Global Risk Institute

You’ve Been Hacked – Now What?
Case Study

Including “You’ve Been Hacked!” Case Study
GRI Annual Risk Survey

2015
- Systemic Risk
- Conduct Risk/Culture
- Stress Testing
- Regulatory...
- Funding and...
- Commodity Prices
- Disruptive Tech
- Cyber Risk
- Risk Aggregation
- AML Risk

2017
- Cyber Risk
- Regulatory Risk
- Global Economic Risk
- Housing Market
- Household Debt
- Interest Rates
- Geopolitical Risk
- Commodity Prices
- Operational Risk
- Global Trade

2018
- Cyber Risk
- Industry Disruption
- Interest Rates
- Global Economic Risk
- Regulatory Risk
- Geopolitical Risk
- Operational Risk
- Housing Market
- Environmental Risk
- Market Risk
Perspective from the World Economic Forum (2018)
Cybersecurity – GRI Disaster Recovery Plan Simulation

- The GRI developed a Board level Cybersecurity wargame, “You’ve Been Hacked!” simulation, to help financial institution Board members and Senior Executives better understand the real world risks of cyberattacks and their ability to respond to them.

- Similar to approaches used in Business Continuity scenarios for years.
Cybersecurity – War Game Simulation Approach

Cybersecurity business simulations help firms better prepare for a cyberattack:

• Simulate a real time attack on a particular firm, or even on an industry as in the case of “Quantum Dawn” (following page)

• Tests the responses protocols (hopefully) already in place at the firm, including technology, business and communication responses

• Using a series of “Murphy’s Law” escalations, the simulation stresses the way the firm interacts across groups and with external stakeholders
Cybersecurity – Industry Example “Quantum Dawn”

In the US, the Securities Industry and Financial Markets Association (SIFMA) has been running an industry wide simulation every two years since 2011

- Goal is to improve sector wide resilience to cyber attacks – both individual firms and industry wide
- Last simulation exercise was held on November 8, 2017 – had 900 participants from 50 firms
- The simulation has improved response protocols and forced collaboration both within the firm and across industry, government, regulators and law enforcement
- Designed by Norwich University Applied Research Institute

Wide scale attack in two waves

1. First, each individual firm faces a specific attack (ex. data breach or distributed denial of service)
2. Second, there is a market-wide disruption affecting critical market infrastructure (market exchanges, alternate trading systems and the overnight settlement system)
Quarterly Meeting of the Board of Directors

Case Study

A regularly scheduled quarterly meeting of the board of directors of a major financial services company.

You are the board of directors who are about to receive the quarterly update from the CEO.
Quarterly Meeting of the Board of Directors

CEO Quarterly Report

- Quarterly Results
- Recent Business Wins
- Upcoming Meeting with Senior Government Officials
- Detailed Financial Results
Quarterly Meeting of the Board of Directors

The internet is trending rumors of a significant system hack into a major financial institution;

Our name is on the list of possible victims and we are starting to get calls from our retail customers.

- The rumor is that both personal and financial information of plan members has been stolen and is about to be released, unless a ransom bribe is paid
- We have no evidence that we have been hacked or that any information has been stolen from us / we have not been contacted and are not convinced we are the target
- And while we normally see hundreds of attempted attacks every day, last night we were bombarded with thousands of attacks; we believe we repelled them
• We have up to date, state of the art cyber security framework and technology tools
• Our malware and detection tools show no evidence of intrusion, and the security firm we retain see no signs of intrusion, although they know of recent sophisticated attacks that have gone undetected for weeks
• At the most recent Board update, the CISO outlined the key aspects of CyberBank’s cybersecurity framework, which includes:
  • Segregation of duties within the technology group
  • Employee and member username and passwords
  • Encryption of critical data
  • Firewalls, intruder detection software
• We also have an Israel based cyber security firm on retainer to help monitor / test our systems
Quarterly Meeting of the Board of Directors

CEO Quarterly Report

• Quarterly Results

• Recent Business Wins

• Upcoming Meeting with Senior Government Officials

• Detailed Financial Results
The CTO has established a crisis management team including the CISO, business leaders, human resources and corporate communications.

The CISO has also just concluded a cross industry conference call, with 30 participants from across the industry and regulators (these calls are now being held every 4 hours)

- 2 firms have detected denial of service attacks in the last 24 hours, but both have been repelled

Possible rogue employees:

- One of our employees who had been involved in the password sharing incident noted by Internal Audit called in sick this morning and we have not been able to reach him
- A mid-level technology employee resigned last week / not likely related to this incident but we are following up

Failsafe switch over to the backup system has failed.
The responsibility for proper disaster recovery and prevention is at the TOP OF THE HOUSE. Key activities such as practicing the disaster recovery plan and security of key systems cannot be downloaded to others.

A detailed cyber security event recovery plan will include specific responsibilities for communicating with and the timing of these communications with each stakeholder group.

The post hack activities of management have sometimes made the problem worse for the firm and its reputation.
Quarterly Meeting of the Board of Directors

CEO Quarterly Report

• Quarterly Results

• Recent Business Wins

• Upcoming Meeting with Senior Government Officials

• Detailed Financial Results
The most recent internal audit review was deemed satisfactory but included the following highlights:

• Role of the CISO is not formalized and is not widely understood across the firm
• Some components of our cyber defenses are past due for upgrade
• There were three incidents in the last year of employees sharing usernames and passwords, in order to complete their work more efficiently
• The cybersecurity framework requires significant upgrade, and must be formalized (including approval by the board of directors)
• The definition of “critical data” needs to be updated and formalized
• Communication to employees is sporadic and rules based – no formal communication on training program

While there were numerous attacks, our current defenses blocked them.
In a cyber attack event you must expect that the problems will cascade and potentially grow. The level of uncertainty will increase and certain fundamentals that you believed about your perimeter protection may be challenged.

Perimeter protection audit is a point in time report. Remember that your technology platform is a constantly changing environment and cyber attackers are constantly innovating their attacks.

There is no such thing as absolute certainty about safety from a cyber attack event and that is why you need a plan for immediate response to a discovered hack. IBM reports that 25% of all firms will be hacked over the next 10 years.
Quarterly Meeting of the Board of Directors

CEO Quarterly Report

• Quarterly Results

• Recent Business Wins

• Upcoming Meeting with Senior Government Officials

• Detailed Financial Results
The CTO has good news – we are not the victim

A Robo-Advisor firm has been identified as the victim

Significant client personal and financial information was stolen and members are reporting significant levels of fraudulent transactions

The hackers were supported by a rogue employee in the technology group who was able to point them to unencrypted data
Cybersecurity – Case Study: “You’ve Been Hacked”

Can we all rest easy now?
Implications – Chief Executive Officer

• Cyber incidents are likely to affect at least 25% of all firms in the next decade
• Most cyber intrusions have existed for 6 months prior to them being discovered by the firm
• Advances in technology such as A.I. and quantum computing will increase the threat level
• The post cyber hack management has sometimes caused more damage than the hack event itself
• More work is required to ensure various types of cyber incidents are part of firm’s Disaster Recovery Plan
• The CEO and all senior management must be directly responsible for cyber security prevention and must regularly practise their roles in post hack activities
Implications – Chief Technology Officer

Attack prevention should only be part of a CTO’s cyber-security toolkit; Developing a post-breach action plan and assessing the impact of potential breaches are equally important.

**Prevention: monitoring, regular third-party audits, training**

**Action plan:**

- Develop a formalized incident response strategy including:
  - Both business and technical response plans
  - A clearly defined communication strategy
- Have an established incidence response team:
  - Management, HR, Technical Specialists, Audit and Risk Specialists, General Council, PR
  - Who should lead (CTO, CRO, CEO)? And is there a contingency plan if leader is unavailable?
  - Must have strong communications within and across teams
  - Maintain forensic readiness (audit logs, investigative team on stand-by)
Board Oversight

Has Our Fictional Board Demonstrated the Appropriate Level of Oversight?
Board Standard of Care

- Corporate statutes require a director “to exercise the care, diligence and skill that a reasonably prudent individual would exercise in comparable circumstances.”

- Enquiry focuses on whether directors have turned their attention to the compliance risk and considered it with a degree of competence that is consistent with what a reasonably prudent person would exhibit in comparable circumstances.

- A breach of a board’s duty to monitor occurs when the board either “utterly fails to implement any reporting or information system or controls” or if “having implemented such system or controls, consciously fails to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention.” (“Caremark” standard)

- Consistent with this standard, a Board must follow through to address problems of which it has notice and this may include adopting modifications to its compliance program to address emerging risks.

- OSFI’s Corporate Governance Guideline likewise describe a Board’s role and responsibilities as approving the internal control framework, and reviewing and discussing the implementation of internal controls, including their effectiveness. An effective Board should be responsive to identified issues or deficiencies, and should oversee the rectification of those deficiencies.
An internal control system, no matter how well conceived and operated, can provide only reasonable— not absolute— assurance to management and the board regarding achievement of an entity's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the realities that judgments in decision-making can be faulty, and that breakdowns can occur because of simple error or mistake. Additionally, controls can be circumvented by the collusion of two or more people, and management has the ability to override the system. Another limiting factor is that the design of an internal control system must reflect the fact that there are resource constraints, and the benefits of controls must be considered relative to their costs. Thus, while internal control can help an entity achieve its objectives, it is not a panacea.

Response Readiness

How Prepared Was Our Fictional Company Relative to OFSI’s Guidance?

Cybersecurity Self-Assessment

- Organization & Resources
- Cyber Risk & Control
- Situational Awareness
- Threat & Vulnerability Risk Management
- Cybersecurity Incident Management
- Cybersecurity Governance
Cybersecurity Self-Assessment

Cybersecurity Incident Management

- Documented incident response procedures
- Communications plan
- Post-incident review process
Questions?

Organization & Resources
Cyber Risk & Control
Situational Awareness
Threat & Vulnerability Risk Management
Cybersecurity Incident Management
Cybersecurity Governance