# INSIDER THREATS: HOW TO SPOT THEM AND HOW TO STOP THEM

## Designing and Implementing an Insider Threat Program

by The Nuix Business Threat Intelligence and Analysis team:
Keith Lowry, Keith Thomas, Chris Newsom, Joe Hoofnagle and Kevin Frank

nuix

Simple. Powerful. Precise.

# CONTENTS

A successful program requires executive leadership and advocacy, clear policy and guidance, and workforce education and training

# EXECUTIVE SUMMARY

More than one-third of all cybercrime incidents and security breaches are caused by insiders. These insiders have many motivations—financial, political, or even emotional—but the common factor is they all inappropriately access an organization's critical-value data.

While governments around the world have communicated the importance of addressing insider threats, real-world efforts have been patchy. It is easy to understand why some organizations have avoided the issue; the challenge of detecting and deterring insider threats appears massive and it is hard to know where to start.

The answer is to focus your efforts on very specific and definable targets: Your organization's critical-value data and the very limited ways in which an insider threat actor could access, gather, and exfiltrate that data from your network.

Using this focus, your organization can develop a proactive insider threat mitigation program that combines three key elements:

- **Understand and Focus** identifies where critical-value data is located, who has access to it and how.
- **Protect and Disrupt** uses intelligence and analysis to identify insider threat actors within systems and networks.
- **Deter and Detect** includes accurate and up-to-date cybersecurity and IT policies, training, and forensic tools.

The key is that this is a program, not just a piece of software. A successful program requires executive leadership and advocacy, clear policy and guidance, and workforce education and training. It must bring together stakeholders from across the organization including human resources, administration, legal, physical security, information security, and information technology.

With these elements in place, your organization can address insider threats before they become messy and costly public problems.

# UNDERSTANDING INSIDER THREATS

More than one-third of all cybercrime incidents and security breaches are caused by insiders.[i] The harm caused by data breaches, theft of intellectual property, loss of financial information and other critical-value data is epidemic. The resulting financial damage to governments, corporations and individuals amounts to hundreds of billions of dollars annually.[ii] But just as importantly, such events damage an organization's reputation, trust and value.

There are many examples of insiders who have used their position to advance personal, political, or nation-state agendas.

- Edward Snowden and Chelsea Manning are very public examples of insiders who exploited their access to highly sensitive information to leak it to third parties.
- The Australian Department of Immigration and Border Protection suffered data breaches in 2014 and 2015 as the result of employee actions. Although these incidents were believed to be inadvertent, the leaked information was highly sensitive.
- Russian agent Anna Chapman and her compatriots were state-sponsored insiders tasked with gaining trust and access inside the financial and government sectors in the United States to steal information for their sponsor's gain.

Insiders also steal or leak financially valuable data, such as credit card numbers and personally identifiable information, which can be used to commit fraud or sold on the black market. Recent examples include:

- The US Federal Communications Commission fined telecommunications company AT&T $25 million after call center employees stole and resold names and Social Security numbers of approximately 300,000 customers.[iii]
- A former employee of UMass Memorial Medical Group, an alliance of hospitals, inappropriately accessed 14,000 patient billing records and used an unknown number of them for fraud.[iv]
- Investment bank Morgan Stanley fired one of its financial advisors after it accused him of stealing 350,000 clients' account data and posting some of it online for sale.[v]

Organizations that hold valuable intellectual property suffer insider thefts of trade secrets, commonly referred to as industrial espionage.[vi] For example, in May 2015, the US Justice Department filed charges against six Chinese nationals who had taken jobs at Silicon Valley microelectronics companies to steal trade secrets relating to acoustic filters for cellphones. They used this stolen technology to produce their own filter circuits which they sold to military and commercial customers in China.[vii]

## Once You're Inside, You're an Insider

The motivations, targets, and methods of malicious insiders are many. In defining an "insider threat" we believe it doesn't matter how someone gains access or whether they are a current or former employee or an external contractor—once a user is inside the system, they are an insider threat. Consequently, we define an insider threat as:

> *An individual who abuses authorized access to systems or information; allows unauthorized others access to systems or information through improper behavior; is an unauthorized user; or who maliciously uses or gains access to systems or information in order to manipulate or extract an organization's critical-value data. Critical-value data includes internal resources, personally identifiable information, financial information, personnel records, security systems, information systems, business equipment, intellectual property, trade secrets, supply chains, or any other information of value to the organization.*

# RESPONSES TO INSIDER THREATS

US President Barack Obama addressed insider threats in Executive Order 13587, published in October 2011.[viii] This Executive Order sought to put in place "structural reforms to improve the security of classified networks and the responsible sharing and safeguarding of classified information". This was merely the beginning of governmental efforts to recognize, define, and map out a program to stem the tide of insider threats.

The Executive Order established the National Insider Threat Task Force (NITTF) under joint leadership of the Attorney General and the Director of National Intelligence with a primary mission of preventing, deterring, and detecting compromises of classified information by malicious insiders.

While political leaders have stressed the importance of dealing with insider threats, broader awareness of the problem and efforts to mitigate it have been patchy. It is easy to understand why some organizations have avoided the issue: the challenge of detecting and deterring insider threats appears massive; many organizations simply don't know where to start. In light of these challenges:

- How can an organization close the gap between the initial attack, discovering the insider threat actor's deeds and taking action to shut down or otherwise mitigate the event?
- How do we stop the Snowdens within our own systems and networks?

## Focus on the Insider Threat Actor

Detecting and disrupting insider leaks are classic "needle in a haystack" searches and it's easy to be intimidated in the face of such complex tasks. It requires us to apply our intelligence in both senses—mental effort and sources of information—toward the task of focusing on what the insider threat actor wants to achieve and the ways in which they can do it.

It is important to understand that while information technology is virtually boundless, human interaction with technology is limited. In other words, there are only so many ways to access, gather, and exfiltrate critical-value data from a system or network. Focusing our efforts on the limited use of technology and the relatively small number of ways in which people can move data yields results much faster than a broader "scattershot" approach.

To achieve this focus, we must bring together many disciplines from across the organization. For example:

- It is easier to identify an insider exfiltrating data if we limit the ways people can interact with systems and networks. One way to achieve this is with IT usage policies and technical measures that prevent employees from connecting USB storage devices to their workstations.
- To focus on protecting important information, not all data, it is necessary to identify and locate an organization's critical-value data, the "crown jewels". This requires cooperation and often negotiation between data owners across the organization.

## No Time to Be Reactive

It is also important to understand organizations cannot afford to take a purely reactive posture toward insider threats. Measures an organization puts in place after a breach has already occurred will most likely come too late to prevent embarrassment, loss of valuable information, or even public scandal.

Perimeter defenses, incident response, and security operation centers are mostly defensive in nature—they typically alert and respond after an event has occurred. Perimeter defenses are designed to keep outsiders from getting into an organization's systems; they are almost powerless against malicious actors who are already inside the network and often have legitimate credentials to access critical-value data.

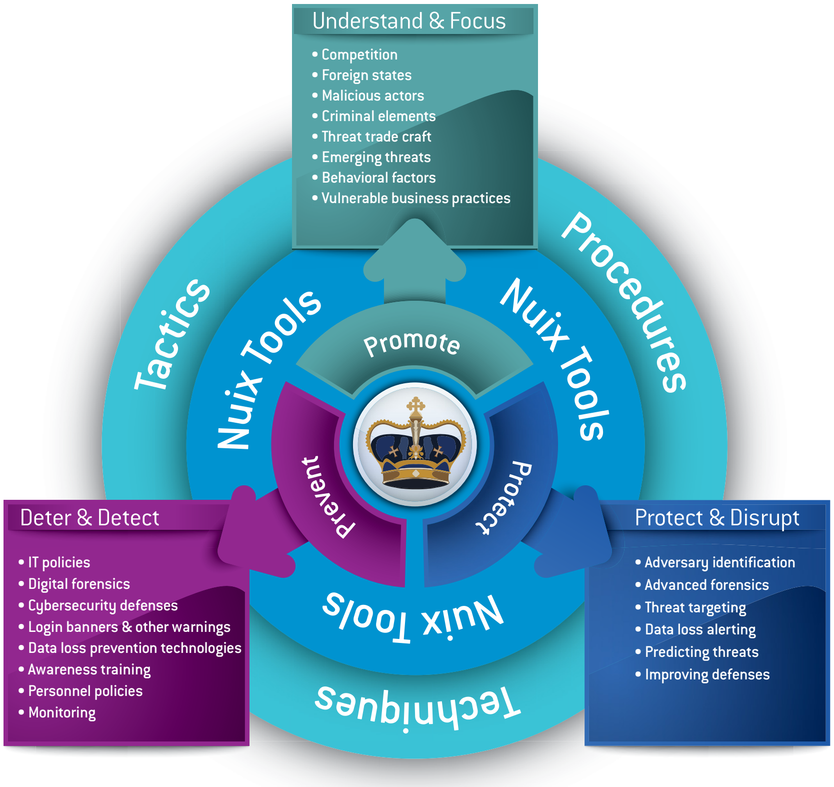
Organizations can become more proactive by broadening the scope of cybersecurity activities from traditional perimeter defenses to a set of policies and processes that limit opportunities for insider breaches and make it easier to identify threat actors.

# DEVELOPING AN INSIDER THREAT PROGRAM

The answer to this challenge is to use small data—limited, specific pieces of information—to find pertinent facts in the big data world. The methodology we have applied in large US Government agencies operationalizes the concept of insider threat mitigation described by the NITTF; a holistic approach that incorporates policies and guidance, education and training, and technology.

We focus our efforts on mitigating insider threats by quickly and efficiently answering the question of who within the network intends on doing us harm. We combine "understand and focus," "protect and disrupt," and "deter and detect" elements to create an organization-wide environment focused on defending against insider threats (see Figure 1):

- **The Understand and Focus** process is used to identify authorized users who have access to critical-value data. We must determine the crown jewels of the organization, where the critical-value data is located, who has access to it, and how they have access. It includes understanding who might be a threat, what options and methods insider threat actors use, and the observable indicators such threat activity creates.
- **Protect and Disrupt** uses intelligence and analysis to clarify and focus investigations and activities in identifying insider threat actors within systems and networks. This means attempting to identify who an insider threat actor is, how the actor is operating within a network, who the insider threat actor's associates may be, and does the actor have past techniques that can be captured and understood.
- **Deter and Detect**, or cyber-defense information, includes having accurate and up-to-date cybersecurity and IT policies, training, good forensic tools, and proper user banners.



Understand & Focus

- Competition
- Foreign states
- Malicious actors
- Criminal elements
- Threat trade craft
- Emerging threats
- Behavioral factors
- Vulnerable business practices

Deter & Detect

- IT policies
- Digital forensics
- Cybersecurity defenses
- Login banners & other warnings
- Data loss prevention technologies
- Awareness training
- Personnel policies
- Monitoring

Protect & Disrupt

- Adversary identification
- Advanced forensics
- Threat targeting
- Data loss alerting
- Predicting threats
- Improving defenses

Figure 1: Elements of Nuix's approach to insider threat mitigation.

The knowledge gained by combining these three elements helps bring into focus:

- Who is attempting to discover and steal the crown jewels
- What method are they attempting to use
- Where they are attempting to take them.

The key is that this is a program, not just a piece of software. Technical aspects alone are insufficient to deter insider threat actors.

Organizations must create an environment hostile to an insider threat actor through an effective policy framework and by focusing energy and scarce resources on the most important data.

## Security Is Everyone's Job

Who is responsible for creating an environment where your organization can be proactive against insider threats? Who is responsible for ensuring that cybersecurity and insider threat policies are brought to life, properly coordinated, and effectively used?

In our experience, executive leadership involvement is the critical factor in program success. Executives must be actively involved in, and advocate for, the insider threat program to set the conditions for success.

Clear policy and guidance, workforce education and training, and distinct lines of authority and responsibility are important elements of a successful insider threat program. The program must also involve a wide range of stakeholders including human resources, administration, legal, physical security, information security, and information technology.

Another key area for success is workforce knowledge. A training and education program that effectively instructs all personnel regarding their individual roles and responsibilities allows everyone to be part of the solution in identifying and defeating threats. To summarize, security is everyone's job.

## Start Now

To mitigate insider threats, organizations must first recognize that there is a threat. Then they must put in place policies, processes, and technologies to address insider breaches before they become public problems; it is too late to put measures in place after an attack. And perimeter defenses are designed to keep the bad guys out of the network, not to protect information from those who have access to it from the inside.

Cybersecurity and insider threat mitigation are mutually supporting. As a consequence, organizations should arrange these programs in a way that encourages collaboration toward the common objective of protecting critical-value data from external and internal threats.

Think about focusing the power of your organization through small data. Most importantly, know that you can't solve this problem with a piece of software or tool; it requires a program.

Success starts at the top of your organization. Advocacy from executive leadership, a streamlined response capability, and applicable education and training will set the conditions for your organization to confront insider threats.

## REFERENCES

i CERT Program at Carnegie Mellon University, 2014 US State of Cybercrime Survey, April 2014

ii Center for Strategic and International Studies and McAfee, Net Losses: Estimating the Global Cost of Cybercrime, June 2014

iii Rebecca R. Ruiz, FCC Fines AT&T $25 Million for Privacy Breach, The New York Times, 8 April 2015

iv Jeff Goldman, Insider Breach Exposes 14,000 UMass Memorial Patients' Data, eSecurityPlanet, 4 February 2015

v Justin Baer, Morgan Stanley Fires Employee Over Client-Data Leak, The Wall Street Journal, 5 January 2015

vi Federal Bureau of Investigation, Economic Espionage: Protecting American's Trade Secrets

vii David E. Sanger And Nicole Perlroth, 6 Chinese Men Indicted in Theft of Code From U.S. Tech Companies, The New York Times, 19 May 2015

viii President Barack Obama, Executive Order 13587—Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, 7 October 2011

## ABOUT THE NUIX BUSINESS THREAT INTELLIGENCE AND ANALYSIS TEAM

The Nuix Business Threat Intelligence and Analysis Team helps organizations understand, deter, detect, disrupt, and respond to insider breaches. Our expert team members have worked on investigations and designed insider threat programs for major U.S. government agencies and corporations.

### Keith Lowry

Keith brings more than 25 years of experience implementing, managing, and directing insider threat, counterintelligence, and intelligence collection programs for organization including the U.S. Food and Drug Administration, Office of the Director of National Intelligence, Office of the Under Secretary of Defense for Intelligence, and the San Jose (California) Police Department.

### Keith Thomas

Keith has 25 years of experience in digital and mobile forensics for local, state and federal law enforcement. His experience includes working as a Special Agent with the U.S. Naval Criminal Investigative Service, state prosecutor's offices and supporting the Department of Defense.

### Chris Newsom

Chris has 15 years of experience in computer forensics, incident response, and insider threat assessment, discovery and mitigation for law enforcement and the federal government including U.S. Food and Drug Administration, the U.S. Department of Defense Computer Forensic Laboratory and the Baltimore Police Department.

### Joe Hoofnagle

Joe has more than 20 years of experience building and leading insider threat, computer forensics, incident response, eDiscovery and information security teams. He has worked at the U.S. Food and Drug Administration, Magellan Health Services and various Fortune 10-1000 organizations. Joe also served as the Technical Editor for the 4th edition of the Shon Harris All-in-One CISSP guide.

### Kevin Frank

With over 30 years of experience, Kevin has worked as a military and civilian intelligence officer, providing operational intelligence to senior decision makers in the military, the U.S. Department of State, foreign partners, international organizations and the Defense Intelligence Agency.

To find out more about Nuix's insider threat program visit

nuix.com/BTIAT

## ABOUT NUIX

Nuix enables people to make fact-based decisions from unstructured data. The patented Nuix Engine makes small work of large and complex human-generated data sets. Organizations around the world turn to Nuix software when they need fast, accurate answers for digital investigation, cybersecurity, eDiscovery, information governance, email migration, privacy, and more.

**North America**
USA: +1 877 470 6849
» Email: sales@nuix.com

**EMEA**
UK: +44 203 786 3160
» Web: nuix.com

**APAC**
Australia: +61 2 9280 0699
» Twitter: @nuix