Insider Predictive Analysis Knowledge System (IPAKS)

Tom Bracewell
Senior Director Insider Threat
Concurrent Technologies Corporation
571-388-6029
bracewet@ctc.com

Insider threat is a risk to national security

- The insider is the main risk to classified systems
- The President recently ordered agencies that operate or access classified computer networks to implement an insider threat detection and prevention program
  - Executive Order 13587, October 2011

A risk to business and critical infrastructures

- Insiders have put businesses out of business
- Insider incidents cost more than breaches
- Incidents have been reported in power and sewage treatment systems

What defines an insider?

- Insiders have knowledge, access and a trust relationship with their enterprise that outsiders lack
- Malicious insiders commit IT sabotage, theft and fraud
- Benign insiders seek to do no harm, but can
- We often use the term ‘insider’ to mean ‘malicious insider’

Why insider threat is a hard problem

- Insider threat is one of the 8 hardest and most critical challenges that the information security research community must address*
- Access, knowledge and trust help the insider succeed
- Insider attacks are hard to detect
- We must predict, deter and look for malicious behavior

* INFOSEC Hard Problems List, 2008

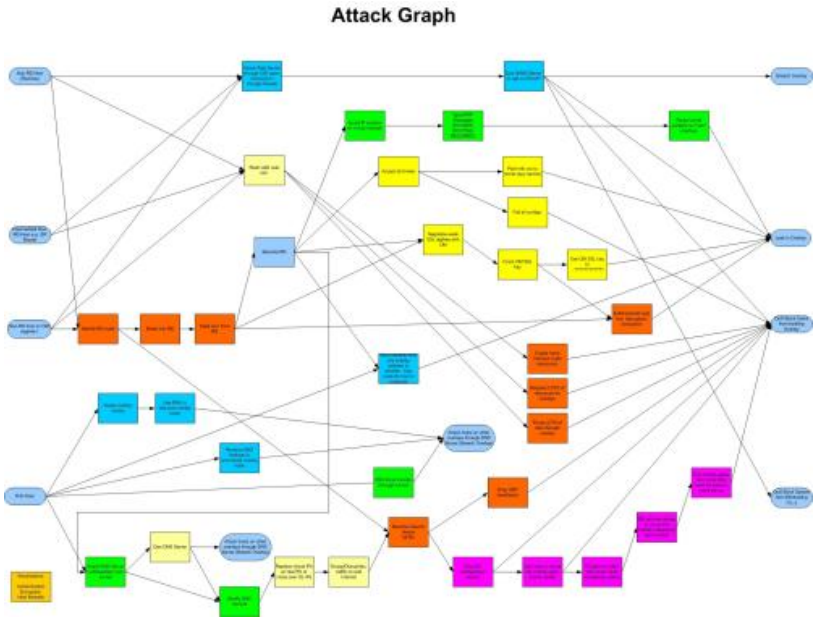
Insiders have advantages

- No need to engage in rule-breaking behavior
- Act in obscurity for long periods of time
- Collude with other insiders
- Subvert audit trails to cover their tracks
- Masquerade as other insiders

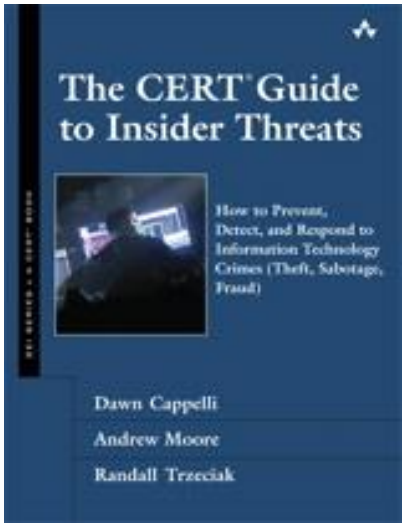
An attack may follow many paths

- An attack path is a series of steps that an insider may take to achieve a malicious goal

- Many different attack paths may reach the same goal

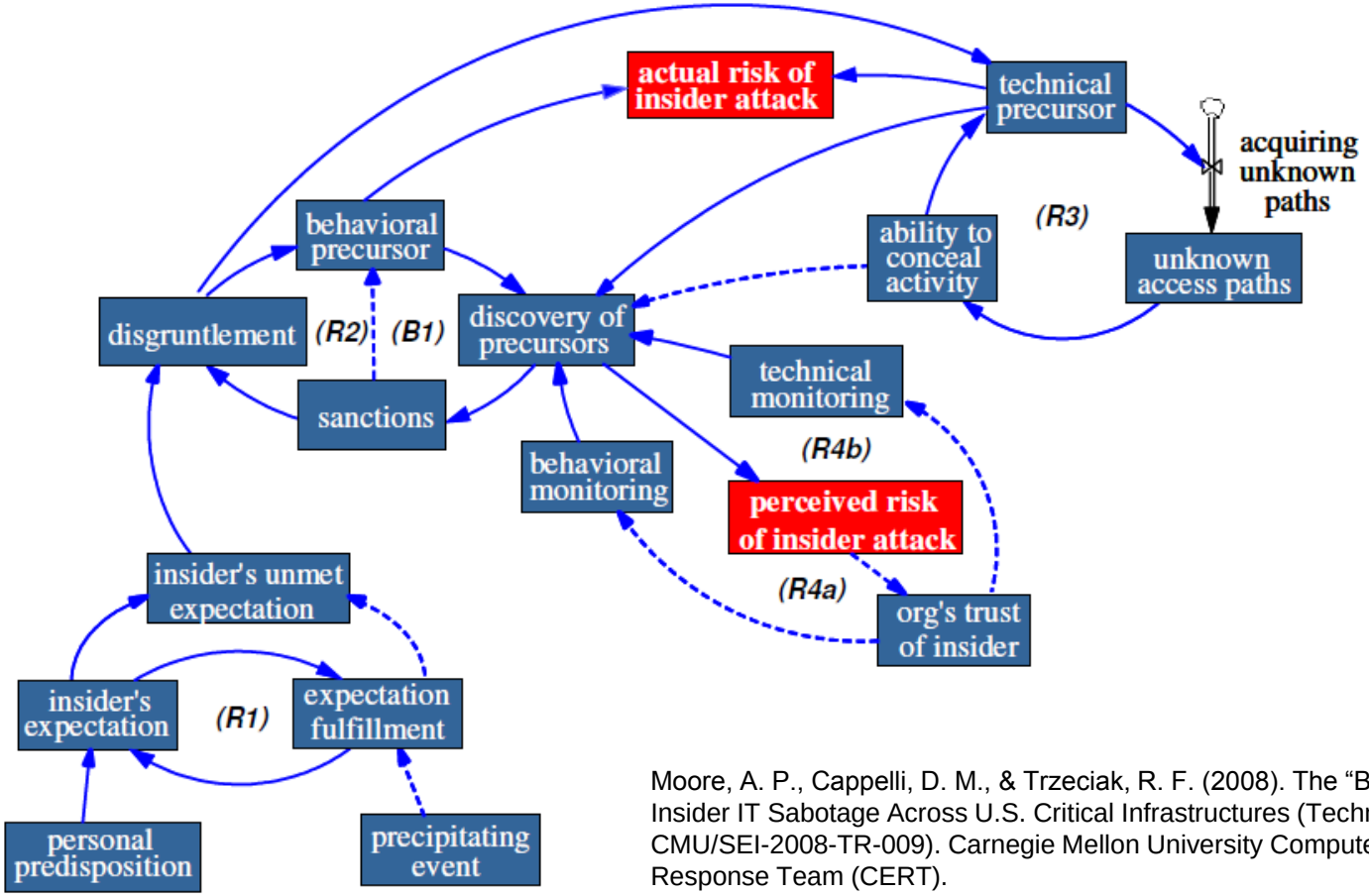


Use a multi-disciplined approach to mitigate insider threat



- Prevent insider threat where possible
- Technology is not the whole solution
- Assess enterprise vulnerability to insiders
- Apply insider threat “best practices”
  - separation of duties, access control
  - training management, IT, human resources, workforce
  - monitor human behavior without violating privacy
  - apply workplace practices that reduce insider threat
- Instrument technology to further mitigate insider threat
- Recognize and avoid certain human behavior patterns

CERT Model of IT Sabotage



Moore, A. P., Cappelli, D. M., & Trzeciak, R. F. (2008). The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures (Technical Note CMU/SEI-2008-TR-009). Carnegie Mellon University Computer Emergency Response Team (CERT).

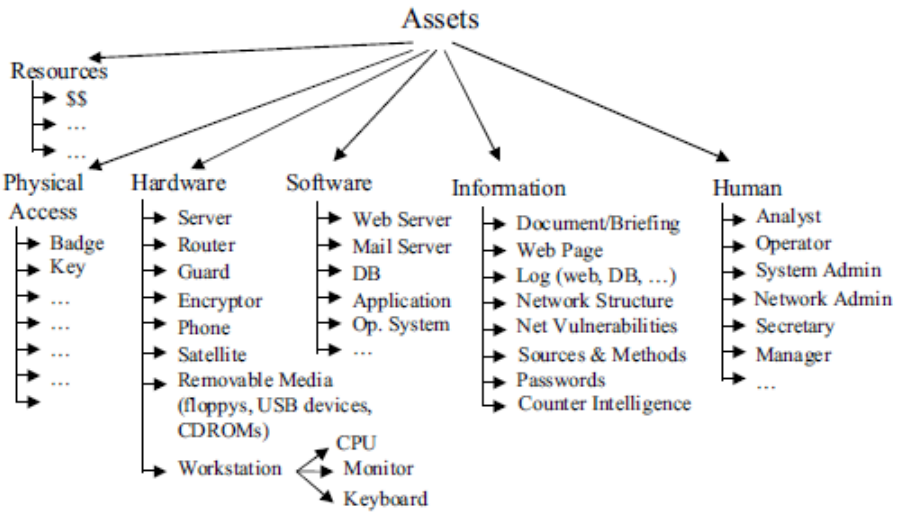
IPAKS addresses the technology challenge

- Insider attacks are largely invisible to today's technology
  - Perimeter defense and anomaly detection won't help
  - End-user monitoring catches simple insider actions, e.g. user sent an email with an attachment that read "proprietary"
- User actions must be interpreted in a larger context than current technologies permit
- IPAKS advances the state of the art by collecting and analyzing diverse observables via semantic computing

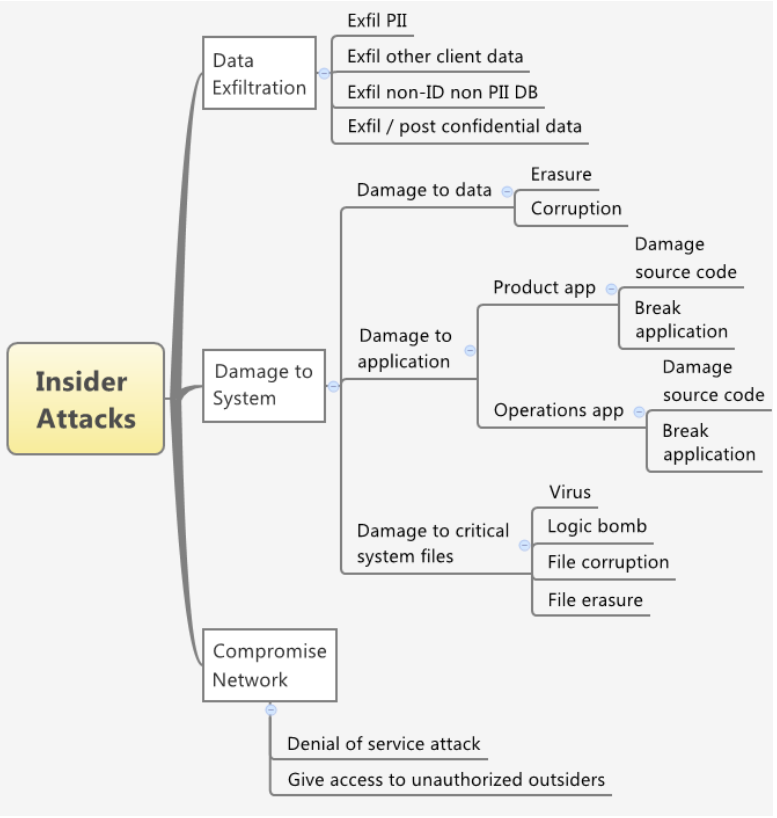
Semantic Computing

- Semantic computing combines semantic analysis, natural language processing and data mining.
- We use semantic computing to represent and reason about domain knowledge (in our case, insider threat).
- A semantic ontology formally represents domain knowledge as a set of concepts and relationships.

Semantic ontologies build on taxonomies



A taxonomy of assets



A taxonomy of insider attacks

Knowledge is represented as triples

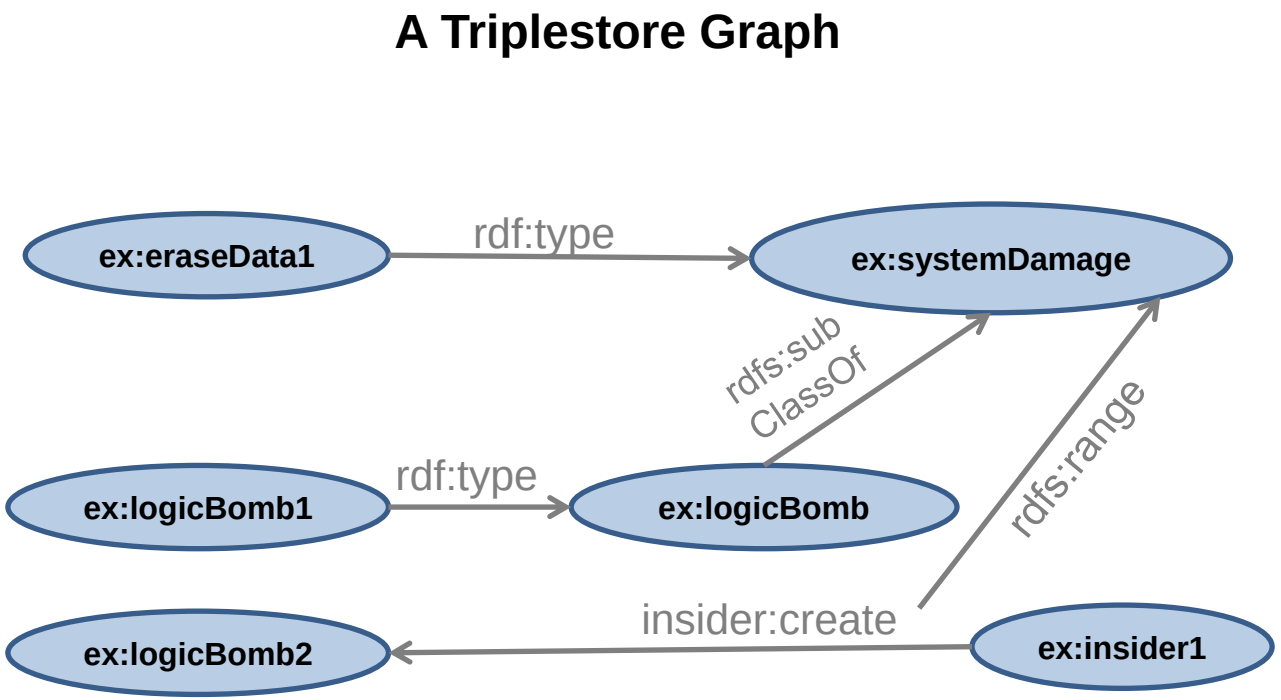
- **eraseData1** is a type of **systemDamage attack**
- **logicBomb1** is an instance of a **logicBomb attack**
- **logicBombs** are **systemDamage attacks**
- **Insiders** create **systemDamage**
- **Insider1** created **logicBomb2**

From this we can infer that

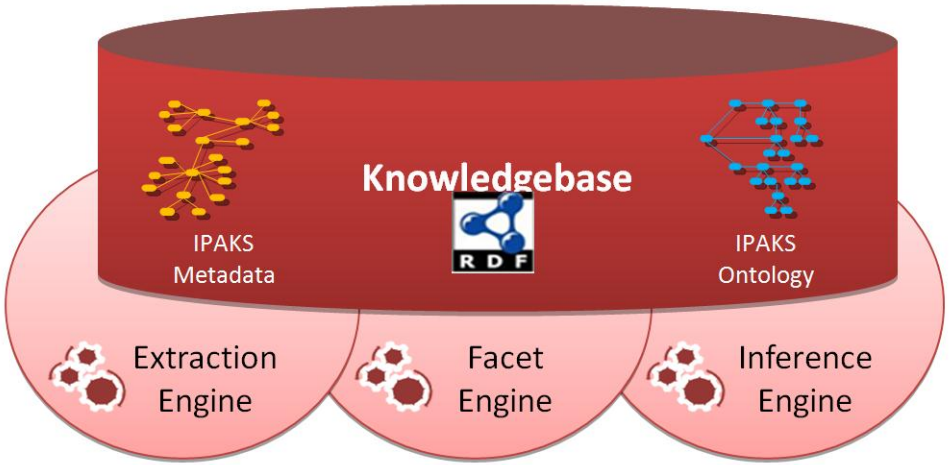
- **logicBomb2** is a **systemDamage attack**

(RDF Knowledge Representation Language)

Triplestore graphs illustrate relationships



IPAKS General Architecture

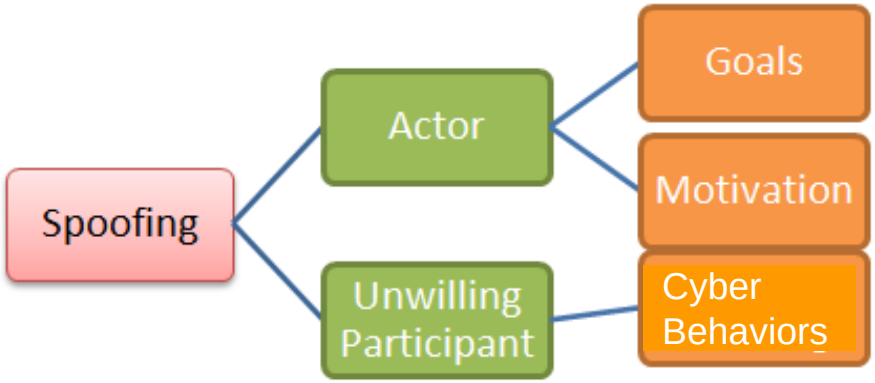


- Extraction Engine provides input and data transf-ormation services
- Facet Engine provides modeling and navigation.
- Inference Engine performs predictive analysis:
  - Identifies attacks from Knowledgebase
  - Identifies potentially novel attacks

A rule set for the Inference Engine (example)

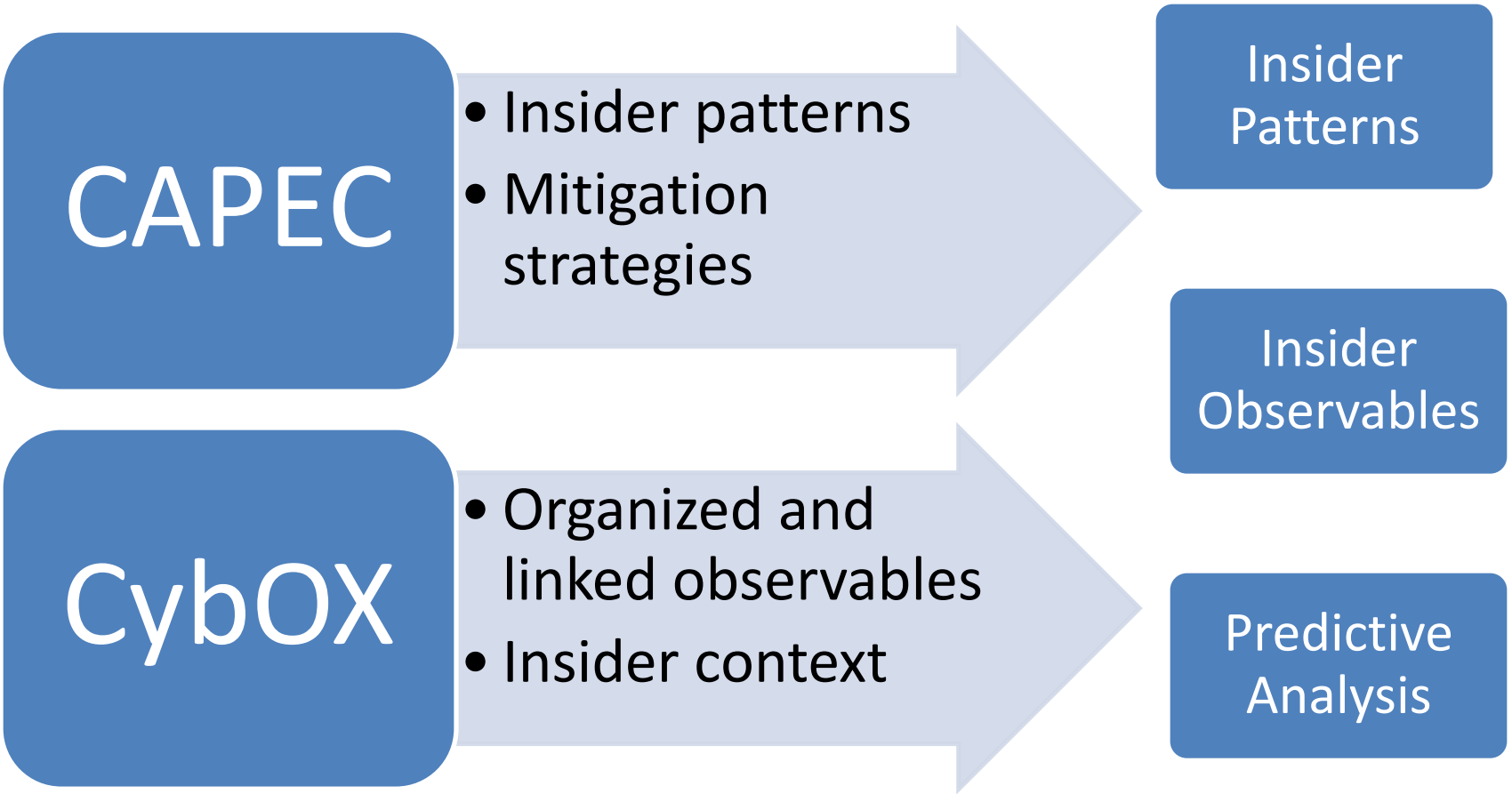
- Find all instances of likely (75% or greater for this example) non-technical insider behavior related to spoofing.
- Combine these results with possible (50% or greater) insider behaviors related to hijacking (e.g., browsing, use of web services, etc.)
- Combine all results with unlikely (20% or less) insider behaviors related to intentional unauthorized access.

Extended Observables (example: spoofing)



- Model of extended observables related to attack
- Spoofing is the attack
- Account may belong to malicious actor or to unwilling participant
- Lower-level observables are goals, motivation, and atypical cyber behaviors

Semantic Modeling with CAPEC and CybOX



Predictive Analysis Pattern Matching

- Patterns are distilled from real world cases (CERT)
- An added layer of abstraction allows pattern matching on concepts rather than specific actions
- Construct statements can be used to fuse graphs containing information collected from multiple sources
- Inferences assert new relationships, creating new links between concepts

Using Patterns we can establish from CERT cases we can map abstraction concepts to observables through our ontology.

Observables – IT Sabotage

Behavior	Observable	Data Type	Possible/Likely Goal or Outcome
Network probing: passive surveillance or active scanning	Network traffic logs: systematic pinging of network nodes; originating IP address(es), ports used	Cyber Behavior	Compromise network
Printing, copying, or downloading mission-critical files or a large number of files	Alert triggered by printing, copying, or downloading any of the mission-critical files or a large number of files	Cyber Behavior	Data exfiltration
Mood swings or poor hygiene	Report from observer of behavior	Reportable Behavior	Damage to system or compromise of network
Disabling or modification of system logs	Other logs?? Inference from other cyber behavior?	Cyber Behavior	Hiding tracks
Deletion of file from critical system or data area	Audit event logs	Cyber Behavior	Damage to system
Use of email to import malware	Suspicious addresses or attachments	Cyber Behavior	Damage to system, data exfiltration, compromise network
Use of remote access to commit sabotage	Traces from logs tracking remote activity (detection of unusual time of day, sudden change in frequency of access, or other anomaly)	Cyber Behavior	Damage to system, data exfiltration, compromise network
After-hours entry to physical facility	Device log audit	Physical Behavior	Any

Observables – IP Theft

Behavior	Observable	Data Type	Goals
Disgruntlement	Report of observed behavior, and subject is scientist or engineer	Reportable Behavior	**The Goal Of Fraud Is Nearly Always IP Theft** • Take stolen IP to new job • Use stolen IP to start new business • Use stolen IP to steal market share for another company • Share trade or defense secrets with foreign government • Aid hacker community in pirating efforts (e.g., posting documentation that helps hackers pirate software, telecommunications services, audio-visual media, etc)
Deception or lying to conceal activities	Discovery of deception or lie	Reportable Behavior	
Exhibits possessive behavior with regard to products or code	Report from observer of behavior	Reportable Behavior	
Data exfiltration by laptop	Large downloads or downloading of sensitive information	Cyber Behavior	
Deletion of file from critical system or data area	Audit event logs	Cyber Behavior	
After-hours remote access	Remote access log entries	Cyber Behavior	
Data exfiltration by email	Large attachments, emails to competitors or foreign destination	Cyber Behavior	
Downloading critical IP 30 days before or after termination	System log entries	Cyber Behavior	

Observables – Fraud

Behavior	Observable	Data Type	Methods and Intermediate Goals
Data exfiltration by telephone or fax	Large fax jobs (from hardcopy or digital file)	Physical / Reportable / Cyber Behavior	**The Ultimate Goal Of Fraud Is Nearly Always Monetary Profit.** • Identity theft • Steal customer base • Creation of fake accounts or fake invoices • Influence outcome for consumers or applications; e.g., fake driver's licenses, guarantee approval of application for political asylum • Submit fake claims to insurance companies or government organizations (e.g., Medicaid, Medicare)
[Evidence of] severe financial need	Report by observer of behavior	Reportable Behavior	
Data modification	Data verification results	Cyber Behavior	
Data exfiltration by email	Large attachments in emails sent to Gmail or Hotmail or other personal email accounts	Cyber Behavior	
Social engineering to gather information in person or by telephone, via research, dumpster diving, impersonating personnel such as tech support or customer service (called pretexting), to gather information about a target company, organization, or person (CAPEC-404)	Report from target or observer	Reportable / Physical Behavior	
Recruitment of other employees	Report by recruitment target	Reportable Behavior	

Sample Fraud Case

Fraudulent Payment for Agricultural Products

- Employees of an agricultural products firm modified vendors' names and addresses to the names and addresses of friends and relatives, generated payment checks to be sent to the fake vendors, and then changed the vendor data back to the original. The fraud was detected when an accountant noticed that the number of checks being issued had increased and further investigation revealed irregularities in the handling of the checks.
- Method: Data modification. Password sharing to subvert separation of duties.
- Accomplices: Other Insiders
- Detection: Check for deviation from normal patterns (in this case, number of checks issued). Routine checks for access privileges that do not match role.
- Prevention: Security awareness training to mitigate risk of password sharing. Monitoring of history logs for suspicious patterns of events, such as rapid multiple changes to the same record.
- The procedure of checking for deviation from normal business process patterns requires the implementation of Key Fraud Indicators (KFI), which are data that result from carrying out core business processes (such as the number of payment checks issued or proportion of applications approved). The procedure of watching for suspicious patterns of events is a Key Fraud Signature (KFS), which defines a pattern of actions to watch for (such as more than one change to a record within a specified time period). Use of KFI, KFS, and other Key Risk Indicators (KRI) is an integral part of the Defense in Depth model, which creates multiple layers of protection from malicious activity.

- Cappelli, D., Moore, A., & Trzeciak, R. (2012). *The CERT Guide to Insider Threats*. Upper Saddle River, NJ: Addison-Wesley.
- Brancik, K. C. (2008). *Insider Computer Fraud*. Boca Raton, FL: Auerbach Publications.

Point of Contact

Tom Bracewell
Senior Director Insider Threat
571-388-6029
bracewet@ctc.com

Acronyms

- CAPEC™ Common Attack Pattern Enumeration and Classification
- CERT Community Emergency Response Team
- CTC Concurrent Technologies Corporation
- CybOX™ Cyber Observable eXpression
- HUMINT Human intelligence
- IPAKS Insider Predictive Analysis Knowledge System
- IT Information Technology
- RDF Resource Description Framework