Air Mobility Command
National Cybersecurity Awareness Month
Newsletter

26 October 2020 Vol 1 Issue 4

Do Your Part.

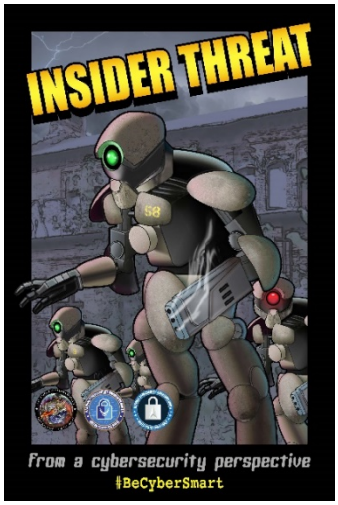
#BeCyberSmart

October is National Cyber Cybersecurity Month

Week 4: Insider Threat

For more information contact your Wing CyberSecurity Office or e-mail the HQ AMC Cybersecurity Office at AMC.Cybersecurity@us.af.mil

What is Insider Threat: According to the National Insider Threat Task Force (NITTF), "an insider is any person with authorized access to an organization's resources to include personnel, facilities, information, equipment, networks, or systems."
The NITTF defines the insider threat as "the risk [that] an insider will use their authorized access, wittingly or unwittingly, to do harm to their organization. This can include theft of proprietary information and technology; damage to company facilities, systems or equipment; actual or threatened harm to employees; or other actions that would prevent the company from carrying out its normal business practice." https://www.cisa.gov/insider-threat-mitigation

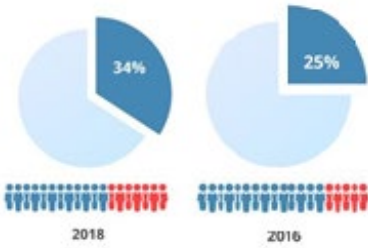


Insider Threats In Action

A disgruntled Texas medical clinic system administrator was asked to resign. Two days after he left, the former employee found his credentials were still active so he created a new admin account and subsequently disabled all other admin accounts then deleted all business data and patient medical records. A year later he ordered 11 iPads using the clinic's account and had them delivered to his house. The FBI eventually caught up with him and he was sentenced to 27 months in prison. https://www.bleepingcomputer.com/news/security

A California security company security guard used an administrative password to access the payroll server and tampered with his timecards for an extra $6,071. The guard was fired once his activities were discovered but 2 weeks later, he hacked into the company's servers to delete emails, software, databases, and backup files. The former employee was fined $318,000 for the company's lost data and income. https://www.bleepingcomputer.com/news/security

Percentage of Companies Impacted By Malicious Insiders



Increase in Cost to Remediate

Source: https://www.ekransystem.com/en/blog/ insider-threat-statistics-facts-and-figures

Five Types of Insider Threat Actors To Look Out For

Careless Worker
Employees or partners Who neglect or ignore the rules of an organization's cybersecurity policy

Inside Agents
Malicious insiders recruited by external parties to sell, alter, tamper with or delete valuable data

Disgruntled Employees
Emotional attackers who seek to harm their organization for some sort of perceived wrong

Malicious Insiders
Employees or partners who use their legitimate access to corporate data for personal gain

Third Parties
Third-party vendors who misuse their access and compromise the security of sensitive data

Be Digitally Adept - Methods to Address the Insider Threat

- Know what good cybersecurity practices are so when you see something abnormal you can ask questions and/or report the activity. Developing a rapport with your colleagues can help identify uncharacteristic behaviors. This may lead to uncovering an insider incident.
- Reoccurring Insider Threat training is important. It reminds us of the key indicators, threats, and how careless actions can impact security. We are all critical sensors to protecting the AMC mission and our personal information. Do You Part. #BeCyberSmart