Cyber security masterclass

Tuesday 26 November 2019

sasig

Our supporters

SentinelOne™

eset ENJOY SAFER TECHNOLOGY™

LogRhythm™

aruba
a Hewlett Packard Enterprise company

Cognizant

AXIS

Freshfields

FIREEYE™

context

kaspersky

NHS Digital

Reliance acsn
Specialists in IT Security Management

TESSIAN

VARONIS

vodafone

KIER

Forthcoming SASIG events

sasig

Thursday 28th November
Threat Intelligence Webex

Thursday 5th December
SASIG Christmas Networking Lunch

Wednesday 11th December
3rd SASIG Gateway

Friday 10th January
8th SASIG HR

Thursday 16th January
2nd Retailing SASIG

Tuesday 21st January
GDPR: How did you do folks?

View the full calendar
www.thesasig.com/calendar

Peter Goodman QPM, NPCC

Fighting cybercrime - the UK’s evolving capability at the national, regional and local levels

Andrew M, NCSC

NCSC’s role and support for large organisations and Board members.

Tea, coffee & networking break

SASIGEvents

@SASIGEvents

/SASIGevents

Oscar O’Connor, Cognizant Security

Security Technology – making sense of the options

Did you know ?

~24000

Malicious
Mobile Apps are
blocked every

Ransomware attacks to

QUADRUPLE

by 2020

IoT attacks were
up by

600%

In 2018

400,000+

NEW Malware daily

75% of attacks

occur at **application**
level

55% of incidents

are caused by misuse of
privileged accounts

NEW Malicious Website
appears every

<2 seconds

NotPetya

Merck $870m

FedEx $400m

Saint Gobain $384m

Maersk $300m

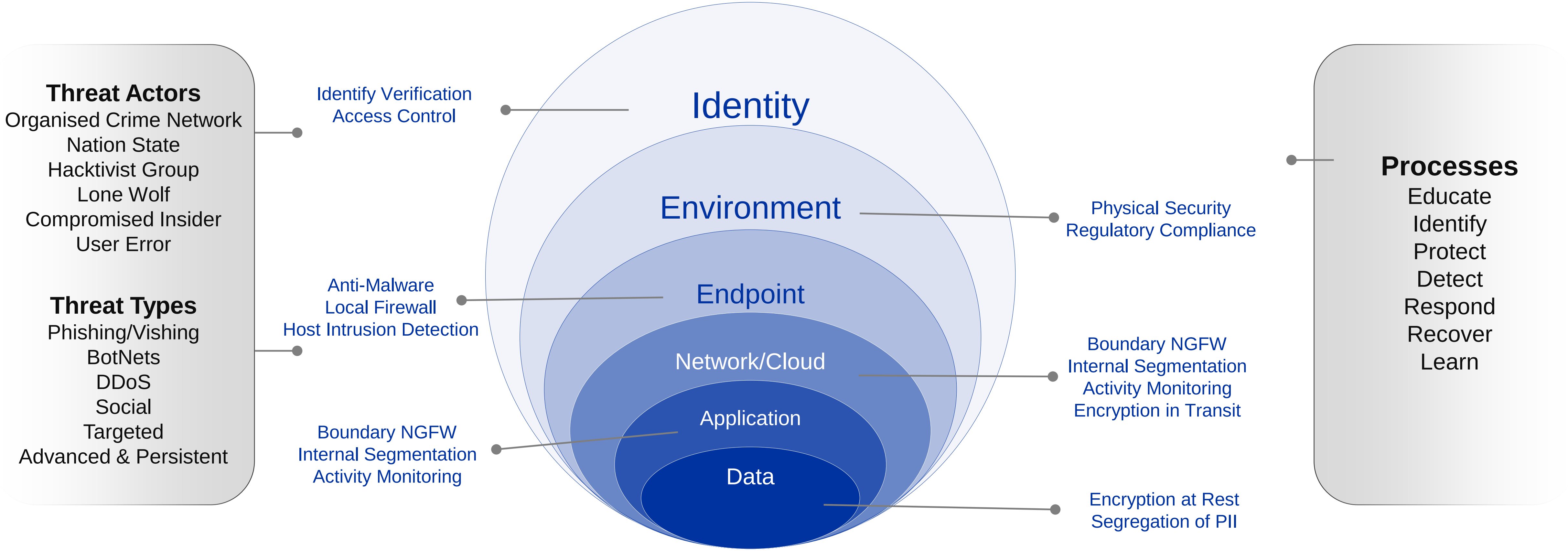
Mondelez $188m

Reckitt Benckiser $129m

Total reported cost >$4bn

Where security technology fits

Statutory, Regulatory & Compliance Issues



Threat Actors
Organised Crime Network
Nation State
Hacktivist Group
Lone Wolf
Compromised Insider
User Error

Threat Types
Phishing/Vishing
BotNets
DDoS
Social
Targeted
Advanced & Persistent

Identity
Identify Verification
Access Control

Environment
Physical Security
Regulatory Compliance

Endpoint
Anti-Malware
Local Firewall
Host Intrusion Detection

Network/Cloud
Boundary NGFW
Internal Segmentation
Activity Monitoring
Encryption in Transit

Application
Boundary NGFW
Internal Segmentation
Activity Monitoring

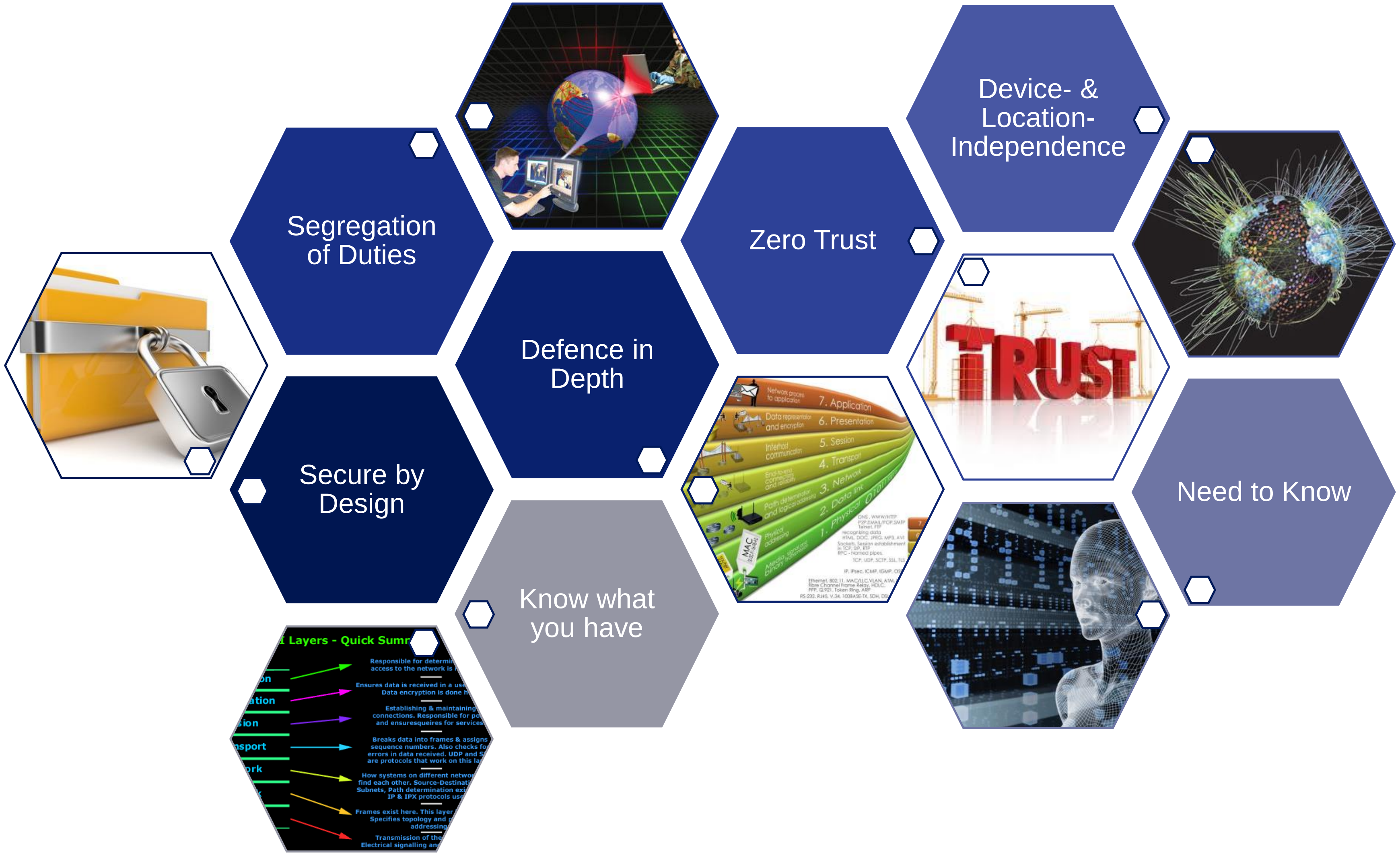
Data
Encryption at Rest
Segregation of PII

Processes
Educate
Identify
Protect
Detect
Respond
Recover
Learn

ANALYTICS

System Behaviour – Access Attempts – Data Movements – Service Quality – Attempted Attacks
GOAL: Separate the normal from the anomalous and investigate in real-time

What technology delivers



Segregation of Duties

Defence in Depth

Secure by Design

Know what you have

Zero Trust

Device- & Location-Independence

Need to Know

Cognizant Security Simplified
– The Golden Thread through IT and business

Ingest

Cognizant manage and integrates the security solution components with

Correlate

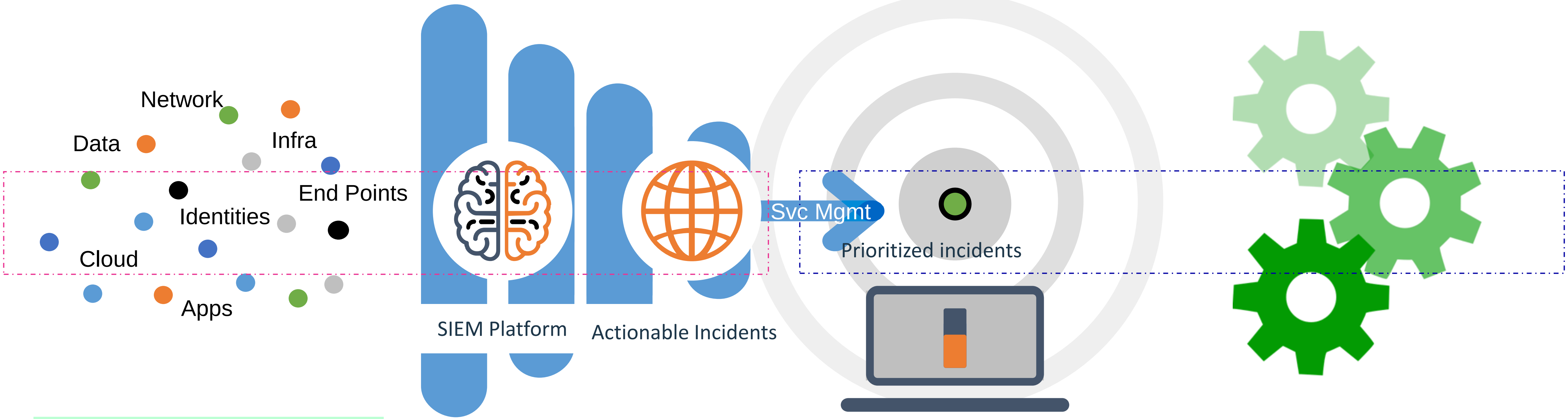
Performs correlation, fine-tune to reduce noise, monitor for threats and potential cyber attacks

Prioritize

Cognizant capture & classify threats for faster response

Orchestrate & Respond

Cognizant integrates the solution components for workflow automation



WELL EXECUTED, INTEGRATED

ACTIONABLE

BUSINESS RELEVANT USE CASES

RESPOND (MACHINE + HUMAN)

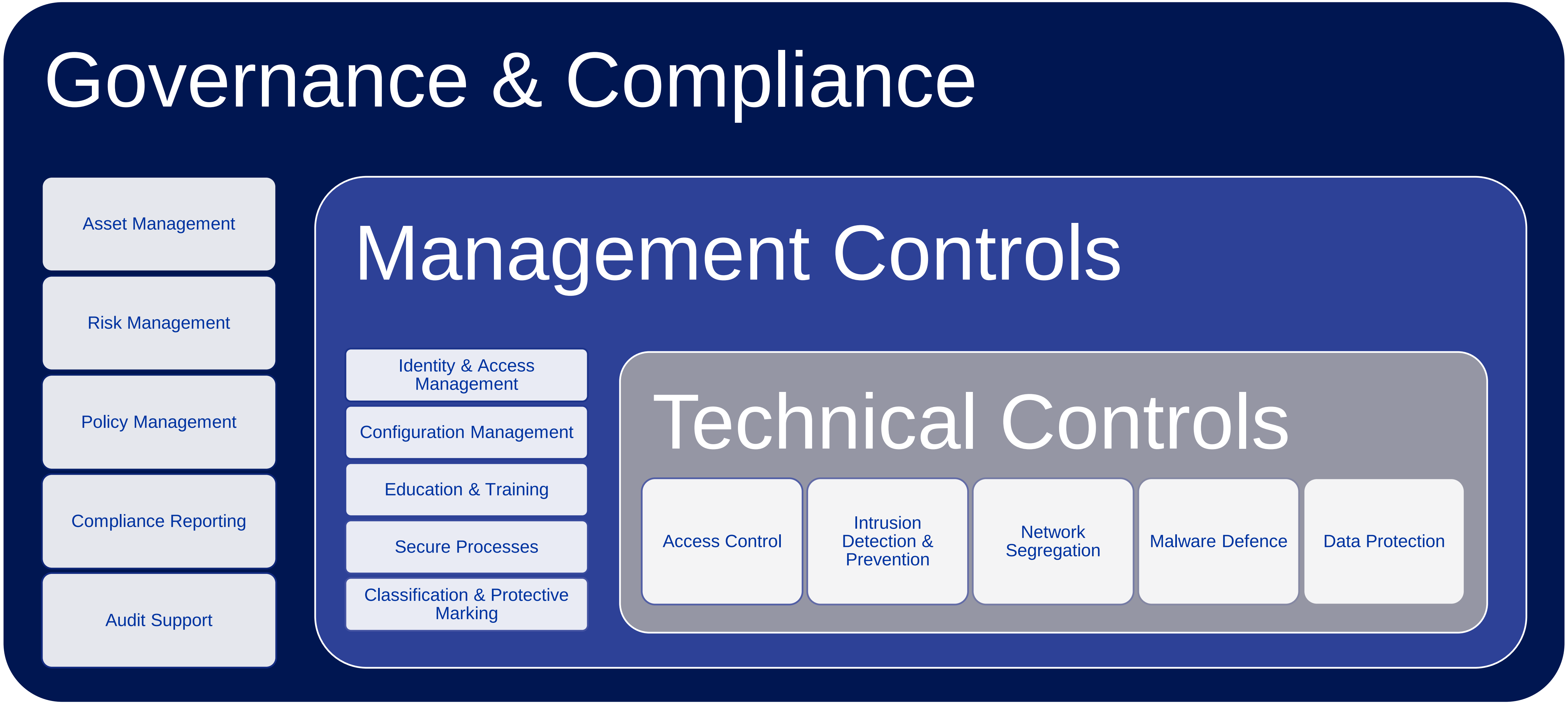
Manage

Cognizant performs Lot5 tasks to manage the in-scope security devices

Cognizant vision is to **integrate** security components for better incident response workflow, **automate,** and ensure that the **business is secure** from known attack vectors

Cognizant Security

What makes a solid foundation?



Governance & Compliance

- Asset Management
- Risk Management
- Policy Management
- Compliance Reporting
- Audit Support

Management Controls

- Identity & Access Management
- Configuration Management
- Education & Training
- Secure Processes
- Classification & Protective Marking

Technical Controls

- Access Control
- Intrusion Detection & Prevention
- Network Segregation
- Malware Defence
- Data Protection

Thank you

Jonathan Lloyd-White,
International Airlines Group

Reaching the boardroom with meaningful metric

Cyber Dashboard | Summary

Identify

- This panel tracks **Risks and Compliance**;
- Risk management - internal controls vs external threats;
- Summary of compliance - standards and regulations;
- Medium to long term - movements happening over quarters, not months
- Group view rather than by business unit.

Protect

- This panel shows current **Control Effectiveness**
- Performance of key controls against leading tolerance measures;
- Short term view - movements happening from month to month;
- There is likely to be a mix of Group and business unit metrics.

Detect, Respond, Recover

- This panel tracks live **Operations and Incidents**;
- Lag indications of control effectiveness – shows where attacks have happened and their seriousness;
- Generated by the Security Operations Centre;
- Dynamic - summarises changes that can happen on an hour by hour or daily basis over the month;
- There will be a mix of Group and business unit metrics.

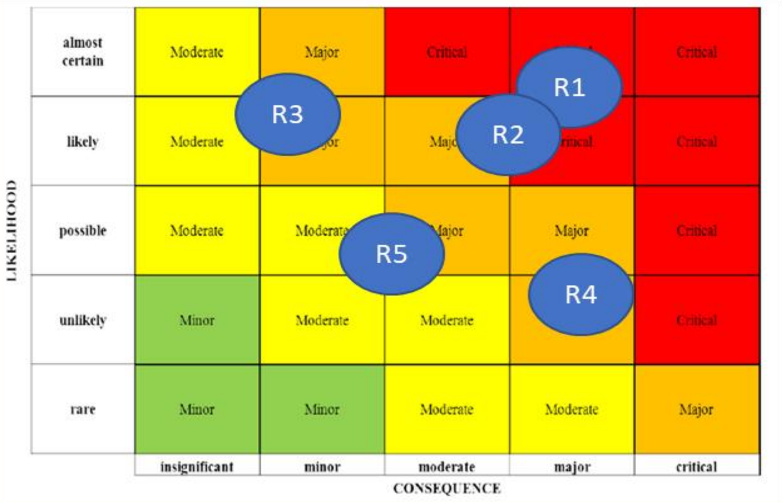
Invest

- This panel shows how **Investment** is improving the maturity of the organisation;
- Tracks projects - how they are reducing the risks, improving controls and decreasing the damage from attacks;
- Long-term view - movements happening over months and years;
- It will predominantly show cross-Group activity.

Cyber Dashboard | Example

[ILLUSTRATIVE]

Identify



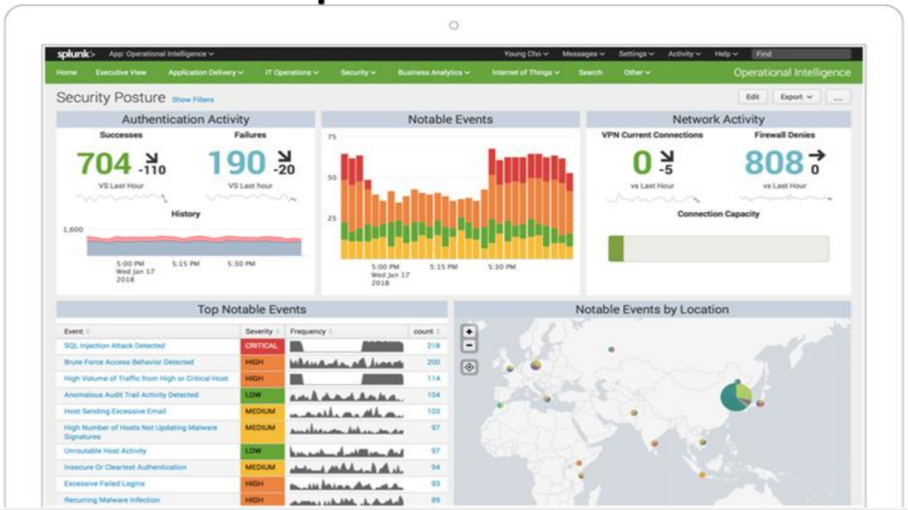
PCI	Unit A	🟥
	Unit B	🟧
	Unit C	🟩
	Unit D	🟥
NIS-D	Unit A	🟩
	Unit B	🟧
	Unit C	🟩
	Unit D	🟥

Text on monthly highlights and movements

Protect

Risk	Control	Description	Red	Amber	Green	Trend	Previous Month	Current Month
Risk 1	Control 1.1	AV	<70	70-94	>95	⬇	🟥	🟧
	Control 1.2	EndPoint	<70	70-94	>95	➡	🟧	🟧
	Control 1.3	Patching	<70	70-94	>95	⬇	🟥	🟩
Risk 2	Control 2.1	Phishing Test	<70	70-94	>95	➡	🟩	🟩
	Control 2.2	Training	<70	70-94	>95	⬇	🟧	🟩
	Control 2.3	Events	<70	70-94	>95	➡	🟩	🟩
Risk 3	Control 3.1	DLP	<70	70-94	>95	⬆	🟧	🟥
	Control 3.2	Reviews	<70	70-94	>95	⬆	🟩	🟧
	Control 3.3	Reports	<70	70-94	>95	➡	🟩	🟩
	Control 3.4	Devices	<70	70-94	>95	⬇	🟥	🟩
Risk 4	Control 4.1	Incidents	<70	70-94	>95	➡	🟩	🟩
	Control 4.2	Alerts	<70	70-94	>95	➡	🟧	🟧
	Control 4.3	Losses	<70	70-94	>95	⬆	🟩	🟥
	Control 4.4	Customers	<70	70-94	>95	⬆	🟧	🟥

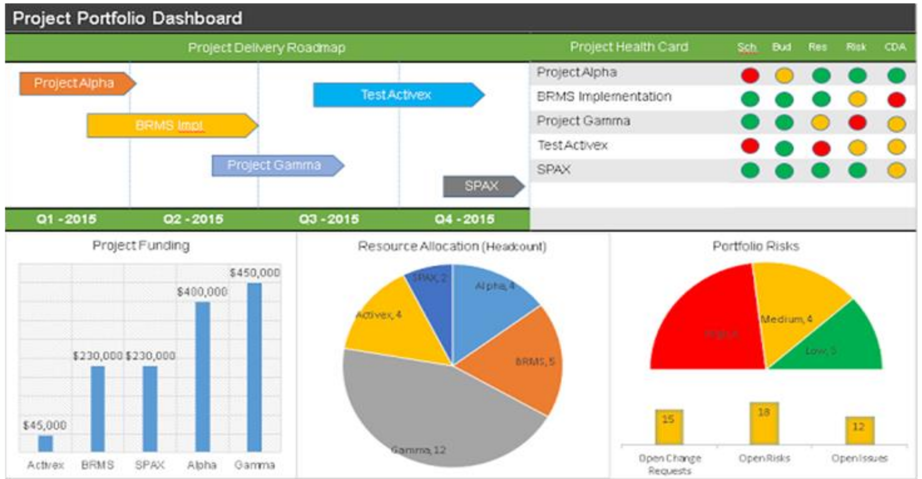
Detect Respond Recover



Event	Severity	Frequency	count
SQL Injection Attack Detected	CRITICAL		218
Brute Force Access Behavior Detected	HIGH		200
High Volume of Traffic from High or Critical Host	HIGH		114
Anomalous Audit Trail Activity Detected	LOW		104
Host Sending Excessive Email	MEDIUM		103
High Number of Hosts Not Updating Malware Signatures	MEDIUM		97
Unroutable Host Activity	LOW		97
Insecure Or Cleartext Authentication	MEDIUM		94
Excessive Failed Logins	HIGH		93
Recurring Malware Infection	HIGH		89

- Highlight key incidents and actions
- Note points for each OpCo

Invest

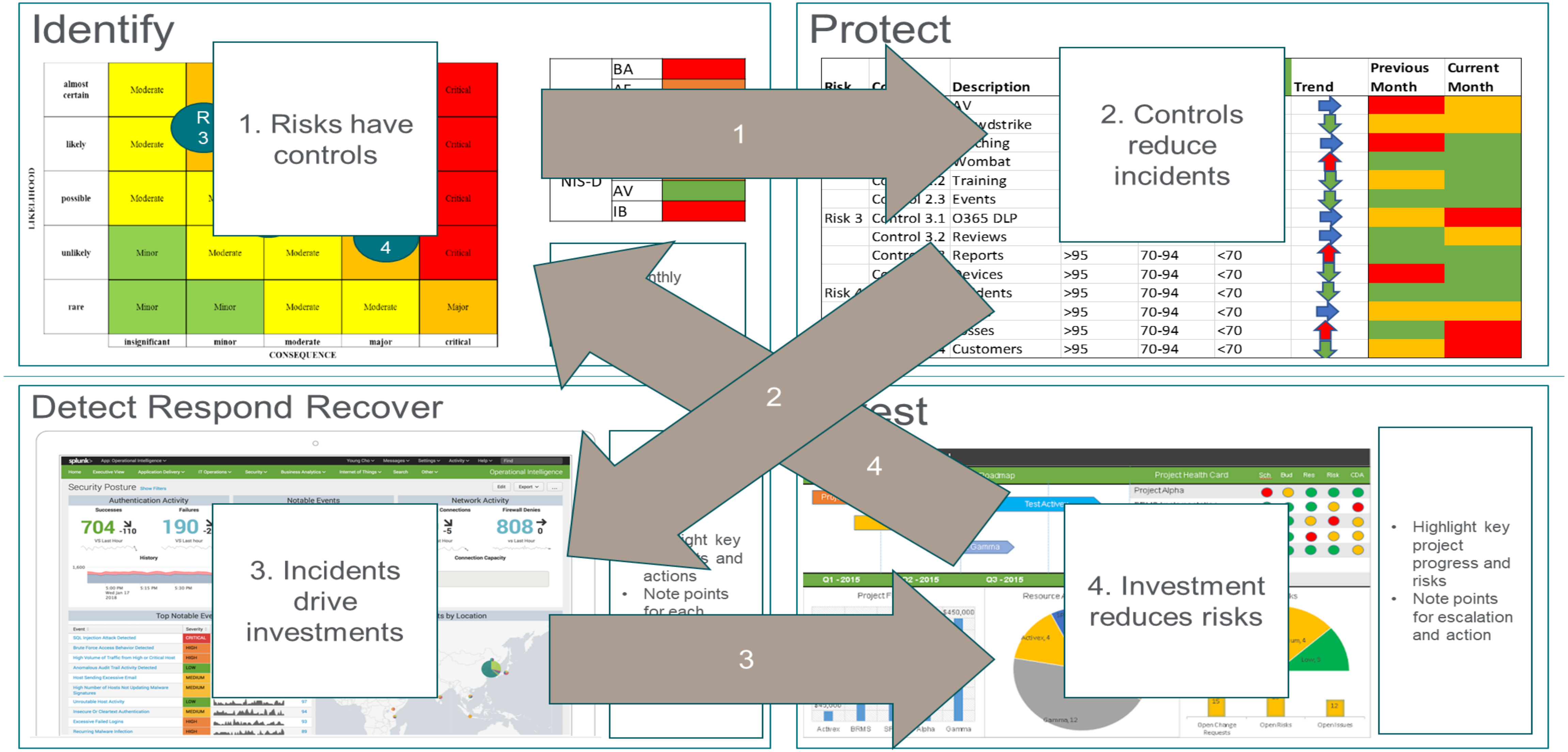


Project Health Card	Sch	Bud	Res	Risk	CDA
Project Alpha	🔴	🟡	🟢	🟢	🟢
BRMS Implementation	🟢	🟢	🟢	🟡	🔴
Project Gamma	🟢	🟢	🟡	🔴	🟡
Test Activex	🔴	🟢	🔴	🟡	🟡
SPAX	🟢	🟢	🟢	🟢	🟡

- Highlight key project progress and risks
- Note points for escalation and action

Cyber Dashboard | Driving Decisions

[ILLUSTRATIVE]



1. Risks have controls

2. Controls reduce incidents

3. Incidents drive investments

4. Investment reduces risks

- Highlight key project progress and risks
- Note points for escalation and action

IAGTech

Hints & Tips

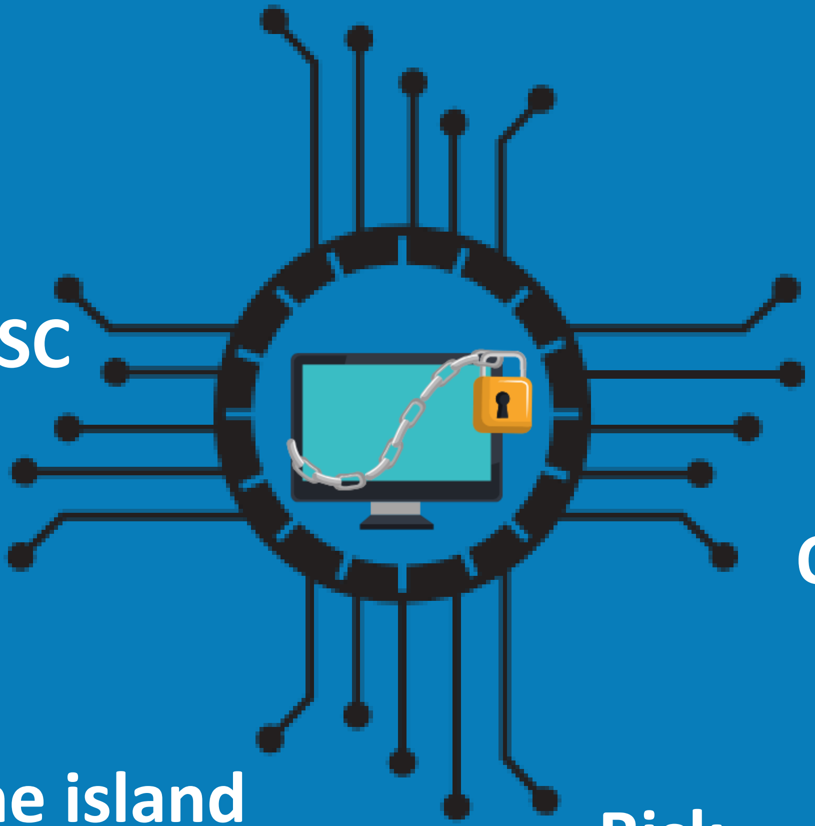
- Use the dashboard, don’t let it use you
- Use the same dashboard structure throughout your governance
- Use it to help structure your agenda over the course of a year (timing is everything)
- Tolerance discussions can be really powerful
- Don’t wait until it’s all in place – it will never be finished
- Keep a strong visual link between risks, controls and investment
- Remember to translate - it’s all about the stories

Denis Philippe,

Jersey Financial Services Commission

Cybersecurity – the view from the Regulator

Agenda



Things to be doing

What's coming

Inside the JFSC

Outlook

Industry and the island

Risk

Cyber-security mission statement

> JFSC held information[1], in all its forms, written, recorded electronically or printed, will be protected from accidental or intentional unauthorized access, modification, or destruction throughout its life cycle.

[1] This includes all information created or owned by the JFSC as well as information collected by or provided to the JFSC by external parties for the execution of the JFSC's activities.

8 security reports from industry

JFSC assisting industry on 4 events / incidents

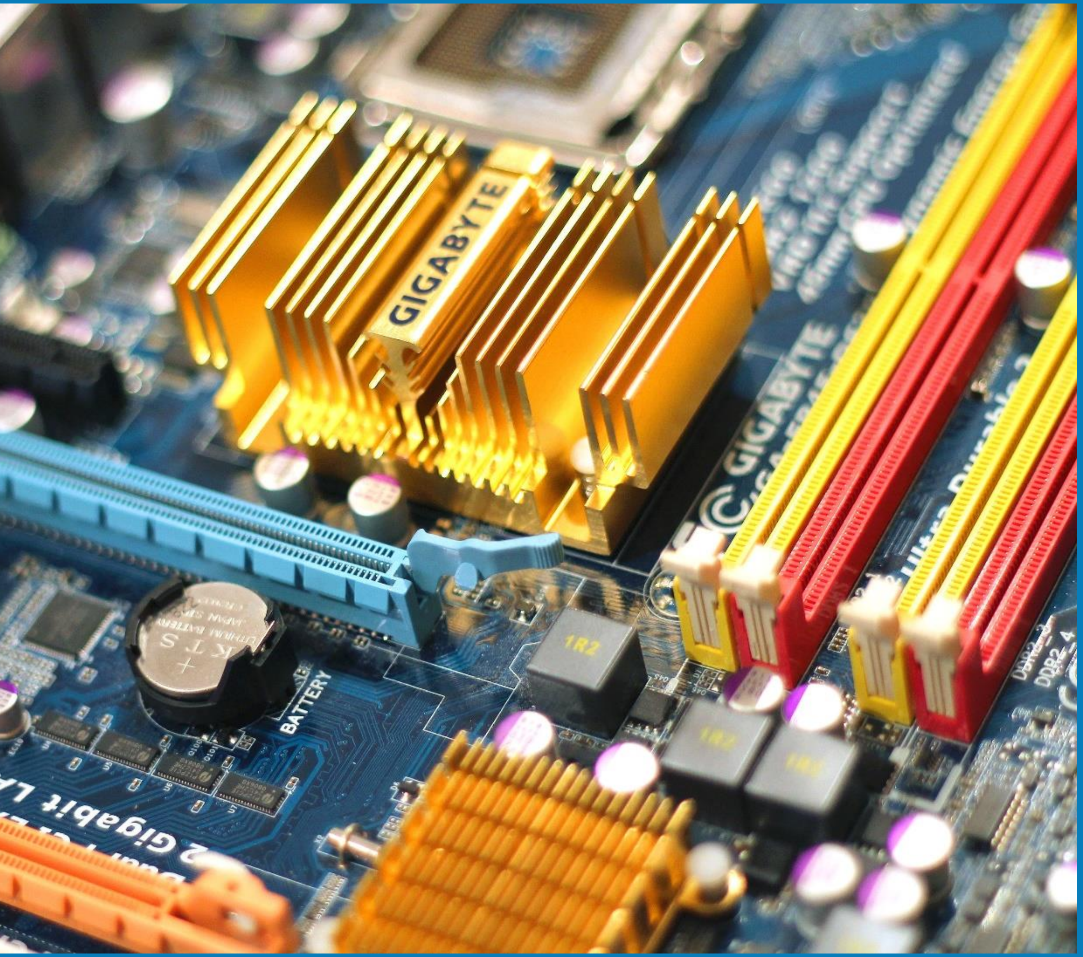
3 engagements via CiSP

9 industry on-site visits

20 banking sector questionnaire responses

Inside the JFSC

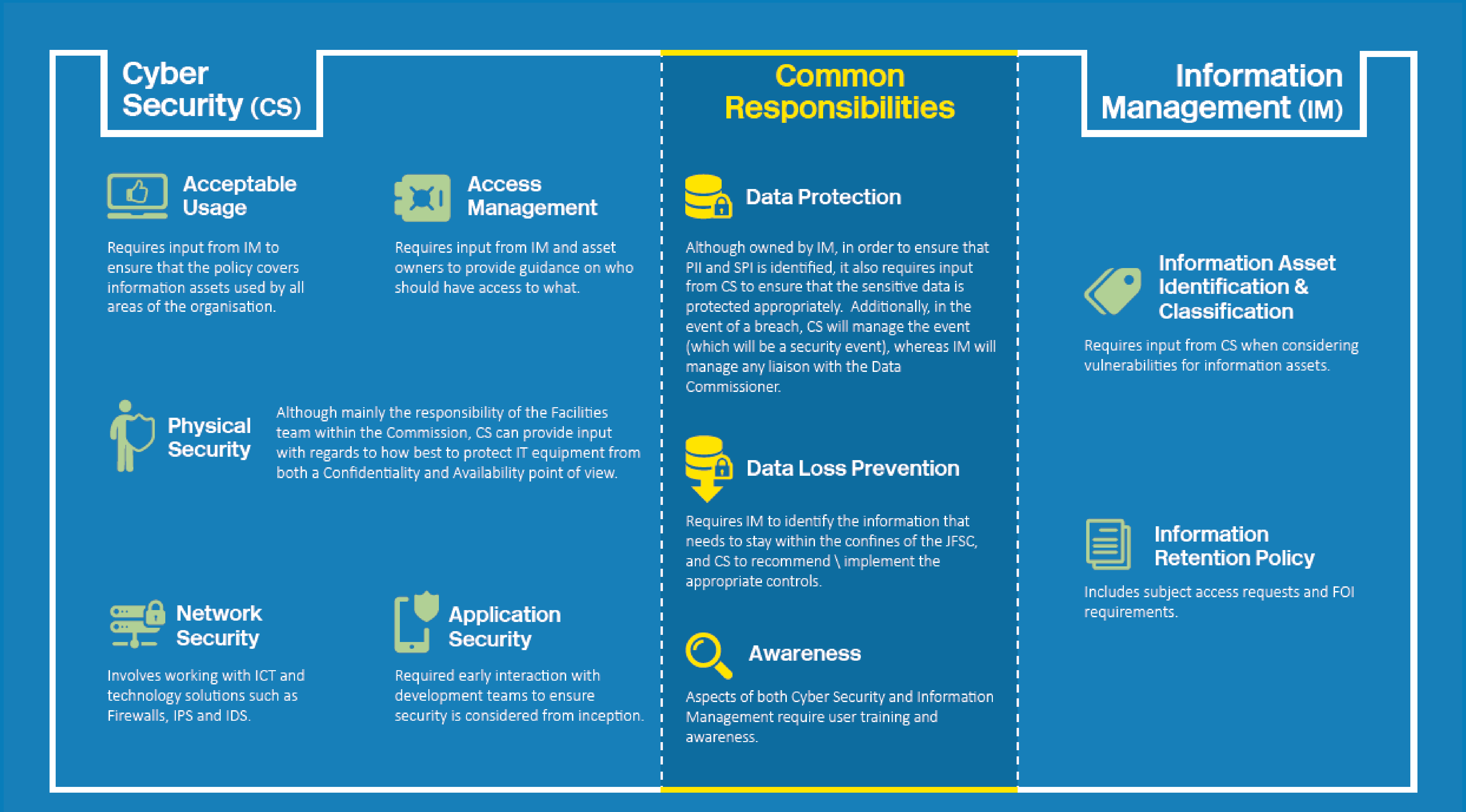
Information security at the JFSC



- Making our transformation programme a security opportunity
- Ensuring our people are part of our defence
- Phishing – do it well, don’t shame people
- Evolving security programme, it doesn’t stop
- Information management and information security – you can’t protect what you don’t know (without burning money!)
- Entering the cloud
- Continuous systems testing
  - Manual, automated, independent, audit

InfoSec (cyber) and info management

› Separate but collaboration between information security and information management



Cyber Security (CS)

Acceptable Usage

Requires input from IM to ensure that the policy covers information assets used by all areas of the organisation.

Access Management

Requires input from IM and asset owners to provide guidance on who should have access to what.

Physical Security

Although mainly the responsibility of the Facilities team within the Commission, CS can provide input with regards to how best to protect IT equipment from both a Confidentiality and Availability point of view.

Network Security

Involves working with ICT and technology solutions such as Firewalls, IPS and IDS.

Application Security

Required early interaction with development teams to ensure security is considered from inception.

Common Responsibilities

Data Protection

Although owned by IM, in order to ensure that PII and SPI is identified, it also requires input from CS to ensure that the sensitive data is protected appropriately. Additionally, in the event of a breach, CS will manage the event (which will be a security event), whereas IM will manage any liaison with the Data Commissioner.

Data Loss Prevention

Requires IM to identify the information that needs to stay within the confines of the JFSC, and CS to recommend \ implement the appropriate controls.

Awareness

Aspects of both Cyber Security and Information Management require user training and awareness.

Information Management (IM)

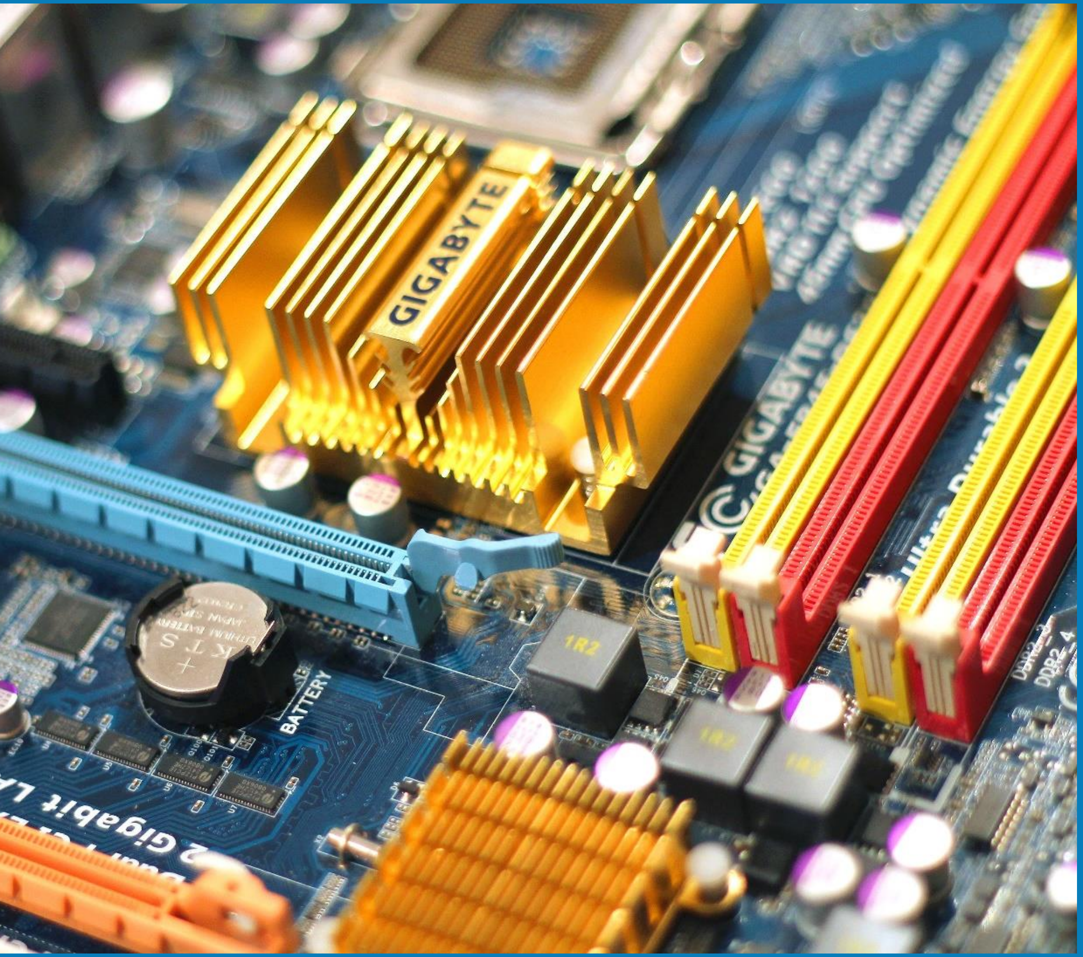
Information Asset Identification & Classification

Requires input from CS when considering vulnerabilities for information assets.

Information Retention Policy

Includes subject access requests and FOI requirements.

Information security at the JFSC



- Making our transformation programme a security opportunity
- Ensuring our people are part of our defence
- Phishing – do it well, don’t shame people
- Evolving security programme, it doesn’t stop
- Information management and information security – you can’t protect what you don’t know (without burning money!)
- Entering the cloud
- Continuous systems testing
  - Manual, automated, independent, audit

What's changing?

- Extensive estate of technical controls
- Additional appointment of an infrastructure specialist
- Continual investment in team training and awareness
- Innovation in the field of solution security
- Full support of the Commission Board and Executive on the investment in security

Security baked in

- Striving to improve the security of the online services we offer
- Working with leading advisors to ensure best possible levels of security and innovation
- New approaches to solution security as seen with the Beneficial Ownership Register and how we provide real time access for law enforcement and other agencies
- Range of advanced security measures to protect PII filed with the Companies Registry - soon to be published.

Looking forward

- We will continue to invest in protecting the information that industry provides us with
- We will extend our systems and security measures as we embraces modern technology services
- We are looking to create a dedicated Cyber Risk team

Industry and the island

Industry – our expectations

- Boards should have a member who is responsible for cyber risk
- Governance should be in place
- You should have a cyber-strategy that is aligned to the business
- Good management information should be relayed through hierarchy to Board
- Have conversations about cyber risk and look at a programme of culture that addresses cyber risk
- We are looking for risk flags, but are not telling you *how* to do it
- Engage with us

Industry risk management

- The Codes of Practice require that registered persons understand and appropriately manage the risks that could affect their business or customers
- **This includes Information Security risk**

Supervisors on-site

Developed an internal toolkit allowing supervisors to examine some of the more technical areas in more detail when on-site.

Your supervisor will be talking to you about:

- How your leaders are directing and supporting activities related to information security
- What policies, procedures and guidance you have in place around information security
- What elements of information security have been included on your risk assessments and how those risks are treated
- How you are promoting training and awareness within your organisation
- How you are monitoring and managing any third parties or suppliers who have access to your information or systems

JFSC participation

Government of JERSEY

Cyber Security Taskforce

JERSEY FRAUD PREVENTION FORUM

Community

- Flexibility and collaboration are key
- Improved intelligence will improve detection
- Understand the landscape threats
- Join, learn, contribute, improve
- JFSC can sponsor/support membership of CiSP

CiSP
Cyber-security Information Sharing Partnership

sasig

CIISF
CHANNEL ISLANDS INFORMATION SECURITY FORUM

Risk

What keeps you up at night?

- People
- Suppliers
- Unclassified data
- Data submissions from industry
- Mobile devices in a mobile workforce.

Sleep easy trying…

People

- Make it easy to do their job
- Make it hard for them to be compromised

Education

- Building the default skillsets of the future
- Keeping people engaged while keeping them aware

What next?

Outlook

- AI and automation - key player, offensive and defensive. Bad guys use it so you should consider it. Time to attack from vulnerability identification will rapidly decrease
- Supply chain attacks will continue to increase across hardware and software. Don’t forget IoT!
- Skills shortage from InfoSec professionals will continue
  - Alternative resourcing approach, grow your own, diversity, cross skill transfer.

Outlook (continued)

Need for smarter training and awareness to mitigate cyber fatigue:

- Deep fakes (voice faking, video and image manipulation) and targeted social engineering
- User behavioural analytics – spotting things early. Post resignation hot spot, review months prior to resignation using security log data (Dawn Cappelli)
- Incident response planning and most importantly practiced!

Things to be doing

- DMARC
- Mandatory TLS for email
- Practice incident response
- Supply chain risk management
- Security monitoring – have visibility of your data estate

Don’t forget to PATCH

Denis Philippe
d.philippe@jerseyfsc.org

Q&A

Lunch & networking break

SASIGEvents

@SASIGEvents

/SASIGevents

sasig

Peter Yapp,
Schillings International LLP

Managing Supply Chain Security

Jonathan Spilky

Account Executive, Tessian

Why the threat of phishing can’t be ‘trained away’

Paul Berriff OBE,
Producer, Director,
Cinematographer and Fine Arts Photographer

9/11 - A First-Hand Experience

Panel and Q&A Session

Thank you

Jersey Financial Services Commission

sasig