Five Steps to Develop a Successful Insider Threat Detection Program

A WHITE PAPER PRESENTED BY LEIDOS

leidos

WHAT ARE THE BIGGEST SECURITY THREATS TO YOUR ORGANIZATION'S DATA? RECENT MEDIA ATTENTION TO HIGH-PROFILE CYBERATTACKS WOULD LEAD AN ORGANIZATION TO THINK EXTERNAL THREATS ARE ITS ONLY CONCERN. UNFORTUNATELY, THIS MISPERCEPTION ALLOWS ONE OF THE BIGGEST THREATS TO YOUR ORGANIZATION'S DATA TO STAY COMPLETELY UNDER THE RADAR—THE THREAT OF INSIDERS. EMPLOYEES, CONTRACTORS, SUPPLIERS, AND EVEN TRUSTED BUSINESS PARTNERS WHO HAVE AUTHORIZED, YET UNCONTROLLED, ACCESS TO SYSTEMS AND/OR SENSITIVE INFORMATION ALL HAVE THE OPPORTUNITY TO DO IRREVOCABLE HARM TO A COMPANY.

INCREASING INSIDER INCIDENTS, COSTLY REPERCUSSIONS

According to the 2014 U.S. State of Cybercrime Survey, 28 percent of companies identified insiders as a source of their cybersecurity threats over the past year.[1] The global economic crisis, increased exposure to foreign intelligence entities, and the propagation of digital data have all contributed to the rise in malicious attacks. A disgruntled or cash-strapped insider may be easily persuaded to expose sensitive information or use it for personal gain, misuse access to internal networks and systems, or create backdoor accounts to gain direct access to sensitive information. The repercussions of a data breach are costly. Juniper Research predicts data-breach losses to reach $2.1 trillion globally by 2019, with an average cost per incident to exceed $150 million by 2020.[2]

Cases in point: Last year, a network engineer who learned he would soon be terminated shut down the organization's network servers and deleted critical data. The company was unable to fully communicate for 30 days, had limited access to data and applications, and lost more than $1 million.[3] Another case involved one investment bank who had information on 350,000 of its wealth-management clients appear online. It was discovered the data was downloaded by an employee and stored on his personal laptop, which was then targeted by hackers.[4]

Unfortunately, many insider threat incidents go undetected thanks in part to the prevalence of a mobile workforce, the bring-your-own-device (BYOD) to work movement and increased use of personal email accounts, USB flash drives and cloud storage services among employees. In an era where all of a organization's sensitive information is stored electronically, it has never been easier to move information outside a company's firewall.

HOW CAN COMPANIES PROTECT THEMSELVES FROM INSIDER THREATS?

Leveraging traditional defense-in-depth models—multi-layered defensive network systems— to secure information is no longer enough, particularly when dealing with an insider who knows where sensitive information resides and how to access it. The best line of defense for organizations of any size across all industries is to develop and execute an insider threat detection program. To do that, an organization must gain buy-in and support from company leaders, leverage the latest technology to detect threats, develop a communications plan for companywide rollout of the program, execute a training and awareness campaign to educate employees about insider threats, and establish a governance structure to continuously evaluate the program.

5 STEPS TO SUCCESS

leidos

GAIN LEADERSHIP SUPPORT

The first key of the program is to gain the support of the executive team. Attaining consensus among leadership will require they have a strong understanding of the types of threats the organization faces and what is at stake if the organization falls victim to the actions of a malicious or unintentional insider. It is important to demonstrate to leaders that the program is aligned with the company's corporate culture and values, that the program is sound legally and ethically, and that regulatory standards are met.

Leadership must then allocate proper financial support to ensure the program can achieve its mission. Outlining what additional technologies, such as insider threat detection software, and personnel are required to support the program and the associated costs will assist in determining the proper budget.

With approval in hand, key stakeholders should be identified and a steering committee established to develop the program. This is clearly a team effort that includes IT, corporate security, information security, human resources (HR), legal, ethics, privacy, communications, and other stakeholder organizations.

Bottom Line: Top executives must actively support and participate in the insider threat detection program for it to be truly successful. Such support ensures it is adopted across the company, empowering the responsible department to implement critical mitigations in a timely manner.

LEVERAGE THE LATEST TECHNOLOGY

Technology plays an important part in the success of a robust insider threat detection program. Most organizations have invested in various types of cyber- and information-security solutions. Additional technology solutions including data loss prevention, host- and network-based monitoring, and decision support tools can be integrated to provide another level of support. However, the overwhelming amount of information these tools produce provide little insight if not partnered with a proper analytical tool.

The latest insider threat detection tools analyze both network and behavioral risk indicators from other business functions such as HR and corporate security. The type of big data analytics found in the WISDOM insider threat intelligence solution provides context and insight in real time, proactively alerting security teams of at-risk employees. This latest technology helps organizations prioritize and drive security operations and investigations, reducing the resource requirements and time commitment necessary to execute an effective program.

Additionally, an effective insider threat detection tool should provide multiple graphical views of results and have a built in link-analysis feature. These tools enable analysts to evaluate relationships between any of the data sets. Visualization of linkages between data sets provide analysts with more accurate leads and allows for better analysis of behavior associated with an insider. Flexibility that allows analysts to tailor risk scores and values unique to their industry and/or enterprise is another important feature to look for. And finally, the tool should encrypt incoming data for security and anonymize score results to prevent profiling.

SELECTING THE RIGHT TECHNOLOGY

AN EFFECTIVE INSIDER THREAT DETECTION SOLUTION SHOULD FOCUS ON BEHAVIOR—NOT DEVICES. AN ORGANIZATION SHOULD NOT BE REQUIRED TO UPGRADE ITS CURRENT SOFTWARE APPLICATIONS OR COMPUTER PLATFORMS TO ACHIEVE SUCCESS. RATHER, A BEST-IN-CLASS THREAT DETECTION SOLUTION WILL EASILY INTEGRATE INTO A COMPANY'S EXISTING INFRASTRUCTURE—INCLUDING WORKING WITH LEGACY SYSTEMS WITHOUT THE NEED FOR SPECIAL PATCHES OR PROGRAMMING—TO SEAMLESSLY INTEGRATE DATA SOURCES ACROSS THE ORGANIZATION.

DEVELOP A COMMUNICATIONS PLAN

A communications plan to launch the insider threat detection program needs to be developed before new policies and protocols are implemented. This communications strategy should be developed in close coordination with the communications, HR and legal teams to ensure messaging aligns with the corporation's culture and values. It is essential to be as transparent as possible but not give away the critical components of the program. Think of it as "opaque transparency."

A three-tiered approach is often used to differentiate the message for the most senior leaders in the organization, mid-level managers and supervisors, and the entire employee population. If you are uncertain how a message will be received, consider previewing the messaging to a small focus group representing a wide demographic of employees. This will help flag language that may be viewed as inflammatory or that creates the impression the program promotes a "big brother" or "snitch" mentality.

Once messaging has been reviewed, finalized and approved, broadcast the information in as many modalities as possible: webinars, emails, podcasts, fliers, posters, and company newsletters. This dissemination plan can later be used for the training and awareness campaign.

EXECUTE A TRAINING AND AWARENESS CAMPAIGN

A well-structured training and awareness program is vital to the success of any insider threat detection program and instrumental in alleviating potential employee concerns. Such a campaign should educate employees about their vulnerability to internal and external threats, discuss tactics used by industry competitors or foreign adversaries, and advise on how they can protect themselves and the company.

Proper training should teach employees how to recognize uncharacteristic behavior among their colleagues—behavior that may be indicative of an insider threat. Employees should also be made aware of how and to whom they should turn to report their concerns.

Administering an insider threat knowledge survey to employees before the training and awareness campaign can determine their baseline knowledge.

Surveying employees after implementation will gauge effectiveness.

Finally, remind employees regularly of company policies and encourage them to be mindful at all times.

ESTABLISH A GOVERNANCE STRUCTURE

An established governance structure is imperative to ensure your insider threat detection program is legally sound, compliant with regulations, and follows the pre-approved concept of operations, policies and procedures. Such a structure provides oversight for incident management processes and investigative procedures, as well as keeps senior leaders informed of critical assets, at-risk employees and trends over time.

Governance activities should include a continuous review of program metrics as a way to gauge the program's effectiveness and provide a cost/benefit analysis. Metrics may include the number of risk alerts generated, inquires conducted, investigations opened, proprietary documents recovered, etc.

leidos

BENEFITS OF AN INSIDER THREAT DETECTION PROGRAM

The benefits of an insider threat detection program far outweigh the time and resources necessary to put a program in place. Training and program awareness alone can deter many unintentional and malicious insiders, but the program's proactive protection of sensitive information safeguards a company from the following outcomes:

- Damaged brand reputation—as well as lost customers/clients— when a sensitive data breach is exposed
- Loss of revenue and competitive position when trade secrets, intellectual property, proprietary research, designs, formulas, or software are stolen
- Issuance of regulatory fines for insider trading or noncompliant use of customer data
- Lost clients (and subsequent lost revenue) when confidential contracts, pricing agreements or strategies are leaked
- Legal repercussions when confidentiality agreements are broken
- Increased security risk when knowledge of an enterprise's business practices, systems and databases are known
- Loss of critical and high-value personnel when salaries, perks or employment contract details

THE KEY TO PROTECTING YOUR VALUABLE INFORMATION

Insider crimes are a very real and costly problem for companies—often more costly than highprofile cyberattacks. Today, with so much of a company's valuable information digitized and increased use among employees of personal devices, personal email accounts, USB flash drives, and cloud storage services, it has never been easier to steal sensitive company information.

With a well-designed and effectively implemented insider threat detection program companies can greatly reduce their likelihood of compromise. By utilizing the latest threat detection tools and properly training employees to safeguard information and to recognize anomalous behavior, a company can more effectively deter, detect and respond to internal risks.

ABOUT THE LEIDOS INSIDER THREAT DETECTION PROGRAM

Industry-leading experience in counterintelligence is the foundation of the WISDOM insider threat intelligence (ITI) solution, providing organizations of any size with proactive identification of potential insider threat activity. This award-winning solution takes a holistic approach to detecting insider threats—seamlessly integrating data sources across the organization with individual modeling behavioral indicators to provide the most robust, advanced insider threat detection program available.

In an environment of increasingly complex insider threats, Leidos is your trusted partner to ensure the protection of your company assets, intellectual property and employees.

leidos

1. “2014 US State of Cybercrime Survey.” May 2014, PwC, 10 June 2015 <http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/pwc-2014-us-state-ofcybercrime.pdf>

2. Doug Drinkwater, “Data breaches to cost businesses £1.3 trillion by 2019,” 12 May 2015, SC Magazine, 12 June 2015 <http://www.scmagazineuk.com/data-breaches-to-cost-businesses-13-trillion-by-2019/article/414170/>

3. “EnerVest Computer Attack Draws Four-Year Federal Sentence,” 20 May 2014, US Attorney’s Office, 17 June 2015 <http://www.justice.gov/usao-sdwv/pr/enervest-computer-attack-draws-four-year-federal-sentence>

4. Ivy Schmerken, “Morgan Stanley Data Theft Exposes Insider Threat & Need for More Restrictions,” 14 January 2015, Information Week, 10 June 2015 <http://www.wallstreetandtech.com/security/morgan-stanley-data-theft-exposes-insider-threat-and-needfor-more-restrictions/d/d-id/1318623>

5. “Symantec Study Shows Employees Steal Corporate Data and Don’t Believe It’s Wrong,” 6 February 2013, Symantec, 29 May 2015 <http://www.symantec.com/about/news/release/article.jsp?prid=20130206_01>

FOR MORE INFORMATION
855-56-CYBER / cyber.security@leidos.com
cyber.leidos.com

XX-LH-V0