DFSA Cyber Risks Outreach

Thursday, 15 December 2016

Ian Johnston

Chief Executive

The Dubai Financial Services Authority (DFSA)

Cyber Risks Outreach

15 December 2016

Cyber Risks Outreach
15 December 2016
Speakers

Stuart Paterson
HSF

Darren Mullins
Deloitte

Oliver Fairbank
Control Risks

Bryan Stirewalt
DFSA

Hamid Qureshi
Thales

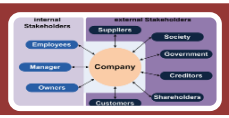
Mohammed Fikri
aeCERT

Bryan Stirewalt

Managing Director, Supervision
The Dubai Financial Services Authority (DFSA)

Cyber Risks Outreach
Regulatory Messages
15 December 2016

Cyber Key Areas of Focus



Understand the Seriousness of the Impact of Cyber including on your Stakeholders

Focus your Governance on your Cyber Risks; 'Own' your Cyber Risks; and Create a 'Security Culture'

Identify your Potential Cyber Risks

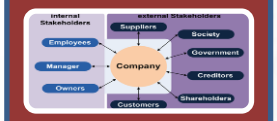
Prevent, Detect and Respond to your Cyber Risks

Safeguard your Clients

Plan and Rehearse your Response to Cyber Attacks

Understand what you must do for DFSA and DIFC Authority and for UAE Agencies; and what they can do for you

7 What and How Cyber Questions



1. **How** have possible impacts on your stakeholders from a major Cyber Attack been considered by <u>you</u> and your Firm - including outsourcing to suppliers and insourcing within your Group? **What** would those impacts be?
2. **How** is the Board / Executive Management overseeing Cyber Risks? **What** is the 'Security Culture' throughout the Firm (reflecting the 'Tone at the Top')?
3. **How** have <u>you</u> identified all key potential Cyber Risks that might impact your Firm? **What** are they?
4. **What** Systems and Controls are in place to prevent/detect/respond to a major Cyber Event? **How** do you measure their effectiveness?
5. **What** plans have been tested to safeguard Clients if the Firm is impacted by a Cyber Attack? **How** were the tests devised and tested?
6. **How** has a successful Response and Recovery Rehearsal been tested for a major Cyber Attack (including for all likely financial consequences)? **What** were the results?
7. **What** are your Cyber Risk responsibilities to DIFCA, DFSA <u>and</u> all relevant UAE Agencies? **How** have you addressed these?

UAE and DIFC Authority Agencies

DIFC Data Protection Commissioner

DATA PROTECTION REGULATIONS

A strict set of rules that are consistent with Data Protection Directive of the European Commission which ensures harmonisation of the data and financial penalties for non-compliance.

مركز دبي المالي العالمي
Dubai International Financial Centre

الهيئة الوطنية للأمن الإلكتروني
NATIONAL ELECTRONIC SECURITY AUTHORITY

DFSA
Dubai Financial Services Authority

ae CERT Computer Emergency Response Team

مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

60 عاماً
شرطة دبي
DUBAI POLICE

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Anti-Money Laundering and Suspicious Cases Unit - AMLSCU

DFSA Rulebook – Cyber Risks

Principles for Authorised Firms
Principles for Authorised Individuals

Remuneration structures align with risk outcomes

Due diligence and supervision of outsourcers

Notifications to the DFSA

Systems and Controls

Management Information to manage Risks

Risk Management Systems and Controls

Effective corporate governance

Effective Systems to Deter Fraud

Business continuity and disaster recovery

Systems and Controls that do not facilitate others to engage in Financial Crime

CYBERCRIME: A LEGAL PERSPECTIVE

HERBERT SMITH FREEHILLS

15 DECEMBER 2016

Stuart Paterson, partner, +971 4 428 6308, stuart.paterson@hsf.com

CYBERCRIME: A LEGAL PERSPECTIVE

- Understand the threat, both to you and your organisation
- Legal risks
- Risk mitigation
- Incident response

UNDERSTAND THE CYBER THREAT

UNDERSTAND THE CYBER THREAT

"*There are two kinds of companies. Those that have been hacked and those that don't know they have been hacked.*"

John Chambers, CEO of Cisco

UNDERSTAND THE CYBER THREAT

- The threat is as old as “computers” themselves
- What has changed?
- Trends: phishing, ransomware, cloud providers
- DFSA letter to SEOs April 2015 (prevent, detect, respond)

LEGAL RISKS AND ISSUES

- UAE Federal Penal Code and Cyber Crimes Law
- Corporate liability
  - negligence, breach of contract regarding data security, failure to provide services to clients (eg banking payment systems)
- Personal liability for directors of ‘victim’ company
  - SEO/directors of DIFC companies: personal liability under DIFC Law for failure to act in company’s best interests. Possible criminal offences?
- Recovery claims?

REGULATORY ISSUES

- Regulatory obligations are based in rules and principles around effective management of risk and controls.
- Regulatory sanctions for failings in these areas.
- Internationally, regulators are prioritising cyber issues to ensure market integrity and consumer protection.
- Increasing UAE government focus (NESA, DESC, aeCERT).

DFSA PRINCIPLES FOR AUTHORISED FIRMS

DFSA Rulebook

- **Principle 3** – Management, systems and controls
- **Principle 10** – Relations with Regulators
- **Principle 11** – Compliance with high standards of corporate governance

RISK MITIGATION

"*There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know*."

Donald Rumsfeld

RISK MITIGATION

- To protect your business, you have to understand it thoroughly; how and where is business done? Use of old IT, third parties (outsourcing). Where are the weaknesses? If you don't know them, they cannot be remedied.

- Prioritise critical assets.

- The IT team are part of the strategy, but the strategy starts with management.

- Integrate cyber strategy with broader risk/compliance strategy. Senior management must set, communicate (policies), implement and test that strategy based on sound knowledge of the business.

- Training, contractual terms, recruitment and other mitigation techniques.

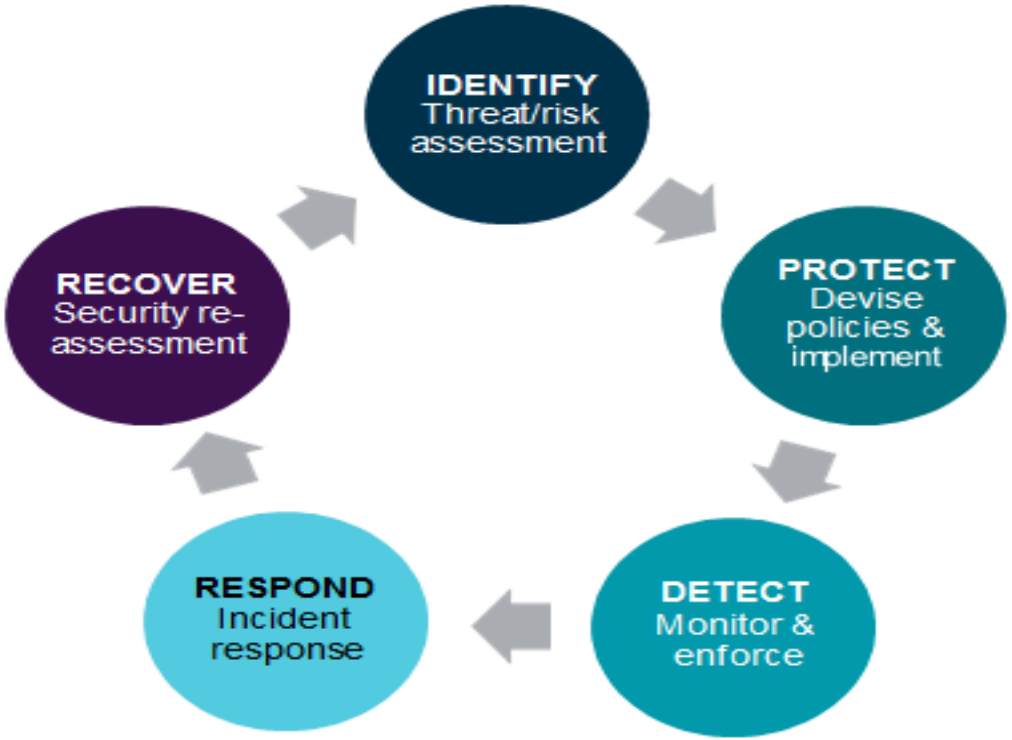
RISK MITIGATION

"*I have a son. He's 10 years old. He has computers. He is so good with these computers it's unbelievable. The security aspect of cyber is very, very tough. And maybe its hardly doable. But I will say, we are not doing the job we should be doing*."

Donald Trump

RISK MITIGATION

Cyber security lifecycle



CREATING A SECURITY CULTURE

Good governance

Senior management engagement, responsibility and effective challenge at the Board level

Identification of key assets

- Identify key assets/information
- Adequacy of protections
- Training of staff to recognise phishing
- Screening staff – is it adequate?
- Testing defences – frequency and adequacy

Detection

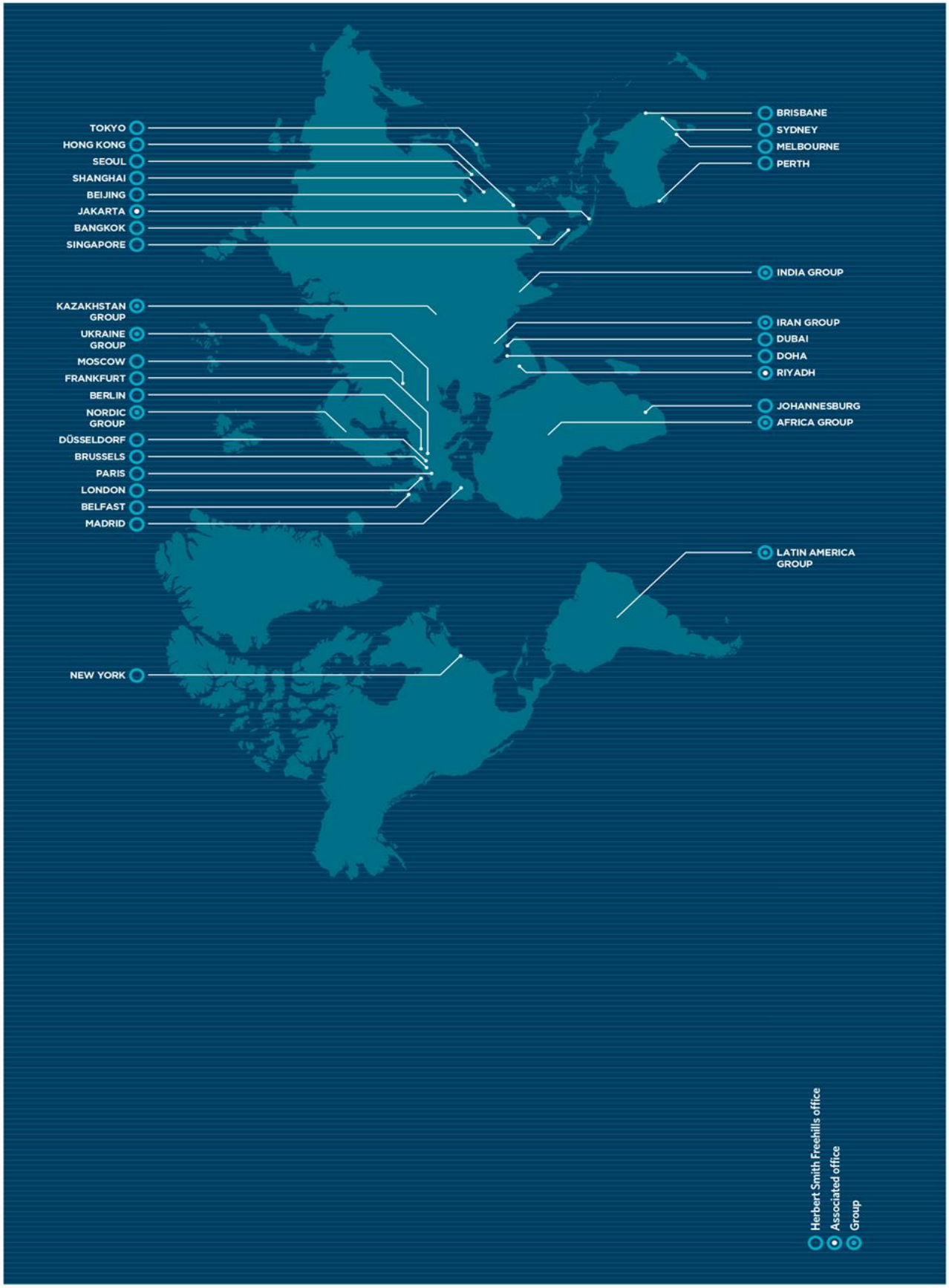
- Do you know whether you have been attacked?
- How quickly ?
- Adequacy of threat intelligence?

Recovery and response

What is your ability to:
- carry on in the event of an unforeseen interruption
- recover from interruptions
- preserve essential data

INCIDENT RESPONSE

- Protect strategic assets
- Preserve evidence and investigate
- Privilege and disclosure
- PR
- Prioritise objectives


TOKYO
HONG KONG
SEOUL
SHANGHAI
BEIJING
JAKARTA
BANGKOK
SINGAPORE
BRISBANE
SYDNEY
MELBOURNE
PERTH
INDIA GROUP
KAZAKHSTAN GROUP
UKRAINE GROUP
MOSCOW
FRANKFURT
BERLIN
NORDIC GROUP
DÜSSELDORF
BRUSSELS
PARIS
LONDON
BELFAST
MADRID
IRAN GROUP
DUBAI
DOHA
RIYADH
JOHANNESBURG
AFRICA GROUP
LATIN AMERICA GROUP
NEW YORK
Herbert Smith Freehills office
Associated office
Group

HERBERTSMITHFREEHILLS.COM

BANGKOK
Herbert Smith Freehills (Thailand) Ltd
T +66 2657 3888
F +66 2636 0657

BEIJING
Herbert Smith Freehills LLP Beijing
Representative Office (UK)
T +86 10 6535 5000
F +86 10 6535 5055

BELFAST
Herbert Smith Freehills LLP
T +44 28 9025 8200
F +44 28 9025 8201

BERLIN
Herbert Smith Freehills Germany LLP
T +49 30 2215 10400
F +49 30 2215 10499

BRISBANE
Herbert Smith Freehills
T +61 7 3258 6666
F +61 7 3258 6444

BRUSSELS
Herbert Smith Freehills LLP
T +32 2 511 7450
F +32 2 511 7772

DOHA
Herbert Smith Freehills Middle East LLP
T +974 4429 4000
F +974 4429 4001

DUBAI
Herbert Smith Freehills LLP
T +971 4 428 6300
F +971 4 365 3171

DÜSSELDORF
Herbert Smith Freehills Germany LLP
T +49 211 975 59000
F +49 211 975 59099

FRANKFURT
Herbert Smith Freehills Germany LLP
T +49 69 2222 82400
F +49 69 2222 82499

HONG KONG
Herbert Smith Freehills
T +852 2845 6639
F +852 2845 9099

JAKARTA
Hiswara Bunjamin and Tandjung
Herbert Smith Freehills LLP associated firm
T +62 21 574 4010
F +62 21 574 4670

JOHANNESBURG
Herbert Smith Freehills South Africa LLP
T +27 10 500 2600
F +27 11 327 6230

LONDON
Herbert Smith Freehills LLP
T +44 20 7374 8000
F +44 20 7374 0888

MADRID
Herbert Smith Freehills Spain LLP
T +34 91 423 4000
F +34 91 423 4001

MELBOURNE
Herbert Smith Freehills
T +61 3 9288 1234
F +61 3 9288 1567

MOSCOW
Herbert Smith Freehills CIS LLP
T +7 495 363 6500
F +7 495 363 6501

NEW YORK
Herbert Smith Freehills New York LLP
T +1 917 542 7600
F +1 917 542 7601

PARIS
Herbert Smith Freehills Paris LLP
T +33 1 53 57 70 70
F +33 1 53 57 70 80

PERTH
Herbert Smith Freehills
T +61 8 9211 7777
F +61 8 9211 7878

RIYADH
The Law Office of Nasser Al-Hamdan
Herbert Smith Freehills LLP associated firm
T +966 11 211 8120
F +966 11 211 8173

SEOUL
Herbert Smith Freehills LLP
Foreign Legal Consultant Office
T +82 2 6321 5600
F +82 2 6321 5601

SHANGHAI
Herbert Smith Freehills LLP Shanghai
Representative Office (UK)
T +86 21 2322 2000
F +86 21 2322 2322

SINGAPORE
Herbert Smith Freehills LLP
T +65 6868 8000
F +65 6868 8001

SYDNEY
Herbert Smith Freehills
T +61 2 9225 5000
F +61 2 9322 4000

TOKYO
Herbert Smith Freehills
T +81 3 5412 5412
F +81 3 5412 5413

Deloitte.

Cybercrime

The current landscape and the hidden costs

December 2016

Strictly Private and Confidential

The Global Threat Landscape

Cyber threat continues to increase in scale and sophistication at an extraordinary rate. At one time, the most advanced cyber-attack tools and methods were restricted to a small handful of national players; now, more actors than ever, including nation state actors and organized criminal enterprises, are developing highly-skilled resources and capabilities, or acquiring them through an expanding black market for illicit activities.

The Current Threat Landscape

The Middle East on High Alert

In addition to the current global cyber threat landscape, the **Middle East faces 3 unique dimensions of risk** which translates in to an elevated level of cyber threat that must be considered.

Regional Geo-Political Instability

Since 2010 the Middle East has seen significant Geo-Political instability which has given rise to various hacktivist groups. These hacktivists groups have reigned cyber havoc on governments, public and private institutions in the region on almost a daily basis since the inception of the turmoil.

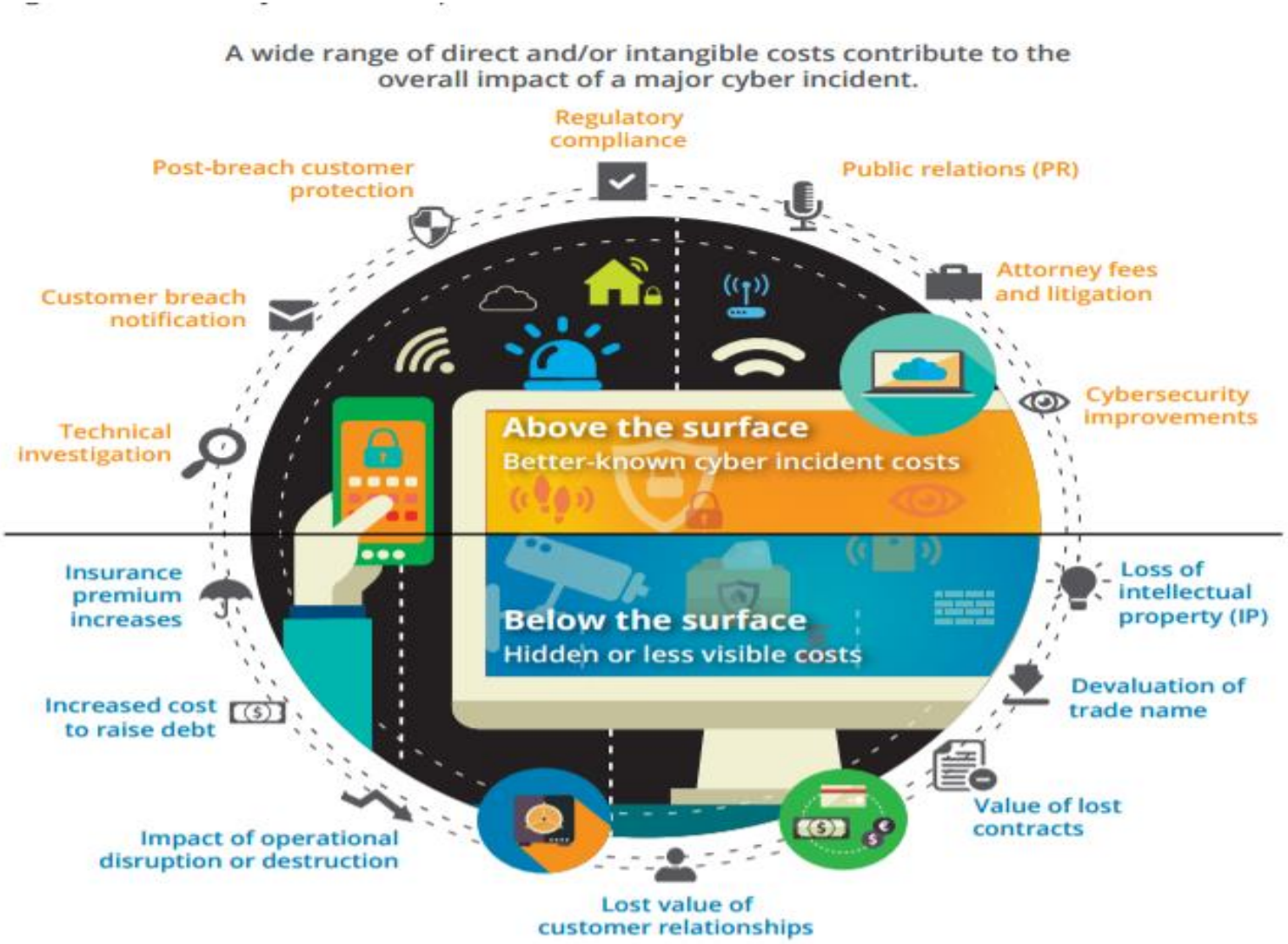
Perceived Economic Wealth

The Middle East in the eyes of the global community is perceived as a region of economic wealth. To cyber criminals who are trying to exploit governments, public and private institutions for financial gains this makes the Middle East a central target for attack and indeed has been.

Significantly Higher than Average Infection Rates

Microsoft, since 2012 has published a quarterly report on the average malware infection rate per country including a global average. With little exception Middle East countries have had at least double the number of infected systems per quarter than the global average.

Hidden Cost of a Security Breach*



*Deloitte Report July 2016

Deloitte.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Any reference to 'In the Middle East since 1926' applies specifically to the Middle East member firm of Deloitte Touche Tohmatsu Limited.

Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 225,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

About Deloitte Corporate Finance Limited

Deloitte Corporate Finance Limited is a company limited by shares, registered in Dubai International Financial Centre with registered number CLO 748 and is authorized and regulated by the Dubai Financial Services Authority. Deloitte Corporate Finance Limited is an affiliate of the UK and Middle East member firms of Deloitte Touche Tohmatsu Limited. The firm's principal place of business and registered office is at Al Fattan Currency House, Building 1, Dubai International Financial Centre, Dubai, United Arab Emirates. Tel: +971 (0) 4 506 4700 Fax: +971 (0) 4 327 3637.

Important Notice

This document has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication. Deloitte Corporate Finance Limited would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. Deloitte Corporate Finance Limited accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Identifying and averting cyber risks

Oliver Fairbank
Senior Analyst, Control Risks

15 December 2016

Control Risks

Control Risks is a global risk consultancy specialising in political, security and integrity risk

Abu Dhabi | Al Khobar | Amsterdam | Baghdad | Basra | Beijing | Berlin | Bogotá | Chicago | Copenhagen | Delhi | Dubai | Erbil | Frankfurt | Hong Kong | Houston | Jakarta | Johannesburg | Lagos | London | Los Angeles | Mexico City | Moscow | Mumbai | Nairobi | New York | Panama City | Paris | Port Harcourt | São Paulo | Seoul | Shanghai | Singapore | Sydney | Tokyo | Washington DC

Control Risks

Three main types of threat actors and three types of attack

Nation states

Cybercriminals

Cyber activists

Confidentiality
(i.e. stealing information)

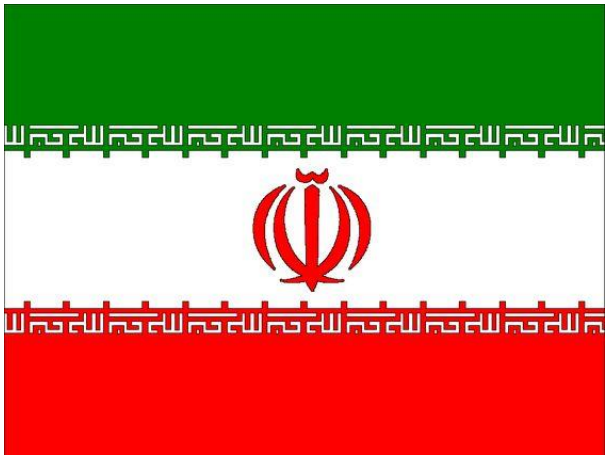
Integrity
(i.e. changing processes)

Availability
(i.e. disrupting or destroying processes)

Control Risks

Nation states are using disruptive attacks against geopolitical rivals

- Initial campaign emerged in August 2012 and targeted state-owned energy companies in the Middle East
- In November the malware was used to target Saudi government bodies
- The disruptive attack was likely preceded by an espionage component designed to steal administrator credentials
- The attack then used a self-replicating worm to spread throughout the target network, before deleting data, overwriting the hard drive and displaying an image
- Despite technical evidence of a common perpetrator, difficulties remain in responding to such attacks



Cybercriminals are targeting sensitive information for financial gain

- Operation Ghoul was the name given to a cybercriminal campaign that stole sensitive data from a range of businesses in the Middle East
- Ghoul targeted more than 90 organisations based in the UAE, particularly focusing on the industrial, manufacturing and engineering sectors
- The group used spear phishing emails against executives because of their presumed access to a firm's most important information
- These emails were laden with commercially available spyware programmes, which were used to copy and transmit information back to the group's command and control servers
- This data was then likely sold via the deep and dark web, potentially to competitors, or directly exploited

Cyber activists are targeting financial institutions to damage reputations

- The high profile of financial sector organisations and the plethora of sensitive data they hold makes them attractive targets for cyber activist groups
- In May 2016 the Grey Wolves claimed a breach of a major GCC-headquartered bank, releasing sensitive data such as customer names and account details
- Along with these ideologically motivated attacks, others conduct operations on a more opportunistic basis
- Broader campaigns, such as those conducted by the Anonymous collective, continue to use more rudimentary techniques against their targets

Organisations can tackle these

START WITH THE THREAT

Organisations need an intelligence-led approach, based on a granular understanding of the threat specific to them. This enables prioritisation of the areas to focus on, so you build defences against the threat you face.

COMBINE SOCIAL AND TECHNICAL

The weaknesses in organisations that are exploited by cyber attackers are a combination of the social and technical. To gain a complete picture, you need to combine an assessment of people, policy and process with technology.

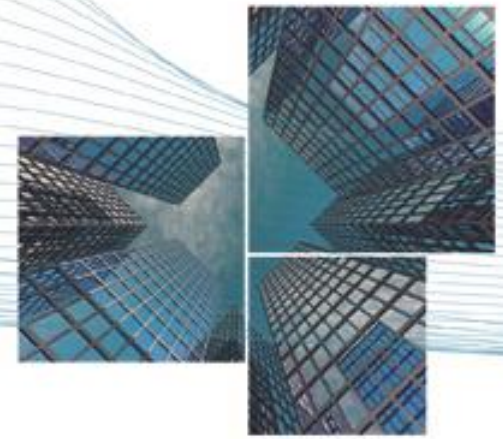
ATTACKER, NOT COMPLIANCE MINDSET

Cyber security is not a compliance exercise: it needs to be approached with an attacker's mindset. Although standards provide a baseline of security, they are not enough to stop most targeted attacks.

BE READY TO RESPOND

Protection is critically important, but a capability to detect and respond to breaches is just as vital. Organisations need to combine technical detection and response processes with crisis plans that have been tested.

Control Risks



www.controlrisks.com

THALES

Middle East Encryption Trends
Protecting Critical Applications & Data

Hamid Qureshi
Regional Sales Manager
Middle East
Thales E-Security

Encryption in the news today

Apple vs. FBI

Attempted $1BN Fraud

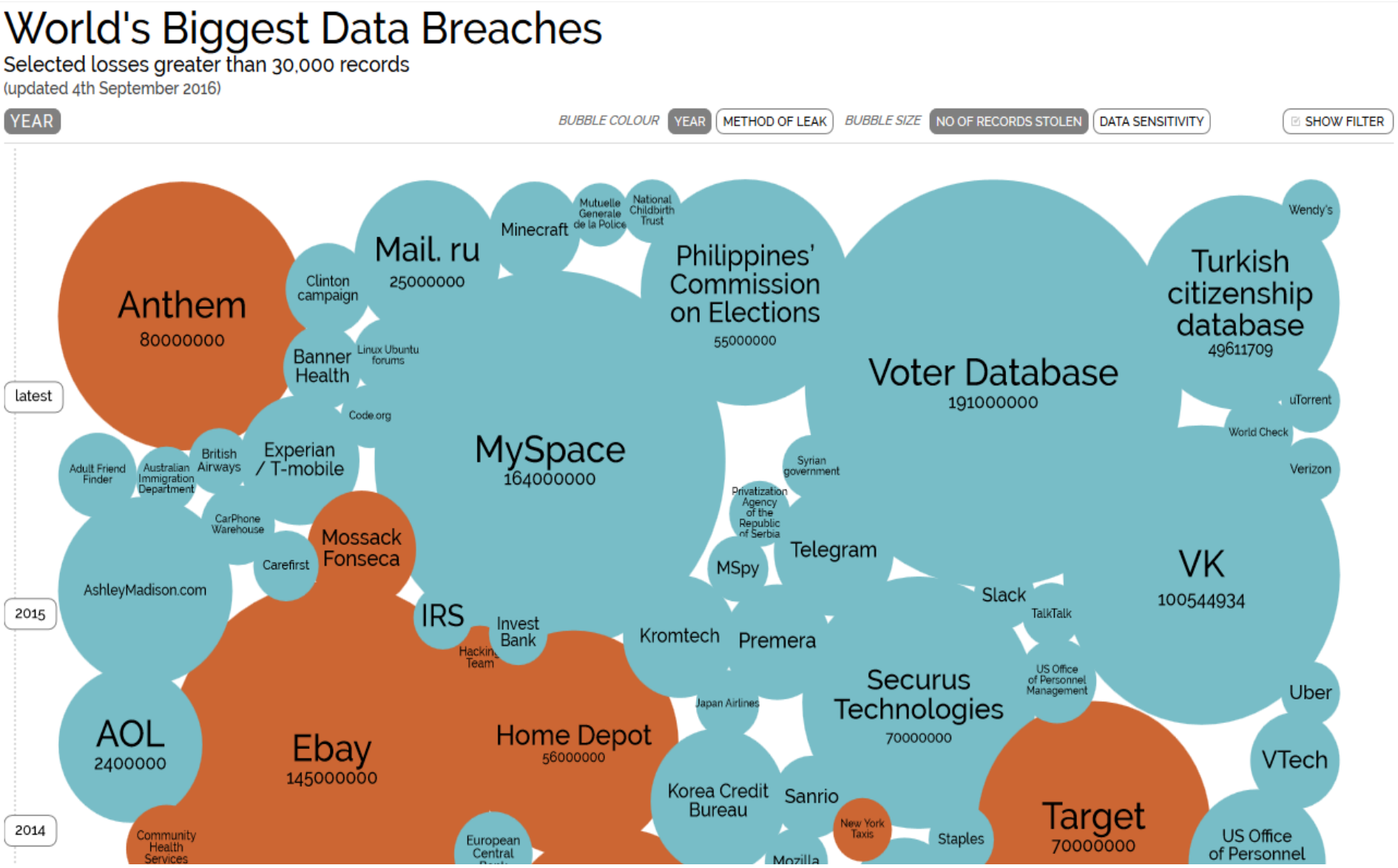
WhatsApp

Khaleej Times

One-third of UAE firms in cyber security breaches

THALES

Today's reality: targeted and successful data breaches



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

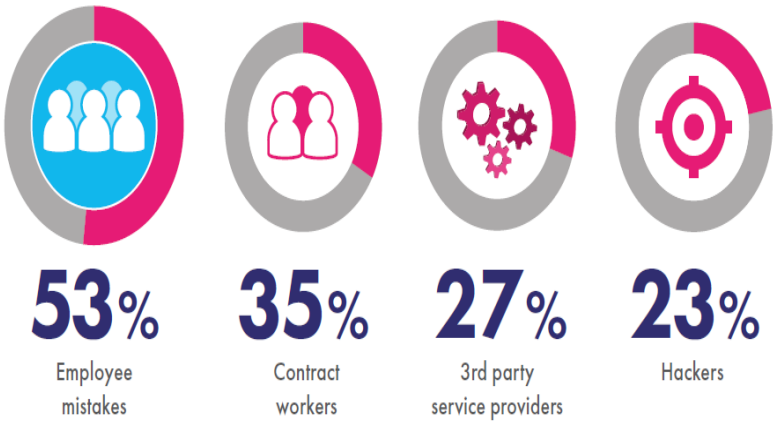
THALES

Summary of Middle East Encryption Report

- Issues addressed here affect companies of all types
- Regulations and privacy concerns are driving the growth of encryption

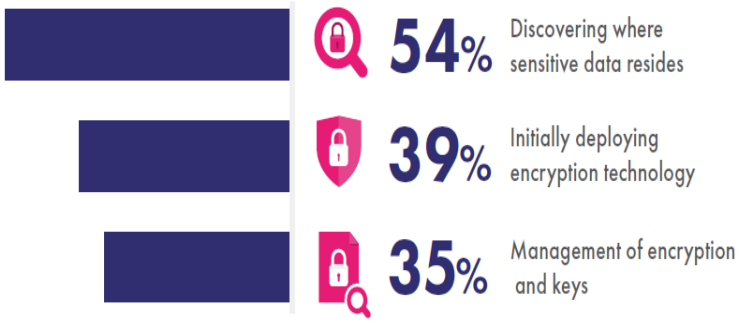
THREATS

The most significant threats to sensitive data are:



ENCRYPTION

What are the biggest challenges to encryption deployment?



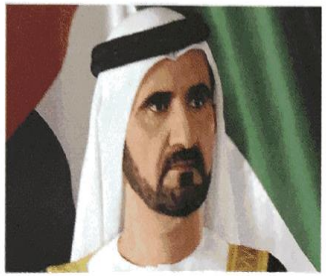
- Encryption use is growing, but so are key management challenges
- The cloud presents both opportunities and threats to security

THALES

Encryption regulation in the UAE

Mohammed issues Cabinet decision on IT security regulations

Friday, December 13, 2013



UAE Vice President, Prime Minister and Ruler of Dubai His Highness Sheikh Mohammed bin Rashid Al Maktoum

UAE Vice President, Prime Minister and Ruler of Dubai His Highness Sheikh Mohammed bin Rashid Al Maktoum has issued Cabinet Decision No. 21 of 2013 on Information Technology (IT) security regulations at federal government entities. Dubai's Information Security Committee (ISC) is coordinating with various government agencies to implement the Information Security Regulation (ISR), aimed at managing the information security environment in Dubai's public sector.

Non-compliance of this resolution may lead to criminal liability under UAE law, which in turn could lead to fines or even imprisonment. In addition, individual employees are already subject to internal disciplinary regulations and penalties of the federal authorities that they work for. Every federal employee is required to sign an acknowledgment and commitment of having understood and being committed to the guidelines. The resolution stipulates that "every User (who) violates the provisions of this Regulation shall be punished according to the disciplinary sanctions set forth in the human resources laws and regulations applied in the FE he/she works for".

"1. provide the greatest protection of the classified, sensitive and confidential information through the effective use of data encryption...

2. provide the appropriate encryption measures to any data sent via the network of other, and basic public communications networks...

3. encrypt and protect confidential data transmitted via readable fixed storage media in the computer...

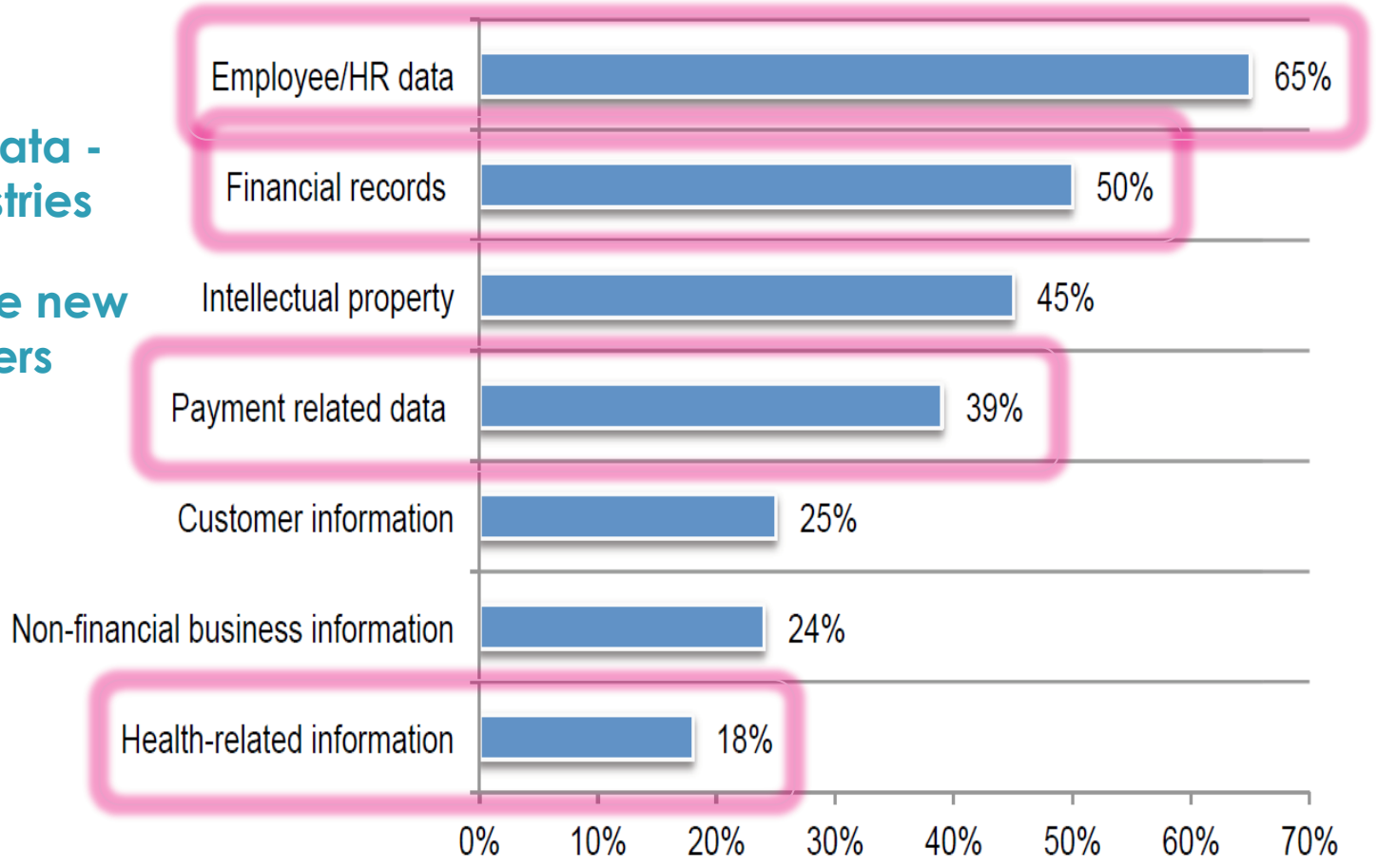
For data encryption, user shall commit to ...encrypt all existing sensitive and confidential data when storing or sending it"

(Article 12: Encryption)

THALES

Data types encrypted

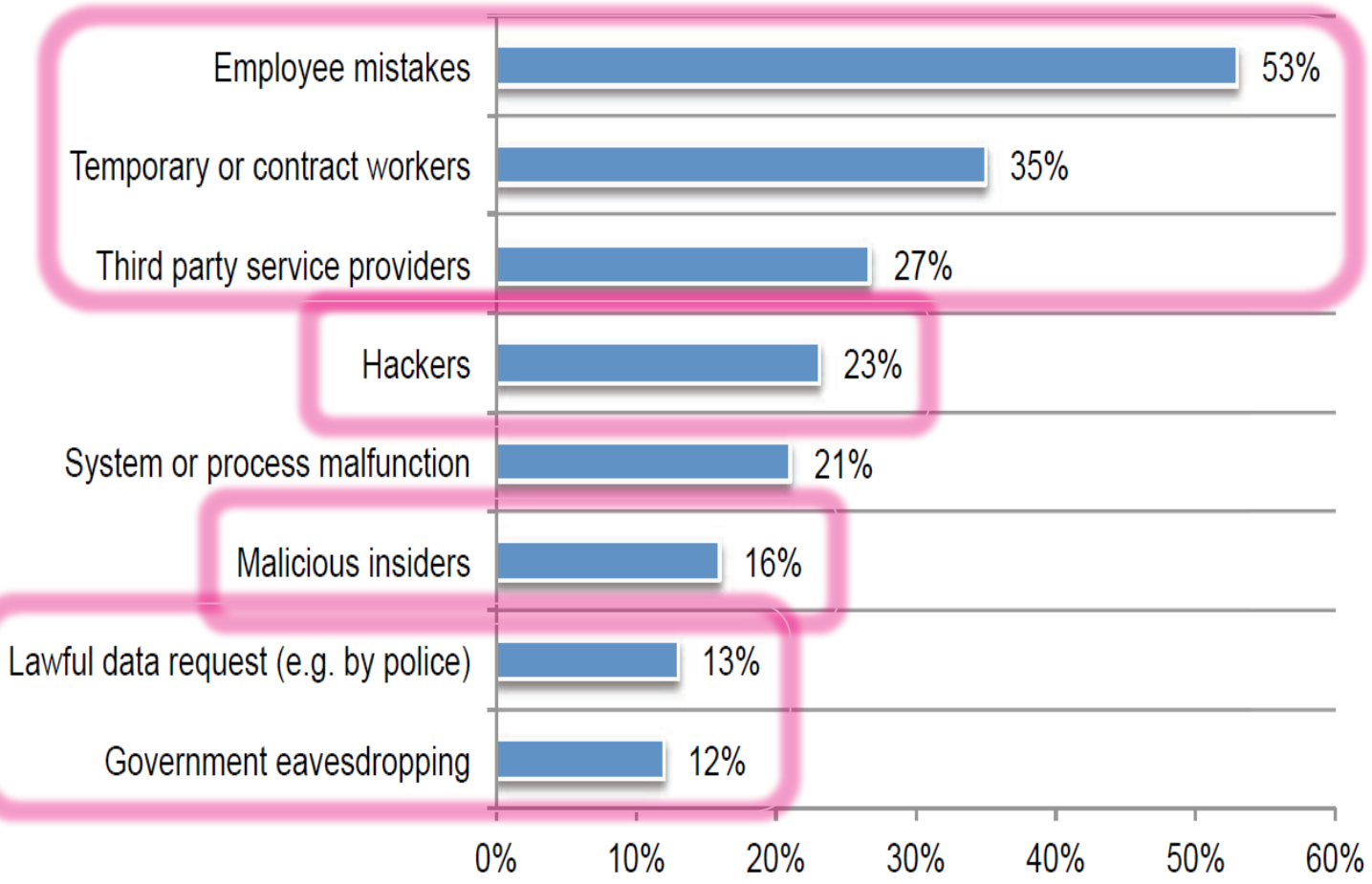
- Financial Data - Regulated
- Employee HR data - affects all industries
- Healthcare - the new target for hackers



THALES

Most significant threats to sensitive/confidential data

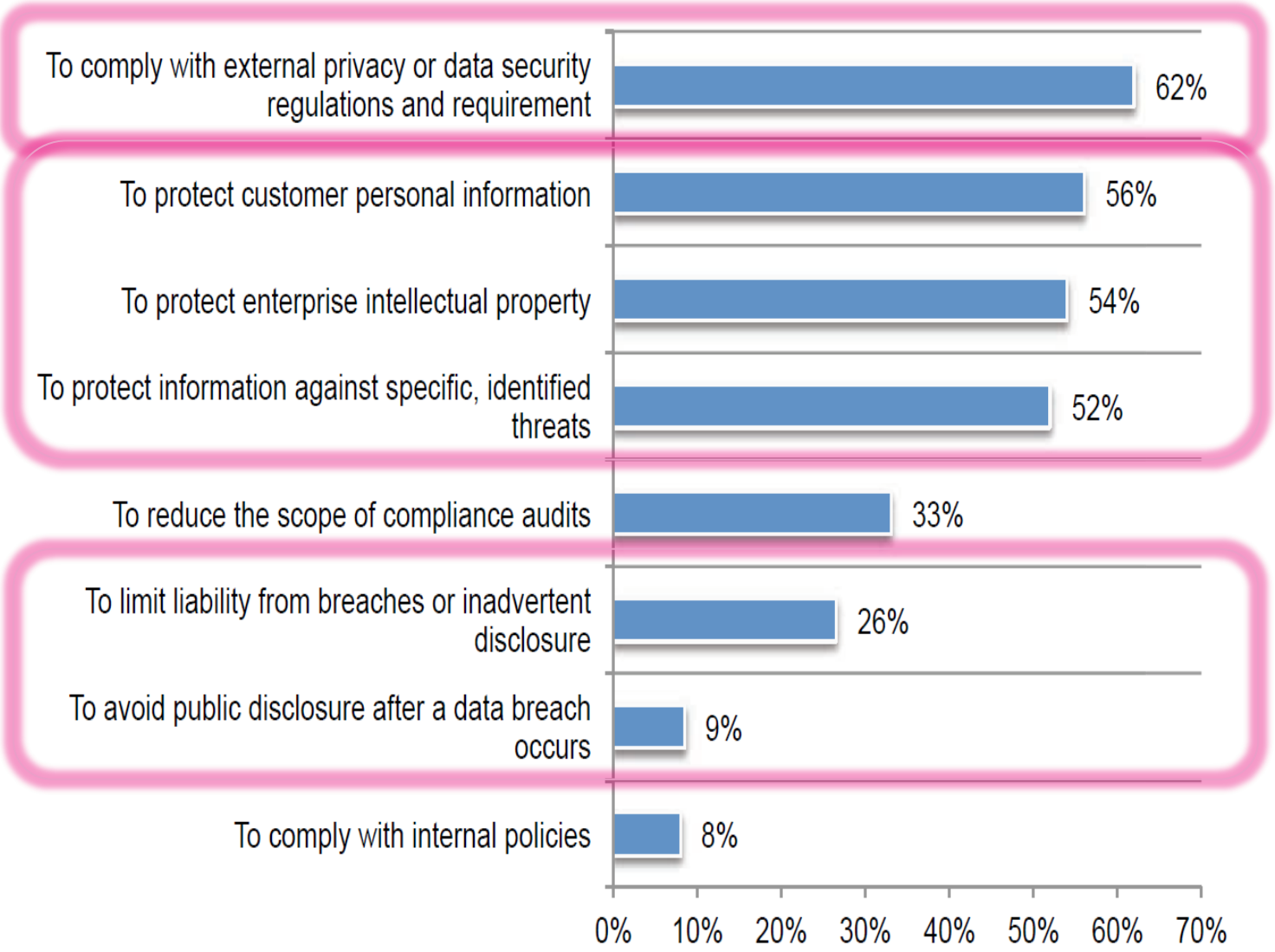
- "Bad guys"
- "Good guys"
- Your guys



THALES

Main drivers for using encryption

- Compliance
- "To Protect"
- No breach disclosure regulations



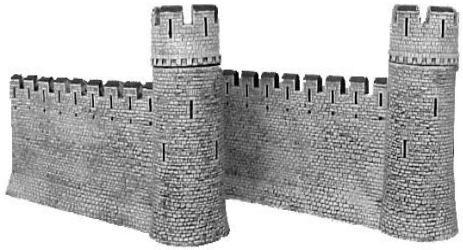
THALES

Take Aways

1. Cryptography is critical in our everyday life

2. Information is valuable

3. Perimeter security is not enough



4. Customers, Employees and Citizens expect you to protect them

THALES

ae CERT Computer Emergency Response Team
فريق الاستجابة لطوارئ الحاسب الآلي

Incident Response

INCIDENT RESPONSE PROCESS

FORENSICS

ae CERT

Computer Emergency Response Team

فريق الاستجابة لطوارئ الحاسب الآلي

1 ADVISORY, EDUCATION AND AWARENESS

Context and Dependencies

Acting as a trusted entity, aeCERT will facilitate such small-group interactions and insure that information interchange and decisions are recorded and communicated in a responsible manner. This interchange will be conducted through hosting information security related events and conference, in addition to sectorized information security forums and round tables.

This section will be responsible in providing alerts and announcements through social media to inform constituents about new developments, such as newly found vulnerabilities or intruder tool.

The services that are provided to the constituents are the following:

CODE	AE-1
TITLE	Information Security Awareness and Workshops
SERVICES DESCRIPTION	Conduct awareness sessions, workshops and seminars about information security in conjunction with the relevant government entities, private sector, academia and public. Providing security assessment before and after the session to evaluate the understanding of the human resources of the session given to them.

CODE	AE-2
TITLE	Specialist Information Security Training
SERVICES DESCRIPTION	Provide structured education and knowledge transfer to constituents about information security issues through formal workshops, training courses, tutorials and simulation facilitated. Providing security assessment before and after the session to evaluate the understanding of the human resources of the session given to them.

2 SECURITY QUALITY

Context and Dependencies

In order to maintain a secure network, it is advisable to perform tests on active networks periodically on a continual basis. This will minimize the risk of attacks and cyber threats since the systems will be up-to-date and patched to the latest updates. Furthermore, aeCERT provides two services to ensure that security quality standards are being met.

Those services are described below:

CODE	SQ-1
TITLE	Vulnerability Assessment
SERVICE DESCRIPTION	Detecting and assessing vulnerabilities in a constituent's IT infrastructure. Provide details of the vulnerabilities and recommendations to fix them.

CODE	SQ-2
TITLE	Penetration Testing
SERVICE DESCRIPTION	Attempting to gain access to the constituents IT infrastructure by exploiting detected vulnerabilities. This service will help assess the efficiency of the security control in place and aims to improve them.

3 MONITORING AND RESPONSE SERVICES

Context and Dependencies

Monitoring and Response team provides specific and specialized security advice to constituents, in addition to offering the most appropriate recommendations that may help in remediating the incident.

The Monitoring and Response team will be responsible for providing proactive services in the form of preliminary alerts and advisories to constituents to improve their infrastructure and related security processes prior to any incident or event occurs or is detected. In addition to, providing support and advice during remediation and recovery from security incidents.

CODE	MR-1
TITLE	Critical Infrastructure Monitoring & Intelligence Gathering
SERVICE DESCRIPTION	Develop actionable intelligence from the analysis threat, incident and vulnerability data. This information, as well as announcements, guidelines, or recommendations that pertain to longer term security issues.

CODE	MR-2
TITLE	Provide Digital Forensics Analysis Services
SERVICE DESCRIPTION	Forensics services include digital forensics investigations (computer forensics and mobile forensics), data recovery and data wiping.

CODE	MR-3
TITLE	Provide Website Defacement Monitoring
SERVICE DESCRIPTION	Crawling constituent websites and alert them in case of a defacement or failure in reachability is detected.

CODE	MR-4
TITLE	Conduct Virus & Malware Analysis
SERVICE DESCRIPTION	Study the behavior of the malware and analyze it malicious system and network activities in infected system.

How to React to…?

Viruses

Accidents

Denial of Service

Stolen Laptop

Social Engineering

THEFT OF PROPRIETARY INFORMATION

System Failure

Hacker Intrusion

Lost Backup Tape

Fire!

Incident Response

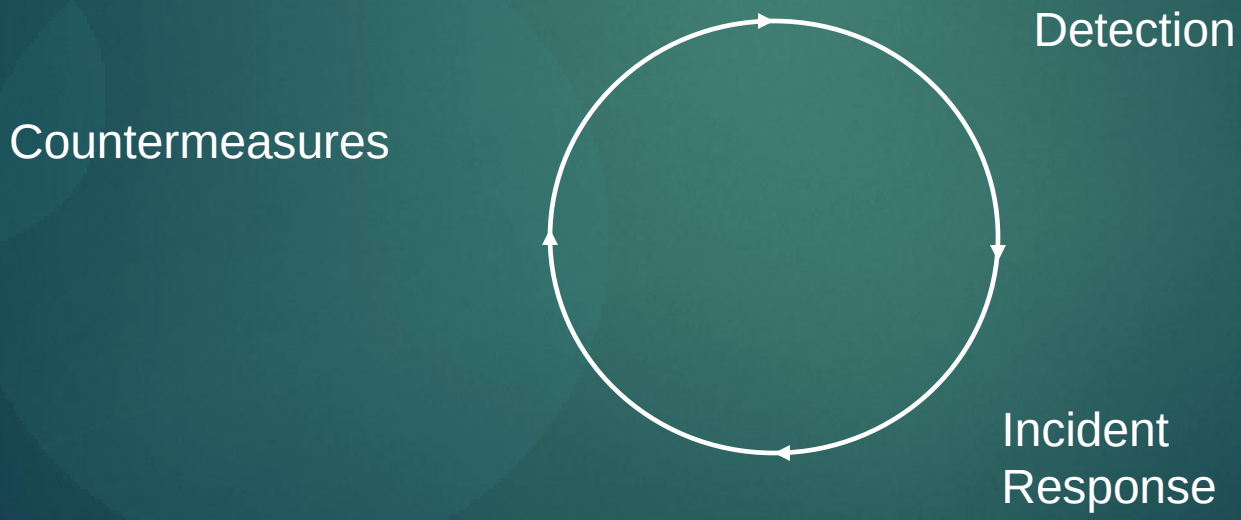
- Incident Response: deals with
  - Adverse events that threaten security.

Incident Response

- Harassment
- Extortion
- Pornography Traficking
- Organized Crime Activity
- Subversion
  - Bogus financial server
- Hoaxes

Incident Response

- Incident Response: Actions taken to deal with an incident.



Rationale for Incident Response

- Abundance of Security-Related Vulnerabilities.
- Availability of Attack Systems and Networks.
- Actual and Potential Financial Loss
- Potential for Adverse Media Exposure
- Need for Efficiency
- Limitations in Intrusion Detection Capabilities.

Incident Response Risk Analysis

- Annual Loss Expectancy (ALE)\
  - Quantitative
  - Qualitative

Incident Response Risk Analysis

- No generally accepted methodology for assessing risks.
- Criteria:
  - Monetary costs.
  - Operations impact.
  - Public relations fallout.
  - Impact on humans.

Incident Response Risk Analysis

- Risk Categories:
  - Break-in.
    - Break-in in a single system at NASA delayed a launch.
    - System was mission critical.
    - Needed to be recertified before launch.
  - Unauthorized execution of programs or commands.
  - Privilege Escalation.
  - Exploitation of CGI
    - Web servers have frequently cgi scripts installed for demonstration purposes.
    - These have known weaknesses.

Incident Response Risk Analysis

- Denial of Service attacks
- Web Defacement
- Virus and worm attacks
- Malicious active content
- Back door attacks
- Spoofing
- Session tampering, hijacking, replay

Incident Response vs. Business Continuity

Incident Response Planning (IRP)

- Security-related threats to systems, networks & data
- Data confidentiality
- Non-repudiable transactions

Business Continuity Planning

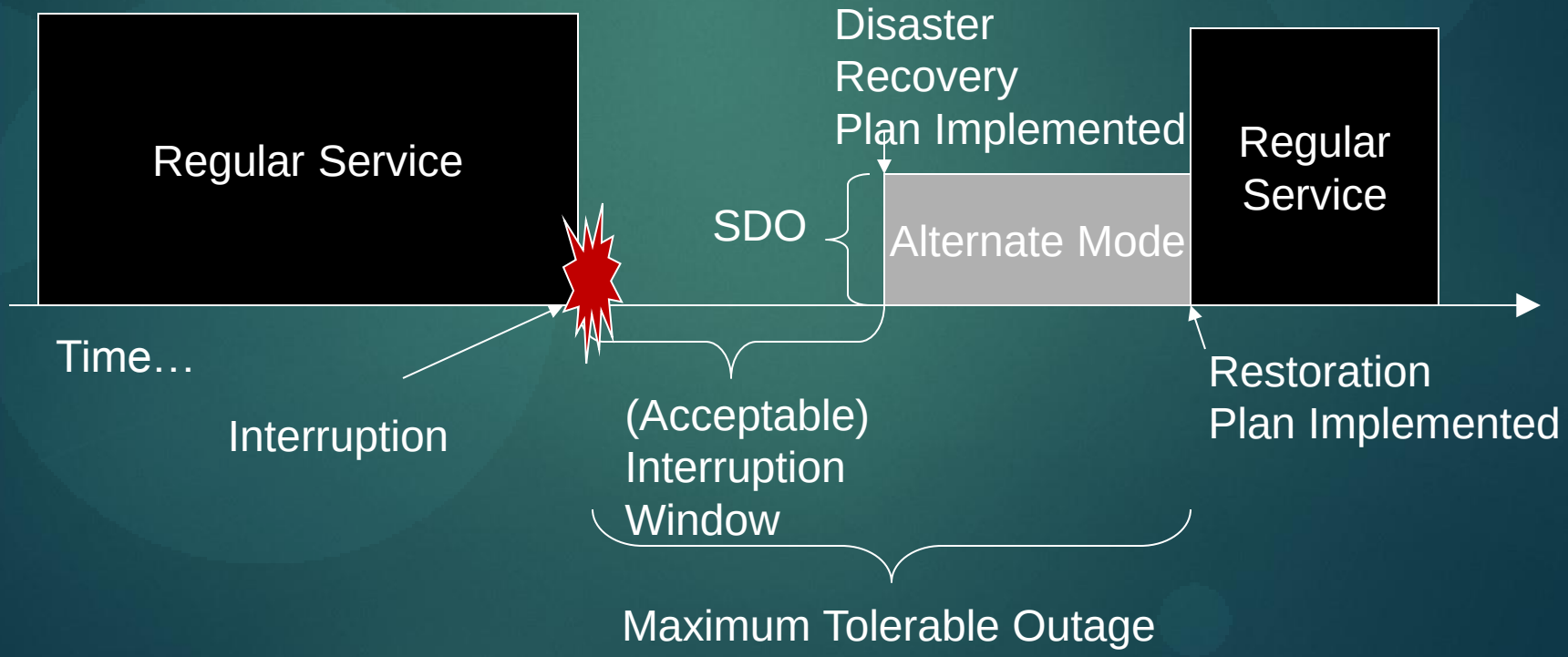
- Disaster Recovery Plan
- Continuity of Business Operations
- IRP is part of BCP and can be *the first step*

Recovery Terms

Interruption Window: Time duration organization can wait between point of failure and service resumption

Service Delivery Objective (SDO): Level of service in Alternate Mode

Maximum Tolerable Outage: Max time in Alternate Mode



Senior Eng. Mohammed Nader Fikri
Monitoring, Incident Handling & Response Analyst

PO Box: 116688 Dubai, United Arab Emirates
M: +971 50 5251212
D: +971 4 230 0345
F: +971 4 230 0940

Mohammed.fikri@aecert.ae

0505251212


Thank You