THE FUTURE OF FINANCE SUMMIT
SHANGRI-LA, BANGKOK, THAILAND
29 - 31 MAY 2019

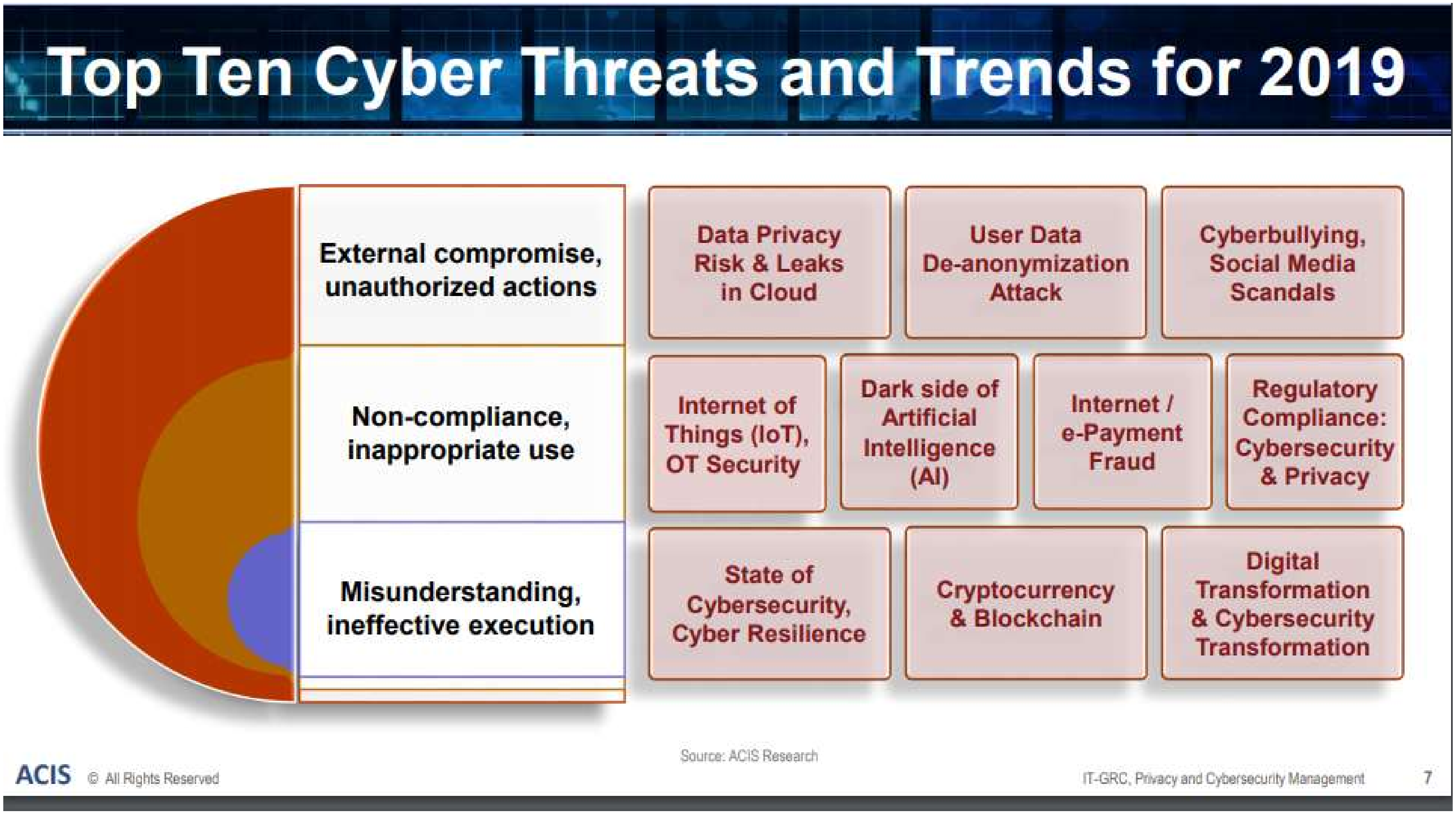
Managing Cybersecurity Risk in the Digital Age

Workshop - 29 May 2019

Admin Program

1. Overview of entire day course (1 hr)
2. Discussion on specific needs of participants (course will be tailored to suit the majority of participants) – 30 minutes
3. Course materials will be emailed to participants
4. Workshop presentation (interactive)
5. Practical exercise (3 to 5 pm)
    1. How to prepare a cybersecurity GRC program
    2. Next steps

Executive Vice President Head of Financial Governance Risk and Compliance Division	Bank of Ayudhya
Senior Vice President Head of Audit Center of Excellence Division	Bank of Ayudhya
Senior Vice President Head of Digital Security and Information Technology Audit Division	Bank of Ayudhya
Head of Channel and Integration Services, Buisness Analysis	Kasikornbank
Head of Operational Risk Department	Bank of Ayudhya
Manager	Bank Islam Brunei Darussala Berhad
Senior Vice President, Head of Risk Management	Maybank Kim Eng Securities



Top Ten Cyber Threats and Trends for 2019

External compromise, unauthorized actions

Non-compliance, inappropriate use

Misunderstanding, ineffective execution

- Data Privacy Risk & Leaks in Cloud
- User Data De-anonymization Attack
- Cyberbullying, Social Media Scandals
- Internet of Things (IoT), OT Security
- Dark side of Artificial Intelligence (AI)
- Internet / e-Payment Fraud
- Regulatory Compliance: Cybersecurity & Privacy
- State of Cybersecurity, Cyber Resilience
- Cryptocurrency & Blockchain
- Digital Transformation & Cybersecurity Transformation

Source: ACIS Research

ACIS © All Rights Reserved

IT-GRC, Privacy and Cybersecurity Management 7

Source: Presentation entitled “Business Driver and Cybersecurity in Digital Transformation” by ACIS PROFESSIONAL CENTER 140/1 Kian Gwan Building 2, 18th Floor, Wireless Road, Lumpini, Pathumwan, Bangkok 10330, Thailand www.acisonline.net ACIS Professional Center Co., Ltd.

AGENDA: Strategic Perspectives

Why top management need to worry about cybersecurity breaches in the companies and businesses.

1. How can I be effective in managing risk at the strategic level in the context of legal and regulatory framework?
2. How do I optimise resources to manage legal & regulatory compliance domestically as well as on a cross border basis?
3. How do I manage the 3 levels of compliance in an integrated and holistic manner:
    - National cybersecurity and compliance laws.
    - Internal corporate compliance & governance requirements.
    - Operational compliance requirements and standards.

Agenda: Leadership & Implementation issues

Implementation Challenges:
What are the challenges to management in implementing a robust and effective Cybersecurity Governance, Risk & Compliance framework within the corporate institutions?

Cybersecurity – Policy and management strategy

- Role of Management and the Leadership team
- Elements of an effective Cybersecurity Governance, Risk & Compliance programs

Agenda: Industry Concerns

How Cybersecurity Laws affect providers of financial services?
What are the industries’ concerns in relation to regulatory over reach in cases involving cybersecurity data breaches?

Perspectives from:

- Banks and financial institutions
- Security and Asset management Companies
- Fintech and start-ups
- Insurance companies
- Regulators and policy makers

Country Case Study

The Singapore Smart Nation Approach

Brief synopsis on the Cybersecurity Laws formulated in Singapore effective August 2018.

Objectives:

1. Strengthening the Protection of Critical information Infrastructure against cyber attacks
2. Authorise Cyber Security Agencies and respond to cybersecurity threats and incidents.
3. Establish a framework for sharing cybersecurity information.
4. Establish a light touch licensing framework for cybersecurity service providers.

CASE STUDY
Singhealth
Cyber attack

- The worst cyber attack in Singapore's history

Today's program at a glance…..

1. A step by step guide to develop a Cybersecurity GRC framework that will help organisations better protect their assets and reputation in the cyber risk environment.
2. How to proactively be ready for cyber attacks through an effective GRC framework that includes robust control measures through policies, procedures and training.
3. How to establish systematic control functions, procedural execution and timely management reporting
4. How to build auditable trust into routine assurance of ICT operations.
   - It includes real world examples and cases to illustrate key concepts and issues for programme participants.

Areas of coverage

- Identify, assess, and report on any information security risk or vulnerability
- Define common areas of risk as they relate to information security at appropriate operational intersections
- Design effective information security strategies
- Evaluate technology solutions and technical knowledge
- How to improve & enforce information security policies
- Develop a communication strategy to promote and expand information security awareness
- How to improve & strengthen information security policies, practices, and solutions, and ensure coverage and compliance across the enterprise

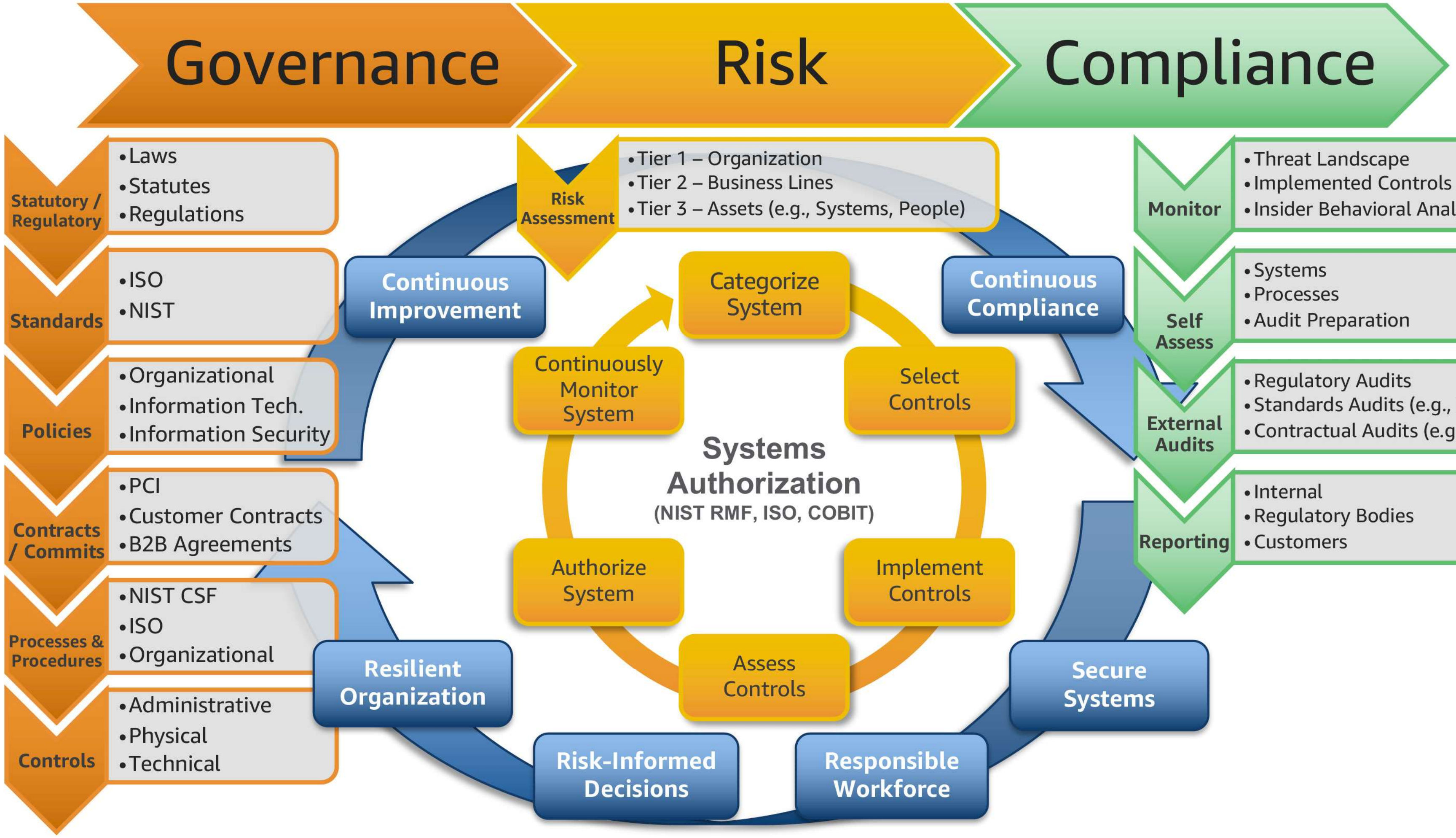
Expected Learning Outcomes

To be able to:

1. Design, develop and maintain a cybersecurity GRC framework geared towards creating a cyber resilient organisation.
2. Better manage cybersecurity risks through robust control measures and standard operating procedures as part of the GRC framework.
3. Ensure compliance with laws and regulations in a more effective manner.
4. Prepare organisations to be ready for cyber attacks in a structured and proactive manner from a human and cultural perspective.

Michael South
AWS, Americas Regional Leader for public sector security and compliance business development

"Governance, risk, and compliance (GRC) programs are sometimes looked upon as the bureaucracy getting in the way of exciting cybersecurity work. But a good GRC program establishes the foundation for meeting security and compliance objectives. It is the proactive approach to cybersecurity that, if done well, minimizes reactive incident response."



Governance

Risk

Compliance

Statutory / Regulatory
- Laws
- Statutes
- Regulations

Standards
- ISO
- NIST

Policies
- Organizational
- Information Tech.
- Information Security

Contracts / Commits
- PCI
- Customer Contracts
- B2B Agreements

Processes & Procedures
- NIST CSF
- ISO
- Organizational

Controls
- Administrative
- Physical
- Technical

Risk Assessment
- Tier 1 – Organization
- Tier 2 – Business Lines
- Tier 3 – Assets (e.g., Systems, People)

Continuous Improvement

Continuous Compliance

Secure Systems

Responsible Workforce

Risk-Informed Decisions

Resilient Organization

Systems Authorization

(NIST RMF, ISO, COBIT)

Categorize System

Select Controls

Implement Controls

Assess Controls

Authorize System

Continuously Monitor System

Monitor
- Threat Landscape
- Implemented Controls
- Insider Behavioral Analysis

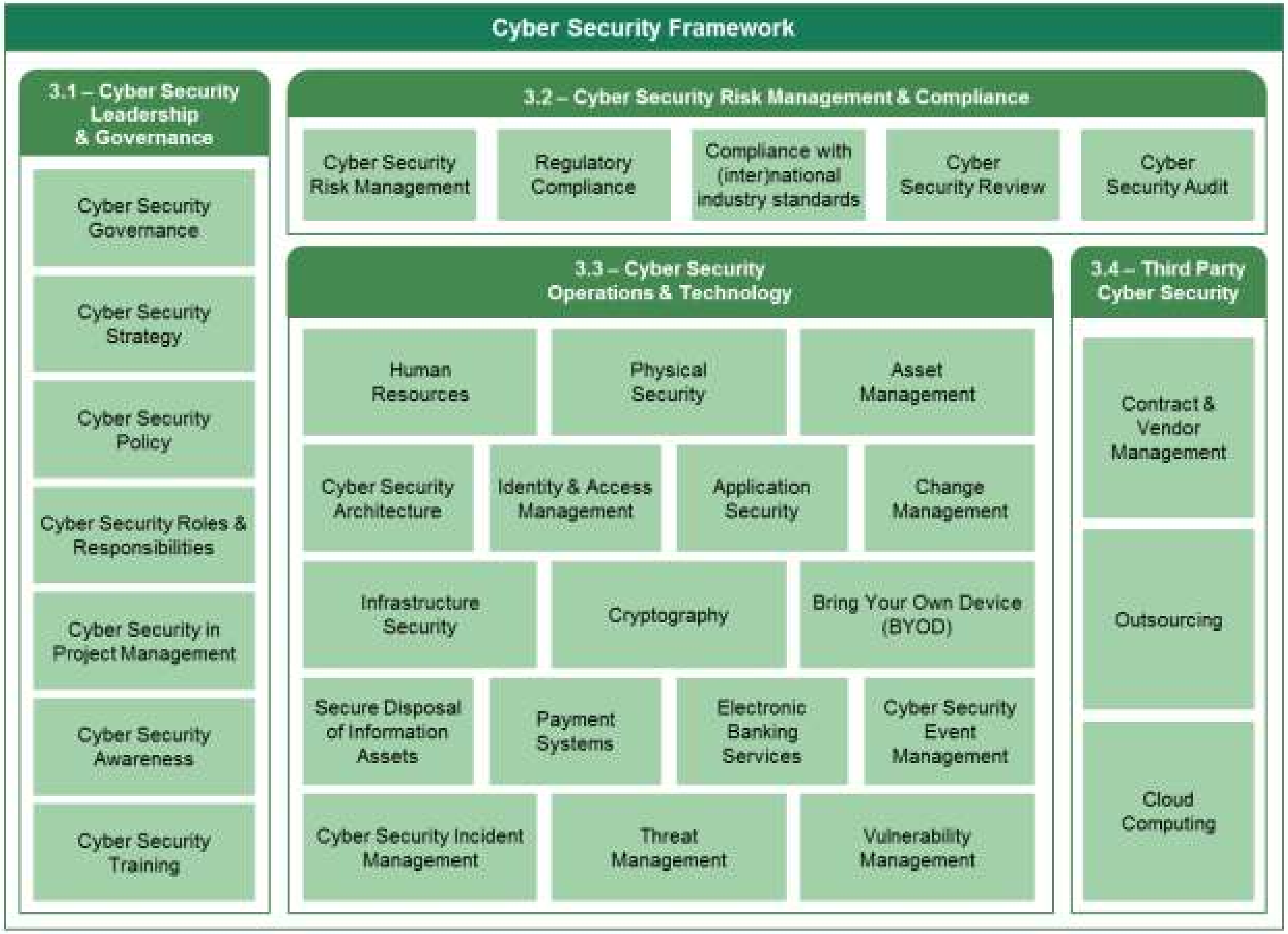
Self Assess
- Systems
- Processes
- Audit Preparation

External Audits
- Regulatory Audits
- Standards Audits (e.g., ISO)
- Contractual Audits (e.g., PCI)

Reporting
- Internal
- Regulatory Bodies
- Customers

https://aws.amazon.com/blogs/security/scaling-a-governance-risk-and-compliance-program-for-the-cloud/

The figure below illustrates the overall structure of the Framework and indicates the cyber security domains and subdomains, including a reference to the applicable section of the Framework.



Cyber Security Framework

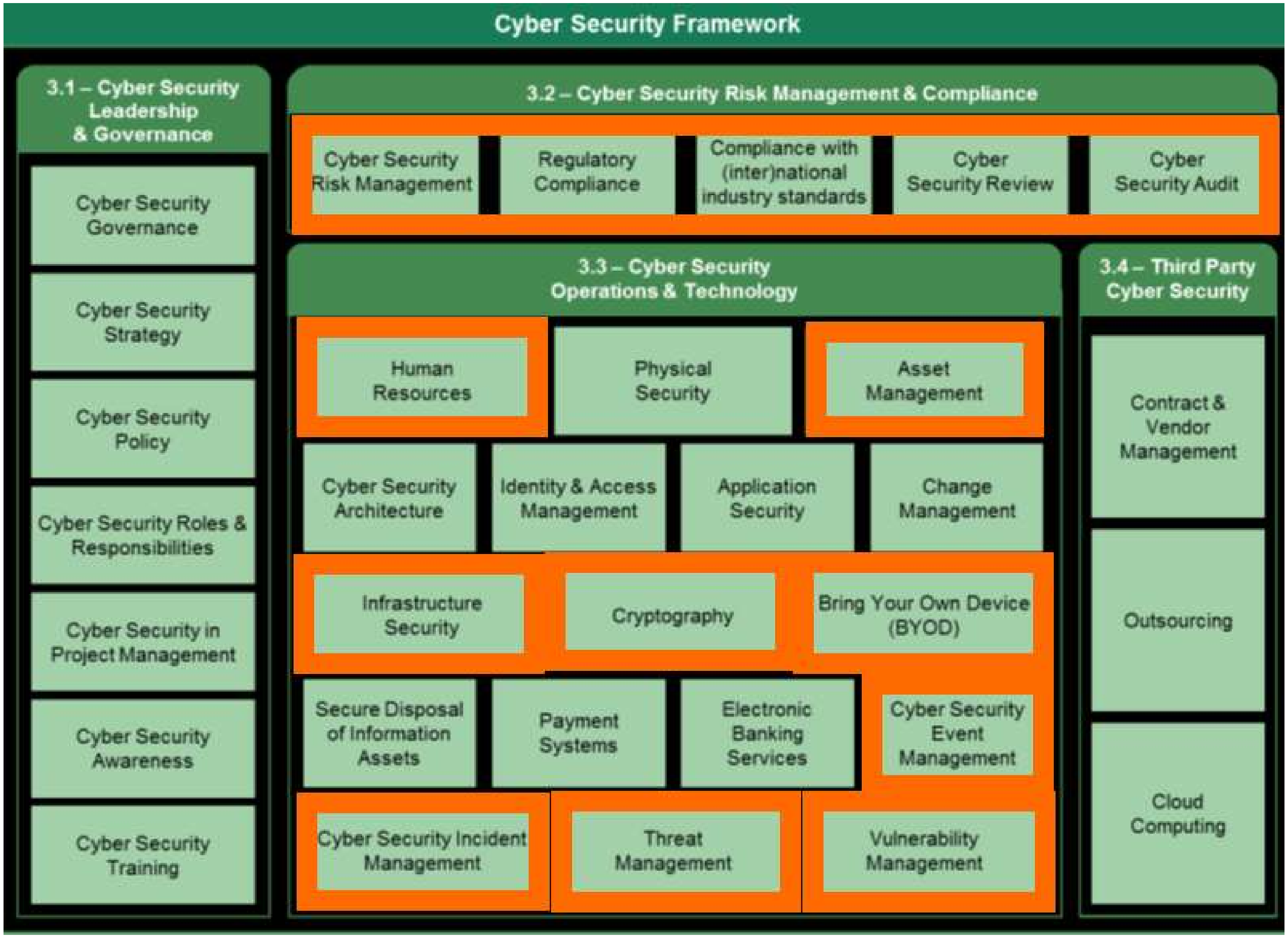
3.1 – Cyber Security Leadership & Governance
- Cyber Security Governance
- Cyber Security Strategy
- Cyber Security Policy
- Cyber Security Roles & Responsibilities
- Cyber Security in Project Management
- Cyber Security Awareness
- Cyber Security Training

3.2 – Cyber Security Risk Management & Compliance
- Cyber Security Risk Management
- Regulatory Compliance
- Compliance with (inter)national industry standards
- Cyber Security Review
- Cyber Security Audit

3.3 – Cyber Security Operations & Technology
- Human Resources
- Physical Security
- Asset Management
- Cyber Security Architecture
- Identity & Access Management
- Application Security
- Change Management
- Infrastructure Security
- Cryptography
- Bring Your Own Device (BYOD)
- Secure Disposal of Information Assets
- Payment Systems
- Electronic Banking Services
- Cyber Security Event Management
- Cyber Security Incident Management
- Threat Management
- Vulnerability Management

3.4 – Third Party Cyber Security
- Contract & Vendor Management
- Outsourcing
- Cloud Computing

Source: Cyber Security Framework
Saudi Arabian Monetary Authority



Cyber Security Framework

3.1 – Cyber Security Leadership & Governance

- Cyber Security Governance
- Cyber Security Strategy
- Cyber Security Policy
- Cyber Security Roles & Responsibilities
- Cyber Security in Project Management
- Cyber Security Awareness
- Cyber Security Training

3.2 – Cyber Security Risk Management & Compliance

- Cyber Security Risk Management
- Regulatory Compliance
- Compliance with (inter)national industry standards
- Cyber Security Review
- Cyber Security Audit

3.3 – Cyber Security Operations & Technology

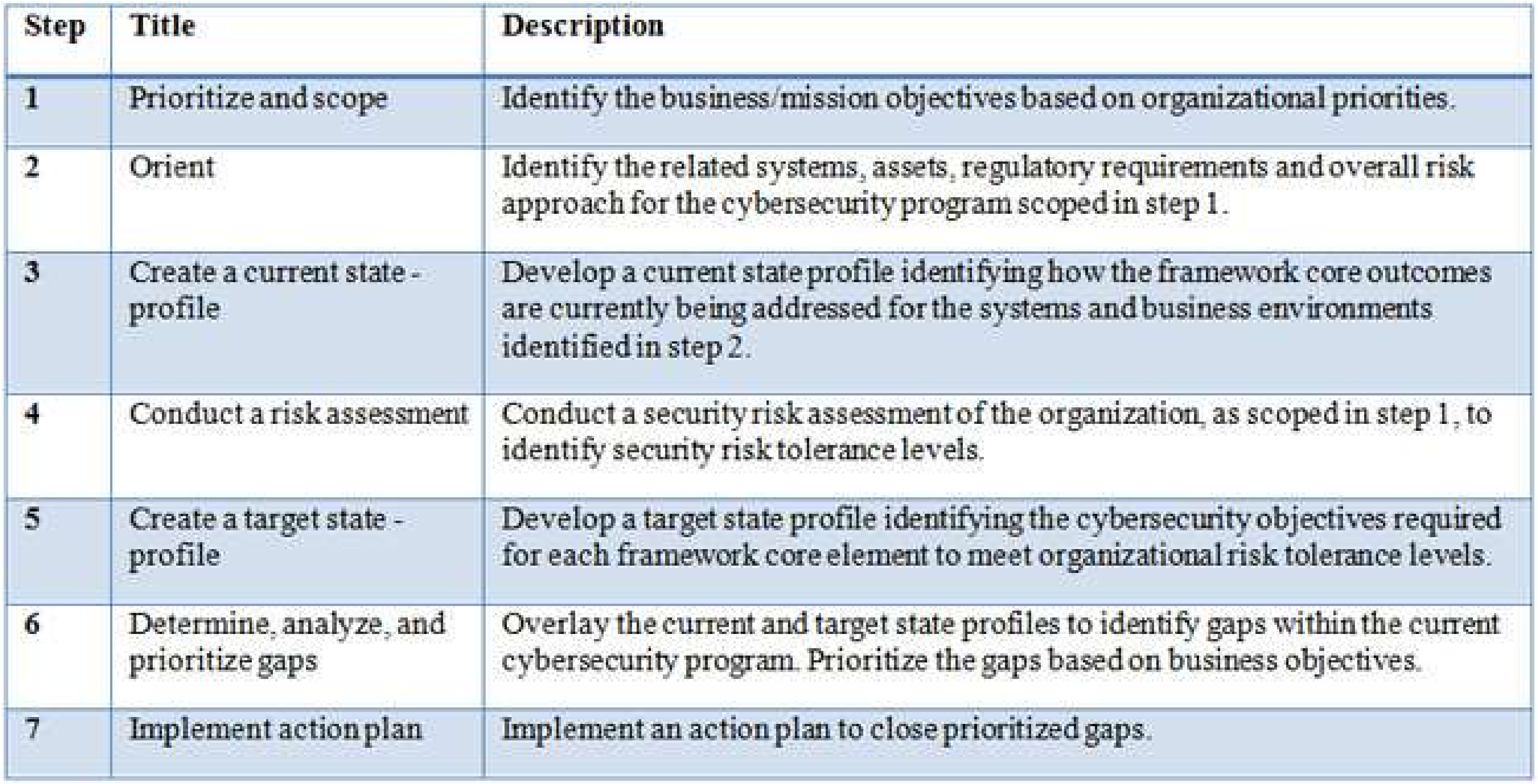
- Human Resources
- Physical Security
- Asset Management
- Cyber Security Architecture
- Identity & Access Management
- Application Security
- Change Management
- Infrastructure Security
- Cryptography
- Bring Your Own Device (BYOD)
- Secure Disposal of Information Assets
- Payment Systems
- Electronic Banking Services
- Cyber Security Event Management
- Cyber Security Incident Management
- Threat Management
- Vulnerability Management

3.4 – Third Party Cyber Security

- Contract & Vendor Management
- Outsourcing
- Cloud Computing

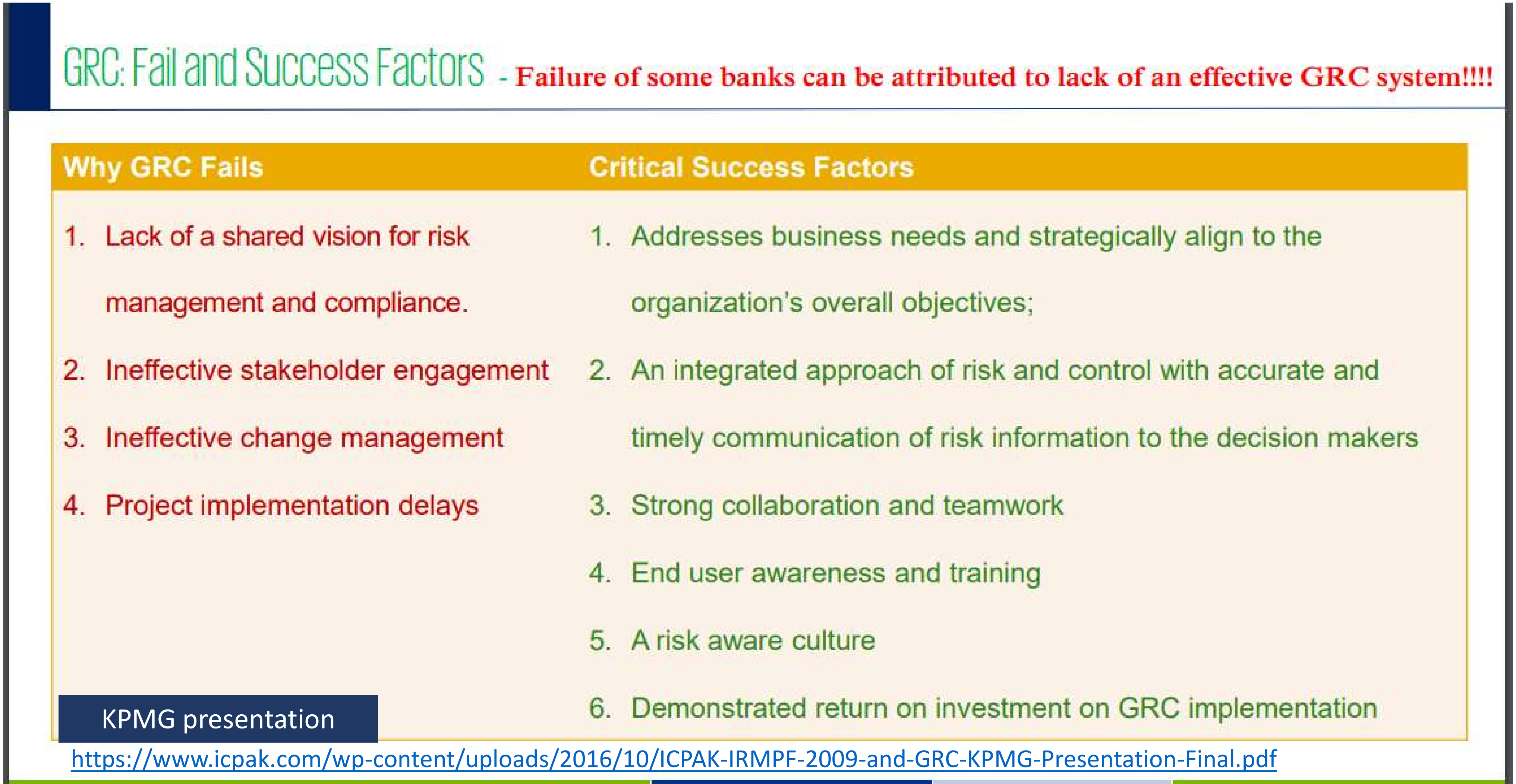
Source: Cyber Security Framework
Saudi Arabian Monetary Authority

Steps to implement a Cybersecurity GRC Program



Step	Title	Description
1	Prioritize and scope	Identify the business/mission objectives based on organizational priorities.
2	Orient	Identify the related systems, assets, regulatory requirements and overall risk approach for the cybersecurity program scoped in step 1.
3	Create a current state - profile	Develop a current state profile identifying how the framework core outcomes are currently being addressed for the systems and business environments identified in step 2.
4	Conduct a risk assessment	Conduct a security risk assessment of the organization, as scoped in step 1, to identify security risk tolerance levels.
5	Create a target state - profile	Develop a target state profile identifying the cybersecurity objectives required for each framework core element to meet organizational risk tolerance levels.
6	Determine, analyze, and prioritize gaps	Overlay the current and target state profiles to identify gaps within the current cybersecurity program. Prioritize the gaps based on business objectives.
7	Implement action plan	Implement an action plan to close prioritized gaps.

SOURCE: Greg Blake, Chief Information Officer, Idaho Housing and Finance Association



GRC: Fail and Success Factors - Failure of some banks can be attributed to lack of an effective GRC system!!!!

Why GRC Fails	Critical Success Factors
1. Lack of a shared vision for risk management and compliance.	1. Addresses business needs and strategically align to the organization's overall objectives;
2. Ineffective stakeholder engagement	2. An integrated approach of risk and control with accurate and timely communication of risk information to the decision makers
3. Ineffective change management	3. Strong collaboration and teamwork
4. Project implementation delays	4. End user awareness and training
	5. A risk aware culture
	6. Demonstrated return on investment on GRC implementation

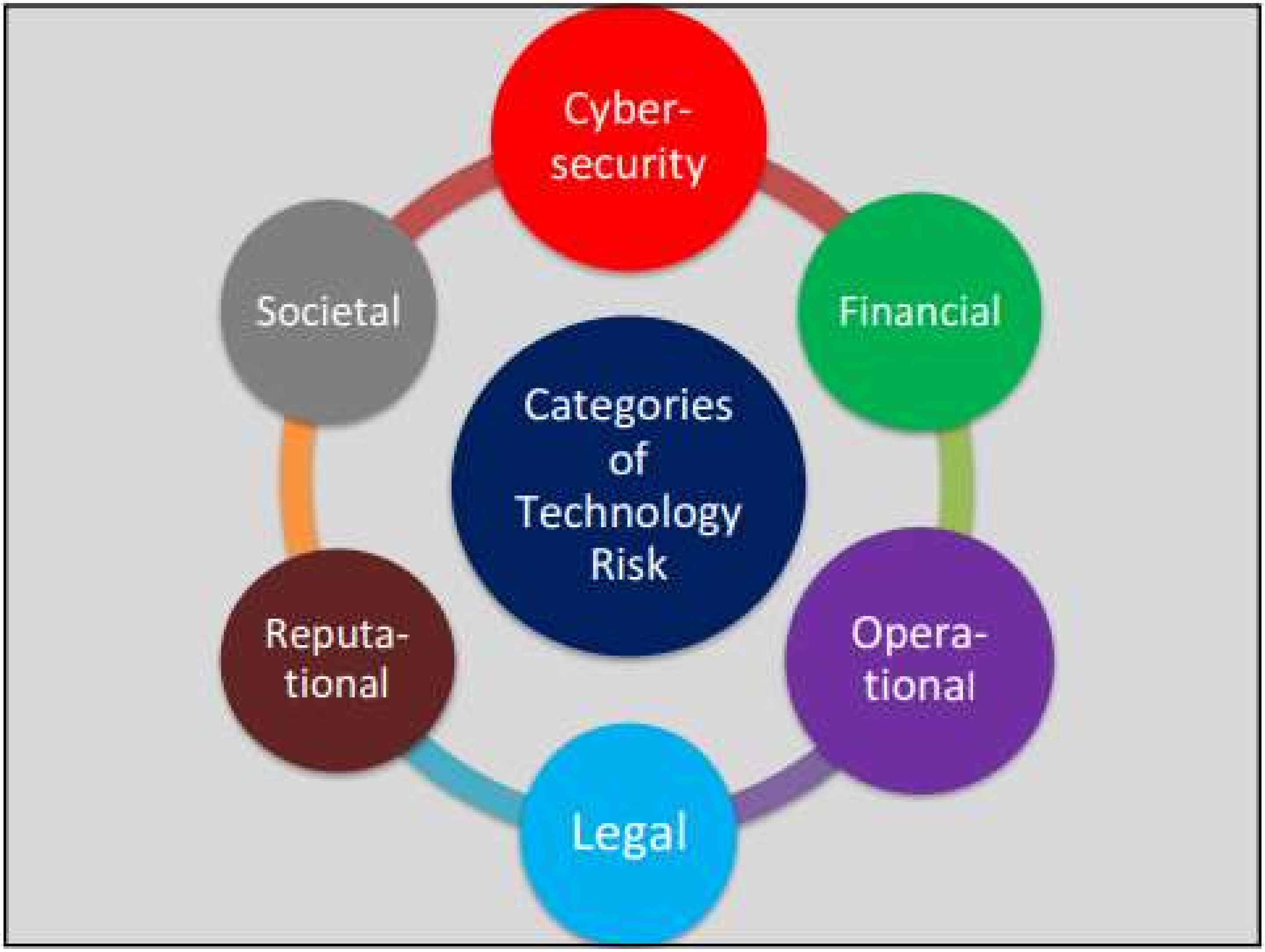
KPMG presentation

https://www.icpak.com/wp-content/uploads/2016/10/ICPAK-IRMPF-2009-and-GRC-KPMG-Presentation-Final.pdf

THE FUTURE OF FINANCE SUMMIT
SHANGRI-LA, BANGKOK, THAILAND
29 - 31 MAY 2019

Managing Cybersecurity Risk in the Digital Age Workshop

Setting the Context



Categories of Technology Risk

Cyber-security

Financial

Opera-tional

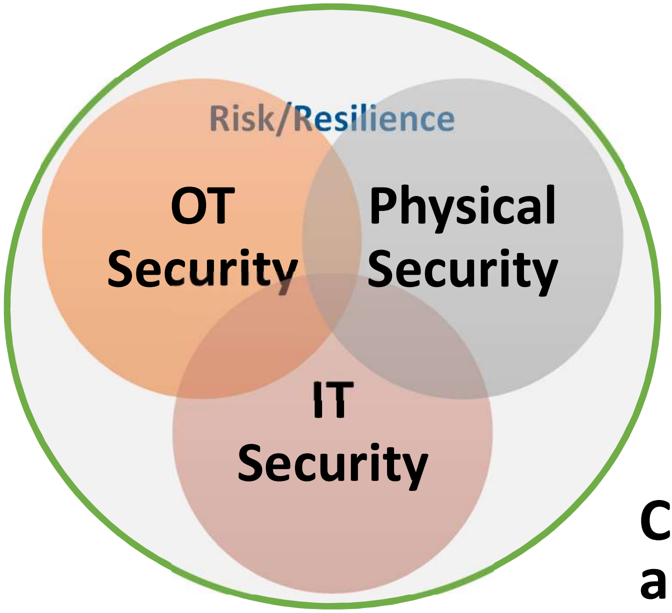
Legal

Reputa-tional

Societal

Defining Cybersecurity

Cybersecurity is the protection of information & technology systems from attacks, damages or unauthorized access.



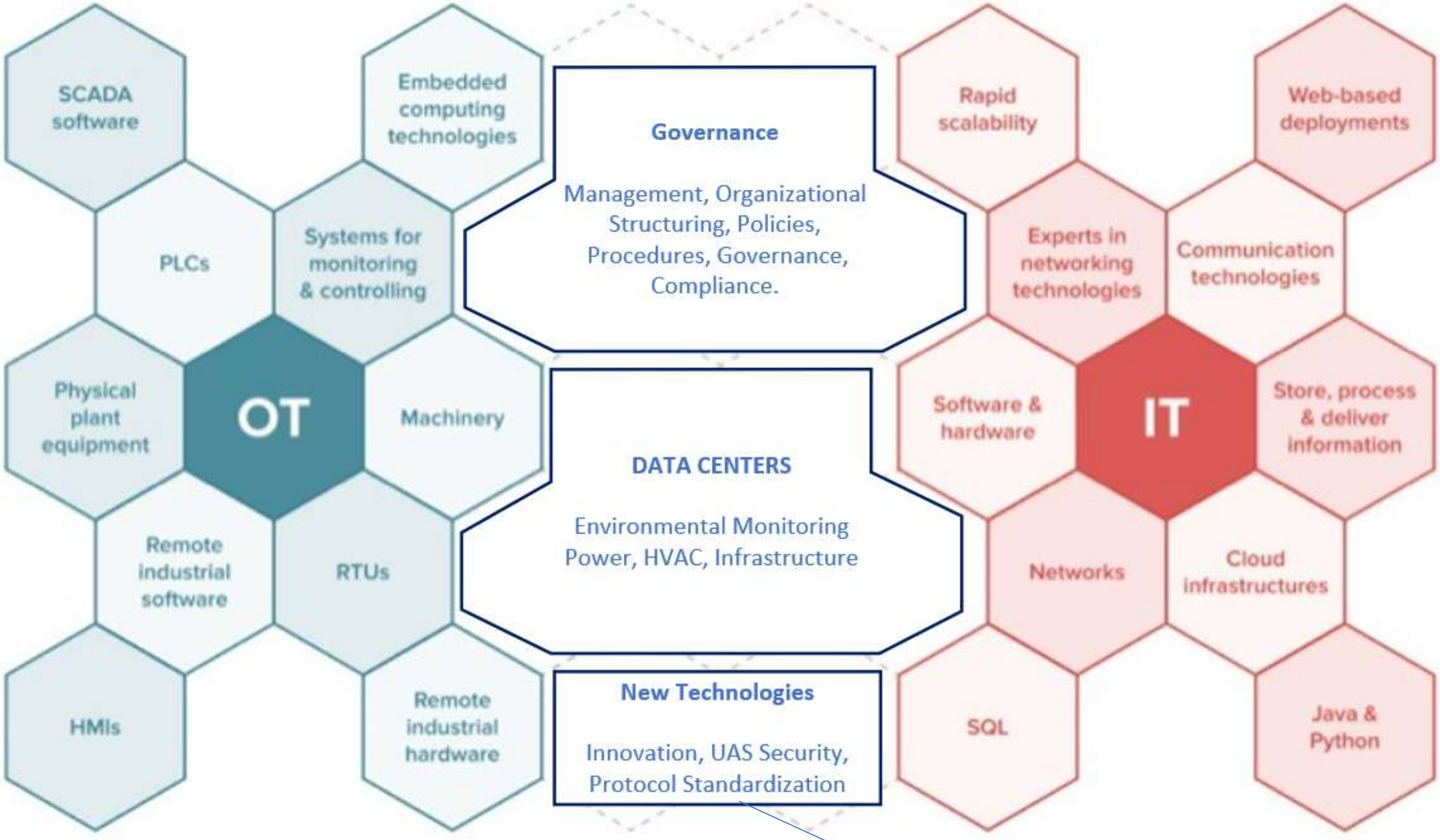
Cybersecurity encompasses solutions against all sorts of breaches and hacking, including internal misuse, corporate espionage, ransomware, crypto-mining and denial of service attacks.

Due Care: Putting reasonable measures in place to protect assets or data.

Due Diligence: Ensuring that security measures remain sufficient to protect that assets or data.

Cybersecurity is only part of a holistic security risk and resilience effort that is required to protect people, assets, and operations.

IT vs. OT Perspective


SCADA software
Embedded computing technologies
PLCs
Systems for monitoring & controlling
Physical plant equipment
OT
Machinery
Remote industrial software
RTUs
HMIs
Remote industrial hardware
Rapid scalability
Web-based deployments
Experts in networking technologies
Communication technologies
Software & hardware
IT
Store, process & deliver information
Networks
Cloud infrastructures
SQL
Java & Python

Governance

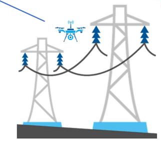
Management, Organizational Structuring, Policies, Procedures, Governance, Compliance.

DATA CENTERS

Environmental Monitoring
Power, HVAC, Infrastructure

New Technologies

Innovation, UAS Security, Protocol Standardization

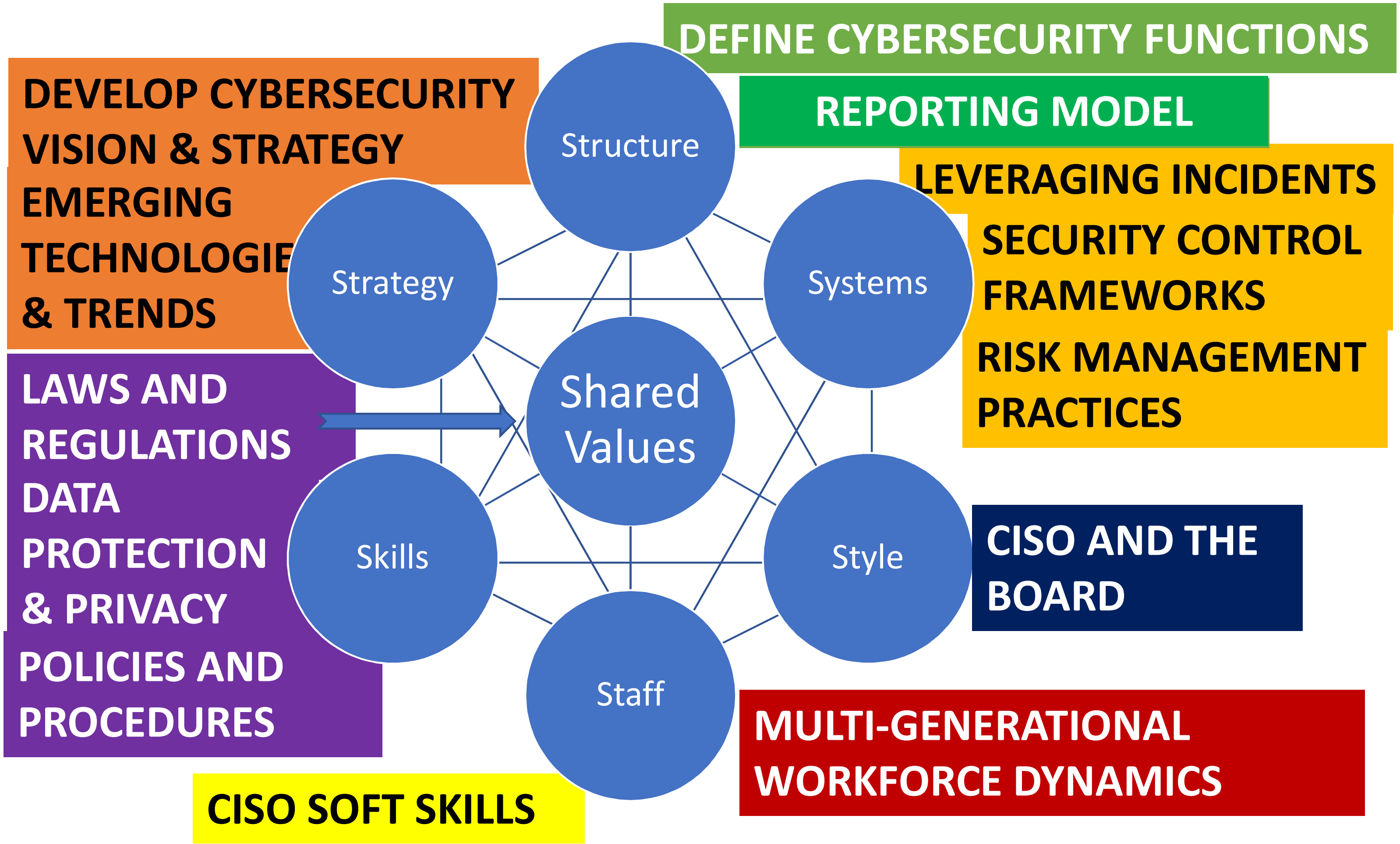


Graphic illustrates the alignment of technologies to IT & OT.

Security, Risk, & Resiliency is an planning aspect of each cell.

Source : https://slideplayer.com/slide/16122887/

Cybersecurity Building Blocks



DEVELOP CYBERSECURITY VISION & STRATEGY

EMERGING TECHNOLOGIE & TRENDS

LAWS AND REGULATIONS

DATA PROTECTION & PRIVACY

POLICIES AND PROCEDURES

CISO SOFT SKILLS

DEFINE CYBERSECURITY FUNCTIONS

REPORTING MODEL

LEVERAGING INCIDENTS

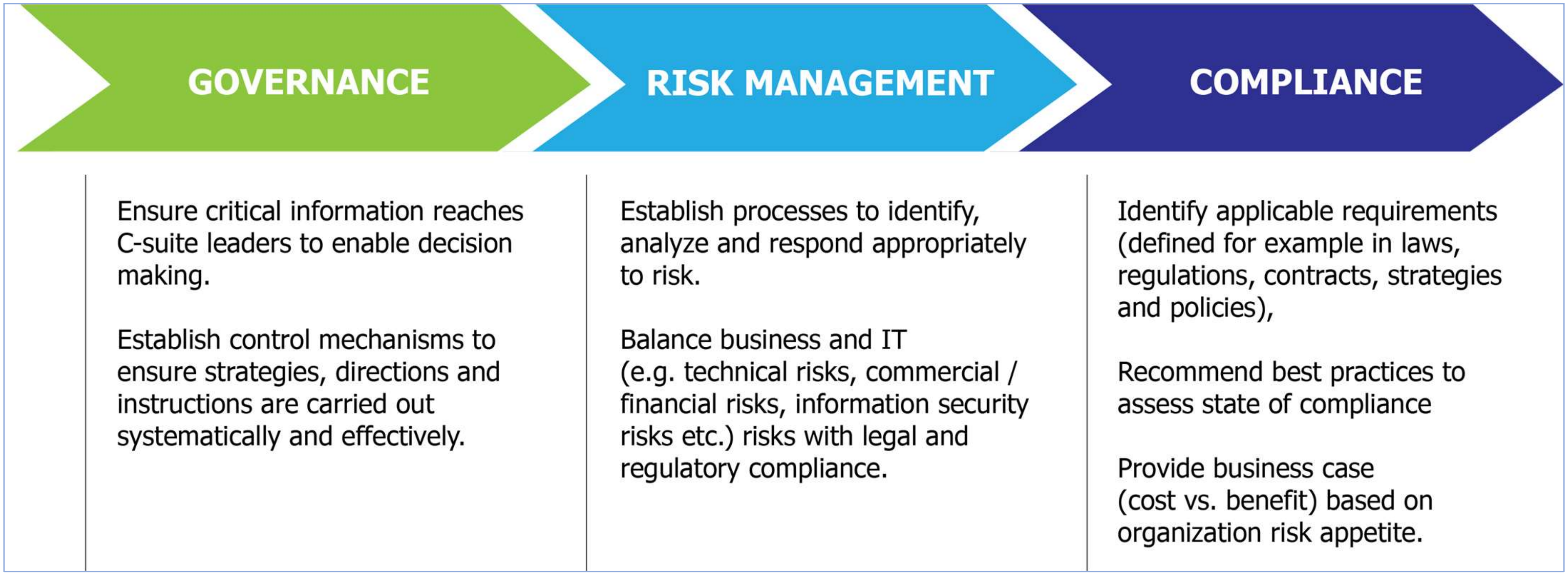
SECURITY CONTROL FRAMEWORKS

RISK MANAGEMENT PRACTICES

CISO AND THE BOARD

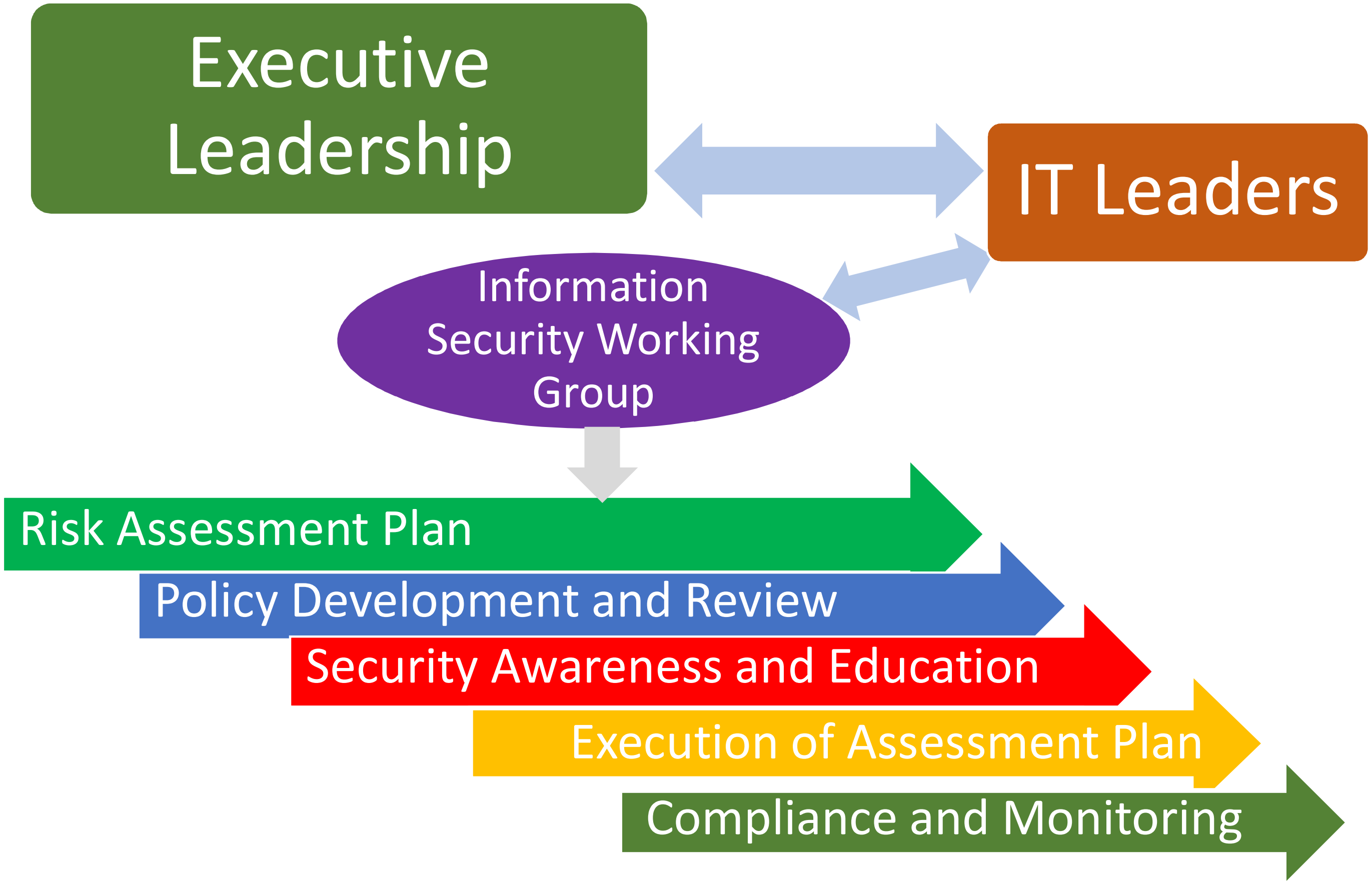
MULTI-GENERATIONAL WORKFORCE DYNAMICS

Governance, Risk, and Compliance (GRC)



GOVERNANCE	RISK MANAGEMENT	COMPLIANCE
Ensure critical information reaches C-suite leaders to enable decision making. Establish control mechanisms to ensure strategies, directions and instructions are carried out systematically and effectively.	Establish processes to identify, analyze and respond appropriately to risk. Balance business and IT (e.g. technical risks, commercial / financial risks, information security risks etc.) risks with legal and regulatory compliance.	Identify applicable requirements (defined for example in laws, regulations, contracts, strategies and policies), Recommend best practices to assess state of compliance Provide business case (cost vs. benefit) based on organization risk appetite.

Governance, Risk & Compliance Cybersecurity Framework



Executive Leadership

IT Leaders

Information Security Working Group

Risk Assessment Plan

Policy Development and Review

Security Awareness and Education

Execution of Assessment Plan

Compliance and Monitoring

IT Governance, Risk, and Compliance (GRC) Framework

- A framework for the leadership, organization, and operation of the institution's IT areas to ensure that those areas support and enable the institution's strategic objectives. (Joanna Grama and Rodney Peterson)[1]
- IT GRC programs align institutional activities with larger institutional goals (i.e., governance) and allow the identification of challenges and opportunities (i.e., risk), and when internal requirements and external mandates are lined up (i.e., compliance), institutional activities have the best chance for success—especially in stormy weather or where danger lurks. (Diana Oblinger)[1]

[1] Joanna Lyn Grama and Rodney Peterson. *Governance, Risk, and Compliance: Why Now?* Educause Review, Vol.48, no.6 (November/December 2013)

GRC & ERM Frameworks

Governance, Risk, and Compliance Framework

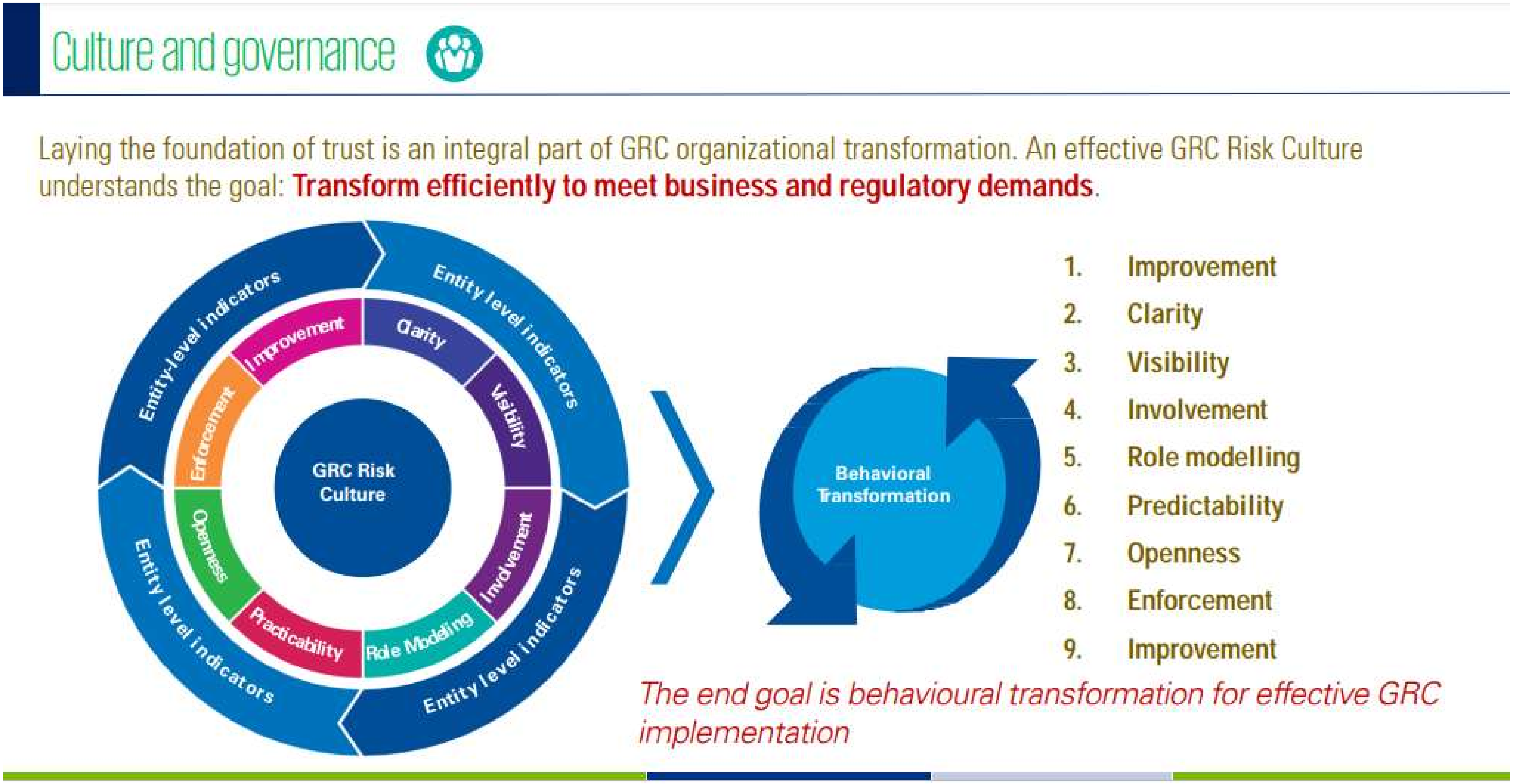
- A structure that an organization uses for governance, risk and compliance initiatives
- A means for establishing governance, identifying and assessing risks, and achieving compliance
- Integrated, collaborative approach for producing desired results. It breaks down silos so that a single united solution can be implemented

Enterprise, Risk, Management Framework

- A method and process for minimizing unexpected volatility through the assessment of risks across every function
- Includes identifying and evaluating risks, and developing mitigation strategies
- Shares the same end goal as GRC: the continued achievement of the institution’s goals and objectives

Value of Integrating Cybersecurity GRC with ERM Frameworks

1. Adds visibility and value to the cybersecurity program
2. Facilitates communication and collaboration across the enterprise
3. Changes the culture to be more cybersecurity aware
4. Cybersecurity can’t be addressed in silos, and just by the IT organization
5. Cybersecurity is only as strong as the weakest link in the institution
6. Using GRC and ERM frameworks make it an enterprise-wide program
7. It has to be viewed as an enterprise issue since it impacts all missions of the organization



Culture and governance

Laying the foundation of trust is an integral part of GRC organizational transformation. An effective GRC Risk Culture understands the goal: **Transform efficiently to meet business and regulatory demands**.

1. Improvement
2. Clarity
3. Visibility
4. Involvement
5. Role modelling
6. Predictability
7. Openness
8. Enforcement
9. Improvement

The end goal is behavioural transformation for effective GRC implementation

Source: KPMG https://www.icpak.com/wp-content/uploads/2016/10/ICPAK-IRMPF-2009-and-GRC-KPMG-Presentation-Final.pdf

Key Take Aways

- Cybersecurity is an enterprise-wide issue and activity
- Cybersecurity can be strengthened by an integrated GRC and ERM frameworks and programs
- Cybersecurity GRC framework needs to be aligned with the institutional strategic plan, goals and objectives
- Cybersecurity GRC must be part of the organization’s culture with a strong focus on the people factor
- Cybersecurity is a strategic risk and requires all to be involved for the program to manage this risk

Hot spots

Organizations can better implement GRC and ensure the intended benefits are realized by focusing on the following "hot spots":

1. Organizational culture and governance
2. Effective change management
3. End user awareness
4. Board accountability for risk

Establishing the Cybersecurity GRC Framework & Programs

Board & Cybersecurity Risk Oversight

- Need for senior management ownership
- Corporate Objectives and Strategic Plans – linked to cybersecurity risk management
- Integral part of risk management framework
  - Regular reporting
  - Failure to link cybersecurity assessments to key organization objectives
- Importance of internal controls

Five Guiding Principles

Boards seeking to enhance oversight of cyber risks

I. Cybersecurity is an Enterprise Risk Management issue:

Not just an Information Technology issue

II. Boards should understand the legal implications of cyber risks

III. Boards should access cybersecurity expertise and discuss regularly – standing agenda item

IV. Board should set expectation that management establish an ERM framework with adequate staffing & budget

V. Board & Management discussion of cyber risk strategies - avoidance, acceptance, mitigation or transfer – with specific plans

Cybersecurity Strategic & Tactical Programs

1. Leadership team to drive the determination of Cybersecurity Goals & Objectives
2. Vision & Mission Statements
3. Types of Plans
    1. Corporate Cybersecurity Strategic Plans
    2. Corporate Cybersecurity Tactical Plans
    3. Cybersecurity Annual Plan
    4. Annual Review and Reevaluation
4. Design a Cybersecurity Metrics Management System
    1. Metrics analysis

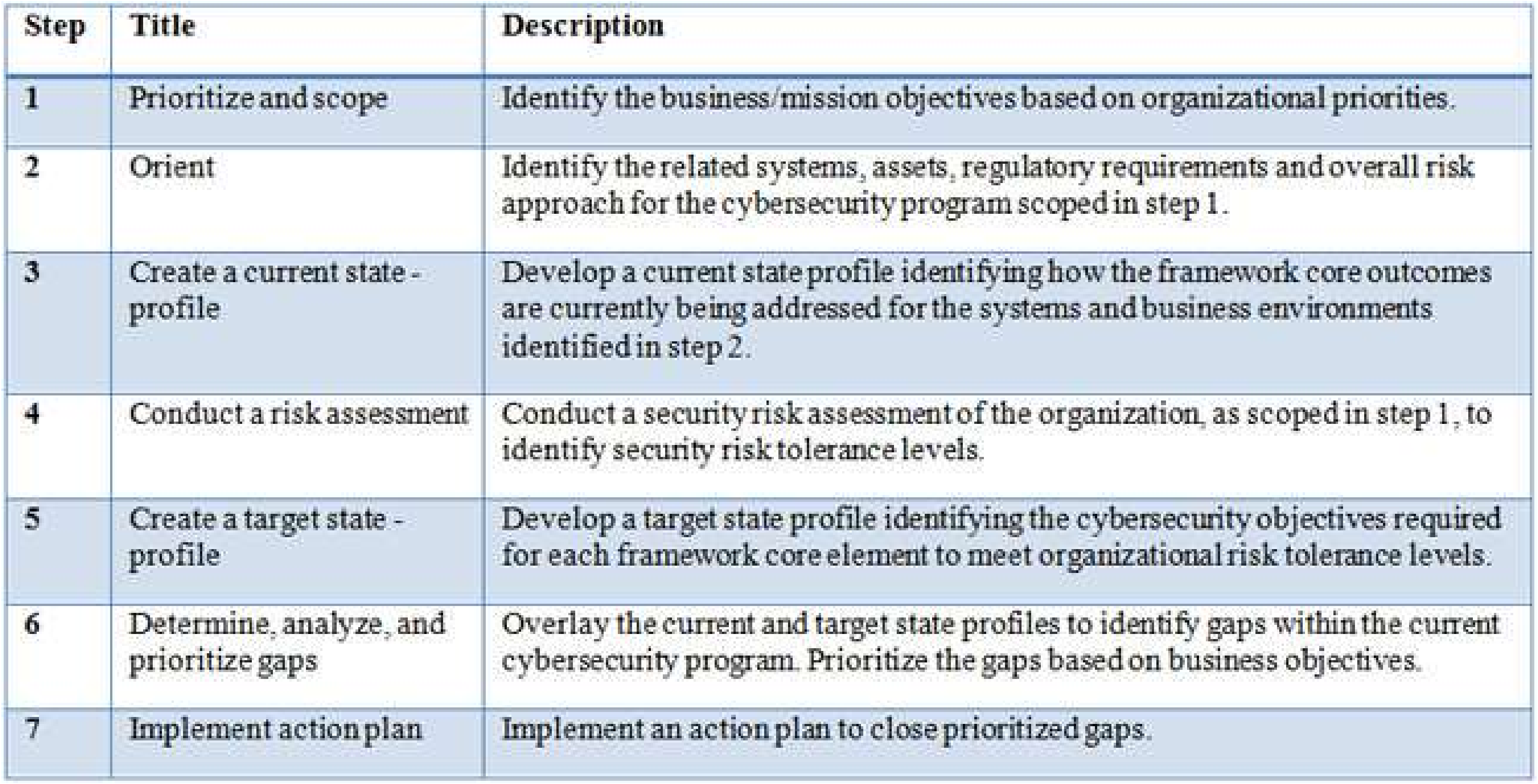
Issues to be considered

- Understand cyber risk environment
- Cybersecurity planning (strategic, tactical, operational)
- Technological developments (big data, analytics and artificial intelligence) impacting cybersecurity arena
- Regulatory and compliance requirements
- SWOT analysis

Design & develop a cybersecurity GRC framework

- Evaluate the organisation risk management culture
- Evaluate the organization’s cybersecurity risk management culture
  - Evaluating risk appetite
  - Risk assessment and analysis
  - Risk management process
    - Identify risks
    - Evaluate risks
      - Determine impact severity
      - Determine risk levels
    - Mitigate risks
      - Avoid, limit or transfer

Steps to implement a Cybersecurity GRC Program



Step	Title	Description
1	Prioritize and scope	Identify the business/mission objectives based on organizational priorities.
2	Orient	Identify the related systems, assets, regulatory requirements and overall risk approach for the cybersecurity program scoped in step 1.
3	Create a current state - profile	Develop a current state profile identifying how the framework core outcomes are currently being addressed for the systems and business environments identified in step 2.
4	Conduct a risk assessment	Conduct a security risk assessment of the organization, as scoped in step 1, to identify security risk tolerance levels.
5	Create a target state - profile	Develop a target state profile identifying the cybersecurity objectives required for each framework core element to meet organizational risk tolerance levels.
6	Determine, analyze, and prioritize gaps	Overlay the current and target state profiles to identify gaps within the current cybersecurity program. Prioritize the gaps based on business objectives.
7	Implement action plan	Implement an action plan to close prioritized gaps.

Technical Aspects

1. Technology deployment
    1. Systems planning
    2. System architecture
    3. Control measures
2. Testing
    1. Penetration testing
    2. Vulnerability assessment
    3. Incident response
3. Monitoring
4. Evaluation
5. Business continuity and disaster recovery

Technical Aspects (continued)

Post Incident Management

- Incident response plan
- Forensic investigation
- Liaise with law enforcement
- Communication

Cybersecurity policies, procedures & control measures

1. Cybersecurity control framework
2. Cybersecurity standards
3. Procedures
4. Auditing compliance
5. Baselines
6. Best practices

Cybersecurity Policy & Governance

- CIA
  - Confidentiality, Integrity & Availability
  - Who is responsible for CIA?
- Cybersecurity Policy
  - Identify assets & cyber risks
  - Design policies & procedures
  - Ensure regulatory compliance
- Cybersecurity Policy Life Cycle
  - Policy development
  - Policy publication
  - Policy adoption
  - Policy Review

Cybersecurity Policy Organization

Cybersecurity Policy Hierarchy

1. Standards
2. Baselines
3. Guidelines
4. Procedures
5. Plans & Programs

Cybersecurity Policy Design

1. Understand your audience
2. Identify policy components
3. Evaluate policy
4. Revising policy – change drivers
5. Authorization of policy

Cybersecurity Standards & Framework

- Commonly used frameworks & Standards
  - NIST Cybersecurity Framework
  - ISO 27000 family
  - COBIT 5 for Information Security
  - ISF Standard of Good Practice for Information Security
  - IT capability Maturity Framework – Information Security Management
  - World Economic Forum Cyber Risk Framework
  - European Union Agency for Network & Information Security
  - PCI-DSS (Payment Card Industry Data Security Standard

Governance & Risk Management

1. What is Governance?
2. Need for Strategic Alignment
3. Regulatory compliance
4. Cybersecurity Vulnerability Disclosure Policies
5. Cybersecurity policies – at user level

Cyber Resilient Organizations

1. Changing approach to risk management
2. Incident response and crisis management
   - ✓Planning
3. Resilience engineering
   - ✓Resilient security solutions
4. Attributes of cyber resilient organizations
5. Financial resilience

Cyber Strategic Performance Management

1. What is cyber strategic performance management?
2. Strategy to measure cybersecurity performance
3. Organizational risk assessment
4. How to create an effective cybersecurity performance management system
    1. Measuring cybersecurity capabilities
    2. Portfolio of initiatives
        1. Measuring progress against initiatives
    3. Measuring protection
5. Pitfalls in measuring cybersecurity performance

Principles behind Cyber Risk Management

1. Meet stakeholders’ needs
2. Design single integrated framework
    1. Structured & proactive approach to assessing & managing risks
    2. Holistic
        1. Cover organizations end to end
        2. Integrated with enterprise risk management
    3. Prioritizing the protection of value
    4. Address uncertainty – make use of best available information
    5. Regulatory compliance
    6. Human & cultural factors
3. Maturity strategy and continual improvements

Cyber Risk Management

1. Understand organization risk profile
2. Focus on crown jewels
3. Humans – the weakest link
4. Complementing preventative with detective measures
5. Focus on organization’s capabilities to respond

Key Risk Indicators

- Need to monitor & review KRIs
- KRIs & KPIs
- KRI design for cyber risk management
  - Risk taxanomy
  - Organizational risk
  - KRI design links Objectives, Risks & Controls
  - Using KRIs for improved decision making
  - Inherent risks, residual risks
  - Dashboard to manage KRIs

Legal & Regulatory Compliance

1. Review of regulatory and legal environment
2. Legal and regulatory risk management framework
3. Accountability and reporting
4. Legal documentation
5. Legal standard operating procedures

Laws & Regulations

- Types of law
  - Cyber laws
  - Computer Offences legislation
  - Cybersecurity Laws
  - Data Protection Laws
- Compliance
- Law Enforcement
  - Cyber crimes

Cybersecurity Maturity Models (CMM)

- CMM measures improvements in capabilities
- Moving up the risk maturity curve

Operational Aspects

Asset Management – Audit & Protect

- Assets and Systems
  - Financial Asset
  - Data Asset
  - Intellectual Property Asset
  - Reputational Asset
- Classification of Asset
  - How does the government classify data?
  - Is data classified differently from a national security vantage point?
  - Who decides how national security data is to be classified
  - How does the private sector classify data?

Physical & Environmental Security

- Secure Facility Layered Defense Model
  - How do we secure the site?
  - How is physical access controlled?
- Protecting Equipment
  - Power supplies
  - Fire risk management

Threat Intelligence

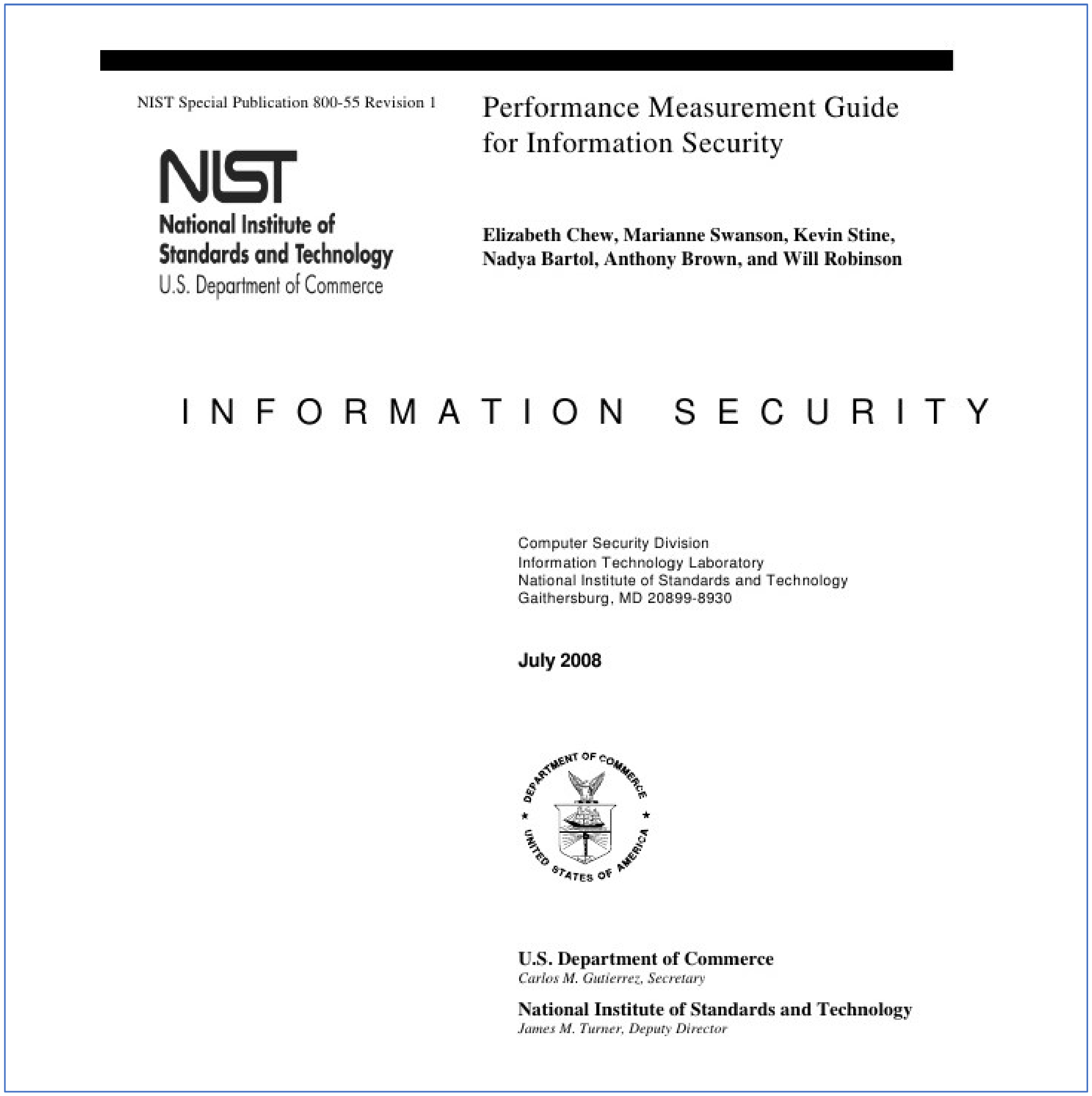
- Source of threat intelligence
- Sharing strategy
- Control measures

Cybersecurity Metrics

- Measurement & Management
- Cyber Threat Metrics
- Measuring the threats for organizations

Metrics are tools to facilitate decision making and improve performance and accountability. Measures are quantifiable, observable, and objective data supporting metrics. Operators can use metrics to apply corrective actions and improve performance. Regulatory, financial, and organizational factors drive the requirement to measure IT security performance. Potential security metrics cover a broad range of measurable features, from security audit logs of individual systems to the number of systems within an organization that were tested over the course of a year. Effective security metrics should be used to identify weaknesses, determine trends to better utilize security resources, and judge the success or failure of implemented security solutions.

Paul E. Black, Karen A. Scarfone, Murugiah P. Souppaya
In book entitled “Cyber Security Metrics & Measures”



NIST Special Publication 800-55 Revision 1

National Institute of Standards and Technology
U.S. Department of Commerce

Performance Measurement Guide for Information Security

Elizabeth Chew, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown, and Will Robinson

INFORMATION SECURITY

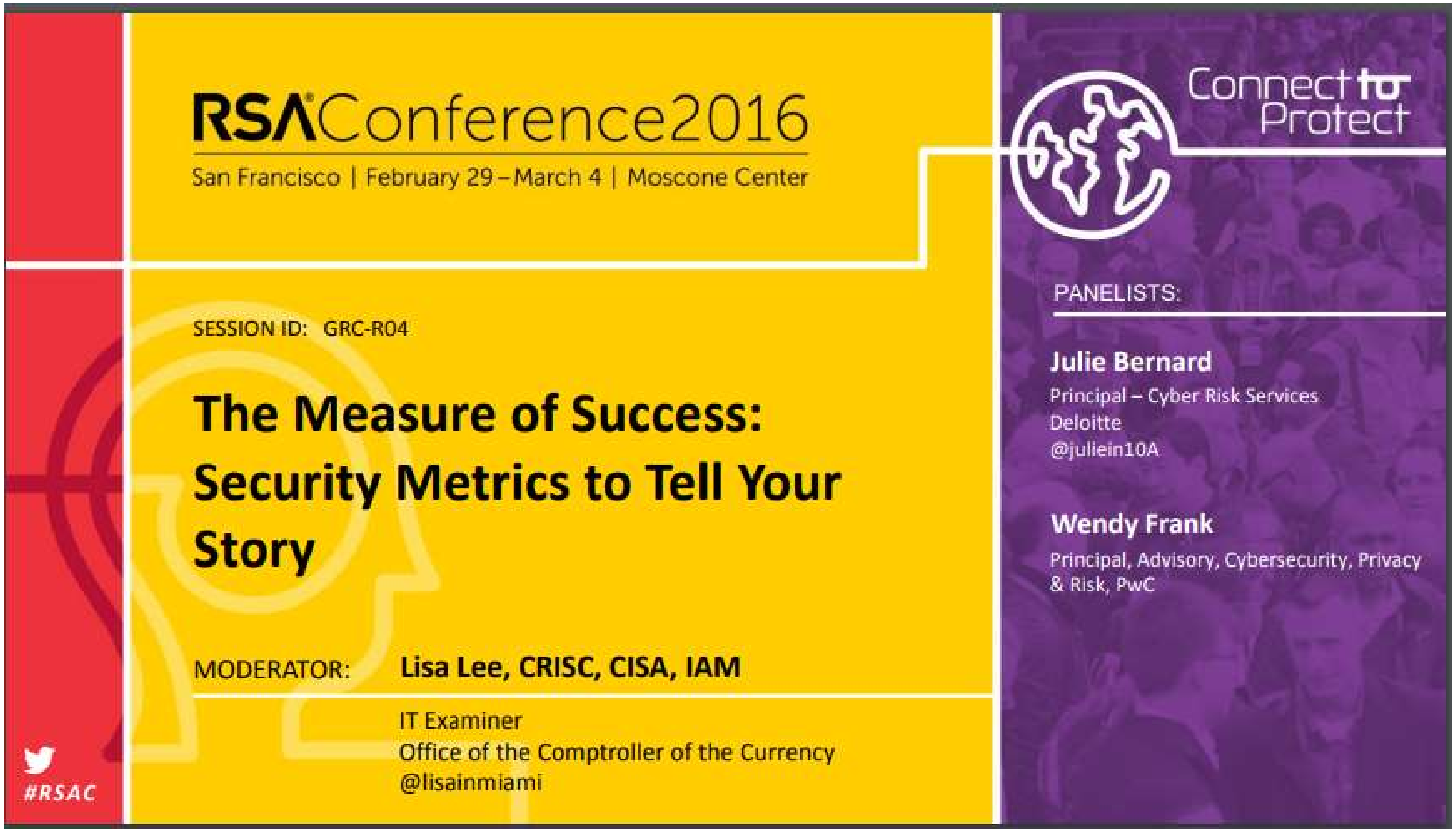
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

July 2008

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
James M. Turner, Deputy Director

Provides guidance on how an organization, through the use of metrics, identifies the adequacy of in-place security controls, policies, and procedures. It provides an approach to help management decide where to invest in additional security protection resources or identify and evaluate non productive controls. It explains the metric development and implementation process and how it can also be used to adequately justify security control investments. The results of an effective metric program can provide useful data for directing the allocation of information security resources and should simplify the preparation of performance-related reports.



RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: GRC-R04

The Measure of Success: Security Metrics to Tell Your Story

MODERATOR: **Lisa Lee, CRISC, CISA, IAM**

IT Examiner
Office of the Comptroller of the Currency
@lisainmiami

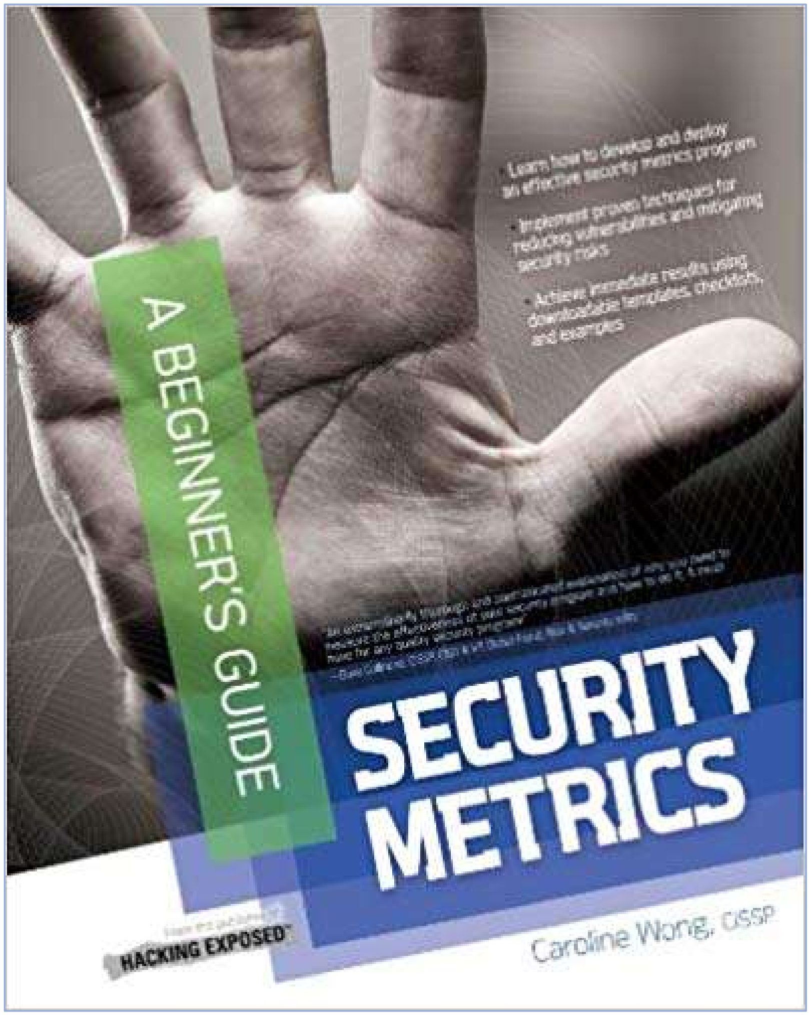
PANELISTS:

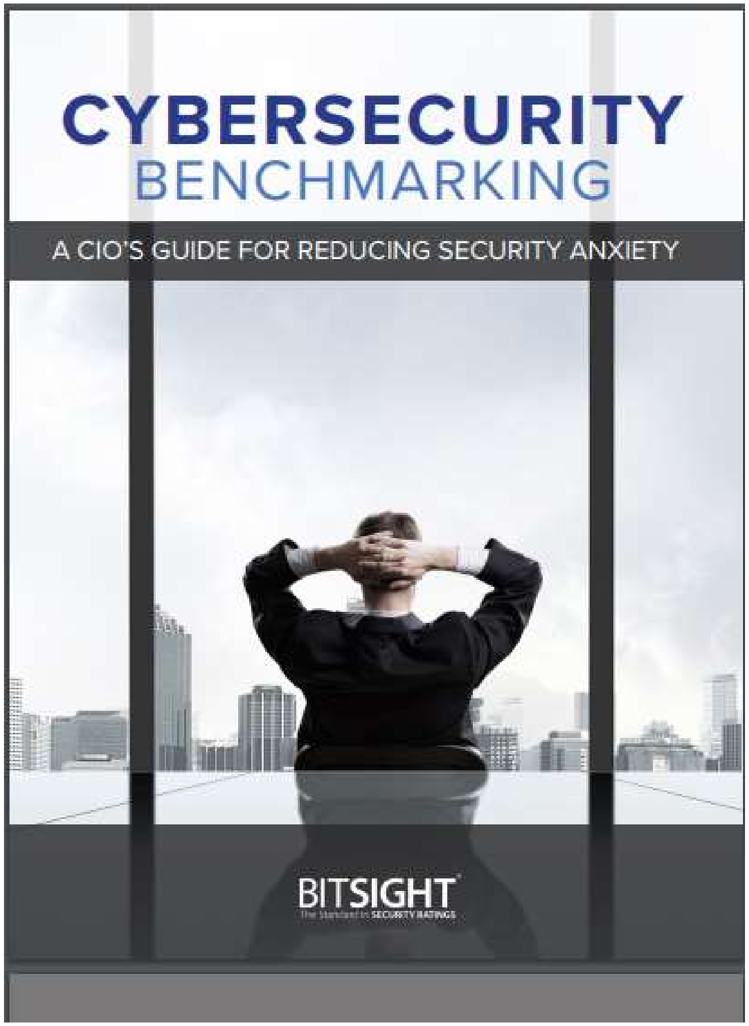
Julie Bernard
Principal – Cyber Risk Services
Deloitte
@julieln10A

Wendy Frank
Principal, Advisory, Cybersecurity, Privacy & Risk, PwC

#RSAC

https://www.rsaconference.com/writable/presentations/file_upload/grc-r04-the_measure_of_success-security_metrics_to_tell_your_story.pdf


A BEGINNER'S GUIDE
Learn how to develop and deploy an effective security metrics program
Implement proven techniques for reducing vulnerabilities and mitigating security risks
Achieve immediate results using downloadable templates, checklists, and examples
SECURITY METRICS
Caroline Wong, CISSP
HACKING EXPOSED



CYBERSECURITY
BENCHMARKING

A CIO'S GUIDE FOR REDUCING SECURITY ANXIETY

BITSIGHT
The Standard in SECURITY RATINGS

How to measure your cybersecurity performance

https://www.slideshare.net/AbhishekSood10/how-to-measure-your-cybersecurity-performance

Value of Cybersecurity metrics

1. Increase in share value for good governance
2. Increased predictability of business operations
3. Protection from civil or legal liability as a result of absence of due care
4. Critical decisions not based on inadequate or faulty information

Cyber Insurance

- Buying cyber insurance
- Cyber insurance market
- Managing portfolios of cyber insurance
- Cyber insurance underwriting
- Cyber insurance and risk management

Cybersecurity Crisis Management & Communications

- Cybersecurity crisis management
  - From incident to crisis management
  - Crisis management operating principles
  - Tools and techniques for managing a cyber crisis
  - Cyber crisis management steps
- SOPs for communications
- Strategic communication to protect reputation

Cybersecurity Economics & Strategies

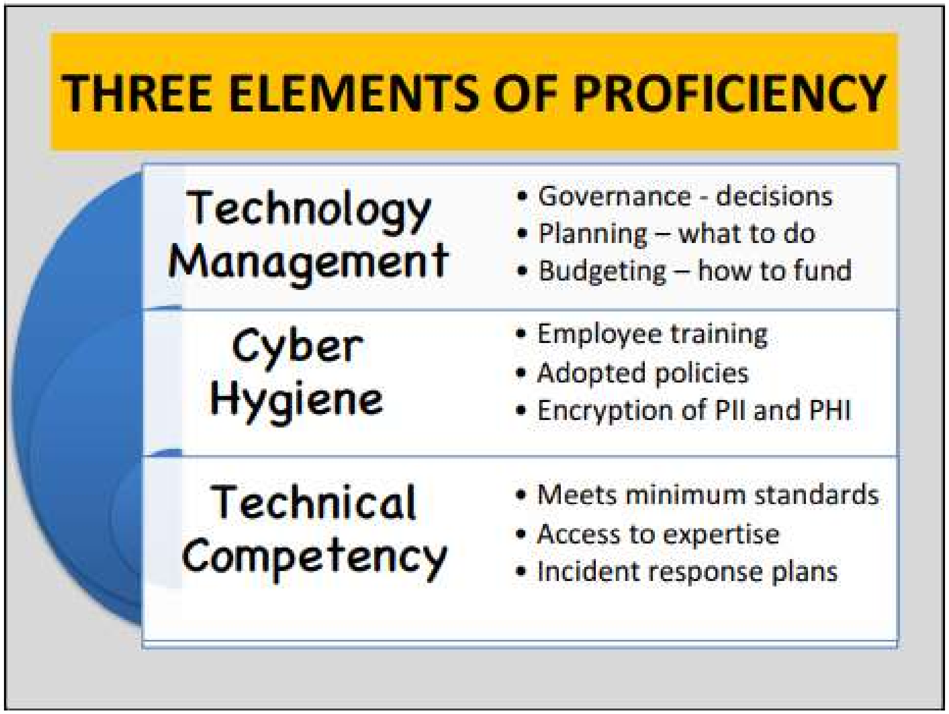
- Cost effectiveness of cybersecurity readiness/enhancements
- Cybersecurity budgets
- Measuring impact & returns on investment

Training & Capability Building

1. Cybersecurity leadership training
2. Specify competencies required
3. Grassroot support and rank and file training

Cybersecurity & HR issues

- Recruitment and cybersecurity
- Onboarding phase
- User provisioning
- Employee Contracts
  - NDA
  - Acceptable Use Agreement
- Cybersecurity Education & Training
  - Knowledge, skills and attitudes



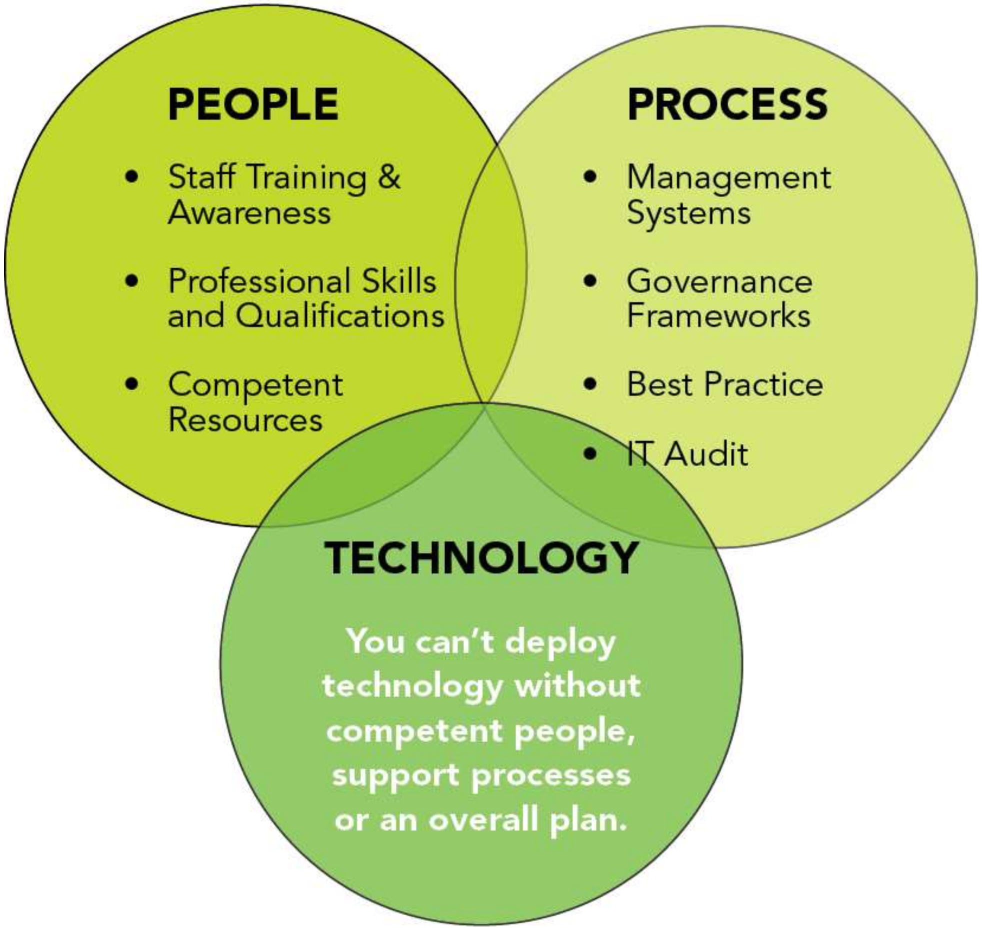
THREE ELEMENTS OF PROFICIENCY

Technology Management
- Governance - decisions
- Planning – what to do
- Budgeting – how to fund

Cyber Hygiene
- Employee training
- Adopted policies
- Encryption of PII and PHI

Technical Competency
- Meets minimum standards
- Access to expertise
- Incident response plans

Cybersecurity & HR issues



PEOPLE

- Staff Training & Awareness
- Professional Skills and Qualifications
- Competent Resources

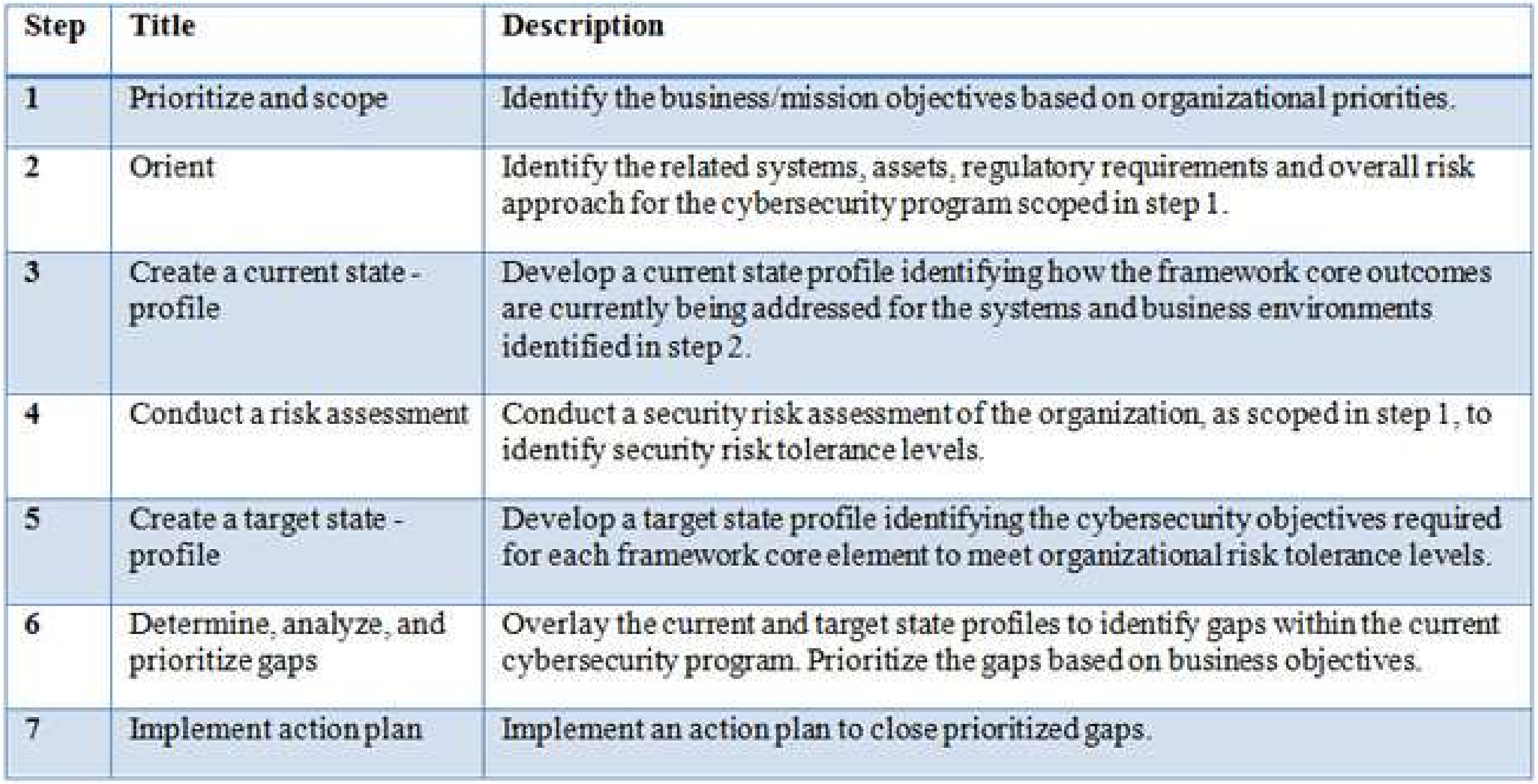
PROCESS

- Management Systems
- Governance Frameworks
- Best Practice
- IT Audit

TECHNOLOGY

You can't deploy technology without competent people, support processes or an overall plan.

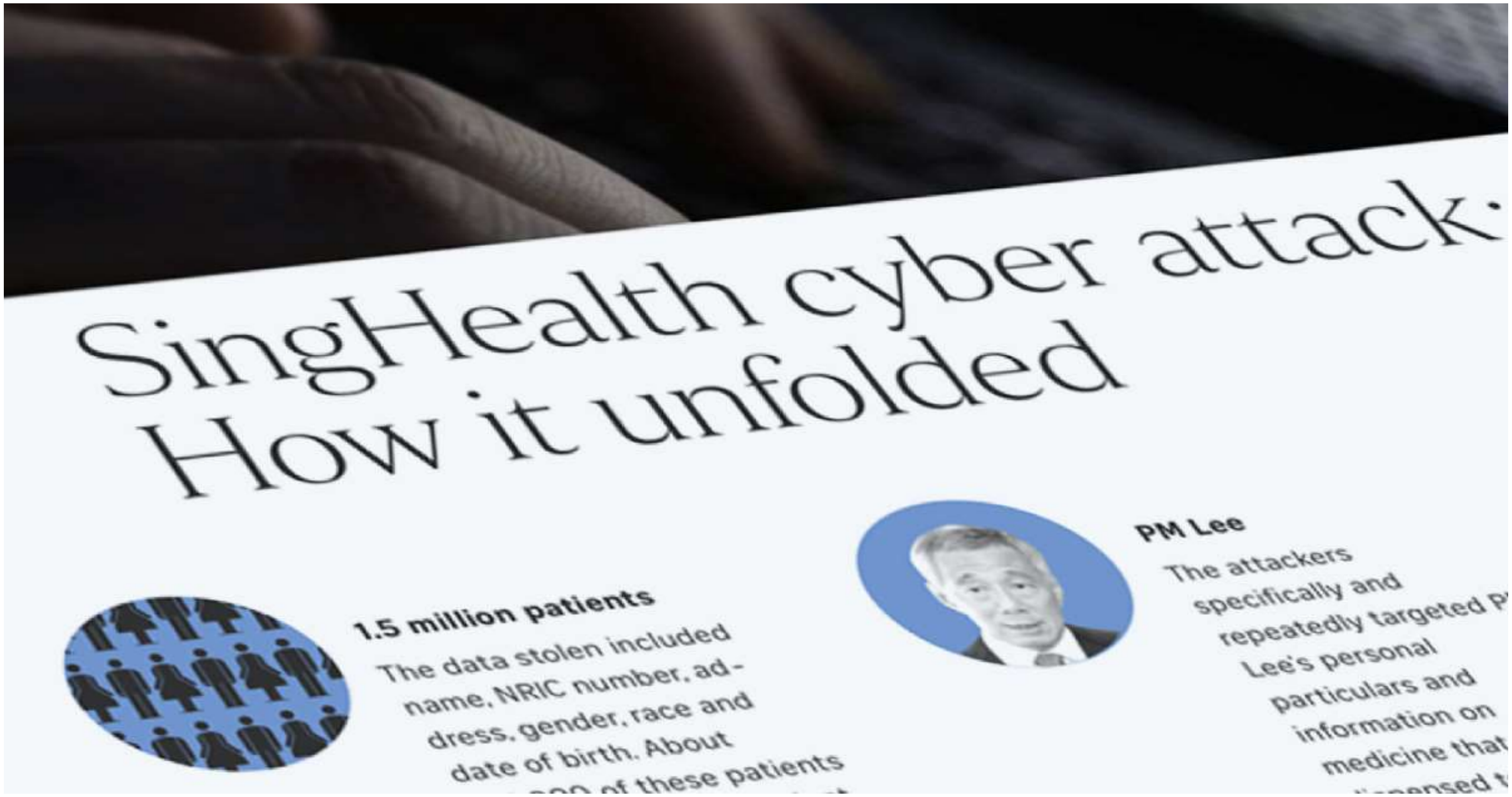
Steps to implement a Cybersecurity GRC Program



Step	Title	Description
1	Prioritize and scope	Identify the business/mission objectives based on organizational priorities.
2	Orient	Identify the related systems, assets, regulatory requirements and overall risk approach for the cybersecurity program scoped in step 1.
3	Create a current state - profile	Develop a current state profile identifying how the framework core outcomes are currently being addressed for the systems and business environments identified in step 2.
4	Conduct a risk assessment	Conduct a security risk assessment of the organization, as scoped in step 1, to identify security risk tolerance levels.
5	Create a target state - profile	Develop a target state profile identifying the cybersecurity objectives required for each framework core element to meet organizational risk tolerance levels.
6	Determine, analyze, and prioritize gaps	Overlay the current and target state profiles to identify gaps within the current cybersecurity program. Prioritize the gaps based on business objectives.
7	Implement action plan	Implement an action plan to close prioritized gaps.

CASE STUDY

Singhealth Cyber attack



SingHealth cyber attack: How it unfolded

1.5 million patients

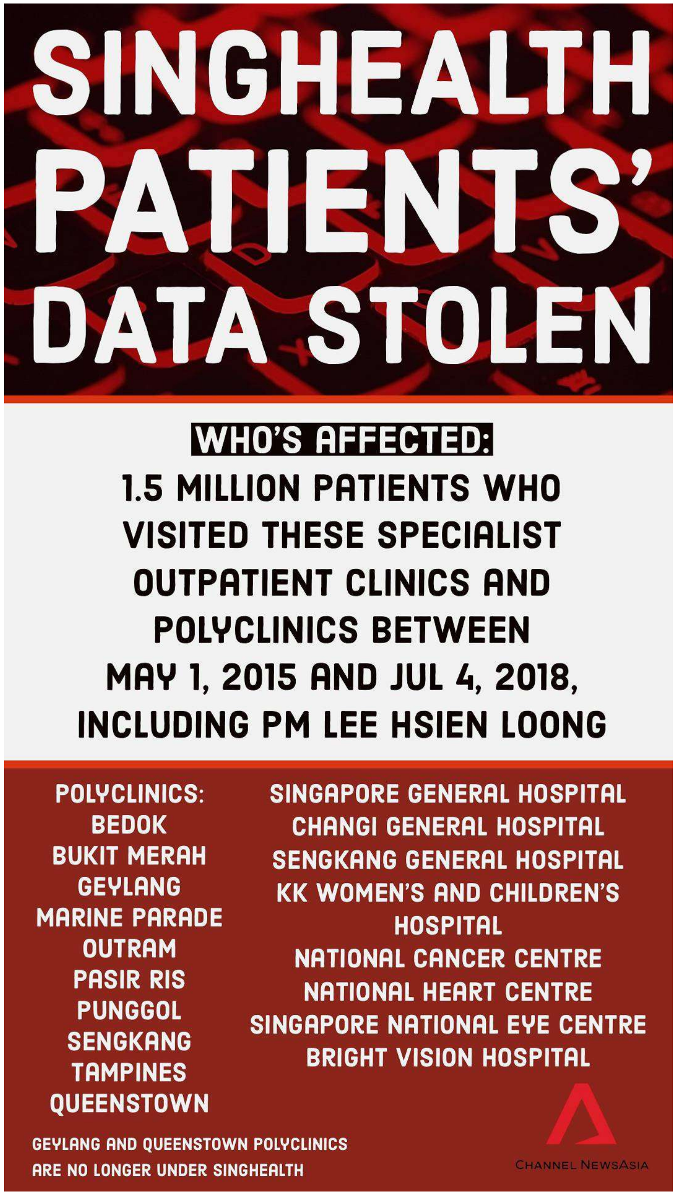
The data stolen included name, NRIC number, address, gender, race and date of birth. About

of these patients

PM Lee

The attackers specifically and repeatedly targeted

Lee's personal particulars and information on medicine that



SINGHEALTH PATIENTS' DATA STOLEN

WHO'S AFFECTED:

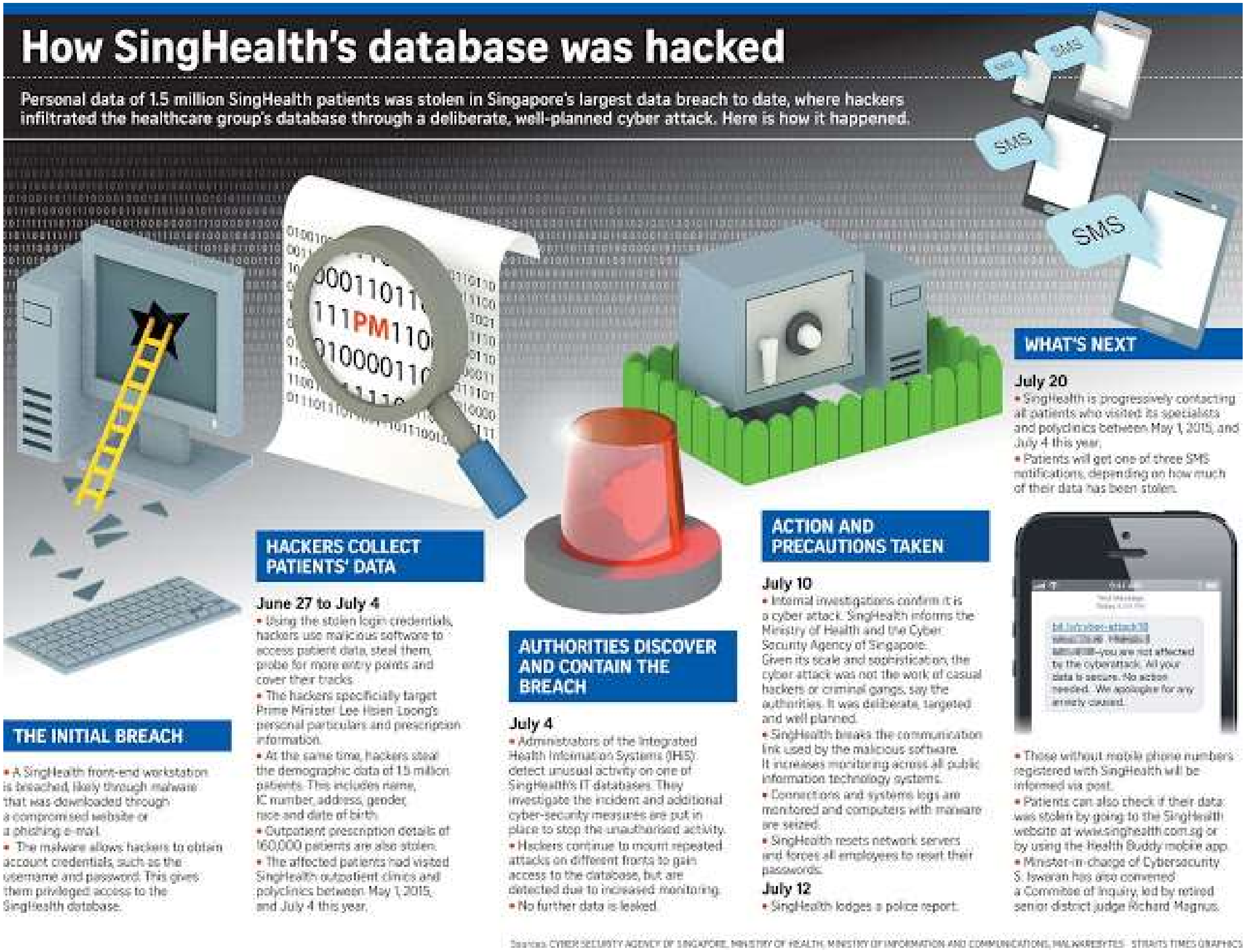
1.5 MILLION PATIENTS WHO VISITED THESE SPECIALIST OUTPATIENT CLINICS AND POLYCLINICS BETWEEN MAY 1, 2015 AND JUL 4, 2018, INCLUDING PM LEE HSIEN LOONG

POLYCLINICS:
BEDOK
BUKIT MERAH
GEYLANG
MARINE PARADE
OUTRAM
PASIR RIS
PUNGGOL
SENGKANG
TAMPINES
QUEENSTOWN

SINGAPORE GENERAL HOSPITAL
CHANGI GENERAL HOSPITAL
SENGKANG GENERAL HOSPITAL
KK WOMEN'S AND CHILDREN'S HOSPITAL
NATIONAL CANCER CENTRE
NATIONAL HEART CENTRE
SINGAPORE NATIONAL EYE CENTRE
BRIGHT VISION HOSPITAL

GEYLANG AND QUEENSTOWN POLYCLINICS ARE NO LONGER UNDER SINGHEALTH

CHANNEL NEWSASIA


SMS
SMS
SMS
SMS
111PM110

How SingHealth's database was hacked

Personal data of 1.5 million SingHealth patients was stolen in Singapore's largest data breach to date, where hackers infiltrated the healthcare group's database through a deliberate, well-planned cyber attack. Here is how it happened.

THE INITIAL BREACH

- A SingHealth front-end workstation is breached, likely through malware that was downloaded through a compromised website or a phishing e-mail.
- The malware allows hackers to obtain account credentials, such as the username and password. This gives them privileged access to the SingHealth database.

HACKERS COLLECT PATIENTS' DATA

June 27 to July 4

- Using the stolen login credentials, hackers use malicious software to access patient data, steal them, probe for more entry points and cover their tracks.
- The hackers specifically target Prime Minister Lee Hsien Loong's personal particulars and prescription information.
- At the same time, hackers steal the demographic data of 1.5 million patients. This includes name, IC number, address, gender, race and date of birth.
- Outpatient prescription details of 160,000 patients are also stolen.
- The affected patients had visited SingHealth outpatient clinics and polyclinics between May 1, 2015, and July 4 this year.

AUTHORITIES DISCOVER AND CONTAIN THE BREACH

July 4

- Administrators of the Integrated Health Information Systems (IHiS) detect unusual activity on one of SingHealth's IT databases. They investigate the incident and additional cyber-security measures are put in place to stop the unauthorised activity.
- Hackers continue to mount repeated attacks on different fronts to gain access to the database, but are detected due to increased monitoring.
- No further data is leaked.

ACTION AND PRECAUTIONS TAKEN

July 10

- Internal investigations confirm it is a cyber attack. SingHealth informs the Ministry of Health and the Cyber Security Agency of Singapore. Given its scale and sophistication, the cyber attack was not the work of casual hackers or criminal gangs, say the authorities. It was deliberate, targeted and well planned.
- SingHealth breaks the communication link used by the malicious software. It increases monitoring across all public information technology systems.
- Connections and systems logs are monitored and computers with malware are seized.
- SingHealth resets network servers and forces all employees to reset their passwords.

July 12

- SingHealth lodges a police report.

WHAT'S NEXT

July 20

- SingHealth is progressively contacting all patients who visited its specialists and polyclinics between May 1, 2015, and July 4 this year.
- Patients will get one of three SMS notifications, depending on how much of their data has been stolen.

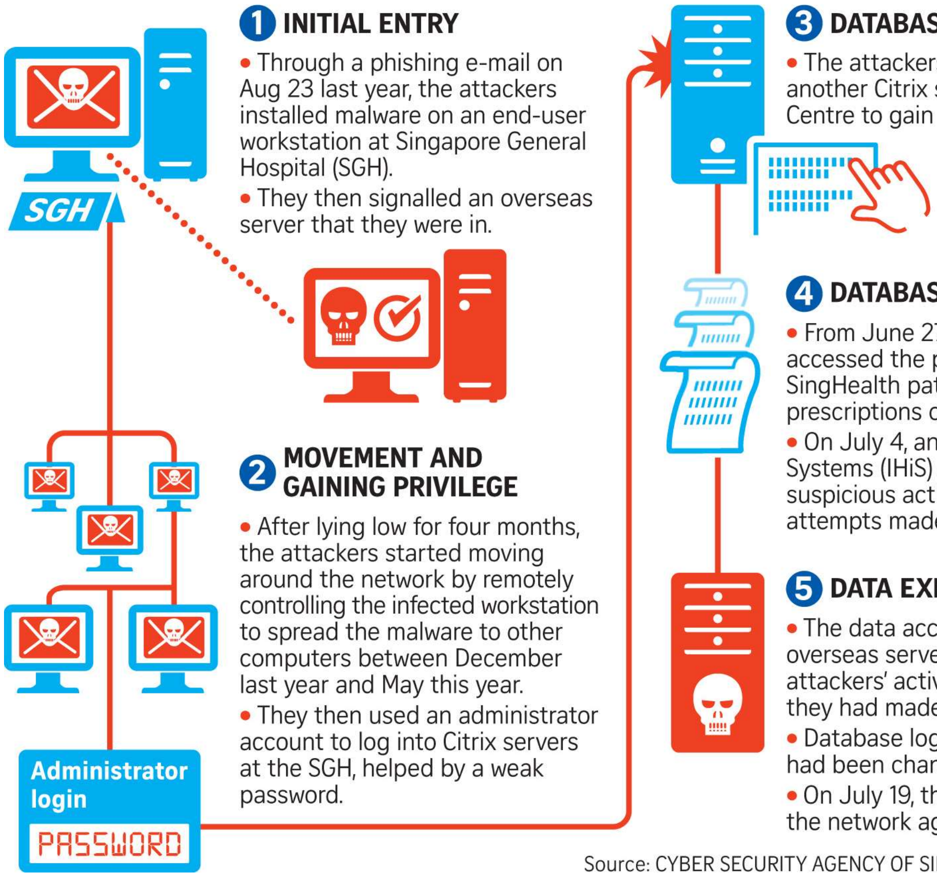
[redacted]—you are not affected by the cyberattack. All your data is secure. No action needed. We apologise for any anxiety caused.

- Those without mobile phone numbers registered with SingHealth will be informed via post.
- Patients can also check if their data was stolen by going to the SingHealth website at www.singhealth.com.sg or by using the Health Buddy mobile app.
- Minister-in-charge of Cybersecurity S. Iswaran has also convened a Commitee of Inquiry, led by retired senior district judge Richard Magnus.

Sources: CYBER SECURITY AGENCY OF SINGAPORE, MINISTRY OF HEALTH, MINISTRY OF INFORMATION AND COMMUNICATIONS, MALWAREBYTES STRAITS TIMES GRAPHICS

The cyber attack

Between June 27 and July 4, cyber attackers stole the personal data of 1.5 million SingHealth patients and the medical prescriptions of 160,000 people, including Prime Minister Lee Hsien Loong. Here is the route they took to access SingHealth's electronic medical records (EMR) database.



❶ INITIAL ENTRY

- Through a phishing e-mail on Aug 23 last year, the attackers installed malware on an end-user workstation at Singapore General Hospital (SGH).
- They then signalled an overseas server that they were in.

❷ MOVEMENT AND GAINING PRIVILEGE

- After lying low for four months, the attackers started moving around the network by remotely controlling the infected workstation to spread the malware to other computers between December last year and May this year.
- They then used an administrator account to log into Citrix servers at the SGH, helped by a weak password.

❸ DATABASE ENTRY

- The attackers secured credentials from another Citrix server at the Healthcare Data Centre to gain access to the EMR database.
- Armed with these credentials, they entered the database on June 26 from a Citrix server at SGH.

❹ DATABASE ACCESS

- From June 27 to July 4, the attackers accessed the personal data of 1.5 million SingHealth patients and the medical prescriptions of 160,000 people.
- On July 4, an Integrated Health Information Systems (IHiS) database administrator noticed suspicious activities and stopped them. Other attempts made that day were also stopped.

❺ DATA EXFILTRATION

- The data accessed was copied to an overseas server. On July 13, IHiS simulated the attackers' activities and found out the data they had made off with.
- Database logs showed that no data had been changed or deleted.
- On July 19, the attackers tried to hack into the network again but were stopped.

Source: CYBER SECURITY AGENCY OF SINGAPORE STRAITS TIMES GRAPHICS

End