ABC072090865

*Economic impact of Cybersecurity in Australian Banks*

**Introduction**

Today, with advent of new technologies, the Information Technology (IT) infrastructure of several organizations are prone to the risk of cyber-attacks around the world. It is noticed that cybercrime remains one of the major threats to the national interests and prosperity. A given nation's wealth and use of technology such as online banking, social media, and government services are turning out to be attractive targets for the organized criminal syndicates (Brown, 2015).

For lucrative financial gains, they will be targeting banking organizations or any other financial institutions by generating a cyber-threat to them. Ransom ware is one of the recent examples that distorted the functioning and operations of majority of the organizations around the world. As per one of the research reports, more than 82% of the risk management executives of major banking institutions find emerging risks in the cybercrime (Barton, Smith, & Weaver, 2010).

The attacks have turned more sophisticated and the IT team of the organization is unable to detect such attacks in the institution. Despite security controls and measures taken by the organization to prevent cybercrime, they are prone to such attacks during any given time. With increasing digitalization and the banking sector expanding around the world, there is a need of an intelligence-based approach to Cybersecurity (Brown, 2015).

It is also important to spread awareness about Cybersecurity so that appropriate measures can be taken in this direction. There are still gaps found in investing into Cybersecurity solutions among the organizations; as per one of the Banking Reports of 2016, more than 75% of the total banks did not deploy appropriate measures to overcome the challenges of Cybersecurity (Brown, 2015).

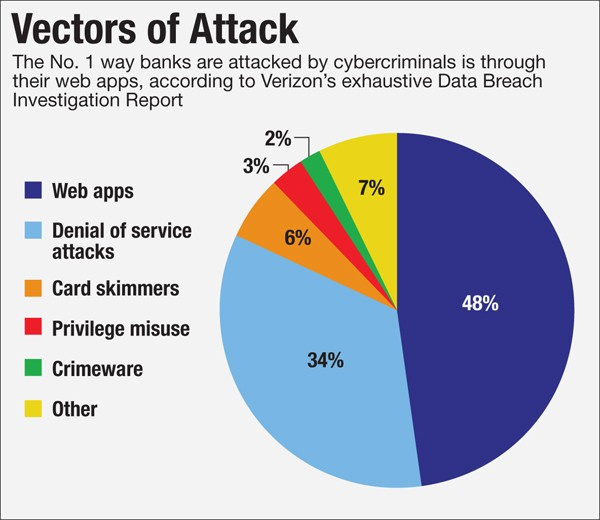
This report will thereby discuss the case scenario of Australian banks and will determine the economic impacts of Cybersecurity in them. It will first identify the risk factors, then determine the economic impacts, and finally, provide necessary recommendations to solve this problem. Only then they will be able to solve the problem of Cybersecurity in a given scenario.

**Project Objective**

Cybersecurity should be viewed as a combination of defense, resilience, and assurance. It is observed that the banking systems are facing one of the biggest threats in their daily operations. It will be difficult for them to recover if they get impacted with any of the cyber-attack on their IT system (Barton, Smith, & Weaver, 2010).

The malicious attack will not only compromise the users' data but will steal financial information, financial data, and might even transfer the funds to other unknown accounts. The attackers will leave the bank answerless in such situations. The banks are today moving toward mobile platforms for streamlining the banking and payment applications; the cyber-criminals are more interested in attacking such mobile banking services of the banks (Cachin, Keidar, & Shraer, 2009).

The mobile banking system allows the attackers to intercept banking sessions on the victim's mobile, which will further allow stealing the information of the user. Once the information is compromised, it becomes easy for the malicious user to transact on the given bank account (Casey, 2011). There are similar other vectors of attack through which banking transactions will be impacted with Cybercrime as shown below:

The Chief Executive Officer of Commonwealth Bank of Australia already stated that Cybersecurity is one of the greatest challenging issues and is also a matter of national importance. Hence, the government along with the IT team needs to first identify the source of major threats of Cybersecurity (Cachin, Keidar, & Shraer, 2009). They can thereby understand the level of potential threats and accordingly provide IT solutions to the banks.

It will help in overcoming the challenges associated with Cybersecurity and will also protect the information of all the customers of a given bank. The objective of this report is to determine the research questions pertaining to identification of research gaps relevant to Cybersecurity in the banking system. It is important to fulfill these gaps so that the banks can protect the data of the customers and subsequently prevent the negative impacts of cyber-attacks on the entire banking system.

**Project Scope**

The scope of this project will include determining the economic impacts of Cybersecurity on the banks when they are impacted with cyber-attacks. It is necessary to determine the overall impact so that appropriate recovery steps can be taken in that direction. However, it is also important to understand the trends and implications of such attacks on the financial institutions (Casey, 2011). The IT team along with the senior management will thereby provide suggestions to overcome such attacks in a given scenario.

**Literature Review**

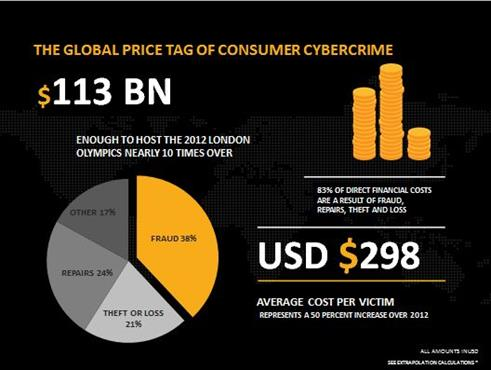
The motivation behind cyber-attack is unknown but the major motivations are shown in Appendix-1. It is thus important to understand the major threats from this cybercrime perspective. There are several such threats through which the operations of the banking sector can be interrupted and can further lead to operational and financial loss to the respective organization (Husarska, 2008).

The malicious attackers will attack on the IT system and database of the banks and will try to steal the information pertaining to the customers. Through DDoS attacks and web application attacks they want to compromise the IT system of the organization. For this purpose, criminals will be sending phishing mails both to the banking system and also to the users (Husarska, 2008). They will be developing fake websites and will try to dupe the consumers so that they can provide their sensitive financial data.

The information will be thus leveraged and will thus directly impact negatively both on the customer and on the banking system. In one of the examples, where the cybercrime took place, the attackers took away the financial and banking data of customer's debit card information. It led to nearly £2.5 million loss to the bank and nearly 9,000 account holders (Jaycox, 2013).

Security Company Kaspersky Lab stated that in the last five years nearly US $113 billion is stolen by the hackers including banking data from more than 30 nations of the world as shown below (Jaycox, 2013). The banking industry not only in Australia but across the globe will thereby face a challenging situation.

The risk of increased attacks will increase and subsequently cybercriminals through their advanced techniques will cause theft of finances and financial data of the organization. It will not only lead to financial loss but will create havoc in a given community (Killebrew, 2008). People will be afraid to put their money in the banks; instead, they will start safeguarding at other locations or even in their homes. It will further increase the risks of physical theft in the community.



**Figure-1: Price Tag of Consumer Cybercrime**

Second, the trust levels of the customers will decreased, if the IT systems of the banks can be easily compromised. As per the Banking Reports of Australia, nearly AUS $ 100 million is already lost in different cybercrime activities. It will take a long time for the banks to get recovered from this situation (Husarska, 2008). Also, the entire banning operations will be impacted due to which the business transactions will get halted for a certain period.

The economic impacts will be huge in such cases, as banks will not only suffer financial loss, but also operational loss in a given working environment. Even, the government will fail to support these organizations in such circumstances as cybercrime is already committed. It cannot be halted in the next phase (Jaycox, 2013); the recovery solutions then need to be implanted and the systems need to be restored in the nearest time.

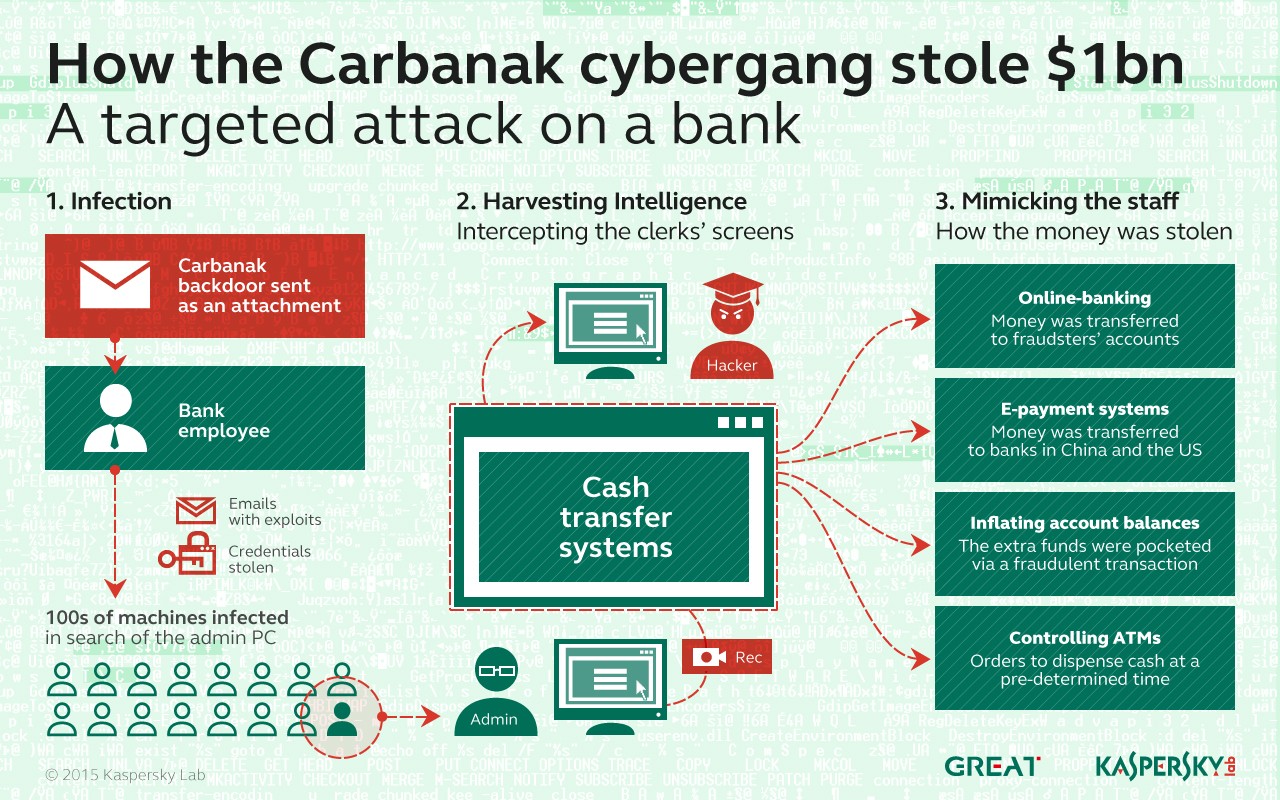
The banking authorities in association with the operations team, IT team, and other concerned regulatory authorities need to deploy security patches that will increase the firewall protection of their networks and systems (Douglis, 2009). There is a need to deploy increased security layers to the database of the banking system.

However, on the contrary, it is observed that the financial industry has not spent enough to keep their pace with the technological innovations specifically in ensuring security to their systems. It is important for the top-level management of the Australian banks to consider these risk factors and then collaborate with IT specialists that will guide them in overcoming the challenges against the criminals of cybercrime (Douglis, 2009).

There are different types of attacks that can disrupt the economic system of the banks. These include spear phishing, email attacks such as Ransom ware, Malware, Trojans, and Viruses that will affect the entire functioning of the organization (Moore, 2005). Also, few researchers have stated that due to internal threats the information of these banks gets compromised.

When an internal employee passes over certain information to third party entities, it will be difficult to track him and hence can lead to possible cyber-attack on the organization. From the impact perspective, people will lose their hard-earned money and will find it difficult to find any system where they can safeguard their money (Moore, 2005).

Even, the government will fail to bring back their trust levels in the banning organization. The customers will not further believe in principles such as transparency, accountability, Code of Ethics, and integrity of a given organization. Even, the banks will be impacted severely during such attacks. Once the hackers gain access to the internal system, they will be mimicking the actions of transferring the cash from the bank to the ATM machines (McCullagh, 2012). This is demonstrated in the below figure:



**Figure-2: Cyber-attack on Bank**

The hackers will then transfer money from the bank into offshore accounts or even in the ATMs of unknown accounts (Bose, 2012). They will thereby gain access to the cash and will thus steal money of the customers. One of the major thefts that took place in similar manner affected *Commonwealth, Westpac*, and *National Australian Banks* where the amount reached the mark of US $10 million. It is thereby important to take steps against cybercrime to overcome such breaches and protect the systems of the organisation.

**Impacts of Cyber-attack on Banks**

It is important to note that the impacts of cybercrime will distort the functioning of the entire banking system in Australia. Consumers will be affected the most as they will be losing their money from their bank accounts. It is the responsibility of the banks and the government to take measures that will first recover financial problems of the customers (Nakashima, 2013).

Second, banks will find it difficult to have financial stability as they are impacted both at operations' end and at financial end. The attack on the Australian Bank Processing Systems will thereby disrupt the entire architecture of the banking system (Nakashima, 2013). It will have a severe impact on the economy as the growth progress of the banks will halt; the customers will lose their trust in the banks and also in their government. It will be a chaos that could lead to other detrimental impacts in the community.

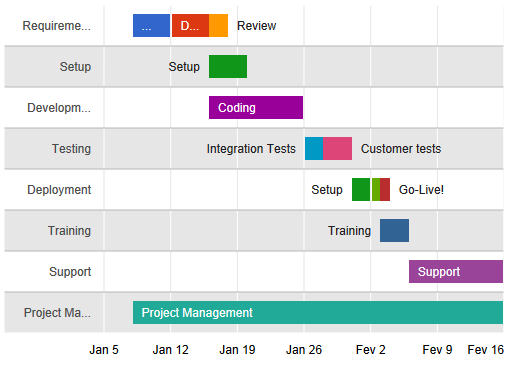
Professor Richard Benhman, the chairman of *Britain's National Cyber Management Center* has warned to all banking institutions to remain prepared for the cyber-attack. To overcome such attacks in the future, the Australian financial services regulator will be implementing new policies and rules for the customers to adhere to Cybersecurity prudential standard (Litzky & Oz, 2008).

The top-level management of the Australian banks will deploy information security risk management system in the organization to overcome the risk factors associated with Cybersecurity. The *Australian Prudential Regulation Authority (APRA)* will be creating a dedicated prudential standard for Cybersecurity that will ensure financial services firms remain secured against the different trends in a given attack (Killebrew, 2008).

**Role of Australian Board of Banks in preventing Cyber-attacks on Banks**

The *Australian Board of Banks* further needs to propose a plan of implementing cyber security solutions for all the banks of Australia. They need to develop a solution through which they will be able to protect the IT assets of these banks and subsequently deny the cyber-attacks in a given scenario. For this purpose, the security team of the organization can implement machine-learning technology and thereby prevent potential breaches and data loss for a given organization.

The following figure- shows the Gantt chart for implementing cyber-security solution in the Australian banks. It will take about 1-2 months of time to complete this project. There are several phases of this project and they need to be completed as shown in the figure.



**Figure-3: Gantt chart for Implementing Cybersecurity solution in Australian Banks**

The organization needs to provide different security mechanism for different types of cyber-attacks in a given scenario. They can establish legitimate presence in the cyber world by implementing different security measure as suggested in this report. Further, they need to upgrade their systems and security patches and also use encryption techniques during the time of transmitting the data from the banking networks to other secured networks across the world (Douglis, 2009).

Only then it will prevent the data transmission process against different types of cyber-attacks taking place in the world. Finally, the intent of the organization should be to protect the information of the customers and make sure that there are no detrimental impacts on the organization (Douglis, 2009). If the system fails, it would lead to heavy financial losses both for the customers and also for the banking organization in Australia.

**Guidelines Issued by the Australian Government on Cyber-attacks on Banks**

There are certain guidelines provided by the government of Australia to these banks to prevent cyber-attacks against a given firm. As per these guidelines, the banking organizations need to clearly define the IT security-related roles and responsibilities for the board members, managers, and the ground-level staff (Bose, 2012). There will be separate governing bodies deployed that will be monitoring cyber mechanisms of the organization.

This team will also maintain information security that will protect the IT assets of the organization. There will be new controls implemented to protect the information assets so that they can overcome the attacks of cybercrime in a given scenario. The IT team will also conduct systematic testing on a regular basis to make sure that these systems are not affected and are performing as per the expectations of the organization (Martin, 2012).

The team will install robust mechanisms such as installing antivirus software, security patches, security standards, and implementing security practices across the organization. All the systems of a given banking organization will be checked for errors, bugs, or any other impact of malicious software (Litzky & Oz, 2008). It will help the team to take immediate measures and thereby prevent the attack impacting the entire system.

Further, the *Australian Board of Banks* need to bridge the threat gap and take certain initiatives that will help the organizations preventing against cyber-attacks. The security team of the organization needs to adjust roles and responsibilities for all the members of the organization. They need to prioritize Cybersecurity as one of the top needs of the organization and there ensure providing security patches into IT systems, design, and architecture (Casey, 2011).

**Conclusion**

Today, the issue of cyber-attack is challenging not only to the banking sector but across all the sectors; it is thereby important to take steps to prevent cyber-attacks and prevent the organization from data loss and financial loss in a given scenario (Moore, 2005).

This report thereby raises important research question on how to prevent the banks against the threats of cyber-attacks. Researchers have suggested different tools and techniques to overcome them but still it seems that the Information and Data assets are prone to the cyber-attacks. Also, the employees of these organizations lack technical skills to overcome these attacks and simultaneously take steps to mitigate them.

There is research gap identified in defining the user processes, user acceptance levels, and training on the customers as well as the staff of the banking institutions (Douglis, 2009). Instead, to broaden the IT services, the banks are suggesting customers to switch to digital services such as Internet banking and Mobile banking. But are these services safe to the customers? This question needs to be answered only after appropriate recommendations are implemented and the banks are deployed with IT security solutions.

The research of this project should thereby focus first on identifying the gaps in the IT security of the banking institutions. Second, it should then provide solutions through which Cybersecurity of the banking system can be strengthen in a given challenging scenario. The top-level management of the organization needs to consider Cybersecurity as of paramount importance. The effective management of handling cyber-attack incidents will help the organization to protect their data sets and subsequently prevent the IT breach in the organization (Richardson & Director, 2008). It will also increase the trust levels of the customers and will subsequently avoid the havoc situation.

Appendix

**Appendix-1: Motivations for Cyber-attack**

