**7 Reasons Why Cybersecurity is Important in Banking**

The banking sector has always been under threat from criminals. In the past these threats only pertained to physical robberies, and later, computer frauds. But today, the sector faces even bigger threats of cyber-crimes with far-reaching effects. It’s not only the banks that face the consequences, but the customers who can have their personal information leaked and misused as a result of network hacks and identity thefts. These potential security risks and threats can cause considerable damage and can lead to significant loss of financial data and funds. This potential is a stark reality and since the banking industry is the backbone of financial sector, it is very important to emphasize on the importance of understanding and mitigating cyber risks to improve cyber security in all the banking processes.

**Importance of Cybersecurity for Banking in Recent Years**

With more customers going cashless, transactions are now made through credit card scanners and online checkout pages. In such situations, a customer’s Personally Identifiable Information (PII) can be stolen, redirected to another location and used for malicious activities. In addition to the customer, it also negatively impacts the bank while recovering the data as it might need to pay millions to recover the information. Not only that, banks also lose their reputation and customer’s trust.

Let us briefly look at seven reasons why cybersecurity is more important now than ever in the banking industry.

1. **Breach can cause a Bank its Reputation**

Since banks hold financial information, data breaches are one of the most common threats they face as leaked information can be misused by cybercriminals in many ways. Even after recovering the financial losses, it is still hard for banks to recover the lost trust due to an insufficient cybersecurity strategy. A strong cybersecurity policy implemented across the bank will not only prevent cyber breaches but also help to gain a customer’s trust and build brand reputation. It is also important to communicate your cybersecurity policy with the customers and ensure them about the protection of their financial and digital assets. An even better strategy would be to integrate artificial intelligence into your cybersecurity measures.

1. **Protection of Customer’s Assets**

Consider that there is a data breach in a bank as a result of weak cyber security and all important financial data of customers is now in the hands of cyber criminals. The customers are not only stressed about what will happen with their financial assets but also have to go through the process of canceling their bank cards, checking transactions and bank statements. Apart from financial loss, the personal information of customers can also be used against them.

With a strong cybersecurity in place, even an attempted data breach will not compromise the sensitive information of customers and will protect their assets.

1. **Avoid Penalty and Consequences**

Banks and financial institutes can face penalties for FDIC noncompliance very easily. To maintain compliance, they need to keep cybersecurity as their utmost priority. With an effective and compliant cybersecurity strategy in place, a bank ensures its customers and regulators that it meets the national and international security standards and rightfully safeguards the data and money of its customers.

1. **Safe Digital Transactions**

With an increased trend in mobile banking and online shopping, hackers have now more opportunities to collect information by hacking into less secure mobile apps or by using phishing techniques to get credit card information. To prevent this, banks must include encryption and multifactor authentication to their mobile applications and [credit card](http://www.cardzgroup.com/BankCards.html) transactions so that the customer’s data is not compromised and their money stays safe.

1. **Handle Third Party Risks**

Banks and financial institutions today cooperate closely with many third-party vendors to reap a number of benefits such as cutting costs, increased efficiency, increased flexibility of internal teams and introducing new technologies and solutions. But this cooperation also brings significant security concerns regarding the access of vendors to the bank’s data and resources. It may unintentionally turn your ally into your enemy and while a bank may delegate certain tasks to third parties, it is still their responsibility to ensure cybersecurity. While your vendor may not be a direct threat, a cybercriminal may attack them to gain access to your data. It is, therefore, important to devise a third-party risk management program which includes a set of tools, policies and activities to manage potential risks posed by subcontractors.

1. **Handle Spoofing**

Spoofing is a cybersecurity threat where a malicious criminal impersonates a bank’s website URL by creating a similar website with exactly the same interface and features. When a user visits that website by mistake or through a given link, they enter their banking information which is collected by the cybercriminal. What is even more alarming is that some new spoofing techniques allow hackers to use exactly the same URL and even target users who visit the actual website of the bank. This threat is very important to be addressed by banks with an effective cybersecurity in place.

1. **Increased Social Engineering**

Even with all your security practices in place, a bank could still fall victim to a social engineering attack, whereby any employee is deceived into giving you critical information due to their lack of knowledge, laziness or utter negligence. Social engineering is believed to be one of the most frequently used way of getting corporate information nowadays. These can come in many forms such as, by phone, phishing emails, in person or through social media. One of the key components of a strong cybersecurity policy includes regular trainings and practical information security awareness sessions for employees to understand and identify social engineering attempts. When employees are vigilant and knowledgeable about such threats, the way they proactively deal with such encounters greatly reduce the chances of leaking sensitive information.

**Final Thoughts**

To deal with cyber risks, banks need to conduct regular security audits to find out their strengths and weaknesses, enable firewalls and updated anti-malware applications, use multi-factor authentication in their mobile and web applications for transactions, deploy biometric systems to identify users, enforce automatic logout after timeout sessions and most importantly, educate employees and customers about day to day cybersecurity practices to avoid a potential data breach from taking place.