Global Challenges and Cyber Security Management - A New Business Priority

Arshad Amir Labba[1], Krishnendu Bal[2], Mallieswari.R[3], Debolina Gupta[4]

[1]Business Analyst, P & BB Technology, Toronto, Canada
[2]Senior Specialist, GIRAS Pvt Ltd, India
[3]Assistant Professor, Ramaiah Institute of Management, Bangalore, India
[4]Assistant Professor, Ramaiah Institute of Management, Bangalore, India

---

ABSTRACT: *In today's digital world, corporates and financial organizations deal with highly sensitive data and information that is crucial for their growth and survival of the company. They may range from intellectual property, customer databases, corporate strategy, etc. But are these organizations doing enough to protect their valuable data from cyber threats? In an age of ongoing digital transformation published on October 13,2019, it is observed that, cybercrime has become one of the today's fastest-growing form of criminal activity. It has thus become an worrying factor for the modern executives to set to cost businesses $5.2 trillion worldwide within five years, according to Accenture.*

Posted on Nov 18, 2019 by Robert Ackerman JR. Cybersecurity must be viewed in the perspective –a business perspective, to be precise. This means, among other things, that companies must be able to aggressively debunk a potpourri of myths. They must realize, for example, that not all assets in the organization must be protected in the same way. Spending more money on cybersecurity may not make the organization more secure-and neither necessarily does buying the most advanced technology. The external hackers are hardly the only threat to the corporate assets. According to Ancarani and Di Mauro, 2018 states that the Internet of Things is exponentially increasing the number of entry points for organizations to defend from nefarious actors. Complex digital value chains expose firms to risks beyond their direct control. The potential damage of cyberattacks is substantial in terms of continuity of business operations, theft of confidential information and reputational harm. A recent survey has shown us that, in the year 2014, organizations reported financial hits of $20 million or more, which has increased by 92% from 2013[1]. This is a clear indication that it is an increasingly critical management issue.

Cyber security was something that did not get a lot of executive attention. It is no longer an issue that concerns only information technology and security professionals, the impact has extended to the c-suite and the boardroom. Corporates need to understand that in this digital global world where an exchange of information can happen only with a click of a button, that information needs to be safeguarded against persistent cyber-attacks.

Keywords: Cyber security, Information, Digital word, Corporates, Intellectual Property

1. INTRODUCTION

As our corporate and financial institutions are technologically evolving every day, a new form of threat has entered this realm, Cybercrime. The protection of valuable intellectual property and business information in digital form against theft and misuse—is an increasingly critical management issue.

Hacking for financial gains, theft, disrupting the networks and servers, etc. are just some of the forms of cybercrimes that can be often seen when scanning the headlines. For example, hackers might target a company's financial function in order to obtain its earnings reports before it is publicly released. With such advance knowledge they can profits by acquiring a dumping stocks. In the latest attacks on JPMorgan Chase, the hacker was on their servers for more than two months before they realized they were compromised. Things got more embarrassing when they failed to identify the extent of damage incurred. The magnitude of data stolen does not only affect them financially but would also dent their reputation in terms of customer loyalty. Cybercrime is a growth industry. The returns are great and the risks are low. $400 billion would be the likely annual cost to the global economy due to cybercrime[2]. With estimates varying from $375 billion at the least to $575 billion,

[1] *Pg 10 of Managing cyber risks in an interconnected world published by PWC*
[2] *Pg 2 of Net losses: Estimating the Global Cost of Cybercrime by Mcafee*

due to cybercrime, these figures would put any country to shame as many smaller countries have less income than the stated losses[3].

Hacking is the predominant method of perpetrating ***cybercrime***. Cybercrime, as defined by *Webster's* (2006), is a crime committed on a computer network. The virtual nature of cybercrime makes it global in scope. *Wall Street Journal* reporter Cassell Bryan-Low (2006), writes that the U.S. Federal Bureau of Investigation ranks cybercrime as its third highest priority, behind only terrorism and espionage in importance

Putting a number on the cost of cybercrime and cyberespionage is the headline, but the dollar figure begs important questions about the damage to the victims from the cumulative effect of losses in cyberspace. The cost of cybercrime includes the effect of hundreds of millions of people having their personal information stolen—incidents in the last year include more than 40 million people in the US, 54 million in Turkey, 20 million in Korea, 16 million in Germany, and more than 20 million in China[4].

In this regard, it is more than evident that cybersecurity is just not a technical matter but it is also a strategic issue that has to be given utmost importance. The companies will have to identify their most sensitive data and invest in the right ways to ensure there is no data breach. Moreover, they should constantly monitor and be vigilant before they fall prey to false sense of security.

This awareness and concern derives from heavy dependence of integrated information systems and technology for Industry 4.0. Manufacturing companies rely on data to run their operations (2019).

The proposed "Cyberbiosecurity" as an emerging hybridized discipline at the interface of cybersecurity, cyber-physical security and biosecurity. Initially, we define this term as "understanding the vulnerabilities to unwanted surveillance, intrusions, and malicious and harmful activities which can occur within or at the interfaces of comingled life and medical sciences, cyber, cyber-physical, supply chain and infrastructure systems, and developing and instituting measures to prevent, protect against, mitigate, investigate and attribute such threats as it pertains to security, competitiveness and resilience."(2018)

Given the increasing pace and complexity of threat, corporations must adopt approaches to cybersecurity that will require much more engagement from the CEO and senior executives to protect critical business information without constraining growth and innovation.

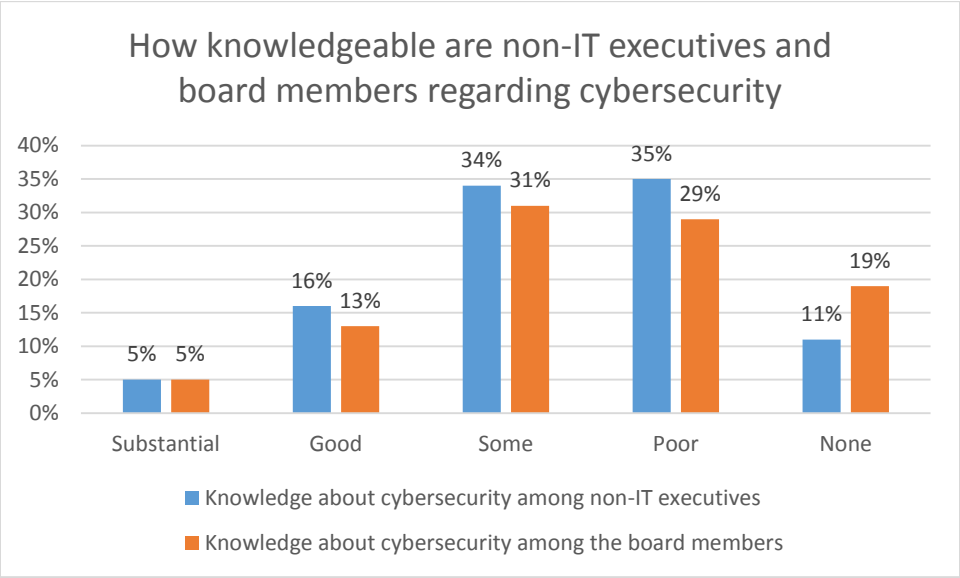
2. BARRIERS TO CYBERSECURITY

Organizations are constraint by several deficiencies which impedes its ability to detect and act against attacks. A recent study has shown that there is a lack of communication between the IT professionals and the upper management when it comes to the importance of cybersecurity.

48% of the professionals believe that their executives have sub-par understanding of the security issues. Thus the executives fail to appreciate the value of putting effective security in place and do not equate it to financial loss. The research from Ponemon has identified that due to data breaches, the average loss of revenue for an organization is $5.4 million[5].

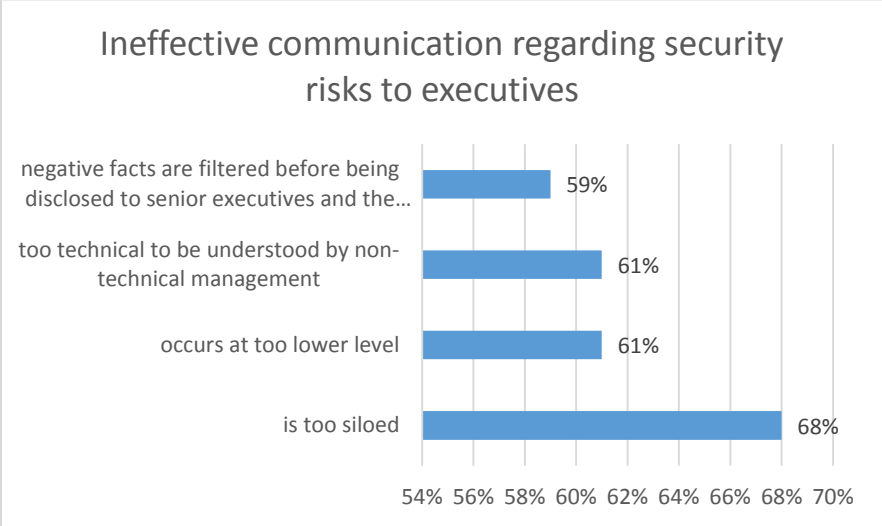
The chart below shows when security professionals were asked when how knowledgeable they thought their non IT executives and board members were:

[3] *Pg 10 of Managing cyber risks in an interconnected world published by PWC*
[4] *Pg 3 of Net losses: Estimating the Global Cost of Cybercrime by Mcafee*
[5] *Pg 2 of Exposing the Cybersecurity Cracks: A Global Perspective by Ponemon Institute*



(Source: Exposing the Cybersecurity Cracks: A Global Perspective 2014)

The first step towards strategic planning should be communicating with the C-levels and the employees of cybersecurity and its importance. 64% of security professionals don't communicate security risk with senior executives or only communicate when a serious security risk is revealed[6]. When asked why communicating relevant security risks to executives was not effective, the following responses were found:

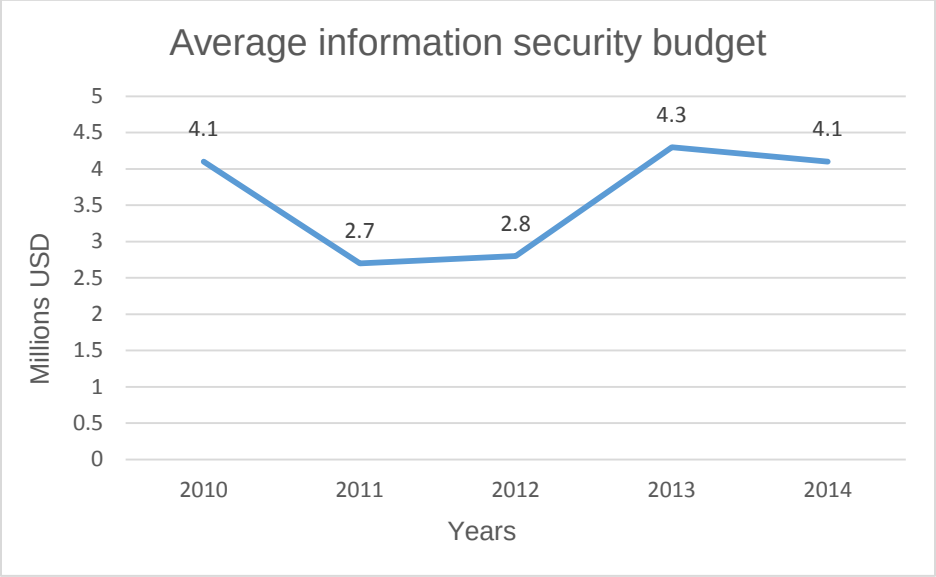


(Source: The state of risk free security management, 2013)

With low levels of understanding and with the growth of advanced threats and risks, upper management may be unsure of where to focus. Therefore, it is necessary to elevate the role of information security in the organization and stress on the fact it is merely just not a technological function. It requires a senior leader, chief information officer, chief security officer – the title doesn't matter, but the person bringing the knowledge to c-level and boardrooms must be able bring the security issues to them and help the management in taking right decisions across multiple platforms.

[6] *Majority of it Professionals Don't Communicate Security Risks by Tripwire.com*

Despite the elevated concerns, there is actually a 4% dip in the security funding in 2014 compared to 2013. It comes as a disappointment as Gartner's forecasted for a 7.9% increase in security spending for the year 2014. After some of the prolific attacks on Target, home depot, UPS, etc. last year it comes as a surprise that organizations haven't stepped up in investing in information security[7].



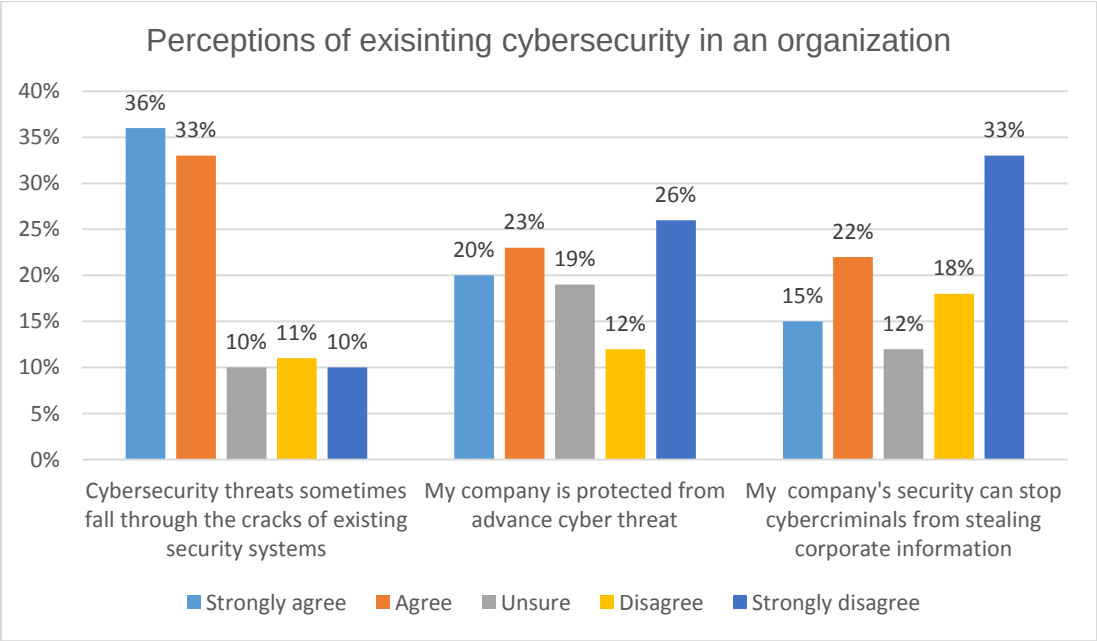
(Source: Managing cybersecurity in an interconnected world)

Return on investment is another reason when lack of investment is concerned with the security function. That is a question that security professionals have been struggling with; how do you show ROI to the upper management and board of directors. The reality is that ROI is unlimited. The real question should be, "what do you lose if you don't have the right security in place". No value can be placed on a company protecting its intellectual property and reputation.

Due to the sophistications of today's threats, companies that have an existing system in place falls short against cyber-attacks. Because of a wide array of security threats, it's challenging to foresee, recognize and reduce the threat. 57% of respondents do not think their organization is capable of protecting it from advance cyber-attacks while 63% doubt they can stop exfiltration of confidential data[8].

[7] *Pg 19 of Managing cyber risks in an interconnected world published by PWC*

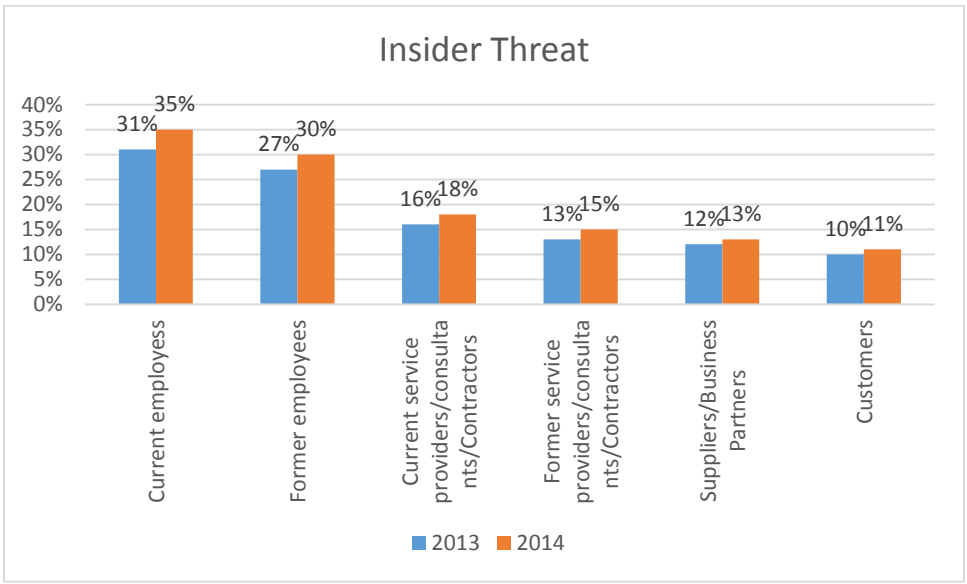
[8] *Pg 3 of Exposing the Cybersecurity Cracks: A Global Perspective by Ponemon Institute*



(Source: Exposing the Cybersecurity Cracks: A Global Perspective 2014)

3. THREATS

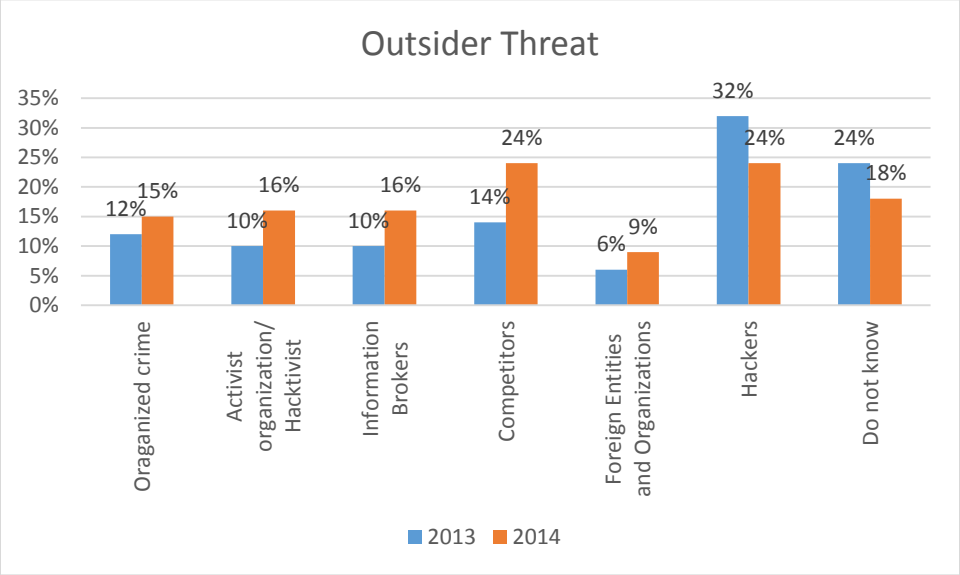
Most of us are under the misconception that threats usually come from the outside. But this is not true and one of the biggest threats faced by any organization is from within; their employees. Insider threats are costlier and damaging than incidents from the outsiders. Insider threat can be intentional or unintentional. For example, failing to change default password or leaving their computers on when they go home. The chart below signifies an increase in 2014 from insider threat compared to 2013



(Source: Managing cybersecurity in an interconnected world)

At the same time, outside threat cannot be ignored which are responsible for lion's share of threat. Since 2008, the Verizon Data Breach Investigations Report has shown that external actors are responsible for the vast majority of the breaches they

investigated. Some of the top reasons why breaches were successful include: weak credentials, malware propagation, privilege misuse, and social tactics[9]. These are precisely the types of weaknesses that trace back to the actions (or inactions) of insiders.



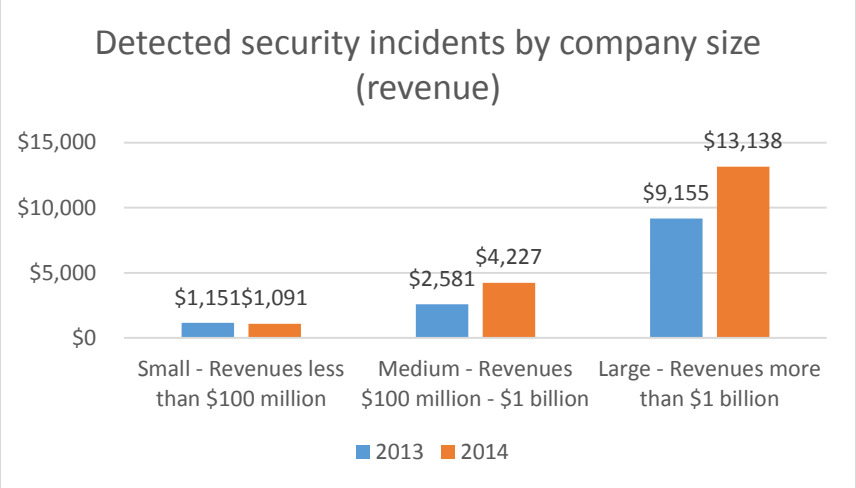
(Source: Managing cybersecurity in an interconnected world)

Cyber Security is at a turning point. In many countries it has become a national policy priority. For developed countries, cybercrime has serious implications for employment. The effect of cybercrime is to shift employment away from jobs that create the most value. Even small changes in GDP can affect employment. In the United States alone, studies of how employment varies with export growth suggest that the losses from cybercrime could cost as many as 200,000 American jobs, roughly a third of 1% decrease in employment for the US. Using European Union data, which found that 16.7 workers were employed per million Euros in exports to the rest of the world, Europe could lose as many as 150,000 jobs due to cybercrime, or about 0.6% of the total unemployed[10]. The most important cost of cybercrime, however, comes from its damage to company performance and to national economies. Cybercrime damages trade, competitiveness, innovation, and global economic growth.

4. INCIDENTS AND FINANCIAL IMPACTS

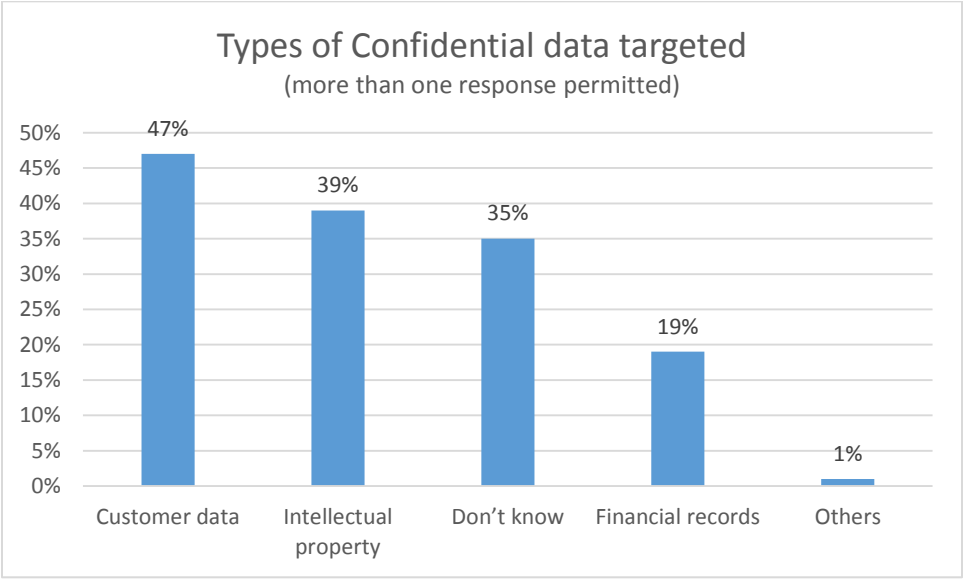
The threat perception is unbiased in their attacks, many small and medium sized companies are under the impression that their size and the minimal security that they have put in place will safeguard them against cyber-attacks. Attacks on information systems operated by small and midsize companies are growing rapidly and are having a severe impact on business operations. Obviously larger firms have more to lose in terms of absolute revenue but the ability of the smaller firms to bounce back after an attack makes it more important that they focus on their information systems.

[9] *Insider vs. Outsider Threats: Can We Protect Against Both? by Securityweek.com*
[10] *Pg 3 of Net losses: Estimating the Global Cost of Cybercrime by Mcafee*



(Source: Managing cybersecurity in an interconnected world)

Larger companies have been investing in securing their information systems which forces the threat actors to shift their focus on middle and small sized business houses which may or may not have follow the necessary security practices. That, in part, explains the 64% jump in the number of incidents detected by medium-size organizations. Small organizations proved the exception in discovering compromises. Companies with revenues of less than $100 million detected 5% fewer incidents this year[11]. The reasons are not immediately clear, but one explanation may be that small companies are investing less in information security, which may leave them both incapable of detecting incidents and a more tempting target to cyber adversaries. Company leaders have to identify their most sensitive data. Anything that has to do with intellectual property, financial records and transactions and business, customer and employee data should always be protected. 37% of the respondents say with certainty that their companies have lost sensitive and confidential data, while 15% are uncertain. But it's a more disturbing fact when 35% of the respondents who lost information due to the threats are unsure as to what was stolen[12]. Respondents were asked if they lost data due to cyber-attack and if yes, what kind of data were lost or stolen.



(Source: Exposing the Cybersecurity Cracks: A Global Perspective 2014)

[11] *Pg 8 of Managing cyber risks in an interconnected world published by PWC*

[12] *Pg 7 of Exposing the Cybersecurity Cracks: A Global Perspective by Ponemon Institute*

Financial impact may include decreased revenues, disruption of business systems, regulatory penalties, and erosion of customers. Non-financial impact may include reputational damage, the pirating of products, diversion of research and development information, impacts to innovation, stolen product designs or prototypes, theft of business and manufacturing processes, as well as loss of sensitive information such as M&A plans and corporate strategy. The cost of stolen Intellectual property (IP) is the most difficult to estimate for the cost of cybercrime, but it is also the most important variable for determining loss.

A US Department of Commerce report found that IP theft (all kinds, not just cybercrime) costs US companies $200 to $250 billion annually. The Organization for Economic Development (OECD) estimated that piracy costs companies as much as $638 billion per year[13]. IP theft can range from paint formulas to rockets.

4.1 Financial crime—the theft of financial assets through intrusions—is the second largest source of direct loss from cybercrime. It is a high-profile crime. When millions of people have their credit card information stolen by hackers, it gets immediate attention. Privacy laws that require reporting when personal information is compromised mean that there are numerous anecdotes of successful attacks. These attacks can cost the victim companies more than $100 million in recovery costs for large incidents, even if the actual amount gained by cybercriminals is much smaller. The best data on cybercrime, unsurprisingly, comes from the financial sector, which is regulated, pays serious attention to cybersecurity, and can easily measure loss. In Mexico, banks lose up to $93 million annually just to online fraud. The National Police Agency estimates that Japanese banks lose about $110 million annually. The 2013 hack against the US retailer Target, alone cost banks more than $200 million[14]. High-profile cyber-heists that garner tens of millions of dollars from banks get a lot of attention and are a global phenomenon.

5. METHODOLOGY

The main aim of this research paper is to highlight cybersecurity as an important issue for strategic business management. The objectives of the research paper is to analyze of the relationship between cyber security and the loss of revenue. Therefore, the project also involves discovering on why there is a deficiency in an organizations ability to protect themselves against cyber-attacks. Finally, the paper will analyze the different kinds of cyber threats in the corporate world.

5.1Research Design

This is a conceptual type of research. Various books, articles and publications were referred to collect and compile the data. Since the aim of the study is to obtain complete and accurate information, the procedure was carefully planned.

5,2 Limitations

This paper relies on data previously collected by other researchers because of the inability to collect data on our own on this topic. All the risks that's involved with cyber-attacks could not be explored due to time constraints.

6. FINDINGS

- Large multinational firms are better equipped to detect cyber threats because of the multilayer security system in place as compared to smaller firms.
- Despite the above finding companies suffer from deficiency in detecting attacks because of low understanding on the part of the management team, the confusion that prevails as to what is to be protected and the fast changing landscape and sophistication of threat around them.
- As business functions move online and as more companies and consumers around the world connect to the Internet losses from the theft of intellectual property and customer data would sequentially increase over the year.

7. RECOMMENDATIONS

Companies concerned should adopt a framework focused on delivering an enhanced collaboration and communication with the management and the IT professionals. The role of the management leadership is imperative for identifying and controlling the financial and operational impacts that would arise out of the situation. The board room must invest in the right

[13] *Pg 13 of Net losses: Estimating the Global Cost of Cybercrime by Mcafee*
[14] *Pg 15 of Net losses: Estimating the Global Cost of Cybercrime by Mcafee*

technologies at the right time *to Educate monitor and protect* their information systems and also the CIO's should keep track of the existing and potential threats that plague the industry which should include state sponsored espionage and evolved espionage spyware. Focus should be laid on employee awareness and training. To improve their security, one option is that the small and medium companies might adopt cyber insurance as a tool to mitigate the risks in a cost effective manner. Cyber risk management puts organizations in the mindset to navigate the rough cybersecurity landscape of the 21st century. Going to extremes trying to avoid breaches is unrealistic. Customers and regulators understand the challenges faced by adversaries such as nation-states, multinational criminal organizations, hacktivists, terrorists and insiders, according to Dave Mahon, chief security officer at CenturyLink Inc.. Victims of cybercrime won't be blamed for being victimized -- they'll be blamed for subpar incident response capabilities, poor recoveries and incomplete disclosures.

8. CONCLUSION

While addressing cyber security it is clear that is not only an IT issue anymore, organizations should approach the realm of cyber security like any other business risk with the management onboard providing and creating a valuable roadmap for the security professionals to act upon in case of a threat. Applying the security dilemma to cyber operations has benefit that can help to determine which cyber security concepts are most important for the non-cybersecurity specialist. Future improvements in technology will someday lead to better cyber security until then company's small and large should devote their resources to better manage risks because its sometimes cheaper to prevent than to cure.

REFERENCES

1. Graham, James. Olson, Ryan and Howard, Rick. (2010), "Cyber Security Essentials"
2. Peter W Singer and Allen Friedman. (2014), "Cyber Security and Cyber war"
3. Lillion Ablon, Martin C Libiki, Andrea A Golay, (2014) RAND National Security Research Division, "Markets for Cyber-Crime Tools and Stolen Data"
4. Mcafee, "RP Economic Impact Cyber-Crime"
5. OECD, "Non-governmental Perspectives on a New Generation of National Cybersecurity Strategies." Digital Economy Papers, No. 212
6. Ponemon, "Exposing cybersecurity cracks"
7. PwC, (2015), "The Global State of Information Security Survey"
8. Securityweek.com, "Insider vs outsider threats can we protect against both"
9. Tripwire.com, "State of security, risk based security for executives risk-management majority of it professionals don't communicate security risks"
10. The Metropolitan Corporate Counsel, "Cyber Attacks Know no Barriers" Volume 21, No. 12 December 2013.
11. Giovanna Culot; Fabio Fattori and Matteo Podrecca "Adressing Industry 4.0 Cybersecurity IEEE Engineering Management Review (Volume : 47,Issue:3,third quarter 3,Sept 1,2019
12. Murch RS, So WK, Buchholz WG, Raman S and Peccoud J (2018) Cyberbiosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy. Front. Bioeng. Biotechnol. 6:39. doi: 10.3389/fbioe.2018.00039
13. https://books.google.co.in/books?hl=en&lr=&id=dE8jDgAAQBAJ&oi=fnd&pg=PP1&dq=Cyber+Security-+a+new+business+priority+and+its+implication+in+the+corp
14. Elms, Eric R, La prade, John D, Maurer, Mathias L "Hacking of Corporate Information Systems: Increasing Threats and Potential Risk Management Techniques CPCU eJournal. Feb2008, Vol. 61 Issue 2, p1-9. 9p. , Database: Business Source Elite
15. Dave Mahon, chief security officer at Century Link. The New Security Model: Four Cyber Risk Management Concepts To Follow 2/4/2018
16. Hacking of Corporate Information Systems:Increasing Threats and Potential Risk Management Techniques by Eric R. Elms, John D. LaPrade, CPCU, CLU, and Mathias L. Maurer Background
17. Elina Haapamäki and Jukka Sihvonen Cybersecurity in accounting research Received 11 September 2018 Revised 15 February 2019 Accepted 18 March 2019