# *Why Does The Finance Industry Need Security Awareness Training*

The financial industry has been changed from conventional accounting system to digital system of accounting.

As the digital accounting systems contain the use of computerized tools, there are also security threats causing millions of dollars being drawn from financial systems.

Here we come up with the challenge of how to use these tools safely?

In the following lines, we are going to discuss the importance of security awareness training for financial industry. We will also address the security threats against financial industry.

**The Need of Security**

It was July 10, 2016 when more than 315,000 financial records were stolen from a payment processor Bluesnap or its customer Regpack. After the vendor confirmation of the breach, it was confirmed that the data was being drawn from their official systems.

Considering the mentioned breach above, each financial institution is facing data breach threats causing an average cost of $3.8 million on annual basis.

**The Anatomy of a Secured Financial System**

Every financial system has a basic function of transacting and recording the entry in the file system. In order to use the same information at the same time, the recorded financial records are shared across expanded networks.

According to security standards, if the transmitted information is not protected under a specific algorithm, it can be tracked and altered down maliciously.

A secured financial system will always ensure security on ends, the sender and receiver. The system will always protect the transmitted data under a specific security algorithm, known as Encryption under special digital certificates.

**Importance of Security Awareness Training for Financial Industry**

Reports show that financial institutes like payment processors and banks had suffered security breaches from attacks executed in shortest times.

Considering the diverse nature of cyber attacks, financial institutes need to conduct security awareness programs for technical and general employees.

In the coming lines, let's have a look at the important factors about why does the Financial Industry need security awareness training.

1. **Secure Development of Financial Transactions**

In official financial environment, each transaction must follow a pre-defined set of security standards. It means every transaction must satisfy a security checklist from initiating a transaction to its final entry.

Security checklist may contain detecting fake requests, signature forgery, indirect checkouts, expiration date checking and validating account limits.

2. **System Failure**

It was about September 2016 when the France largest web hosting company OVH faced the world's largest DDoS attack. They recorded a sum of 1TBPS data traffic against their servers, launched from millions of hacked smart devices.

According to Search Security, a Distributed Denial of Service Attack is an attack on digital infrastructures, consisting of sending large data traffic which breaks down the normal function of the system.

In the same way, financial industry is flooded with forged data theft attacks. If the technical resources are not properly trained and educated, as well as employers, financial institutes will face 55% of malicious attacks from outsiders.

3. **Social Engineering**

Social Engineering is a type of attacks, in which an attacker exploits the human weaknesses to gain access to some sensitive information.

A typical attack consists of sending a spoofed email to end users, asking them to change their passwords to some hacker choice phrase.

According to CSO, the average number of attacks against financial services, including social engineering, is four times higher than other industries.

To stay safe from social engineering attacks, financial industry needs to educate their man-power for staying safe from hacker tools like Social Engineering Toolkit. They must also educate their people with security precautions important for avoiding such attacks.

**Security Threats Finance Industry Faces**

According to Symantec report, over 600 financial institutions are targeted by Financial Trojans.

Trojans are specific hacking tools designed to steal sensitive data. When a Trojan made for stealing financial records is settled in the system, it gathers and sends sensitive financial data back to its author.

The number of security threats to financial industry is high, however we are going to discuss the most active in the following lines.

**1. Application Level Attacks**

When the main functional system of a financial institute is attacked, we categorize the attack as Application Level attack, where Application is referred to the core responsible for handling routine system tasks.

Application level attacks can take the whole system down. According to a study published on Applicure, there were more than 70% attacks recorded from outsiders, compromising application level core of the systems.

With the aim of staying safe from Application level attacks, financial institutions need to conduct a weakness finding process like Penetration Testing. The purpose of penetration testing process is to ensure finding and fixing security weaknesses in the system.

## 2. Data Breach or Theft

According to a study published on Credit Cards, about 12% of breaches have occurred in financial services sector.

Another study shows that USA, Germany and India is facing high volume of financial Trojan attacks.

Keeping in mind the growing attacks of data breach on financial industry, the need to educate and taking security measures is mandatory.

## 3. Account Takeover

One of the most trending security threats against financial industry is account hijacking. In this case, the attacker takes over the account by Technical or Social Engineering, changes security credentials and takes all the fruits away from the original account holder.

According to a study published by FBI, there were more than 400 cases reported about account takeover.

In order to stay safe, the best practice to prevent account hijacking is to follow the genuine security precautions of a system. Other than original ones, there are millions of fake sources trying to trap employee unwanted actions.

## 4. Emerging Technology Changes

Software vendors are constantly updating their financial accounting tools. The changing nature of technology opens door for Zero Day Vulnerabilities and causes large affection until the fix is made.

To avoid affection from technological change, financial firms are subjected to update their systems on timely basis.

## Conclusion

Financial firms need to educate their man-power as well as update their technical systems on timely basis. They are also subjected to adopt the latest technology

trends under professional advice and take necessary steps to avoid newly designed attack patterns. It is also mandatory to apply security patches as they are announced by official vendors.

**References**


- Bankrate - http://www.bankrate.com/finance/banking/us-data-breaches-3.aspx
- Security Week - http://www.securityweek.com/320000-financial-records-apparently-stolen-payment-processor
- Expanded Ramblings - http://expandedramblings.com/index.php/cybersecurity-statistics/
- Veracode - https://www.veracode.com/security/man-middle-attack
- Hacker Space - http://hackerspace.kinja.com/how-to-defend-yourself-against-mitm-or-man-in-the-middl-1461796382
- Security Affairs - http://securityaffairs.co/wordpress/54036/hacking/distributed-guessing-attack.html
- The Hacker News - http://thehackernews.com/2016/09/ddos-attack-iot.html
- Search Security - http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack
- Credit Cards - http://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php
- Owasp - https://www.owasp.org/index.php/Social_Engineering
- CSO Online - http://www.csoonline.com/article/2938767/advanced-persistent-threats/report-banks-get-attacked-four-times-more-than-other-industries.html
- Social Engineering - http://www.social-engineer.org/framework/se-tools/computer-based/social-engineer-toolkit-set/

- Symantec - http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_world_of_financial_trojans.pdf
- Kaspersky - https://usa.kaspersky.com/internet-security-center/threats/trojans#.WMvxMlWGPIU
- Applicure - http://www.applicure.com/blog/web-application-hacking-facts-figures
- Payments Cards and Mobile - http://www.paymentscardsandmobile.com/targeted-countries-financial-trojans-2015/
- FBI Study - https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector
- Fire Eye - https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html
- Microsoft Security Bulletins - https://technet.microsoft.com/en-us/security/bulletins.aspx