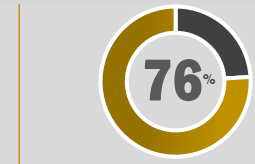
BTAC BULLETIN

BEHAVIORAL SCIENCE | LAW ENFORCEMENT & COUNTERINTELLIGENCE | CYBERSECURITY I EMPLOYEE MANAGEMENT RELATIONS I THREAT ASSESSMENT & MANAGEMENT

CYBER THREATS

CYBERSECURITY AND THE InT ENTERPRISE

The Department of Defense (DoD) relies on critical communications and network infrastructures, systems, and data to enable mission success. Such reliance requires advanced technical security systems, professionals, and leadership to detect, deter, and mitigate threats from a technical and human Insider Threat (InT) perspective. In most organizations, the Chief Information Security Officer (CISO) serves as a catalyst for aligning protective cybersecurity measures with organizational requirements to meet an everchanging threat landscape and ensuring stakeholder and leadership awareness of risk impacting mission success. The integration of cybersecurity as part of the insider threat multi-disciplinary team, enables the nexus between human behaviors, risk indicators, and cyber manifestation required to proactively detect behavioral indicators and effectively coordinate cyber security mitigation strategies with the insider threat professionals.



76% of organizations reported cyber insider attacks in 2024, an increase from 66% in 2019[1].

CYBERSECURITY INDICATORS[3]

1. **Access and permission "testing":** *Attempting access to files and services without a need to know*
2. **Data exfiltration and excessive printing/copying prior to departure**
3. **Using personal accounts/ devices for official use**
4. **Unexplained computer configuration changes**
5. **Unauthorized data deletion, modification**
6. **Mobile devices in unauthorized spaces**
7. **Unusual accounts, services, and files outside network baselines**
8. **Threatening or nonsensical online correspondence**
9. **Privilege escalation:** *Privileged escalation through unsolicited request or technical exploitation*

CYBER DETECTION

Concerning behaviors often materialize in the cyber domain undetected by rudimentary tools lacking the real-time analytic and collaborative capabilities required to identify and report nuanced behaviors. The CISO creates a symbiotic relationship with the InT multidisciplinary team by advocating for advanced technologies and fostering a cybersecurity incident response strategy that incorporates behavioral based incidents as a critical element of a proactive InT program.

Advanced technology and strategies that expand User Activity Monitoring (UAM) include:

- Artificial Intelligence (AI) and machine learning capabilities offered by Extended Detection and Response (XDR) and User and Entity Behavior Analytics (UEBA)
- Mobile device and removable media data exfiltration prevention using Mobile Device Management (MDM), Data Loss Prevention (DLP), and wireless intrusion detection/prevention technologies
- Adopt zero trust assumed breach strategy that restricts user, privileged user, and device permissions to limit potential damage across security domains

CYBER MITIGATION[2]

The coordination of mitigation strategies between the CISO and the InT Program is vital for information sharing and comprehensive threat mitigation planning.

- Stakeholder collaboration to identify and prioritize critical data.
- Symbiotic multidisciplinary InT relationship; enable indicator, incident, and data sharing.
- Promote a security aware culture, conduct periodic awareness training
- Leverage advanced solutions to identify behaviors and close security gaps.
- Enable strict access control and multi-factor authentication to buildings and systems
- Create an employee screening and exit strategy plan

TAKE OUR SURVEY
Give feedback on the BTAC Bulletin.
(Right click and copy link to a new window)

1. Cybersecurity Insiders. (2024). *2024 Insider Threat Report* 2. Randazzo, M.R., Keeney, M., Kowalski, E., United States Secret Service's National Threat Assessment Center, Cappelli, D. (2005, June). "Illicit Threat Study: Illicit Cyber Activity in the Banking and Finance Sector." 2. Critical Infrastructure and Security Agency (2020, November). Insider Threat Mitigation Guide. 3. Center for Development of Security Excellence (CDSE) (2021, November). *Insider Threat Potential Risk Indicators (PRI) Job Aid*.