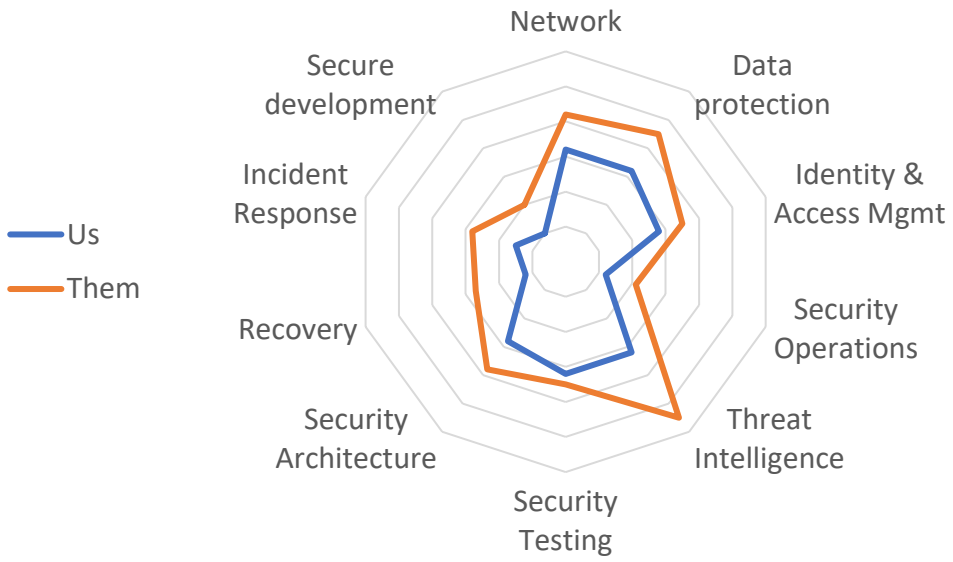
- Technology used
- Business processes
- Supply chains / third-party integrations
- Legislative requirements
- Regulatory requirements
- Operating models
- Critical assets

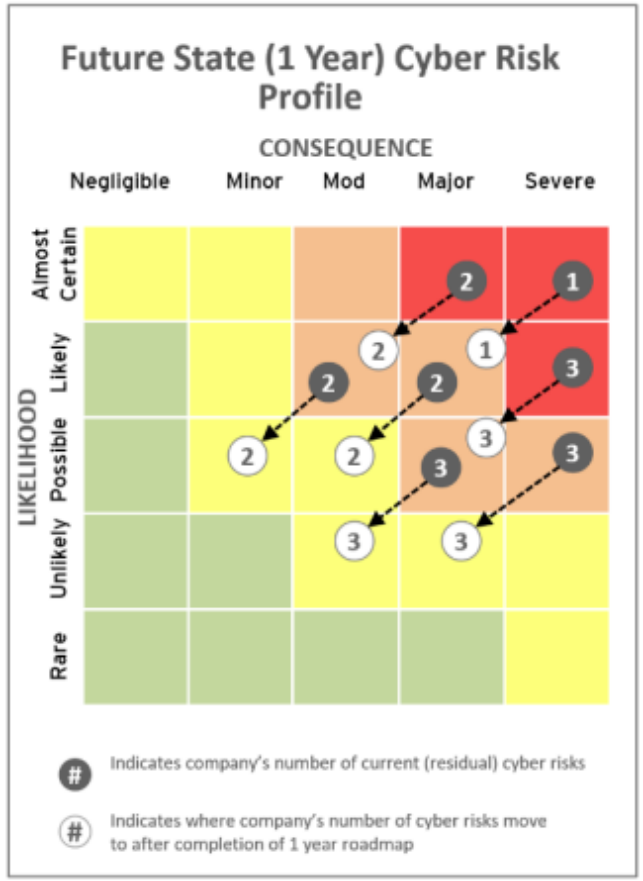
Threat Landscape

Threat actors	Motivations	TTPs	Consequences
Insiders	Carelessness / Money	Data exfiltration	IP theft / Data breach
Script kiddies	Boredom / reputation	Vulnerability exploitation	Operational disruption
Hacktivists	Idealism	Defacement / Denial of Service	Reputational impact
Cyber criminals	Money	Phishing	Financial loss
APTs	Politics	Zero days	Total shutdown

Cybersecurity's role in an organisation

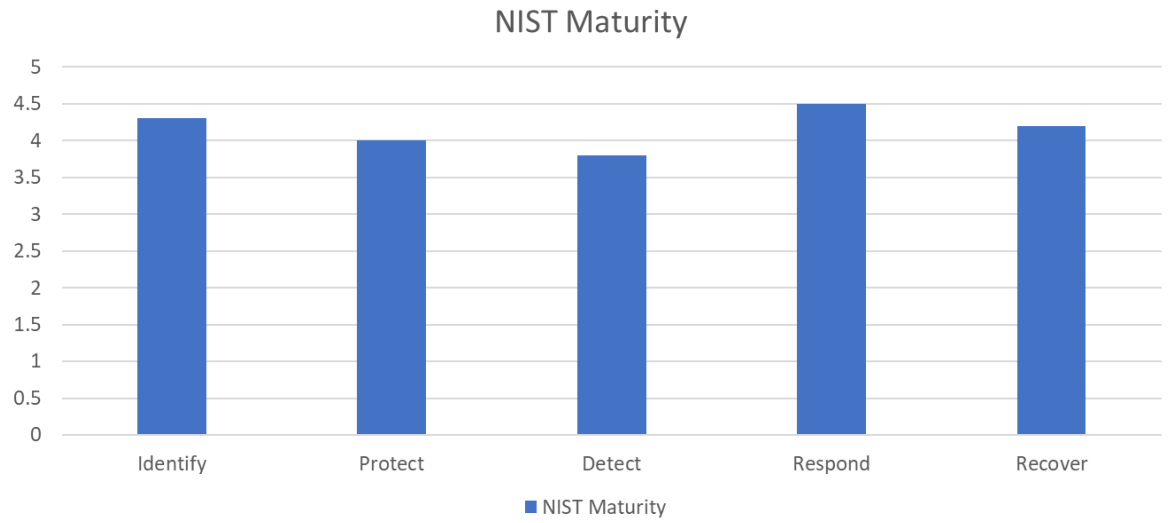




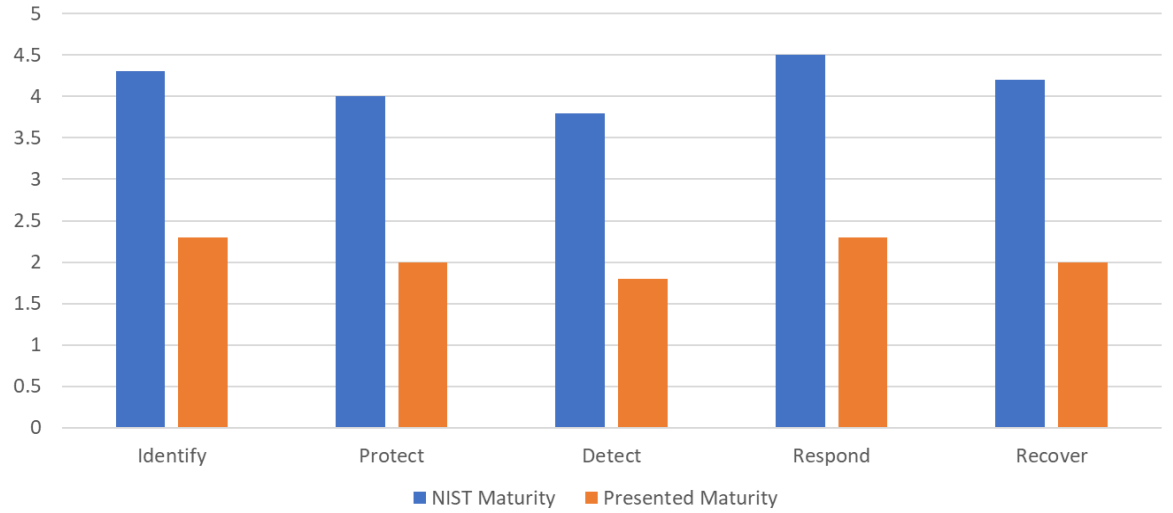


Case study 2 – Making the case for cyber

- Client had a high cyber maturity
- Recommendation to focus uplift efforts on specific, highest priority threats



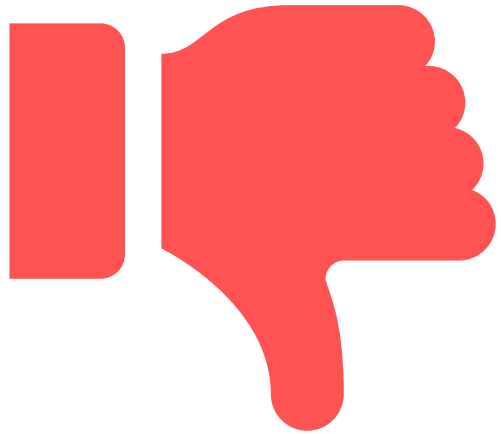
- Client argued for a lower rating
- Used alternate scoring mechanisms to artificially lower their score



Case study 2 – Making the case for cyber

“My Board doesn’t understand cyber. I’ve spent years educating them about NIST, and getting them comfortable with the NIST bars. If I tell them we’re mature against NIST, they won’t fund me anymore.”

Case study 2 – Making the case for cyber



What does good cyber governance look like?

1. Policy
2. Standards
3. Processes
4. Tools

Optional

5. Cybersecurity Strategy
6. Architecture
7. Patterns
8. Controls library

Writing Policy

- An Information Security Policy contains principles for Information Security.
- It defines the intent of the information security function.

Principle	Statement
Confidentiality	Sensitive information is accessible only to those authorized to have access.
Integrity	The accuracy and completeness of information and processing methods is maintained.
Availability	Information and essential services are available to authorised users when needed.
Least privilege	Access privileges and permissions will be assigned according to least privilege.
Risk based	Security controls will be applied commensurate to the risk posed to the business.
Auditability	Actions affecting information are traceable to individuals who can be held responsible.

Writing Standards

- An Information Security Standard contains control statements.
- It defines the requirements that must be met to meet the intent.

Framework	Framework Statement	Company Statement	Standard
NIST CSF: PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected.	Data at rest must be encrypted with approved cryptographic algorithms.	Cryptography
Essential 8: Patch Applications	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.	External-facing assets must be scanned daily.	Vulnerability Management
APRA CPS234: Paragraph 30	An APRA-regulated entity must ensure that testing is conducted by appropriately skilled and functionally independent specialists.	Security controls must be independently tested at least annually.	Security Testing

Case Study 3 – Writing standards

- Writing standards is as much art as it is science.

Framework	Framework Statement	Company Statement	Standard
NIST CSF: PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected.	Data at rest must be encrypted with approved cryptographic algorithms.	Cryptography

Case Study 3 – Writing standards

- Writing standards is as much art as it is science.

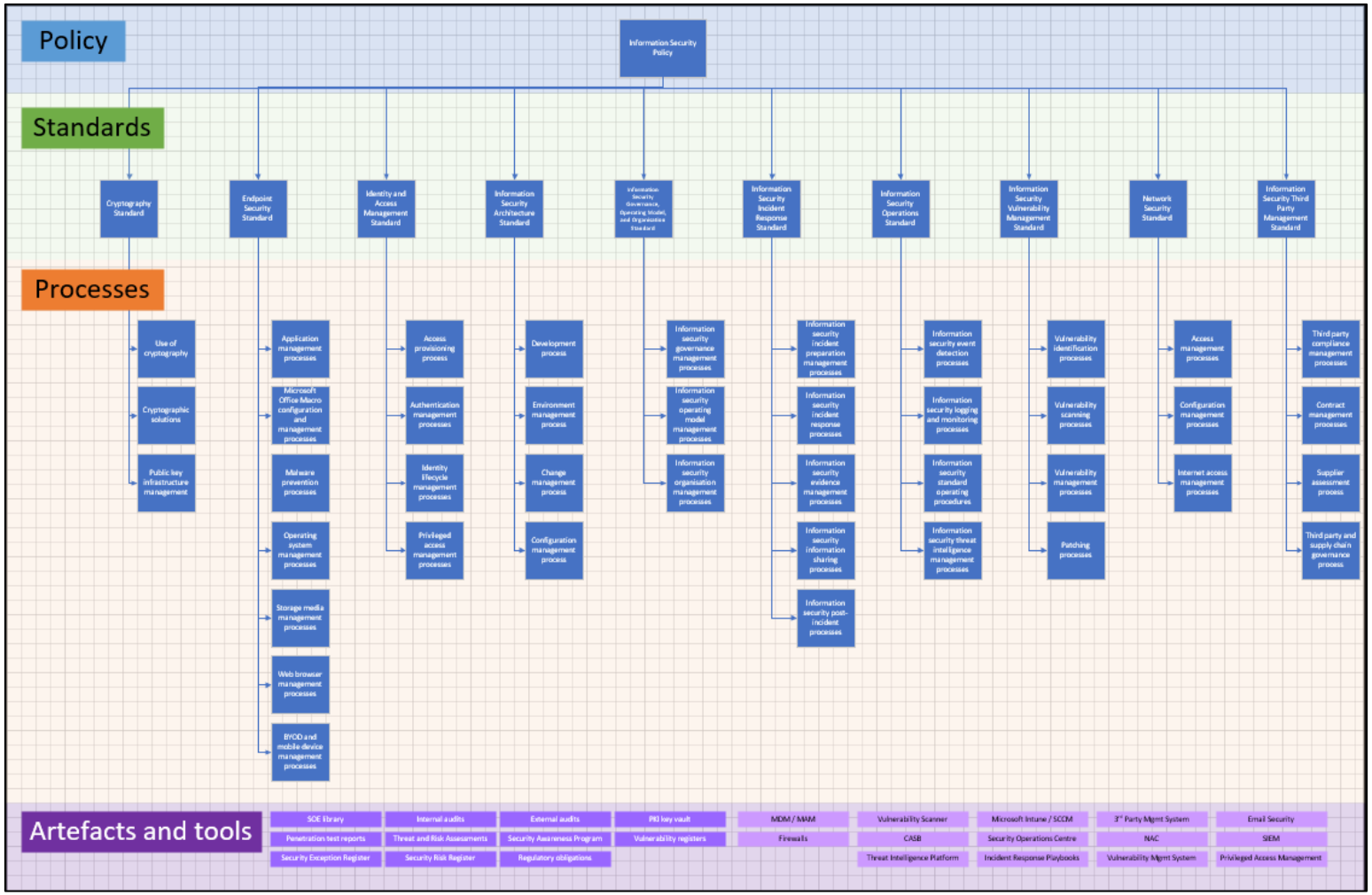
Framework	Framework Statement	Company Statement	Standard
NIST CSF: PR.DS-01	The confidentiality, integrity, and availability of data-at-rest are protected.	All data at rest must be encrypted using the Advanced Encryption Standard (AES) with a key length of 256 bits (AES-256), implemented in either Cipher Block Chaining (CBC) mode or Galois/Counter Mode (GCM). For CBC mode, a unique initialization vector (IV) of 128 bits must be generated using a cryptographically secure random number generator for each encryption operation.	Data Protection

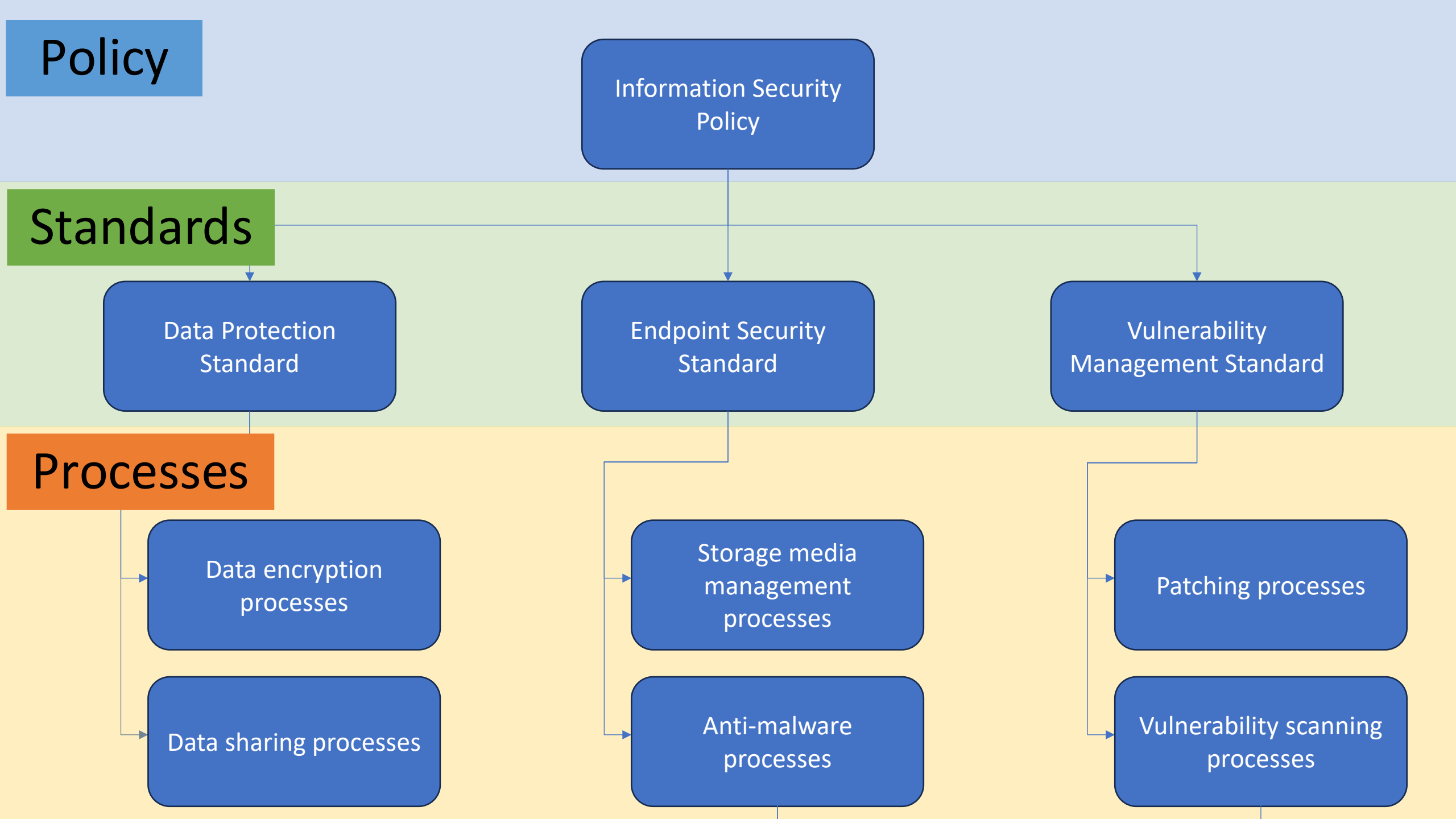
Case Study 3 – Writing standards

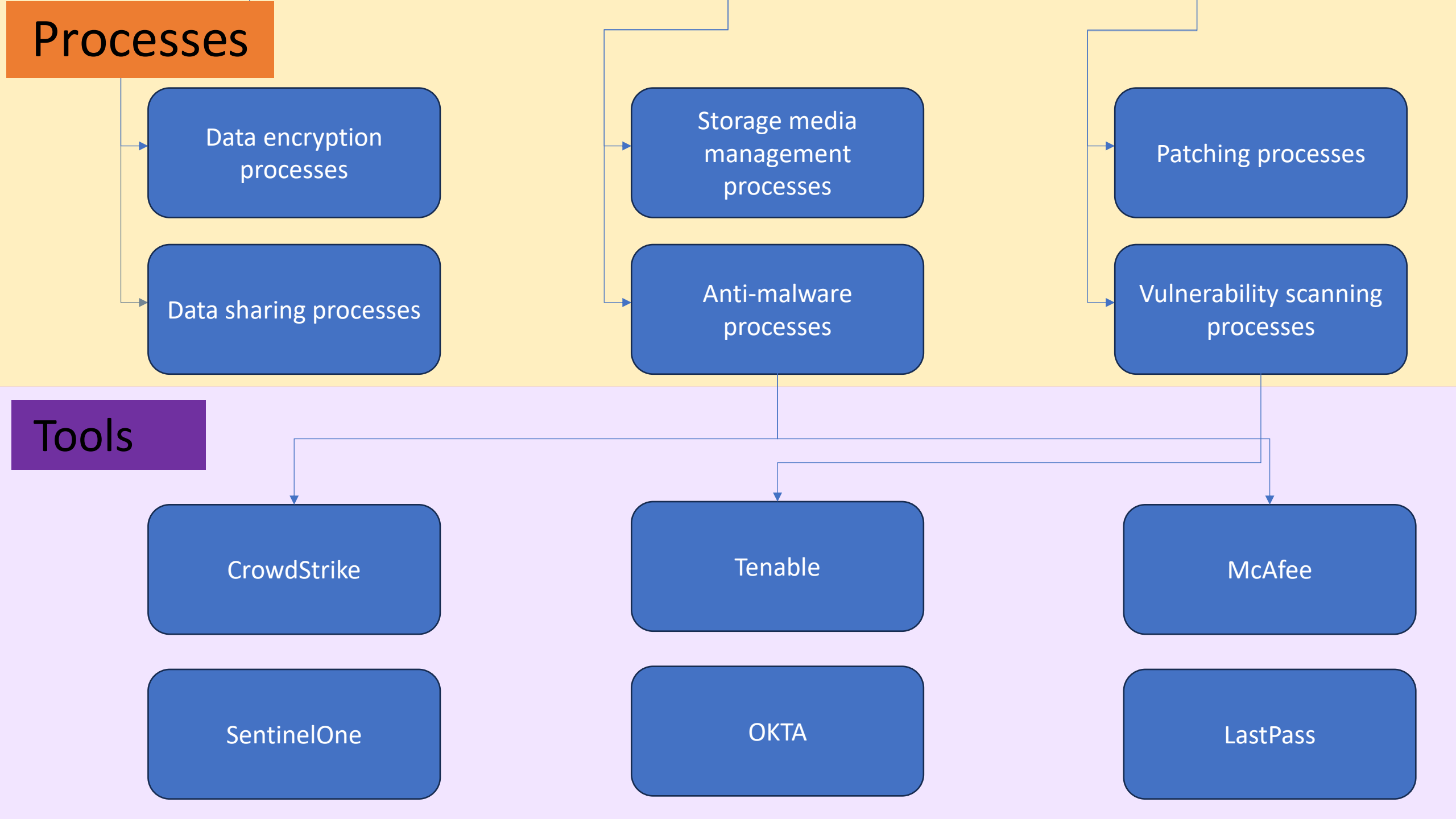
- Writing standards is as much art as it is science.

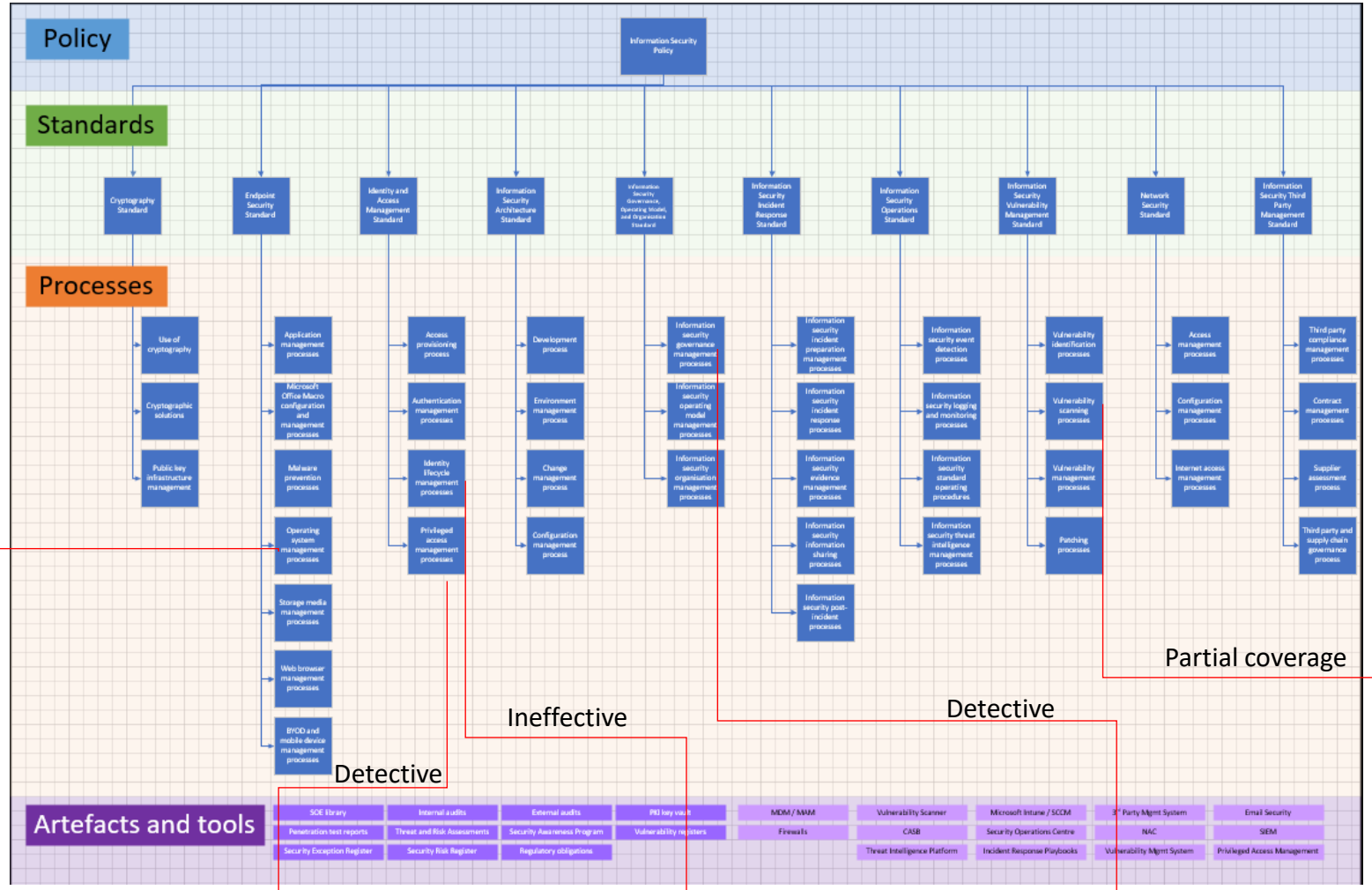
Statement 1	Statement 2
Sensitive data must be encrypted with approved cryptographic algorithms.	All data at rest must be encrypted using the Advanced Encryption Standard (AES) with a key length of 256 bits (AES-256), implemented in either Cipher Block Chaining (CBC) mode or Galois/Counter Mode (GCM). For CBC mode, a unique initialization vector (IV) of 128 bits must be generated using a cryptographically secure random number generator for each encryption operation.

Creating a Cyber Reference Architecture

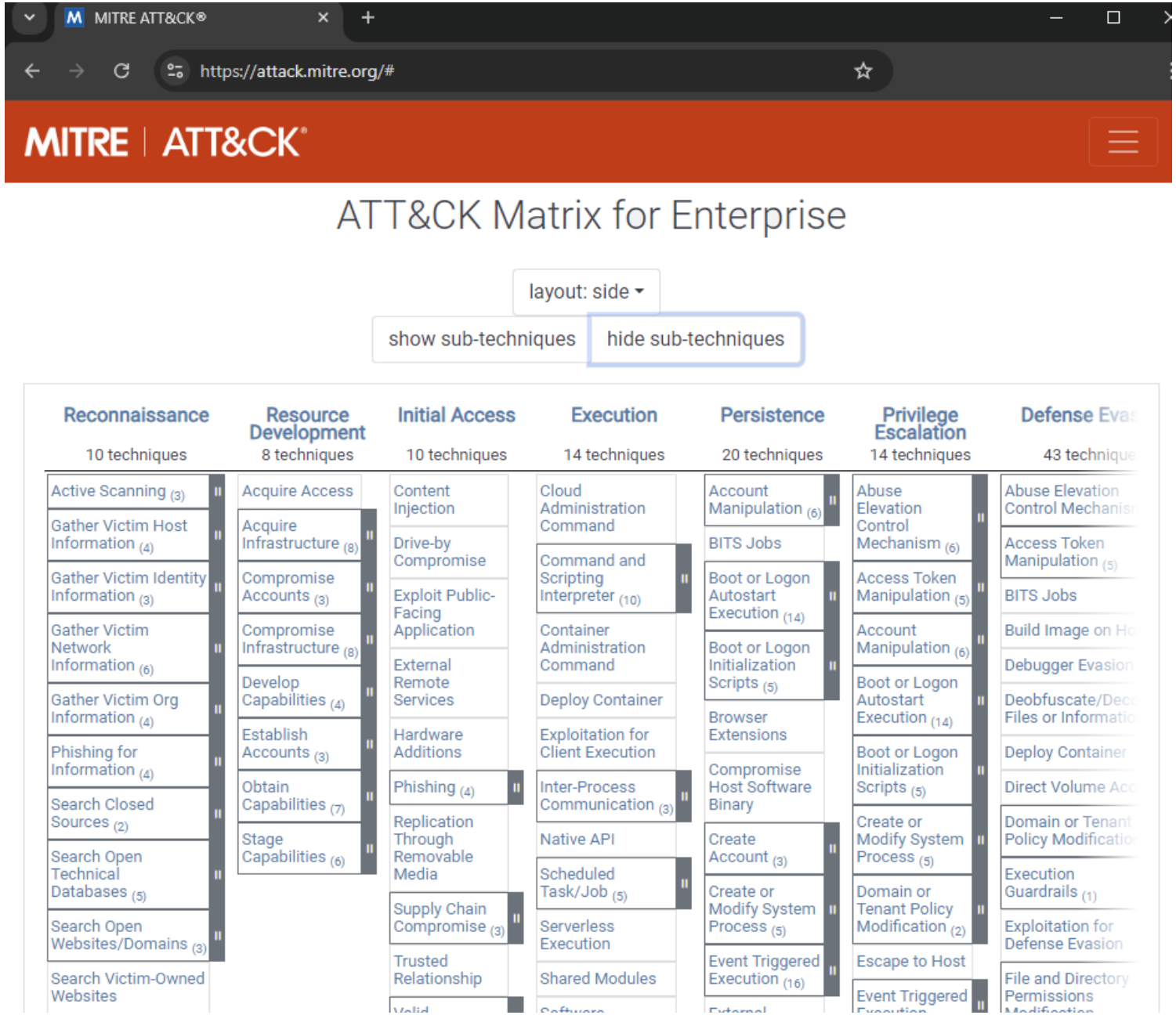


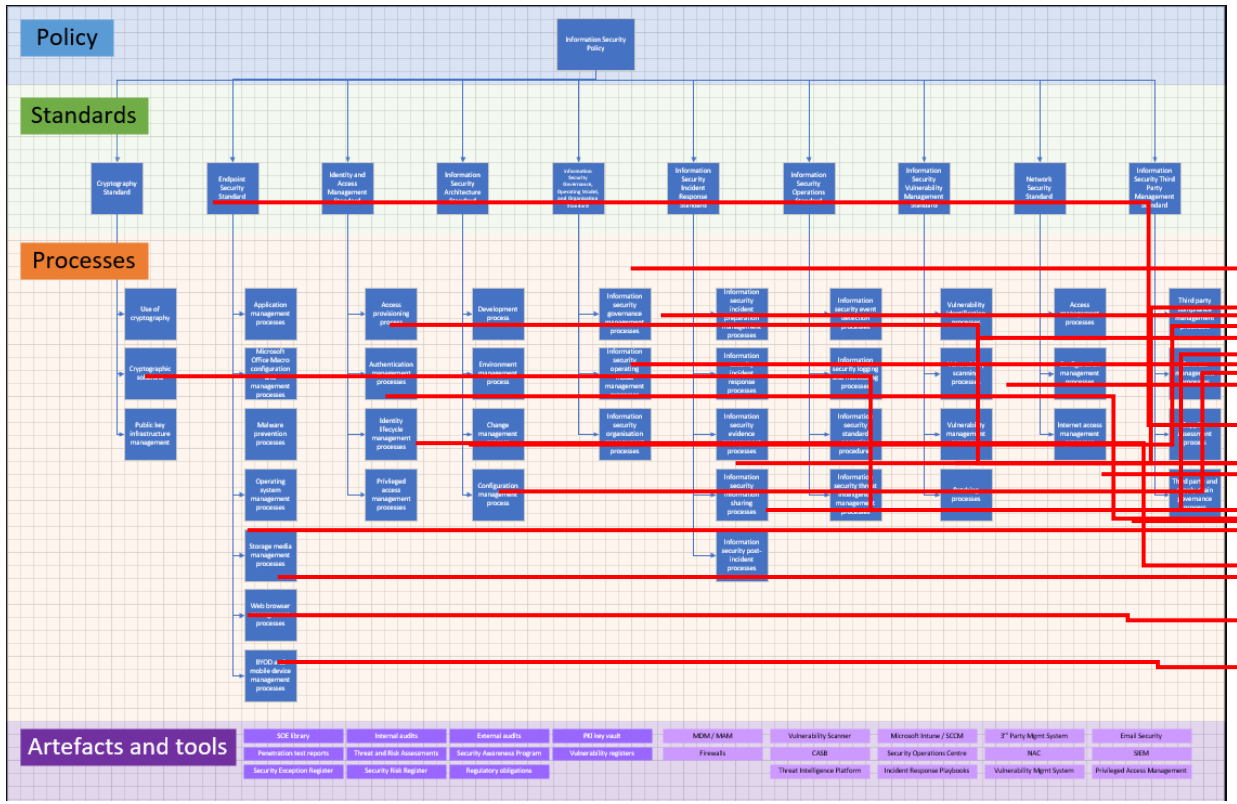

Policy
Information Security Policy
Standards
Data Protection Standard
Endpoint Security Standard
Vulnerability Management Standard
Processes
Data encryption processes
Data sharing processes
Storage media management processes
Anti-malware processes
Patching processes
Vulnerability scanning processes

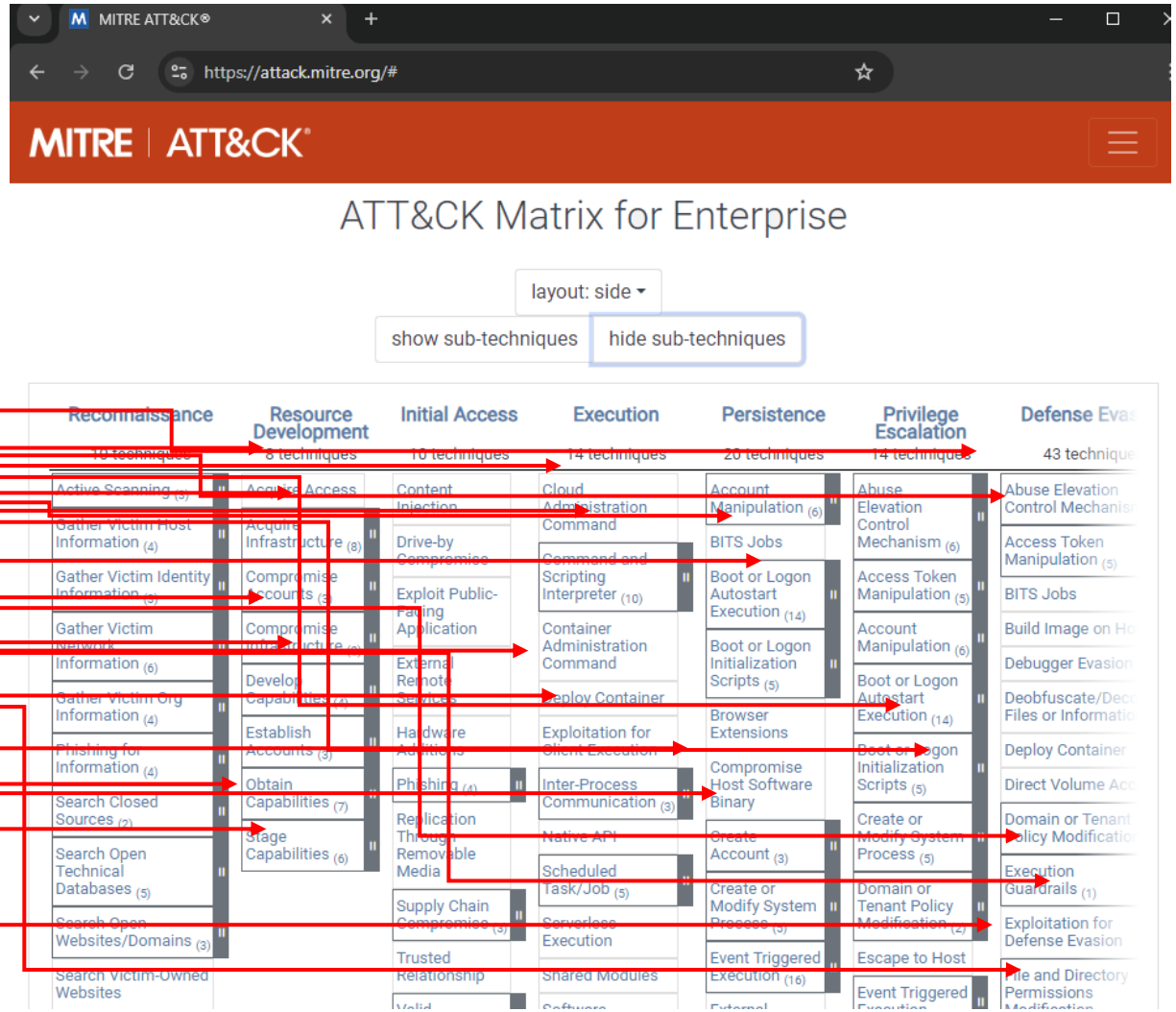

Processes
Data encryption processes
Data sharing processes
Storage media management processes
Anti-malware processes
Patching processes
Vulnerability scanning processes
Tools
CrowdStrike
SentinelOne
Tenable
OKTA
McAfee
LastPass



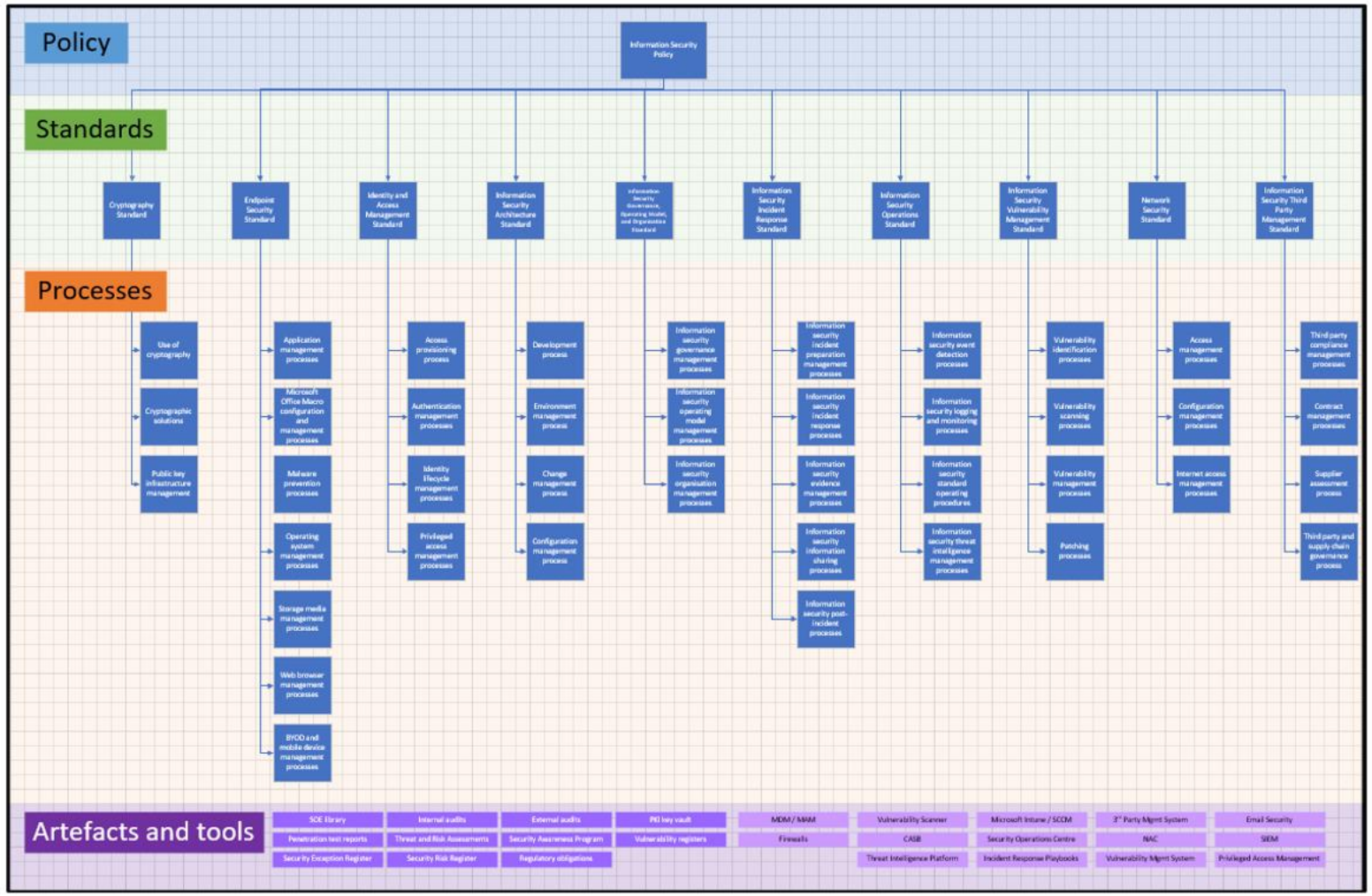
Initial access – Phishing → Persistence – Valid Account → Defence Evasion - Masquerading → Lateral Movement – Remote Services → Exfiltration – Exfiltration over Alternate Protocol


MITRE ATT&CK®
https://attack.mitre.org/#
MITRE | ATT&CK®
ATT&CK Matrix for Enterprise
layout: side
show sub-techniques
hide sub-techniques
Reconnaissance
10 techniques
Active Scanning (3)
Gather Victim Host Information (4)
Gather Victim Identity Information (3)
Gather Victim Network Information (6)
Gather Victim Org Information (4)
Phishing for Information (4)
Search Closed Sources (2)
Search Open Technical Databases (5)
Search Open Websites/Domains (3)
Search Victim-Owned Websites
Resource Development
8 techniques
Acquire Access
Acquire Infrastructure (8)
Compromise Accounts (3)
Compromise Infrastructure (8)
Develop Capabilities (4)
Establish Accounts (3)
Obtain Capabilities (7)
Stage Capabilities (6)
Initial Access
10 techniques
Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing (4)
Replication Through Removable Media
Supply Chain Compromise (3)
Trusted Relationship
Execution
14 techniques
Cloud Administration Command
Command and Scripting Interpreter (10)
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication (3)
Native API
Scheduled Task/Job (5)
Serverless Execution
Shared Modules
Persistence
20 techniques
Account Manipulation (6)
BITS Jobs
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Browser Extensions
Compromise Host Software Binary
Create Account (3)
Create or Modify System Process (5)
Event Triggered Execution (16)
Privilege Escalation
14 techniques
Abuse Elevation Control Mechanism (6)
Access Token Manipulation (5)
Account Manipulation (6)
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Create or Modify System Process (5)
Domain or Tenant Policy Modification (2)
Escape to Host
Defense Eva
43 technique
Abuse Elevation Control Mechanis
Access Token Manipulation (5)
BITS Jobs
Build Image on Ho
Debugger Evasion
Deobfuscate/Dec Files or Informatio
Deploy Container
Direct Volume Acc
Domain or Tenant Policy Modificatio
Execution Guardrails (1)
Exploitation for Defense Evasion
File and Directory Permissions

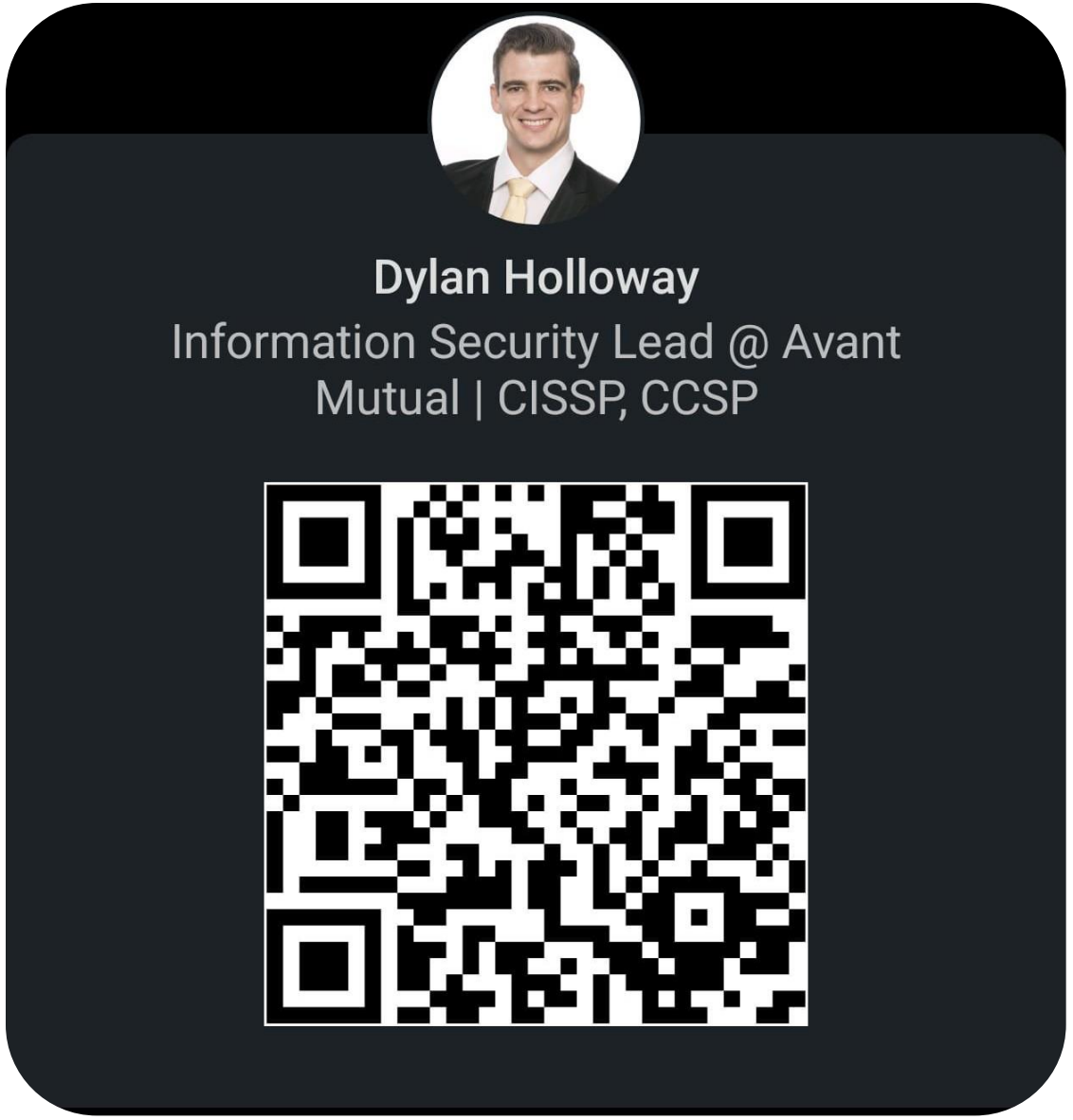

Policy
Standards
Processes
Artefacts and tools


MITRE ATT&CK®
https://attack.mitre.org/#
MITRE | ATT&CK®
ATT&CK Matrix for Enterprise
layout: side
show sub-techniques
hide sub-techniques
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Active Scanning
Gather Victim Host Information
Gather Victim Identity Information
Gather Victim Network Information
Gather Victim Org Information
Phishing for Information
Search Closed Sources
Search Open Technical Databases
Search Open Websites/Domains
Search Victim-Owned Websites
Acquire Access
Acquire Infrastructure
Compromise Accounts
Compromise Infrastructure
Develop Capabilities
Establish Accounts
Obtain Capabilities
Stage Capabilities
Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing
Replication Through Removable Media
Supply Chain Compromise
Trusted Relationship
Valid Accounts
Cloud Administration Command
Command and Scripting Interpreter
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication
Native API
Scheduled Task/Job
Serverless Execution
Shared Modules
Software Deployment Tools
System Services
User Execution
Windows Management Instrumentation
Account Manipulation
BITS Jobs
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Browser Extensions
Compromise Host Software Binary
Create Account
Create or Modify System Process
Event Triggered Execution
External Remote Services
Hijack Execution Flow
Implant Internal Image
Modify Authentication Process
Office Application Startup
Pre-OS Boot
Scheduled Task/Job
Server Software Component
Traffic Signaling
Valid Accounts
Abuse Elevation Control Mechanism
Access Token Manipulation
Account Manipulation
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Create or Modify System Process
Domain or Tenant Policy Modification
Escape to Host
Event Triggered Execution
Abuse Elevation Control Mechanism
Access Token Manipulation
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain or Tenant Policy Modification
Execution Guardrails
Exploitation for Defense Evasion
File and Directory Permissions Modification

Creating a Cyber Reference Architecture



Thank you


Dylan Holloway
Information Security Lead @ Avant Mutual | CISSP, CCSP