Cyber security masterclass
Tuesday 26 November 2019
Our supporters
Forthcoming SASIG events

**Thursday 28th November**
Threat Intelligence Webex

**Thursday 5th December**
SASIG Christmas Networking Lunch

**Wednesday 11th December**
3\(^{rd}\) SASIG Gateway

**Friday 10th January**
8th SASIG HR

**Thursday 16th January**
2\(^{nd}\) 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
NCSC’s role and support for large organisations and Board members.

Andrew M, NCSC
Tea, coffee & networking break
Oscar O’Connor, Cognizant Security

Security Technology – making sense of the options
Did you know?

~24000 Malicious Mobile Apps are blocked every day.

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
- Anti-Malware
- Local Firewall
- Host Intrusion Detection

Endpoint
- Boundary NGFW
- Internal Segmentation
- Activity Monitoring

Network/Cloud
- Boundary NGFW
- Internal Segmentation
- Activity Monitoring

Application
- Encryption in Transit

Data
- Encryption at Rest
- Segregation of PII

Processes
- Educate
- Identify
- Protect
- Detect
- Respond
- Recover
- Learn

GOAL: Separate the normal from the anomalous and investigate in real-time

System Behaviour – Access Attempts – Data Movements – Service Quality – Attempted Attacks

© 2019 Cognizant
What technology delivers

- Segregation of Duties
- Secure by Design
- Defence in Depth
- Zero Trust
- Device- & Location- Independence
- Need to Know
- Know what you have
- 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

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
What makes a solid foundation?

Governance & Compliance

Management Controls

Technical Controls

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

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

© 2019 Cognizant
Thank you
Jonathan Lloyd-White, International Airlines Group
Reaching the boardroom with meaningful metric
### 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

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

<table>
<thead>
<tr>
<th>Risk</th>
<th>Control</th>
<th>Description</th>
<th>Red</th>
<th>Amber</th>
<th>Green</th>
<th>Trend</th>
<th>Previous Month</th>
<th>Current Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk 1</td>
<td>Control 1.1</td>
<td>AV</td>
<td>&lt;70</td>
<td>70-94</td>
<td>&gt;95</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk 2</td>
<td>Control 1.2</td>
<td>Endpoint</td>
<td>&lt;70</td>
<td>70-94</td>
<td>&gt;95</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk 3</td>
<td>Control 1.3</td>
<td>Patching</td>
<td>&lt;70</td>
<td>70-94</td>
<td>&gt;95</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk 4</td>
<td>Control 2.1</td>
<td>Phishing Test</td>
<td>&lt;70</td>
<td>70-94</td>
<td>&gt;95</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Detect Respond Recover

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

Invest

- Highlight key project progress and risks
- Note points for escalation and action
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
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
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 and implement the appropriate controls.

- **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 Management (IM)**

- **Awareness**: Aspects of both Cyber Security and Information Management require user training and awareness.
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 embrace 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
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?
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
Lunch & networking break

SASIGEvents

@SASIGEvents

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

Jonathan Spilky
Account Executive, Tessian
Paul Berriff OBE, Producer, Director, Cinematographer and Fine Arts Photographer

9/11 - A First-Hand Experience
Panel and Q&A Session
Thank you