INSIDER THREAT TIP CARD

We often think of cyber threats as coming from an anonymous criminal, hundreds of miles away behind a computer screen. However, current and former employees who have intimate and valuable knowledge about a company are also capable of committing a cybercrime.

An insider threat occurs when a current or former employee, contractor, or business partner who has or had authorized access to an organization’s network, system, or data, intentionally misuses that access in a manner to commit a cybercrime.¹

DID YOU KNOW?

- 28 percent of electricity events were known to be caused by insider threats.²
- 46 percent of the most costly cybercrime events were a result of an insider threat.³
- 34 percent of insider threat cases were targeted towards collecting personally identifiable information (PII).⁴

TIPS TO MITIGATE INSIDER THREATS

Insider threats are a result of a combination of organizational, behavioral, and technical issues. The Department of Homeland Security’s United States Computer Emergency Readiness Team (US-CERT) recommends the following best practices for addressing these issues and mitigating an insider threat:

- Incorporate insider threat awareness into periodic security training for all employees.
- Implement strict password and account management policies and practices.
- Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
- Ensure that sensitive information is available to only those who require access to it.
- Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.
- Develop a formal insider threat mitigation program.

BEHAVIORAL INDICATORS

A good way to prevent an insider threat is to train your employees to recognize some common behavioral indicators among their colleagues. US-CERT has identified the following behavioral indicators of malicious threat activity:

² Ibid
³ Ibid
⁴ Carnegie Mellon University, "Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector" 2012.
• Remotely accesses the network while on vacation, when sick, or at odd times during the day.
• Works odd hours without authorization.
• Unnecessarily copies material, especially if it is proprietary or classified.
• Expresses interest in matters outside the scope of their duties.
• Shows signs of drug or alcohol abuse, financial difficulties, gambling, illegal activities, poor mental health, or hostile behavior.

IF YOU’VE BEEN COMPROMISED

• Follow your organization’s rules and regulations regarding cyber threats.
• Report computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or www.us-cert.gov.
• Inform local law enforcement as appropriate.
• Report stolen finances or identities and other cybercrimes to the Internet Crime Complaint Center at www.ic3.gov.
• Report fraud to Federal Trade Commission at www.FTCComplaintAssistant.gov

RESOURCES AVAILABLE TO YOU

**US-CERT.gov**

**IC3.gov**
If you are a victim of online crime, file a complaint with the Internet Crime Complaint Center (IC3) at www.ic3.gov.

**FTC.gov**