ACTIVE THREAT INTELLIGENCE DIGEST

FEBRUARY 2017

FOR AN ANALYTIC AND OPERATIONAL ADVANTAGE

WWW.KIERNAN.CO

Welcome to Kiernan Group Holdings' (KGH) *Active Threat Intelligence Digest*. This monthly newsletter covers topics of interest regarding elements of the active threat phenomenon: ***active shooter incidents***, ***workplace violence***, ***insider threats***, and ***terrorism***, with a focus on planning and prevention.

Identifying an insider threat is rarely easy, but there are ways to find threats and limit risk.

Source: BetaNews

In this Issue...

In the Next Issue...

Insider Threats Pose Risk to People, Property, and Proprietary Information

By Bob Pecha, Senior Analyst

Insider Threat, one of the four dimensions of Active Threat, is the risk that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the security of organizations, agencies, universities, and corporations. The threat can include espionage, terrorism, unauthorized disclosure of national security or corporate proprietary information, or the loss or degradation of resources or capabilities.

For corporations, insider information may include company proprietary information that might give a competitor an edge in business decisions, scientific research, and other sensitive corporate data. For the government, classified or sensitive national security information could be divulged or compromised.

Four Dimensions of Active Threat

The 2016 Verizon Data Breach Investigations Report noted that insider misuse or leakage of information accounted for 77 percent of the information security incidents in 2015.

A key aspect of Insider Threat is whether the information is shared wittingly or unwittingly. Divulging information could be accidental or negligent as well as intentional. According to a report by the independent Information Security

Forum, inadvertent breaches are more common than malicious ones. Likewise, the U.S. Department of Health and Human Services' Office for Civil Rights noted the top five breaches of sensitive health care information for the first few months of 2016 involved theft, misplacing or improperly disposing of information, and unauthorized email access.

The Threat to People – Violence in the Workplace

The first aspect of Insider Threat is the protection of people. That includes protection of personnel engaged in battlefield operations, personnel at facilities away from the field of conflict, or employees in the corporate environment. The threat could come in many forms including:

- Terrorists learning key insider information about a target—such as troop movements or vulnerabilities—and how to best carry out an attack
- An insider acting on behalf of, or inspired by, a terrorist organization to do physical harm
- Disgruntled or frustrated employees
- Employees facing disciplinary or removal actions
- Employees who are experiencing mental health issues or other personal problems—such as financial strains—that may cause them to act violently

Terrorism – Examples of insiders conducting attacks on behalf of, or in support of, terrorist organizations are highly visible and publicized. The November 2009 shooting at Fort Hood, Texas, by Nidal Hasan is one of the most visible examples of an insider acting out in support of a terrorist ideology. He used his knowledge of the base, its vulnerabilities, troop schedules, and movements to achieve tragic results. Similarly, the married couple, Syed Rizwan Farook and Tashfeen Malik, used his status as an insider to access the holiday party in San Bernardino, California they attacked in 2015.

Workplace violence is often a less visible form of threat to people from an insider. While highly visible events get attention at the time of the incident, many situations do not have the visibility to make them newsworthy.

CASE STUDY

Patrick Henry Sherrill is an example of an insider who caused significant carnage in the workplace. On August 20, 1986, Sherrill entered his place of employment, the United States Post Office facility in Edmond, Oklahoma. He wore his letter carrier's uniform and carried a cloth sack containing three pistols. Being an insider his presence was not questioned or deemed inappropriate. Once inside, he opened fire on his coworkers, killing 14 and wounding six before turning a gun on himself and committing suicide. Included among the dead was one of Sherrill's supervisors who had reprimanded him the day before the shooting.

In all, 4,836 fatal work injuries were recorded in the United States in 2015, a slight increase from the 4,821 fatal injuries reported in 2014, according to the US Bureau of Labor Statistics. Workplace homicides rose by two percent to 417 cases in 2015, with shootings increasing by 15 percent, the first increase since 2012. Assailants in workplace homicides differed greatly depending on the gender of the decedent. Approximately 43 percent of female decedents were fatally assaulted by a relative or domestic partner; the corresponding figure for male decedents was two percent.

The Threat to Property

The threat to property is much more than mere vandalism. On a large scale, the threat to property could be in the form of sabotage, a long-used form of irregular warfare. Having an insider who knows the location, security and vulnerabilities of property would certainly increase the chances of success. However, property destruction could also be a form of revenge. But physical property is only one aspect.

A disgruntled insider could also damage a company's intellectual property. While we've discussed insiders providing proprietary information to other companies or governments, this type of damage is caused by leaking information that could seriously hurt the company's brand or business.

The Threat to Information

Providing **information** to unauthorized sources, whether foreign governments, news reporters, corporate competitors, or any other person or group not authorized to receive the information, constitutes a significant portion of the threat. Prominent recent examples of unauthorized disclosure by an insider include Chelsea Manning and Edward Snowden. Yet history is rich with employees who were targeted by foreign governments to betray their country. Today the cyber realm makes countering that threat more difficult than in the past. The cyber aspect of the Insider Threat presents its own set of problems to include tradecraft that is more difficult to detect. While organizations have safeguards in place it is still possible for an insider to intentionally access data for seemingly legitimate purposes and provide that information to unauthorized recipients.

The challenge is not limited to government classified or sensitive information. In the corporate world, it includes threats to patents, proprietary information, trade secrets, negotiating positions, and sensitive scientific information. The chart below, covering events in 2014, provides an excellent example of the problem in the corporate world.

In addition to the intentional dissemination of critical material, inadvertent disclosure of information through social media is a growing concern. Tidbits of information—known as Essential Elements of Friendly Information (EEFI)—may by themselves not disclose pertinent data. However, taken together with information gleaned from other sources, these tidbits could yield significant clues to protected information.

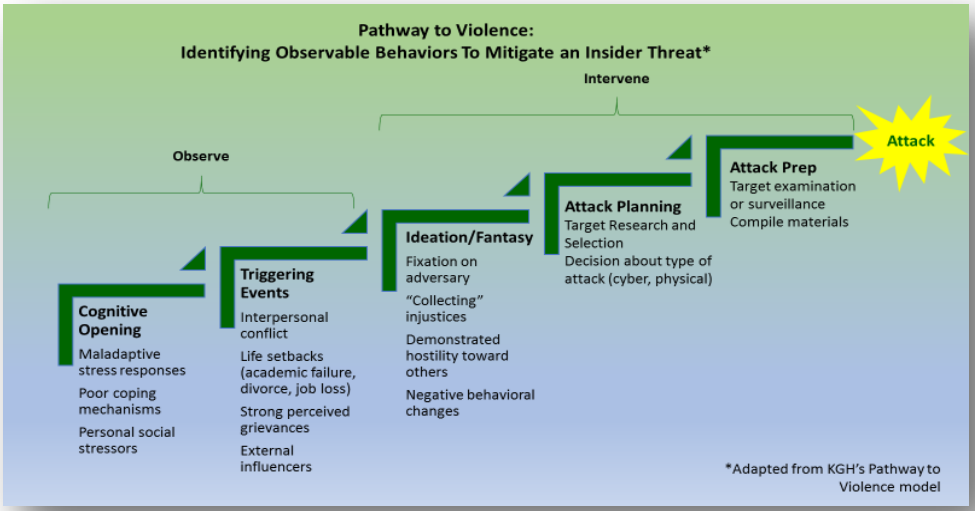
Identifying Insider Threats Using "Pathway to Violence" Indicators

Individuals contemplating committing an act of aggression against an organization—whether physically violent or

In general, the pathway of engaging in an insider threat attack relies on four primary factors:

1. An individual's perception of a lack of alternatives to engaging in violence to redress grievance(s).
2. Triggering events or enabling conditions in one's environment.
3. An individual's capability to embark on violent action.
4. The absence of internal and external protective factors to preempt or prevent such violence.

Early identification of susceptible individuals at risk of engaging in an insider threat is critical to the prevention of an attack. Throughout this pre-



incident process, potential aggressors may leave verbal, written, or behavioral clues or "leakage" in which they communicate their intentions and plans indirectly. When those in their immediate surroundings hear or observe such individuals' ideas and plans for violence prior to their incidents, understanding how to pick up this "leakage" of risk factors is critical to preempt potential violence at the earliest stage possible. Noticing leakage during the "Observe" stages may allow for referral of such individuals to mental health counselors.

Steps Toward Protecting Your Organization

Implement an all-inclusive and integrated Insider Threat program. While looking at anomalies on official IT systems is important, it isn't the only thing. In some cases, a company's security and Information Assurance (IA) operations work at odds. IA's goal is to maintain the security of the system and keep bad things out. Security wants to look deeper and see what the individual may be doing on the system. A cogent security/IA policy needs to be established by senior leadership.

The Human Resource department is a key element in identifying potential threats. They receive reports from supervisors about employee performance problems. Through an employee assistance program, they know which employees are facing personal or financial difficulties. They set guidelines for employee standards of conduct. Finally, they are the element that executes adverse personnel actions.

Maintain awareness of what is being said on social media sites. Some government and business organizations employ web scrapers that search for terms that may be vital to the business and EEFIs.

Threats to Faith-Based Organizations on the Rise

By Dr. Joshua Sinai, Senior Analyst

Faith-based organizations (FBOs) (also known as religious institutions/houses of worship) are intended to serve as sanctuaries for their members "from all the evil that happens in the outside world." For many reasons, however, FBOs have become targets for a spectrum of threats such as hate crimes, active shooters, workplace violence, and even terrorism. While violence against FBOs is rampant around the world, particularly in regions such as the Middle East and South Asia, such attacks have also been occurring in the United States, with several causing high fatalities. These include the August 5, 2012 shooting rampage by Wade Michael Page, aged 40, at the Sikh Temple in Oak Creek, Wisconsin, in which six people were killed and four others wounded, and the June 17, 2015 shooting rampage by Dylann Roof, aged 21, who shot and killed nine people during a prayer service at the Emanuel African Methodist Episcopal Church in Charleston, South Carolina. Although they have not caused fatalities so far, the continuous approximately 140 anonymous and mostly phone call bomb threats across the country against Jewish religious institutions from January to March 2017, have also included several desecrations of Jewish cemeteries. These and other types of attacks and threats against FBOs attest to the growing danger posed by such threats in the United States.

Why are FBOs targeted by such threats? The reasons for such targeting vary from certain religious facilities being considered as national icons, so attacking them would generate worldwide publicity for the extremist attackers' cause, to viewing religious sanctuaries as local community embodiments of wider inflammatory or polarizing issues involving an FBO.

With key vulnerabilities characterizing FBOs highlighted by the presence of large gatherings of people of a particular faith in a single location at specific times and a perception by their adversaries that religious facilities are "soft targets" because they have little security in place, FBOs have responded by implementing a variety of protective measures, such as emergency preparedness response plans and protocols and technological defensive systems.

5 THINGS TO KNOW ABOUT INSIDER THREATS

#1
Insider threats pose risks to people, property, and proprietary information.

#2
The divulging of information by an insider can be witting or unwitting.

#3
Violent attacks against coworkers by insiders usually are driven by perceived grievances or domestic situations.

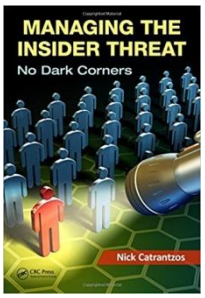
#4
Many malicious insiders demonstrate actions that can be identified along a Pathway to Violence. Those actions can be identified and monitored.

#5
Companies, agencies, and organizations can take measures to mitigate and prevent insider threats.

Active Threat Bookshelf

Review by Dr. Joshua Sinai

Nick Catrantzos, *Managing the Insider Threat: No Dark Corners* (Boca Raton, FL: CRC Press, 2012), 363 pages, $76.95 [Hardcover], ISBN: 978-1-4398-7292-5.



This is an authoritative and comprehensive textbook on the manifestations of the insider threat and the methods required to mitigate the challenges presented by the threat. It is divided into three parts: Part I, "Diagnostics" (defining the nature of the threat and the danger posed by such individuals who possess "legitimate access and occupies a position of trust" in an organization that is ultimately betrayed, and various analytical approaches employed to assess this threat); Part II, "Key Players" (the types of 'insiders' ranging from those who wage cyber sabotage or breaches on behalf of foreign governments or political causes, those who seek financial gain, to those who engage in workplace violence); and Part III, "Making a Difference" (the role of background investigations in vetting employees who might present an 'insider' threat, how to recognize deception by potential insiders, and the components of a preventative program to mitigate such threats to an organization, including considerations for employing external consultants to upgrade defenses against such threats). As a textbook, each chapter includes a summary conclusion, questions for classroom discussion, exercises for group projects, and endnotes. The appendices include additional questions and issues for further discussion, as well as an answer guide. This textbook is ideal for university courses and as a practical handbook for security departments that focus on countering the insider threat. What is especially noteworthy about this textbook is that it was published prior to the insider attacks by Bradley Manning and Edward Snowden – but had its insights and preventative guidelines and protocols been employed at the time could have aided in preventing such costly breaches into the U.S. government's national security classified information systems. The author, a veteran security director, teaches homeland security and emergency management at the School of Management, University of Alaska.