Information and Cyber Security (ICS)

Business Continuity Planning

UK Chamber of Commerce, April 2020

Classification: PUBLIC
Document Owner: Michael Kwofie, Country Information Security Risk Officer
Group CISRO - ISRO Regions, Standard Chartered
Updated: 17 April 2020

What we'd like you to take away from this session

01 An understanding Information and Cyber Security (ICS) Risk

Overview of cyber threats, trends and impact

02 Business Continuity Management

BCM Overview
BCM Components
Planning stages
Challenges
Playbook

03 Q&A

Overview of cyber threats, trends and impact

An understanding of Information and Cyber Security (ICS) Risk

What global regulators are concerned about in managing ICS risk

Standard Chartered

Accountability & Culture

- Good Governance and Accountability required
- FCA expects 'good cyber hygiene, a good security culture and good governance'
- Top/Down security culture paramount

Risk-based

- Risk-based approach to considering cyber risk expected
- Hong Kong Monetary Authority CSF Initiative established a common risk assessment criteria

Third party management

- Increased focus on third parties management of cyber risk
- Cloud providers and IT infrastructure included in assessments
- European supervisory authorities monitor firms' use of cloud computing and potential build-up of cyber risks.

Incident management

- Must establish and test capabilities, evidenced through increased number of industry / regulator exercises.
- Monitoring and alerting of incidents is integral to the response and recovery of cyber related incidents.

Cyber security resilience

- Increasingly following NIST Framework for supervising financial institutions with more focus on Response and Recovery
- BoG released a Cyber and Information Security directive for all banks with great emphasis to cyber resilience
- The National Cyber Security Center under the Ministry of Communications has a draft cyber security legislation that seeks to ensure cyber resilience to all critical infrastructure

Information sharing

- Information on threats, vulnerabilities, incidents and responses should be shared

Impacts of Cyber Crime

Standard Chartered

Direct Costs	Indirect Costs	Intangible Costs
Investigation & Remediation *3rd party specialist fees* *Maersk costs estimated at $300m+*	**Increased Cyber Insurance Premium** *3x increase for hacked organisations.* *Hiscox sees 40% annual rise in cyber insurance*	**Damage to Brand** *Harder to attract new customers.* *TalkTalk loses over 100,000 customers following hack*
Regulatory Sanction *GDPR breaches - 4% global revenue* *Tesco fined $21.4m by FCA*	**Customer Fraud** *Bank of Valetta suffers loss of $14.7m in fraudulent payments following cyber attack*	**Heads Roll** *Bangladesh Bank Chief resigns following cyber theft of $81m*
Customer & Business Redress *Health insurer Aetna agrees additional $0.6m in settlement agreements following breach*	**Class Action Lawsuit** *Workers brought a claim against Morrisons after an employee stole and published data of nearly 100,000 staff*	**Merger Value** *$350m reduction in Yahoo takeover price by Verizon*

Threats cause ICS risk. In SC, ICS Risk is defined as

ICS risk is the risk of failing to identify, assess and protect the **confidentiality, integrity and availability (CIA)** of **information assets, information systems and technical infrastructure** from internal or external threats.

Threats may impact…

1) Confidentiality

2) Integrity

3) Availability

Bank Assets

Information Assets

e.g. Business, personal data, legal agreements

Information Systems

eg Software and hardware that process data

Technical Infrastructure

eg Platforms on which data and systems operate


SECURITY
RECOVERY
RESILIENCE
CONTINGENCY
BUSINESS
OPERATE
PLANNING
INCIDENT
CONTINUITY
MANAGEMENT
PROCEDURES
RISK
ORGANIZATION
PLAN
PREPARATION
STANDARD
DISASTER

Business continuity management (BCM)

"**Business continuity** is about **having a plan to deal with difficult situations**, so your organization can **continue to function with as little disruption as possible**. Business continuity is a process-driven approach which can be standardised, and which leads an organisation out of a major incident so that it can continue operations"

Organizations today are **exposed to a wide range of risks** which if not well prepared for could **throw them out of business**.
Lesser impacts could be

- **loss of competitive advantage,**
- **fines or**
- **reputational damage.**

Events that could impact businesses include **:**

Natural disasters | Cyber attacks | Pandemics | Regulatory Compliance failures | Disruptive technologies | Technology failure | Supply chain failure |

Estimated **$5,600** a minute of unplanned downtime costs to organizations, on average*

More than **40%** of businesses will never reopen after a major natural disaster*

A BCM programme is crucial. Benefits include:

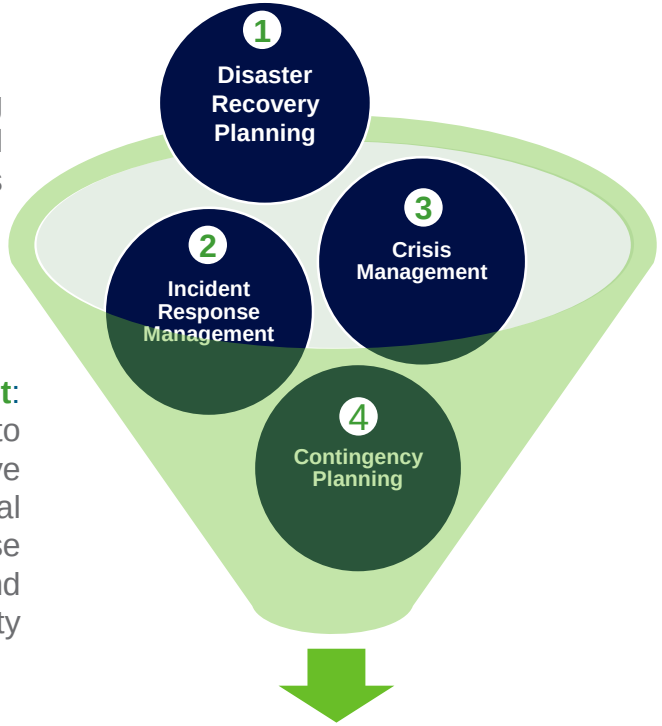
1. Builds confidence among your customers and employees.
2. Mitigate risks and financial exposure
3. Serves to provide the organization with a competitive advantage.
4. Provides assurance that the organization can continue operating in disruptive events
5. Compliance with regulatory or legal requirements
6. Preserves brand value and reputation

Source: itgovernance.co.uk/business-resilience
https://www.thebci.org/knowledge/introduction-to-business-continuity.html
https://www.gartner.com/smarterwithgartner/stress-test-your-business-continuity-management/
* Gartner is a global research and advisory firm providing information, advice, and tools for leaders in IT, finance, HR, customer service and support, communications, legal and compliance, marketing, sales, and supply chain functions.

Business continuity management components

1 **Disaster Recovery Planning:**
Process focused on building continuity capabilities for critical IT infrastructure and business applications

2 **Incident response management**:
Defines the necessary steps to address and minimize the negative impact of a physical or logical incident threating enterprise resources (people, physical and logical assets), e.g., theft, security breach or natural disasters



3 **Crisis management (CM):**
Defines the steps necessary to address and mitigate the effect of a negative event, often while the event is still happening (e.g., fire, tornado, earthquake, severe weather)

4 **Contingency planning :**
Process of developing advance arrangements and procedures that enable an enterprise to respond to an event that could occur by chance or unforeseen circumstances

Business Continuity Management

A set of processes and resources to identify possible threats, calculate their potential impact and provide the necessary practices to prevent, mitigate and recover from disruptions. The most common BCM processes include disaster recovery, crisis management, incident response management and contingency planning.

Isaca.org. (2012). Business Continuity Management: Emerging Trends
https://www.itgovernance.co.uk/blog/how-to-write-a-business-continuity-plan-the-easy-way

Business continuity planning steps

Standard Chartered

Step 1:
Conduct a Risk Assessment

- A thorough assessment and evaluation of an organizations resilience exposures
- Assessment of the potential impact of various business disruption scenarios
- Prioritization of findings and development of a roadmap

Step 2:
Conduct a Business Impact Analysis (BIA)

- Critical business processes and workflows as well as the supporting production applications, internal and external dependencies. ***(Holistic view / result is preferable)***
- Critical resources skill sets and contacts
- Obtaining executive sign-off of Business Impact Analysis

Step 3:
Develop the Plan

- Synthesize the Risk Assessment and BIA findings to create an actionable and thorough plan
- Recovery assumptions, including Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO). (these targets must be validated and ensure that the plan will achieve these targets.
- Develop departmental plans
- Identify all stakeholders and actors in the plan
- Review plan with key stakeholders to finalize (It is necessary to get as many perspectives from various staff and all departments to get the wholistic view and buy-in for the plan.)

Step 4:
Create awareness about the plan

- Executive management team reviews and signs off on the overall plan once completed.
- Brief and socialize plans with all actors.
- The plan should easily be available and readily accessible to all actors

Step 5:
Test Plan & Maintenance

- Conduct periodic simulation exercises to ensure key stakeholders are comfortable with the plan steps
- Review the plan periodically (agreed frequency)
- Validate the Business Impact Assessments at least on an annual basis

https://www.itgovernance.co.uk/blog/how-to-write-a-business-continuity-plan-the-easy-way
https://www.eci.com/blog/135-five-steps-of-business-continuity-planning-for-investment-firms.html

Common Challenges to a BCM programme

	Challenge	Solution
	**Lack of commitment to the BCM programme** Senior management too busy to oversee or participate in the programme Programme treated as a checklist project and not necessary, approached as a technology project. Delegates to lower level resource. Reduces the visibility and seriousness of the programme.	**Addressed by senior management taking accountability for the programme**. Appoint someone who will be responsible for the programme. Establish a formal committee or working group with the necessary terms of reference, authority, representation of key departments and stakeholders, meeting schedules, annual activity time table. Create awareness on benefits. Senior management participation in all stages is key for **success.**
	**Wrong assumptions used in the planning phase** Inaccurate assumptions made about items such as the expectations of the various stakeholders in terms of recovery time and point objectives, criticality and availability requirements of systems, extent of dependence on 3rd parties, internal controls of 3rd parties,	Addressed by involving all relevant stakeholders during the BIA and development of the plan. Simulation exercises to involve these stakeholders
	**Lack of a communication plan** Lack of a communication plan will lead to disinformation to internal and external stakeholders during an incident. In regulated industries, there may be mandatory requirements for communicating to regulators within specified timeframes.	Addressed through preparation of adequate communication plans for all relevant stakeholders, scripted messages and templates in advance.
	**Lack of awareness, training and testing** Lack of awareness of role holders on what actions to take or what decisions will be required during an incident. Without routinely testing the plan, the organization cannot be sure of how well the programme will work or what challenges will be encountered in a real event.	This can be addressed by running as many possible scenarios as possible to get a sense of success or failures, identify weaknesses to your plan and make the necessary adjustments and improvement.

https://www.isaca.org/resources/isaca-journal/past-issues/2012/key-issues-challenges-and-resolutions-in-implementing-business-continuity-projects

Using the Playbook Concept

- Term especially used in American football, a **Playbook** contains **the team's strategies and plays.**
- Essentially collections of information that outlines clarity about any given subject.
- Information must be documented to ensure that it is **concise, actionable**, **can be communicated** and **used in decision making**.
- **Designed to guide the organization** in **responding to and managing crisis** caused by any crises
- **Focuses on crisis management** during **crisis events** with **defined impact led roles and responsibilities**

"the art of war is of vital importance to the State. It is a matter of life and death, a road either to safety or to ruin. Hence it is a subject of inquiry which can on no account be neglected“

Sun Tzu, Art of War

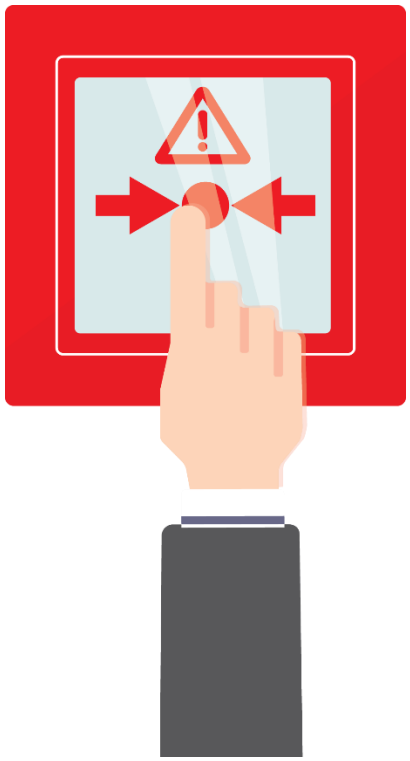
Factors to consider during a crisis event

- Increased cyber attack opportunities
  - E.g. several COVID-19 Themed campaigns through emails, and social media.
  - Crises present opportunities for threat actors to take advantage of vulnerable people.
- Heighten cyber security awareness campaigns
- Beware of scams

- 3rd party dependence risks
- The BCM posture of critical 3rd parties has direct impacts on the organization's posture
- Opportunity to validate suppliers BCM plans and readiness

- Many requirements will arise to change normal settings to accommodate the crises situation
- Ensure a dispensation process to record and formally approve every deviation from the organization's policies and standard operating procedures.
- This will need to be reviewed after the organization gets back to normal times

Key takeaways



1. Assess risks and impacts holistically
2. Prepare a crises management response plan to each scenario
3. Assign roles and responsibilities
4. Create the right level of awareness
5. Test strategies for effectiveness and right fit
6. Incorporate the plan into your BAU

Q&A Time

THANK YOU

DISCLAIMER

- This material has been prepared by one or more members of SC Group, where "SC Group" refers to Standard Chartered Bank and each of its holding companies, subsidiaries, related corporations, affiliates, representative and branch offices in any jurisdiction, and their respective directors, officers, employees and/or any persons connected with them. Standard Chartered Bank is authorized by the United Kingdom's Prudential Regulation Authority and regulated by the United Kingdom's Financial Conduct Authority and Prudential Regulation Authority.
- This material is not research material and does not represent the views of the Standard Chartered research department. This material has been produced for reference and is not independent research or a research recommendation and should therefore not be relied upon as such. It is not directed at Retail Clients in the European Economic Area as defined by Directive 2004/39/EC. It has not been prepared in accordance with legal requirements designed to promote the independence of investment research and is not subject to any prohibition on dealing ahead of the dissemination of investment research.
- This material is for information and discussion purposes only and does not constitute an invitation, recommendation or offer to subscribe for or purchase any of the products or services mentioned or to enter into any transaction. The information herein is not intended to be used as a general guide to investing and does not constitute investment advice or as a source of any specific investment recommendations as it has not been prepared with regard to the specific investment objectives, financial situation or particular needs of any particular person.
- Information contained herein is subject to change at any time without notice, and has been obtained from sources believed to be reliable. Some of the information herein may have been obtained from public sources and while SC Group believes such information to be reliable, SC Group has not independently verified the information. Any opinions or views of third parties expressed in this material are those of the third parties identified, and not of SC Group. While all reasonable care has been taken in preparing this material, SC Group makes no representation or warranty as to its accuracy or completeness, and no responsibility or liability is accepted for any errors of fact, omission or for any opinion expressed herein. The members of SC Group may not have the necessary licenses to provide services or offer products in all countries, and/or such provision of services or offer of products may be subject to the regulatory requirements of each jurisdiction, and you should check with your relationship manager or usual contact. Any comments on investment, accounting, legal, regulatory or tax matters contained in this material should not be relied on or used as a basis to ascertain the various results or implications arising from the matters contained herein, and you are advised to exercise your own independent judgment (with the advice of your investment, accounting, legal, regulatory, tax and other professional advisers as necessary) with respect to the risks and consequences of any matter contained herein. SC Group expressly disclaims any liability and responsibility whether arising in tort or contract or otherwise for any damage or losses you may suffer from your use of or reliance of the information contained herein.
- This material is not independent of the trading strategies or positions of the members of SC Group. It is possible, and you should assume, that members of SC Group may have material interests in one or more of the financial instruments mentioned herein. If specific companies are mentioned in this material, members of SC Group may at times seek to do business with the companies covered in this material; hold a position in, or have economic exposure to, such companies; and/or invest in the financial products issued by these companies. Further, members of SC Group may be involved in activities such as dealing in, holding, acting as market makers or performing financial or advisory services in relation to any of the products referred to in this material. Accordingly, SC Group may have conflicts of interest that may affect the objectivity of this material.
- You may wish to refer to the incorporation details of Standard Chartered PLC, Standard Chartered Bank and their subsidiaries at http://www.sc.com/en/incorporation-details.html.
- This material is not for distribution to any person to which, or any jurisdiction in which, its distribution would be prohibited.
-