VIDEO/Podcasts/vlogs This video and all related information and materials ("materials") are owned by Carnegie Mellon University. These materials are provided on an "as-is" "as available" basis without any warranties and solely for your personal viewing and use. You agree that Carnegie Mellon is not liable with respect to any materials received by you as a result of viewing the video, or using referenced web sites, and/or for any consequence or the use by you of such materials. By viewing, downloading and/or using this video and related materials, you agree that you have read and agree to our terms of use (http://www.sei.cmu.edu/legal/index.cfm).

DM19-0876

Title: Insider Threat Mitigation, We can help!

Hello, this is Randy Trzeciak from the CERT Division with your SEI Cyber Minute.

September 2019 has been designated "Insider Threat Awareness" month by the FBI, DHS and OUSD.

As stated, by the sponsors of Insider Threat awareness month, past compromises of national security information by insiders have made America less safe by providing sensitive information to our adversaries.

Since 2001, CERT's National Insider Threat Center has been assisting the Department of Defense, the U.S. Government, Law Enforcement, Industry, and Academia to identify and mitigate threats posed to critical assets by trusted insiders. Threats can originate from current or former employees, trusted business partners, including contractors, sub-contractors, cloud services providers, others in your supply chain, or any other individual granted electronic or physical access to your critical assets.

The foundation of our research is an empirical data set of nearly 3000 incidents where insiders, either with malicious intent or unintentionally, impacted the confidentially, integrity, or availably of a critical system, service, or data set. This data allows us to be a leading edge, applied-research organization, providing guidance and support to information security programs and practitioners around the world.

If you are an organization required to comply with Executive Order 13587 or NISPOM Conforming Change 2, requiring you to build a formal insider threat program, OR if you are an organization not mandated to build a formal program but you are interested in addressing these threats, here's how we can help.

On our insider threat website, you will find over 125 publications with actionable intelligence on insider threat mitigation.

Recent publications include:

- The Common Sense Guide to Mitigating Insider Threats, Sixth Edition, which is a collection of 21 best practices for insider threat mitigation, complete with case studies and statistics
- Balancing Organizational Incentives to Counter Insider Threat, a study on how positive incentives can complement traditional security practices to provide a better balance for organizations' insider threat programs
- Navigating the Insider Threat Tool Landscape: Low Cost Technical Solutions to Jump-Start an Insider Threat Program, an exploration of the types of tools that organizations can use to prevent, detect, and respond to multiple types of insider threats

In addition to the technical notes and reports, you can also keep up to date on our research by following our insider threat blog. We recently completed an insider threat blog series describing:

- Patterns and Trends in Insider Threats across Industry Sectors. This series describes insider threat patterns and trends in
    - Entertainment
    - Healthcare
    - Information Technology
    - State and Local Government

  - Finance and Insurance, and
  - Federal Government

We also assist organizations by measuring the effectiveness of their insider threat mitigation capabilities by performing:

- Insider Threat Vulnerability Assessments, and
- Insider Threat Program Evaluations
- Insider Threat Trainings

Thank you for watching this SEI Cyber Minute. For more information, please visit the SEI Website to find additional resources available to you or send me an email message at info@sei.cmu.edu.