Risk Insights

SECURITAS

BUILDING A COMPREHENSIVE APPROACH TO INSIDER THREATS

The first thing that business leaders should do about the insider security threat is to take it seriously. Although there is widespread recognition that the threat is very serious, in most sectors there is insufficient follow-through to build the threat-specific plans, organizational structures, and controls to deal with it.

What needed is a comprehensive approach that addresses and leverages the unique aspects of the insider threat. Technology by itself is not the answer; the critical human dimension of the insider threat must also be addressed.
A comprehensive approach would include the following:

Establishing a threat-aware culture of institutional integrity and personal reliability
Company culture is a product of many factors, a culture of institutional integrity and personal reliability is conducive to success in almost any enterprise. Factors for achieving this includes the following:

- Create an environment in which self- directed employee actions reflect a high degree of institutional integrity and reliability
- Articulate clear expectations in an enterprise Acceptable Use Policy governing IT resources
- Create a safe environment to self-report accidental actions that challenges security
- Provide regular insider threat awareness training as well as realistic phishing training exercises
- Establish a set of institutional values reflecting the desired culture, select leaders based on their adherence to these values

Building a multi-disciplinary program
Establish an executive committee to manage an integrated multidisciplinary program designed to deter, prevent, detect, and respond to insider threats and to limit their impact. The program should have the active participation of the functional organizations across the business such as Risk, IT, Cybersecurity, Physical Security, Human Resources, Fraud, and General Counsel.
The program should include the following:

- Creation and oversight of policies
- Regularized workflow, processes, and meetings to actively and collectively review threat intelligence
- Implementation and oversight of personnel reliability processes from pre-employment background checks to off-boarding procedures to assess and act upon personnel security risks
- Definition of requirements for employee training and awareness of insider threats and prevention measures

Building and operating security controls
Many of the security controls that already exist (or should exist) within the enterprise can be effective in detecting and preventing the results of insider threat activity.
Key technical controls include the following:

- Access controls and data protection
- Data loss prevention technology, data backups and exfiltration monitoring
- Configuration management for secure configurations

Monitoring and detecting insider behaviour
The program should seek to prevent insider attacks by capturing observable indicators of potential activity before insiders act. Intelligence on the insider threat generally comes from within the enterprise through either technical data or behavioural indicators:

Technical:
The most significant sources of cyber-related technical intelligence are the real-time alerts and outputs of security appliances, network- and host-based sensors, and data loss prevention tools.

Non-technical:
Unique to the insider threat is the availability of a large amount of relevant non-technical behavioural observable. Integrating operational intelligence information at the intersection of cybersecurity, fraud detection, and physical security can yield critical insights about potential insider threats.
Examples of non-technical cyber data includes the following:

- Email behaviour and workday activities
- Job performance
- Indicators of affiliation: degree of participation in company

Analysis of this type of data through automated and manual processes can identify patterns of behaviour that indicate at-risk employees or imminent insider attacks.

E13.062018

WALSONS BUILDING FAITH

For Security Solutions:
Call: +919717495402
Email: contact.us@securitas-india.com

For Background Verification:
Call: +91 9978990585
Email: ev.screen@securitas-india.com

www.securitas.in
National Command Centre : 1800 103 8797