THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Office of Research Security Newsletter

February 2020

Protecting Your Most Valuable Assets: How to Identify and Maintain Your Institution's Trade Secrets

An institution's trade secrets generally include confidential information with commercial value. Trade secret protection may be available by common law, under state laws, or under federal law. In addition, there may be both civil and criminal causes of action for the misappropriation and theft of trade secrets.

For instance, the Defend Trade Secrets Act of 2016 (DTSA) is a United States federal law that allows an owner of a trade secret to sue in federal court when its trade secrets have been misappropriated through "improper means."[1] Such "improper means" can include "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means."[2]

Trade secrets can be used by institutions to protect numerous types of information… Moreover, trade secrets can have an indefinite life, so long as they are kept secret and confidential...However, institutions must take numerous steps in order to maintain the enforceability of their trade secrets. Such steps include: (1) identifying the trade secrets; and (2) taking "reasonable measures" to maintain the secrecy of the trade secrets.

https://www.natlawreview.com/article/protecting-your-most-valuable-assets-how-to-identify-and-maintain-your-institution-s

2020 Annual Security Refresher Training

Please don't wait until the end of 2020 to complete this required training

Location: Bob Jones Auditorium, Redstone Arsenal

April 28, 2020 – 12pm-2pm
May 11, 2020 – 11am-1pm
June 3, 2020 – 11am-1pm
June 25, 2020 – 11am-1pm
July 27, 2020 – 11:30am-2pm

Location: Von Braun Research Hall room M50, UAH

April 8, 2020 – 10:30am-1:00pm
April 29, 2020 – 9:30am-11:30am
May 13, 2020 – 9:30am-11:30am
May 27, 2020 – 9:30am-11:30am

Harvard Chemistry Chairman Charged on Alleged Undisclosed Ties to China

Charles Lieber is accused of lying to Defense Department, National Institutes of Health about Chinese government funding

By Aruna Viswanatha and Kate O'Keeffe

The chairman of Harvard University's chemistry department was arrested on charges of lying about receiving millions of dollars in Chinese funding, in an escalation of U.S. efforts to counter what officials said is a plot by Beijing to mine U.S. universities to catapult China to the forefront of scientific development.

A federal criminal complaint alleges that Charles Lieber, a pioneer in nanotechnology, misled the Defense Department and the National Institutes of Health about his participation in China's Thousand Talents Plan while the U.S. agencies were spending more than $15 million to fund his research group in the U.S.

Through its government-backed Thousand Talents Plan and hundreds of similar programs, China pays scientists around the world to moonlight at Chinese institutions, often without disclosing the work to their primary employers.

The case was one of three presented Tuesday by federal authorities in Massachusetts, with each underscoring U.S. concerns that the Chinese government is trying to obtain cutting-edge U.S. research by exploiting U.S. universities and their professors and researchers. Prosecutors have brought a series of cases charging Chinese Americans and Chinese nationals working in the U.S., prompting concern in the scientific community that authorities were racially profiling people. Mr. Lieber is among the first non-Chinese scientists and highest-profile targets to date.

https://www.wsj.com/articles/harvards-chemistry-chair-charged-on-alleged-undisclosed-ties-to-china-11580228768

Disk-wiping malware, phishing and espionage: How Iran's cyber attack capabilities stack up

US warns that cyberattacks could be part of Iran's plans as tensions rise. This is what Iran's current offensive cyber capabilities look like.

By Steve Ranger

Tensions between the United States and Iran are raised after the killing of Iranian IRGC-Quds Force commander Qassem Soleimani via a US drone strike while he was in Iraq. Iranian leaders have vowed to retaliate against the US, with the US Department of Homeland Security warning that previous Iranian plans have included "cyber-enabled" attacks against a range of US targets.

So, if Iran decided to use cyber means to respond, what would that potentially look like?

Iran has long been seen as one of the four countries that pose the greatest online threats to the US, along with China, Russia and North Korea, and there has been a long history of Iranian cyber intrusions against the US.

https://www.zdnet.com/article/hard-disk-wiping-malware-phishing-and-espionage-how-irans-cyber-capabilities-stack-up/

OFFICE OF RESEARCH SECURITY STAFF

DENISE SPILLER

Security Administrator

824-6444

denise.spiller@uah.edu

JANINE WILISON

Associate Security Administrator

824-3025

janine.wilson@uah.edu

APRIL MCMEANS

Assistant Security Administrator

824-6048

april.mcmeans@uah.edu

CAITLYN SCHOENIG

Security Assistant

824-4717

caitlyn.schoenig@uah.edu

MARIAH WILKINSON

Student Specialist II

824-4818

mariah.wilkinson @uah.edu

RYAN WILKINSON

Student Specialist I

824-4717

ryan.wilkinson @uah.edu