KPMG

Cyber security

What is an insider threat?

By Dharmik Karania

Insider threat is an active and complicated threat which affects all organizations in both the private and public sector.
An insider is any individual who has/ had authorized access to company resources. These resources can include but not limited to information about business strategy, payroll information, pricing and cost information, trade secrets, organization strengths, weaknesses and future plans.
Insider threat is the risk that the individual will use this classified data to cause harm to the organization. This can happen unintentionally through negligence or by an accident or intentionally for financial gain or to sabotage.
The National Institute of Standards and Technology (NIST) has published guidelines related to insider threats. NIST special publication 800-53, Revision 5 entitled "Security and Privacy controls for information systems and organizations" includes controls and guidelines for addressing insider threats as part of its comprehensive cybersecurity framework.

> Insider threat is the risk that the individual will use this classified data to cause harm to the organization.

Dharmik Karania
IT Audit Associate
KPMG Kenya
dkarania@kpmg.co.ke.

The views and opinions are those of the author and do not necessarily represent the views and opinions of KPMG.

NIST 800-53 addresses insider threats with best practices such as:

1. System Hardening by giving access to ONLY those resources needed by the individual to perform their job function
2. Perform enterprise-wide risk assessment.
3. Enforce clearly documented policies and controls.
4. Make use of a Security Information and Event Management System (SIEM) to log, monitor actions on the network.
5. Ensure regular back-ups of data is performed.
6. Regular awareness and training plan for all employees.
7. Establish procedures for responding to security incidents.
8. Ensuring background checks, personnel screening, and security clearance is obtained for all employees.

How can KPMG assist?

KPMG can support your organization strengthen its cyber defences in the following ways.

- Cyber Maturity Assessment (CMA)
- Incident response readiness and planning review.
- Vulnerability assessment and Penetration Testing (VAPT)
- Third-party security risk management review
- Cyber risk quantification