BCC&I

THE BENGAL CHAMBER

BUSINESS-iT CONCLAVE 2016

CYBER SECURITY

CYBER SECURITY- A THOUGHT PAPER

Contents

Foreword

Hackers, insiders, criminals and nations have motives for gaining access to information and systems to disrupt or destroy them. Keeping in view the increased pace of technological development, and the growing dependency of organizations on digital information and their interconnectivity, we are posed with a challenging business risk in form of cyber security which requires a dynamic solution.

This report provides a perspective on the overall exposure for organizations in the current time and the various key factors which need to be considered upon to deal with this risk in holistic and integrated manner. The challenges increase due to constant change and adoption of emerging technology and need of hour is to be more proactive than being reactive to cyber security incidents.

Further, the implications of cyber risk have led to increased awareness at the board level, which many organizations today are not being able to address adequately. This study report also provides suggested methods which organizations could consider to enhance overall maturity to deal with cyber security risk and provide board governance on cyber.

I am sure that this report shall assist all of you in addressing the significant risk to which the entire industry is exposed upon.

Ambarish Dasgupta
President
The Bengal Chamber of Commerce and Industry

Overview

Technology has provided significant opportunities to the global world, however at the same time it has exposed the organizations to risk. Cyber security has emerged as one of the key risk areas, which has moved up on the board level agenda. The risk has been constantly evolving due to increased adoption of technology across various business processes in enterprises. Given the threat environment it's become imperative for enterprises to proactively manage this risk.

Stakeholders and regulators are increasingly challenging boards to step up their oversight of cyber security and calling for greater transparency around major breaches and the impact they have on the business. The cyber security landscape and the associated threats is not a new thing the speed of evolution is what is changing.

Attackers today are driven by range of motivation, including financial gain, to corporate espionage, to raising the profile and terrorism. The recent report on Cybercrime in India highlighted that 72% of Indian organizations have suffered cyber security attack and 65% of these attacks were driven by financial gains. The study also highlighted that 64% of these attacks were targeted at directors and members of senior management.

What is at stake?

Since many global organizations have been victims of cybercrime over recent years, board oversight of cyber security is no longer just a leading practice—it is a necessity. Cybercrime has caused various type of losses to the organizations.

Potential impacts across enterprises may include:

- Reputational losses causing impact on market value; loss of goodwill and confidence across stakeholders
- Penalties which may be legal or regulatory fines such as regulatory fines, e.g., for data privacy breaches, and customer and contractual compensation
- Financial impact due to unauthorized transactions
- Intellectual property losses (covering patented information and trademarked materialand commercially sensitive data)
- Administrative resource to correct the impact such as restoring client confidence, communications to authorities, replacing property, and restoring the organization business to its previous levels

Cyber security - Boardroom Agenda

Cyber risk has emerged as near the top of board and audit committee agendas. Investors, governments, and global regulators are increasingly challenging board members to actively demonstrate diligence in this area.As per KPMG's Cybercrime survey 2015, 41% of respondents state that cyber security is part of the Board agenda.

This further gets covered in Global Audit Committee Survey conducted by KPMG 2015, which states that nearly 50 percent of global organizations have either board or audit committees with primary oversight responsibility for cybersecurity risk; yet, only 10 percent say that the quality of information they receive about cybersecurity is excellent.

Which leads to following critical questions

- Are we doing enough to manage the risk from cyber, still not being able to provide the information to board/ audit committee?
- Do we have adequate means of communication as part of cyber program?
- What framework should be followed such that holistic perspective on cyber security is brought upon?

A robust approach to manage cyber risk, which includes the topic in board level decision making, can reduce volatility and uncertainty, and deliver value right across to the organization by achieving the best possible outcome. To effectively address the board room agenda, organizations should be aware of thefollowing :

THREAT	Do you know what elements of the cyber threat are particularly relevant to your business ? Do you know your key assets that need to be protected ?
MONITOR & IMPACT ANALYSY	Do you know monitor and detect any anomalies on your network? What is the worst cases scenario? In what way could cyber threats really harm your business?
RESPOND & SHARE	Do you have adequate incident management plan to respond to incidents? Are you sharing and getting intelligence on emerging threats?

Constantly evolving cyber threat environment

Change is a constant factor in today's world. That may be a cliché, but it is also the challenging truth when it comes to cyber security. The cyber threat environment remains chaotic as attacks are not expected to go down and increasingly they are becoming more innovative and they learn from environment which make them constantly evolving.

As per KPMG's Cybercrime survey 2015, 61 per cent respondents indicated that malware, and 41 percent stated that social engineering, are the nature of cyber-attacks faced by organizations. This indicates that the attacks are not only focused on technology weaknesses, but there is a large focus on exploiting the human weakness. Few of the other key elements captured in the report shows that the cyber threat environment has emerged significantly in India:

- 72 per cent respondents indicated that they witnessed attack during the year, compared to 49 per cent in the previous year, which indicates the frequency and spread of attacks is much wider.
- 63 per cent respondents indicated that impact of cyber-attacks was financial impact during the year, compared to 45 per cent in the previous year, which indicates that the attacks are extremely focused.
- 64 per cent respondents indicated that directors/ senior management was most vulnerable to cybercrime, compared to 32 per cent in the previous year, which clearly indicates that the attacks are targeted.

While the attacks and threat vectors are constantly emerging, some of the facts/ advancement and adoption of technology poses constant challenge for organizations.

The internet wasn't designed to be secure

Cyberspace, which includes the internet and a range of other interconnected systems, was designed to simplify the sharing of digitally stored information. As such it is inevitable that some will use this interconnected network to circumvent the privacy of others to access, disrupt or even destroy information. Security has therefore been something of an afterthought, often retro-fitted onto an internet that has flourished owing to the ability to access information, as well as benefit from freedoms of expression and anonymity.

Machine to machine attacks

Studies suggest that the rise in the connected machine to the internet have increased exponentially on a yearly basis.The usage of smartphones and gadgets such as smart watches, tablets which constitute the "Internet of Things (IoT)" are an easy playground for cyber criminals which have been targeting them to launch a host of machine initiated attacks. These attacks are targeted to either acquire sensitive information and/or exploit them to sabotage the machines.

Convergence of non IT networks (traditionally known as Operational Technology network) with IT network has resulted in exposure of control systems, such as ICS, SCADA, etc.

Third party vendors and service providers

Suppliers and third party vendors are integral part of global organizations today and they provide services which ranges from operational services to strategic services, including cloud based computing services. These service providers provide own set of challenges to organizations, considering that the information gets exposed to external environment which may not be always secured and the concept of having strong external perimeter also diminishes.

Adoption of mobility

Mobility has transformed the way information is exchanged, accessed and processed across corporates. While on one side it has brought in huge productivity but at the same time it has brought unique set of challenges from cyber security view point. Mobility has resulted in proliferation of devices and the concepts of BYOD (Bring your own device) has added on to ensuring consistent security measures being deployed across set of devices.

There have been multiple industry sectors which have been targeted by cyber attackers or have the potential of being targets in the future, including:

AUTOMOTIV E
AEROSPACE
ENERGY PROVIDERS
RETAIL BANKS
PROFESSIONAL & LEGAL
DEFENCE
ADVANCED MANUFACTURI
RENEWABLE ENERGY
INVESTME NT BANKS
RESEARCH INSTITUTES
PHARMACEUTI CALS &
MINING & NATURAL
COMMUNICATI ONS
WIDER FINANCIAL
ACADEMIA

Emerging technologies adding to complexities

New Techniques to conceal identity

As computer forensics has evolved to identify and trace malicious activities, the cyber criminals have also developed techniques to avoid detection. One such technique being used is “Ghostware” which does not leave any trace behind while performing the malicious activity.

Other technique being used is “Two faced Malware”. Many organizations use sandbox testing before deploying any new software in the environment. In sandbox testing the codes are subjected to deeper inspection to observe it they change their behaviors under any circumstances. The two faced malware behaves differently when under inspection/ surveillance and turn into a malicious code once it not under any suspicion or surveillance.

Cloud Services

Proliferation of cloud has led to wider adoption of technology across various streams in organizations. With the increase in cloud based services, cyber criminals are also enhancing their techniques to break into them due to the information they contain. The attacks today are launched through various techniques including malwares.

Attacking cloud services and the related applications on mobile devices will give cyber criminals access to the mobile devices there by acting as remote sites to launch and perform attacks.

Social Media

Social media continues to be providing new ways to connect across set of people and is today an integral part of the strategy of organizations. These platforms not only helps one to be connected with their family and friends but also to exchange thoughts and ideas.

Today the power of this medium is widely recognized to grow and expand business. But this medium is also on the target of cyber criminals which use social engineering to extract information from individuals and then use the same for their vested interests.

Hackers have been using the information posted though posts and share and then use authentic looking phishing emails in order.

It’s not only about technology

Cyber security may appear to be driven by technology, but the reality is that unless adequate balanced approach focusing on people, technology and process is not brought upon, it will not be feasible for management to deal with this threat.

Studies suggest that Executive Board considers Cyber security as a technical issue, and a certain section stating that cyber security focuses too much on technology. This clearly implies a lack of attention to the other two pillars of a complete and balanced strategy: that is people and processes.This view is closely interlinked with the fact that cyber security is a relatively young issue.

The reality is that technology is just one part of the equation in the domain of cyber security and an isolated technological approach will lead to a false sense of security. In other words, an organization using a tool without having clarity on the issue at hand is doing nothing but disservice to the practice.

Closer look at most of the global incidents which have been captured extensively by the media makes us realize that the impact on these organizations was primarily due to not being able to respond and recover from incidents in structured manner. Studies suggest that controls have been looked at or revised on occurrences of incidents, rather than being more proactive.

It’s imperative for organizations to have following key elements as part of the overall cyber security framework:

- Awareness of employees and other key stakeholders
- Comprehensive cyber security incident management framework
- Roles and responsibility of key stakeholders during incident
- Communication management framework during incidents
- Recovery process from cyber security incidents
- Forum to get alerts on threat intelligence and threat sharing

Organizations must develop their Cyber capabilities and shift from a reactive to proactive approach with a holistic view. Two key drivers for multiple organizations continue to be:

1. Incidents act as main driving force for cyber security investments

2. Compliance due to contractual requirement/ statutory requirements

Reactive investments in security are driven by fear. There are organizations which continuously scan threats and analyze data patterns and have been able to develop capabilities to predict the character of nature of future incidents.The maturity level of organizations can roughly be divided into four stages of cyber strategies, ranging from reactive, structured, and integrated to predictive. To achieve the highest level of maturity which is key for high-profile organizations where the stakes are high organizations must find new ways.They should of course focus on being well informed of possible threats and invest in a proper defense. However, they should not do this in an isolated way, but rather use the knowledge and experience of peers, both in the public and private sector. A joint effort is essential to the maintenance of a high level of intelligence.

A multidisciplinary approach helps to avoid specialist blindness and brings in the necessary new perspectives to improve predictions of risk areas.

Immediate future: machines getting on internet

At this moment, we are going through transformation which is blurring the lines between physical, digital, and biological spheres. This creates massive strategic challenges and opportunities for many companies. And it also changes the dynamics of cyber security as the interconnectedness of the world accelerates.

Objects and machines, including cars to utilities to health care devices and life support systems are now connected 24/7. In this shift towards complete connectivity it is evident that part of our longstanding technology can no longer keep up with the pace.

We have witnessed media reports that show how new (and sometimes unexpected) vulnerabilities emerge. These examples draw a lot of public attention as their character is media-savvy. However the biggest risk is probably in other area; for instance, how hackers may exploit devices to gain entry to corporate and government networks and databases.

This may result in obtaining control over industrial systems that control power plants, the energy grid, water supply, and damming traffic infrastructure. The changing dynamics has two perspectives. On the one hand the variety and number of devices is exploding, which brings new challenges to manage the multitude of devices and systems; on the other hand the level of interaction between all these devices also increases, which allows a domino effect and thus multiplies the impact of a possible disturbance.

With India as a country developing multiple smart cities, there is a huge challenge of protecting cyber space including systems and cloud systems as the cyber threat would increase manifold.

There are no easy answers in this domain. But it is clear that this trend leads us to a new reality in cyber security which is no longer confined to cyber space but also comprises our physical world.Thus, cyber security is in fact a license to operate. It will become a prerequisite for success and a differentiator in the market space.

“All the attacker needs to do in order to get to the data is identify a weak link in the chain of connected devices”

Privacy is also a major concern for the “Internet of Things” as information is now shared on various devices. Users do believe to take the necessary precautions while storing information but at times there are things beyond their control.

It is also a point for the industry to take lessons as they are in the process of providing gadget and smart devices to user’s, they must also ensure that best practices relating to coding, patching, usage of secure protocols which can prevent vulnerabilities are also embedded in their culture to minimize impacts from them.

Way Forward

There is no silver bullet which addresses all the concerns and risks to which organizations are exposed due to cyber security. The most optimal answer lies in having an integrated approach focusing on elements, including risk assessments, governance, culture, technology and cyber insurance.

Cyber security risk assessment

Organizations should create a risk profile for their organization based on the following factors:

Business Environment

- What is the business environment?
- In which market does the organization work?
- What all linkages does the organization have with other parties which can add cyber security risk?

Threats

In which sector does the organization works or is involved with, which could lead it to be a possible target for attackers?

Vulnerabilities

Which all vulnerabilities does the organization have from a technical, people, process perspective which can be exploited?

Intended Targets

What could be the intended targets within the chain or relationships?

Legislation

What all legislations related to cyber security the organization needs to adhere to?

By covering the above domains, organizations can then come up with their cyber risk exposure which would help them in concentrating on the exact areas requiring attention. There are various approaches available which can be followed by organizations and more recently there is a mobile application (Cyber KARE) launched by KPMG for conducting the same.

Cyber security simulation drills

Organization should ensure that cyber-attack simulation drills are performed on a periodic basis to enable the employees with the protocol to be followed and also imbibe it in the organization culture. The primary purpose is to provide training which helps in better response to such cyber incidents.

The challenge posed by cyber threats are very dynamic. It is also related on how organizations respond to it. As the response to cyber-attack must be quick and precise because a wrong judgment could further escalate the damage or the compromise.

Awareness on changing threat

Knowing the enemy

The threats that emanate from cyberspace are many and varied, and not all of them apply to every organization. The less informed may assume that all cyber threats are relevant to their business and some commentators who seek to spread fear, uncertainty and doubt do nothing to dispel these assumptions.

There is great commercial advantage to be gained from better understanding those that seek to target organizations for their valuable information. Appreciating their motivations and intentions allows organizations to plan their business activities with a clear sight of what the risks are.

Knowing your enemy can drastically reduce the chances of successful threats. The key is to have good cyber threat intelligence in place as a basis for prioritizing threats, assessing the risk exposure and being able to respond.

Threat intelligence can help organizations anticipate threats by distilling the relevant intelligence from the myriad information feeds available in and outside their organization. Mastering threat intelligence is key to an agile and adaptive cyber governance. To live up to this promise, threat intelligence should be more than raw information. The intelligence has to be both consumable and actionable. If not, even start-of the-art information is only interesting at best.

Designing a comprehensive framework

Adopting industry established frameworks

Organizations may vary in their approach to address cyber security issues at hand by either designing their own frameworks based on the business environment or use industry practices standard, such as the one developed by National Institute of Standards and Technology (NIST).The NIST standard is at the discretion of the organization whether they wish to use the same or not but it may be fruitful as it covers practices from a large number of other bodies such as International Standardization Organization (ISO) which have been successfully implemented. The framework is a risk based guidelines which helps organization identify, implement and improve cyber security practices cutting across industries.

The basis of the framework is on risk management. While cyber security is to be addressed and taken care by the board and senior management, having it expressed in terms of risk makes it easier to understand and deal with it. And, accordingly prioritize investments.

The framework guides organizations to assess themselves by gauging their current approach against the recommended practices which are processes, procedures and risk assessment techniques. This if followed by identification of a target profile where organizations identify the outcomes necessary to improve their approach to cyber security.Once the current assessment has been done and a target profile is selected the framework helps identify the gaps that should be worked upon in order to increase the cyber security preparedness.

The framework defines five activities that are core for having an effective cyber security mechanism:

- Identify: Understanding of how cyber security risks should be managed related to systems, assets, data, and capabilities;
- Protect: Controls and safeguards required for protection against cyber security threats;
- Detect: Monitoring of the activities to provide real time inputs on cyber security;
- Respond: Incident response capabilities
- Recover: Plans in place for business continuity in the event of a cyber-breach.

Board Governance

Management should develop comprehensive process for governance with board and audit committee to ensure that the key stakeholders are comprehensively informed on the overall position of the organization.

Some of the key areas which organizations should consider answering as part of overall governance framework should include:

- What are the new cyber security threats and risks, and how do they affect our organization?
- Is our organization's cyber security program ready to meet the challenges of today's and tomorrow's cyber threat landscape?
- What key risk indicators should I be reviewing at the executive management and board levels to perform effective risk management in this area?

Management should also develop board level dashboards which can be presented on quarterly basis to provide an overview of the progress being made across cyber security domain

Cyber Insurance

Cyber insurance is emerging as one of the risk treatment measures for organizations, which would not solve the problem at hand or mitigate the risk but it does limit the damage to an extent.

Cyber insurance is a domain which is getting more mature globally and increasingly being adopted across regions. In country, this has emerged as an option which organizations have started evaluating and insurance providers within the country are also coming up with solutions which are aligned with the local cyber security laws and implications.

With the increase in awareness and understanding, the studies indicate this will be an option which shall be considered by many organizations.

References

1 Cyber Risk: An executive overview by Philip Hodgins KPMG UK

2 Cyber Security from the Front lines, June 2015 by Greg Bell, KPMG US

3 Cyber Risk in the Boardroom for Global Platinum Clients, March 2016 by Malcolm Marshall, Greg Bell and Paul Taylor, KPMG US

4 Connecting the dots: A proactive approach to cyber security oversight in the boardroom by KPMG US

5 Cyber Security: A theme for the Boardroom by John Hermans, KPMG Netharlands

6 Cyber watch report by KPMG Canada

7 Cyber Risk: What does it mean for your organization? June 2015, by Philip Hodgins KPMG UK

8 Cybercrime survey report 2015 by KPMG India

9 Clarity on Cyber security, May 2015 by KPMG Switzerland

10 Clarity on Cyber security, May 2016 by KPMG Switzerland

11 Security: Time Indian Firms Start Looking From Insurance Prism by T M Arun Kumar. www.itroadmap.in

12 Cyber insurance sees growing demand among corporates By M Saraswathy, June 2015, Business Standard

13 Digital India, Smart City initiatives face cyber threats by Dibyendu Mondal

BCC&I
THE BENGAL CHAMBER

Regd Office BCC&I Royal Exchange 6 Netaji Subhas Road Kolkata 700 001
P +91 33 2230 8396 | 3711 | 3733 | 3746 **F** +91 33 2230 1289
E bencham@bengalchamber.com www.bengalchamber.com