Contents

Abstract 2

Introduction 2

Aims of Research 3

Background 3

- Reaction required from Board of Directors 5
- The paradox 5

Literature Review 6

Cyber threats as of 2016 6

- The ever-rising machine-to-machine attacks 6
- The general attack trends and the most vulnerable devices 7
- Cloud related cyber threats 7
- Law Enforcement related hack attacks; ‘ghostware’ and ‘blastware’ 7
- Two faced Malware 7
- Defending against Cyber threats 8
- Beware of disgruntled employees 8
- Uninformed, laid back and careless employees 8
- Use of mobile devices 9
- Usage of Cloud computing or data storage 9
- Device firmware based threat (if unpatched or unattachable) 9
- Employment of 3rd party specialized technology companies 9

General approach to ensure data security 10

- Executive involvement in matters of cyber security 10
- Heat Mapping Sessions between Executives and experts 10
- KPIs (Key Performance Indicators) 11
- Cyber security threat incident simulation 11
- Examine new technologies related security implications 11

MacAfee Labs Report on cyber security for 2017-2020 12

- Hardest to resolve security threats 13
- Effectiveness of threat-related defense 13
- Cloud computing related threats, regulatory and vendor response 14
- Crown Jewels would be retained by companies 14

Weak authentication schemes 15
Eastwest and Northsouth attack vectors 15
Service Layers Gaps 16
Visibility and control issues 16
Hackers would try to avail speed, anonymity, and scale by resorting to cloud 16
Denial of Service for ransom attacks 16
Global Threat Perception and Attitude Measurements for 2017 17
Emerging Technologies are the main source of uncertainty increase 17
Threats appear Overwhelming to IT professionals 17
Sector wise Industry perceptions 17
Cybersecurity Market Report Q4 2016 18
Market size 18
Data Analysis 20
Discussion 20
Conclusions/Recommendations 20
Critical evaluation 21
Areas for further research 21
References 21

Abstract

The paper presents all the major threats related to cyber security for businesses at the end of the year 2016 as well as estimation regarding the 2017-2021 period. Cyberthreat related damages and costs during this period are assessed and the total amount of expected. cyber security-related investment is described as well. Threats due to the new and emerging technologies are discussed and IoT and cloud computing are discussed to highlight the potential for cyber threats that would hit these technologies due to possible vulnerabilities. The analysis in made to figure out if indeed cyberthreats constitute a strategic threat to businesses and should they discuss it on the board and give it strategic importance. The evidence is presented to indicate that indeed cyber threat is an existential threat to businesses. The cyber threats in cloud computing are discussed and emerging technologies are described as the most vulnerable. Estimates for investment in cyber security worldwide in 2017 and till 2021 are presented as well as the possible damage costs during the same period in the future.

Introduction

Even though billions of dollars are being spent worldwide on protecting data residing with business organizations large and small, it is not uncommon to find a news about a security

breach somewhere in the world. The giant corporations who have literally fool proof (as per contemporary standards) security are no exceptions to this breach. Most often, the data breach is a result of an external hack attack. Such attacks are growing increasingly frequent and even more complex and more targeted with every passing day. In most cases, the attacks have one aim; the hackers aim to gain financially. There exist some advanced forms of hack attacks referred to as APTs (Advanced Persistent attacks) which are extremely stealth type of malware attacks. This type of malware would enter the organization's cyber systems and it would appear as if nothing has happened. It would start permeating through the internal systems and mutating into many variants that in turn would not do any harm either apparently. thus, by being apparently harmless, it would avoid detection. With time, it would start accessing the valuable targeted data in a stealth mode and then would start transmitting this to its originator. The kind of data it targets are usually such corporate assets as assets on Intellectual Property, business secrets, data related to company's finances and customers. Not only the firm risks losing financially, but great damage to its goodwill and reputation can occur due to such customer related private data breaches. It is for this reason that Cyber security can be termed a strategic issue for both large and small organizations. The very basis of its operation; customer confidence is jolted if a data security breach occurs even once.

Aims of Research

This research aims to analyze the strategic importance of issues related to cyber security and malware protection for business organizations and attempts to explore the preventive and remedial actions these organization can take to mitigate or preferably eliminate such threats.

The research aims at scouring the literature available to find answers to the following research questions:

- Do cyber security and malware threats constitute a Strategic threat to businesses?
- Are business organization aware of the strategic importance of the issue?
- What steps are being taken by these organizations to strategically tackle cyber security threats?
- Is the cybersecurity issue being taken up at the Board level in view of its existential importance?
- How confident are businesses and IT professionals about dealing with increasing threats?
- What budget allocations would be done by organizations aimed at cyber security in 2017?

Background

Increasingly, the business organizations are burdened with the effort required to mitigate the security breaches and the impact on the organizations both financially and goodwill-wise is rising. The news networks are usually quick to jump on such news and they get highlighted promptly thus causing serious dents in the company's reputation. As the business world and cyber systems are increasingly being regulated, most often, the business organizations are bound by regulation to disclose the security breaches to the news media. At other times, the clients

make it mandatory for the organizations to report the breaches. Even if the news does not get to the networks directly from the organizations, the hackers themselves advertise it to the news media by reporting it online. In either of these cases, the result is the same. The organizations tend to lose reputation built with years of hard work and due diligence and on top of this, the financial losses are substantial as well. The financial losses that would accrue in the future due to lost reputation or client confidence are another matter which cannot even be calculated precisely.

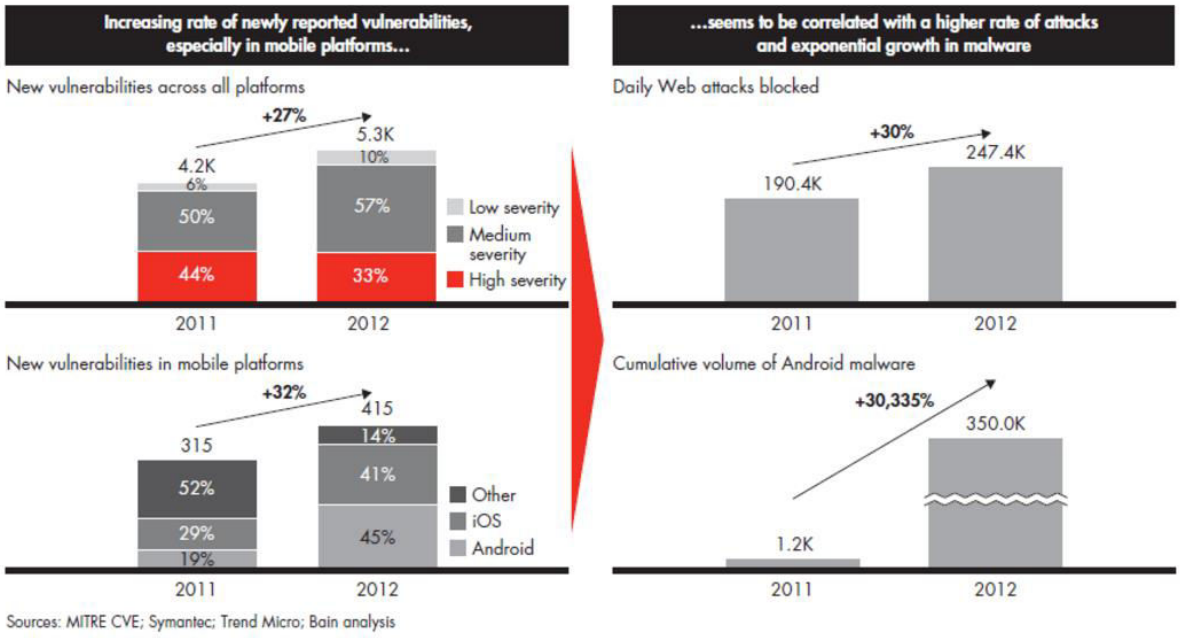


Figure 1 Cyber-attacks in 2011 and 2012

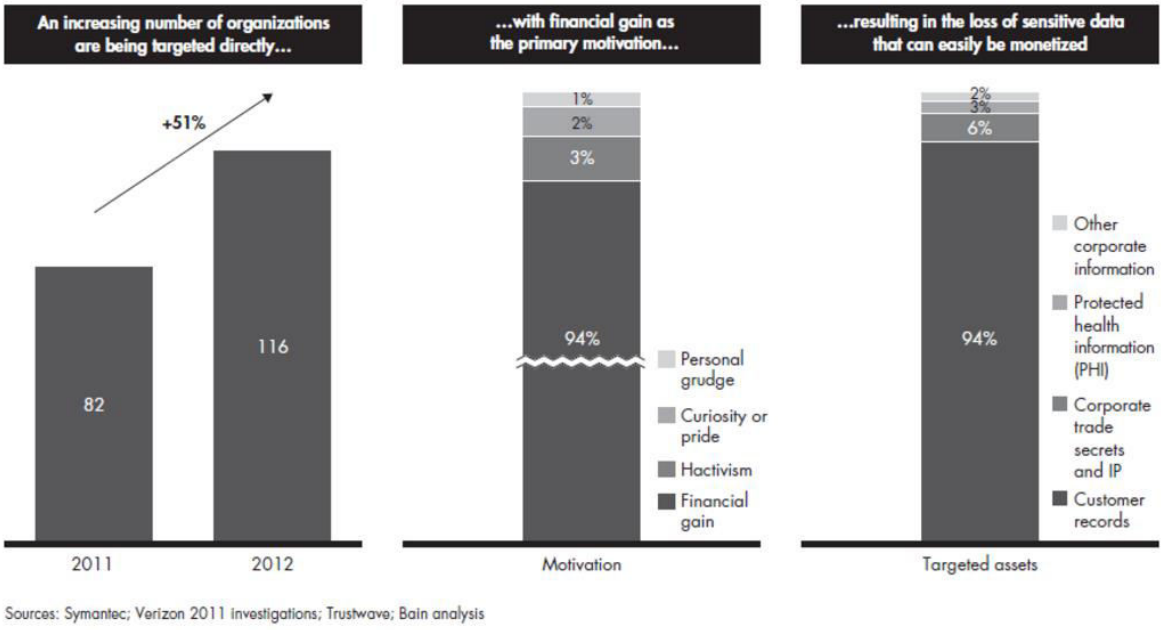


Figure 2 Hackers looked for financial gains

As an example, in October 2013, a hack attack on such a reputable company as Adobe Systems had caused a huge theft of data as hackers stole the identity and linked data of up to 38 million Adobe account holders. Not only that, the hack attack pilfered the source code that powers up such premier products from Adobe as Adobe Reader, Adobe Photoshop, and Adobe ColdFusion. Such a serious strategic threat leads to very serious consequences for any business organization that stores customers' private data. It is obvious that in an increasingly online world, most business organizations dealing directly with customers would be keeping this data with them. However, such a breach which hits on the sensitive privacy issues can lead to a tumbling stock price, huge sales losses and negative or even hostile press immediately following the news of the security breach. In the medium and long term, there could be serious legal consequences like lawsuits from business partners and customers, and long and lengthy investigations by Federal or State agencies. The breach of the source code of a software product is extremely worrisome for a software company. The hackers can find vulnerabilities in the code and exploit them to the extent that it can affect the operation and performance of these products on many digital platforms like PCs, tablets, and cell phones Similarly, in December 2013, a massive security breach was encountered by Target corporation. The hackers could pilfer debit and credit card data related to 40 million Target customers. This occurred over an entire 19-day period. target had 2,000 retail stores at that time and the POS systems at these outlets could have been the main source of this data breach. The malware employed by hackers had likely hacked through these outlets (Syed Ali, 2014).

Reaction required from Board of Directors

In response to such highly serious and strategically damaging security threats, it is imperative that the CEO and Board of Directors of all business organizations think about security in a new and strategic way. It should not be a low-level IT department task. It is a strategic matter and must be dealt with a cyber security strategy starting at the Board level. The absence of such a strategy can result in the complete annihilation of business. Literally, the life of a lively, throbbing organization can be just a few hacks away if a proper strategic level defense mechanism is not established. In the layman language, while you protect your hard assets by building a strong, protected and secure building, you need to protect your cyber and soft assets by building a cyber security system at a strategic level.

The paradox

Interestingly, cyber security was present in all organizations that faced the hack attacks. Most of the hacked companies belonged to such fields as banks, media, and technology. There were many universities and retail companies as well. Even security agencies were not spared. All these organizations are aware of the need to protect information and thus it came as shock to the world that of all the organizations that could have been targeted, such perceptively well-defended organizations got hacked (Syed Ali, 2014).

Unfortunately, senior board members and higher level management in most companies does not have the necessary understanding of cyber security related issues and their severe impact on the very existence of the business to be able to think about investment trade-offs and the possible risks involved. There has been some positive development as at least a few organizations are now considering cyber security as a strategic issue. In one company, the CEO directly liaises with senior executives responsible for security. Many companies are posting their CIOs in all business units thus enabling Senior Executives level strategic thinking. Some others are now reporting cyber security related issues directly to the risk committees of the Boards (James Kaplan, 2011).

Literature Review

Cyber threats as of 2016

The language being used by cyber security professionals is enough to instill fear in the mind of an organizational executive. The threats as they exist as of 2016 include but are not limited to machine-to-machine attacks, ghostware, two faced malware, headless worms, jailbreak, etc. the very names suggest the intensity of the virility these threats carry to an increasingly online world (as well as systems that are offline or closed but occasionally one of their peripheries connects to an online source) (Taylor, 2015).

Hackers have been launching high-profile cyber attacks which are increasingly growing in complexity on almost everything ranging from infrastructure related sites to devices linked with the medical field. There literally is an arms race going on between those who want to attack and

those who want to defend. The technologies and skills involved might be very similar. The venues where cyber-attacks take place then act battleground where the technologies employed by the two sides are tested. It is being mentioned by security experts that almost half a million cyber-attacks are taking place literally every minute in the cyberspace. The ones we hear about are the ones that succeed and are reported in the news. The overwhelming majority of these attacks simply fail due to adequate defense at sites and many which succeed on small businesses are never reported as hackers get away with blackmailing business owners and get paid to halt the attack (Taylor, 2015).

The ever-rising machine-to-machine attacks

In 2016, as per Gartner; a research company, there were approximately 6.8 billion connected devices in 2016 which were 30% or so more than how ma there were i 2015. This number is likely to grow to a whopping 20 billion by 2020. Thus, for every single human being on this planet, there would be between 2 and 3 connected devices. The emerging technology; the IoT (Internet of Things) would end up connecting many devices with each other. Thus, the opportunity and the expanse provided to hackers would increase many folds. In other words, the potential attack surface is increasing at an unprecedented pace. As per Derek Manky, the global security strategist for Fortinet, the playground available to the hackers has increased tremendously and all this is happening while the consumer related private information as well as vital corporate data is literally suspended in the middle. A lot of devices that are connected belong to consumers like their PCs, tablets or cellphones in which security is not the priority no. one, thus, the connection to these insecure devices could result in a higher level of cyber-attacks (Taylor, 2015).

The general attack trends and the most vulnerable devices

As more and more cloud computing is used by businesses all over the world, the more the mobile devices are used and the more the Internet of Things develops, the importance of security and prevention of cyber-attacks and disaster management after a successful attack would go sky high. In fact, most businesses already realize this importance even if they have not taken any concrete measures to guard themselves. Smartphones are at the forefront when it comes to cyber-attack potential. Cybercriminals are likely to target them simply because of their huge plentitude. Moreover, they can be attacked in a variety of ways, e.g. web browsing or malicious apps. These are referred to as 'drive-by' attacks as certain malicious websites 'fingerprint' them and when connected to the phone, they would 'read' their 'vulnerabilities.' Thankfully, at least Apple by its code review that it took makes its devices more secure as compared to others. It is thus able to block a lot of unwanted and potentially harmful apps before they can reach the device with the consumer. However, that still does not guarantee a 100% secure environment. Nasty codes in the form of headless worms have been targeting headless devices like smartphones and watches, and even medical devices. It is easy to imagine what kind of threat multiplication can occur when devices in the billions are connected. Using our imagination, by 2020, an attack surface of 20 billion devices could lead to a giant attack which could engulf say 15 million machines or more. This level of ‘device outage’ would be catastrophic, to say the least. (Taylor, 2015).

Cloud related cyber threats

The cloud computing and its infrastructure which includes VM or virtual machines have a strong likelihood of facing serious threats. Malware specially built to crack through their firewalls is being built. Increasing ‘Virtualization‘ and the spread of the private as well as the hybrid cloud is further enhancing the potential attack surface. The cloud also has connections with mobile apps and thus cyber criminals using portable devices would be able to attack the cloud from remote locations. This would allow them to target corporate servers and networks (Taylor, 2015).

Law Enforcement related hack attacks; ‘ghostware’ and ‘blastware’

Because of enhancement in the forensic capabilities of law enforcement agencies, hackers are likely to resort to ghostware. Ghostware is a term pointing to malware that would attack but then erase its tracks. This malware can penetrate networks, and steal data and then make it hard to track. the law enforcement is likely to have a hard time reacting to this type of threat. It shows that both the hackers and the defenders are going through major technological upgrades. Apart from using ghostware, hackers are resorting to the use of 'blastware' which annihilates a system when it interacts with it. Hackers try to use it on infrastructure websites and systems and such an attack ca have devastating consequences. It is therefore very important for business organizations to develop high profile response capabilities to such malware and these capabilities of any organization would be critical for its survival in the coming years (Taylor, 2015).

Two faced Malware

In the presence of multiple threats in the cyberspace, businesses test new software technologies in a 'sandbox.' It is a safe environment for testing software. once it passes this stage, it is then installed and run on main organizational systems. Hackers have tried to crack this technology too. They have developed a malicious software called 'two-faced malware' that creeps into the system as it appears harmless. Once inside, it shows its real face and morphs into a virulent malicious code (Taylor, 2015).

Defending against Cyber threats

Even though security breaches at renowned organizations have been making headlines for quite some time, the businesses, in general, are still showing inertia in moving fast o these challenges at a strategic level. Most hack attacks and security breaches have been related to pilfered data, DDoS (Distributed Denial of Service) which are very serious nature threats not just hampering the business operations of organizations but have potential of damaging companies beyond repair if the company ends up losing a good chunk of customers and gets boiled down in lawsuits and legal wrangling. The business in general, despite these existential levels of threats, seem quite unprepared to tackle this head-on and address these on a strategic level. This is highlighted by a 2014 survey conducted by Trustwave with 476 IT professionals who reported that most businesses do not have either any system or only a partial system which is capable of fully controlling and tracking extremely sensitive corporate data (Schiff, 2015).

As the first line of defense, the business organizations can take the following steps to start off and then further advance to a long-term strategy for cyber security:

Beware of disgruntled employees

Disgruntled or rogue employees especially those who have routine access to company data and might belong to IT department with admin control capability can cause serious data breaches from inside. The notorious Sony attack is now considered to be an insider attack rather than one initiated by North Korea. One step that can be taken to guard against this menace is to terminate all the privileged credentials accounts that are redundant and not in use or belong to departed employees. Moreover, the privileged credentials must be monitored very diligently so that no exploitation possibilities are left. It is extremely important to have the right type of protocols that log and track all activity of these privileged accounts. In the case of any harmful or malicious action, immediate alerts should be generated alerting the managers so they can react in the initial stages of the attack (Schiff, 2015).

Uninformed, laid back and careless employees

Ray Potter, CEO of SafeLogic states that a careless or uninformed employee who tends leave his unlocked phone in a cab is as dangerous as a mole who leaks valuable information to competitors. Any employee who has not been trained on the best practices regarding security; the one who would visit suspicious websites, opens emails with malicious content in attachments or clicks on suspicious links is a threat to the security environment of the business. The employees would require proper security related training and best practices explained to them. This must not be left to their own ability to know. Training sessions are required that teach them how to use passwords that are hard to hack. They should be able to defend against key loggers and phishing agents. Of course, they need to be provided with ongoing tech support too. Employees should learn to use separate passwords for each site and change them periodically. Employees should be asked to use two-factor or multifactor security levels (e.g. RFID cards, retina scanners, One Time Passwords (OTPs), fingerprint scanning, etc. to ensure more protection.) and the IT department can use encryption to make their communications more secure (Schiff, 2015).

Use of mobile devices

Whenever employees use their own mobile devices to access company data and communicate, they might sometimes not be very careful about the frequent password change. as per a British Telecom study based in the US, close to 68% of global companies had suffered breaches thus mobile devices related breaches during a 12-month period in 2014/2015. The 'Bring your own Device' practice is increasing in organizations and so is the risk associated with these devices. If an app ends up installing a malware or a Trojan, the company's network even though it might be behind a VPN or a secure firewall can still get affected. The company needs to have a well-defined BYOD policy which should be communicated to all employees. This way, both the company, and employees would have better control on their own devices. in case, any of the mobile devices is stolen, the company would be able to reduce risk by minizine or eliminating data loss. Containerization based privacy protection while at the same time corporate data protection can be made possible by implementing sophisticated and advanced mobile security systems. Applications related to company usage and the data should be separated. This achieves containerization. which in turn would ensure encryption and control of IT department on corporate data. This would include all configuration and credentials as well. This provides literally an impeccable defense. Hybrid or private clouds could be used to further lower the risks

from BYOD practices. These types of clouds have all the advantages of a public cloud but with much enhanced, secure and privacy assured environment. in these, the encryption keys are kept on-site regardless of which device the data gets stored (Schiff, 2015).

Usage of Cloud computing or data storage

The crypto-gold standard or AES 256-bit encryption is the best defense against cloud-based threats of data loss or hacks. The business retains the encryption key and even on a public cloud, the data would not be accessed by an unauthorized party. The data breaches in 2014 occurred mainly because most of the companies involved had not implemented such an encryption system (Schiff, 2015).

Device firmware based threat (if unpatched or unattachable)

Many servers, routers, or printer employ firmware that might not have been patched for vulnerabilities or it might not be patchable. Thus, a threat exists as these vulnerabilities could be exploited by hackers to pilfer data. Some companies are still using Windows Server 2003. It is no longer getting security patches from Microsoft and nor any security updates. as there are at least 10 million of these still being used, all those companies using these are vulnerable to hack attack. Organization must start a patch management initiative. this would keep all devices updated always. 'Venerability management' technology needs to be deployed across the organization. This checks the status of all devices. However, a better policy would be simply to take out the equipment that does not get patched within a certain time interval.(Schiff, 2015).

Employment of 3rd party specialized technology companies

Outsourced vendors must be brought in service for specialized technology related applications. Most franchise providing restaurants across the United States use outsourcing for system maintenance and support of their POS systems to 3rd party support companies. These companies must use tools for remote access and while doing so might not be able to follow all necessary security protocols especially in the case of passwords used for remote connections to a variety of clients. They could end up using the same default password for all clients thus causing a vulnerability if a hacker can get his hands on that password. The case of Target is a case i point. The hack was done using the 3rd party service provider's credentials as they had been pilfered. As per 2015 a study, 76% of the breaches that occurred were routed through 3rd party access to corporate data. This does not mean that those third parties had malintent. They simply did not have the necessary protocols in place or ended up not following best security practices. Most organizations do not vet their vendors properly for such practices. It is, for this reason, this threat becomes serious. Normally, a breach progresses by attacking a low-level PC o the network and can upgrade itself to higher levels as it jumps through the various security levels and privileges. Businesses normally have very good security built around their main servers but it is the low-level PCs that are not protected and the breach starts exactly there. For this reason, all organizations need to ask their service providers to implement best practices such as multi-factor authentication. they should establish separate credentials for each user and must be able to log the entire trail of the audit process. As soon as the service is over, their privileges must be removed. Any further attempts to log in should generate red alerts. .(Schiff, 2015).

General approach to ensure data security

It is a general realization among companies that data breaches would likely occur if protocols are not in place. a risk assessment must be conducted at a professional level to ascertain data locations throughout the organizations and evaluate the security mechanisms built around it. In case a data breach occurs, a well in place 'disaster management system' ensuring continuity of business should take over. Which person from legal, IT and PR departments would do what should be included in this plan in writing and communicated to the concerned persons (Schiff, 2015).

Executive involvement in matters of cyber security

Most business executives now realize that cyber security being a strategic issue just cannot be left to the IT department. Well-built cyber security can even provide a competitive advantage as it can lead to a development of trust in partners and clients. Companies can beat their competitors in cyber security related issues. while business executives do realize this strategic importance, most of them are still slow in implementing proper policies and procedures that would give their organizations this competitive edge. A survey conducted by Deloitte has highlighted four ways in which executives can engage with cyber security issues to their advantage (Niemantsverdriet, 2016).

Heat Mapping Sessions between Executives and experts

One excuse that was found to be widespread among the executive responses was about the shortage of funds allocated to cyber security. However, it can be a misjudgment when one tries to put a quantity to risk without proper evaluation. Experts recommend Sessions that map heat i.e. identify the intensity of risk by conducting a meeting with experts in risk and threat intelligence management. Once the most valuable data sets have been identified and associated risk assessed, only then, a proper evaluation of risk and its heat would be ascertained which would allow the company to strategically allocate funds accordingly. The Deloitte executives first determined their valuable data (the crown jewels; as they called it) and related it to the company to arrive at a final evaluation. A model was then prepared and the variables in the model could be tweaked to see if more needs to be spent on prevention techniques or more on monitoring and disaster management planning. How best to avoid risk can thus be determined with this technique. Once this is ascertained, executives have a figure which they can discuss with top business leaders at the strategic level. (Niemantsverdriet, 2016).

KPIs (Key Performance Indicators)

When the business executives discuss the cyber security-related risk management issues with company leadership, the most serious risks must be highlighted clearly. The risk indicators that point to these risks must also be mentioned to make them get the full picture. Moreover, whatever methods that need to be devised or employed need to be explained as well. In managerial terms, KPIs offer a standard measure of performance and these along with other metrics can be used to make a good presentation. This would greatly facilitate the leadership in

their decision making regarding resource allocation and determining its priority. Data breach related laws and regulations would emphasize these KPIs as well (Niemantsverdriet, 2016).

Cyber security threat incident simulation

Just like every fire related program requires a drill to be conducted at the concerned location, similarly, a simulation of a cyber risk threat incident would prove to be a good drill. This would enable to the executives to see what sort of damage might be done to their systems. The various weak and vulnerable spots especially the blind spots would become visible. Moreover, executive and employee alertness and a quick response would also be evaluated. Many other challenges that the firm might face during an actual attack would also become evident. The employees would come to an understanding that cyber-attack is not just an IT department related matter and that a combined and cohesive response is required on part of the CEO, CIO, the legal advisor, and the marketing and communications departments alike. The firm gets to achieve a tailored response to every possible conceivable threat (Niemantsverdriet, 2016).

Examine new technologies related security implications

This is by far the most important of all aspects. Many new technologies are being incorporated into the business world each day. All these technologies offer plenty of opportunities and open new horizons. Just like pushing the edge beyond frontiers would involve the unexpected and the unknown, these technologies could involve the risk of unknown and the unexpected. Security is considered as mutually exclusive to innovation. However, if the security aspect has been well-taken care off, the innovation could even be accelerated with confidence. all technological innovations applied by the company or explored into must be assessed and examined based on security risks. this process should be a part of the company's announced strategy (Niemantsverdriet, 2016).

The CIO, of course, needs to be a bit more active and responsible for this issue. He must be able to assume a strategic role and play it in such a way that the other executives feel the need for cyber security and feel responsible too. Cybersecurity needs to be a part of the main strategy of any business organization. There might be many ways to accomplish it but its importance must be understood by all company executives starting from the CEO. This way, the firm can ensure a competitive advantage that would help steer the business in the volatile and often insecure business world (Niemantsverdriet, 2016).

MacAfee Labs Report on cyber security for 2017-2020

MacAfee Labs; one of the leading cyber security experts and researchers in threat, and threat intelligence and the thought leadership required for cyber security. They have compiled data from prominent threat vector files, the internet, emails, and networks and have come up with critical analysis, real-time threat intelligence, to reduce cyber risks and build upon cyber security in a 2017 related report. The report dwells on big threats and how to deal with them early on. They had taken input from Intel security based thought leaders and discussed with them the hardest pressed security threats. These were then grouped and presented as 6 large prominent groups. Apart from that, they concentrated on threats related to cloud computing along with 11 experts from Intel security. The team assessed the cloud-based threats that would emerge in

2017-2020 and how best the legal and industrial response could be put forward against them. The report opens down the possible threats and breaches mention how geopolitics would affect these, and how legal and regulatory actions would affect the business environment based on these. The report separately dwells on the possible CSV's (Cloud Service Vendors) and security companies' responses. The last topic touched upon by this report deals with IoT related possible threats. Cooperation from 100 Intel security thought leaders was sought who helped predicted breaches and threats, legal issues and security vendors' reactions to these. (McAfee Labs:2017 Threats Predictions, 2016).

The report is in 2 parts and the later part specifically targets 2017 and the threats that would appear throughout the year. It covers vulnerabilities of various kinds, ransomware, threat intelligence as a part of defense mechanism, and attacks related to portable devices.

Some salient points include:

- Ransomware threats would likely increase in 2017 peaking at the midyear and then recede
- Major progress would be made in the field of sharing threat intelligence
- Cyber security companies and actual physical security companies are likely to come closer
- Hacking activists (Hacktivists) would make hits at consumer data and infringe upon privacy leading to legal and industrial responses
- Law Enforcement agencies and security vendors would up co-operation to track down cyber criminals
- Vulnerabilities in most common and popular apps would reduce
- There would be a continuous rise in 'fakes'. These are the fake advertisements, security-related warnings, and reviews. This could lead to a loss of trust on the Internet. Socially engineered infringes would be handled via machine learning (McAfee Labs:2017 Threats Predictions, 2016).

Hardest to resolve security threats

There are unending challenges being faced by digital information security. Mere incremental changes in threats must be responded to daily through security updates and patches. Every time a new software comes out, it also enables many random vulnerabilities. As soon as the new threats are discovered, urgent fixes or notifications are immediately sent to consumers. However, these responses cannot handle to threats on a 'big picture' scale. Very basic and thorough research needs to be initiated and altogether a new class of products needs to be developed which would require a great deal of time and effort. The focus needs to be sustained and cooperation between professionals from multiple industries is required to work as a cohesive team to achieve the desired results. Because of increasing use of cloud computing, the boundary between internal and external networks would start disappearing. Moreover, more and more new devices are being introduced in the market leading to a higher level of challenges as traditional methods of protection do not seem to work (McAfee Labs:2017 Threats Predictions, 2016).

Effectiveness of threat-related defense

There is a continuous dance going on between attackers and defense experts. Figure 4 illustrates how a threat's defense's effectiveness charts out over time. New technique's effectiveness goes up as it is developed as it is deployed across platforms, and combines with other defenses, but as the cybercriminals start to respond to it by developing countermeasures, it starts to go down. The main challenge faced by the security industry is how to increase this lifecycle of the defense technique or product. There is a requirement to move to the upper and right portion of the curve all the way to the dotted red line.

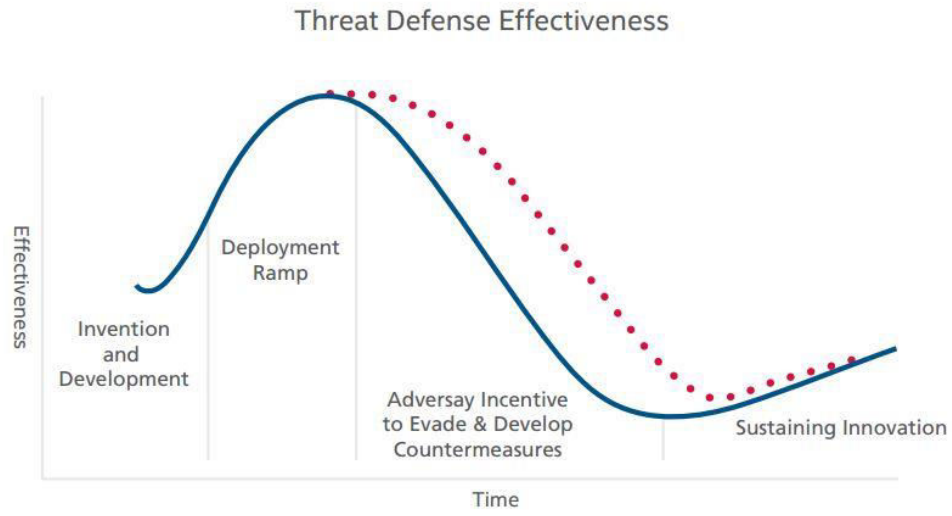


Figure 4 Threat level PLC Source: (McAfee Labs:2017 Threats Predictions, 2016)

The lifecycles can be increased through a range of activities which can include:

- The asymmetry related to digital information between the hackers and the security vendors needs to be minimized.
- The hacks and attacks could be made more expensive to execute and the level of profit they entail can be reduced
- The security mechanism can be made more visible warding off threats
- Tools and credentials that can be exploited need to be identified
- Data spread at various independent non-central locations needs to be protected.
- Without the use of agents, detection and protection should be made possible (McAfee Labs:2017 Threats Predictions, 2016).

The threat defense effectiveness is the key to staying well ahead of hackers and attackers. The most important prerequisite to this goal is multiple industry collaboration to solve the 'big picture' threats that are hard to address using simple patches and updates. Industries need to share relevant information and such resources as predictive analytics can be utilized along with making

security more visible and increasing protection of decentralized data storage to increase the PLC of defense mechanisms (McAfee Labs:2017 Threats Predictions, 2016).

Cloud computing related threats, regulatory and vendor response

BPO (Business Process Outsourcing) outsources work but the risks stay with the source company. CSVs are getting popular with time because of the rather economical software power they provide to users who prefer not to invest heavily in software and hardware infrastructure. Public and hybrid clouds are now storing or accessing a lot of sensitive data and processes that are business critical. The Hacktivists are likely to respond to this shift and would look for vulnerabilities. By 2020, the trust in the cloud computing would reach greater heights and more and more data would interact with it, leading to a higher level of interest among the attackers. CSVs would continuously update their security protocols. Ultimately, there is a high likelihood that almost all businesses would start to rely on the cloud computing platforms (McAfee Labs:2017 Threats Predictions, 2016). Branch networks are even more vulnerable to threats. In 2015, 30% of the attacks were targeted sat branch networks (Threat Defense for Branch Networks, 2016).

Crown Jewels would be retained by companies

Despite the heavy reliance of cloud computing, the crown jewels of the business would stay with the companies concerned. Interestingly, the public clouds are more secure than many private cloud because of their reliance on stronger security measures and have stronger security professionals supporting them. Companies would have to figure out exactly what goes up in the cloud and what stays back with them with proper security protocols implemented. Many organizations that are reluctant to move to the cloud today should know that they are already on it. Many of their employees use such services as Google drive, Dropbox, OneDrive, iClouds, etc. and these are all cloud based platforms. for those who have moved to the cloud already, there is a drop in the level of priority for security concerns. CSVs might provide different levels of security in the future based on service agreements. In the next 4 years, the cloud is likely to become a lot more event driven rather than just being a server. There would be short lifespans associated with containers as compared to VM (Virtual machines) and would function on data and code that would eventually disappear. This would result in tremendous efficiency and speed but could end up generating more security related threats (McAfee Labs:2017 Threats Predictions, 2016).As far as what constitutes the crown jewels, company board deliberations and decisions, merger and acquisition strategies and plans, product, service or business process design, other trade secrets are some of the crown jewels that the companies would like to protect and retain with themselves beside the Intellectual property (Lovejoy, 2016).

Weak authentication schemes

Weak authentication schemes would continue to plague the business world even for cloud computing. Most attacks would attempt to pilfer credentials. Both passwords and persons creating them would be the weakest link. Cloud platforms do not use any better authentication techniques either. Patient thieves who would dig into social media would garner passwords, personal info, and cloud credentials to achieve their aims. Scams and fake recruitments,

phishing, would continue to rise. The inclination to use the same password on all platforms would be a main source of vulnerability. Brutal attacks on administrative account credentials would likely go up. Companies would need to be cautious about suspicious administrator activity as well (McAfee Labs:2017 Threats Predictions, 2016). Online banking and payment systems these days are highly insecure as well. Most of the countermeasures used by such institutions have serious vulnerabilities to attack. The real danger comes from Trojans which can penetrate through even two-factor authentication systems. Some experts propose OTP (One-Time password) schemes for high profile accounts in banking and payment systems (Oscar Delgado1, 2008).

Eastwest and Northsouth attack vectors

Traditionally most attacks used to follow Northsouth attack vectors. this involved going up and down the stack to up their privileges and exploit any existing vulnerability with the aim of getting access to some specialized application. Eastwest attacks move horizontally from one container to another, across cloud platforms and can even jump through different organizations. Attackers would broaden attack surface using the cloud and would try to attack many organizations at the same time or will try to implant malware into their security systems for exploitation later (McAfee Labs:2017 Threats Predictions, 2016). Eastwest threat visibility ability requires the organizations to be able to see the threats that have already entered their systems either originating from outside or inside. It is of paramount importance to detect these threats whether they originate from zero-day exploits or phishing emails. Various networking tools can be employed to detect these. firewalls, flows, and bump-in-wire technology is prominent among these technologies (Mullican, 2015).

Service Layers Gaps

Service layers' coverage gaps and settings without any consistency would prove to most vulnerable. Organizations are not yet fully cognizant on what responsibilities they should have and what to expect from Cloud Service providers. This leads to the potential vulnerabilities. there is nothing that the technology can do here. It is a misinterpretation of the process. Without any false assumptions, organization need to jot down the sharing mechanism in relation to responsibilities with the vendor. Both organizations and providers need to agree on terminology first as that might be the cause of confusion as there is a plentitude of security protocols in the business environment of today and they have different standards that they adhere to. Such failures of process controls would offer the great potential of attacks (McAfee Labs:2017 Threats Predictions, 2016).

Visibility and control issues

As cloud moves data around, it provides powerful features but complicates security and privacy. Some employees get paid to share their passwords. Organizations might attempt to keep data within national borders, or within a safe company, environment or avoid a certain type of cloud environments. The ability to maneuver within the cloud is normally not as much as the organization would want. Behavioral analytics patterns related to consensual usage of credentials can be an asset (McAfee Labs:2017 Threats Predictions, 2016). A new European survey conducted in the last quarter of 2016 studied the opportunities and threats related to IoT.

Research showed awareness on part of moist company executives about the usefulness of IoT but did not seem to have an idea of how they would be protecting all those devices connected to the internet. The study involved 201 senior IT decision makers in the United Kingdom, Austria, Switzerland and Germany. It was found out that an average business would probably be handling up to 7000 devices in the next one and half year. The smaller businesses were no exception. They would be connected to hundreds of devices as well. The healthcare related institutions and businesses seemed to be lagging as far as any vision of IoT is concerned. 65% of the respondents had either none or very little idea of how they would go about security issues in this highly connected IoT world. Interestingly, most IoT systems are open sourced so there would be a lack of standardization leading to more variants in terms of threats (Alvarez, 2016).

Hackers would try to avail speed, anonymity, and scale by resorting to cloud

Once an attacker starts using the cloud resources, it could take weeks or even months to track the pilferage and shut it down. attackers can potentially launch brute-force attacks, and Northsouth and Eastwest attacks via many vectors. they can even resort to 'agile' form of attacks which evade detection by rotating between various sites and crossing borders. This could lead to warehousing of pilfered data by these hackers for huge financial gain. They would change IP addresses, accounts, locations, containers, and others to hide their identities. this scenario is not likely to undergo any major change in the next 4 years (McAfee Labs:2017 Threats Predictions, 2016).

Denial of Service for ransom attacks

These would continue to increase for cloud-based organizations and cloud service providers as well. An attack on the provider would temporarily cripple multiple clients. However, CSVs can hinder such attacks if they are traditional due to tighter security. However, in case a vulnerability is found, they would have to face these new forms of attacks on any of the multiple points between the cloud and the organization. DNS Servers, the Internet connection itself, and a variety of technological infrastructure. The attackers would be able to launch an attack on exclusively on an organization on the cloud for ransom without disrupting the entire cloud (McAfee Labs:2017 Threats Predictions, 2016). Prevention against DDoS attacks normally employ firewalls as first line of defense. They off-load malicious codes to a certain cloud service provider who has the mechanism required to counter them. Multiple layers of threat reduction are the best way to handle DDoS attacks (Promedia, 2015).

Global Threat Perception and Attitude Measurements for 2017

Tenable Network surveyed 504 IT security practitioners across the globe and assessed their perceptions and attitudes towards cyber threats. Their Assurance Report Card for Global cyber security reflects an overall reduction in the perception related to global security against risks. As far as Risk assessment is concerned, the score was 61%. Security Assurance index stood at 79%. The overall average was 70% which showed a 6% decline as compared to 2016. This means that there is more uncertainty in perceptions for 2017 as compared to 2016 for overall security related issues.

Emerging Technologies are the main source of uncertainty increase

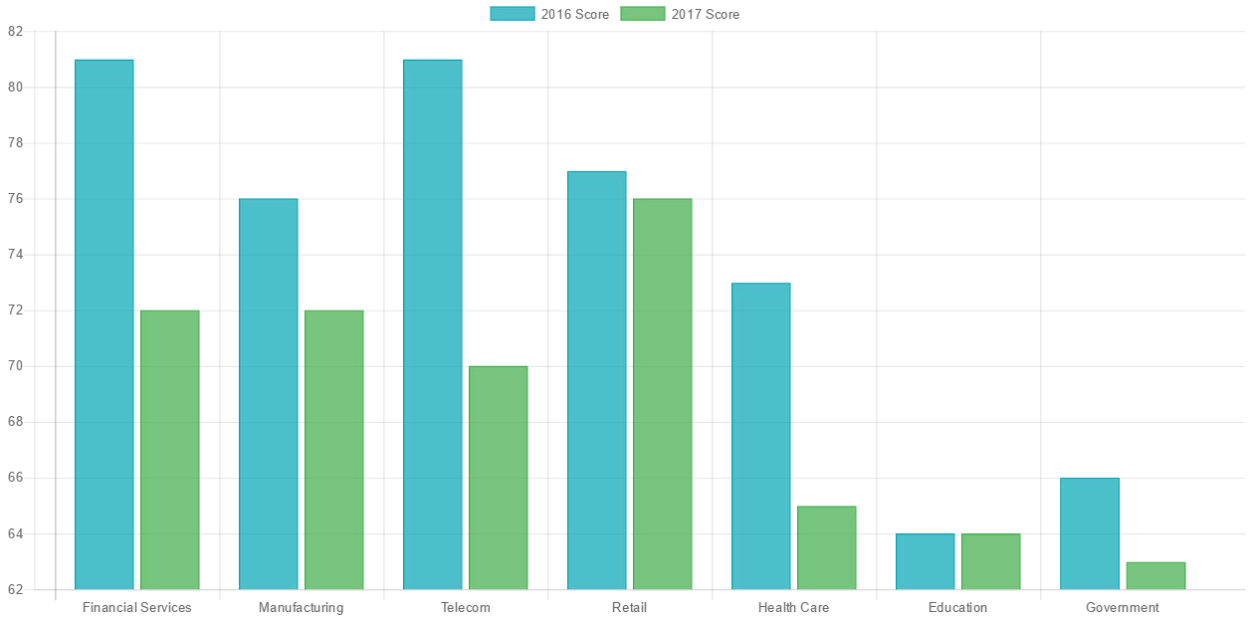
The Cloud Services and portable devices were perceived by respondents to be the most insecure. Even containerization stood at 52%, DevOps at 57% and portable devices at 57% in terms of Risk Assessment. Apparently, containerization and DevOps increase the decentralization in an organization and the IT security people do not feel that they would be able to have full control throughout the organization.

Threats appear Overwhelming to IT professionals

While Emerging technologies offer new horizons to explore and benefit from, the advancement made by hackers in improving attack mechanisms offers a nightmare scenario. regardless of the size of investment made in security-related issues, it appears that organizations would remain vulnerable due to gaps in security because of technological complexity. Therefore, it is not sufficient on part of business organizations to be aware of the threats alone. They need to seriously work on assessing their strengths and weaknesses related to cyber security. Comparing the 2016 and 2017 results for Risk Assessment country wise in terms of Security Assurance show India at 84%, the US at 78%, Germany at 62%, had a confidence level of only 48%.

Sector wise Industry perceptions

Industry wise Confidence scores were as follows: Retail Industry lost 1 point as compared to 2016 while Telecommunication Industry and the Financial Services Industry showed the highest drop in confidence. As shown in Figure 5 below: (Global Cybersecurity 2017 Assurance Report Card, 2016).



	Retail	Financial Services	Manufacturing	Telecom	Health Care	Education	Government
Risk Assessment	66%	59%	59%	60%	54%	64%	59%
Security Assurance	86%	85%	86%	81%	76%	63%	67%
Overall Score	76%	72%	72%	70%	65%	64%	63%
Overall Grade	C	C-	C-	C-	D	D	D
2016 Grade	C+	B-	C	B-	C	D	D

Figure 1Confidence level by Industry 2017 Source: (Global Cybersecurity 2017 Assurance Report Card, 2016)

Cybersecurity Market Report Q4 2016

Cybersecurity Ventures prepare Cybersecurity Market report every 3 months. Their last quarter report published for 2016 has analyzed the venture capital, market size, cyber threats, etc. based on industry forecast from many professionals. (Cybersecurity Market Report, 2016).

Market size

- As per this report, approximately 1 trillion dollars are likely to be spent on cybersecurity related issues worldwide in the 2017-2021 period. The IT professionals are having a hard time keeping pace with the dramatic upsurge in ransomware and cybercrime activities and as the cyber threats are increasingly shifting focus from PCs and laptops to portable devices. The hacker-for-hire phenomenon is on the rise and will continue rising and more and more unprotected devices would get on the IoT (Cybersecurity Market Report, 2016).
- The report forecasts a 12-15% rise year-on-year as far as growth of cyber security industry is concerned all the way to 2021. Some other reports in the IT industry have projected an 8-10% growth on a similar basis. The lower figure might be since many

large corporations did not publicly announce the security breaches they had had and are a bit secretive about the size of their cyber security related allocations in the budgets. The reasons could be protecting their reputation from damage or on the other hand, they do not want to irritate the hackers who attacked them (Cybersecurity Market Report, 2016).

- At least some of the corporations would disclose their true budgets. J.P. Morgan Chase & Co has allocated a $500 million for the next period which is twice that of what was allocated in the last period. Bank of America wants to put no bounds on cyber security as they attach highest possible importance to it. Even the US government would be spending 35% more than the $14 billion they spent in 2016 allocating a total of $19 billion. Simple incremental increases would hardly be witnessed. Most of the businesses especially large corporations are likely to double their cyber security related budgets in 2017 (Global Cybersecurity 2017 Assurance Report Card, 2016)
- The new approach to cyber security does not simply revolve around the IT infrastructure consisting of PCs, laptops, portable devices, networks, servers, interfaces and data centers, etc. but would broaden itself to include non-IT related environments and platforms. These would include security related to automobiles, IoT, aviation, IIoT (industrial IoT), etc. These would form part and parcel of the cyber security market segments (Cybersecurity Market Report, 2016).
- Technology has parallels in the cottage industry as there are myriads of Value-added Resellers (VARs), System Integrators and IT solution and services providers. They cumulatively are responsible for creating the security shield or envelope around the IT infrastructure. Most of these companies are not large so they do not report their cybersecurity resources that they allocate to budgets. Even, the renowned security companies with brand distinction have not yet mechanisms or divisions available to report revenues thus confounding the task of market size forecasting. With passing time, many Attorneys, legal advisors, and CPAs etc. are entering the field of cyber security because of the recent data breaches worldwide. This is an attractive field for them as it promises good revenues (Cybersecurity Market Report, 2016).
- A look at the consumer side of the story would point to spending on cyber security that is hard to quantify. They are not only spending on anti-virus, and anti-malware software etc. they are also spending to get repair services for virus or malware removal, installation services for protection apps and packages, data recovery services in case of a data breach, and on training or user education. thus, the cyber security market is far larger than just the part associated anti-virus and anti-malware packages and apps. Both time and money is being spent by the consumer on cybersecurity related issues (Cybersecurity Market Report, 2016).
- The total cost of the global annual cybercrime related costs is likely to cross the #6 trillion mark by 2021. These unintended costs would be linked with high profile data breaches, financial theft, productivity loss, IP theft, personal/financial data theft, fraudulent activities, financial embezzlement, business-as-usual disruption cost, retrieval of hacked data and its restoration costs, forensics, and most of all serious harm to reputation in which case it is hard to assign a number value.

Data Analysis

The data presented in the literature review shows clearly that while executives are aware of the dangers of cyber threats and are also willing to tackle these issues, the strategic effort required is still lacking as cyber security is not just an IT department related issue. Corporations and other organizations need realize the threat at the Board or Strategic level and consider cyber threats to be 'existential threats and allocate resources accordingly against it. The data also shows that malware, two faced malware, Trojans, ghostware, blastware ransomware, etc. would increase tremendously because of hacker skills getting better and because of the rising use of portable devices and cloud computing. The cloud especially needs to be singled out for extra precaution. Companies would continue to spend more and allocate higher than ever budgets in 2017 for cyber security however some corporations would be reluctant to disclose their true budgets fearing reputation damage or trying to avoid irritating the hackers. The Risk assessment reports indicate that the Company or business confidence in cyber security would decline in 2017 and they would remain skeptical, however, this would not prevent them in allocating substantial amounts to cyber protection. The cyber security costs would touch $6 billion per year in terms of damage and the investment in protection would rise to as high as $1 trillion in the 2017-2021 period.

Discussion

The rapid development of technology opens new horizons and expands the frontiers of knowledge further outwards. While this provides businesses and consumers with countless opportunities to avail these new technologies, it gives way to many new and hitherto unknown cyber threats which would traumatize the cyber world and businesses and consumers alike as the hacker technologies would also advance with time. The element of surprise is always with the hacker. They attack at a place and timing of their choosing. Therefore, besides designing and combatting with remedial cyber protection, the best practice would emphasize on cyber threat prevention by improving credentials and protocols and using multiple factor authentication. Both Northsouth and east-west attacks would be common so the organizations would have to worry about all connected devices like IoT and portable devices besides their servers, networks and PCs and laptops. Companies would spend more on cyber security in 2017 however still, the cybersecurity-related incidents would still cause significantly high damage both financially and reputation wise as well.

Conclusions/Recommendations

The most important conclusion from the literature review and the discussion above is that cyber threats are a strategic challenge for any organization, therefore, the businesses need to raise its importance to the strategic level and allocate resources and personnel accordingly. In no case, should the task be left to the IT department only? Teams consisting of personnel from Finance, operations, Sales and marketing, IT, and other functional departments should get together and devise a cyber security strategy together and then make sure that each person is aware of the cybersecurity policy. Each point in the organization where the cyber-attack can take place should

be protected. As far as threats are concerned, they would continue to increase in 2017 and the damage they inflict upon businesses in terms financial and reputational loss would increase further. However, so would the investment in cyber protection. The 'trust' in cyber security would go down in 2017 because of emerging technologies exposing the systems to new threats and the fast adaptation of emerging technologies that is taking place. Regulation would continue to fall behind innovation on one hand and cyber threat progression. At least $1 trillion dollars would be spent on cybersecurity in 2017.

Critical evaluation

The research presented covers all major cybersecurity threats to businesses and highlights the importance organizations attach to them. The paper strongly recommends that the businesses regard the cyber threat as an 'existential; threat as a major attack might simply ruin the entire business by causing huge losses and reputation damage. Therefore, strategic level threat perception and cyber security related policy making are required. The entire business process needs to be designed to minimize this threat while keeping consumer expectations a top priority. The security mechanism should not appear as overwhelming to the consumer but must still be taking care of all major threats. The research presented includes data on cyber-attack related costs on businesses in the 2017 to 2021 period and estimates the amount of money that would be spent on cybersecurity in 2017 and beyond.

Areas for further research

A lot of research on cloud computing-related threats is included in this paper however, this is one area which deserves a lot more attention to detail. There would be an exponential rise in the usage of cloud in the next 5 years and thus a dramatic rise in threats related to vulnerabilities in the cloud is also imminent. This area requires more research which would specifically concentrate on threats related to cloud computing related cyber security issues. The area of IoT on a similar pattern needs to be considered in more detail as it would result in a myriad of devices connected to each other. Thus, both The Cloud computing platforms and IoT which are going to be quite popular in the future require a lot of additional research in regards to their potential for cyber threat attraction.

References

Alvarez, D. (2016). European Survey Finds That 65% of Enterprises Lack Visibility and Control of IoT Devices on Their Network. *IT Security Guru*.

(2016). *Cybersecurity Market Report.* Cybersecurity Ventures.

(2016). *Global Cybersecurity 2017 Assurance Report Card.* Tenable Network Security.

James Kaplan, S. S. (2011). Meeting the cyber security challenge. *Mckinsey and Company*.

Lovejoy, K. (2016). Protecting Crown Jewels in the Digital Age. *IBM on Wired.com*.

(2016). *McAfee Labs:2017 Threats Predictions.* McAfee Labs: and Intel Security.

Mullican, T. (2015). East-West Visibility: Seeing the Peripheral Threats. *OPTIV*.

Niemantsverdriet, J. (2016). Cyber security: essential part of modern business. *Deloitte*.

Oscar Delgado1, A. F.-S. (2008). *Analysis of new threats to online banking authentication schemes.* ACTAS DE LA X RECSI, SALAMANCA.

Promedia. (2015). Closing the Gap in Network Security: The Biggest Threats of 2015. *Promedia*.

Schiff, J. L. (2015). 6 Biggest Business Security Risks and How You Can Fight Back. *CIO*.

Syed Ali, V. P. (2014). Why Cybersecurity is a Strategic Issue. *Bain and Company*.

Taylor, H. (2015). Biggest cyber security threats in 2016. *CNBC*.

Threat Defense for Branch Networks. (2016). *Lancope*.