RESEARCH AND INNOVATION SECURITY AND COMPETITIVENESS INSTITUTE
THE TEXAS A&M UNIVERSITY SYSTEM

Open Source Media Summary

April 11, 2024

BIS SENIOR ENFORCEMENT OFFICIAL WARNS EXPORT INDUSTRY OF RISKS, CONSEQUENCES FOR LACK OF ROBUST COMPLIANCE

Kharon Staff | Kharon | March 31, 2024

A senior official at the U.S. Department of Commerce's Bureau of Industry and Security (BIS) gave a cautionary tale to companies in the export sector to start investing in their compliance programs early on rather than wait for an enforcement action to be taken against them to remediate. Speaking at BIS's annual update conference on March 28, Assistant Secretary for Export Enforcement Matthew Axelrod warned that companies trying to cut corners to finalize a deal is not worth it, as "the stakes have never been higher" given the current geopolitical landscape. "It's not worth prioritizing short-term profits over long-term reputational risk," Axelrod said. He emphasized that an effective and robust compliance program is essential in order to identify and manage risks with new or existing customers, suppliers, and distributors.

Read the full article here.

DOD CYBER OFFICIALS DETAIL PROGRESS ON ZERO TRUST FRAMEWORK ROADMAP

Joseph Clark | DOD News | April 3, 2024

The Defense Department is on track to implement its zero trust cybersecurity framework by the end of fiscal year 2027, senior Pentagon information technology officials said this week. David McKeown, who serves as the DOD's deputy chief information officer, underscored the significant progress the department has made in implementing what he said will be a transformational change in how the department approaches cybersecurity. "Zero trust integration offers the most robust and reliable approach to cybersecurity, ensuring that our systems are resilient against evolving threats, while safeguarding our nation's interests," McKeown said today during his keynote address as part of a virtual two-day Zero Trust Symposium hosted by the Defense Acquisition University. "It is not just a program, or a new application, zero trust is an evolution of our entire security landscape," he said. "By embracing it, we not only protect our data, but we strengthen our defenses and preserve our way of life."

Read the full article here.

A STEALTH ATTACK CAME CLOSE TO COMPROMISING THE WORLD'S COMPUTERS

The Economist | April 2, 2024

In 2020 XKCD, a popular online comic strip, published a cartoon depicting a teetering arrangement of blocks with the label: "all modern digital infrastructure". Perched precariously at the bottom, holding everything up, was a lone, slender brick: "A project some random person in Nebraska has been thanklessly maintaining since 2003." The illustration quickly became a cult classic among the technically minded, for it highlighted a harsh truth: the software at the heart of the internet is maintained not by giant corporations or sprawling bureaucracies but by a handful of earnest volunteers toiling in obscurity. A cyber-security scare in recent days shows how the result can be near disaster. On March 29th Andres Freund, an engineer at Microsoft, published a short detective story.

Read the full article here.

UNIVERSITIES OPPOSE FEDERAL PLAN TO BOLSTER RESEARCH MISCOUNDUCT OVERSIGHT

Kathryn Palmer | Inside Higher Education | April 2, 2024

The federal Office of Research Integrity (ORI) is proposing changes that would give the government more oversight of investigations of research misconduct at colleges and universities. But scores of university and research hospital leaders and the organizations representing them are opposed and say the proposed rules would be burdensome to institutions and could potentially deter people from reporting alleged research misconduct, among other perceived negative consequences. "The proposed regulations inappropriately fail to recognize that ORI and institutions conduct separate research misconduct review processes that are necessarily subject to different Standards," reads a letter the Council on Governmental Relations (COGR), which represents research institutions, wrote to ORI, which is under the U.S. Department of Health and Human Services.

Read the full article here.

CANADA'S BIOSECURITY SCANDAL: THE RISKS OF FOREIGN INTERFERENCE IN LIFE SCIENCES

Brendan Walker-Munro | The Strategist | April 2, 2024

In July 2019, world-renowned biological researchers Xiangguo Qiu and Keding Cheng were quietly walked out of the Canadian government's National Microbiology Lab (NML). The original allegation against them was that Qiu had authorised a shipment to China of some of the deadliest viruses on the planet, including Ebola and Nipah. Qiu and Cheng, a married couple, subsequently lost their security clearances and were then fired by the NML in January 2021. At the time, both were subject to investigations by the Royal Canadian Mounted Police and the Canadian Security Intelligence Service (CSIS). The NML said both had lost their positions for 'breaches of policy'; it did not say what those breaches or policies had been.

Read the full article here.

THE IC'S NEW OSINT STRATEGY GETS THE BASIC RIGHT

Emily Harding | Center for Strategic and International Studies | April 2, 2024

The intelligence community (IC) published its first-ever open-source intelligence (OSINT) strategy in March. It is a big-picture, priority setting document—an essential, basic step to re-launch OSINT as a serious intelligence discipline. The unclassified version may be thin on details, but it provides insight into the fundamental challenges the IC is facing trying to integrate OSINT into its current practices. OSINT has taken many forms over the years, but in this modern iteration, it is more powerful and more essential than it has ever been before. What once was largely translation work is now deriving unique insights from massive, public datasets, using the power of cloud computing and artificial intelligence (AI) to find all the needles in the haystack, and sharing those insights with a wide range of customers.

Read the full article here.

FEDERAL GOVERNMENT AFFECTED BY RUSSIAN BREACH OF MICROSOFT

Rebecca Heilweil, Tim Starks, AJ Vicens and Elias Groll | Cyberscoop | April 4, 2024

The Cybersecurity and Infrastructure Security Agency issued an emergency directive this week to address the impact on federal agencies from a breach of Microsoft carried out by a hacking unit linked to Russia's foreign intelligence agency, according to three government officials familiar with the matter. In a briefing Tuesday, CISA executives discussed with federal officials an operation believed to have been carried out by the hacking group known as Midnight Blizzard and discussed the directive. "CISA continues to provide guidance to Federal Civilian Executive Branch agencies regarding actions to secure accounts potentially placed at risk through the Midnight Blizzard campaign disclosed by Microsoft in January 2024," Scott McConnell, a spokesperson for the agency, told Scoop News Group on Wednesday.

Read the full article here.

THE FBI IS TELLING PASSENGERS TO AVOID USING USB CHARGING POINTS IN AIRPORTS BECAUSE THEY COULD INFECT YOUR PHONE WITH SPY MALWARE

Mateusz Maszczynski | PYOK | April 4, 2024

The FBI is warning airline passengers to avoid using free USB charging points in airports because they could be loaded with spy malware that will infect phones and other electronic gadgets and steal your personal data, including passwords and other sensitive data. Cyber security experts have coined the term 'juice jacking' for this type of crime, leading the Federal Communications Commission to issue several warnings about the threat in recent years. The FBI and the FCC warn that any public USB charging station, including in hotel lobbies and airports, could be vulnerable to Juice Jacking, although both agencies aren't actually aware of any specific instances of this type of crime actually taking place in real life.

Read the full article here.

US AVOIDS 'DIGITAL SECURITY CRISIS' AFTER DEVELOPER UNCOVERS SABOTAGE IN SAFTWARE

Fox News | April 5, 2024

German software developer Andres Freund was running some detailed performance tests last month when he noticed odd behavior in a little known program. What he found when he investigated has sent shudders across the software world and drawn attention from tech executives and government officials. Freund, who works for Microsoft out of San Francisco, discovered that the latest version of the open source software program XZ Utils had been deliberately sabotaged by one of its developers, a move that could have carved out a secret door to millions of servers across the internet. Security experts say it's only because Freund spotted the change before the latest version of XZ had been widely deployed that the world was spared a digital security crisis.

Read the full article here.

FORMER FBI AGENT ON THE ALARMING EVOLUTION OF CYBERTHREATS

Adam Burroughs | Smart Business Dealmakers | March 27, 2024

Robert Anderson Jr. served more than 20 years in the FBI, overseeing criminal and cyber investigations worldwide, including the Edward Snowden investigation. After the FBI, he served as managing director for a global organization helping companies respond to and recover from thousands of data breaches, as well as evaluate M&A target companies for cybersecurity vulnerabilities. The now Chairman and CEO of Cyber Defense Labs sat down with Smart Business Chief Content Officer Dustin Klein at the Dallas Smart Business Dealmakers Conference to discuss a range of issues, from Anderson's transition to the boardroom to his insights for business leaders on the evolution of cybersecurity threats.

Read the full article here.

EXEC AT US BATTERY MANUFACTURER PICTURED AT CHINESE COMMUNITST PARTY MEETINGS

Philip Lenczycki | Daily Caller | April 5, 2024

A director of an American firm that's building battery manufacturing plants in the U.S. has been pictured attending multiple Chinese Communist Party (CCP) meetings, according to a Daily Caller News Foundation review of the website of the firm's China-based parent company. Gotion Inc., the California-based subsidiary of Chinese battery manufacturer Gotion High-Tech Co. (Gotion High-Tech), is planning to build massive electric vehicle battery plants in Michigan and Illinois, both of which stand to benefit from taxpayer funding. Gotion Inc. Vice President Chuck Thelen has repeatedly denied any CCP ties, but a DCNF investigation found the company's chief technology officer attended two CCP meetings in China.

Read the full article here.

WHY THE THREAT OF A 'NIGHTMARE' CHINESE SUPERCOMPUTER JUST GOT A STEP CLOSER

Matthew Field | The Telegraph | April 4, 2024

A cyber security official at the US State Department had noticed something unusual. An internal IT security system, nicknamed "Big Yellow Taxi", had flagged unusual activity on its corporate Microsoft account. The tech team quickly raised its concerns to Microsoft, hopeful that the alert was just a false positive. What rapidly emerged, however, was that a Chinese government hacking group – codenamed Storm-0558 – had compromised the emails of hundreds of US government officials. An official US government post-mortem included one frightening possibility: that China had developed a quantum supercomputer, capable of cracking all Western encryption and rendering cyber defences useless. Victims of the hack, discovered on 15 June last year, included Gina Raimondo, the US commerce secretary, the US Ambassador to China, and dozens of high ranking officials and politicians across America and the UK.

Read the full article here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute

USEFUL RESOURCES

GUIDELINES FOR FEDERAL RESEARCH AGENCIES REGARDING FOREIGN TALENT RECRUITMENT PROGRAMS

Office of Science and Technology Policy | February 14, 2024

These guidelines are issued in accordance with Section 10631(b) of the CHIPS and Science Act of 2022 ("the Act"),1 which provides that "the Director of the Office of Science and Technology Policy, in coordination with the interagency working group established under section 1746 of the National Defense Authorization Act for Fiscal Year 2020 (42 U.S.C. 6601 note; Public Law 116-92), shall publish and widely distribute a uniform set of guidelines for Federal research agencies regarding foreign talent recruitment programs".

View the full resource here.

POLICY REGARDING USE OF COMMON DISCLOSURE FORMS FOR THE "BIOGRAPHICAL SKETCH" AND THE "CURRENT AND PENDING (OTHER) SUPPORT" SECTIONS OF APPLICATIONS BY FEDERAL RESEARCH FUNDING AGENCIES

Office of Science and Technology Policy | February 14, 2024

This policy requires federal research funding agencies to use harmonized common disclosure forms for the Biographical Sketch and the Current and Pending (Other) Support portions of funding application packages for grants and cooperative agreements (i.e., the Common Forms), except as otherwise provided below. The National Science and Technology Council (NSTC) Research Security Subcommittee has worked to develop consistent disclosure requirements, as directed under section 4(b) of National Security Presidential Memorandum 33 (NSPM-33)1 , including with resolution of comments submitted through the Paperwork Reduction Act (PRA) notice published in the Federal Register.

View the full resource here.

PROTECT YOURSELF: COMMERCIAL SURVEILLANCE TOOLS

The National Counterintelligence and Security Center | January 2022

Companies and individuals have been selling commercial surveillance tools to governments and other entities that have used them for malicious purposes. Journalists, dissidents, and other persons around the world have been targeted and tracked using these tools, which allow malign actors to infect mobile and internet-connected devices with malware over both WiFi and cellular data connections.

View the full resource here.

WELCOME TO OUR FREE RESOURCES

Data Abyss | L J Eads

An insightful individual once shared with me the perspective that in this era of Great Power Competition, our duty for some is to enlighten and educate. This resonated deeply with me, as my training and education have afforded me a unique viewpoint not accessible to many. It has enabled me to perceive the world through a lens of interconnectedness. Embracing this role of educator, I have taken the initiative to develop a series of free, open-source Science and Technology Trackers. These tools are designed to illuminate the intricate ties between the global community and China, highlighting the potential risks involved.

View the full resource here.

THE TEXAS A&M UNIVERSITY SYSTEM

The Research and Innovation Security and Competitiveness Institute