WHITE PAPER

Raytheon

The Financial Industry and the Insider Threat:
Total Awareness Leads to Secured Enterprise.

Through SureView® Insider Threat, financial and banking organizations monitor and analyze behaviors in real time, with complete context. Then, they eliminate risks posed by insiders.

The Problem: New Times. New Crimes. Same Thread.
For the financial industry, prospects for an "inside job" have existed as long as there have been banks – with every, single incident linked by one thematic thread: information.

Before the Digital Age, individual crooks, gangs or even major syndicates cultivated alliances with disgruntled bank tellers, security guards and other vulnerable employees. The employees shared enough insights to circumvent alarm systems, or break into a vault, or intercept a Brink's truck filled with money to deliver.

Back then, the illegal activity was limited to a very narrow window of time, as the thieves could only steal so much before they'd have to flee. And therein lays a major difference between the inside job of then and now.

Today, insiders are still passing on information to the bad guys, frequently in the form of proprietary and otherwise sensitive data. We can consider mobile devices as the modern day equivalent of those Brink's trucks – out and about all over the map, and operated by users whose practices lead to exposure. The alarm system is now a cybersecurity program which too often depends upon an inadequate hodgepodge of firewalls and patches, transforming the IT network into a susceptible "vault" ripe for the modern version of the inside job.

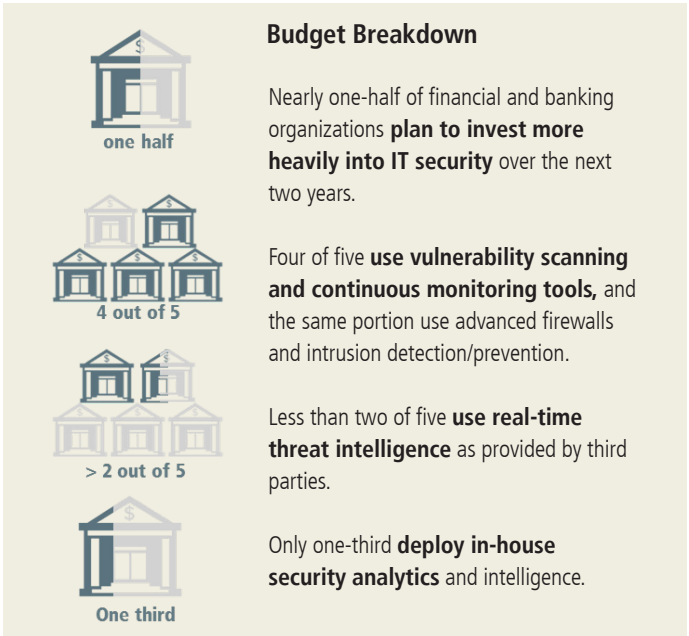

Figure 1 Budget Breakdown:[1]

More than one-half of organizations overall have experienced an insider cybercrime incident, according to the 2013 U.S. State of Cybercrime Survey from the CERT Insider Threat Center at the Carnegie Mellon University Software Engineering Institute. That's up significantly from 41% in 2004.[2]

As with prior generations, the insiders are still disgruntled, yet they've armed themselves with intimate knowledge of an enterprise's business practices, systems and applications. Assuming they're in good standing, they're considered "trusted" members of "the team." That means they're capable of causing far greater damage than their counterparts of yesteryear, over an indefinite stretch of time. They don't require a liaison from the underworld to initiate action either; many of the lowest of staffers are technologically proficient enough to steal funds and/or proprietary data on their own. They can create more losses than external threats because they have full access to systems with minimal – if any – restrictions to overcome.

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.

The findings raise red flags. Nearly one-quarter of survey respondents say that abuse on the part of internal employees or contractors presents the biggest source of security concerns within their organization (ranking it #1 among all risks), and a mere 16% feel "very" prepared to fend off intrusions aimed at financial systems and accounts.

As a result, the financial sector experiences the most cases of fraud, and the second most in IT sabotage and theft of intellectual property perpetrated by malicious insiders, according to CERT. In addition, there are the users who introduce risks inadvertently, through ill-conceived behaviors which external parties readily exploit. These users can be "tricked" into clicking on a malware-containing URL, and infecting the network. Or they'll lapse into sloppy habits, such as sending corporate materials to their home computers on vulnerable, private email accounts. In fact, the majority of professionals admit to emailing business documents from their workplace to their personal email, and most of them never delete the data after transferring it, further inviting risk.[3]

1 Risk, Loss and Security Spending in the Financial Sector: A SANS Survey

2 http://resources.sei.cmu.edu.

3 http://www.symantec.com/about/news/release/article.jsp?prid=20130206_01&om_ext_cid=biz_socmed_twitter

While insiders represent just under one-fifth[4] of all security incidents, they can cause more problems than external adversaries. They're already "behind the firewall," entrusted and even empowered to take initiatives and pursue day-to-day objectives which could cloak less-than honorable intent. Regardless of the legitimacy of their motivations, they'll access sensitive or internal information simply as part of the "normal" aspects of their routines.

Breakdown of Insider Threats

2013 incidents report

Number of reported global breaches: **1,300**
Portion attributed to insider threats: **8%**

Number of reported security incidents: **63,000**
Portion attributed to insider threats: **18%**

Figure 2. Overall Breakdown of Insider Threats[5]

When the worst happens, institutions struggle to assess how much these crimes cost them, as one-half of the Raytheon/SANS survey respondents admit that they can't quantify their losses after an attack. When they can, the numbers are quite unsettling. The average amount of loss per insider cyber case within the financial sector surpasses[6] $750,000, according to CERT.

Because of the ability to go undetected, the rogue employee and/or adversary partner can compromise the network indefinitely, removing as they wish, information related to credit-card accounts, monetary assets and confidential data. An average of five years will pass between the hiring of an employee who will commit insider threat and the start of the fraud, allowing much time to build a false sense of trust. Then, the employee will enjoy a wide-open window – 32 months on average – from the launching of the fraud plan and its eventual detection.[7] Give financial-industry insiders at least 32 months to "hide in plain sight," and they'll commit an average of 58 individual thefts.

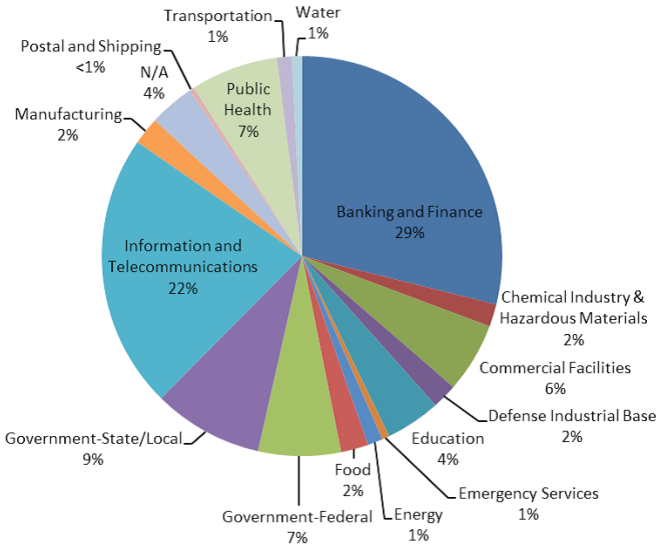

Figure 3. Banking and Finance Industry Leads All Sectors for Insider Threats:[8]

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.

Figure 4. Insider Threats of the Financial Sector [9]

4 http://www.verizonenterprise.
5 Verizon 2014 Data Breach Investigations Report
6 http://www.sei.cmu.edu/reports
7 http://www.sei.cmu.edu/reports

8 The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud) http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=30310
9 http://www.sei.cmu.edu/reports/12sr004.pdf

The stakes are high, especially given the unique challenges impacting this industry. With their influence on local, domestic and global economies, financial institutions must comply with a long list of regulatory standards with respect to the SEC, the Gramm–Leach–Bliley Act (GLB) and others. They have to incorporate judicious procedures to collect and manage their customers' personally identifiable information (PII). They need to stand vigilant against both insider and rogue trading. The latter will dig a company into a deep, monetary hole, triggered when an employee covers up a mistake by not reporting it, subsequently making poor decisions to conceal the original trading error. Losses then accumulate with every, subsequent action to "cover up the mess." A long list of rogue traders have duped many a venerable organization, including Kweku Adoboli, whose deceptions caused $2.3 billion[10] in losses for UBS; and the "London Whale," a.k.a. Bruno Iksil, whose losses reached $2 billion at JPMorgan Chase.[11]

All of which speaks to the urgency for better solutions – solutions to confront these threats head-on, as part of a decidedly proactive, multi-layer plan that combines advanced monitoring, visibility, analytics, prevention and mitigation.

In this white paper, you'll learn how these institutions can assemble such a plan, and how the ensuing, enhanced visibility into internal user behaviors swiftly establishes a profound sense of assurance and even confidence. And you'll understand that tech alone cannot deliver these outcomes, that insider threat efforts must match IT innovation with human insights.

The Solution: "Easy Button" Falls Short

As for an answer, there is an "easy button" to press, and many companies are doing just that, by going out and buying a prevention/detection product. Plug it in, play and forget about it, right? Unfortunately, they soon discover that the easy button no longer suffices in today's environment.

That's because an exclusively tech-driven approach will always fall short. Certainly, IT solutions matter, as does the tech department's valued input. But both must align with business-side executives and users to address all entry opportunities for the insider threat while not disrupting productivity and/or diminishing brand reputation/strength.

Indeed, a successful insider threat program thrives upon a step-by-step, multi-layered execution strategy. The strategy should be so embedded within daily activities, that it's perceived as part of the corporate culture as opposed to a "necessary evil" forced upon users from IT. When the program reaches this level of internal acceptance, it fosters a universal awareness about not only what needs to get done, but why it needs to get done. Such awareness is in short supply today. A staggering 38% of the The SANS Institute survey participants don't know how much of their IT budget is spent on security. Keep in mind that these participants were CIOs, IT security managers, security analysts and other key tech-side professionals. One can expect the percentage to be far lower outside the IT department.

Without augmented awareness, our financial institutions increase their exposure. To avoid this, they have to go beyond the traditional standards of assigning privileges, controlling authorization and targeting outside threat vectors. They have to engage in more than solely post-event audit controls. Leadership has to enact policies and processes that demonstrate a realistic understanding of people's behavior. Without the human factor, the solutions will remain woefully lacking. While technology introduces new threat vectors, the technology itself doesn't initiate the problems. Human behaviors do.

A fully integrated, enterprise security environment reigns supreme here, and support must come from the very top leadership levels. The CEO announces the program launch, and C-suite members give top-down direction for immediate and long-term goals. A business case will determine any expected metrics-based ROI outcomes. All stakeholders – board members, the legal department, HR and, of course, IT – will be brought on board in the very beginning stages.

In the following sections, we will guide you through the nine critical steps of a comprehensive threat management program, and illustrate how emerging tech innovation from Raytheon is empowering organizations to implement a rigorous, 24x7x365 auditing/monitoring program to detect, mitigate and prevent insider threats.

The Nine Critical Steps of Insider Threat Management

1. Implementing an Integrated Approach

First, let's debunk a bit of a myth, that managing insider threats is about "events." It's not. Because when the situation at hand is about an "event," the damage is done.

Instead, think of managing these threats as a process, a continuous cycle of policy review/implementation, along with monitoring, auditing, mitigating and remediating.

10 http://www.businessweek.com/news/2013-12-13/ubs-wins-dismissal-of-suit-over-2-dot-3-billion-rogue-trader-loss

11 http://en.wikipedia.org/wiki/2012_JPMorgan_Chase_trading_loss

With this, your organization can assess which solution will work within current (and forecasted) scale, in addition to the cultural dynamics. The latter directly addresses the crucial human aspects of the program. Effective monitoring will get at the root of the threat while focusing on behaviors. Beyond detecting the wide range of threats, it will provide context. Only then can the insider threat program team pursue efficient and appropriate remediation, whether it's training users, counseling individuals, enacting stronger policies or conducting more thorough investigations.

When you operate within this enterprise-wide view, you'll remove the burden of added complexities and costs—not to mention the greatly increased potential for error—which result from building separate systems for perimeter and desktop/mobile environments.

To respond to the urgency for a "big picture" perspective, we've developed Raytheon SureView® Insider Threat, an integrated solution which monitors your entire enterprise ecosystem without disrupting business continuity. Its implementation and ongoing life cycle have minimal impact on the existing IT infrastructure and never diminish a user's experience. Yet, it delivers incredibly powerful and cost-beneficial protection, with a solution revealing questionable behavior and resolving serious incidents that could place your organization at risk.

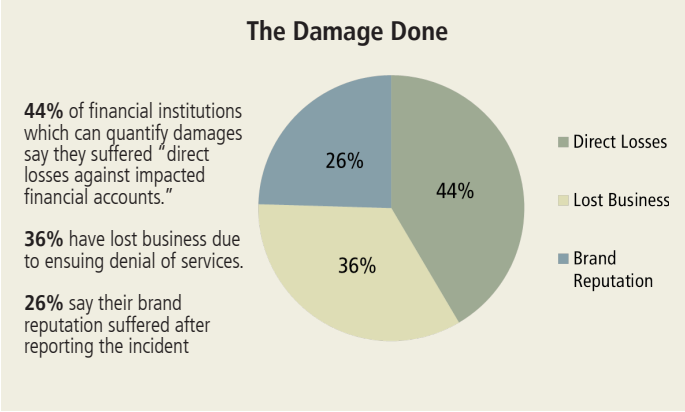

Figure 5. The Damage Done:[12]

SureView Insider Threat's platform detects and prevents insider (as well as external) threats with the following support:

- ***Threat elimination.*** SureView Insider Threat establishes the broad monitoring of your data and assets for risk indicators. If a violation is detected, it further targets specific events for investigation and produces complete context in the form of video replay.

- ***Total coverage.*** Only SureView Insider Threat can thoroughly track all communication vectors at the endpoint to detect threats normally hidden by encrypted traffic and files, and continue monitoring while desktops are offline. Since SureView Insider Threat is on the endpoint, it brings clear-text visibility of encrypted email, files and web sessions which are collected immediately pre-encryption and/or post-decryption. Its sophisticated engine even allows you to monitor threats composed of linked yet seemingly harmless individual actions.

- ***Contextual, actionable awareness.*** SureView Insider Threat monitors endpoint communications and applications in real-time. It also generates the details, insight and context to assess the severity of the incident, fix the problem and build the policies to stop it from happening in the future.

- ***"Real" event identification and enterprise scalability.*** SureView Insider Threat's policy engine and analytics minimize false positives and false negatives. It strictly monitors what the deployed policies specify, and its ability to create fine-grained policies keeps you from sifting through thousands of non-substantive alerts to find the "real" events. Built for speed and simplicity of deployment, SureView Insider Threat scales easily to large enterprise installations.

2. Targeted Investigations

Insider threats do not occur in isolation. Someone within your organization started a chain of events which resulted in the issue. SureView Insider Threat can provide the investigative tools to target and investigate everything that happened before – and after – it occurred. It delivers context, including DVR-like incident replay. You will not only pinpoint the root cause of the issue, but you'll confidently take the appropriate measures to fix it.

To track insider trading, for example, SureView Insider Threat looks for communications containing ticker symbols, access information linked to stock-trading websites and other trading-related data. It compiles and records each of these events, "telling the story" of all related user activities in context. Thus, management is equipped with the background necessary to determine if the user's behavior was inadvertent or malicious, and whether disciplinary and/or legal action is required.

3. Protect Intellectual Property

Intellectual property represents perhaps the most important asset of a financial institution. If compromised, the organization can lose market exclusivity and competitive advantage, which will hurt the bottom line. SureView Insider Threat discovers when intellectual property is leaked or stolen via accidental or

12 Risk, Loss and Security Spending in the Financial Sector: A SANS Survey

deliberate methods — whether via email, clipboard cut-and-paste, screen captures, printing, copies to USB drives, etc.

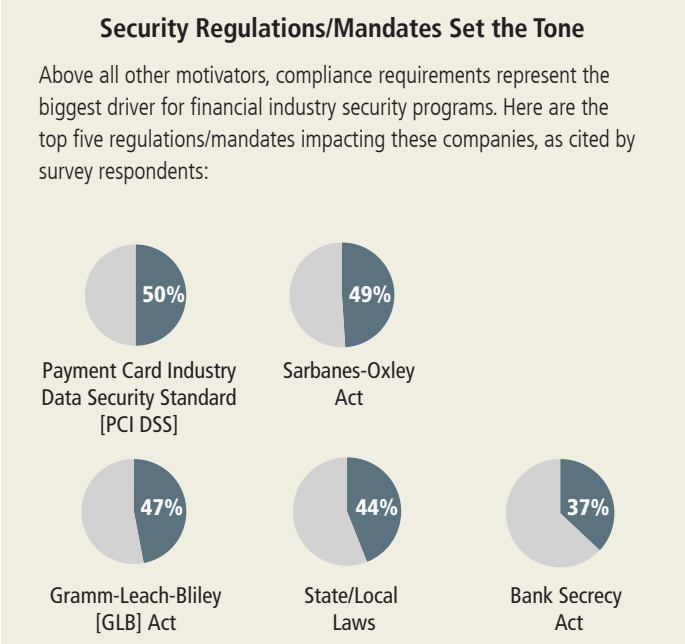

Figure 6. Security Regulations/Mandates Set the Tone[13]

SureView Insider Threat will detect tampering even if the computer is detached from the network, the files are encrypted, or some other type of evasion is attempted. Unique features such as disconnected caching and event-correlating analytics will unravel the most complex activity.

4. Prevent Customer Data Theft

Global financial institutions store millions of confidential customer records. Whether accidental or deliberate, a loss could make devastating impact upon the stock price, brand reputation and bottom line. Often, third-parties will have authorization to customer databases, thereby elevating exposure to risk. SureView Insider Threat extends throughout the enterprise and to these third-party groups, with policies measuring leading indicators of vulnerability. These vulnerabilities include large volumes of unmonitored USB drive copies, off-hours printing of customer records, changes to Society for Worldwide Interbank Financial Telecommunication (SWIFT) messages or customer data being sent unencrypted or encrypted. Any one of these individual incidents can be replayed, so that the appropriate remediation can be taken. SureView Insider Threat will record whenever customer data is being "cut and pasted" between applications using the clipboard; send an alert if instant messages are transmitted while the user has the customer database open; and enable additional monitoring if a user deliberately disables a network connection to hide illicit actions. With this intelligence, it can help you build more vigilant policies for third-party associations.

5. Detecting Fraud

Those who commit fraud go to great lengths to hide their tracks, or disguise the activity so it looks legitimate. SureView Insider Threat's rich incident documentation and video replay allow the administrator to easily distinguish ordinary behaviors from potential fraud, minimizing false positives. One real-world example: A bank's computer programmer took advantage of his privileged access to log on remotely to a branch manager's desktop, and installed a logger program to collect all keystrokes. Once the branch manager accessed her desktop, the programmer successfully captured her user ID and password, and copied it to a network file share to retrieve later. He then remotely accessed her desktop to copy and encrypt the identification number and password of a major, billion-dollar corporate account. Next, he uninstalled the keystroke logger from the branch manager's desktop and removed the event log for the entire sequence to cover his tracks.

His intent was to divert funds from the hijacked account to his own. However, thanks to SureView Insider Threat, the bank had implemented policies and practices which led to the detection of the programmer's remote logon to the branch manager's desktop. Further reporting tracked his installation and removal of the keystroke logger; his copying and pasting activity to a server; and his emailing of encrypted information after business hours. The sophisticated pre-built policy engine monitored, captured and reported on every one of these seemingly isolated events for targeted investigation, and the bank was able to step in before any crime occurred. With SureView Insider Threat's replay, the complete, suspicious sequence on the part of the programmer was viewed in context, which supplied powerful evidence and grounds for successful prosecution.

6. Monitoring and Controlling High-Risk Users

Clearly, the large majority of workers don't seek to commit fraud. So SureView Insider Threat distinguishes accidental violations, as well as deliberate yet non-criminal policy infringements (because a staffer may not harbor ill-will, but could still cut corners to accomplish an assigned task). Still, there are those who — due to their job function — could use their privileged credentialing to intentionally harm the company. Since they pose this degree of threat potential, they merit greater scrutiny. To protect the data, SureView Insider Threat ships with a pre-built policy pack designated for high-risk, privileged users, to monitor application logons, creation of user accounts and log file access.

13 Risk, Loss and Security Spending in the Financial Sector: A SANS Survey

Over time, SureView Insider Threat transforms the corporate culture, through better policy oversight so the management team knows when policies are broken at any level. This results in a reduction of incidents, while requiring less resource allocation.

7. Enhancing Compliance

More than ever, the financial industry faces regulatory pressures – seven of ten respondents in our survey cited the need to demonstrate compliance as the primary driver behind their security program. That's more than any other motivating factor, over the avoidance of data breaches, the reduction of risk and the general improvement of information-assurance posture.

SureView Insider Threat solutions ensure regulated data is protected and compliance is enforced. They monitor communications and documents containing credit data and PII throughout desktop channels, including non-network activities such as printing and sending copies to mobile storage. You can incorporate pre-built policies so regulated data is not transmitted in instant messages, and send alerts to appropriate managers if large volumes of customer data are sent to a printer. You can track customized billing databases and customer monitoring applications. Armed with context of any violation in the form of full documentation and video replay, the chief compliance or security officer then takes informed action to minimize future incidents. This could involve a standard user prompt to notify the policy violator, or, if needed, the outright blocking of specific, high-impact activity.

8. Document Fingerprinting

SureView Insider Threat will fingerprint an organization's critical intellectual property or sensitive document library. Particular to financial institutions, this covers electronic proof of funds (POFs) and verification of deposits (VODs). Most current technologies simply hash high-risk documents and compare the stored hash with files as they leave your network — a process easily circumvented. It just takes a word change or an extra period to significantly alter the hash value of the newly changed document, allowing its misappropriation to go undetected. Therefore, these technologies only determine misuse if the entire document is copied. To overcome this, SureView Insider Threat identifies fractional movements within a fingerprinted document, flagging abusive behaviors and capturing sensitive document changes before encryption or deletion.

9. Monitoring Mobile Users

The monitored user may include employees and contractors performing the roles of system administrators and operations specialists, as well as users with privileged access.
In today's increasingly mobile society, some of these users will undoubtedly work off-site remotely with authorization to privileged systems and information. They could connect via public or private networks, or work offline.
The majority of organizations feel that endpoint visibility is important, our survey shows, but only 42% are conducting endpoint monitoring. When the endpoints are as scattered – and subject to increasingly user-dictated operating systems and applications due to mobility/Bring Your Own Device (BYOD) – the lack of endpoint accountability cannot continue. With SureView Insider Threat, it won't. The solution uniquely monitors mobile users at their endpoints, identifying policy violations and collecting events, whether mobile users are connecting or not.

Conclusion: Greater Confidence, Greater Trust

Ultimately, a comprehensive program builds confidence throughout an organization. Users will go about the business of serving customers by opening checking accounts, offering low-interest credit cards, managing retirement portfolios, etc., entirely certain that the program team is proactively safeguarding the company from all internal rogue activity. They know that – should a colleague unwittingly download malware which could disrupt operations – the team will swiftly spot the compromise and stop it in its tracks. This cultivates a welcome sense of trust enterprise-wide, with managers and employees comforted that any data for which they're responsible – including everything generated by proprietary documents, fiscal reports and customer products – is protected. And they realize that none of the added measures will interfere with their ability to do their jobs.

Raytheon's SureView Insider Threat is the ideal solution for insider threat detection and prevention. It sets the standard for enterprise monitoring, investigations and policy enforcement, mitigating intellectual property theft, data loss and other threats while successfully pursuing deep forensic investigations into known violations and incidents via:

- Industry-leading, **continuous endpoint monitoring and incident reconstruction** with the SureView Insider Threat endpoint agent, which was developed and tested in our country's most critical, federal networks.
- The first and only **DVR-like incident replay** capability.
- Hundreds of **pre-built policies** covering intellectual property and customer data protection, fraud prevention, privileged user monitoring, corporate governance enforcement and legal compliance demonstration.

In prior decades, authorities could not command the state of awareness which they can now. This often put them in the position of reacting to inside jobs only after the crime was committed, by investigating witnesses and other parties in an attempt to find the likely culprit.

Today, organizations can adopt a much more proactive approach. They can disarm insider threat parties in advance, because the one "weapon" the parties need – information – will no longer serve its purpose. Not when the threat team already knows everything the insiders know, and are taking action to thwart their intentions before they have a chance to begin. And that is when a financial institution proves itself worthy of the trust of its users, managers, partners and customers.

About Raytheon Cyber Products

Raytheon Cyber Products and its SureView family of cybersecurity solutions deliver end-to-end visibility that allow organizations to detect, contain and control cyber threats. For over two decades, we've leveraged Raytheon's cyber expertise and research & development resources to deliver technologies that bridge the gap between defense-grade and enterprise cybersecurity.

Additional References

FBI/Cert Investigations Tips
http://www.cert.org/tech_tips/FBI_investigates_crime.html

High Tech Crime Investigation Association
http://www.htcia.org/

Department of Justice Cybercrime Information
http://www.usdoj.gov/criminal/cybercrime/searching.html

For further information contact:

Intelligence, Information and Services
Cyber Products
12950 Worldgate Drive, Suite 600
Herndon, Virginia
20170 USA
866.230.1307

www.raytheoncyber.com

Raytheon

Customer Success Is Our Mission