Public Policy on Network Security that affects to Telecommunications Industry in Europe

Cyber Security Conference Bangkok, August 10th 2018

Jens Broberg, VP Head of security Operations, Telenor Group

INTRODUCTION

EU is strengthening their Cyber Security Posture and pushing for Cyber Security Certifications.

Jens will talk about how EU initiatives to increase cyber resilience and how Telenor works with cybersecurity based on a continuously updated risk and threat picture and provide perspectives on regulations and national capabilities.

As well as the need for Authorities & industry to collaborate to succeed in providing Cyber security for societies.

Jens Broberg,
BSc Security & Risk management,
jens.broberg@telenor.com

- **VP, Head of Security Operations @ Telenor**
- **Director, Head of Security Operations @ Ericsson**
- **Director, Head of Security @ Ericsson Middle East**
- **Volunteer: Head of Security for Ericsson Response** (NGO org supporting UN with communication in disaster zones)
- **11 years in Swedish Defense Force**

Agenda

- Presentation of Telenor Global Business Security
- EU Cyber security Policy and developments
- Conclusion / Recommendation
- Questions

172 MILL. SUBSCRIPTIONS ACROSS SCANDINAVIA AND ASIA

TELENOR NORWAY
SUBS: 3 MILLION
FOUNDED: 1855
The country's largest telecom operator

TELENOR SWEDEN
SUBS: 2.6 MILLION
ENTRY: 2001
The country's second largest mobile operator

TELENOR DENMARK
SUBS: 1.8 MILLION
ENTRY: 2004
The country's second largest mobile operator

TELENOR PAKISTAN
SUBS: 40 MILLION
ENTRY: 2004
The country's second largest mobile operator

GRAMEENPHONE
BANGLADESH
SUBS: 59.9 MILLION
ENTRY: 1996
The country's largest mobile operator. Listed on the Dhaka Stock Exchange and the Chittagong Stock Exchange

TELENOR MYANMAR
SUBS: 18.8 MILLION
ENTRY: 2013
The country's second largest mobile operator

DTAC
THAILAND
SUBS: 24.3 MILLION
ENTRY: 2000
The country's third largest mobile operator. Listed on the Stock Exchange of Thailand and Singapore Exchange

DIGI
MALAYSIA
SUBS:11.8 MILLION
ENTRY: 1999
The country's third largest mobile operator. Listed on Bursa Malaysia

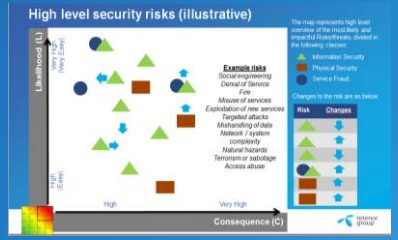
Telenor Group is one of the world's major mobile operators. We keep our customers connected across Scandinavia and Asia. Our more than 30,000 employees are committed to responsible business conduct and being our customers' favourite partner in digital life. Connecting the world has been Telenor's domain for more than 160 years, and we are driven by a singular vision: to empower societies.

With effect from Q1, Telenor India is treated as an asset held for sale and discontinued operations in Telenor's financial reporting.

The Telenor Group is listed on the Oslo Stock Exchange

telenor group

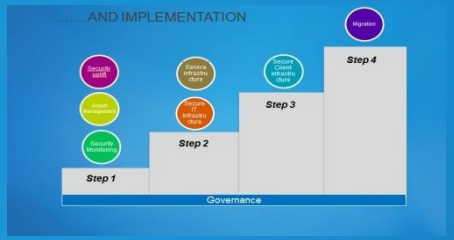
THE CYBER SECURITY JOURNEY – TELENOR GROUP



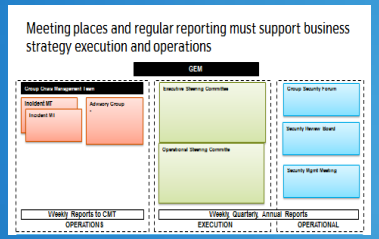
Calibrate risks

Strategy

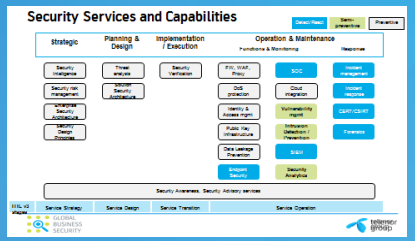
Set Ambitions



Implement Defendable Architecture



Define Governance



Develop Capabilities

Executive sponsors

Global Operating Model

Security culture

A Vision for Security in 2020

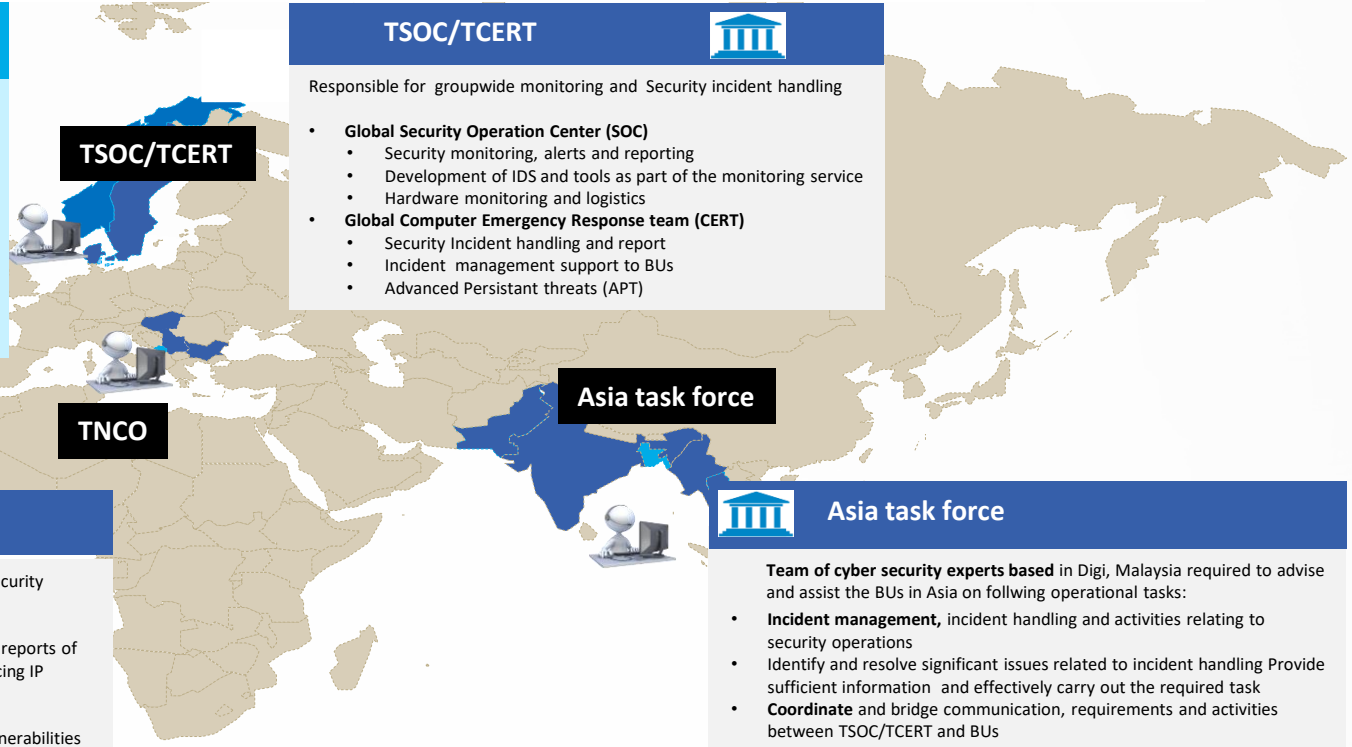
We always protect people in their digital life and security is the foundation for everything we do

GLOBAL OPERATING MODEL WITH SEVERAL DELIVERY CENTRES

GBS

Global responsibility for developing, implementing and maintaining a consistent and visible security culture throughout Telenor Group with the following functions:

- **Security Governance**
- **Security Operations**
- **Transformation and Projects**
- **Business Development**
- **Security Intelligence**



TSOC/TCERT

Responsible for groupwide monitoring and Security incident handling

- **Global Security Operation Center (SOC)**
  - Security monitoring, alerts and reporting
  - Development of IDS and tools as part of the monitoring service
  - Hardware monitoring and logistics
- **Global Computer Emergency Response team (CERT)**
  - Security Incident handling and report
  - Incident management support to BUs
  - Advanced Persistant threats (APT)

"TNCO"

Responsible for the following groupwide security areas:

- **Vulnerability Management**
  - Managed vulnerability scans and reports of mobile networks and Internet facing IP infrastructure
  - Reports of all findings
  - Project management to track vulnerabilities and remediation assignment

Asia task force

Team of cyber security experts based in Digi, Malaysia required to advise and assist the BUs in Asia on follwing operational tasks:

- **Incident management,** incident handling and activities relating to security operations
- Identify and resolve significant issues related to incident handling Provide sufficient information and effectively carry out the required task
- **Coordinate** and bridge communication, requirements and activities between TSOC/TCERT and BUs
- Provide **awareness** and report on key **risk** and concerns encountered in the course of security operations activities

CYBER SECURITY – A MATTER OF INTERNATIONAL HEADLINES

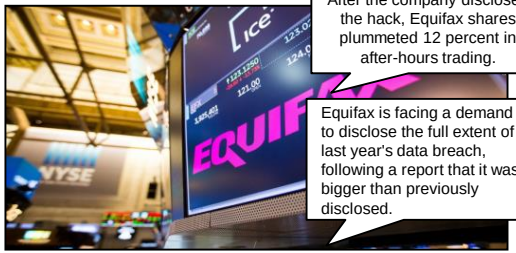
Singapore's government health database in the country's worst breach of personal data, stealing records on 1.5 million patients including the prime minister's own personal drug prescriptions. Monday, 23 Jul 2018

Hackers have infiltrated Singapore's government health stealing records on 1.5 million patients

50 million Facebook profiles harvested for Cambridge Analytica in major data breach
The Guardian, March 17th 2018

Facebook's shares lost 5 per cent of their value overnight in response to claims that the company did not adequately protect its users' data.

Data of 143 million Americans exposed in hack of credit reporting agency Equifax,
Washington Post, Sep 5th 2017



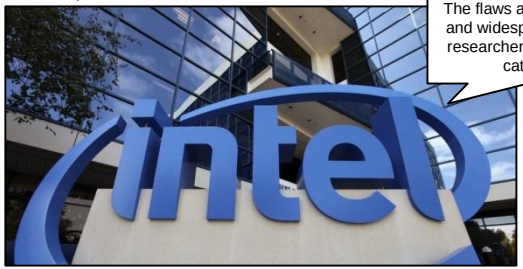
After the company disclosed the hack, Equifax shares plummeted 12 percent in after-hours trading.

Equifax is facing a demand to disclose the full extent of last year's data breach, following a report that it was bigger than previously disclosed.

Swisscom data breach exposes 800,000 customers, Reuters, Feb 7th 2018

Unknown parties misappropriated the access rights of a sales partner, gaining unauthorized access to customer data.

Apple says Spectre and Meltdown vulnerabilities affect all Mac and iOS devices,
BBC, Jan 4th 2018



The flaws are so fundamental and widespread that security researchers are calling them catastrophic.

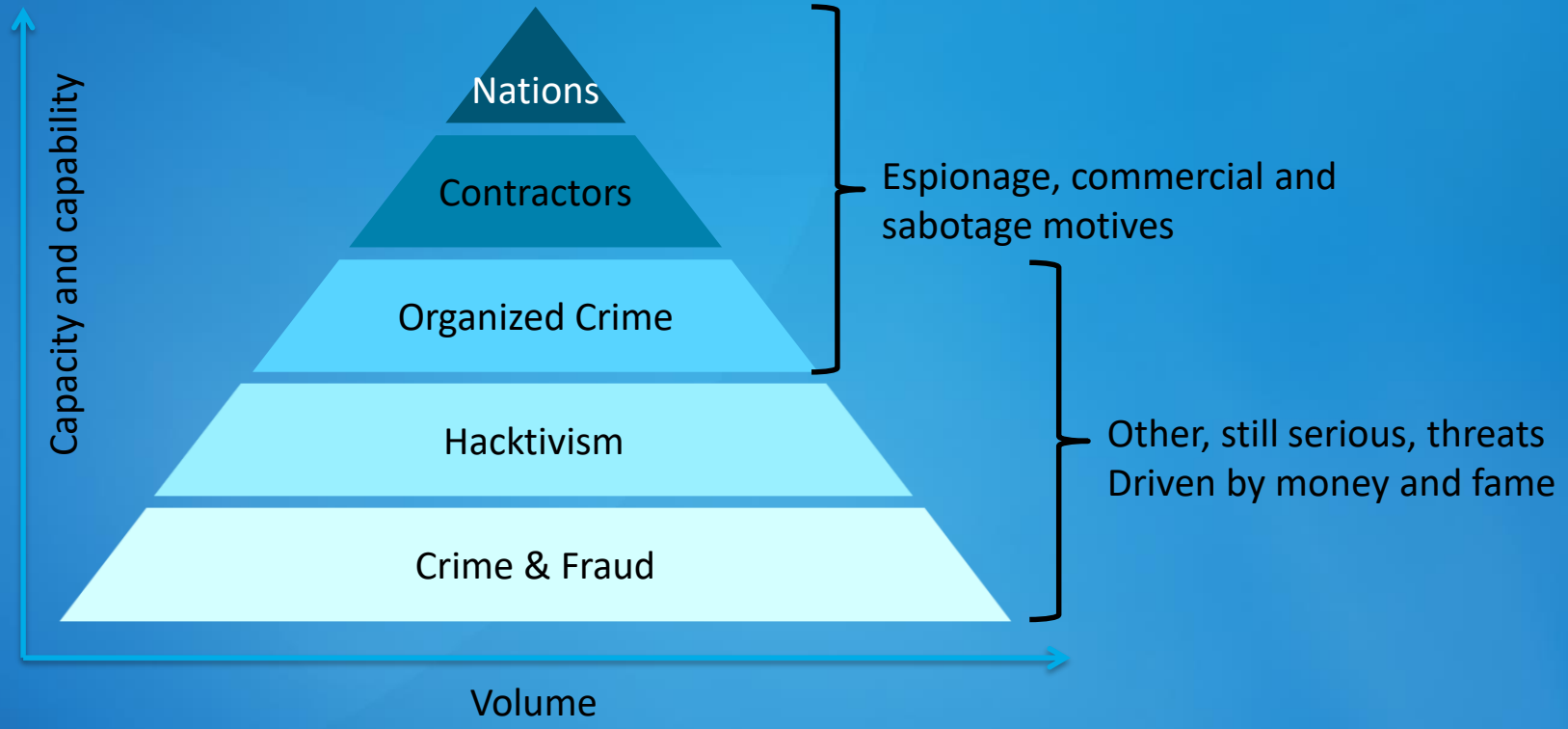
Deloitte hit by cyber-attack revealing clients' secret emails
Guardian, Sep 25th 2017

The hacker compromised the firm's global email unrestricted "access to all areas".

The breach affected up to 350 clients, some of which were very high profile, including US government departments.

telenor group

THREAT ACTORS - WHO ARE BEHIND CYBER ATTACKS?



CYBERSECURITY IS A CULTURAL CHANGE JOURNEY

Security threats are human adversaries ranging from simple crime to advanced persistent threats. Our industry needs to manage all levels.

Security is a change journey and we must master the basics in order to succeed with advanced threats.

Security culture is about much more than competency and technology, it is about mindset and behaviors. Security is everybody's responsibility.

CYBERSECURITY – PROTECTING PEOPLE IN THEIR DIGITAL LIVES WITH SECURITY AT THE FOUNDATION OF EVERYTHING WE DO

- To take the position as a trusted and secure provider in all markets, Telenor has to focus on customer data protection and defend our critical infrastructure.
- Cyber security threats have increased significantly and as a network operator and provider of digital services, cybersecurity has a high priority.
- We depend on our suppliers and third-parties. We depend on collaboration with the ecosystem to strengthen our security through our people, processes and technology.
- We believe that new cybersecurity legislation (e.g., security of critical infrastructure and customer data) should take a risk based approach based on an assessment of the proportionality of regulatory intervention, applied consistently across and with flexibility for technological changes and cross border data transfer.
- Governments and policy makers must continue to expand their focus to ensure that citizens are informed and equipped to deal with cybersecurity.

April 2018

telenor group

Cybersecurity – Protecting people in their digital lives, with security at the foundation of everything we do

To take the position as a trusted and secure provider in all markets, Telenor has to focus on customer data protection and defend our critical infrastructure.

The cyber security threat has increased significantly over the past few years due to the digitalisation of society and customers' use of digital networks and services. Extreme weather, human and technical errors or hostile acts that manipulate or paralyse networks and services are factors that make us vulnerable.

As a network operator and provider of digital services, cybersecurity has high priority at Telenor. The quality and reliability of our telecommunications services depends on the stability of our network and the networks of other service providers with which we interconnect. These networks are vulnerable to damage or service interruptions, some of which could be caused by cybersecurity attacks. Repeated, prolonged or complex network or IT system failures could damage our services and consequently weaken the trust our customers place in us as a reliable communications provider.

We depend on suppliers and third-party providers for supply and maintenance of equipment and services. Problems related to the supply chain may adversely affect our business and operations. We work closely with our suppliers to prevent any loss, misuse or unauthorised disclosure of confidential information. This includes placing high security demands on our suppliers, who must ensure adequate levels of privacy and security to stay in business. Telenor conducts a high degree of network monitoring and carries out announced and un-announced inspections of the work performed by third parties.

In the following we present our view on how to respond to the global cybersecurity challenge.

Telenor's Commitment

Telenor is committed to providing secure, well-functioning networks and services, and has a strong interest in doing so. Our customers and society in general should have confidence in Telenor as a trustworthy supplier of safe, reliable and secure telecommunications and digital services.

To meet the fast evolving threats in the cyber domain, Telenor has developed a holistic, Group-wide and long-term security strategy aiming at securing Telenor's global business. A key element in this strategy is to continue to build critical security capabilities and competencies in all Telenor companies, as well as establishing a global security operating model. To Telenor, security is our license to operate.

A secure infrastructure built on collaboration

At Telenor we are continuously developing governance, culture and competence in order to strengthen our ability to design, deploy and operate secure infrastructure and services, both internally and externally through collaboration with our suppliers and third-party providers. This includes developing and strengthening our security monitoring system and tools, our processes, organisation and people.

A key objective for Telenor is to protect people in their digital life with security at the foundation of everything we do. To accomplish this, we are investing in security competence across our own organisation as well as with our suppliers and third-party providers, to ensure the same level of

https://www.telenor.com/media/public-policy/cybersecurity-a-must-win-battle-for-telenor/

EU DEVELOPMENTS - CYBERSECURITY

Cybersecurity is an absolute priority for the EU. The European Commission adopted a cybersecurity package in September 2017 to improve:

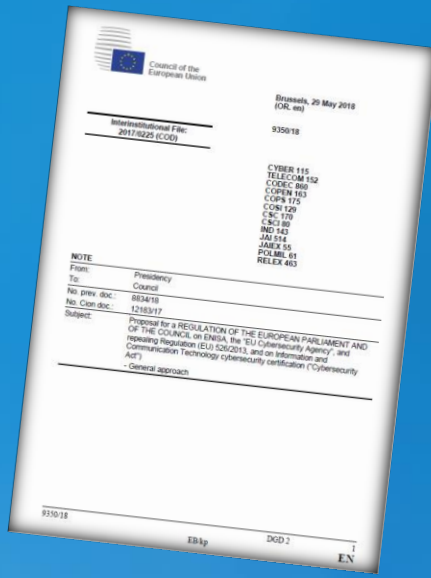
- ✓ Resilience (Proposal for a Regulation (Cybersecurity Act), Communication "Making the most of NIS" and “Blueprint” Recommendation to Member States on the coordinated response to large-scale cybersecurity incidents and crises
- ✓ Deterrence (with special focus on cybercrime)
- ✓ Defense (with special focus on international dimension and relations EU/NATO)

Cyber Security in Europe http://www.consilium.europa.eu/en/policies/cyber-security/

EU CYBERSECURITY ACT

Council expected to adopt a General Approach on the Cybersecurity Act at the Council of Ministers on 8th June 2018.

- ✓ Sets up a European Certification Framework to reduce / avoid fragmentation in the Digital Single Market and promote cybersecurity certification in a generalized manner in Europe.
- ✓ Provides ENISA with more resources (mandate, budget, staff) and defined role in the European Security Certification Framework (Operational cooperation, capacity building, information sharing).
- ✓ Lays down the procedure for creation of EU-wide voluntary certification schemes for specific products or services. Risk based approach, more product information for consumers, improved governance, common actions and stronger member state participation.


Council of the European Union

Brussels, 29 May 2018
(OR. en)

Interinstitutional File:
2017/0225 (COD)

9350/18

CYBER 115
TELECOM 152
CODEC 860
COPEN 163
COPS 175
COSI 129
CSC 170
CSCI 80
IND 143
JAI 514
JAIEX 55
POLMIL 61
RELEX 463

NOTE
From: Presidency
To: Council
No. prev. doc.: 8834/18
No. Cion doc.: 12183/17
Subject: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")
- General approach

9350/18 EB/kp DGD 2 1 EN

THE EU GENERAL DATA PROTECTION REGULATION (GDPR)

- Increased territorial scope (extra-territorial applicability)
- Penalties
- Consent
- Breach notification
- Right to access
- Right to be forgotten
- Data portability
- Privacy by design
- Data protection officers

Telenor position «Ensuring safe use of new technogies»: https://www.telenor.com/media/public-policy/privacy-position/

SWEDEN

SOFF
Swedish Security & Defence Industry Association

- There are strong forces in Industry pushing for a clearer strategic partnership between public and private sector in Sweden.
- Private companies have very good insight in new technology and R&D and there needs to be a systematic dialog between the public and private actors in the cyber defense arena.
- One area that is critical is Threat intelligence, situational awareness and understanding of the risk and threats that in the cyber arena.
- Maybe most important: a strategic approach in terms of competence training in the Cyber Security area.

USA

Gen. Paul Nakasone, shown in this video capture during an appearance at the Aspen Security Forum July 21, is advocating for a more expansive partnership between the government and the private sector amid an array of cyberthreats.

- Information from Cyber Command and the NSA will be used in a new National Risk Management Center that hopes to share cyber threats between the government and the private sector
- ”Resiliency begins with a dialogue,” Nakasone said.
- Bridge the gap between the government and some of the top companies in the United States that make up the critical parts of American digital life.

CHALLENGES AND OPPORTUNITIES

telenor group

Challenges

- ✓ Cost – Best practice Cyber security, Best practice IT, Training, Certification,
- ✓ Continuously evolving threat landscape
- ✓ Lack of Collaboration
- ✓ Lack of competence and experienced Cyber security professionals

Opportunities

- ✓ Commitment
- ✓ Collaboration between Governments, Education & Private sector
- ✓ Strategic initiatives with universities
- ✓ Military service as a cyber specialist
- ✓ Compliance to National Cyber Security Policies

RECOMMENDATIONS

Collaboration

- Encourage and nurture close and trusted public – private collaboration
- Confidential exchange of threat information between parties
- Reward transparency and openness about threats
- Build a framework for crisis / incident preparedness
- Establish clear guidelines and interfaces for notifications
- Education & Universities

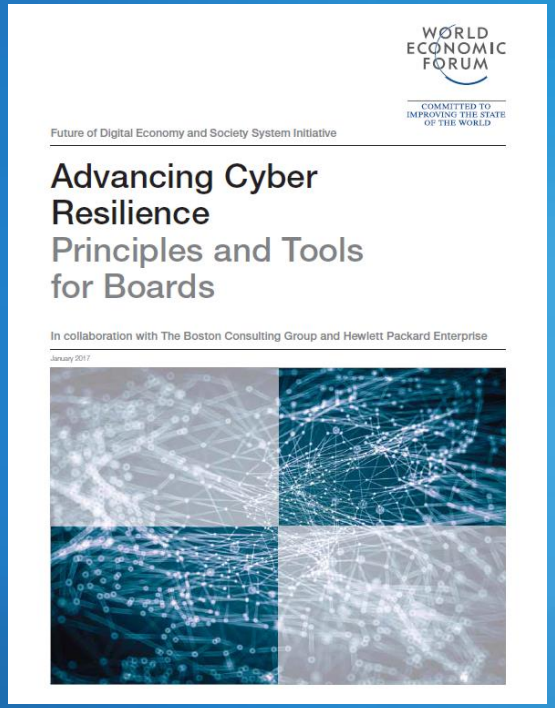
Capabilities

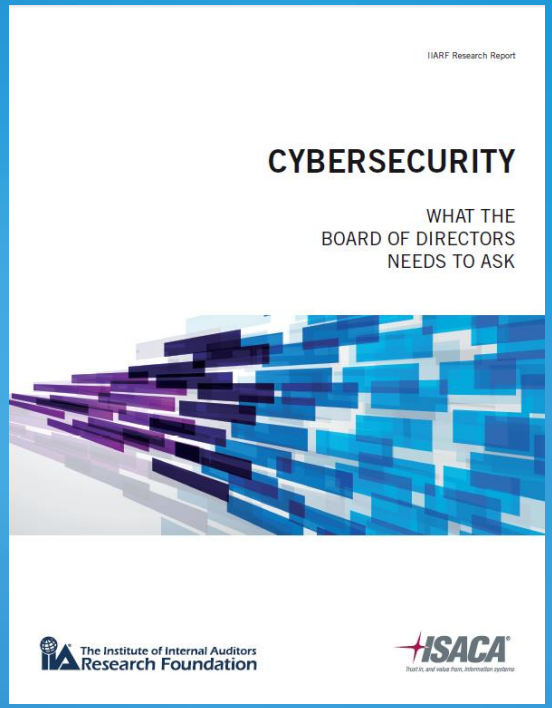
- Build and develop expert capabilities to support the industry
- Invite industry to support establishing and developing capabilities
- Invest in strengthening public cybersecurity awareness

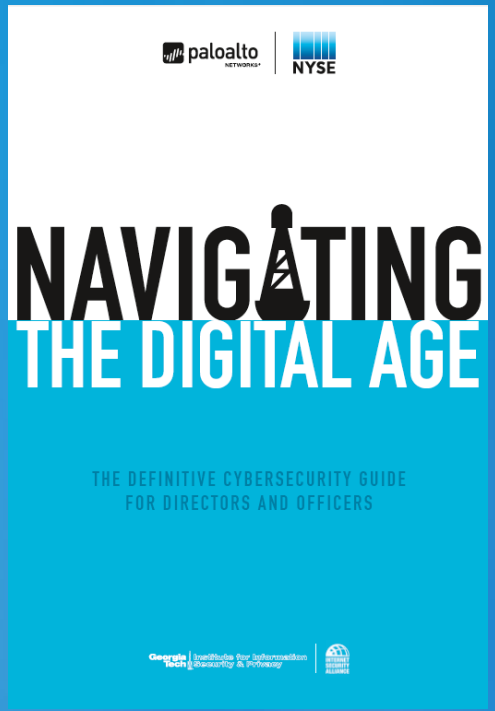
Regulation and frameworks

- Risk based and consistent regulation that enable new technologies
- Encourage the use of standards and certification

CYBER SECURITY TOOLKIT FOR EXECUTIVES AND BOD MEMBERS







Questions and answers