February 21, 2020

www.pica.net

Insider Threats - 5 Minute Quick Training©

Are you and your company addressing the insider threat risk? Does your current risk assessment include insider threats? PICA's 5-Minute Quick Training © provides basic talking points for use with your CEO, risk management, human resources, and security teams.

What is an Insider threat? A current or former employee, contractor, or business partner who has (or had) authorized access to an organization's resources or facilities and has an unforeseeable financial or emotional need triggered by a perceived or real threat or opportunity. FBI statistics indicate that 72% of all thefts, fraud, sabotage, and accidents are caused by a company's own employees. Another 15 to 20% comes from contractors and consultants. Only about 5%to 8% is attributed to outsiders. Insider threats generally fall into one of three categories of employees: negligent, exploited, or malicious.

Types of Insider Threats:

- Fraud/Theft (physical or intellectual property)
- Physical and/or Cyber Sabotage
- Workplace violence
- Accidental leaks

Prevention Quick Tips:

Fraud

- Identify and track anomalies in financial systems
- Dual approval for changes to address or electronic payments for vendors
- Positive pay
- Spam training

Theft of intellectual property (personal gain or on behalf of a foreign government)

- Policies prohibiting or restricting personal external hard drives
- Limit amount of data that can be downloaded or sent external via Email
- Segregation of duties (does everyone need access to everything?)
- Classification of data and access restrictions.

Sabotage (Physical and Cyber)

- Identify high risk individuals
- Track recurring issues
- Access audits
- Predictive analytics

Workplace violence

- Supervisory training for red flags (indicators of potential violence)
- Pre-employment background checks and drug testing
- Physical security
- Employee+ assistance programs
- Active shooter training

Summary

Insider threats are an important component of a holistic risk management, loss prevention, and security strategy. It is important to clearly document and consistently enforce policies and controls, monitor, track and respond to suspicious or disruptive behavior and anticipate and manage negative issues.

Contact PICA Corporation for additional information or support.

Visit our Website