

Victorian Chapter – FS SIG

Auditing for Cyber security preparedness

Presented by

Ashutosh Kapsé

CISM, CISA, CRISC, ISO27001LA, CCSK, IRAP

**Head – Information security, technology risk & audit
IOOF Holdings Ltd.**

Disclaimer

Any logos, trademarks used, belong to the respective organisations and they own the sole right to use and reproduce them.

This presentation is intended to provide general information only and has been prepared without taking into account, any particular person's / organisation's objectives, business situation, needs or risk profile. Any person / organisation, before acting on this information, should consider the appropriateness of this information with regards to their personal / organisation's objectives, business situation, needs or risk profile. We recommend you obtain Audit and Risk advice specific to your situation before making any Risk / Audit related decisions.

Reference to any tools, technologies or organisations is not meant as endorsement, advertising or support of those products/technologies. The reference is purely to relay my experience and personal opinion.

Acknowledgements:

National Institute of Standards and Technology

Steven Ross – Risk Masters Inc, USA

Lockheed Martin whitepaper – Eric M. Hutchins, Michael Cloppert & Rohan Amin.

What we will cover today (Agenda)

- Cyber attacks – myths and reality
- ASIC report 429
- Auditing - Cyber attack preparedness

Cyber security



The Institute of
Internal Auditors
Australia

Information
security



Cyber security



Cyber

H
S
By

f

More on Carabank APT - The \$1B Cyber Crime

Posted Thursday, 19 February 2015

We wrote about the Anunak/Carbanak hacker gang in a previous entry but there is a nicely detailed report now available on-line. Full infographic here

SECURELIST

How the Carbanak cybergang stole \$1bn A targeted attack on a bank

1. Infection



2. Harvesting Intelligence Intercepting the clerks' screens



3. Mimicking the staff How the money was stolen



© 2015 Kaspersky Lab

GREAT KASPERSKY

The importance of APT detection has never been greater. Layered security approaches, file integrity monitoring measures (system hardening, control (to maintain a high standard) and for breach detection and when an APT attack

“

There are only two types of
companies: those that have been
hacked, and those that will be.

”

Robert Mueller, FBI Director
RSA Conference 2011



Aggressive Vendor marketing

Myths

Myth no 1 - Something we have not seen before



"You know, you can do this just as easily online."



Myth no 2

Cyber attacks are unstoppable

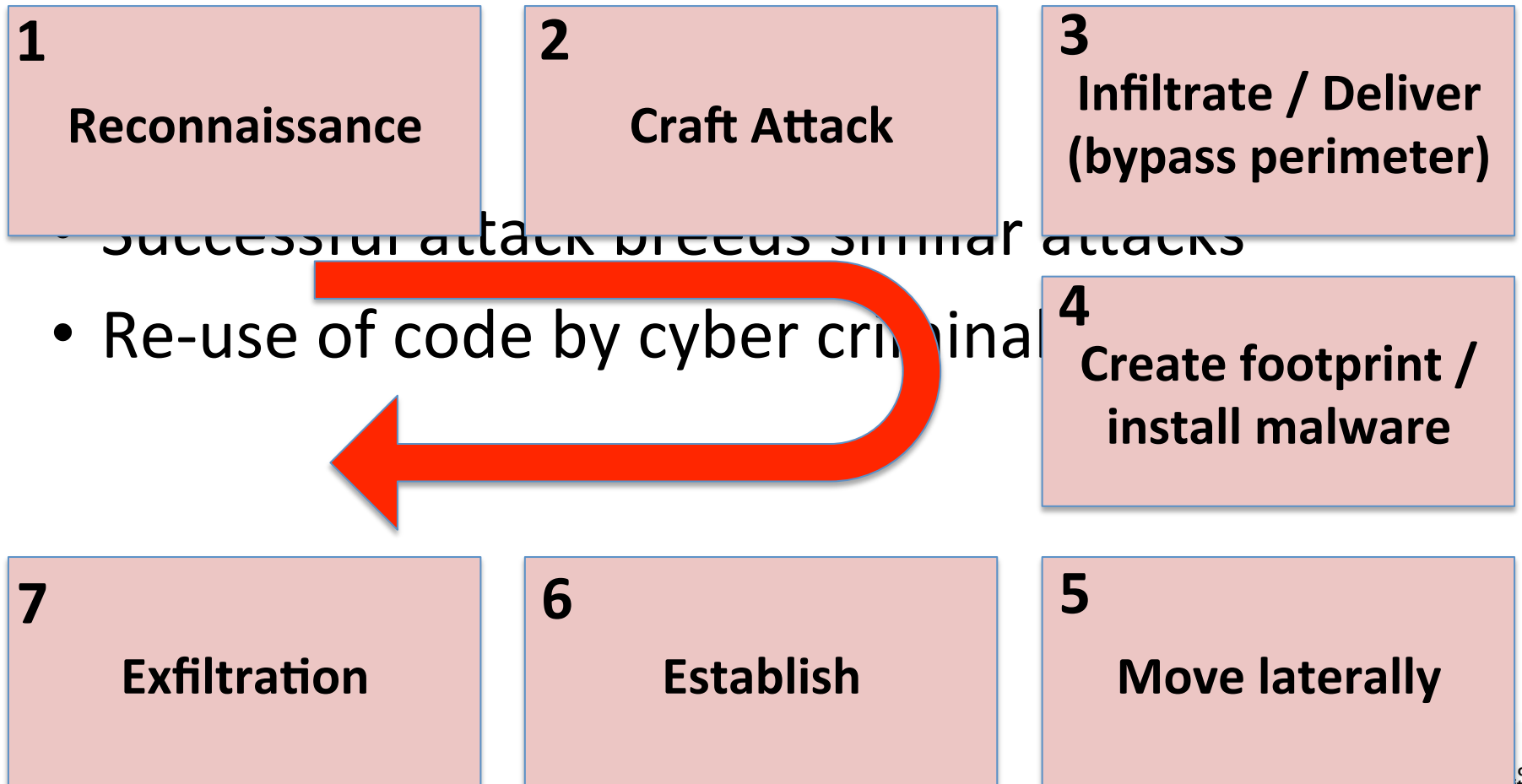
- Bad things do happen (pandemics, war, crime, terrorism...) but we treat them as manageable problems
- Cyber attacks are no different

Myth no 3

Each cyber attack is different (more advanced than previous) hence prevention is impossible

- Huge differences depending on cause & effect of each type of attack

Cyber attack-flow



What this means

- With appropriate preparation and control framework, organisations, regulators and customers can create comprehensive cyber security programs & use it to assess and improve readiness.

ASIC Report 429

“Cyber resilience: Health Check”

Report highlights importance of Cyber resilience to ASIC’s regulated population

“ASIC intends to “incorporate cyber resilience in our surveillance programs across our regulated population”

Control Framework



NIST (National Institute of Standards and Technology)
Cyber security framework

Improving Critical
Infrastructure Cybersecurity
Executive Order 13636

Slightly modified for cyber-assessor



Note: this is my modification not NIST or by any other standards body

- This framework is the closest thing we have to a “standard” of cyber security controls
- It provides structure but not necessarily content

Elements of the framework

| | |
|----------|--|
| Accept | Understand that cyber attacks are a real threat and this may occur in your organisation |
| Identify | Develop your organisation's understanding to manage the cyber security risk to organisation's systems, assets, data and capabilities |
| Protect | Develop and implement a prioritised set of safeguards to ensure delivery of organisation's business activities |
| Detect | Develop and implement appropriate activities to identify occurrence of a cyberattack |

Elements.... Cont'd

Respond

Develop and implement prioritised set of activities to respond to detected cyber attack event

Recover

Develop and implement prioritised set of processes to restore business critical activities and operations after a cyberattack event.

Auditing “Acceptance”

Accept

Understand that cyber attacks are a real threat and this may occur in your organisation

- Is there a management directive to deal with cyber attack threat?
 - Board level
 - Executive level
 - CIO level
- Is there appropriate funding
 - Personnel
 - Insurance
 - Technology
 - Expert assistance (3rd party)
- Is there appropriate structure?
- Who owns the problem? The solution ?

Auditing - Identify

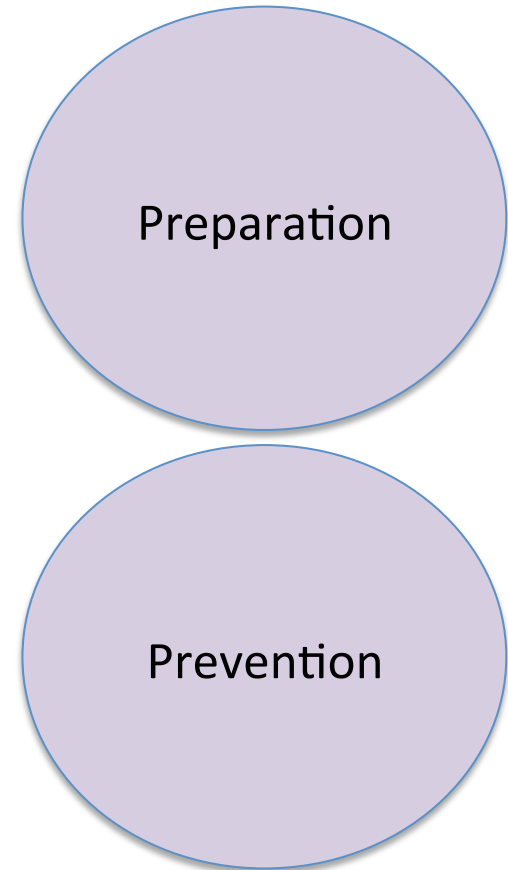
| | |
|----------|----------------------|
| Identify | Asset management |
| | Business environment |
| | Governance |
| | Risk assessment |
| | Risk management |

Auditing “Identify”

- Is there an inventory of information assets?
- Does every business function know
 - What system it relies on?
 - What data these systems have access to?
 - Where those systems are?
- Are the “owners” identified?
 - Governance
 - Business owners (risk management)
 - IT owners
 - DR champion (both IT & business)
 - Expert assistance (3rd party)
- Business continuity

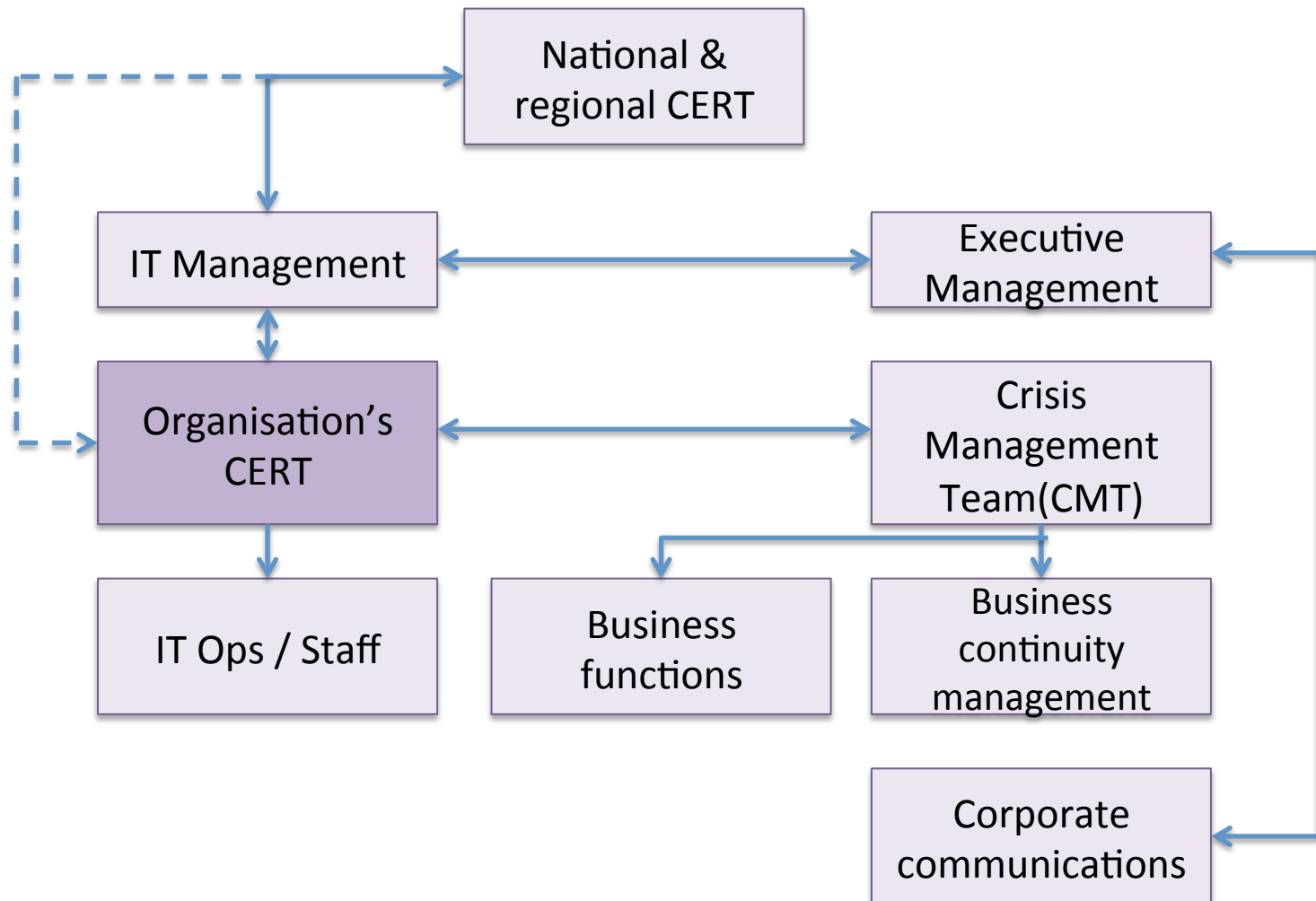
Protect

| | |
|---------|---|
| Protect | Access control |
| | Awareness & training |
| | Data security |
| | Information protection processes & procedures |
| | Protection technologies |



Auditing “Preparation”

- Is there an organisational structure to prepare for prevention, detection & recovery?



Auditing “Preparation” - 2

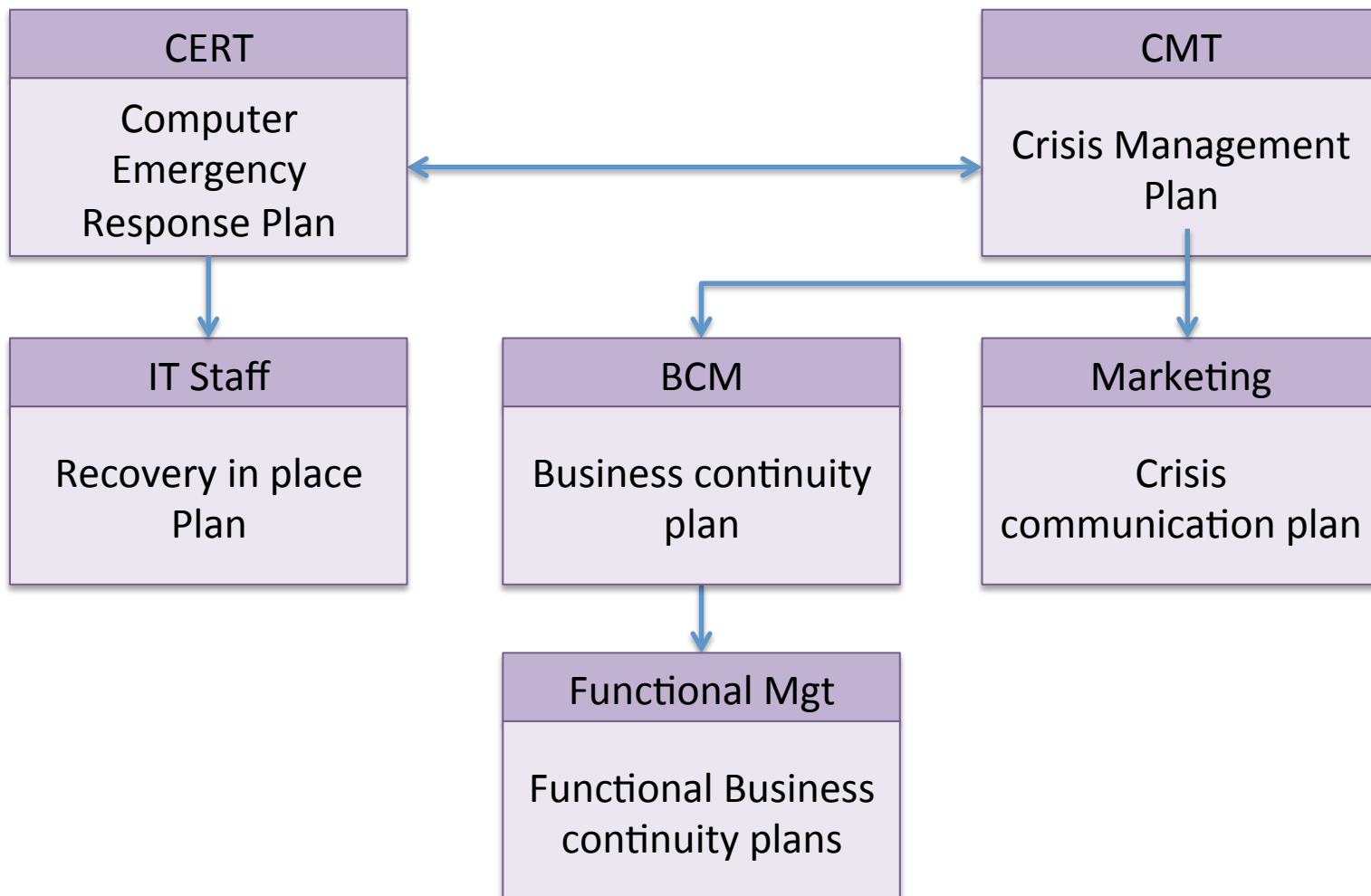
- Is there a **Proactive** Computer Emergency Response team (internal)?
- Some organisations do have existing CERT
- Cyber attacks require CERT somewhat different, from a traditional CERT
- A proactive CERT requires specific mandate, investment in personnel, tools, emergency procedures and communication protocols
- Requires very tight co-ordination with business Crisis Management Team

Cyber-attack ready CERT

| | Traditional CERT | Cyber CERT |
|--------------------|--|--|
| Membership of CERT | Flexible & incident dependent. Functional leaders with others added at time of incident. | Pre-selected. IT Executives, functional leaders, IT ops, systems admins, technicians, operators. (potential external expert) |
| Preparation | Extension of current jobs | Focused team & roles, rehearsals, scenario preparation, Prepare recovery environment |
| Activation | At time of problem | On-going. Preparedness, monitoring, daily activity |
| Decision-making | Limited | Complete with IT |

Auditing “Preparation” - 3

- Is there plan ?
- Do existing plans address cyber attacks?



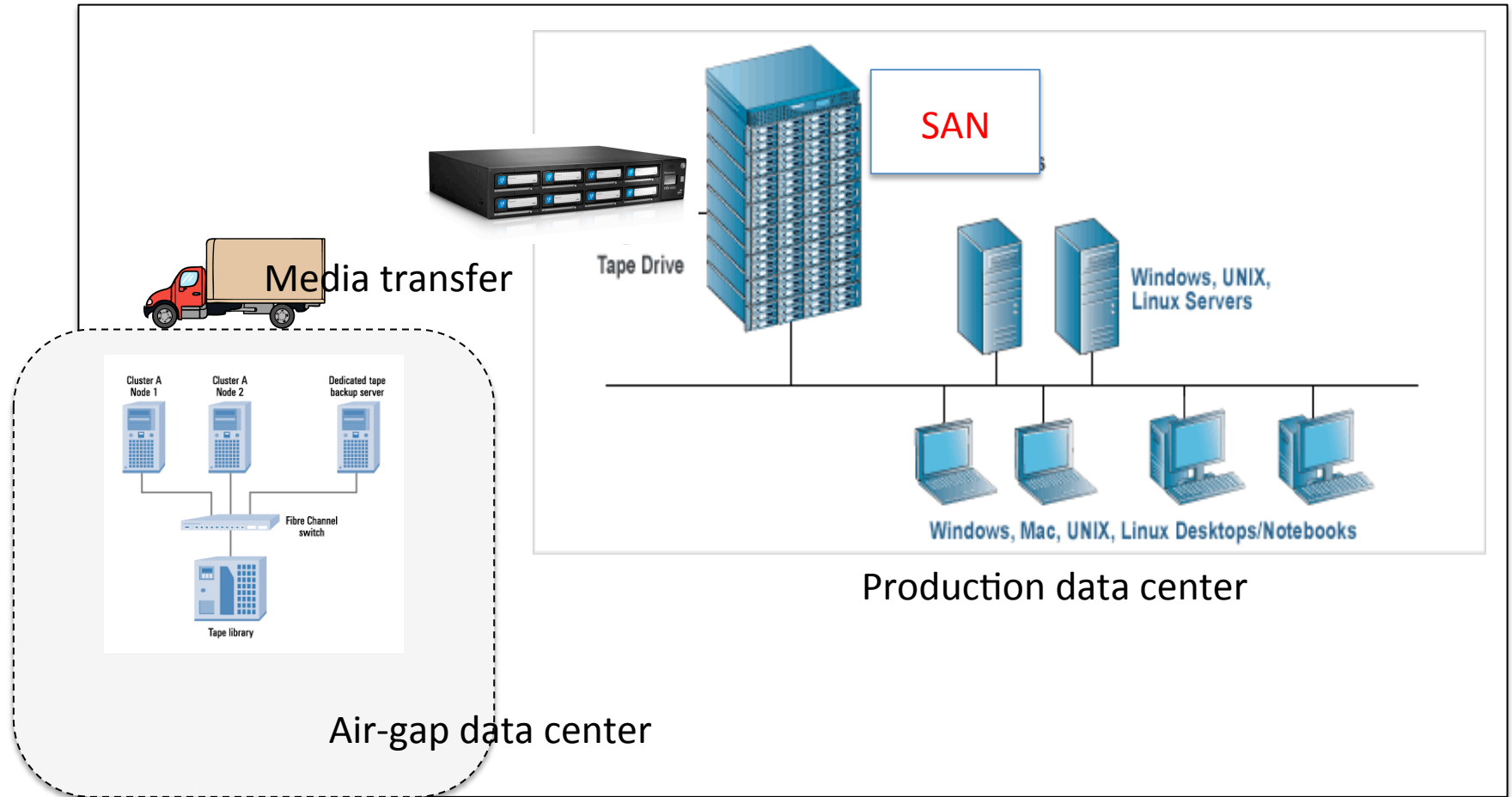
Auditing “Protection” 1

- Does the organisation have basic preventive tools?
 - Firewalls
 - Intrusion detection / prevention tools
 - Encryption
 - Web / mail filters
 - End point protection
 - The people to make them all work
 - CERT
 - Operators
 - Security administrators
 - Help/service desk
 - End users
- Training ? – appropriate for cyber protection
- Change control in IT

Auditing “Protection” - 2

- Does the organisation have **advanced** preventive tools?
 1. Air gap data center?
 2. Next Generation firewall?
 3. Zero trust architecture?

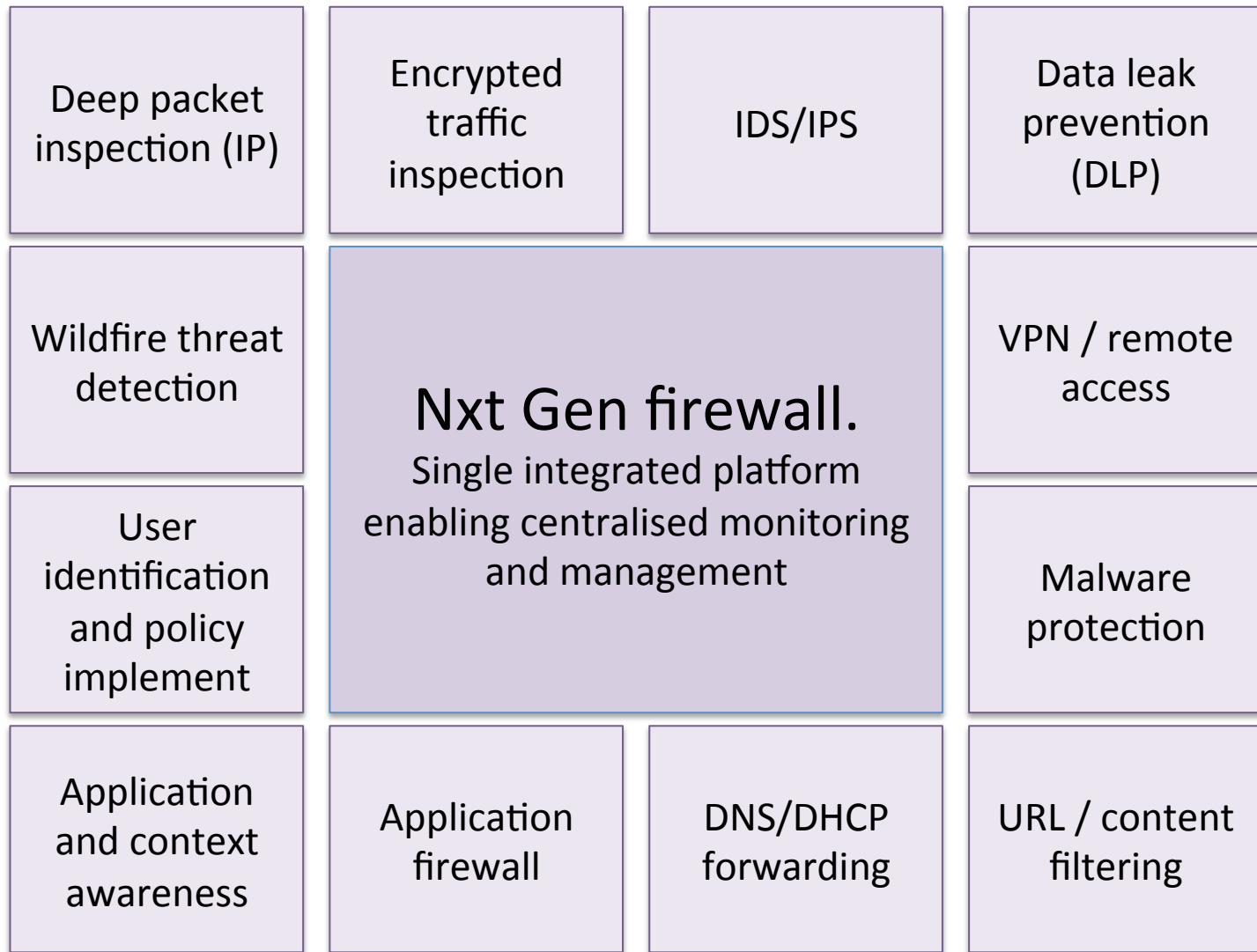
Air-gap data center



- Repository for trusted images
- Backups of data

Next Generation Firewall

- Not new technology as such
- Integrates multiple security point solutions into a single device
- User and application aware (not just IP address and port aware)
- Content and context awareness
- Dynamic posture through “sandboxing”



Detect

Detect

Anomalies & Events

Security Continuous monitoring

Detection processes

Auditing “Detect”

- More about process/procedures
- Is any one “awake” at the switch
- Detection roles & processes
- Security continuous monitoring
 - Vulnerability and Patch status?
 - On-going testing of web facing applications?
 - CMDB and configuration management?
- Any advanced detection systems?
 - Anomaly detection / Heuristics
 - User behavior monitoring
 - Database monitoring
- Usually weakest point in the chain

Respond

| | |
|---------|----------------|
| Respond | Communications |
| | Analysis |
| | Mitigation |
| | Improvements |

Auditing “Respond”

- Does CERT practice routinely for cyber-attack response?
- Are there response procedures?
 - Taken from scenarios
 - Learning from previous incidents
- Log of attacks / attempts?
 - Is root cause analysis performed
 - Lessons learnt / implemented

Recover

Recover

Recovery planning

Improvements

Communications

Auditing “Recover”

- Weakest auditing point
- No attack – nothing to audit?
- If there was attack & recovery – audit
 - Quality of recovery process & effectiveness
 - Report on opportunity for improvement
- Audit whether BCP/DR caters for Cyber attack recovery (usually only caters to natural disasters)
- In a way you are auditing recovery while auditing preparation

Ashutosh Kapsé

MBA, CISM, CRISC, CISA, ISO27001LA, IRAP Certified, CCSK

Head – Information security, technology risk & audit

IOOF Holdings Ltd. (ASX : IFL)

ashutosh.kapse@ioof.com.au

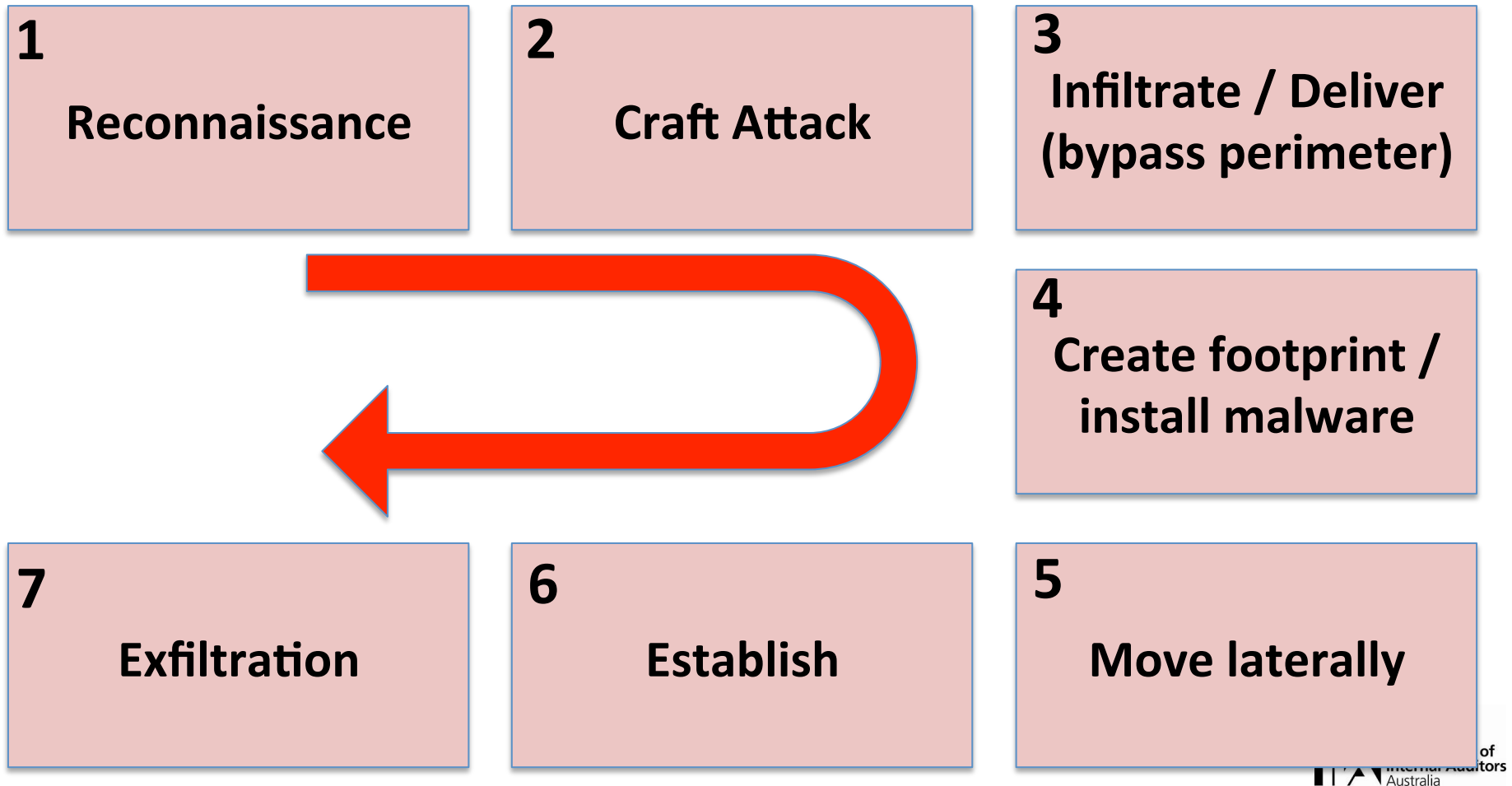
ashutosh.kapse@gmail.com

Three Key things

Three Key things to remember for Auditors

1. Cyber kill chain (how attackers behave)
2. Forget the hype – KIS principle (cyber basics)
3. Use the “Accept – Identify – Protect – Detect – Respond – Recovery” pillars for auditing

Cyber attack flow



Cyber security basics

Audit the basics to start with

1. Where is your most sensitive data located?
2. How many applications/servers/endpoint devices do you have to patch and protect?
3. Do you have a security awareness program for all your employees?
4. Are your office locations and facilities protected from unauthorized access?
5. Who do employees call when there's a security incident?
6. Is your network being monitored for malicious traffic?
7. Are you collecting logs for your most critical systems?

Control framework



Thank you

Ashutosh Kapsé

MBA, CISM, CRISC, CISA, ISO27001LA, IRAP Certified, CCSK

Head – Information security, technology risk & audit

IOOF Holdings Ltd. (ASX : IFL)

ashutosh.kapse@ioof.com.au

ashutosh.kapse@gmail.com