Proposed Solutions for Banking Industry to Prevent Insider Threats

Xiaoting (Theresa) Liu

Table of Contents

Abstract

Recent high-profile cyber security attacks have dominated the business agenda. With high profile business and customer data up for grabs, not to mention the opportunity to disrupt or defraud a business, the financial services sector makes a highly tempting target. Insiders threats cost huge loss to the banking industry not only the unintentional attacks but also malicious attacks. The threats lead all kinds of attacks in banking systems and thus results data and information loss. This paper is conducted to research cost effective solutions to address insider threats issue for the banking industry.

Introduction

Traditional banking system has a great potential to achieve a higher level of operation by integrating technology, which is called modern banking system. The allure of modern banking lies on its availability and convenience that allow customers to control their accounts remotely and independently. Modern banking system has a unique advantage on its data volume and variety that allow us to discover the trends and patterns for future product development (Mungai & Bayat, 2018). As the modern banking is growing recently, the risk of managing bank's system and customers information is higher, especially insider threats.

In this paper, we will start with some researches regarding cyber security and insider threats in banking industry and learn from the possible solutions with current available insider threats prevention technologies. A cost-effective proposal will be provided at the end to solve the problem statement.

Problem Statement

Our company is an investment company with very proprietary and highly sensitive software technology that provides competitive differentiation in the marketplace. The CEO has seen a Forrester report, which says insiders are responsible for more than half of your data breaches. In addition to the cost of data loss ranging from $500K to $1M per year, the company's future itself may be drastically impacted if the data falls in the wrong hands. The CEO has asked to implement security processes and technologies to ensure insider threat protection. This paper will propose a solution, estimate cost and time required to implement and justify the solution.

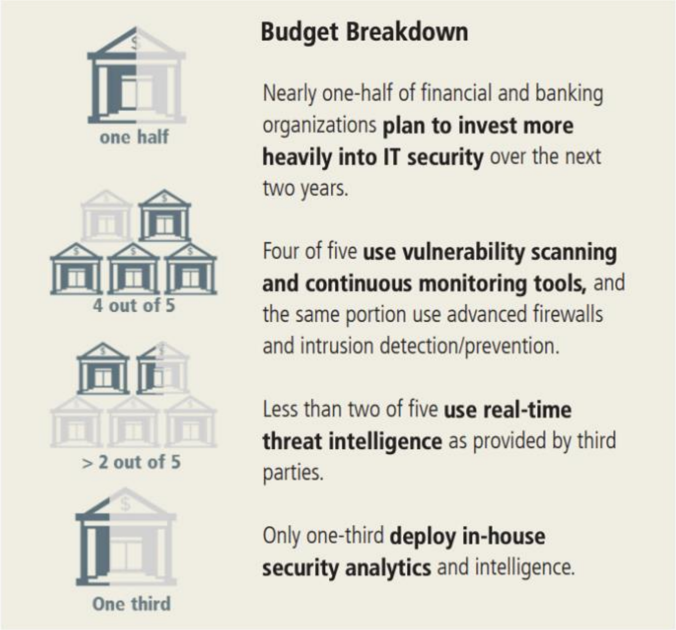
Related Researches

Current Situation with Cyber security in Banking Industry

According to the whitepaper by Bitdefender (2818), there are some facts that banking industry does face difficulties to deal with security.

- Lack of specialists, tools, budget and knowledge are the main roadblocks for financial sector, shows a Bitdefender survey over 118 companies. 118 IT security purchase professionals from large companies in the US and Europe, are providing worrying details of how difficult it is to cover security of operations.
- 47.5% of financial institutions were breached in the past year
- 58.5% of financial institutions have experienced an advanced attack or seen signs of suspicious behavior in their infrastructure.
- 83.9% of surveyed execs think EDR-like tools are a solid solution in preventing attacks.

The whitepaper (2018) also indicates that to ensure success, hackers have developed attack strategies to target particular companies in the financial services industry. In fact, research shows that the number of security incidents in this sector has tripled in the past five years, and the containment cost has increased by 9.6 percent (2018). According to the IBM X-Force Threat



Budget Breakdown

Nearly one-half of financial and banking organizations **plan to invest more heavily into IT security** over the next two years.

Four of five **use vulnerability scanning and continuous monitoring tools,** and the same portion use advanced firewalls and intrusion detection/prevention.

Less than two of five **use real-time threat intelligence** as provided by third parties.

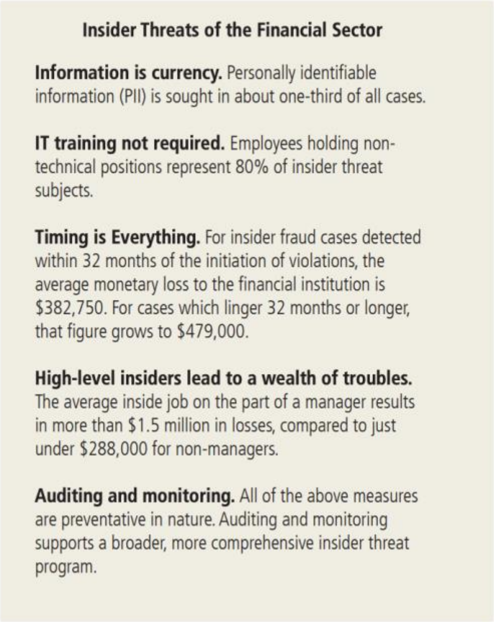
Only one-third **deploy in-house security analytics** and intelligence.

Figure 1 Budget Breakdown

Intelligence Index 2017, the financial services industry experienced the highest number of cyber-attacks in 2016. 58% of these attacks were caused by insiders. 53% of insider attacks were inadvertent, and only 5% were malicious. To call attention to this issue, Raytheon and The SANS Institute recently released the survey report, “Risk, Loss and Security Spending in the Financial Sector: A SANS Survey.” A total of 293 global financial industry IT professionals took part, including CIOs, IT managers/directors, high-ranking security officers or security/forensics analysts (Raytheon).

Cybersecurity Threats in Banking Industry

According to the IBM X-Force Threat Intelligence Index (2017), the financial services industry experienced the highest number of cyber- attacks in 2016. 58% of these attacks were caused by insiders, 53% of insider attacks were inadvertent, and 5% were malicious. Insider threat poses huge loss to organizations since malicious insiders have enough knowledge to attack highly sensitive information. Moreover, preventing and detecting insider attacks is a hard job because malicious insiders follow legal paths to launch attacks. This threat leads all kinds of attacks in banking systems in the amount of loss it causes. Insider threats generally refer to employee (on or off duty), contractors, business partners of enterprises or organizations who should have access to the organization’s systems, networks and data. An insider threat is an action taken



Insider Threats of the Financial Sector

Information is currency. Personally identifiable information (PII) is sought in about one-third of all cases.

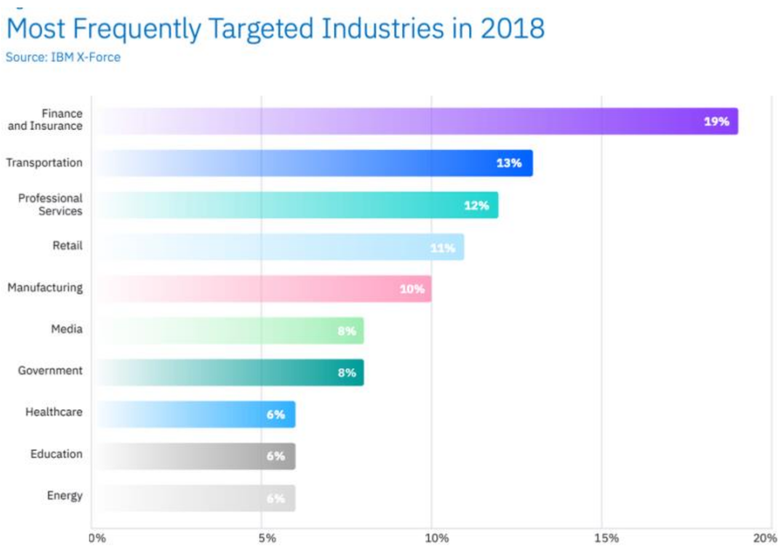
IT training not required. Employees holding non-technical positions represent 80% of insider threat subjects.

Timing is Everything. For insider fraud cases detected within 32 months of the initiation of violations, the average monetary loss to the financial institution is $382,750. For cases which linger 32 months or longer, that figure grows to $479,000.

High-level insiders lead to a wealth of troubles. The average inside job on the part of a manager results in more than $1.5 million in losses, compared to just under $288,000 for non-managers.

Auditing and monitoring. All of the above measures are preventative in nature. Auditing and monitoring supports a broader, more comprehensive insider threat program.

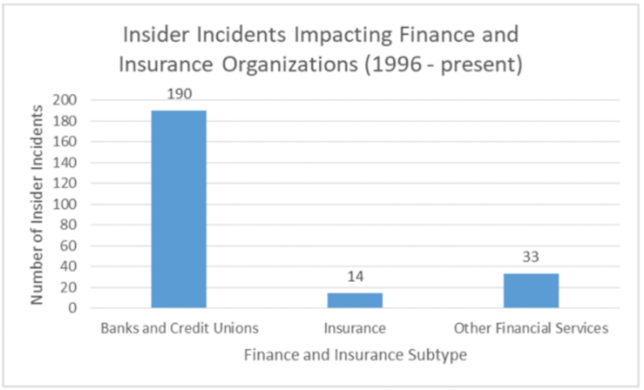
by an insider to negatively affect the confidentiality, integrity and availability of information in an organization’s information system by using legally obtained access rights. Those attackers come from internal users, so it is more difficult to detect and more harmful.

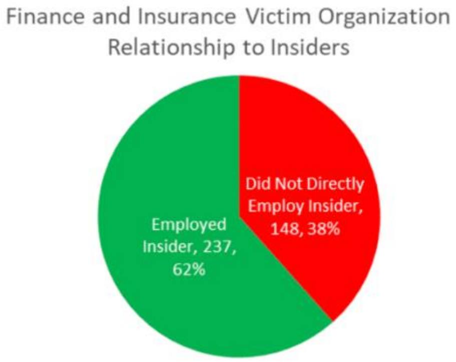

Most Frequently Targeted Industries in 2018

Source: IBM X-Force

From the graph at the right side (X-Force Threat Intelligence Index 2019), we can see that banking and finance industry are most frequently targeted industries in 2018. According to a 2018 Cost of Insider Threats: Global Organizations report, “a malicious insider threat can cost an organization $2.8M per year, or an average of $604,092 per incident.” For instance, Morgan Stanley was forced to pay $1M penalty for failing to protect their customer records; Wells Fargo reported insider fraud by employee who created almost 2M accounts for their clients without their knowledge or consent (Eliyahu, 2019).

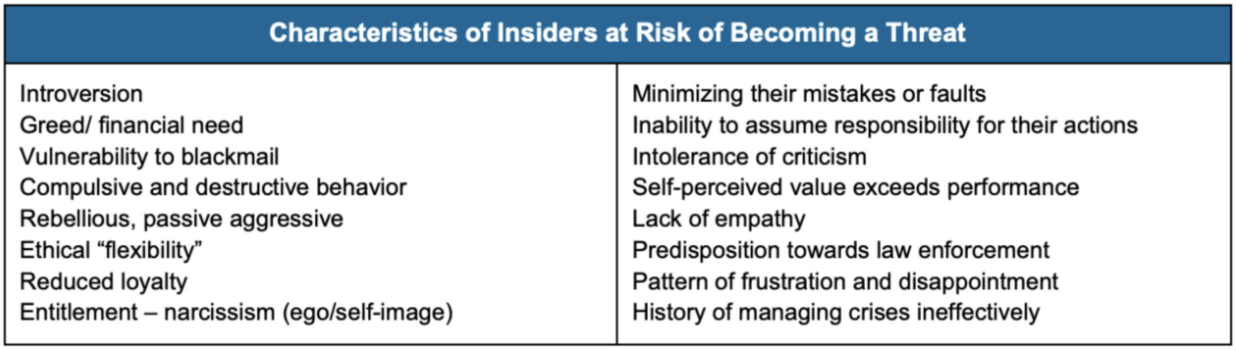
Miller (2018) provides future details on insider threats across industry sectors. She discusses information security regulations and insider threat metrics based on Finance and Insurance incidents from CERT National Insider Threat Center (NITC) Incident Corpus. In total, her team identified 237 malicious, non-espionage insider incidents where a Finance and Insurance organization was both the victim organization and the direct employer. There were 148 additional incidents where a Finance and Insurance industry organization was impacted by a Trusted Business Partner (e.g., temporary employees, outsourced computer support, or cleaning services) or an insider incident at another organization (Miller, 2018). Among all insider threats, fraud is the most frequent incidents type in this industry. Miller (2018) also indicates 49.5% of the insiders were employed for 5 years or more.





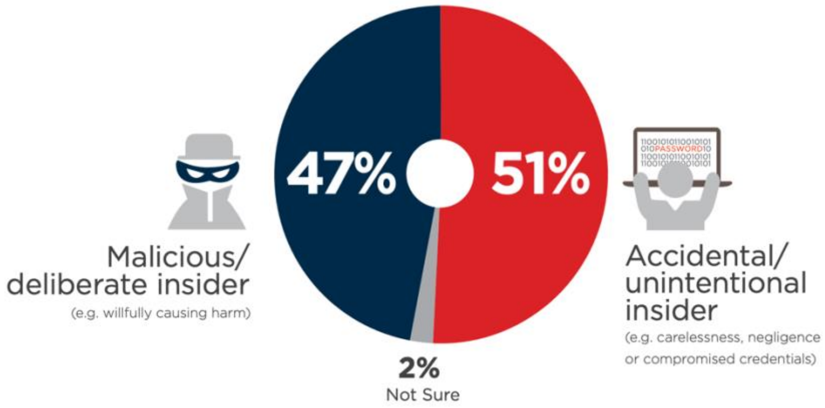
Insider Threat

According National Cybersecurity and Communications Integration Center (2014), an insider threat is generally defined as a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems. Insider threats, to include sabotage, theft, espionage, fraud, and competitive advantage are often carried out through abusing access rights, theft of materials, and mishandling physical devices. Insiders do not always act alone and may not be aware they are aiding a threat actor (i.e. the unintentional insider threat). National Cybersecurity and Communications Integration Center (2014) also identifies some general behavior characteristics of insiders at risk of becoming a threat such as introversion, compulsive and destructive behavior, reduced loyalty, intolerance of criticism, and lack of empathy, etc.



Characteristics of Insiders at Risk of Becoming a Threat	
Introversion	Minimizing their mistakes or faults
Greed/ financial need	Inability to assume responsibility for their actions
Vulnerability to blackmail	Intolerance of criticism
Compulsive and destructive behavior	Self-perceived value exceeds performance
Rebellious, passive aggressive	Lack of empathy
Ethical “flexibility”	Predisposition towards law enforcement
Reduced loyalty	Pattern of frustration and disappointment
Entitlement – narcissism (ego/self-image)	History of managing crises ineffectively

There are two types insider threats are identified by the CA Technologies Insider Report (2018). The report indicated that people is often associate the term “Insider Threats” with malicious employees intending to steal information from the company; however, negligent employees or contractors unintentionally cause an equally high percentage of threats to the company.



Malicious Insider Threat. Looking back to the document provided by National Cybersecurity and Communications Integration Center, there are some indicators of malicious threat activity are identified:

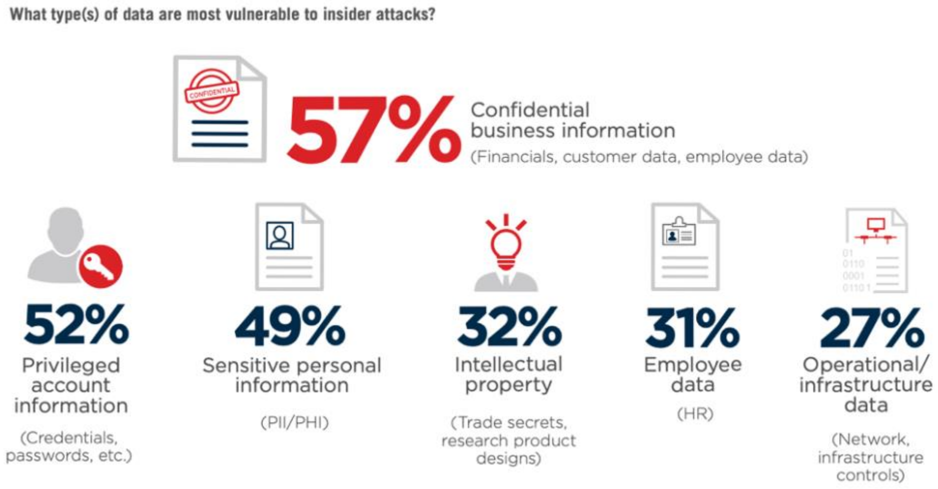
- Remotely accesses the network while on vacation, sick or at odd times
- Works odd hours without authorization
- Notable enthusiasm for overtime, weekend or unusual work schedules
- Unnecessarily copies material, especially if it is proprietary or classified

- Interest in matters outside of the scope of their duties
- Signs of vulnerability, such as drug or alcohol abuse, financial difficulties, gambling, illegal activities, poor mental health or hostile behavior, should trigger concern. Be on the lookout for warning signs among employees such as the acquisition of unexpected wealth, unusual foreign travel, irregular work hours or unexpected absences

Unintentional Insider Threat. It is defined by the CERT Insider Threat team (2013) that an unintentional insider threat is (1) a current or former employee, contractor, or business partner (2) who has or had authorized access to an organization's network, system, or data and who, (3) through action or inaction without malicious intent (4) causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems. There are four types of unintentional insider threats that account for virtually all of the incidents:

- DISC, or accidental disclosure (e.g., via the internet)—sensitive information posted publicly on a website, mishandled, or sent to the wrong party via email, fax, or mail
- UIT-HACK, or malicious code (UIT-HACKing, malware/spyware)—an outsider's electronic entry acquired through social engineering (e.g., phishing email attack, planted or unauthorized USB drive) and carried out via software, such as malware and spyware
- PHYS, or improper or accidental disposal of physical records—lost, discarded, or stolen nonelectronic records, such as paper documents
- PORT, or portable equipment no longer in possession—lost, discarded, or stolen data storage device, such as a laptop, PDA, smart phone, portable memory device, CD, hard drive, or data tape

Among these insiders, the Insider Threats 2018 Report indicated both regular employees (56%) and privileged IT users (55%) pose the biggest insider security risk to organizations, followed by contractors (42%). Further details on types of data are most vulnerable to insider attacks are identified in this report. From below graph, we can see that confidential business information such as financial, customer data and employee data are the most vulnerable type.



Recommended Solution

Bitdefender (2018) indicates that financial services firms deal with high volumes of critical data. Cybercriminals move fast, knowing that access to this information is a gold mine, as they can sell it to the highest bidder on the dark web, or even use it themselves for fraud and other illegal endeavors. Naturally, this raises mitigation costs. The data breach recovery cost is higher for financial institutions and considering all industry US companies spent $7.35 million per breach last year according to the global overview report from IBM and the Ponemon Institute, these organizations are in for some dramatic numbers.

In general, Alton (2018) provides some suggestion on how to prevent malicious insider threats and unintentional insider threats.

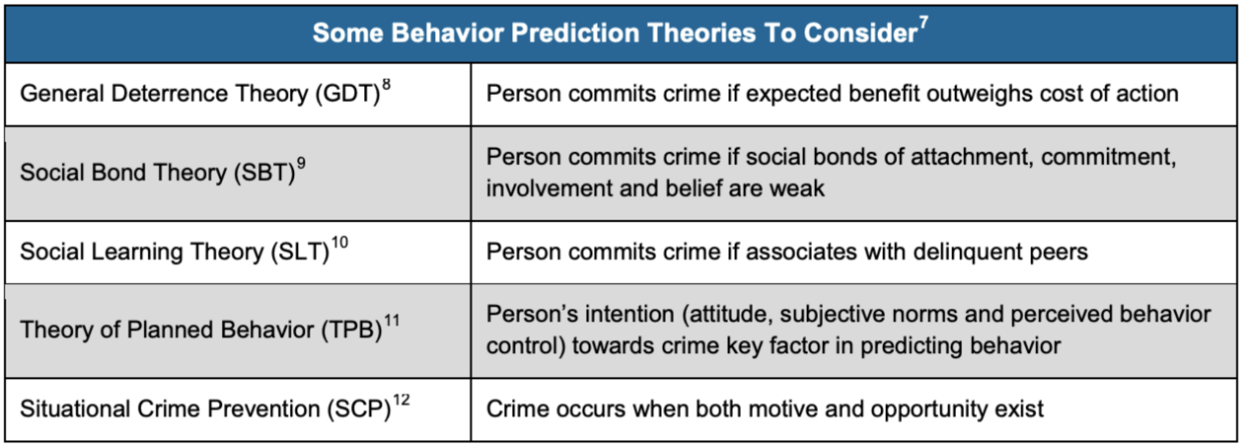
Malicious Insider Threats:

- Don’t stop at employee training. Consider implementing an employee monitoring solution. For example, this solution might flag when employees access files they’re not supposed to or forward large amounts of sensitive data to an off-company address.
- Carefully manage permissions, including tiered permissions for sensitive information and terminating access for employees who have left your company.
- Educate your IT department about the range of behavioral patterns associated with insider crimes such as fraud, intellectual property theft and knowingly configuring software to promote data breaches

Unintentional Insider Threats:

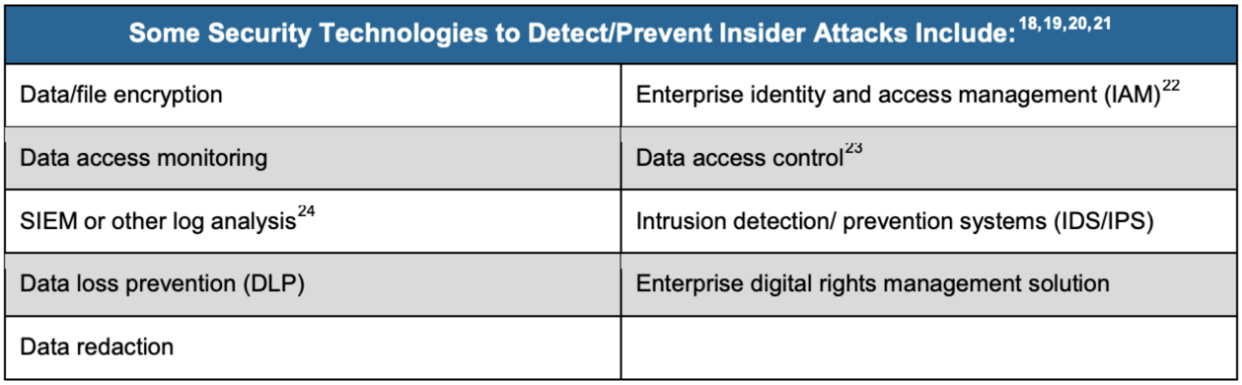
- Make attendance for trainings mandatory and ensure that anyone who has fallen through the cracks receives immediate training.
- Schedule regular training reviews — at least annually — to keep employees updated on changing technologies and emerging threats.
- Leverage end-point security solutions that help keep individual devices, such as laptops and smartphones, safe. If a device is lost or stolen, the information on the device can be wiped remotely to avoid the risk of data exposure.
- Employ security tools that help keep your network and digital interactions safe. Programs can be used to identify suspicious emails, block unsecure websites and capture malware before it ever enters the network. Combining technology with training can lead to the best long-term results.

While National Cybersecurity and Communications Integration Center also lists some theories to identify behavior indicators. A good understanding of risk characteristics and events that may trigger those characteristics is essential.



Some Behavior Prediction Theories To Consider[7]	
General Deterrence Theory (GDT)[8]	Person commits crime if expected benefit outweighs cost of action
Social Bond Theory (SBT)[9]	Person commits crime if social bonds of attachment, commitment, involvement and belief are weak
Social Learning Theory (SLT)[10]	Person commits crime if associates with delinquent peers
Theory of Planned Behavior (TPB)[11]	Person's intention (attitude, subjective norms and perceived behavior control) towards crime key factor in predicting behavior
Situational Crime Prevention (SCP)[12]	Crime occurs when both motive and opportunity exist

Besides the theoretical concepts, there are some technologies can help to prevent insider threats. Among them, we identify three technologies we can apply to our bank's situation: Security Information and Event Management, User Entity Behavior Analytics Tool and Data Loss Prevention.



Some Security Technologies to Detect/Prevent Insider Attacks Include:[18,19,20,21]	
Data/file encryption	Enterprise identity and access management (IAM)[22]
Data access monitoring	Data access control[23]
SIEM or other log analysis[24]	Intrusion detection/ prevention systems (IDS/IPS)
Data loss prevention (DLP)	Enterprise digital rights management solution
Data redaction	

Security Information and Event Management (SIEM). According to Carnegie Mellon University, A SIEM can help insider threat programs by consolidating logs into a central location and automatically prioritizing events, making those with a higher priority more visible to an analyst for action (Spooner, Silowash, Costa and Albrethsen, 2018). A typical SIEM can process hundreds to hundreds of thousands of events per second. With such a large volume of data, the SIEM rules must be finely tuned and the system configured appropriately to help determine which events are important to both the InTP and the organization's mission. The SIEM will process the events, categorizing and correlating them according to those specific rules. It can also be configured to email high priority alerts to insider threat program staff. InTP staff should have the ability, via dashboards or other means, to review and explore all events captured by the SIEM. Different organizations use SIEM systems for different purposes, so SIEM benefits vary across organizations. SIEM architectures available today include SIEM software installed on a local server, a local hardware or virtual appliance dedicated to SIEM, and a public cloud based SIEM service. There are three benefits of applying SIEM to the company (Scarfone, 2018):

1. Streamline compliance reporting. Many organizations deploy the tools for these SIEM benefits alone, including streamlining enterprise compliance reporting efforts through a centralized logging solution. An organization without a SIEM system is unlikely to have robust centralized logging capabilities that can create rich customized reports, such as those necessary for most compliance reporting efforts. In such an environment, it may be necessary to generate individual reports for each host or to manually retrieve data from each host periodically and reassemble it at a centralized point to generate a single report. Another reason why SIEM tools are so useful is that they often have built-in support for most common compliance efforts. Their reporting capabilities are compliant with the requirements mandated by standards such as the Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS) and the Sarbanes-Oxley Act.

2. Detect the undetected. SIEM tools offer increased detection capabilities by correlating events across hosts. By gathering events from hosts across the enterprise, a SIEM system can see attacks that have different parts on different hosts and then reconstruct the series of events to determine what the nature of the attack was and whether or not it succeeded. In other words, while a network intrusion prevention system might see part of an attack and a laptop's operating system might see another part of the attack, a SIEM system can correlate the log data for all of these events. A SIEM tool can determine if, for example, a laptop was infected with malware which then caused it to join a botnet and start attacking other hosts.

3. Improve the efficiency of incident handling activities. A SIEM tool can improve efficiency primarily by providing a single interface to view all the security log data from many hosts. Examples of how this can expedite incident handling include:

- it enables an incident handler to quickly identify an attack's route through the enterprise;
- it enables rapid identification of all the hosts that were affected by a particular attack; and
- it provides automated mechanisms to stop attacks that are still in progress and to contain compromised hosts.

User Entity Behavior Analytics Tool (UEBA). According to Digital Guardian, User and entity behavior analytics, or UEBA, is a type of cyber security process that takes note of the normal conduct of users. In turn, they detect any anomalous behavior or instances when there are deviations from these “normal” patterns. For example, if a particular user regularly downloads

10 MB of files every day but suddenly downloads gigabytes of files, the system would be able to detect this anomaly and alert them immediately. UEBA uses machine learning, algorithms, and statistical analyses to know when there is a deviation from established patterns, showing which of these anomalies could result in a potential, real threat. UEBA can also aggregate the data you have in your reports and logs, as well as analyze file, flow, and packet information (Brook, 2018). As such, UEBA is a very important component of IT security, allowing you to:

1. Detect insider threats. It is not too far-fetched to imagine that an employee, or perhaps a group of employees, could go rogue, stealing data and information by using their own access. UEBA can help you detect data breaches, sabotage, privilege abuse, and policy violations made by your own staff.
2. Detect compromised accounts. Sometimes, user accounts are compromised. It could be that the user unwittingly installed malware on his or her machine, or sometimes a legitimate account is spoofed. UEBA can help you weed out spoofed and compromised users before they can do real harm.
3. Detect brute-force attacks. Hackers sometimes target your cloud-based entities as well as third-party authentication systems. With UEBA, you are able to detect brute-force attempts, allowing you to block access to these entities.
4. Detect changes in permissions and creation of super users. Some attacks involve the use of super users. UEBA allows you to detect when super users are created, or if there are accounts that were granted unnecessary permissions.

5. Detect breach of protected data. If you have protected data, it is not enough to just keep it secure. You should know when a user accesses this data when he or she does not have any legitimate business reason to access it.

Data Loss Prevention. Data loss prevention (DLP) technologies generally protect data from leaving systems through unauthorized channels. When considering DLP technologies for use in an environment, you must consider the three types of data the system will be monitoring and protecting: data at rest, data in motion, and data in use. One of the more common ways to protect data at rest is through the use of encryption. Organizations can designate the use of encryption for certain types of data. For example, personally identifiable information (PII) or protected health information (PHI) might require the use of encryption depending on where it is stored. If the data leaves one storage location and is later stored at another location, such as data leaving a server for storage on removable media, the DLP solution might mandate the use of encryption on the removable media. The DLP solution can also check to verify that the media being used to store the data is authorized. For example, DLP solutions can enforce the use of particular USB flash drives with certain serial numbers or from specific manufacturers.

OpenDLP. OpenDLP is a client/server-based tool that can scan endpoints for sensitive data. The client portion of the application is a service that resides on user workstations that scans the workstation based on settings pushed to it from the OpenDLP server. The OpenDLP server manages the results of the scans. OpenDLP also has the ability to scan Microsoft SQL Server and MySQL databases for sensitive information. It should be noted that OpenDLP does not prevent data loss, but instead identifies where sensitive data lives in your organization.

MyDLP. MyDLP is a data loss prevention solution that has both a free community edition and a paid enterprise edition. The community edition has a limited feature set, while the enterprise version includes additional features and commercial support. The MyDLP website, http://www.mydlp.com, does not provide information to compare the two versions; however, the Internet Archive contains a version of their website with information about how the two versions compare. This comparison might not be accurate today, but it does provide an idea of the features the software offers

Proposed Solutions

After researching the possible solutions to prevent insider threats, here are the estimated cost to apply non-technical and technique solutions to the bank's operation. Cybrary for Business allows the organization to implement career development programs for the IT and cyber security teams. Affordably invest in the company's security by investing in the team members hired to protect the most important assets. Help shape the employees' future and ensure they retain within the organization for years to come. Technical solution includes software implementation and self-development will cost a bit more the non-technical solutions.

Solution	Cost
Non-Technical Solution: Regular Employee Training (Cybrary)	$ 0 - $100 / month
Technical Solution: Security Information and Event Management (SIEM). User Entity Behavior Analytics Tool (UEBA). Data Loss Prevention (DLP).	$400 - $3,000 / month
Total Cost	$400 - $3,100 / month

Conclusion

This paper aims to identify the insider threats in banking system and look for solutions to address our business problem. After identifying different types of insider threats, there are some proposed solutions that can help with our banking system. Non-technical solution such as regular employee training is needed to educate employee from being unintentional insider threats. One of the best ways to reduce negligence by unintentional insider threats is to educate them on safety and make sure employees are aware of the security risks the bank faces and how to deal with the risks. Besides that, technical solutions such as SIIEM, UEBA and DLP should be applied to the software system to increase protection to bank's data and information. Insider data threats present another layer of complexity for IT professionals to manage, requiring careful planning with regards to access controls, user permissions and monitoring user actions. There are numerous methods and security tools available to help cybersecurity professionals detect and analyze insider attacks. A vast majority of the respondents identified the use of more than one security tool in their organization. By merging and analyzing these disparate sources, organizations are better able to deal with security breaches. The purposed solutions cost is between $400 to $3,100 per month, and annually cost would be $4,800 to $37,200. Compared to the insider threats cost from $500K to $1M, applying employee training and installing insider threats prevention software only cost about 10% of the insider threats loss.

Reference

Alton, L. (2018, October 31). Two Types of Cybersecurity Insider Threats and How To Prevent Them. Retrieved from https://blog.centurylink.com/two-types-of-cybersecurity-insider-threats-and-how-to-prevent-them/

Bitdefender (2018). Top Security Challenges for the Financial Services Industry in 2018. Retrieved from https://www.bitdefender.com/files/News/CaseStudies/study/240/Bitdefender-Top-Security-Challenges-for-the-Financial-Whitepaper-EN-interactive.pdf

Brook, C. (2018, December 5). What is User and Entity Behavior Analytics? A Definition of UEBA, Benefits, How It Works, and More. Retrieved from https://digitalguardian.com/blog/what-user-and-entity-behavior-analytics-definition-ueba-benefits-how-it-works-and-more

CA Technologies (2018). Insider Threats 2018 Report. Retrieved from http://ca-security.inforisktoday.com/whitepapers/insider-threat-2018-report-w-4131#dynamic-popup

Eliyahu, T. (2019, May 14). Financial Cyber Threats: 10 Case of Insider Bank Attacks. Retrieved from https://www.sentinelone.com/blog/financial-cyber-threats-10-cases-of-insider-bank-attacks/

IBM. (2017, May). IBM X-Force Threat Intelligence Index 2017. Retrieved from http://branden.biz/wp-content/uploads/2017/06/IBM-X-Force-Threat-Intelligence-Index-20.pdf

Insider Threat Team, CERT. (2013). Unintentional Insider Threats: A Foundational Study (CMU/SEI-2013-TN-022). Retrieved from the Software Engineering Institute, Carnegie Mellon University website: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=58744

X-Force Threat Intelligence Index 2019. (2019, February). Armonk, NY: IBM Security

Mungai, K., & Bayat, A. (2018). The Impact of Big Data on the South African Banking Industry. Proceedings of the International Conference on Intellectual Capital, Knowledge Management & Organizational Learning, 225–236. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&AuthType=sso&db=bth&AN=136627116&site=ehost-live&scope=site

National Cybersecurity and Communications Integration Center (2014, May 2). Combating the Insider Threat. Retrieved from https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf

Raytheon. The Financial Industry and the Insider Threat: Total Awareness Leads to Secured Enterprise. Retrieved from https://www.raytheon.com/sites/default/files/capabilities/rtnwcm/groups/cyber/documents/content/rtn_244836.pdf

Scarfone, K. (2018, August). SIEM benefits include efficient incident response, compliance. Retrieved from https://searchsecurity.techtarget.com/feature/Three-enterprise-benefits-of-SIEM-products

Spooner, D, Silowash, G., Costa, D. & Albrethsen, M. (2018, June). Navigating the Insider Threat Tool Landscape: Low Cost Technical Solutions to Jump-Start an Insider Threat Program. Retrieved from https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_521706.pdf