Non-Standard Behaviour Detection and Risk from Insider

Speaker: Pramod Bhatt
Email: pramod.bhatt@yahoo.com
+91 98201 90842

5 December 2013

Speaker Bio

Pramod is a seasoned professional with over 17 years of experience in the field of security and Intelligence. Earlier, he headed Protective Intelligence practice of Deutsche Bank in South Asia. He was intelligence advisor to regional and country heads of Physical Security, Anti-Fraud, Cyber Forensics, Executive Protection, Business Continuity and Crisis Management in Asia Pacific region.

Prior to this, Pramod worked as a risk management consultant in South Asia. He consulted a number of Fortune 500 companies from banking, mining, oil and gas, construction, ITES, automotive and philanthropy sector to help them combat the business and operation risks prevalent in Asia. Before his corporate career, Pramod commanded an intelligence unit of Indian Army.

Pramod is an alumnus of Risk Leadership School London and Indian Institute of Management Ahmadabad. He is also a trained criminologist. Pramod has spoken at several international events such as Strategic and Competitive Intelligence Professional (SCIP) Conference in the USA, ASIS International conferences in the USA and Malaysia, CSO Round Table in Malaysia, Asia Crisis & Security Group in India and Competitive Intelligence Conference in India. He also delivered guest lectures at premier institution such as Institute of Management Studies and Tata Institute of Social Science.

http://www.linkedin.com/in/pramodbhatt

Insiders Risk

Insiders?

- Who are the insiders?
- Why do they steal/damage information?
- How do they steal/damage information?
- How is it detected?
- How to indentify insider?

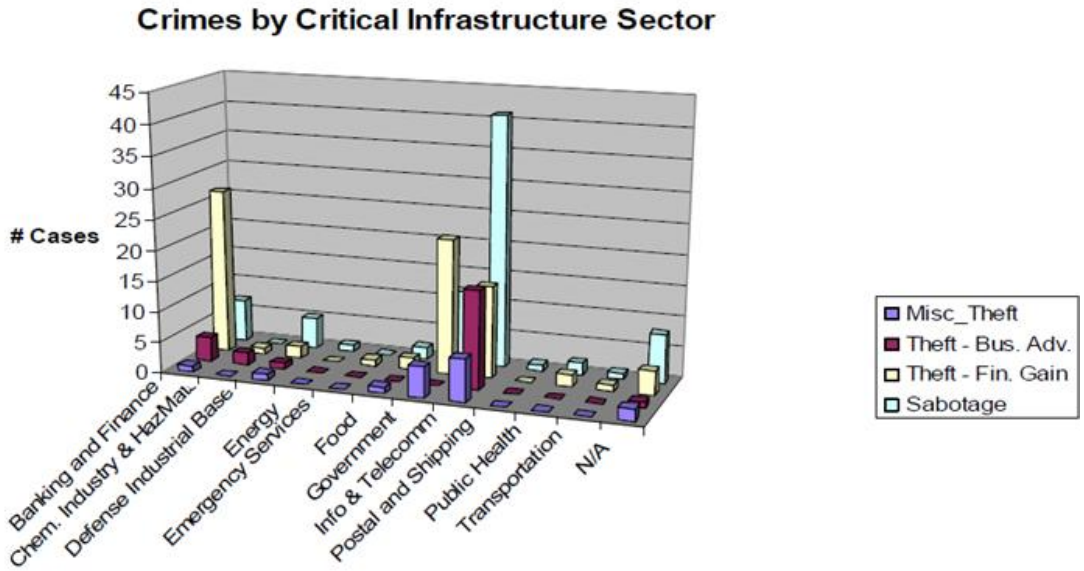
Who are Insiders?

A current or former **employee, contractor**, or **business partner** who has or had **authorized access** to an organization's network, system, or data and **intentionally exceeds** or **misuses** that **access** in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.

Why do they do it?

Intentions:

- **IT sabotage:** To harm a specific individual or organization.
- **Theft or modification for financial gain**
- **Theft or modification for business advantage**
- **Miscellaneous:** Not motivated by financial gain or business advantage.



Breakdown of Insider Threat Cases** (190 cases were analyzed by CERT)

Source: Carnegie Mellon University

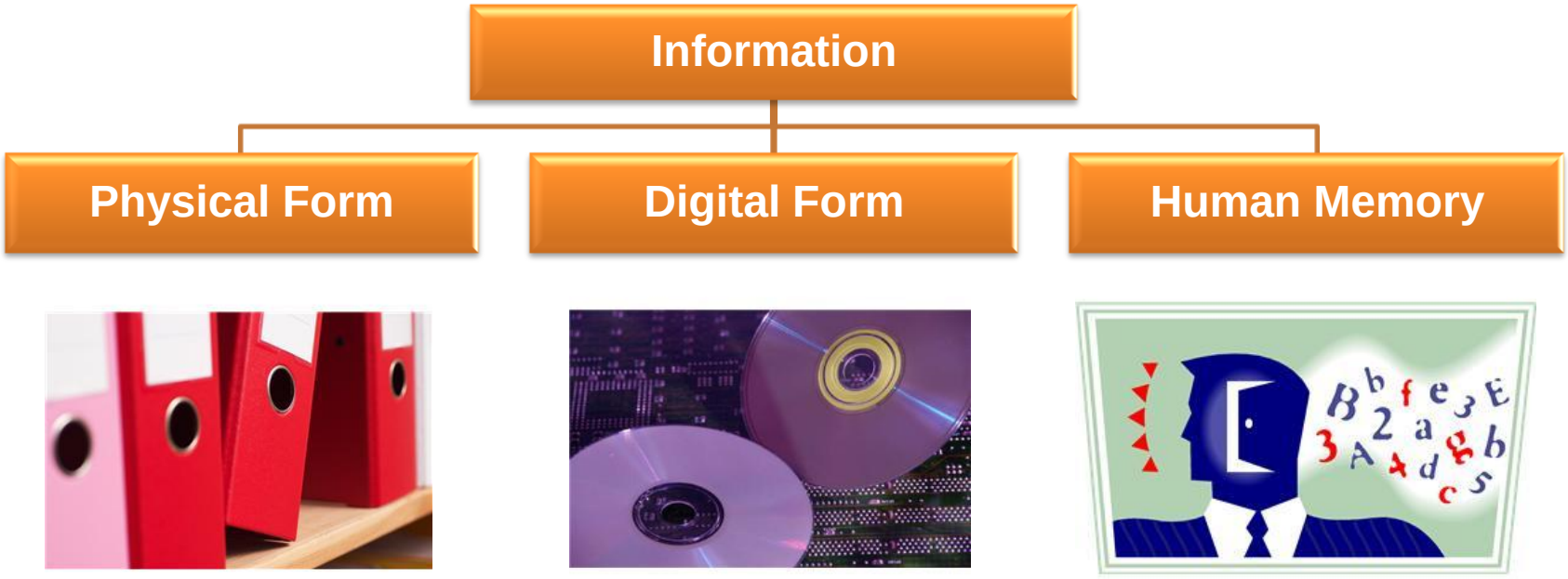
Trends: Risk from Insider

	IT Sabotage	For Financial Gain	For Business Advantage
Current/former employee	Former	Current	Current
Type of position	Technical (e.g. system administrators or database administrators)	Non-technical, low-level positions with access to confidential or sensitive info (e.g. data entry, customer service)	Technical (71%) - scientists, programmers, engineers; Sales (29%)
Gender	Male	Equally split between male and female	Male
Target	Network, systems, or data	Customer or Personally Identifiable Info	Intellectual Property – 71%; Customer Information – 33%
Access used	Unauthorized access	Authorized access	Authorized access
When	Outside normal working hours	During normal working hours	During normal working hours
Where	Remote access	At work	At work
Recruited by outsiders	None	Half recruited for theft; less than one third recruited for modification	Less than one fourth
Collusion	None	Almost half colluded with another insider in modification cases; 2/3 colluded with outsiders in theft cases	Almost half colluded with at least one insider; half acted alone

Source: Carnegie Mellon University

Security must Facilitate, not Hinder, Business

Information and Insider



Information Protection from Insider

Physical Form	• Monitor and secure the physical environment • Document controls - printing, accountability and destruction • Document classification • Clean desk policy etc.
Digital Form	• IT access control – trace access path; approval process etc. • Strict password and account management policies • Enforce separation of duties and least privilege • Log, monitor, and audit employee online action • Deactivate computer access following termination etc.
Human Memory	• ***Address Behavioural Aspects***

“Best practices for mitigating insider risks continue to evolve – Let’s contribute!!!”

Addressing Behavioural Aspects

Training and Controls

- Communication, Education, and Training
- Policies and Other Controls etc.

Monitor and Respond

- ***Develop Non-Standard Behaviour (NSB) Indicators***
- ***Develop tools to monitor NSB Indicator***

Fictitious Case (NSB): Info Theft For Business Advantage

Time: 10 minutes

Mr Keen Kumar, an employee of Zoom Investment Bank (ZIB), manages big ticket clients. He is among few employees who has been with the bank for more than 10 years. Keen Kumar do not possess a business degree but he worked very hard and started handling big ticket clients. Meanwhile ZIB grew at a fast rate and recruited several new client managers. Bank also hired Miss Smarty, a business graduate from one of the top business school, as Head of Private Banking to manage the expanded team of client managers.

All client managers, including Keen Kumar, had to report to Miss Smarty. Prior to this Keen Kumar, being the senior most client manager, use to report to Country Head of ZIB. He also had access to confidential business info such as clients' info, marketing data and business research report.

When Smarty was recruited to lead the team, Keen Kumar started feeling confined to his current role. He started receiving instructions on how to manage clients and felt micro-managed. After about four weeks, he started expressing dissatisfaction to his colleagues for not being considered to lead the team. He also missed an important training organised by Smarty for all client managers. Meanwhile Miss Smarty added a layer of governance that restricted access to Bank's client and business data – access needed approval of Country Head. She asked all client managers to send her a list of bank's propriety databases to which they had access/ need access along with explanation.

Following this, Keen Kumar was found to be rarely coming to office. He was mostly on client meetings outside bank and use to complete most of his regular office work from home. Even though his client meetings expenses have increased, his performance started declining. Bank lost some of the big ticket clients, who were being handled by Keen Kumar. When Miss Smarty met him to discuss the issue of loss of clients and sudden decline in his performance, he behaved rudely and had heated argument with her. Following this, Keen Kumar cancelled his summer vacation. He stayed late night in the office stating that he is working hard to improve his performance.

After one week Keen Kumar resigned from ZIB and did not divulge the name of new company which he was planned to join. After a few weeks he joined At Your Service Bank (AYSB), the ZIB's rival bank. In next few weeks, ZIB started loosing their clients to AYSB.

Miss Smarty instituted an investigation to find the reasons of loss of big ticket clients. Investigation revealed that Keen Kumar had access to confidential client and business data exceeding his authorised limit. Keen Kumar accessed this data from home and emailed it to his personal email ID, which he later deactivated. He also printed a number of confidential documents containing client information before he resigned. His expense sheets revealed that he met a number of clients who later defected to AYSB.

Please answer and ready to discuss the following question. Please follow SMART (Specific, Measurable, Attainable, Relevant, and Timely) technique to answer the question:

1. **Identify Non-Standard Behaviour (NSB) indicators in this case.**
2. **What are the various methods to monitor/track these NSB indicators?**

1. Non-Standard Behaviour (NSB) Indicators

Solution: Be ready to discuss your solution during the session

“Best practices for mitigating risks from insider continue to evolve – Let’s contribute!!!”

2. Methods to monitor/track NSB indicators

Solution: Be ready to discuss your solution during the session

“Best practices for mitigating risks from insider continue to evolve – Let’s contribute!!!”

Solution: Info Theft For Business Advantage

Non-Standard Behaviour (NSB) Indicators	Methods to monitor/ track these indicators	
	Tracking of NSB Indicators	Monitoring Tool/Use of tech

Conclusion