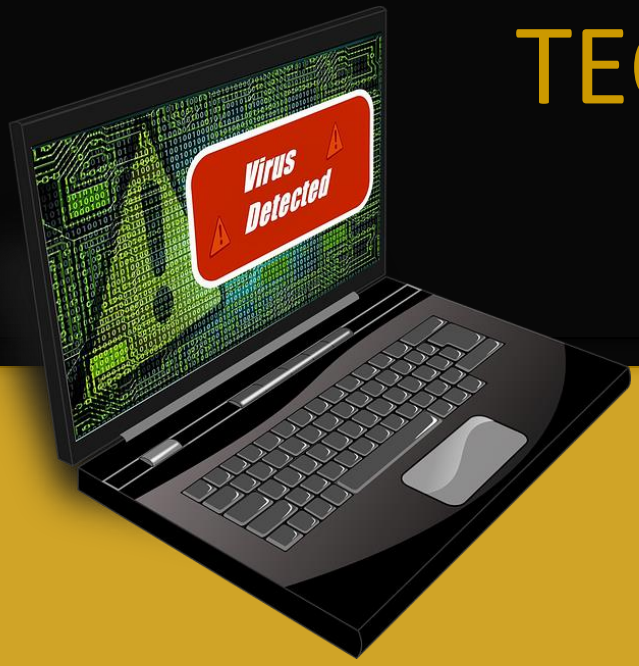
UPPING YOUR GAME-FIGHTING FRAUDSTERS WITH CUTTING EDGE TECHNOLOGY



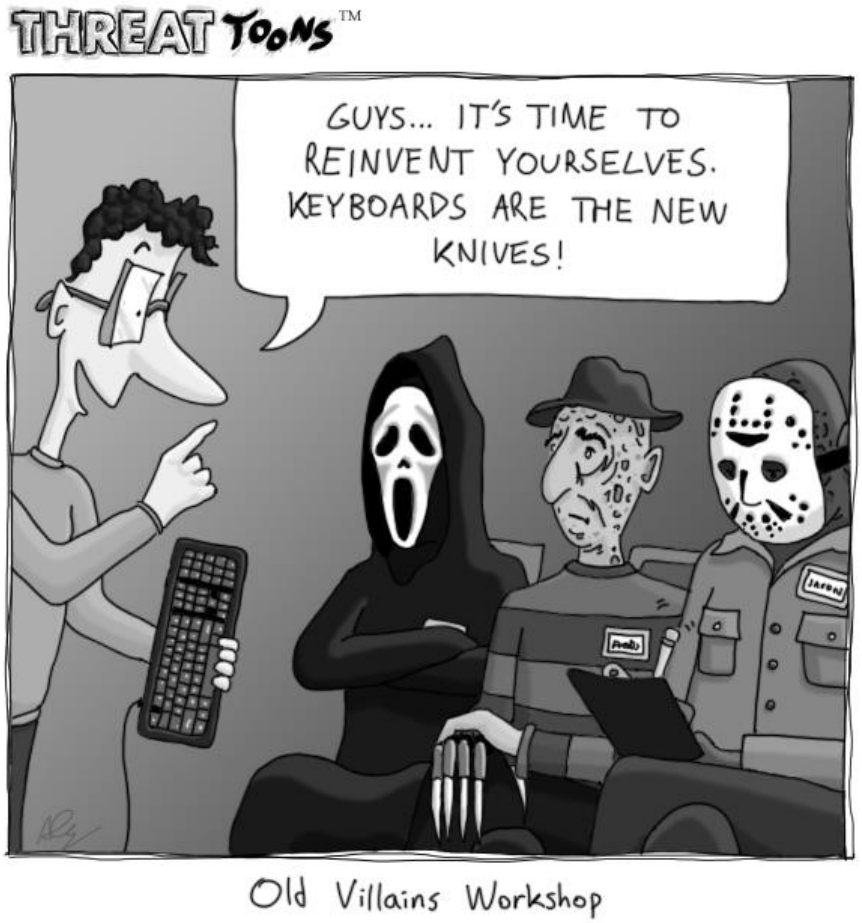
INVESTIGATING CYBER THREATS

What is a Cyber Threat?

For a cybersecurity expert, the Oxford Dictionary definition of cyber threat is a little lacking: "the possibility of a malicious attempt to damage or disrupt a computer network or system." This definition is incomplete without including the attempt to access files and infiltrate or steal data.

However, in the cybersecurity community, the threat is more closely identified with the actor or adversary attempting to gain access to a system. Or a threat might be identified by the damage being done, what is being stolen or the Tactics, Techniques and Procedures (TTP) being used.

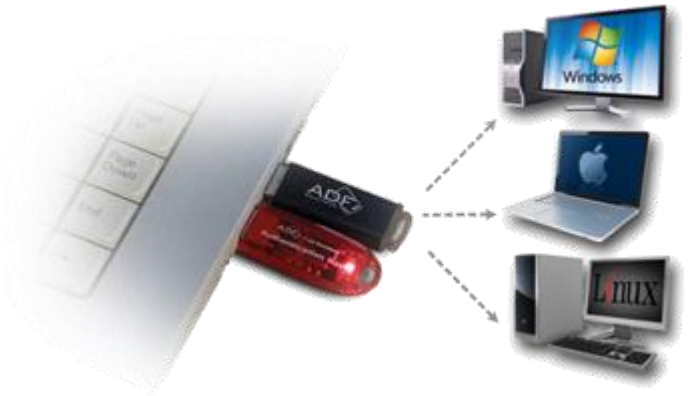
INVESTIGATING CYBER THREATS



INVESTIGATING CYBER THREATS

Types of Cyber Threats

1.Social Engineered
2.Unpatched Software (such as Java, Adobe Reader, Flash)
3.Phishing
4.Network traveling worms
5.Trojans
6.Advanced Persistent Threats



Best Practices for Defense and Protection

In-House IT Security Efforts:

- Strong end user education – compliance based practices for handling data, recognizing phishing attempts and procedures to counteract human engineering attempts
- Up to date software
- Firewall and anti-virus*
- IDS/IPS* – intrusion detection systems and intrusion prevention systems
- Security event monitoring*
- Incident response plan*

Best Practices for Defense and Protection

Security Partner Efforts:

- Penetration testing and vulnerability scanning
- Advanced threat monitoring of endpoints
- Always up to date threat intelligence
- Emergency incident response staff and investigators on call

BIG QUESTION

Can Security Beat the Well-Armed Adversary?

Applying Best Practices in selecting and employing new anti-fraud technologies

Fraud, according to Black's Law Directory, consists of "all multifarious means that human ingenuity can devise which are resorted to by one individual to get an advantage over another by false suggestions or suppression of the truth."

Fraud is costly to organizations and is bad for the economy. Technology enables fraudsters to commit and conceal traditional fraud schemes more easily. For example: Fraudsters can easily produce a fake document, such as an account statement, to deceive others.

Cont.....

As technology is advancing, so are schemes to commit fraud. The reliance on automated tools to help perpetuate these schemes provides new challenges in the detection and prevention of fraud.

Cont.....

Technology is also a tool that can help prevent and detect fraud.

Real-time fraud prevention and detection tools - reduce the time it takes to detect fraud, thereby reducing the cost of fraud.

Relationships among different IT systems and applications used to identify high-risk areas and drill down to specific transactions.

Computer forensic technology and software packages are available to assist in the investigation of fraud — where computers are used to facilitate the fraud — or to identify red flags of potential fraud.

Computer Forensics

Computer forensics is an investigative discipline that includes the preservation, identification, extraction, and documentation of computer hardware and data for evidentiary purposes and root cause analysis.

Examples of computer forensic activities include:

1. Recovering deleted mails.
2. Monitoring emails for indicators of potential fraud.
3. Performing investigation after termination of employment.
4. Recovering evidence after formatting a hard drive.

Computer forensic activities help establish and maintain continuous chain of custody, which is critical in determining admissibility of evidence in courts.

An IT fraud risk assessment

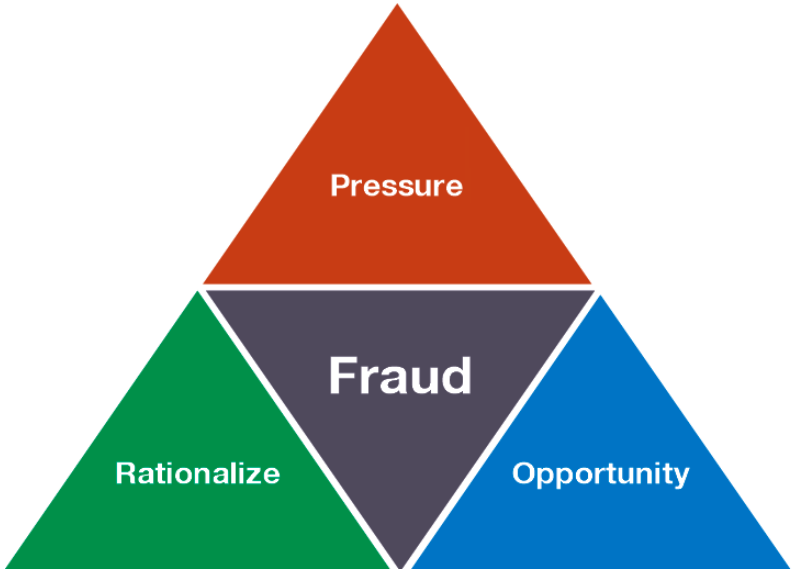
An IT fraud risk assessment is often a component of an organization's larger enterprise risk management program. As management is responsible for (ERM) programs, IT management should focus efforts on successfully completing the IT fraud risk assessment.

In many organizations, internal auditors may be asked to participate in these assessments because of the unique skill sets they offer in identifying and assessing risks.

The IT fraud risk assessment is a tool that assists IT management and internal auditors in systematically identifying where and how fraud may occur and who may be in a position to commit fraud.

Cont.....

A review of potential fraud exposures represents an essential step in addressing IT management's concerns about IT fraud risks. Similar to an enterprise risk assessment, an IT fraud risk assessment concentrates on fraud schemes and scenarios to determine the presence of internal controls and whether the controls can be circumvente



An IT Fraud Risk Assessment Key steps

An IT fraud risk assessment usually includes the following key steps:

- Identify relevant IT fraud risk factors
- Identify potential IT fraud schemes and prioritizing them based on the likelihood of the impact.
- Mapping existing controls to potential fraud schemes and identifying gaps.
- Testing operating effectiveness of fraud prevention and detection controls.
- Assessing the likelihood and business impact of a control failure and/or fraud incident.

Assessing fraud schemes

The following are two approaches to assessing fraud schemes from the fraudster's perspective:

1. **The control weaknesses approach** — looks at the potential for fraud by examining the key controls, determining who could take advantage of a control weakness, and determining how he or she could circumvent a control that may not be working properly.
2. **The key fields approach** — Looks at the potential for fraud by considering the data being entered, which fields could be manipulated (and by whom), and what would be the effect.

Both approaches seek to determine who could be committing fraud, what the fraudster could be doing, and what the symptoms of fraud would look like in the data.

Brainstorming with employees from key business areas is a good technique for assessing fraud and is useful with both of these approaches.

Access to Systems or Data for Personal Gain

Some of the most valuable information desired by individuals perpetrating a fraud in the IT area resides in the form of digital assets maintained by the organization. Therefore, it is critical for organizations to include this area in their fraud risk assessment.

Most organizations collect, create, use, store, disclose, and discard information that has market value to others outside the organization. This data can be in the form of employee or customer personal information, such as government issued identification numbers, social identification numbers, bank account numbers, credit card numbers, checking account numbers, bank routing numbers, and other personal information.

Cont.....

Whether the perpetrator is an individual with authorized access to the data or a hacker, this information can be sold to others or used for personal gain for crimes such as identity theft, unauthorized purchases on stolen credit cards, counterfeiting of credit cards, or stealing or diverting money from a bank account.

Insiders, by virtue of having legitimate access to their organizations' information, systems, and networks, pose a significant risk to employers. Employees experiencing financial problems may be tempted to use the systems they access at work every day to commit fraud.

Cont.....

Employees motivated by financial problems, greed, revenge, the desire to obtain a business advantage, or the wish to impress a new employer, may choose to steal confidential data, proprietary information, or intellectual property from their employers. Furthermore, technical employees can use their technical abilities to sabotage their employers' systems or networks in revenge for negative work-related events.

Fraud Analytics Using Descriptive, Predictive and Social Analytics

Fraud is an uncommon, well-considered, imperceptibly concealed, time-evolving and often carefully organized crime which appears in many types of forms-Van Vlasselaer et al. (2015).

Detect fraud earlier to mitigate loss and prevent cascading damage

Early detection is a key factor in mitigating fraud damage, but it involves more specialized techniques than detecting fraud at the more advanced stages. These techniques are effective for fraud detection across industry boundaries, including applications in insurance fraud, credit card fraud, anti-money laundering, healthcare fraud, telecommunications fraud, click fraud, tax evasion, and more, giving you a highly practical framework for fraud prevention.

Cont.....

It is estimated that a typical organization loses about 5% of its revenue to fraud every year. More effective fraud detection is possible, and any organization must implement the following to put a stop to the revenue leak.

- Examine fraud patterns in historical data.
- Utilize labeled, unlabeled, and networked data.
- Detect fraud before the damage cascades.
- Reduce losses, increase recovery, and tighten security.

The longer fraud is allowed to go on, the more harm it causes. It expands exponentially, sending ripples of damage throughout the organization, and becomes more and more complex to track, stop, and reverse.

Data-driven auditing: A predictive modeling approach to fraud detection and classification

By analyzing real-life accounting data, the proposed model can identify anomalous transactions and directly focus on exceptions for further investigation in real time, thus offering a significant reduction in manual intervention and processing time in audit operations.

The idea of the predictive audit is that instead of only looking backward to audit the past events and create adjustments based on changes or errors that have already occurred, auditors can perform the audit in a way that they could rapidly detect (predictive) or prevent (preventive) irregularities and anomalies or create adjustments in an ex-ante manner.

Cont.....

Based on analytic methods, the predictive audit can predict the possible outcomes of a process from operational parameters.

Auditors and management can use this information for auditing and/or management purposes. For example, fraudulent service cancelations can be predicted to detect employees who violate corporate policies (Kuenkaikaew and Vasarhelyi, 2013).

More importantly, external auditors can predict final audit results based upon quarterly and/or monthly data, and, thus do not have to wait to perform all the year-end data verification processes prior to issuing an opinion

Predictive Audit Characteristics

AREA	TRADITIONAL AUDIT	PREDICTIVE AUDIT
Control Approach	Detective (Backward)	Preventive (Forward)
Objective	Support audit opinion on financial statements	Support not only for financial purposes; include but not limited to operational audit, compliance, and control monitoring
Audit area	Financial statements at an account balance level	High risk areas in financial statements and operation processes at transaction, sub-account, and account levels
Frequency	Periodic	Continuous or close to the event or frequent
Measurement	Static	Dynamic
Method	Manual - Manual confirmations - Document vouching by sampling - Inventory counts Use statistics and/or ratios	Automated - Automatic confirmations - Data analysis of entire population - RFID, barcode Use data analysis and/or data mining techniques

Types of Prediction

Past and exogenous data
knowledge of the processes

In order to:

Predict risks, control trends, level and flows, and other parameters of the business process.

Limitation

Need historical examples to learn from (i.e., a labeled data set of historically observed fraud behavior).

This reduces their detection power with respect to drastically different fraud types making use of new mechanisms or methods, and which have not been detected thus far and are therefore not included in the historical database of fraud cases from which the predictive model was learned.

Applying Best Practices in selecting and employing new anti-fraud technologies

Are perpetrators of fraud becoming more sophisticated at covering their data trails?

FRAUD-DETECTION TECHNIQUES

It is important to stress that these three different types of techniques may complement each other since they focus on different aspects of fraud and are not to be considered as exclusive alternatives.

Expert-based rule
Descriptive analytics
Predictive and social network analytics.

SOCIAL NETWORK ANALYTICS

Extends the abilities of the fraud-detection system by learning and detecting characteristics of fraudulent behavior in a network of linked entities.

Social network analytics allows including an extra source of information in the analysis, being the relationships between entities, and as such may contribute in uncovering particular patterns indicating fraud.

INTERACTIVE SESSION

Collins Ojiambo Were

0726487695

ojiambo@gmail.com

THANK YOU GOD BLESS