CYBER SECURITY – A BOARD ISSUE

*Nayan Mehta

Introduction

A few years, cyber security was not discussed in Board meetings. Information security was considered as the risk which was supposed to be solely managed by the Chief Information or Technology Officer. Over last few years, cyber attacks have been increasing on companies and other institutions across globe.

Many corporates have fallen prey to cyber attacks resulting in loss of important information, loss of business, regulatory inquiries, litigations, and most of all, loss of reputation and increasing risk to long term sustainability of the organization

In recent past, the world has seen a number of cybersecurity breaches. And they were not about internal security breaches only. These include viral, state-sponsored ransomware, leak of spy tools from US intelligence agencies and full-on campaign hacking.

Recent Cyber Breaches

National Health Service Hospitals (UK), Merck, Maersk, Rosnoft and many others

A hacking group named Shadow Brokers released some alleged National Security Agency tools, including a Windows exploit known as EternalBlue in April 2017. This exploit has been used by by hackers to infect targets in two high-profile ransomware attacks. While Microsoft had released the patch for the bug in March 2017, many users had not applied it making them vulnerable to WannaCry infection. Then, in May 2017, a strain of ransomware called WannaCry spread across the world, attacking hundreds of thousands of entities. The ransomware temporarily affected National Health Service hospitals and facilities in the United Kingdom creating chaos for many patients.

Another wave of ransomware infections that partially leveraged Shadow Brokers Windows exploits hit computers worldwide thereafter. This malware, called Petya, NotPetya, Goldeneye and a few other names, was more advanced than WannaCry. It infected networks in multiple countries—like the US pharmaceutical company Merck, Danish shipping company Maersk, and Russian oil giant Rosnoft.

Cloudflare

In February 2017, Cloudflare, the internet infrastructure company, announced that a bug in its platform caused random leakage of potentially sensitive customer data. Cloudflare offers performance and security services to about six million customer websites. The vulnerability was immediately patched but the data leakage could have started about 5-6 months ago. The hackers did not seem to have used the data malevolently. However, any exposed sensitive data creates risks.

Deep Root Analytics

Deep Root Analytics hosted database containing personal information of US voters on an Amazon S3 server. Due to misconfiguration, more than a terabyte of voter information for 198 million US voters was publicly accessible to anyone on the web. Though, misconfiguration does not amount to hack, it remains a critical and common cybersecurity risk for both institutions and individuals.

Equifax

In September 2017, Equifax announced that 143 million US-based users had their personal information compromised this year. Attackers reportedly exploited a vulnerability on Equifax's website to steal names, Social Security numbers, birthdates, addresses, and, in some cases, driver's license numbers. Credit card numbers for approximately 209,000 people and certain dispute documents with personal identifying information for approximately 182,000 people were also accessed. In this case, Equifax remained vulnerable due to non-application of software patch. Data breaches are fairly common, although those impacting Social Security and driver's license numbers are rarer and more serious. The fact that Social Security numbers are included in the breach makes it likely that victims will be targeted for identity theft.

J P Morgan Chase

In 2014, the attackers stole the login credentials of a J P Morgan employee and were able to access the server. The J P Morgan security team apparently neglected to deploy two-factor authentication on one of the company's many servers, leading to the absence of a security layer that might have otherwise prevented the attack. Following the initial intrusion, the attackers were eventually able to gain access to more than 90 servers at the bank, but didn't manage to steal sensitive financial information before they were detected and blocked in August.

The attackers were able to access customer records revealing email addresses, home phone numbers and mailing addresses for more than 60 million household customers, potentially affecting the

customer trust and creating potential data privacy issue leading to embarrassment for the company and loss of customer trust.

Slack

Slack, a chat app for businesses that replaces intra-office email. It's also acts as an aggregator and plugs into other services like Twitter, Skype, GitHub and Dropbox. Many companies use it to get things done among teams.

In February 2017, Slack disclosed that a four day intrusion allowed hackers to obtain access to user names, email addresses and passwords, and any other information that users may have optionally added to their profiles to integrate with other services, like Skype IDs and phone numbers.

After the incident, Slack released two-factor authentication and a kill-switch. The password kill-switch for team owners allows for both instantaneous team-wide resetting of passwords and forced termination of all user sessions for all team members across all apps and devices.

Sony Pictures

In November 2014, a hacker group by the name "Guardians of Peace" (GOP) leaked a release of confidential data from the film studio Sony Pictures. The data included personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of then-unreleased Sony films, and other information. The hackers then employed a malware to erase Sony's computer infrastructure.

The hackers involved claim to have taken more than 100 terabytes of data from Sony, but that claim has never been confirmed. The attack was conducted using malware. Components of the attack included a listening implant, backdoor, proxy tool, destructive hard drive tool, and destructive target cleaning tool. Thus, it was large scale attack with an intent to gain repeated entry, extract information, destroy data, as well as remove evidence of the attack.

Sony Pictures had to set aside $15 million to deal with damages from the hack. Sony co-chairperson Amy Pascal announced that she would step down and instead will become more involved with film production under Sony.

Any number of businesses across globe are prone to similar or greater risk if targeted with a similar attack. Considering the severity of its impact, cyber attacks are not long being treated as a technology issue but are now considered a business risk requiring enterprise-wide attention. Boards need to recognize this and view them as a risk that is to be managed and integrated into the overall business strategy and operations.

Types of Cyber Risks

Board should be aware of the various ways in which a cyber attack can be launched on the Company's IT infrastructure. The form of cyber attack depends on the type of information being sought by the intruder. The five major types of cyber attacks are -

Phishing attacks

Phishing is perhaps the most commonly reported form of cyber attack. There are many types of phishing attacks making it difficult to control them.

One of the common phishing attack is one where the hackers send out hundreds of thousands of emails with an attachment or link hoping that someone will click on them. If the said attachment is opened, the malware in the attachment gives them access to the user's computer system and information in it.

Fake emails / Spoofing

In this case, the attacker sends an email to an official in any corporate impersonating his superior with an instruction to wire funds. Many a times, corporate officials do end up becoming a prey to such emails and actually wire transfer funds as desired by the attacker. In this type of attack, the attacker does not target data, the target is money and once it's transferred, recovering the same would be very unlikely.

Then there are websites that are replica of actual websites with minor change in web address. If the user is not careful and makes mistake in typing the web address, he would actually end up entering his login id and password in a spoofed website and the same may then be used by the attacker to log in and take control of the account.

Brute force attack

Brute force attack is mainly used to attack a password-protection mechanism. The brute force attack uses a specially designed software to go through hundreds of thousands of different words, combinations of words and numbers to try to crack user password. This is not a common form of attack as it is easy to identify and take corrective action.

Distributed Denial of Service attack (DDoS)

The basic intention of this type of attack is to shutdown user's website / network and stall operation of the user's business. This is achieved by overloading user's server with too many connections to a point where the entire website / network chokes and goes down.

Malware, spyware, ransomware

Malware, spyware and ransomware are different types of malicious software with different objectives. The reason for introducing them in the system can be theft/destruction of data, surveillance, cause business disruption, cause reputational loss, target money or a combination of the same. There are also Trojan horses and key loggers that track keystrokes to gain access to passwords or gain access to the user's system.

If the malware is introduced into a user's system, it will cause the intended damage, and that intended damage could be erasing all the information contained on your hardware.

In case of spyware, hackers introduce a software into the user's system that looks for the simplest form to track keystrokes to get passwords or electronically spy on network, whether to gain access to

confidential information or spying in order to gain access to unidentifiable information.

In case of ransomware, the hackers use the information and/or control on the user's system to demand ransom for release of the same.

The Risk

Since many global organisations have been victims of cyber crime over recent years, board oversight of cyber security is no longer just a leading practice – it is a necessity. Investors, governments, and global regulators are increasingly challenging board members to actively demonstrate diligence in this area.

Regulators expect personal information to be protected and systems to be resilient to both accidental data leakage and deliberate attacks.

Potential impacts and possible implications for the board include:

- Intellectual property losses, including patented information and trademarked material, client lists, and commercially sensitive data
- Property losses of stock or information leading to delays or failure to deliver
- Reputational loss, which may lead to a decline in market value, and loss of goodwill and confidence by customers and suppliers
- Legal expenses, including damages for data privacy breaches/compensation for delays, regulatory fines and the cost associated with defense
- Time lost and distraction to the business due to investigating how the breach occurred and what information (if any) was lost, keeping shareholders advised and explaining what occurred to regulatory authorities
- Administrative cost to correct the impact such as restoring client confidence, communications to authorities, replacing property, and restoring the organisation's business to its previous levels.

Board's Responsibility

The Board's role in understanding and monitoring cybersecurity risk is becoming increasingly important in view of lawsuits being filed against Boards on data security and breach issues.

Retail giant, Target, is now facing a shareholder derivative lawsuit alleging Target's board members and directors breached their fiduciary duties to the company by failing "to maintain proper internal controls" related to data security and misleading affected consumers about the scope of the breach after it occurred. That complaint alleges Target was damaged by having to pay costs associated with the data breach, including expending money for credit monitoring services for affected customers, causing Target "to be exposed to millions of dollars of potential liability in class-action lawsuits," and through "substantial damage" to "the company's sales during the 2013 holiday season, its market capitalization, goodwill, consumer confidence and brand trust."

Wyndham Worldwide Corporation and certain of its officers and directors are also defending against a similar cybersecurity-related derivative lawsuit related to the three data breaches the company sustained from April 2008 to January 2010. That complaint alleges, "In violation of their express promise to do so, and contrary to reasonable customer expectations" the company and its subsidiaries "failed to take reasonable steps to maintain their customers' personal and financial information in a secure manner." The complaint alleges further that the individual defendants "failed to ensure that the company and its subsidiaries implemented adequate information security policies," and the company's property management system server "used an operating system so out of date" that the company's vendor "stopped providing security updates for the operating system more than three years prior to the intrusions" and allowed the company's software to "be configured inappropriately."

The actions of Wyndham are also being held to scrutiny in a Federal Trade Commission (FTC) enforcement action—which just survived a significant motion to dismiss in April—alleging Wyndham violated Section 5(a) of the FTC Act, which prohibits "acts or practices in or affecting commerce" that are "unfair" or "deceptive". According to the FTC's complaint, Wyndham and certain subsidiaries failed "to maintain reasonable and appropriate data security for consumers' sensitive personal information." The fact that this complaint was allowed to proceed foreshadows future regulatory enforcements actions against companies for maintaining inadequate cybersecurity measures.

Irrespective of the final outcomes, these suits highlight that the board plays a fundamental role in preventing and detecting risks associated with information security breaches.

Regulator's Views

The Securities and Exchange Commission hosted a roundtable at its Washington, D.C., headquarters on March 26, 2014, to discuss cybersecurity and the issues and challenges it raises for market participants and public companies, and how they are addressing those concerns.

In India, Securities & Exchange Board of India (SEBI) is planning to put in place a long-term cyber security framework for markets amid concerns over malicious software script targeting systems and possible data breaches. According to the watchdog, Market Infrastructure Institutions (MIIs) should have well laid out change management and standard operating procedures that should encompass all areas related to technology and operations. Among others, SEBI has been stressing on the importance of sharing information on instances of technology-related disruptions, cyber threats and attacks among MIIs so as to enhance their situational awareness.

In May 2017, SEBI had set up a high-level panel on cyber security to suggest measures to safeguard the capital markets from such attacks. The Committee would advise SEBI in developing and maintaining cyber security and cyber resilience requirements aligned

with global best practices and industry standards in accordance with the need of Indian capital market structure.

In August 2017, both stock exchanges in India, the BSE and National Stock Exchange, alerted market entities to guard against a malicious software script that targets critical sectors like energy and finance to steal information from personal computers and passes them on to adversaries outside the country.

The Reserve Bank of India has constituted an inter-department Standing Committee on Cyber Security to establish an ongoing system of security review and analysis of the emerging threats to protect the Indian banking system from cyber attack. The main aim of this Committee is to review the threats inherent in the upcoming and existing technology, adoption of security protocols, interface with various stakeholders and suggest possible policy interventions to strengthen cyber security preparedness of the banking system

Role of Directors In Mitigating Cybersecurity Risk

While cybersecurity risk is often considered an intimidating area for directors to address due to its technical nature, it is important to remember that directors are not required to be experts in this area but are entitled to rely on management and outside experts for advice. In attempting to fulfill their fiduciary duties to the company by managing cybersecurity risks, the following are some guideposts for directors to follow:

- Develop a high-level understanding of cyber-risks facing the company through briefings from senior management and others;
- Consider retaining outside consultants to evaluate the company's security risk management;
- Ensure that the company has at least one committee that is responsible for overseeing and understanding cybersecurity issues, controls and procedures;
- Ensure that the vendors the company retains have adequate security measures in place to protect data and that there are sufficient contractual clauses between the company and the vendor regarding such security;
- Facilitate a culture that views cybersecurity as a business issue that all employees should understand and participate in. As part of that, companies should consider employee training and awareness programs;
- Include a cyber-expert on the company's board of directors or receive regulator reports from a cybersecurity expert that are discussed at board meetings;
- Ensure the company has an updated plan to respond to a cybersecurity attack, should it experience one. As part of that, senior management should become familiar with the legal and contractual requirements to determine what steps they would be required to take if the company fell victim to a data breach;
- Ensure that the applicable directors' and officers' insurance covers data breach lawsuits.

Although the risk of shareholder lawsuits cannot be eliminated entirely, taking one or more of the aforementioned steps may reduce the likelihood of directors being held accountable in data breach lawsuits against the company. The Directors can no longer ignore cybersecurity issues because of the increasing likelihood of a suffering a breach, resulting losses, expenses and possibility of lawsuit challenging the Board's role in that breach.

***Mr. Nayan Mehta**, Chief Financial Officer of BSE Ltd.

ASSESSORS INVITED

IOD Institute Of Directors — Building Tomorrow's Boards

Would you like to be an assessor of these most prestigious awards

We are constantly on the lookout for volunteers, professionals or quality people nominated by their organisations who can become certified examiners for Golden Peacock Awards

GOLDEN PEACOCK AWARDS SECRETARIAT
invites for specialists in the areas of

CORPORATE GOVERNANCE & SUSTAINABILITY

A most rewarding and rich learning experience

Golden Peacock Awards® — A Strategic Tool to Lead the Competition

Please send your CV at info@goldenpeacockaward.com

GOLDEN PEACOCK AWARDS SECRETARIAT

M-56 A, Greater Kailash Part - II (Market), New Delhi-110048, India • Board Nos.: +91-11- 41636294, 41636717, 41008704
Fax: +91-11- 41008705 • Email: info@iodglobal.com

www.goldenpeacockaward.com