ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

https://asce.tamus.edu

THE OPEN SOURCE
MEDIA SUMMARY

December 30, 2020

INSIDER THREAT PROGRAM MATURITY FRAMEWORK

National Insider Threat Task Force

The National Insider Threat Task Force (NITTF) is charged under Executive Order (EO) 13587 with reviewing and, when appropriate, adding to or modifying the Minimum Standards1 and guidance in coordination with the executive branch departments and agencies (D/As) subject to the EO. The Minimum Standards provide the basic elements necessary to establish a fully functional insider threat program (InTP) and thereby serve as milestones in the InTP maturity process. The insider threat is a dynamic problem set, requiring resilient and adaptable programs to address an evolving threat landscape, advances in technology, and organizational change. The effort requires continual evaluation and updated perspectives and approaches. In furtherance of this effort, the NITTF has developed, in collaboration with executive branch D/As, an InTP Maturity Framework (hereafter referred to as "Framework") to enhance the Minimum Standards. The Framework identifies key elements within the Minimum Standards construct to enable D/As to increase the effectiveness of program functionality, garner greater benefit from InTP resources, procedures, and processes, and tightly integrate InTP procedures and objectives with their distinct missions and challenges.

Read the full article here.

TRY AS IT MIGHT, AMERICA CANNOT STOP FOREIGN CYBER SNOOPING

David V. Gioe | The National Interest | December 23, 2020

Americans concerned about cybersecurity and foreign influence operations may have been tempted to collectively exhale a sigh of relief in the immediate aftermath of the recent presidential election. Years of investment in election security seemed to have paid off. Over a month after the 2020 election, there have been no confirmed cases of foreign entities penetrating America's electoral infrastructure to change vote tallies. Before he was abruptly fired, Cybersecurity and Infrastructure Security Agency (CISA) Director Christopher Krebs claimed his agency had no evidence that the election was tampered with by foreign adversaries. Any hopeful feelings that the United States may have turned a corner in cybersecurity or that Russian intelligence officers were either deterred from targeting the United States or simply snoozing at their keyboards were dashed this week when the Trump administration acknowledged a massive cybersecurity breach that may have enabled Russian intelligence to steal enormous amounts of information from across key federal agencies and departments, including the State Department, the Department of Homeland Security, Treasury, Commerce, and parts of the Pentagon.

Read the full article here.

TECH GIANTS ARE GIVING CHINA A VITAL EDGE IN ESPIONAGE

Zach Dorfman | Foreign Policy | December 23, 2020

In 2017, as U.S. President Donald Trump began his trade war with China, another battle raged behind the scenes. The simmering, decadelong conflict over data between Chinese and U.S. intelligence agencies was heating up, driven both by the ambitions of an increasingly confident Beijing and by the conviction of key players in the new administration in Washington that China was presenting an economic, political, and national security challenge on a scale the United States had not faced for decades—if ever. Beijing was giving China hawks in the United States plenty of ammunition. That same year, hackers working for China's People's Liberation Army would mastermind a massive breach of Equifax, one of the United States' largest credit reporting firms. The military-linked hackers absconded with a dizzying amount of personal data, including Social Security numbers, home addresses, birth dates, driver's license numbers, and credit card information. Roughly 145 million Americans had their personal data exposed by the hack.

Read the full article here.

INTERNATIONAL TRIO INDICTED IN AUSTIN FOR ILLEGAL EXPORTS TO RUSSIA

U.S. Department of Justice | December 18, 2020

A four–count federal grand jury indictment returned in Austin and unsealed today charges three foreign nationals – a Russian citizen and two Bulgarian citizens – with violating the International Emergency Economic Powers Act (IEEPA), Export Control Reform Act (ECRA), and a money laundering statute in a scheme to procure sensitive radiation-hardened circuits from the U.S. and ship those components to Russia through Bulgaria without required licenses. "Time and again, we find the Russians attempting to get access to sensitive American technology. The defendants here are charged with exporting radiation-hardened chips to Russia, knowing that it was illegal to do so and establishing a business in Bulgaria to circumvent U.S. enforcement authorities," said Assistant Attorney General for National Security John C. Demers. "I am gratified by our whole-of-government response to this flagrant example of U.S. export controls evasion." "Today's indictment demonstrates that the United States Attorney's Office, the Department of Justice and our federal partners will follow those who seek to evade U.S. export enforcement laws wherever our investigations lead. National security remains our highest priority. We must never allow our most sensitive technology to fall into the hands of those who would seek to use it against us," said U.S. Attorney Sofer.

Read the full article here.

OUR EXPERTS' 2021 FOREIGN INTERFERENCE POLICY WISHLIST

Alliance for Securing Democracy | December 21, 2020

Every December, the Alliance for Securing Democracy team tries to take a step back and look at the foreign interference landscape, and to take stock of where new laws and policies would have the greatest impact at strengthening our institutions from foreign interference and protecting our values. This effort is more important than ever this year, as the change of administration offers new opportunities to take action on a wide range of issues. We asked our experts to each put forth one recommendation that would make the United States, and the community of liberal democracies to which it belongs, safer, stronger, and freer. The breadth of the responses presents a wide range of domains in which progress can be made, while also illustrating the hydra-headed nature of the foreign interference threat.

Read the full article here.

IN THE MEDIA: UNIVERSITIES WARN FOREIGN INTERFERENCE MEASURES MUST BE 'CAREFULLY CALIBRATED'

Lisa Visentin, The Sydney Morning Herald | Group of Eight Australia | December 21, 2020

Australia's elite research universities have warned that partnerships with Chinese institutions, including those which have led to world-leading research developments, could be jeopardised if the Morrison government fails to carefully calibrate foreign interference measures. The Group of Eight, which represents the eight universities that account for 70 per cent of academic research, says the collaboration of University of Sydney professor Edward Holmes in the first genome sequencing of COVID-19 – a project involving a consortium of Chinese universities and institutions – is a key example of research that "might not have occurred" under stricter policy settings. It also highlighted as another example the work of Monash University Professor Paul Zimmet AO in an international team, which included Peking University Professor Linong Ji, that found that elderly people with diabetes who contracted COVID-19 faced a much higher risk of dying.

Read the full article here.

RUSSIAN HACKERS COMPROMISED MICROSOFT CLOUD CUSTOMERS THROUGH THIRD PARTY, PUTTING EMAILS AND OTHER DATA AT RISK

Ellen Nakashima | The Washington Post | December 24, 2020

Russian government hackers have compromised Microsoft cloud customers and stolen emails from at least one private-sector company, according to people familiar with the matter, a worrying development in Moscow's ongoing cyberespionage campaign targeting numerous U.S. agencies and corporate computer networks. The intrusions appear to have occurred via a Microsoft corporate partner that handles cloud-access services, those familiar with the matter said. They did not identify the partner or the company known to have had emails stolen. Like others, these people spoke on the condition of anonymity to discuss what remains a highly sensitive subject. Microsoft hasn't publicly commented on the intrusions. On Thursday, an executive with the tech giant sought to downplay the issue's significance. "Our investigation of recent attacks has found incidents involving abuse of credentials to gain access, which can come in several forms," Jeff Jones, Microsoft's senior director for communications, said.

Read the full article here.

DHS WARNS US BUSINESSES OF CHINA'S DATA-COLLECTION PRACTICES

Sean Lyngaas | CyberScoop | December 21, 2020

As Washington is absorbed with the fallout of a suspected Russian hacking operation against U.S. organizations, the Department of Homeland Security is warning American companies not to be complacent when it comes to cyberthreats from China. A 15-page "business advisory" released Tuesday by DHS cautions that Chinese intelligence services could collect and exploit data held by U.S. firms doing business in China, highlighting longstanding concerns from U.S. officials. Beijing has denied allegations of economic espionage. The advisory is an acknowledgement that, despite efforts by both the Trump and Obama administrations to curb China's alleged theft of intellectual property, it is still a rampant problem for U.S. officials. It comes after the top U.S. counterintelligence official said this month that China had increased its influence operations targeting incoming Biden administration personnel and their associates.

Read the full article here.

PARLIAMENTARY INQUIRY INTO NATIONAL SECURITY RISKS AFFECTING HIGHER EDUCATION

Peter Bentley | Innovative Research Universities | December 22, 2020

The IRU has responded to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) Inquiry into national security risks affecting the Australian higher education and research sector. The terms of reference for the inquiry target "foreign interference, undisclosed foreign influence, data theft and espionage", with the intent to assess how extensive these are for universities; how aware universities are about them; and how useful the Australian Government response and support are to minimise the risks to universities. Against the Inquiry's terms of reference, the IRU submission targets the fourth element concerning the "adequacy and effectiveness of Australian Government policies and programs" as the area where the Joint Committee can best advance an effective response to foreign interference in universities. The Inquiry will gather other evidence about the extent of the issue and universities' understanding of this.

Read the full article here.

MEASURES TAKEN BY THE GO8 TO MITIGATE THE THREAT OF FOREIGN INTERFERENCE IN ALIGNMENT WITH THE UFIT GUIDELINES

Governance and Risk Frameworks to mitigate the threat of foreign interference in alignment with the UFIT Guidelines from Australian National University, University of Adelaide, University of Melbourne, Monash University, University of Sydney, UNSW Sydney, University of Queensland, and the University of Western Australia.

Read the full document here.

WECHAT BECOMES A POWERFUL SURVEILLANCE TOOL EVERYWHERE IN CHINA

Jin Yang | The Wall Street Journal | December 22, 2020

China's do-everything app, WeChat , has become one of the most powerful tools in Beijing's arsenal for monitoring the public, censoring speech and punishing people who voice discontent with the government. Authorities are increasingly using the app from Tencent Holdings Ltd. to justify arrests or issue threats, say dissidents, consumers and security researchers. Wang Shengsheng, a labor and women's rights lawyer, said authorities were monitoring her WeChat and text messages earlier this year so they could gather evidence to thwart her legal career. Local public security and party discipline officials in her hometown also tracked down her father as part of their efforts to tarnish her reputation, she said. "People always say that all of your communications on WeChat are out in the open. I never fully grasped what that meant until the recent incident," she said. "Now I'm terrified."

Read the full article here.

"AMATEUR" MISTAKES SINK THIEVES OF U.S. TECHNOLOGY WORKING FOR CHINA

Scott Tong | Market Place | December 22, 2020

Quitting to join a competitor and lying about it. Googling "clear computer data" to hide one's digital tracks. Stuffing devices with stolen data into a locker during a police raid. Not exactly the hallmarks of professional corporate spies. A bungled theft of U.S. semiconductor secrets lies at the center of a Justice Department case against defendants linked to a state-owned Chinese chipmaker seeking production know-how. The rookie mistakes, analysts say, amount to a case study in what not to do in the high-stakes world of economic espionage. In the complex case, American investigators in October secured a guilty plea from United Microelectronics Corp. (UMC), a Taiwan-based semiconductor manufacturer, for "possessing and receiving a trade secret belonging to Micron Technology," an Idaho-based American chipmaker.

Read the full article here.

HOW RUSSIAN SPY GAMES MOVED ONLINE: MASSIVE BREACH SHOWS HOW ESPIONAGE IS CARRIED OUT IN THE 21ST CENTURY

Mike Snider and Jessica Guynn | USA Today | December 18, 2020

Forget KGB agents Russian intelligence officers masquerading as ordinary Americans to slip inside government agencies and steal national security secrets like in television's "The Americans." The massive cyber assault on the U.S. government and private companies perpetrated through networked computer systems is what 21st century espionage most commonly looks like. And these kinds of confrontations on a digital battlefield, cybersecurity researchers say, are our new normal. We are in a state of "unpeace," not quite war but close and potentially just as dangerous. In this case, a nation-state, believed to be Russia, infiltrated the software supply chain on which the nation relies.

Read the full article here.

WHY THE US GOVERNMENT HACK IS LITERALLY KEEPING SECURITY EXPERTS AWAKE AT NIGHT

Brian Fung | CNN Business | December 16, 2020

The US government is reeling from multiple data breaches at top federal agencies, the result of a worldwide hacking campaign with possible ties to Russia. Investigators are still trying to figure out how much of the government may have been affected and how badly it may have been compromised. But what little we know has cybersecurity experts extremely worried — with some describing the attack as a literal wakeup call. "I woke up in the middle of the night last night just sick to my stomach," said Theresa Payton, who served as White House Chief Information Officer under President George W. Bush. "On a scale of 1 to 10, I'm at a 9 — and it's not because of what I know; it's because of what we still don't know."

Read the full article here.