Preparing your C-Suite for a Cyber Crisis

Andrew Sheves – Regester Larkin

Orlando, September 12, 2016
Introduction

Aim and objectives

Aim:
» To help your business reduce its exposure to strategic cyber events and enhance organizational resilience.

Objectives:
» Identify gaps in your strategic cyber readiness.
» Improve organizational preparedness for a cyber event.
» Understand how to communicate with stakeholders, customers and the public during and after a cyber event.
What do we mean by crisis?

Crisis – an abnormal or unstable situation that threatens the organization’s strategic objectives, reputation or viability (BS 11200, Crisis Management).

Origins of a crisis

- Fire / explosion
- Contamination
- Workplace violence
- Regulatory breach
- Bribery / FCPA violation
- Weather event
- Terror attack
- Civil unrest
- Disruptive technology
- Regime change
The scope of the challenge

Cyber events – then...

Images: [Link to visualization] Data Source: DataBreaches.net, IdTheftCentre, press reports

Research: Miriam Quick, Ella Hollowood, Christian Miles, Dan Hampson
...and now

![Data Breaches Chart](http://www.informationisbeautiful.net/visualization/worlds-biggest-data-breaches/)

**Data Source:** DataBreaches.net, IdTheftCentre, press reports
**Research:** Miriam Quick, Ella Hollowood, Christian Miles, Dan Hampson

---

**Cyber preparedness remains a concern**

- In our 2015 crisis management survey, only 21% of respondents felt their organization was prepared for a cyber event.
- This compares to 64% who felt prepared for a physical incident and 37% for an environmental incident. Only 25% felt prepared for a terrorist event.
It won’t happen to me….

“There are two types of companies: those that have been hacked, and those who don't know they have been hacked.”

John Chambers, Cisco

Cyber challenges

Uncertainty  Jargon  Unfamiliar

Client / customer / business effects  Villain status  Personal concern = public outrage
Cyber crisis readiness

1. Crisis management... is a distinct component of an organisation’s wider resilience framework.
2. Requires strong, effective leadership at all levels.
3. Requires a clearly-defined structure and powers.
4. Requires trained, skilled and experienced professionals to fulfil specific responsibilities.
5. Requires procedures and tools that support an organisation’s crisis response.
6. Requires a culture that values the importance of external goodwill and relationships.
Resilience

Crisis management is a distinct component of an organisation’s wider resilience framework.

» Integrate cyber threats into threat and risk assessments and horizon scanning.
» Ensure there is a cyber ‘seat’ at the table during resilience planning and preparation.
» Bring cyber elements into ‘mainstream’ BCM and CM preparation.

Leadership

Crisis management requires strong, effective leadership at all levels.

» Involve leaders in training and exercises.
» Identify and prepare the cyber ‘czar’ and CMT rep.
» Identify and prepare the cyber link into the CMT.
» Prepare cyber leaders at all levels.

46% said a lack of senior management buy-in is an obstacle to preparedness.
Structures

Crisis management requires a clearly-defined structure and powers.

» Clarify ownership of the technical cyber response.
» Integrate the technical elements into the overall response.
» Delineate mandates and decision-making powers.
» Identify external responsibilities and allocate internal ownership.

Skills

Crisis management requires trained, skilled and experienced professionals to fulfil specific responsibilities.

» Identify and train technical staff.
» Prepare cyber ‘liaison’ officers to bridge technical / non-technical discussions.
» Train cyber response teams in general incident and crisis management.
» Include cyber scenarios in training for IMTs, CMTs and communications teams.
» Run full spectrum cyber simulations.
Procedures

Crisis management requires procedures and tools that support an organisation’s crisis response.

- Align cyber response plans with general IM and CM plans.
  - Align terminology.
  - Align severity and reporting thresholds.
  - Align structures.
- Utilize standard report formats and basic procedures.

Culture

Crisis management requires a culture that values the importance of external goodwill and relationships.

- ‘Normalize’ cyber and treat as another technical challenge.
- Build relationships between technical and non-technical teams.
- Speak to suppliers, clients and consumer groups.
Talking about cyber – the challenges

» Uncertainty – the ‘don’t knows’.
» Providing non-technical answers to technical questions.
» Jargon.
» Long timelines.
» ‘Wicked’ decisions with no good answer.
» Essential third party support.
Talking about cyber - strategies

» Prepare your internal and external ‘cyber whisperers’.
» Develop playbooks.
» Normalize cyber and integrate into CM training and exercises.
» Differentiate between types of cyber events and clarify cause and effect.

Cause...

- Data theft
- Data tampering
- Non-compliance
- Data corruption / loss
- External hack
- DDoS attack
- Worm
- Change in regulation
- Jurisdictional differences
- Ransomware
- Incident-led
- Issue-led
...and effect

- C - Our data has been compromised
- I - Our data has been tampered with
- A - Our data is unavailable

Cause and effect

- Internal:
  - Data theft
  - Data tampering
- External:
  - External hack
  - DDoS attack
  - Worm
  - Ransomware

Non-compliance
- Data corruption
- Data loss

Change in regulation
- Jurisdictional differences

Image – Central Oregon Community College
Summary

» Normalize cyber - integrate with risk assessments and horizon scanning.
» Find your cyber czar.
» Align and integrate cyber contingency planning.
» Train and exercise.
» Prepare to ‘talk cyber’ internally and externally - find and train your ‘cyber whisperers’.
Presenter information

Andrew Sheves
Director, Regester Larkin Americas
T: +1 713-821-1534
asheves@regesterlarkin.com
www.regesterlarkin.com

ADVANCING SECURITY LEADERS
congress.isc2.org #ISC2Congress