International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Exploring the Cyber Threat Landscape and Cyber Crisis Management Model

Dr. Jnaneswar K[1], Gayathri Ranjit[2]

[1]Associate Professor - HR, TKM Institute of Management, Musaliar Hills, Karuvelil, Kollam

[2]Assistant Professor - Systems, CET School of Management, College of Engineering, Trivandrum

Abstract: ***As cybercrime runs rampant, reports of major cyber incidents and data breaches that would have been unimaginable just a few years ago has now become reality, wreaking havoc on organizations around the globe. These breaches can have a significant, potentially devastating effect on a company's reputation or financial position. Yet too many organizations continue to treat these breaches as technical problems that require technical solutions. Companies need to remain prepared for such cyber crises. This entails not only creating—and testing—an incident response plan, but also establishing the capability to respond to a significant cyber event with a cyber crisis management solution. Such a cyber crisis management solution can be an organization's key to data breach security and survival. A well-planned and efficiently executed cyber crisis management solution can serve as an organization's ticket to data breach survival. The article explores the cyber landscape and cyber crisis challenge and shows how managing cyber crisis can lead to enhanced cyber security. Secondary data has been taken from various journals and websites and Price WaterHouse Coopers 2015 report on Cyber Crisis Management. Based on the data, a crisis management model and cyber crisis management solution is developed.***

Keywords: cyber crime, cyber crisis, cyber crisis management model

1. Introduction

The societal developments of the last decade have made ICT systems a crucial part of our daily lives. The last decade has brought about new possibilities and produced unprecedented developments within the areas of communication and information sharing. However, these developments have at the same time brought with them new risks and threats, such as the 2013 Distributed Denial of Service (DDoS) attacks on the Dutch banking system, which resulted in thousands of people being unable to access their accounts online or use mobile payment systems.1 Another example is the hacking of Indiangovernment officials‟ e-mail accounts, 12,000 of which were penetrated in 2012.

Crisis management is broadly defined as an organization‟s preestablished activities and guidelines for preparing and responding to significant catastrophic events or incidents (i.e., fires, earthquakes, severe storms, workplace violence, kidnappings, bomb threats, acts of terrorism, etc.) in a safe and effective manner. A successful crisis management planincorporates organizational programs such as emergency response, disaster recovery, risk management, communications and business continuity, among others.[3] In addition, crisis management is about developing an organization‟s capability to react flexibly and thus be able to make the prompt and necessary decisions when a crisis happens. If an organization prepares for the "worst-case scenario," then it can handle other situations as well. Teamwork and rehearsal are also critical success factors.[4]

2. Literature Review

2.1 Crisis Management

Never before has crisis management been more important. As recent events have shown, the business community, as well as communities at large, is vulnerable to disruptions that can be extremely costly. Examples of recent crises that resulted in lost lives, displaced families and communities, shutdown businesses and damaged economy are hurricanes Rita and Katrina, the London bombings, the South Asia tsunami, the Northeast blackout and the September 11 terrorist attacks. Other serious events, such as financial failure from poor business management, workplace violence, fires, cybercrime, computer viruses, product tampering or union strikes, can also lead to substantial damage and loss.

Through crisis management planning, organizations can be better prepared to handle unforeseen events that may cause serious or irreparable damage. Traditionally, HR has not been funded or designed to organize or oversee safety and security initiatives. However, regardless of the organization size, HR leaders today have a strategic role and responsibility to ensure their organizations are aware of the human side of a crisis and plan ahead to help minimize its effects.[5] To be most effective, HR leaders work collaboratively with top-down commitment to develop enterprise-wide solutions. As emphasized by HR management gurus Ulrich and Brockbank, "as change agents, HR strategic partners diagnose organization problems…help set an agenda for the future and create plans for making things happen."[6]

2.2 Cyber Crisis

IT (Information Technology) systems are vulnerable to a variety of disruptions from a variety of sources such as natural disasters, human error, and hacker attacks. These disruptions can range from mild (e.g. short-term power outage, hard disk drive failure) to severe (e.g. equipment destruction, fire, online database hacked). Crisis (and Disaster Recovery) planning refers to those interim measures needed to recover IT services following an emergency or system disruption. Interim measures may

include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or the performance of IT functions using manual methods to minimize the business impact.

Cyber crimes are becoming more and more common in the world of e-business. In fact, sensitive information is stolen at a rate that was unfathomable just a few years ago. However, the reputation hit a company can take after a cyber incident is even more costly.

There are three groups of criminals who work to create havoc in the cyber world:

- **Hacktivists:** Hacker activists who steal and disseminate confidential information in order to damage the victim‟s reputation.
- **State-sponsored:** Criminals who steal information for competitive advantage.
- **Organized Crime:** Groups that steal information about customers and sell it underground.

The goals of these groups include the following:

- Significantly disrupting business operations
- Leaking sensitive information to the public for financial gain or a reputation hit to the company
- Obtaining sensitive economic information
- Gaining control of infrastructure
- Maintaining remote access and steal sensitive customer data or corporate information for extortion purposes

These groups often gain access to an entity‟s system and are able to maintain their infiltration for periods of time that can extend into years. Often times, companies try and put out a quick fire by patching the technical holes that caused the breach. However, the problem isn‟t solved at this point, as then the company has been exposed to operational, financial, and litigation risks. In order to be fully prepared, companies need to have to create the capability to respond to a major event in the cyber universe.

3. Objectives of Study

The objectives of the study are to:

- Explore the cyber threat landscape
- Understand the cyber crisis challenge
- Counter cyber threats through a cyber incident response model

4. Cyber Crisis Challenge

Cyber risk is a key commercial and reputational vulnerability that has moved quickly up the risk register in recent years. It is here to stay and looks set to grow and develop in complexity and capacity. Global standards body, BSI Group, defines a crisis as an „abnormal and unstable situation that threatens an organisation‟s strategic objectives, reputation or viability‟. So a cyber-crisis is not a glitch, interruption or business continuity incident but an event that strikes at the heart of an organisation. The case studies are building up, and the most recent high-profile, high-impact cyber security breach, where 70 million customers‟ personal data was stolen, cost the US retail giant Target its CEO and CIO, and 2.5 per cent in like for like sales the following quarter as customers stayed away.

Most organisations are improving their systems‟ resilience but the threats are constantly evolving and continue to grow faster than the ability of most to respond. In this gap there is potential for an organisation to be faced with a cyber-crisis: a serious hack, attack or failure, or a poorly handled corporate response to a security breach.

5. Preparing Senior Leadership Teams for a Crisis

Any crisis, whether it originates from an operational accident, performance failure, corporate governance or policy issue, is about strategic leadership and decision-making under acute pressure and time deadlines.

If the impact of a cyber-attack or security breach is severe and far reaching enough for a crisis to be declared, the crisis management team will be posed with the same challenges of any other crisis and, broadly, be required to deliver the same response strategy. The team should be asking itself:

- How can we protect our customers?
- How can we minimise reputation damage?
- How can we shore up stakeholder trust?
- What will the impact be on the organisation in three, six months or a year‟s time?
- Does this crisis present an opportunity to change the business and address underlying risks?

An effective crisis response is most vulnerable when the crisis management team becomes focused on resolving the technical issue or incident. There needs to be understanding of the vulnerabilities, potential scenarios and potential impacts of decisions the team might need to take in a cyber-crisis.

6. Response Plan for Cyber Crisis

Over the past decade, data breaches and cyber intrusions have increasingly resulted in inquiry and follow-on hearings. Some companies appear to survive these inquiries relatively unscathed, but others respond in a way that opens the door to further criticism of their handling of the incident. Often, the outcome depends not on the number of records compromised or the nature and scope of the intrusion, but rather on the extent to which the organization can demonstrate a structured and orderly handling of the cyber event.

To cultivate an environment in which a structured, orderly response will shine through in the event of a cyber breach and ensuing inquiry, organizations should strive to incorporate these major elements of a cyber crisis response life cycle (Figure 1).

Figure 1: Key elements of a structured and orderly cyber crisis response

Source: Cyber crisis management: A bold approach to a bold and shadowy nemesis-Price Waterhouse Coopers Report 2015

6.1 Cyber Incident Response Process

Traditionally, companies facing a cyber incident, such as a denial of service attack on their network, have treated the breach as a technical problem and responded with a technical response (e.g., by implementing anti-DDOS measures or otherwise increasing security perimeter controls). Companies facing a cyber incident will encounter peril if they assume that a particular incident is a one-time manifestation of a technical problem that can be solved with a technical solution. Significant security incidents will require an entire cyber crisis management solution across the cyber incident response life cycle, from react, to respond, to resolve (Figure 2).

Figure 2: Cyber Incident Response Process

Source: Cyber crisis management: A bold approach to a bold and shadowy nemesis-Price Waterhouse Coopers Report 2015

7. Cyber Crisis Management Model

In the resolution stage, the company may need to develop and implement a remediation plan to ensure that security vulnerabilities are properly repaired against future attacks. (Figure 3).

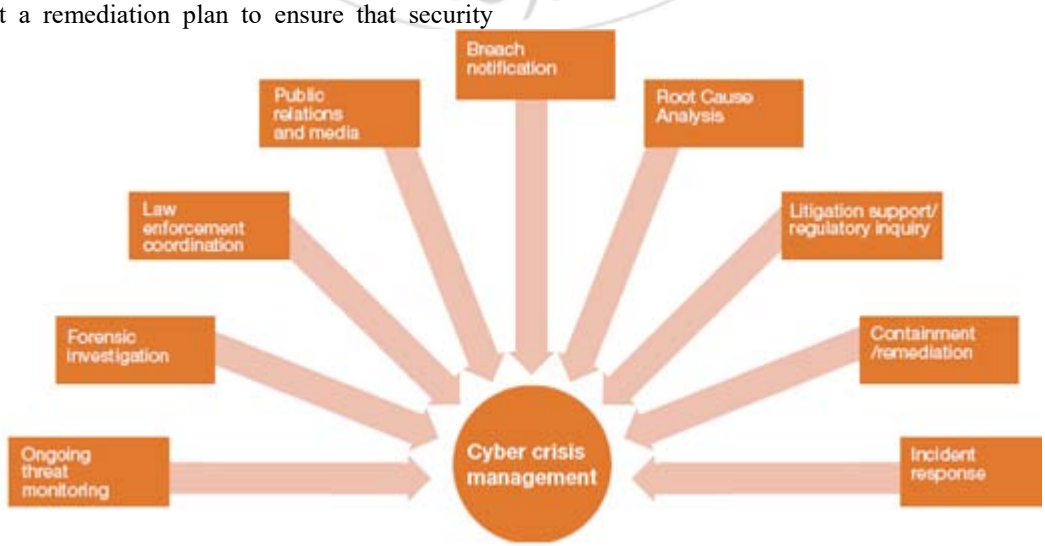

Figure 3: Cyber crisis Management Model

Most of the organizations may have internal capabilities to carry out some of these actions; however, most organizations will lack the expertise and resources to carry out many of the discrete tasks, and will need to bring in any number of external parties.

Services requiring outside specialists include:

- **Threat support analysis services**
  Monitor the criminal underground and analyze the extent to which the attack may be ongoing against the victim‟s systems and network.
- **Incident response teams**
  Provide cyber investigative human and technical resources, incident management, investigation and containment support, and remediation of security control weaknesses.
- **Forensic investigation service***s*
  Efficiently secure and analyze compromised systems and electronic information. These services can include forensic preservation and analysis of computer systems, live memory, malicious software(malware), network traffic, and monitoring logs.
- **Sensitive data discovery services**
  Identify sensitive data in structured and unstructured database environments, as well as identify instances of data leakage involving intellectual property and trade secrets.
- **Advanced network analysis and breach indicator services**
  Identify evidence that may indicate a past breach or a compromise in progress. These services often involve investigation of network traffic and critical data stores for breach indicators and internal and Internet based penetration testing.
- **Customer notification, mailing services and** call center support
  Provide a full array of customer care services in the event the compromise involves personally identifiable information and triggers requirements under state and federal data breach notification laws.
- **Fraud mitigation services**
  Provide credit monitoring solutions to customers whose personal information was compromised as a result of the incident.
- **Public relations services**
  Assist with the rapid development and deployment of a public relations and communications strategy at the forefront of a crisis.

8. Developing a Cyber Crisis Management Solution

A cyber crisis management solution can help you recognize the inefficiencies of an uncoordinated incident response process that relies on independently operation parties who are performing discrete services toward a common goal. A cyber crisis management team can manage all the moving parts of a crisis response (separate from but closely aligned with the more narrowly focused internal cyber incidentresponse team).

The core incident response team is composed of a technical investigative team of technical subject matterspecialists. Moving upward, the team broadens to include an incident team leader and others less involved in the daily technical response. Moving upward again, the broader core team will ultimately include non-IT management stakeholders from legal, finance, and other senior executives.

The cyber crisis management team should act as the program management office, or liaison, between the internal incident response team and the broader environment that includes an array of internal andexternal groups, ensuring the proper coordination among the players. Ultimately, it‟s this team that will lead the organization into a structured and orderly cyber crisis management response to the security incident.

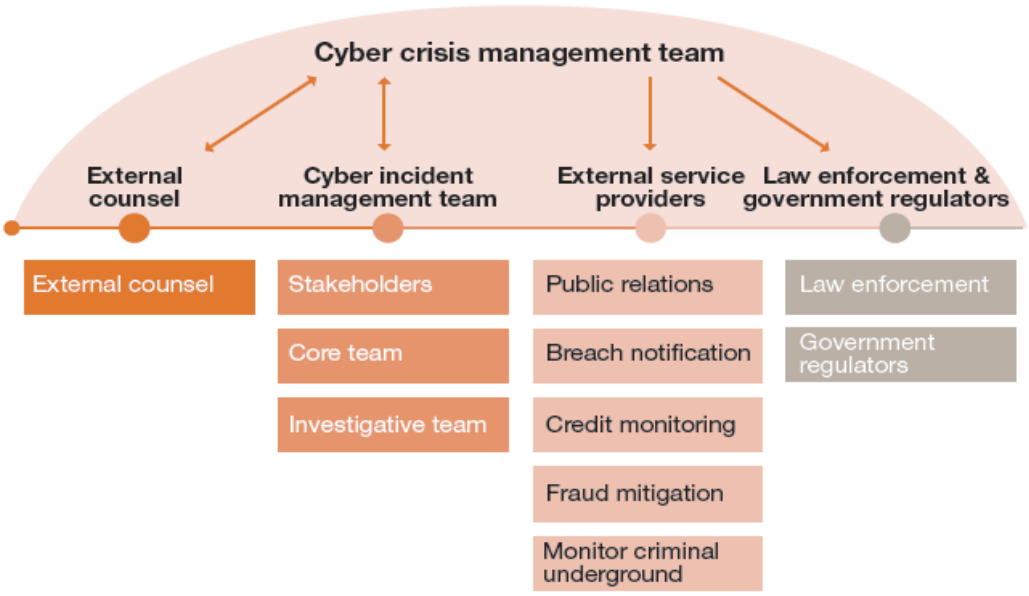

Figure 4: Crisis Management Solution
(Source: Price water House Coopers Report)

9. Conclusion

The cyber threat landscape continues to breed new, advanced cyber issues capable of targeting and successfully compromising any organization. These sophisticated, highly motivated groups gain broad access to the company‟s computer systems and networks and are able to maintain that access for days, months, and sometimes years, causing continuous damage. In responding to these cyber incidents, companies often take an overly technical approach, and, in doing so, leave the company significantly exposed to operational, financial, and litigation risks.

Organizations need to ensure that they‟re well-prepared to survive a cyber security breach by applying a new approach to managing these incidents. The response to today‟s breed of cyber crime should reflect the realities of the evolving cyber threat landscape and embrace the establishment of a cyber crisis management solution. A well planned and efficiently executed cyber crisis management solution can serve as an organization‟s ticket to data breach survival.

References

[1] Blythe, B. T. (2004, July). The human side of crisis management.Occupational Hazards, www.cmiatl.com.
[2] Claire, Snowden., 2014 „Managing a Cyber crisis: What is the most effective way to prepare leadership teams for a high tech threat?‟, Regester Larkin, June 2014.
[3] Clark, J., & Harman, M. (2004, May).On crisis management and rehearsing a plan. Risk Management, 51, 5, 40-44.
[4] European Union Agency for Network and Information Security, 2014, „Report on Cyber Crisis Cooperation and Management‟, Greece.
[5] Fegley, S., & Victor, J. (2005, October).2005 disaster preparedness survey report. Alexandria, VA: Society for Human Resource Management.
[6] PricewaterhouseCoopers, 2015, „Cyber Crisis Management: A bold approach to a bold and shadowy nemesis‟, Report, US.
[7] Society for Human Resource Management.(2005). Glossary of human resource terms.Retrieved from www.shrm.org/hrresources/hrglossary_published.
[8] Ulrich, D., &Brockbank, W. (2005).The HR value proposition. Boston, MA: Harvard Business School Press.
[9] U.S. Department of Homeland Security. Preparing makes business sense. Retrieved August 10, 2005, from www.ready.gov/business/overview.html.
[10] Vallee, F. &Dircksen, M., 2011, „Extended Cyber Crisis Factors for Success in International Trade‟, World Customs Journal, 5(2), 1-94.