Franklin Stevens

Professor Charles Alexander

ENGV 306 Advanced Composition

Miscalculations: The misinterpretations of insider threats

Ansbach, J., & Sharton, B. (2020, September 1). *Risk Management Magazine - Preventing Insider Threats to Cybersecurity*. Risk Management Society. Retrieved May 30, 2022, from <https://www.rmmagazine.com/articles/article/2020/09/01/-Preventing-Insider-Threats-to-Cybersecurity->

Describes how insiders can intentionally and unintentionally cause attacks—workplaces going home with no training on connecting to networks or using the equipment. Additionally, intentional could be caused due to losing jobs or returning to the office.

Burkett, R. (2013, March). *An Alternative Framework for Agent Recruitment: From MICE to RASCLS*. Calhoun: Institutional Archive of the Naval Postgraduate School. Retrieved May 30, 2022, from <https://calhoun.nps.edu/bitstream/handle/10945/43831/Burkett-MICE%20to%20RASCALS_2013.pdf?sequence=1&isAllowed=y>

Cybersecurity and insider threats in the present day. Individuals will turn into insiders for themselves or others. Pay and benefits mean nothing when they seem coercive. We must root out the practice by attacking the ideology. Where do we strike the doctrine?

Insider Threat definitions and current legalese regarding state and corporate definitions

Why people turn - CIA employment in turning people compared to several articles on individual liberties are being taken.

It is an opinion of those fighting for their rights, corporations perceiving this as a threat and employing tactics and strategies to stop it. Punishment?

Why are governments not paying attention?

Aftermath and an example of the battlefield that can take place. Why doctrine and regulations will have the opposite effect that governments and corporations hope to achieve.

\

CBS Interactive Inc. (2022, April 17). *Russian hacking group compromised US power companies - 60 Minutes*. CBS News. Retrieved May 30, 2022, from <https://www.cbsnews.com/news/russian-hacking-group-u-s-power-companies-60-minutes-2022-04-17/>

APT’s are rampant and are especially true with the war going on. The article mentions getting access into highly restrictive areas but lacks mentioning the culprits responsible. Russians and Chinese have used insiders before, even turning FBI agents. You should be able to find the links to the papers.

CISA. (n.d.). *Defining Insider Threats*. CISA. Retrieved May 30, 2022, from <https://www.cisa.gov/defining-insider-threats>

The government organization CISA, Cybersecurity and Infrastructure Agency, defines an insider as a member, whether past or present, of an organization with trusted access to sensitive material and processes. They then exploit this trust for various purposes and can provide access to different people or other organizations. Their advanced knowledge of business and security practices gives them enormous flexibility to conduct espionage. This is also the case for unwitting personnel who provide material to others without their knowledge. Espionage is not the only method available to them, as they can also conduct violence, sabotage, and cyber attacks. The article does not explain why individuals or groups become insiders, though.

Costa, D. (2017, March 7). *CERT Definition of 'Insider Threat' - Updated*. SEI Blog. Retrieved May 30, 2022, from <https://insights.sei.cmu.edu/blog/cert-definition-of-insider-threat-updated/>

Daniel Costa from Carnegie Mellon explains insider threats in a broader organizational sense and includes Community Emergency Response Team definitions. Largely the definitions and thinking seem to be the same. Insider Threats are those who have access to trusted material and take that material for some purpose. They can utilize several methods to gain this material, including violent and non-violent. The question is, why? What makes people turn?

Etchie, M. (2021, October 22). *The Biggest Cyber Threat Isn't Hackers, It's Insider Threats*. Infosecurity Magazine. Retrieved May 30, 2022, from <https://www.infosecurity-magazine.com/next-gen-infosec/cyber-threats-hackers-insider/>

Malicious insider threats and some information about why the attacks take place. Very general outline. It does not go into the aspects of individuals and, more importantly, why they choose to conduct their attacks.

Gatlan, S. (2021, September 1). *Fired NY credit union employee nukes 21GB of data in revenge*. Bleeping Computer. Retrieved May 30, 2022, from <https://www.bleepingcomputer.com/news/security/fired-ny-credit-union-employee-nukes-21gb-of-data-in-revenge/>

The article goes over an insider attack at a New York Credit Union. Juliana Barile destroyed 21 GB of data related to mortgage loans and other files on the filer server. This was an act of revenge due to her firing, but it doesn’t describe why. Some misconfigurations allowed her to access the server, despite receiving the request for termination and account suspension.

*ICE Is a Domestic Surveillance Agency*. (2022, May 11). Schneier on Security. Retrieved May 30, 2022, from <https://www.schneier.com/blog/archives/2022/05/ice-is-a-domestic-surveillance-agency.html>

ICE is regarded as a domestic surveillance agency. They freely employ avenues to spy on people with “billions of data points” from private companies to spy on people with no judicial provocation. Homeland Security has a nearly infinite budget but continues its enforcement unchallenged while infuriating the citizens it stands for.

James, D. (2022, May 16). *IT admin gets 7 years for wiping his company's servers to prove a point*. PC Gamer. Retrieved May 30, 2022, from <https://www.pcgamer.com/it-admin-gets-7-years-for-wiping-his-companys-servers-to-prove-a-point/>

A senior IT professional had several points about the lack of security emplacements and that they felt like they were being ignored. Then, in defiance, she completely deleted Lianjia, a real estate company in China. Han Bing and others are culprits in the matter and are a part of the security team. Bing remotely connected to the server and wiped it, something the company thought was impossible. It indicates lax security procedures, but what about Bing? Could things have been different had they listened or attempted to listen to them?

114th Congress. (2016, July 12). *Text - H.R.3361 - 114th Congress (2015-2016): Department of Homeland Security Insider Threat and Mitigation Act of 2016*. Congress.gov. Retrieved May 30, 2022, from <https://www.congress.gov/bill/114th-congress/house-bill/3361/text>

A congressional bill that marks the Insider Threat Act, marking it as a crime and denotes the definitions of individuals, groups, and their actions.

Pipikaite, A., Barrachin, M., & Crawford, S. (2021, January 21). *These are the top cybersecurity challenges of 2021 | World Economic Forum*. The World Economic Forum. Retrieved May 30, 2022, from <https://www.weforum.org/agenda/2021/01/top-cybersecurity-challenges-of-2021/>

Top challenges of cybersecurity. It lists dependence, lack of expertise, lack of prosecuting criminals, and increasing complexity in cybersecurity attacks. The article stresses that organizations must remain flexible and accountable to keep pace. Why then is it so difficult to support individuals in these organizations? The lack of prosecution of cybercriminals is alarming. Are they choosing to go “rogue” once they obtain the prerequisite skills?

Reddit. (n.d.). *r/anti-work*. Reddit.com. Retrieved May 30, 2022, from <https://www.reddit.com/r/antiwork/comments/umkrob/antiwork_from_i_quit_to_we_revolt/?utm_source=share&utm_medium=ios_app&utm_name=iossmf>

The theory behind insider threats - is the concept that enough is enough in a world where the perception is to work to death and obtain nothing from it. When capitalism seems exploitative, then people fight fire with fire. They no longer care about the repercussions because they theorize it is far worse to stay than fight for their own.

Rhysider, J. (2022, March 21). *Adam – Darknet Diaries*. Darknet Diaries. Retrieved May 30, 2022, from <https://darknetdiaries.com/episode/113/>

This is an excellent episode from Darknet Diaries that highlights the perspective of why an individual chooses to perform their attacks. In this instance, Adam highlights that he was highlighted for a criminal record by being fired, despite already doing time, having no reason to fire him, and a lack of communication combined with an unempathetic demeanor. Is it the practice of IT to secure networks, or should employers and HR staff stop responding with antiquated beliefs and principles to employees?

Darknet diaries highlight several reasons people would defect from their employer and become insiders. Numerous stories highlight the underground world. Most of them all begin with some belief in mind, some nobler than others, but the central concept is that they do it to make money. Perhaps insider attacks are more easily accomplished because there is more to gain by doing it than not doing it? If these people had avenues to which they could go so they wouldn’t have to become insiders, would we see insider attacks fall?

Rosenthal, M. (2022, March 22). *17 Real Insider Threat Examples*. Tessian. Retrieved May 30, 2022, from <https://www.tessian.com/blog/insider-threats-types-and-real-world-examples/>

This article details Insider threat attacks and some specifics about individuals. It does not go into why those particular individuals went to those extremes. It did mention one about an individual being furloughed and who subsequently attacked the company and stole material. The problem here is why did they lay that person off? Someone who had a demonstrative ability to continue working was let go for what purpose?

Shabad, R. (2022, May 10). *Treasury Secretary Yellen says reversing Roe v. Wade would have 'damaging effects on the economy'*. NBC News. Retrieved May 30, 2022, from <https://www.nbcnews.com/politics/politics-news/treasury-sec-yellen-says-reversing-roe-v-wade-damaging-effects-economy-rcna28150>

The ideals of Insider Threats intertwine with the world around them. People will often go to extremes for their dreams and, more importantly, to survive. Would it stand to reason that if people had no choice, they would have no other choice?

Toulas, B. (2022, May 14). *Angry IT admin wipes employer's databases, gets 7 years in prison*. Bleeping Computer. Retrieved May 30, 2022, from <https://www.bleepingcomputer.com/news/security/angry-it-admin-wipes-employer-s-databases-gets-7-years-in-prison/>

This article describes the one above but from a different source.

US Department of Justice. (2021, August 31). *Brooklyn Woman Pleads Guilty to Unauthorized Intrusion into Credit Union's Computer System*. Department of Justice. Retrieved May 30, 2022, from <https://www.justice.gov/usao-edny/pr/brooklyn-woman-pleads-guilty-unauthorized-intrusion-credit-union-s-computer-system>

A Justice department article regarding additional insider threat attacks and why they occurred: still doesn’t describe why in very much detail.