apvera

Insider Threat Intelligence for Financial Services Industry

White Paper
Published April 2016

Index

1.Executive Summary

Financial institutions are the backbone of today´s highly globalized economic environment. With the world´s 50 largest banks having a combined market capitalization of more than US$ 4,240 billion, it is not unusual that financial services are becoming a prime target for cyber-attacks such as financial fraud, unauthorized access, and identity thefts.[1]

Financial services worldwide have to "juggle" between constantly evolving cyber threats and sometimes contradictory compliance obligations. Additionally, employees with legitimate access, service providers, and various contractors make a serious attack vector if and when their security credentials are compromised. As a result, cyber-attacks have become even more frequent and their potential impact has made insider threats a number one challenge that financial executives need to deal with at all levels of their organization.

This white paper analyzes the security threats and challenges faced by financial institutions and provides Apvera´s view on how to mitigate risk and compliance in order to prepare, defend, and strengthen their security from constantly growing insider threats.

[1] TOP Banks in the World 2014 ranked by market capitalization. 2016. TOP Banks in the World 2014 ranked by market capitalization . Available at: http://www.banksdaily.com/topbanks/World/market-cap-2014.html

2. Hidden Risks within the Financial Services Industry

The shift from the traditional brick and mortar business models to digital customer-focused channels has resulted in customers and prospects expecting complete privacy and security of their data. Data breaches due to cyber-attacks and insider threats present a tremendous danger to businesses in their efforts to keep their data safe.

2.1 What Does Insider Threat Mean?

Since financial services are highly driven by research and development, thousands of employees interact with enterprise data on a daily basis. While insider threats can take several different forms, all attacks caused by them are initiated from the inside of an organization. Since most security solutions are focused on dealing with attacks from outsiders, antiviruses, firewalls and IDS/IPS will not be able to properly deal with the threat. Insider threats are responsible for over 60% of attacks that stem from either malicious intent or from employee´s unintentional actions thus making the cost associated with losing and misusing this data one of the highest risk factors that financial institutions have to face.

2.2 New Business and IT Trends

2.2.1 Bring Your Own Devices (BYOD)

The introduction of cloud computing services and the opportunity for employees to work using their own smart phones through the adoption of BYOD/BYOS policies have brought the additional risk for the financial services industry and their processes. Employees are allowed to carry company laptops, tablets, and smartphones in and out of the office, or use their own devices to enter their organization´s networks, this makes the risk for organizations losing their data has risen significantly.

2.2.2 More Open Networks

In today´s fast-paced business environment, the use of outsourcing, contractors, and third-party technology solutions has increased significantly. While these have helped organizations to achieve greater business agility, they have also opened them to attack. These new trends in technology have brought new and complex requirements in data sharing, as well as new challenges in the field of information security. Additionally, today's privacy regulations, as well as those being considered by regulatory bodies all over the world, are completely inadequate to protect financial companies from the risks associated with these new technologies.

2.2.3 Social Engineering

Financial services who, up to recently, operated as somewhat closed systems, are especially prone to attacks. Today´s attackers know that the best way to gain access to an organization without getting caught is with the “help” of an insider. They can spend a considerable amount of time on tricking or bribing employees in order to get their access information since it is needed to carry out their attack.

2.3 So Who is Attacking Your Network?

2.3.1 Negligent Insiders

Most insiders are ordinary negligent employees who expose confidential data by accident. As employees in an organization, most of them have access to sensitive data and can inadvertently lose control of it or give access to the attackers without even knowing that they did something wrong. Some employees in this category expose their organization to risk when they bypass their organization´s security policies. For instance, by simply downloading unauthorized software or using unsecured Wi-Fi networks, they can expose their security credentials to attackers.

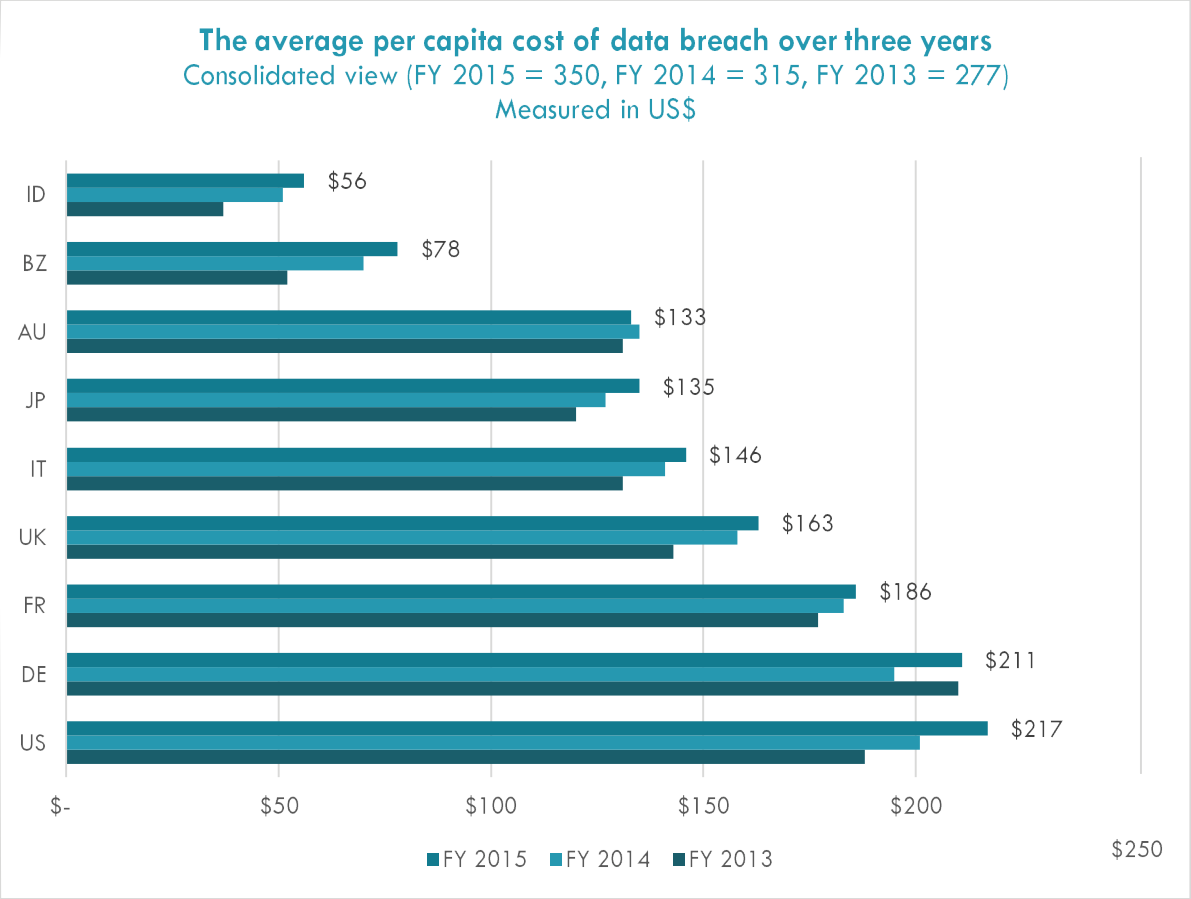
2.3.2 Malicious Insiders

Aside from negligent insiders, organizations can be exposed to security risks from employees who intentionally want to harm the organization either by stealing data or damaging their systems. These malicious insiders can have diverse motivation responsible for their actions. In some cases, they are motivated by their dissatisfaction on the job while in other cases they simply become tempted by the money they can earn by selling the organization´s private data on the black market. Additionally, there have been cases where other nations or competing organizations have planted insiders within an organization with the sole purpose of stealing trade secrets and intellectual property. Cases of Bradley Manning and Edward Snowden show that insiders can be motivated with particular ideological movements which can lead to theft and exposure of confidential data.

3. Impact

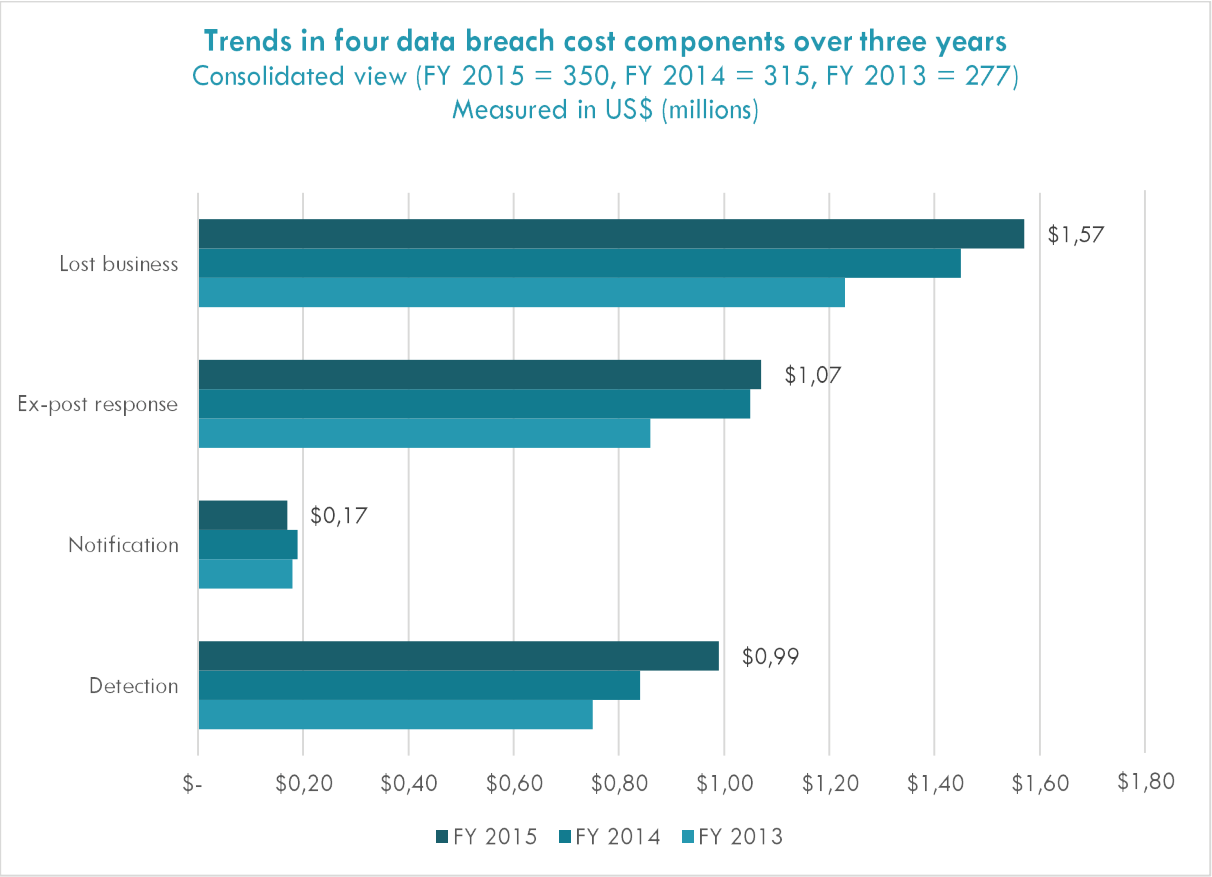
Industries that are heavily regulated, such as healthcare and financial services, have a per capita data breach cost that is significantly higher than the average. In a recently published annual Cost of Data Breach Study by IBM and The Ponemon Institute, the global average cost for a record compromised in a data breach has risen 12% in the last two years and is now at $154.

The study included 350 organizations in 11 countries and two countries with the highest average cost per record are the United States at $217 and Germany at $211. Highly regulated industries such as financial services, healthcare and education have a significantly higher per capita data breach cost than the overall mean of $154.



The Ponemon Institute and IBM have established four cost categories caused by a data breach which encompasses the whole lifecycle of a data breach. They are lost business, post-breach costs, detection and escalation costs, and notification costs.

[1] IBM 2015 Cost of Data Breach Study United States. 2016. IBM 2015 Cost of Data Breach Study - United States. Available at: http://www-03.ibm.com/security/data-breach/ .



With an average cost of a data breach climbing up to $3.8 million, the detection and escalation cost category accounts for only a quarter of the total cost of a data breach. These costs include forensic and investigative activities, audit services, crisis management and communications to management and board of directors. Cost such as database creation, determination of regulatory requirements, outside experts and secondary contacts with customers are all essential in the post-breach category. Even after the breach has been identified and customers notified, the biggest impact on the affected organization is the lost business. These costs include everything from brand damage and reputation losses to customer turnover rate and diminished goodwill from business partners.

Due to their roles and the architecture of systems that they maintain, system administrators and other business users that have privileged access have easy access to the most sensitive business data. For the financial services sector in the United States, it is obvious that the concerns associated with inside threats and potential damage from them are quickly climbing on the top of their security agendas. Insider threats have evolved from being only an IT issue and are becoming one of the biggest business issues that financial services have to deal with.

4. Regulatory Framework

4.1 Background

The events in the last couple of years have once again brought to attention debates on how to protect customers´ privacy in the digital age. From Edward Snowden´s intelligence leaks in the U.S. to new regulatory framework in Europe to security breaches in major retail and financial institutions, privacy has become the main concern for most people who expect their private data to be protected at all time. When that privacy is related to people´s money, the pressure that is put on organizations and their security professionals can become unbearable. However, many organizations do a poor job of identifying and classifying data based on their importance and sensitivity.

According to the Benchmarking the Accounting & Finance Function, a study from Robert Half and Financial Executives Research Foundation, the research affiliate of Financial Executives International (FEI), 99% of financial executives in the U.S. and 96% in Canada are certain that their compliance costs will rise or stay the same over time. Compliance-related burdens are also expected to rise which will put financial services industry in an even more unenviable position. Financial services are already struggling to recover lost income from their traditional revenue streams and dealing with sometimes contradictory regulatory compliance requirements is becoming an even bigger struggle.

4.2 SEC OCIE Cyber Security Exams

Financial institutions are faced with a constantly increasing number of complex cyber security risks and these trends have triggered an increased interest of United States Securities and Exchange Commission (SEC). SEC specifically focuses on financial institutions, hedge funds, and private equity managers. As it is clear that cyber security is a business challenge as much as an IT challenge, traditional methods of addressing cyber security risks are not enough. As a result, SEC´s office of Compliance, Inspections and Examinations (OCIE) released a sample document that details 6 areas that OCIE examiners plan to evaluate when conducting their cybersecurity exams.

1. IDENTIFICATION OF RISKS/ CYBER SECURITY GOVERNANCE

Types of documentation that may be requested include documentation of a cyber security governance structure and operating model, formal security P&Ps, and cyber insurance documentation. Apvera believes financial institutions have to demonstrate clear accountability in managing cybersecurity risks. Their IT need to have a deep understanding of their network composition, especially parts of it that are accessed by third parties. These organizations should consider conducting periodical reviews of their cyber insurance security in order to assure that their current cyber insurance meets their business requirements.

2. PROTECTION OF FIRM NETWORKS AND INFORMATION

Types of documentation that may be requested include documentation supporting the use of published cyber security risk management process standards, security controls (e.g., training and awareness, access management and certifications, data protection, DOS protection, secure software development life cycle), and compliance with P&Ps. Apvera believes organizations have to demonstrate their understanding of risk management and that their existing security architecture does a great job in protecting their data across the complete data lifecycle. SEC has also highlighted training as one of the key components of network and data protection which means that organizations need to implement controls to contain their data within their infrastructure.

3. RISKS ASSOCIATED WITH REMOTE CUSTOMER ACCESS AND FUNDS TRANFER REQUESTS

Types of documentation that may be requested include documentation of fraud controls (e.g., authentication and standard operating procedures governing fraud management). Apvera believes financial services should take extra care when connecting with third parties and their environments that they do not control. They need to enhance their monitoring capabilities to better differentiate between normal and anomalous behavior.

4. RISKS ASSOCIATED WITH VENDORS AND OTHER THIRD PARTIES

Types of documentation that may be requested include documentation of third-party security assessments and management of risks associated with vendors and other third parties. Considering the fact that key functions can be outsourced to third parties, it is important for financial organizations to establish a secure enterprise that incorporates an approach to managing risks associated with third parties.

5. DETECTION OF UNAUTHORIZED ACTIVITY

Types of documentation that may be requested include documentation for threat awareness, threat detection, event correlation, data loss prevention and vulnerability testing. One particularly challenging aspect of cyber risk management is determining that the measures designed to mitigate cyber security risks are consistent with the organization´s risk model. This will prevent the communication gap between cyber security professionals and information security officers which can lead to failure in identifying potential risks.

6. OTHER INFORMATION (EG. EXPERIENCES WITH CERTAIN CYBER THREATS)

Types of documentation that may be requested include documentation of prior security incidents (e.g., malware, spear phishing, rogue employees, and fraud), documentation of loss of client information and documentation of threat intelligence monitoring of insider threats and global threats. Tracking prior cyber incidents and loss of sensitive information, together with constant monitoring for insider threats can greatly help organizations in their efforts to better understand and remediate potential weaknesses in their security infrastructure.

5. Mitigating The Risks

Considering the fact that cyber threats are evolving very quickly, long-term implementation plans to address cybersecurity risks can become obsolete very quickly, as well. This is why it is very important for organizations to meet SEC expectations and invest in a program that will allow them to become secure, vigilant and resilient in dealing with both inside and outside security threats.

5.1 Risk and Compliance

Financial services need to monitor compliance but they need to address all threats in a timely manner with an equal amount of importance. This can be achieved with a flexible risk and control solution that will allow organizations to continuously monitor and identify new threats and prevent them from doing any damage. Additionally, regulatory compliance requirements should be centralized in order to achieve consistency. By doing this, financial services institutions can further reduce the overall cost of compliance and even provide compliance status for multiple regulatory compliance bodies.

Financial services should try to build a more holistic approach to data security which includes both the technology solutions for managing insider threats and a comprehensive data governance framework for compliance requirements. All data flow, both internal and external, should be identified and mapped to their organizational environment and control. Regular risk assessments should be done in order to identify gaps in security, followed by implementation of a roadmap to mitigate all possible risks. Strict regulatory compliance accompanied by a mandatory disclosure of data breaches requires financial institutions to be able to do comprehensive analyses of all such incidents. This can be done by investing a significant amount of time and money into building their own sophisticated threat mitigation solution or already available solution provided by a trusted partner.

5.2 IT Security Professionals

Financial services with their IT and security professionals should take steps in making sure that they are managing the new technology trends such as SaaS and BYOD as best as possible. All devices should be secure and pose no threat or risk to the organization. This is perhaps the biggest challenge that financial services are facing. From an almost closed system, they are quickly opening their gates and allowing access to everyone with a mobile device and an Internet connection. Financial services industry should incorporate a detailed threat assessment and management framework that will ensure that all risks are adequately managed. This solution should have clearly defined roles and responsibilities through an entire organization and periodic risk assessments that will effectively help them to mitigate risk and compliance.

6. Insider Threat Intelligence by Apvera

6.1 Types of Insider

In order to detect behavior patterns that could lead to a data breach, it is important to understand types of insider threats. Unauthorized access is when a user, employee in case of insider threats, tries to gain access to resources or networks that surpass their level of access. They may also begin using services that are in violation of their company policies, called policy violations. Before employees can extract data, they first need to store it and they can use programs to identify internal scanning activities. The other two commons threats are data loss when employees send a large amount of information outside of their network, and data hoarding where employees download and collect large amounts of data which can indicate an attempt to package and steal sensitive information.

Detecting all these behaviors early can mean the difference between thwarting a potential insider attack and becoming the victim of one. Appropriate situation awareness and identify anomalous network activity are needed to shut down an attack before it's too late. Unfortunately, it takes more than just technology to protect your business from insider threats.

6.2 Apvera Insight™

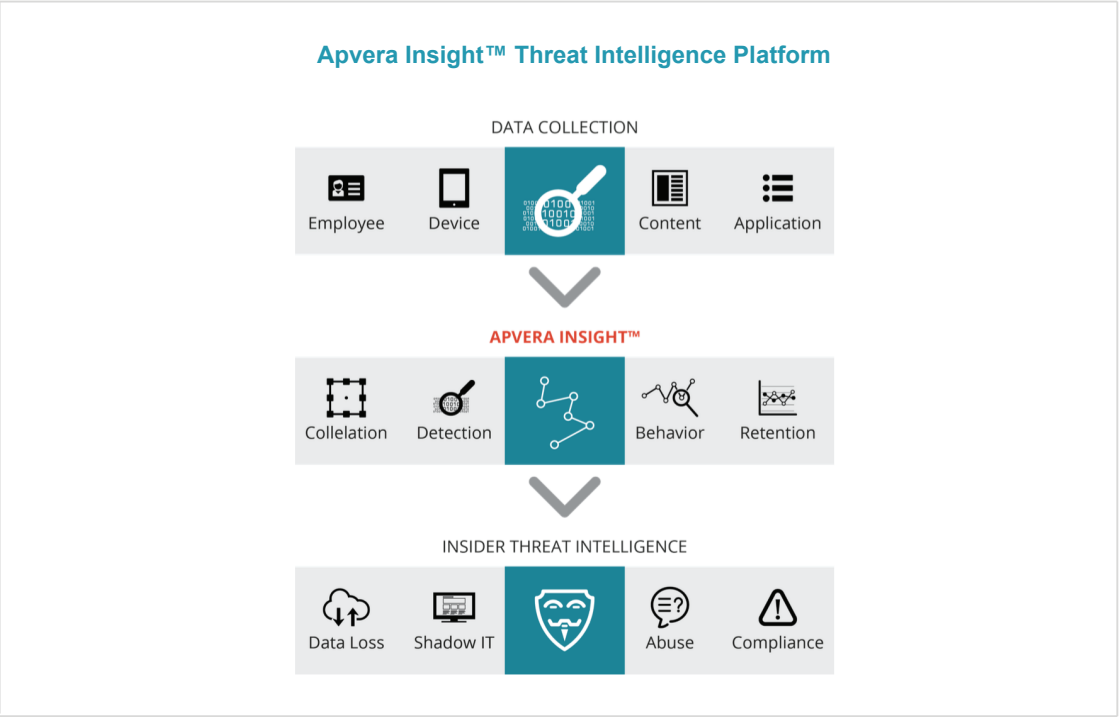
Understanding employees and their behavior is the key to determining possible insider threats. Apvera Insight™ enables financial services to create a self-learning profile of each individual user, device, content, and application in order to quickly identify deviations from normal behavior.

Employees are predictable as are their activities. Identifying deviances in their behavior over a period of time or compared to peers within a group can indicate fraudulent or malicious intent. With Apvera Insight™, behavior patterns for users, devices, and applications can be analyzed to reveal anomalies, even when they occur in very low frequency and over extended periods of time

Apvera Insight™ assesses the severity of all threats so enterprises can review them in real time and take immediate and automated preventive actions. The Apvera Insight™ platform supports the entire IT adoption life cycle, providing unparalleled visibility, usage analytics, and policy enforcement. With Apvera Insight™ in place, financial services and their employees can use both internal and external resources from any device while seamlessly enforcing organization´s data security, compliance and governance policies. This way, financial services, together with their IT and security professionals are able to manage new technology trends.

Apvera Insight™ is an intuitive, affordable and powerful insider threat solution for financial services as it enables them to constantly safeguard their environment and monitor it for any suspicious activity from employees, contractors, and vendors.

Apvera Insight™ offers context-aware, which means to identify employee behavioral patterns and reveal anomalous insider threats in an actionable manner reducing financial and data loss.



6.2.1 Collect and Learn

Apvera Insight™ sensor technology can be leveraged to seamlessly monitor huge volumes of data for potential threats. The platform delivers the pervasive visibility and security context needed to accurately baseline network behavior and pinpoint malicious activity. Its high scalability allows it to monitor even the largest and most dynamic networks such as financial services and their complex ecosystems

Collect & Learn

Gain real-time situational awereness of all users, devices and traffic on your network

Monitor contextual user activity from users, data and activities to devices and locations

Manage risks and guide users toward corporate approved cloud applications

In-depth security analytics uncover the unusual behaviours associated with APT

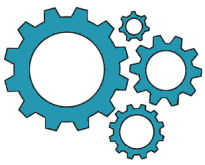
6.2.2 Analyze and Predict

Apvera Insight™ enables users to draw upon sophisticated deep behavior anomaly detection and analytics to identify threats that bypass conventional defenses. Providing a 360° view with a full audit trail of user and device activity, Apvera Insight™ allows users to pinpoint threats before they can evolve to devastating data breaches, inconsistent policies and security inconsistencies.

Analyze & Predict	
	Transform data into actionable security intelligence for detecting full range of threats
	Obtain updated security algorithms for advanced protection against today's top threats
	Easily drill down into massive amounts of data to pull out the most relevant intelligence
	Understand the who, what, when, where, why and how of compromised insider threats

6.2.3 Engage and Protect

Apvera Insight™ allows users to take quicker and more informed responses to a wide range of security issues. Automated mitigation features through Apvera preventative sensor technology enables users to take action by swiftly shutting down potential threats and enforce security policies to meet security, compliance, and governance requirements.

Engage & Protect	
	Quickly and effectively respond to threats, before, during, and after a security incident
	Enables enterprises to build a continuous response process for security threats
	Identify and prevent high-risk activities and anomalous behaviours
	Enforce consistent policies, enforce access control and extend DLP policies to cloud

7. Beyond Technology

While Apvera Insight™ covers all aspects of insider threats, there are still some things that companies can do to lower the risk associated with insider threats.

Background Checks and Screening

Organizations, especially financial services, should conduct thorough background checks before hiring their employees, contractors, and third-party vendors.

Partner Evaluation

Recent data leaks associated with contractors and payment card heists have proven once again that adversaries can and will infiltrate systems via third parties. However, most organizations do not address third-party security and can find themselves in situations where they are working with completely unprotected partners. Attackers can easily use these partners as the weakest link and access your network through their insecure systems.

Comprehensive Employee Exit Strategies

Most malicious insiders conduct their unsavory activities within the first 30 days of leaving the company. Organizations need to take extra care in ensuring that employees´ and contractors´ access to data and resources has been revoked immediately after resigning.

Management Training

Insiders that commit crimes often engage in certain behaviors before or during the commitment of their crime. Behaviors such as threatening the organization or bragging how much damage they could do, can be noticed by managers who are trained and educated to recognize such kinds of behavior. This way, organizations might be able to identify and prevent the threat before it could do any damage.

Employee Assistance

In some cases, personal and financial stress can motivate people to commit crimes at their working place. There are a number of steps and constructive approaches that organizations can take to handle these personal circumstances. For instance, establishing a confidential employee assistance program can be a source of comfort and advice for these employees.

8. About Apvera

Apvera is a next-generation security intelligence platform that helps organizations to mitigate compliance and risk by providing them with a way to get insight into users´ behavioral usage patterns within their environment while identifying all anomalies that can lead to malicious behavior. Corporate application usage has been gravitating toward SaaS adoption outpacing IT's ability to manage and deliver timely secure alternatives. The risk of security compromises is increasing alongside the number of applications that users leverage every day. As the number of vulnerabilities continues to grow, and an increasing number of attacks becomes public, a shift in mindset on how we deal with these attacks is fundamentally challenged. Enterprises are no longer able to rely on traditional preventative measures, but forced to innovate through other means of countermeasures.

Apvera helps companies understand enterprise security by focusing on user interaction levels and how relationships with services and applications may be deemed a threat; ensuring compliance with IT policies. By applying machine learning, Apvera leverages predictive analytics to understand the user behavior to precisely anticipate and prevent future security breaches by identifying irregularities in usage behavior.

apvera

UNITED STATES
2443 Fillmore St
Suite #380-7232
San Francisco, CA 94115

SINGAPORE
20 Maxwell Rd
Suite #09-17
Singapore, 069113

sales@apvera.com

+1 415 891 2270

+65 3158 8697