ASCE
ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM
https://asce.tamus.edu

THE OPEN SOURCE MEDIA SUMMARY

April 12, 2023

FINDING COLLECTIVE ADVANTAGE IN SHARED KNOWLEDGE

Michael M. Crow and Lisa Margonelli | Issues in Science and Technology | March 28, 2023

The CHIPS and Science Act aims to secure American competitiveness and innovation by investing $280 billion in domestic semiconductor manufacturing, scientific innovation, and regional development. But if past government investments in science and technology are any guide, this will affect American life in unexpected and profound ways—well beyond manufacturing and scientific laboratories. On this episode, Michael Crow, president of Arizona State University, talks to host Lisa Margonelli about the CHIPS and Science Act in the context of previous American security investments. Investments in food security and agriculture in the 1860s and nuclear security in the 1940s and ’50s created shared knowledge that benefitted all Americans. Early agricultural programs, for example, turned farmers into innovators, resulting in an agricultural sector that can feed many people with very little labor. In similar ways, today’s quest for digital security could make the country more secure, while also changing how individuals live and work with information.

Read the full article here.

GLOBAL | ASSESSMENT OF CHINESE INDUSTRIAL ESPIONAGE RISKS

Dragonfly Intelligence | March 29, 2023

Since China’s reopening in early 2023 several of our clients have asked us about the tactics and targeting of Chinese industrial espionage. There is incomplete data on this issue. But open source reporting suggests that Chinese intelligence officers mostly direct these, though private foreign and Chinese citizens are often involved. The number of reported China-related espionage cases has significantly increased over the past two decades. And acquiring commercial technology makes up the majority (51%) of recently reported espionage cases. Chinese state agencies are likely to intensify their operations in the wider Asian region in the medium term. With more firms operating in sensitive sectors having reduced their presence in mainland China, Chinese threat actors will need to target companies abroad. Key technologies are likely to be more easily accessible in countries such as South Korea, Japan, Europe and Southeast Asia compared to the US due to them having comparatively fewer safeguards. Chinese state-owned or controlled entities are likely to use both illegitimate and legitimate means such as investments and acquisitions to achieve this. Industrial espionage is likely to focus on several key industries. The graphic below, sets out those in which China intends to quickly develop self-sufficiency, as stated in the country’s 14th Five Year Plan and the Made in China 2025 Plan.

Read the full article here.

ALARMED TECH LEADERS CALL FOR AI RESEARCH PAUSE

Laurie Clarke | Science | April 11, 2023

An open letter calling for a pause on the development of advanced artificial intelligence (AI) systems has divided researchers. Attracting signatures from the likes of Tesla CEO Elon Musk and Apple co-founder Steve Wozniak, the letter, released early last week, advocates for a 6-month moratorium to give AI companies and regulators time to formulate safeguards to protect society from potential risks of the technology. AI has galloped along since the launch last year of the image generator DALL-E 2, from the Microsoft-backed company OpenAI. The company has since released ChatGPT and GPT-4, two text-generating chatbots, to frenzied acclaim. The ability of these so-called "generative" models to mimic human outputs, combined with the speed of adoption—ChatGPT reportedly reached more than 100 million users by January and major tech companies are racing to build generative AI into their products—have caught many off guard. "I think many people's intuitions about the impact of technology aren't well calibrated to the pace and scale of [these] AI models," says letter signatory Michael Osborne, a machine learning researcher and co-founder of AI company Mind Foundry.

Read the full article here.

OLD TACTICS COULD SLOW CHINA'S ADVANCES IN TECHNOLOGY RACE

Philip Athey | National Journal | April 6, 2023

China has rapidly become one of the most advanced technological powers in the world. But the factors that have allowed China's tech sector to grow so rapidly, including the acquisition of foreign tech and top-down planning, have become a burden as the nation attempts to transition from imitator to innovator. Fewer than 20 years ago, the Chinese domestic tech sector was largely a national and international afterthought. But in 2006, the Chinese Communist Party released its Medium-to Long-Term Program for the Development of Science and Technology, kick-starting its tech revolution. As part of its race to tech dominance, China invested massively in advanced industries including semiconductor production, artificial-intelligence research, and printing technology. Beijing also expanded its policy on forced transfer of technology and intellectual property, essentially forcing foreign businesses to hand over their tech secrets to China. The plan worked, and China's tech industry rivals any nation's.

Read the full article here.

7 METRICS TO MEASURE THE EFFECTIVENESS OF YOUR CYBERSECURITY STRATEGY

Mark Lynd

Do you ask yourself is our cybersecurity strategy working? Is it cost-effective? Are we getting real value for what we are paying for? Is our leadership confident in our efforts? In today's chaotic world where the number and sophistication of threats are rising, it is very challenging. It seems every day the news cycle reports on yet another organization victim of a cyber-attack. So, it is important to have confidence and assurance that your cybersecurity strategy is performing. To ensure that your cybersecurity strategy and measures are effective and up to date, it's essential to monitor and track performance using specific tactical metrics. We will cover seven key metrics that should be measured to ascertain the effectiveness of your organization's cybersecurity strategy. Quantitative assessments and key performance indicators (KPIs) play a crucial role in understanding how well your cybersecurity program is performing. Let's dive deeper into these key metrics and explore how they can help you improve your cybersecurity performance.

Read the full article here.

AI CHIPS: WHAT THEY ARE AND WHY THEY MATTER

Saif M. Khan | Center for Security and Emerging Technology | April 2020

Artificial intelligence will play an important role in national and international security in the years to come. As a result, the U.S. government is considering how to control the diffusion of AI-related information and technologies. Because general-purpose AI software, datasets, and algorithms are not effective targets for controls, the attention naturally falls on the computer hardware necessary to implement modern AI systems. The success of modern AI techniques relies on computation on a scale unimaginable even a few years ago. Training a leading AI algorithm can require a month of computing time and cost $100 million. This enormous computational power is delivered by computer chips that not only pack the maximum number of transistors—basic computational devices that can be switched between on (1) and off (0) states—but also are tailor-made to efficiently perform specific calculations required by AI systems. Such leading-edge, specialized "AI chips" are essential for cost-effectively implementing AI at scale; trying to deliver the same AI application using older AI chips or general-purpose chips can cost tens to thousands of times more.

Read the full article here.

ZERO TRUST MATURITY MODEL

Cybersecurity & Infrastructure Security Agency

Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. The goal is to prevent unauthorized access to data and services and make access control enforcement as granular as possible. Zero trust presents a shift from a location-centric model to a more data-centric approach for fine-grained security controls between users, systems, data and assets that change over time; for these reasons. This provides the visibility needed to support the development, implementation, enforcement, and evolution of security policies. More fundamentally, zero trust may require a change in an organization's philosophy and culture around cybersecurity. CISA's Zero Trust Maturity Model is one of many roadmaps that agencies can reference as they transition towards a zero trust architecture.

Read the full article here.

NY QUIETLY BANNED TIKTOK ON GOVERNMENT DEVICES 3 YEARS AGO

Brendan J. Lyons | Times Union | April 11, 2023

More states are moving to ban TikTok on government equipment, but New York was one of the first to do so — quietly adopting an internal policy in June 2020 that prohibited its use on mobile devices as officials sought to strengthen security measures and guard against cyber threats and other data intrusions. "New York state has blocked the use of TikTok on ITS-issued mobile devices for more than two years," said Scott Reif, a spokesman for the state Office of Information Technology Services. "We seek to meet people where they are and remain vigilant in protecting critical state assets, and urge New Yorkers to use caution when using TikTok and all social media platforms to protect their privacy and security." Reif said there are a small number of exceptions to the policy in which public relations platforms for NY.gov, I Love NY and the Metropolitan Transportation Authority have used TikTok "to communicate with New Yorkers." Despite the policy directive, there also is a bill in the Legislature that would create a law prohibiting any state employee from downloading or using the TikTok application on government-issued devices, including mobile phones and laptops.

Read the full article here.

FBI WARNS AGAINST USING PUBLIC PHONE CHARGING STATIONS

Rohan Goswami | CNBC | April 10, 2023

The FBI recently warned consumers against using free public charging stations, saying crooks have managed to hijack public chargers that can infect devices with malware, or software that can give hackers access to your phone, tablet or computer. "Avoid using free charging stations in airports, hotels or shopping centers," a tweet from the FBI's Denver field office said. "Bad actors have figured out ways to use public USB ports to introduce malware and monitoring software onto devices. Carry your own charger and USB cord and use an electrical outlet instead." The FBI offers similar guidance on its website to avoid public chargers. The bulletin didn't point to any recent instances of consumer harm from juice jacking. The FBI's Denver field office said the message was meant as an advisory, and that there was no specific case that prompted it. The Federal Communications Commission has also warned about "juice jacking," as the malware loading scheme is known, since 2021.

Read the full article here.

SUPPLY CHAIN RISK MANAGEMENT

Office of the Director of National Intelligence | The National Counterintelligence and Security Center

The mission of NCSC's Supply Chain and Cyber Directorate (SCD) is to enhance the nation's supply chain and cyber security, leveraging multidisciplinary counterintelligence and security expertise to inform, guide, and coordinate integrated risk decisions and responses with strategic partners. The 6th Annual National Supply Chain Integrity Month focuses on Supply Chain Risk Management (SCRM) – The Recipe for Resilience. NCSC encourages our stakeholders and partners to apply SCRM methodologies to protect our most critical supply chains. SCRM allows government and industry to defend against the known threats to our supply chains while building resilience to future risks. The need to build resilience in supply chain security is urgent now more than ever. Organizations must include all aspects of SCRM into their recipe for resilience. Acquisition Security, Information Security, Counterintelligence, Insider Threat Risk Management, and Cybersecurity are all key ingredients to understanding your organization’s risk appetite.

Read the full article here.

THE TEXAS A&M
UNIVERSITY SYSTEM

The Academic Security and Counter Exploitation Program is coordinated by The Texas A&M University System Research Security Office as a service to the academic community.
https://rso.tamus.edu

Academic Security and Counter Exploitation Program | *The Open Source Media Summary* | April 12, 2023 | Page 4 of 5

ASCE
ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM

USEFUL RESOURCES

INSIDER THREAT TOOLKIT

Center for Development of Security Excellence | Defense Counterintelligence and Security Agency

Do you have a question about how to do something or need more information about a topic? This toolkit will quickly point you to the resources you need to help you perform your role in the Insider Threat field.

View the full resource here.

SAFEGUARDING THE PUBLIC – DON'T BE A PAWN OF REPRESSIVE FOREIGN GOVERNMENTS

National Counterintelligence and Security Center | U.S. Department of Justice Federal Bureau of Investigation | March 2023

Foreign intelligence entities (FIEs) and elements working on behalf of repressive regimes have sought to use U.S.-based persons to facilitate their efforts to threaten or harm perceived critics and opponents in the United States. Consider the following steps to help protect those in the United States exercising their rights and to keep yourself from being used as a pawn in repressive foreign plots.

View the full resource here.

THE TEXAS A&M
UNIVERSITY SYSTEM

The Academic Security and Counter Exploitation Program is coordinated by The Texas A&M University System Research Security Office as a service to the academic community.
https://rso.tamus.edu