Weekly Security Articles 02-March-2022

Contribution Managers:
Christopher Sundberg
Kirsten Koepsel
Ann Marie van den Hurk
Daniel DiMase

Please Take our On-Line Survey

We would like to keep the Weekly Security Articles of Interest of interest relevant and timely. Please take a few minutes to answer our brief survey.

Thank you!

Link to Survey: https://forms.gle/L95wrYfa5sh3cZRQ8

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

TLP Definition: https://www.cisa.gov/tlp

Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

If you have publicly available contribution that you would like to share that may be added to this weekly report in the future, please send them to daniel.dimase@aerocyonics.com *along with the URL for the document.*

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Events - Online

Energy Sector Cybersecurity Community of Interest Meeting

March 3, 2022

From the article: “Join the NCCoE and your peers and colleagues in the energy sector for our next Community of Interest (COI) meeting. We’ll be joined by Pete Tseronis, CEO of Dots and Bridges, who will moderate an informal discussion with the NCCoE and our project collaborators on the example solution demonstrated in our latest cybersecurity practice guide, NIST SP 1800-32, Securing Distributed Energy Resources, and other cybersecurity considerations for industrial control systems and grid modernization.”

Source: https://www.nccoe.nist.gov/get-involved/attend-events/energy-sector-cybersecurity-community-interest-meeting

ERO CIP-012 Small Group Advisory Session General Session Webinar

March 8, 2022

From the article: “The Electric Reliability Organization (ERO) Enterprise will host a General Session webinar to provide information for those preparing to implement CIP-012-1 for Communications between Control Centers.”

Source: https://www.npcc.org/news/detail/ero-cip-012-small-group-advisory-session--general-session-webinar-

Standards and Performance Metrics for On-Road Autonomous Vehicles

March 8,-9, 2022

From the article: “However, on-road autonomous vehicles can pose a risk in the event of unexpected system performance. NIST is a nonregulatory government agency under

Link back to Table of Contents

the Department of Commerce that is equipped to develop test methods, metrics, and standards to characterize the performance of these complex systems. Therefore, NIST is currently determining focus areas of interest to characterize the performance of autonomous vehicles to mitigate risk to manufacturers as well as consumers."

Source: https://www.nist.gov/news-events/events/2022/03/standards-and-performance-metrics-road-autonomous-vehicles

Building the NIST AI Risk Management Framework: Workshop #2

March 29-31, 2022

From the article: "The second in a series, this workshop is part of NIST's efforts to foster an open, transparent, and collaborative process as it creates a Framework to manage risks to individuals, organizations, and society associated with AI. Building on community input to date, NIST will release a first draft of the Framework in advance of the event where AI experts and stakeholders across sectors will further advance the guidance document."

Source: https://www.nist.gov/news-events/events/2022/03/building-nist-ai-risk-management-framework-workshop-2

MICROELECTRONICS Foundations and Futures an executive course

April 27-29, 2022

From the article: "Recent years have revealed more than a few vulnerabilities in US security and technology supply chains, not the least of which being our dependence on advanced microelectronics. From semiconductor shortages to malign microchip actors to overseas dependencies, we face a host of challenging obstacles for this vital industry. How have we gotten here? Where are we going? Why do we need reform now? Find the answers to all this and more in Potomac Institute for Policy Studies' flagship executive course—Microelectronics: Foundations and Futures."

Source: https://potomacinstitute.org/events/education

Link back to Table of Contents

Events - Conferences

PARTS AND MATERIAL MANAGEMENT CONFERENCE

March 7 - 10, 2022

From the website: “Is your program having problems with DMSMS and obsolescence? Are the problems getting worse? Do you have questions about intellectual property rights, additive manufacturing, cyber security, and counterfeit prevention? Do you want to meet DMSMS and parts management experts who can help improve your situation?

Last year has been a time of important and positive changes for the DoD DMSMS and parts management communities. In the closing months of 2020, DoDI 4245.15, DoD DMSMS Management was published. This is the first DoD DMSMS instruction in more than 40 years! In addition, DoDI 5000.88, Engineering of Defense Systems which includes a requirement to implement parts management processes was also published.

The 2021 Parts and Materials Management Conference provides you with new information to successfully meet these new requirements, shows what is happening in the DMSMS community, and addresses your questions. You will have opportunities to interact and exchange ideas with specialists from government, industry, and academia, express your views and ideas on improving DMSMS and parts management, and meet with technical experts. You will experience state of the art technologies that can be applied to parts and material management at the training sessions and the exhibit hall.

Source: http://www.pmmcmeeting.org/

COLLABORATION ON QUALITY IN THE SPACE AND DEFENSE INDUSTRIES FORUM

March 15-17, 2022

From the article: “29th Annual Collaboration on Quality in the Space and Defense Industries Forum (CQSDI)

2022 CQSDI Program Highlights
Panels:

- Getting the upper hand on your supply chain through analytics
- Adapting to the new norm of maintaining a healthy supply chain
- Software IV&V tools and implementation strategies
- Young/New Quality Professionals and Effective Mentoring
- Assuring the Mission: Balancing Requirement Reduction and Risk
- Managing Risk and Compliance in Cyberspace – standardizing and

Link back to Table of Contents

implementing new controls in Aerospace and Defense

Source: https://asq.org/conferences/quality-space-defense

11th Automotive Cybersecurity Summit 2022 Detroit

March 29-31, 2022

From the webpage: “The automotive cybersecurity industry has seen great change in recent months. Today, the industry faces a sea of regulatory changes and mandates including the Software Bill of Materials, UN ECE 155 & 156 Regulations and the latest ISO/SAE21434 standard. The new rules and regulations have required companies to host cybersecurity management systems in-house, adding additional staffing, cost and time requirements to production. So, how can the industry tackle these new challenges?”

Source: https://www.automotive-iq.com/events-automotive-cybersecurity

IEEE International Symposium on Hardware Oriented Security and Trust (HOST)

June 27 - 30, 2022

From the website: “Rapid proliferation of computing and communication systems with increasing computational power and connectivity into every sphere of modern life has brought security to the forefront of system design, test, and validation processes. The emergence of new application spaces for these systems in the internet-of-things (IoT) regime is creating new attack surfaces as well as new requirements for secure and trusted system operation. Additionally, the design, manufacturing and the distribution of microchip, PCB, as well as other electronic components are becoming more sophisticated and globally distributed with a number of potential security vulnerabilities. Therefore, hardware plays an increasingly important and integral role in system security with many emerging system and application vulnerabilities and defense mechanisms relating to hardware. IEEE International Symposium on Hardware Oriented Security and Trust (HOST) aims to facilitate the rapid growth of hardware-based security research and development. HOST highlights new results in the area of hardware and system security. Relevant research topics include techniques, tools, design/test methods, architectures, circuits, and applications of secure hardware.”

Link back to Table of Contents

Call for Papers: HOST 2022 invites original contributions in all areas of overlap between hardware and security.

Source: http://www.hostsymposium.org/index.php

Symposium on Counterfeit Parts and Materials

June 28-30, 2022

Abstracts due March 11, 2022

From the article: “This symposium will provide a forum to cover all aspects of changes in the electronic parts supply chain on how an organization performs part selection and management through the whole life cycle of the parts. Going beyond anecdotes and examples of counterfeit parts, this symposium focuses on the solutions that are available and are under development by all sectors of the industry.”

Source: https://smta.org/mpage/counterfeit

Request for Comments

Cybersecurity Considerations for Open Banking Technology and Emerging Standards

Comments due: March 3, 2022

From the article: “This report contains a definition and description of open banking, its activities, enablers, and cybersecurity, and privacy challenges. This report is not intended to be a promotion of OB within the U.S but rather a factual description of the technology and how various countries have implemented it. Any proposal of a specific API that would be compatible across heterogeneous systems was purposely avoided in this report.”

Source: https://csrc.nist.gov/publications/detail/nistir/8389/draft

Federal Management Regulation (FMR); Internet GOV Domain

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Effective date: January 10, 2022

Comments: due in 60 days

From the article: “This interim rule implements provisions of the DOTGOV Act of 2020 that transfer ownership, management and operation of the DotGov Domain Program from the General Services Administration (GSA) to the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).”

Source: https://www.federalregister.gov/documents/2022/01/10/2021-28421/federal-management-regulation-fmr-internet-gov-domain

Additional Source: https://www.nextgov.com/cybersecurity/2022/01/gsa-seeks-comments-transfer-gov-domain-cybersecurity-agency/360517/

NISTIR 8286C (Draft) - Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight

Comments due: March 11, 2022

From the article: “Draft NISTIR 8286C describes methods for combining risk information from across the enterprise, including notional examples for aggregating and normalizing the results from cybersecurity risk registers (CSRRs) while considering risk parameters, criteria, and business impacts.”

Source: https://csrc.nist.gov/publications/detail/nistir/8286c/draft

NIST Requests Public Comments on SP 800-106, Randomized Hashing for Digital Signatures

Comments due: March 16, 2022

From the article: “NIST is in the process of a periodic review and maintenance of its cryptography standards and guidelines. Currently, we are reviewing the following publication:
NIST Special Publication (SP) 800-106, Randomized Hashing for Digital Signatures, 2009. ”

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://csrc.nist.gov/news/2022/public-comments-requested-on-sp-800-106

FERC Seeks to Tighten Cyber Security for Electric Grid Cyber Systems

Comments due 60 days from January 20, 2022

From the article: "On January 20, FERC issued a Notice of Proposed Rulemaking (NOPR) that proposes to strengthen its Critical Infrastructure Protection Reliability Standards by requiring internal network security monitoring for high and medium impact bulk electric system cyber systems."

Link to notice: https://ferc.gov/media/rm22-3-000

Additional sources:
https://www.jdsupra.com/legalnews/ferc-seeks-to-tighten-cyber-security-1758315

https://www.spglobal.com/platts/en/market-insights/latest-news/electric-power/012022-ferc-takes-initial-step-to-address-internal-network-threats-through-cyber-standards

https://www.natlawreview.com/article/ferc-seeks-to-tighten-cyber-security-electric-grid-cyber-systems

Chemical Facility Security News summary: https://chemical-facility-security-news.blogspot.com/2022/01/review-nerc-cip-and-internal-network.html

2022 Silent Data Corruptions at Scale request for proposals

Proposals due: March 21, 2022

From the article: "We are soliciting proposals focusing on mitigation of silent data corruptions within internet applications due to hardware faults affecting the data center computing stack (from hardware to compilers to applications). Proposals could range from hardware and architectural level mitigations and design strategies to test architecture evolution to software resiliency for silent data corruption. "

Source: https://research.facebook.com/research-awards/2022-silent-data-corruptions-at-scale-request-for-proposals/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

SP 800-219 (Draft) Automated Secure Configuration Guidance from the macOS Security Compliance Project (mSCP)

Comments due: March 23, 2022

From the article: “This publication provides resources that system administrators, security professionals, security policy authors, information security officers, and auditors can leverage to secure and assess macOS desktop and laptop system security in an automated way. It introduces the mSCP, describes use cases for leveraging the mSCP content, and gives an overview of the resources available on the project’s GitHub site.”

Source: https://csrc.nist.gov/publications/detail/sp/800-219/draft

SP 800-140C Rev. 1 (Draft) - CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759 (2nd Draft)

Comments due: March 25, 2022

Source: https://csrc.nist.gov/publications/detail/sp/800-140c/rev-1/draft

SP 800-140D Rev. 1 (Draft) - CMVP Approved Sensitive Parameter Generation and Establishment Methods: CMVP Validation Authority Updates to ISO/IEC 24759 (2nd Draft)

Comments due: March 25, 2022

Source: https://csrc.nist.gov/publications/detail/sp/800-140d/rev-1/draft

Incentives, Infrastructure, and Research and Development Needs To Support a Strong Domestic Semiconductor Industry

Comments due: March 25, 2022

From the notice: “The Department of Commerce (Department), with the assistance of

the National Institute of Standards and Technology (NIST), is seeking information in order to inform the planning and design of potential programs to: Incentivize investment in semiconductor manufacturing facilities and associated ecosystems; provide for shared infrastructure to accelerate semiconductor research, development, and prototyping; and support research related to advanced packaging and advanced metrology to ensure a robust domestic semiconductor industry."

Source: https://www.federalregister.gov/documents/2022/01/24/2022-01305/incentives-infrastructure-and-research-and-development-needs-to-support-a-strong-domestic

Related article: https://www.commerce.gov/news/press-releases/2022/01/commerce-department-requests-information-supporting-strong-us

DOE Launches $140 Million Program to Develop America's First-of-a-Kind Critical Minerals Refinery

RFI due: March 31, 2022

From the article: "The U.S. Department of Energy (DOE) today released a Request for Information (RFI)(link is external) on the design, construction and operation of a new facility to demonstrate the commercial feasibility of a full-scale rare earth element (REE) and critical minerals (CM) extraction and separation refinery using unconventional resources. When built, this first-of-a-kind facility, supported by $140 million investment from the Bipartisan Infrastructure Law, will support American manufacturing jobs, and help build a strong domestic supply chain for the next generation of clean energy technologies vital to reaching President Biden's goal of a net-zero emissions future. "

Link to RFI:
https://www.fedconnect.net/FedConnect/default.aspx?ReturnUrl=%2ffedconnect%2f%3fdoc%3dDE-FOA-0002686%26agency%3dDOE&doc=DE-FOA-0002686&agency=DOE

Source: https://www.energy.gov/articles/doe-launches-140-million-program-develop-americas-first-kind-critical-minerals-refinery

Request for Information: Partnerships for Coupling Innovation and Manufacturing Through Critical On-shore Prototyping

Comments due: April 5, 2022

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the article: “The Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) is seeking information from the domestic microelectronics (ME) community to help inform DoD’s objectives, assumptions, and initiatives pursuant to the Fiscal Year (FY) 2021 National Defense Authorization Act (NDAA) (Pub. L. 116-283), including the CHIPS (Creating Helpful Incentives to Produce Semiconductors) for America Act, and pending legislation on potential funding of these efforts through the United States Innovation and Competition Act (USICA) and passage of the America Creating Opportunities for Manufacturing, Pre-Eminence in Technology, and Economic Strength (America COMPETES) Act of 2022. ”

Source: https://sam.gov/opp/656b39ff64ec4d4fa47ff9820d1c554b/view

Additional sources:
https://www.defensenews.com/battlefield-tech/2022/02/25/pentagon-wants-to-bolster-domestic-microelectronics-base-with-new-innovation-network/

https://breakingdefense.com/2022/02/for-microelectronics-dod-wants-lab-to-fab-prototyping-hubs/

NISTIR 8270 (Draft) Introduction to Cybersecurity for Commercial Satellite Operations (2nd Draft)

Comments due: April 8, 2022

From the article: “Space operations are vital to advancing the security, economic prosperity, and scientific knowledge of the Nation. However, cyber-related threats to space assets and their supporting infrastructure pose increasing risks to the economic promise of emerging markets in space. This second draft of NISTIR 8270, Introduction to Cybersecurity for Commercial Satellite Operations, presents a specific method for applying the Cybersecurity Framework (CSF) to commercial space business and describes an abstracted set of cybersecurity outcomes, requirements, and suggested controls.”

Source: https://csrc.nist.gov/publications/detail/nistir/8270/draft

Responding to and Recovering from a Cyber Attack: Cybersecurity for the Manufacturing Sector

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Comments due: April 14, 2022

From the article: “Constant threats of destructive malware, malicious insider activity, and even honest mistakes create the need for manufacturers to be able to respond to and quickly recover from a cyber event that impacts industrial control systems and plant operations.”

Source: https://www.nccoe.nist.gov/manufacturing/responding-and-recovering-cyber-attack

Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Comments due: April 25, 2022

From the article: “The National Institute of Standards and Technology (NIST) is seeking information to assist in evaluating and improving its cybersecurity resources, including the “Framework for Improving Critical Infrastructure Cybersecurity” (the “NIST Cybersecurity Framework,” “CSF” or “Framework”) and a variety of existing and potential standards, guidelines, and other information, including those relating to improving cybersecurity in supply chains. ”

Source: https://www.federalregister.gov/documents/2022/02/22/2022-03642/evaluating-and-improving-nist-cybersecurity-resources-the-cybersecurity-framework-and-cybersecurity

Additional sources:
https://www.nist.gov/news-events/news/2022/02/nist-seeks-input-update-cybersecurity-framework-supply-chain-guidance

https://chemical-facility-security-news.blogspot.com/2022/02/review-nist-rfi-to-support-csf-supply.html

https://www.csoonline.com/article/3651368/nist-seeks-information-on-updating-its-cybersecurity-framework.html

Reports - Government

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

In studying tech supply chain, feds cite open source products, device firmware

From the article: "Open-source software and device firmware are two of the biggest areas of vulnerability in the supply chains for information and communications technology, according to a federal report Thursday that called for better risk management practices and improved monitoring efforts by government and industry."

Link to DOC report: https://www.commerce.gov/sites/default/files/2022-02/Assessment-Critical-Supply-Chains-Supporting-US-ICT-Industry.pdf

Source: https://www.cyberscoop.com/supply-chain-risk-homeland-security-commerce-report/

New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021

From the article: “Newly released Federal Trade Commission data shows that consumers reported losing more than $5.8 billion to fraud in 2021, an increase of more than 70 percent over the previous year.

The FTC received fraud reports from more than 2.8 million consumers last year, with the most commonly reported category once again being imposter scams, followed by online shopping scams.”

Source: https://www.ftc.gov/news-events/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers

Additional sources:
https://www.bleepingcomputer.com/news/security/ftc-americans-report-losing-over-58-billion-to-fraud-in-2021/

CHALLENGES FACING DOD IN STRATEGIC COMPETITION WITH CHINA

From the article: “According to the 2021 Interim National Security Strategic Guidance, China is increasingly assertive and the only competitor potentially capable of combining its economic, diplomatic, military, and technological power to mount a sustained challenge to a stable and open international system.”

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.gao.gov/assets/gao-22-105448.pdf

The Biden-Harris Plan to Revitalize American Manufacturing and Secure Critical Supply Chains in 2022

From the article: “One year ago, President Biden signed Executive Order 14017 directing an all-of-government approach to assessing vulnerabilities in – and strengthening the resilience of – the United States’ critical supply chains. Within six months of taking office, the Administration completed a comprehensive review of the supply chains for four critical products, identified solutions to secure those supply chains against a wide range of risks and vulnerabilities, and established a first-of-its-kind Supply Chain Disruptions Task Force (SCDTF) to address the challenges arising from a pandemic-affected economic recovery.”

Includes links to seven industrial base reports

Source: https://www.whitehouse.gov/briefing-room/statements-releases/2022/02/24/the-biden-harris-plan-to-revitalize-american-manufacturing-and-secure-critical-supply-chains-in-2022/

DOE Releases First-Ever Comprehensive Strategy to Secure America’s Clean Energy Supply Chain

From the article: “The U.S. Department of Energy (DOE) today released America’s first comprehensive plan to ensure security and increase our energy independence. The sweeping report, “America’s Strategy to Secure the Supply Chain for a Robust Clean Energy Transition,” lays out dozens of critical strategies to build a secure, resilient, and diverse domestic energy sector industrial base that will establish America’s role as a global leader in clean energy manufacturing and innovation.”

Report: https://www.energy.gov/policy/articles/americas-strategy-secure-supply-chain-robust-clean-energy-transition

Source: https://www.energy.gov/articles/doe-releases-first-ever-comprehensive-strategy-secure-americas-clean-energy-supply-chain

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

NISTIR 8374 Ransomware Risk Management: A Cybersecurity Framework Profile

From the article: “Ransomware is a type of malicious attack where attackers encrypt an organization’s data and demand payment to restore access. Attackers may also steal an organization’s information and demand an additional payment in return for not disclosing the information to authorities, competitors, or the public. This Ransomware Profile identifies the Cybersecurity Framework Version 1.1 security objectives that support identifying, protecting against, detecting, responding to, and recovering from ransomware events. The profile can be used as a guide to managing the risk of ransomware events. That includes helping to gauge an organization’s level of readiness to counter ransomware threats and to deal with the potential consequences of events.”

Source: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8374.pdf

Zero trust will be ‘incomplete experiment’ without prompt follow-up, report says

From the article: “The Biden administration has done well in building momentum behind its zero trust initiatives, but a focus on short-term goals — to the exclusion of long-term planning — runs the risk of undershooting a sustained impact. That’s the warning contained in a new report from the National Security Telecommunications Advisory Council on the state of zero trust adoption in the federal government.”

Link to report:
https://www.cisa.gov/sites/default/files/publications/Final%20Draft%20NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management.pdf

Source: https://federalnewsnetwork.com/cybersecurity/2022/02/zero-trust-will-be-incomplete-experiment-without-prompt-follow-up-report-says/

Technology Vision for an Era of Competition

From the article: “The Office of the Under Secretary ofDefense for Research and Engineering (OUSD(R&E) will spearhead a National Defense Science and Technology strategy for the Department of Defense (DoD), informed by the 2022 National Defense Strategy (NDS) and structured around three strategic pillars: mission focus, foundation building, and succeeding through teamwork.”

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.cto.mil/wp-content/uploads/2022/02/usdre_strategic_vision_critical_tech_areas.pdf

Technologies for American Innovation and National Security

From the article: “Today, the United States is releasing an updated list of critical and emerging technologies (CETs) that can play an important role in our nation’s security. Last updated in 2020, this list represents a subset of novel, advanced technologies with the potential to chart new pathways in American innovation and strengthen our national security.”

Link to updated list: https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf

Source: https://www.whitehouse.gov/ostp/news-updates/2022/02/07/technologies-for-american-innovation-and-national-security/

HHS Report Warns of EMR and EHR Security Risks

From the article: “The U.S. Department of Health and Human Services’ Health Sector Cybersecurity Coordination Center (HC3) recently issued a report entitled “Electronic Medical Records in Healthcare” that discussed security risks applicable to electronic medical records (EMRs) and electronic health records (EHRs). EHRs and EMRs are prime targets for cyber attackers because protected health information (PHI) can be sold on the dark web or black market.”

Link to report: https://www.hhs.gov/sites/default/files/2022-02-17-1300-emr-in-healthcare-tlpwhite.pdf

Source: https://www.jdsupra.com/legalnews/hhs-report-warns-of-emr-and-ehr-8782159/

New Sandworm Malware Cyclops Blink Replaces VPNFilter

Summary: UK's NCSC, CISA, and NSA have released a new joint advisory on Sandworm/voodoo bear using a new malware known as Cyclops Blink.

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Link to report: https://www.cisa.gov/uscert/sites/default/files/publications/AA22-054A%20New%20Sandworm%20Malware%20Cyclops%20Blink%20Replaces%20VPN%20Filter.pdf

Source: https://us-cert.cisa.gov/ncas/current-activity/2022/02/23/new-sandworm-malware-cyclops-blink-replaces-vpnfilter

FREE CYBERSECURITY SERVICES AND TOOLS

From the article: “As part of our continuing mission to reduce cybersecurity risk across U.S. critical infrastructure partners and state, local, tribal, and territorial governments, CISA has compiled a list of free cybersecurity tools and services to help organizations further advance their security capabilities. This living repository includes cybersecurity services provided by CISA, widely used open source tools, and free tools and services offered by private and public sector organizations across the cybersecurity community. CISA will implement a process for organizations to submit additional free tools and services for inclusion on this list in the future.”

Source: https://www.cisa.gov/free-cybersecurity-services-and-tools

Additional sources: https://www.zdnet.com/article/cisa-publishes-guide-with-free-cybersecurity-tools-resources-for-incident-response/

https://www.bleepingcomputer.com/news/security/cisa-compiles-list-of-free-cybersecurity-tools-and-services/

https://securityaffairs.co/wordpress/128182/hacking/cisa-list-free-cybersecurity-tools.html

Defense R&D contractors inadequate in protecting sensitive data, IG says

From the article: “Contractors that research and develop new technologies for the Department of Defense are not consistent in safeguarding the DOD’s controlled unclassified information, according to a new audit by the Pentagon’s inspector general.”

Link to the IG report: https://media.defense.gov/2022/Feb/24/2002944191/-1/-1/1/DODIG-2022-061.PDF

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.fedscoop.com/defense-rd-contractors-inadequate-in-protecting-sensitive-data-ig-says/

European Cybersecurity Agencies Issue Resilience Guidance for Decision Makers

From the article: "The European Union Agency for Cybersecurity (ENISA) and the European Union's Computer Emergency Response Team (CERT-EU) last week published a set of best practices to help organizations boost their cyber resilience."

Link to guidance: https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience

Source: https://www.securityweek.com/european-cybersecurity-agencies-issue-resilience-guidance-decision-makers

Reports - Industry

Dragos reports rise in vulnerabilities and ransomware, as ICS/OT systems digitally transform

Summary: Industrial Cyber summarizes the Dragos ICS/OT Cybersecurity report for 2021.

Link to download report: https://www.dragos.com/year-in-review/#section-findings

Source: https://industrialcyber.co/threats-attacks/dragos-reports-rise-in-vulnerabilities-and-ransomware-as-ics-ot-systems-digitally-transform/

Manufacturing was the top industry targeted by ransomware last year

Summary: IBM X-Force releases report on Threat Intelligence Index 2021.

Link to report: https://www.ibm.com/downloads/cas/ADLMYLAZ

Source: https://www.tripwire.com/state-of-security/security-data-protection/manufacturing-was-the-top-industry-targeted-by-ransomware-last-year/

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Podcasts/Videos

CHIPS Act and Onward: Next Steps to Reshore Semiconductor Manufacturing

From the article: Congress is moving toward approving funding for the 2020 CHIPS Act to reshore semiconductor chip production to the United Stated to address current shortages and long-term supply challenges. Once the funds are appropriated, the Executive Branch will have to implement the CHIPS Act expeditiously to rebuild leading edge manufacturing capacity in the U.S, and work with Congress to develop a long-term strategy to restore America's semiconductor leadership and secure supply chains for the U.S. and its friends and allies.“”

Source: https://secureenergy.org/chips-act-and-onward-next-steps-to-reshore-semiconductor-manufacturing/

Could cyberattacks draw U.S. into Ukraine war?

From the article: “If Russian hackers target the U.S. because of the Ukraine conflict, says America's first cybersecurity czar, Richard Clarke,' If it's a big enough attack...we could very easily find ourselves in a shooting war with Russia.'”

Source: https://www.cnn.com/videos/tech/2022/02/26/could-cyberattacks-draw-u-s-into-ukraine-war.cnn

Incident Command System for ICS Improves Response to CyberSec Incidents – Brian Peterson – ESW #262

From the article: “This discussion will provide a brief overview of the Incident Command System for Industrial Control Systems processes and describe how ICS4ICS will help companies better manage industrial cyber incidents. We will discuss how ICS4ICS will enable companies to work with government agencies and mutual aid partners when a cyber incident impacts an entire industrial sector or multiple sectors.”

Source: https://securityweekly.com/shows/incident-command-system-for-ics-improves-

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

response-to-cybersec-incidents-brian-peterson-esw-262/

Ukraine conflict ignites fears over cyberwarfare

From the article: “As Putin bulks up Russian troops at the Ukrainian border, national security experts warn that the Russians may target key digital infrastructure.”

Source: https://abcnews.go.com/Nightline/video/ukraine-conflict-ignites-fears-cyberwarfare-83079851

DHS warns of urgent cyberattack threat as Russia tensions escalate

From the article: “The Department of Homeland Security warns “every organization in the United States is at risk from cyber threats” with Russia potentially considering “escalating its destabilizing actions.” The agency is urging businesses, agencies and more to shore up defenses, especially to protect critical infrastructure.”

Source: https://www.nbcnews.com/nightly-news/video/dhs-warns-of-urgent-cyberattack-threat-as-russia-tensions-escalate-133792837903

Patches/Advisories

Review – 3 Advisories Published – 2-22-22

Source: https://chemical-facility-security-news.blogspot.com/2022/02/review-3-advisories-published-2-22-22.html

CISA Adds Two Known Exploited Vulnerabilities to Catalog

Source: https://us-cert.cisa.gov/ncas/current-activity/2022/02/22/cisa-adds-two-known-exploited-vulnerabilities-catalog

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

FATEK Automation FvDesigner

Source: https://us-cert.cisa.gov/ics/advisories/icsa-22-055-01

Mitsubishi Electric EcoWebServerIII

Source: https://us-cert.cisa.gov/ics/advisories/icsa-22-055-02

Schneider Electric Easergy P5 and P3

Source: https://us-cert.cisa.gov/ics/advisories/icsa-22-055-03

Baker Hughes Bently Nevada 3500

Source: https://us-cert.cisa.gov/ics/advisories/icsa-21-231-02

Iranian Government-Sponsored MuddyWater Actors Conducting Malicious Cyber Operations

Source: https://us-cert.cisa.gov/ncas/current-activity/2022/02/24/iranian-government-sponsored-muddywater-actors-conducting

New Sandworm Malware Cyclops Blink Replaces VPNFilter

Source: https://us-cert.cisa.gov/ncas/current-activity/2022/02/23/new-sandworm-malware-cyclops-blink-replaces-vpnfilter

Review - Public ICS Disclosures – Week of 2-19-22

Source: https://chemical-facility-security-news.blogspot.com/2022/02/review-public-ics-disclosures-week-of-2_26.html

Review – 4 Advisories Published – 2-24-22

Source: https://chemical-facility-security-news.blogspot.com/2022/02/review-4-advisories-published-2-24-22.html

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Broadcom Software Discloses APT Actors Deploying Daxin Malware in Global Espionage Campaign

Source: https://us-cert.cisa.gov/ncas/current-activity/2022/02/28/broadcom-software-discloses-apt-actors-deploying-daxin-malware

CISA Releases Advisory on Destructive Malware Targeting Organizations in Ukraine

Source: https://us-cert.cisa.gov/ncas/current-activity/2022/02/26/cisa-releases-advisory-destructive-malware-targeting-organizations

CISA Adds Four Known Exploited Vulnerabilities to Catalog

Source: https://us-cert.cisa.gov/ncas/current-activity/2022/02/25/cisa-adds-four-known-exploited-vulnerabilities-catalog

Mozilla Releases Security Update for Mozilla VPN

Source: https://us-cert.cisa.gov/ncas/current-activity/2022/02/25/mozilla-releases-security-update-mozilla-vpn

Cisco Releases Security Updates for Multiple Products

Source: https://us-cert.cisa.gov/ncas/current-activity/2022/02/24/cisco-releases-security-updates-multiple-products

CVE-2021-36260 | hikvision vulnerability

Summary: Rapid7 analyzes the hikvision camera security flaw and provides advice for securing the cameras.

Source: https://attackerkb.com/topics/mb8q72U2LT/cve-2021-36260

Ukraine

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

New data-wiping malware used in destructive attacks on Ukraine

From the article: "Cybersecurity firms have found a new data wiper used in destructive attacks today against Ukrainian networks just as Russia moves troops into regions of Ukraine."

Source: https://www.bleepingcomputer.com/news/security/new-data-wiping-malware-used-in-destructive-attacks-on-ukraine/

Additional sources:
https://www.darkreading.com/attacks-breaches/new-data-wiping-malware-discovered-on-systems-in-ukraine

https://www.cyberscoop.com/ukraine-wiper-malware-eset-sentinelone-whispergate/

https://www.theregister.com/2022/02/23/ukraine_wiper_malware/

https://securityaffairs.co/wordpress/128361/malware/ukraine-ransomware-decoy-wiper.html

https://www.securityweek.com/destructive-hermeticwiper-malware-targets-computers-ukraine

https://securityaffairs.co/wordpress/128349/malware/wiper-malware-hermeticwipe-ukrain.html

https://www.bleepingcomputer.com/news/security/ransomware-used-as-decoy-in-data-wiping-attacks-on-ukraine/

https://cyberintelmag.com/attacks-data-breaches/new-data-wiping-malware-employed-in-ukraines-devastating-cyberattacks/

https://securityintelligence.com/posts/new-destructive-malware-cyber-attacks-ukraine/

https://www.welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/

Ukraine Accuses Belarusian Hackers of Phishing Attacks Aimed at Military

From the article: "A spearphishing attempt targeting private email accounts belonging to

Ukrainian military forces personnel was announced today by the Computer Emergency Response Team of Ukraine (CERT-UA)."

Source: https://cyberintelmag.com/attacks-data-breaches/ukraine-accuses-belarusian-hackers-of-phishing-attacks-aimed-at-military/

Additional sources:
https://www.cyberscoop.com/ukrainian-cyber-officials-warn-of-new-wave-of-phishing-attacks/

https://securityaffairs.co/wordpress/128397/apt/belarusian-unc1151-targets-ukraine.html

https://www.bleepingcomputer.com/news/security/ukraine-links-phishing-targeting-military-to-belarusian-hackers/

https://www.bleepingcomputer.com/news/security/ukraine-links-phishing-targeting-armed-forces-to-belarusian-hackers/

https://www.darkreading.com/endpoint/ukrainian-troops-targeted-in-phishing-attacks-by-suspected-belarusian-apt

Ukraine calls on independent hackers to defend against Russia, Russian underground responds

From the article: "While Ukraine calls for hacker underground to defend against Russia, ransomware gangs make their moves."

Source: https://securityaffairs.co/wordpress/128410/cyber-crime/ukraine-russia-hacking-undergrounds.html

Additional sources:
https://www.theregister.com/2022/02/25/ukraine_cyber_russia/

https://www.zdnet.com/article/ukraine-calls-for-underground-hackers-to-protect-critical-infrastructure-report/

Conti ransomware group announces support of Russia, threatens to retaliate against any Western attacks

Link back to Table of Contents

From the article: "An infamous ransomware group with potential ties to Russian intelligence and known for attacking health care providers and hundreds of other targets posted a warning Friday saying it was “officially announcing a full support of Russian government.”

Source: https://www.cyberscoop.com/conti-ransomware-russia-ukraine-critical-infrastructure/

Additional sources:
https://www.bleepingcomputer.com/news/security/ransomware-gangs-hackers-pick-sides-over-russia-invading-ukraine/

https://www.csoonline.com/article/3651498/conti-gang-says-its-ready-to-hit-critical-infrastructure-in-support-of-russian-government.html

United States And United Kingdom Accuse Russia of Cyberattacks Against Ukraine

From the article: "As tensions between Russia and Ukraine rise, Britain has joined the United States in accusing the GRU military intelligence agency of distributed denial-of-service operations."

Source: https://cyberintelmag.com/attacks-data-breaches/united-states-and-united-kingdom-accuse-russia-of-cyberattacks-against-ukraine/

Additional sources:
https://securityaffairs.co/wordpress/128174/cyber-warfare-2/russia-gru-ddos-ukraine.html

White House Denies Considering Massive Cyberattacks Against Russia

From the article: "The White House has disputed claims that Vice President Joe Biden has given permission for launching significant cyberattacks against Russia to disrupt the country’s capacity to maintain its military operations in Ukraine."

Source: https://cyberintelmag.com/attacks-data-breaches/white-house-denies-considering-massive-cyberattacks-against-russia/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Additional sources:
https://threatpost.com/white-house-denies-mulling-massive-cyberattacks-against-russia/178658/

Ukraine hit by DDoS attacks, Russia deploys malware

From the article: "The EU has sent a cyber response team to Ukraine as rumours of a planned Russian invasion reach fever pitch. Meanwhile, IBM's infosec division says the UK was one of the most targeted countries in Europe for cyberattacks last year…."

Source: https://www.theregister.com/2022/02/23/ukraine_ddos_russia_malware/

Cybercriminals Seek to Profit From Russia-Ukraine Conflict

From the article: "Dark web threat actors are looking to take advantage of the tensions between Russia and Ukraine, offering network access and databases that could be relevant to those involved in the conflict, according to a new report from Accenture."

Source: https://www.securityweek.com/cybercriminals-seek-profit-russia-ukraine-conflict

EU to Activate Cyber Response Team to Help Ukraine

From the article: "The European Union is set to activate an EU cyber response team to help Ukraine face Russian attacks, the unit's leader Lithuania said on Tuesday."

Source: https://www.securityweek.com/eu-activate-cyber-response-team-help-ukraine

As Russia invades, Ukrainian government networks suffer high-profile DDoS disruption

From the article: "A series of Ukrainian government websites were inaccessible Wednesday after what a government official described as a “mass DDoS attack,” marking the second apparent distributed denial-of-service disruption to hit government sites there in the last eight days."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.cyberscoop.com/ukraine-government-networks-ddos-disruption-russia-invasion/

Russia, Ukraine and the Danger of a Global Cyberwar

From the article: "On the morning of February 22, 2022, the world woke to the news that Russia had moved troops into two separatist regions of eastern Ukraine. At the time of writing, it is not yet a full invasion of Ukraine, but Russia did conduct attacks on February 24, hitting cities with airstrikes and artillery in what was called a “special military operation” by Russian President Vladamir Putin."

Source: https://www.securityweek.com/russia-ukraine-and-danger-global-cyberwar

The war may show up on your doorstep in an email

From the article: "If you live outside of Ukraine, you may be asking how you will be impacted by the Russian invasion and how you can prepare."

Source: https://www.amperesec.com/news/the-war-may-show-up-in-an-email

Russia Sanctions May Spark Escalating Cyber Conflict

From the article: "The West has promised tougher sanctions are coming, but experts warn these will almost certainly trigger a Russian retaliation against America and its allies, which could escalate into cyber attacks on Western financial institutions and energy infrastructure."

Source: https://krebsonsecurity.com/2022/02/russia-sanctions-may-spark-escalating-cyber-conflict/

Ukrainian government and banks once again hit by DDoS attacks

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the article: "The sites of several Ukrainian government agencies (including the Ministries of Foreign Affairs, Defense, and Internal Affairs, the Security Service, and the Cabinet of Ministers), and of the two largest state-owned banks are again targeted by Distributed Denial-of-Service (DDoS) attacks."

Source: https://www.bleepingcomputer.com/news/security/ukrainian-government-and-banks-once-again-hit-by-ddos-attacks/

Putin's government warns Russian critical infrastructure of potential cyberattacks

From the article: "The Russian government warned its domestic critical infrastructure operators Thursday of the “threat of an increase in the intensity of computer attacks,” and said that any failure in the operation of critical infrastructure that doesn’t have a “reliably established” cause should be considered “the result of a computer attack.”

Source: https://www.cyberscoop.com/russia-cyberdefense-critical-infrastructure-warning/

7 Steps to Take Right Now to Prepare for Cyberattacks by Russia

From the article: "A lot of the recommended preparation involves measures organizations should have in place already."

Source: https://www.darkreading.com/threat-intelligence/7-steps-to-take-right-now-to-prepare-for-cyberattacks-by-russia

Anonymous launched its offensive on Russia in response to the invasion of Ukraine

From the article: "The popular collective Anonymous declared war on Russia for the illegitimate invasion of Ukraine and announced a series of cyber attacks calling to action its members."

Source: https://securityaffairs.co/wordpress/128392/hacktivism/anonymous-cyber-attacks-russia.html

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Cyber Attack Risks Poised to Soar as Russia Attacks Ukraine

From the article: "Russia's military assault against Ukraine is likely to be accompanied by a wave of cyberattacks that could wreak havoc on computer systems far beyond the countries' borders, security experts warn."

Source: https://www.securityweek.com/cyber-attack-risks-poised-soar-russia-attacks-ukraine

Fears Rise of Potential Russian Cyberattacks on US, Allies Over Sanctions

From the article: "If past is precedent, the cyber impact of the war in Ukraine could be broad and bruising, experts say."

Source: https://www.darkreading.com/attacks-breaches/fears-rise-of-potential-russian-cyberattacks-on-us-allies-over-sanctions

Tech's role in the Ukraine war

From the article: "Ukraine is estimated to have about 200,000 tech workers, many of whom work for companies overseas."

Source: https://www.protocol.com/newsletters/sourcecode/ukraine-war-tech

Spear Phishing Attacks Target Ukraine Organizations, Payloads Include the Document Stealer OutSteel and the Downloader SaintBot

From the article: "An attack in early February targeted an energy organization in Ukraine with OutSteel and SaintBot. The attack is part of a larger campaign."

Source: https://unit42.paloaltonetworks.com/ukraine-targeted-outsteel-saintbot/

More Cyber Attacks Disable Ukrainian Websites

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the article: “Various financial and government websites in Ukraine were temporarily disabled on Wednesday by heavy denial-of-service attacks that resembled ones last week attributed to Russia by U.S. officials.”

Source: https://www.nextgov.com/cybersecurity/2022/02/more-cyber-attacks-disable-ukrainian-websites/362339/

Biden: ‘Prepared to Respond’ if Russia Pursues Cyberattacks Against US

From the article: “President Joe Biden warned Thursday that the federal government would respond to Russian aggression in cyberspace.”

Source: https://www.nextgov.com/cybersecurity/2022/02/biden-prepared-respond-if-russia-pursues-cyberattacks-against-us/362401/

Biden Puts DHS in Charge of Russia-Ukraine Threats to the Homeland

From the article: “The Department of Homeland Security has pulled together officials from across all levels of government and the private sector to manage any stateside fallout from Russia’s invasion of Ukraine. ”

Source: https://www.nextgov.com/cybersecurity/2022/02/biden-puts-dhs-charge-russia-ukraine-threats-homeland/362474/

Russia Could “Absolutely” Lash Out at US Through Cyber, Lawmaker Warns

From the article: “Russia is expected to increase its cyber attacks as it continues a military assault on Ukraine, and one lawmaker warns that the U.S. should be prepared for future high level digital attacks.”

Source: https://www.nextgov.com/cybersecurity/2022/02/russia-could-absolutely-lash-out-us-through-cyber-lawmaker-warns/362557/

Link back to Table of Contents

Will Biden's 'Severe Costs' on Russia Include Cyber Attacks?

From the article: "What if the "severe costs"—the damage the United States and its allies cause to the Russian military and government should they invade Ukraine—comes not with just sanctions, but through the use of cyber operations? Will we ever know?"

Source: https://www.nextgov.com/ideas/2022/02/will-bidens-severe-costs-russia-include-cyber-attacks/362231/

Russia Sanctions May Spark Escalating Cyber Conflict

From the article: "President Biden joined European leaders this week in enacting economic sanctions against Russia in response to its invasion of Ukraine. The West has promised tougher sanctions are coming, but experts warn these will almost certainly trigger a Russian retaliation against America and its allies, which could escalate into cyber attacks on Western financial institutions and energy infrastructure."

Source: https://krebsonsecurity.com/2022/02/russia-sanctions-may-spark-escalating-cyber-conflict/

More Cyber Attacks Disable Ukrainian Websites

From the article: "Various financial and government websites in Ukraine were temporarily disabled on Wednesday by heavy denial-of-service attacks that resembled ones last week attributed to Russia by U.S. officials."

Source: https://www.nextgov.com/cybersecurity/2022/02/more-cyber-attacks-disable-ukrainian-websites/362339/

Russian Invasion of Ukraine and Resulting US Sanctions Threaten the Future of the International Space Station

From the article: "New U.S. sanctions on Russia will encompass Russia's space agency, Roscosmos, according to a speech U.S. President Joe Biden gave on Feb. 24,

Link back to Table of Contents

2022.
In response to these sanctions, the head of Roscosmos on the same day posted a tweet saying, among other things, “If you block cooperation with us, who will save the ISS from an uncontrolled deorbit and fall into the United States or Europe?””

Source: https://www.nextgov.com/emerging-tech/2022/02/russian-invasion-ukraine-and-resulting-us-sanctions-threaten-future-international-space-station/362508/

Cyber Siren Warning - When State Actors Attack

From the article: “Russia began a physical invasion of Ukraine Wednesday night, and as the United States responded with sanctions, the threat of cyberattacks against American companies became more acute. Major American businesses – from banks to critical infrastructure companies – are preparing for possible cyberattacks after Russia threatened “consequences” for nations interfering with its invasion of Ukraine.”

Source: https://www.jdsupra.com/legalnews/cyber-siren-warning-when-state-actors-2587529/

Security Measures to Deploy Now to Defend Against a Russian Cyberattack

From the article: “On February 22, 2022, U.S. Department of Homeland Security Secretary Alejandro Mayorkas warned critical infrastructure organizations located in the United States of possible cyberattacks by Russian state-sponsored actors in retaliation for sanctions imposed by the United States in response to Russia’s invasion of Ukraine.”

Source: https://www.jdsupra.com/legalnews/security-measures-to-deploy-now-to-8629044/

The radiation will never be higher in Chernobyl? oops!

Summary: Potential overrun issue with digital meters at Chernobyl. A reason why the reporting numbers spiked (and stayed) at 65500 nonsieverts/hr.

Source: https://catless.ncl.ac.uk/Risks/33/07/#subj1.1

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The war may show up on your doorstep in an email

From the article: "You may not be able to tell the difference between an attack email related to Russian cyber war and the typical phishing email that shows up in your inbox. "If it's going to come in, it's going to look surprisingly familiar," Lee said. Be on the lookout for email and links that ask for your password, as well as random updates to software, he recommended. And remember that these fake emails can look very legitimate."

Source: https://www.amperesec.com/news/the-war-may-show-up-in-an-email

Destructive 'HermeticWiper' Malware Targets Computers in Ukraine

From the article: "The wiper abuses legitimate drivers associated with an application called EaseUS Partition Master. It attempts to corrupt the master boot record (MBR) of every physical drive, as well as every partition on these drives. This is the second destructive malware attack aimed at Ukraine in 2022. In January, threat actors defaced Ukrainian government websites and unleashed wiper malware named WhisperGate, which had been disguised as ransomware."

Source: https://www.securityweek.com/destructive-hermeticwiper-malware-targets-computers-ukraine

Ransomware Used as Decoy in Destructive Cyberattacks on Ukraine

Summary: Ransomware was used as a decoy while a Wiper utility was installed on a vulnerable system.

Source: https://www.securityweek.com/ransomware-used-decoy-destructive-cyberattacks-ukraine

Cyber attacks on Ukraine: DDoS, new data wiper, cloned websites, and Cyclops Blink

Link back to Table of Contents

From the article: “This Thursday morning, Russia started its invasion on Ukraine and, As predicted, the attacks in the physical world have been preceded and accompanied by cyber attacks.”

Source: https://www.helpnetsecurity.com/2022/02/24/cyber-attacks-ukraine/

Ukraine invasion: How a digital cold war with Russia threatens the IT industry

From the article: “In the five years since I first explored the potential impact of a Digital Cold War on the IT industry, tensions with Russia have gotten worse, especially following a series of cyberattacks on systems in the United States. These include Russia's involvement in the SolarWinds breach, as well as its interference with the 2016 US presidential elections via attacks on the Democratic National Committee infrastructure and the purchasing of tens of millions of ads on Facebook in an attempt to sow discontent among US voters.”

Source: https://www.zdnet.com/article/how-a-digital-war-with-russia-threatens-the-it-industry/

When will Russia attack GPS? Interview with former CIA analyst George Beebe

From the article: “Based on the ASAT demonstration and unclassified reports from the U.S. Director of National Intelligence, it is pretty clear that Russia can destroy all, or at least most, GPS satellites in one go.
What is less clear, is whether Russia would really do that.”

Source: https://www.gpsworld.com/when-will-russia-attack-gps-interview-with-former-cia-analyst-george-bebee/

Biden has been presented with options for massive cyberattacks against Russia

From the article: “President Joe Biden has been presented with a menu of options for the U.S. to carry out massive cyberattacks designed to disrupt Russia’s ability to sustain its military operations in Ukraine, four people familiar with the deliberations tell NBC News.”

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.nbcnews.com/politics/national-security/biden-presented-options-massive-cyberattacks-russia-rcna17558

Russian News Outlet Forced Offline by Cyberattack, Anonymous Claims Responsibility

From the article: “Hackers associated with the Anonymous collective claimed responsibility Thursday night for cyberattacks that briefly took down a number of websites identified with the Russian government—in retaliation, they said, for the Ukraine invasion.”

Source: https://www.thedailybeast.com/anonymous-hackers-claim-responsibility-for-cyberattacks-against-russian-state-news-site-rtcom

US banks are worried about the possibility of a massive Russian cyberattack, says cybersecurity CEO

From the article: “CrowdStrike's CEO said that bank executives in the US are worried about a potential Russian cyberattack.”

Source:https://www.msn.com/en-us/news/world/us-banks-are-worried-about-the-possibility-of-a-massive-russian-cyberattack-says-cybersecurity-ceo/ar-AAUiZ8y

Russian Government Websites Are Currently Down

From the article: “Several Russian government websites, including the official Kremlin site, appear to be inaccessible as of Thursday morning.”

Source: https://www-vice-com.cdn.ampproject.org/c/s/www.vice.com/amp/en/article/bvnpnv/russian-government-websites-are-currently-down

Ukraine calls for volunteer hackers to protect its critical infrastructure and spy on Russian forces

Link back to Table of Contents

From the article: “The government of Ukraine is calling on the hacking community to volunteer its expertise and capabilities, following the invasion of the country by Russian forces.”

Source: https://www.bitdefender.com/blog/hotforsecurity/ukraine-calls-for-volunteer-hackers-to-protect-its-critical-infrastructure-and-spy-on-russian-forces/

Silicon Valley Must Pull the Plug on the Kremlin

From the article: “That is the situation Google, Facebook, Twitter and other U.S. tech firms are faced with right now, as they host, distribute, amplify and in some cases help monetize Vladimir Putin’s propaganda outlets– including Russian state media that are already registered as foreign agents, as well as the official accounts of Putin’s government and its officials. With military vehicles pushing west across Ukraine, bombs falling on its cities, and blood already shed in its streets, Putin’s propaganda machine continues to advance its message on American social media platforms, part of a wholly illegal, unconscionable attack.”

Source: https://techpolicy.press/silicon-valley-must-pull-the-plug-on-the-kremlin/

Biden ‘Prepared to Respond’ If Russia Cyberattacks US

From the article: “President Joe Biden warned Thursday that the federal government would respond to Russian aggression in cyberspace.”

Source: https://www.defenseone.com/threats/2022/02/biden-prepared-respond-if-russia-cyberattacks-us/362405/

Anonymous: the hacker collective that has declared cyberwar on Russia

From the article: “Cyber conflicts are fought in the shadows, but in the case of Russia’s invasion of Ukraine, it is a group that calls itself Anonymous that has made the most public declaration of war. Late on Thursday the hacker collective tweeted from an account linked to Anonymous, @YourAnonOne, that it had Vladimir Putin’s regime in its sights.”

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia

Ukraine says its 'IT Army' has taken down key Russian sites

From the article: “Key Russian websites and state online portals have been taken offline by attacks claimed by the Ukrainian cyber police force, which now openly engages in cyber-warfare.”

Source: https://www.bleepingcomputer.com/news/security/ukraine-says-its-it-army-has-taken-down-key-russian-sites/

Russia vs Ukraine - The War in Cyberspace

From the article: “Just before Russia launched an invasion of Ukraine on February 24, Ukrainian government websites were disrupted by distributed denial-of-service (DDoS) attacks, and cybersecurity firms reported seeing a new piece of destructive malware on hundreds of devices in the country.”

Source: https://www.securityweek.com/russia-vs-ukraine-war-cyberspace

Cyber officials urge agencies to armor up for potential Russian attacks

From the article: “U.S. cybersecurity officials are urging federal agencies and large organizations to remain vigilant against the threat of Russian cyberattacks amid the country’s ongoing invasion of Ukraine. ”

Source: https://thehill.com/policy/international/russia/595945-cyber-officials-urge-federal-agencies-to-armor-up-for-potential

Ransomware Used as Decoy in Destructive Cyberattacks on Ukraine

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the article: "Ransomware was used as a decoy in some of the recent data-wiping cyberattacks against organizations in Ukraine, Symantec reports."

Source: https://www.securityweek.com/ransomware-used-decoy-destructive-cyberattacks-ukraine

Articles of Interest

Conti Ransomware 'Acquires' TrickBot as It Thrives Amid Crackdowns

From the article: :Experts at threat intelligence and ransomware disruption company AdvIntel believe the notorious TrickBot malware has reached its limits, but its development team appears to have been “acquired” by the Conti ransomware gang, which has been thriving amid recent crackdowns."

Source: https://www.securityweek.com/conti-ransomware-acquires-trickbot-it-thrives-amid-crackdowns

Additional sources:
https://www.cyberscoop.com/trickbot-shutdown-conti-emotet/

https://securityaffairs.co/wordpress/128190/cyber-crime/conti-ransomware-takes-over-trickbot.html

https://www.csoonline.com/article/3651492/trickbot-operators-slowly-abandon-the-botnet-and-replace-it-with-emotet.html

https://www.darkreading.com/threat-intelligence/trickbot-comes-up-with-a-new-set-of-tricks

https://cyberintelmag.com/malware-viruses/trickbot-group-most-likely-moving-its-activities-to-new-malware/

https://threatpost.com/trickbot-break-researchers-scratching-heads/178678/

https://securityintelligence.com/posts/new-malware-trickbot-anchordns-backdoor-upgrades-anchormail/

https://www.bleepingcomputer.com/news/security/trickbot-malware-operation-shuts-

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

down-devs-move-to-bazarbackdoor/

NSA-linked Bvp47 Linux backdoor widely undetected for 10 years

From the article: "A report released today dives deep into technical aspects of a Linux backdoor now tracked as Bvp47 that is linked to the Equation Group, the advanced persistent threat actor tied to the U.S. National Security Agency."

Source: https://www.bleepingcomputer.com/news/security/nsa-linked-bvp47-linux-backdoor-widely-undetected-for-10-years/

Additional sources:
https://cyberintelmag.com/malware-viruses/equation-groups-bvp47-covert-hacking-tool-revealed-in-detail-by-chinese-experts/

https://securityaffairs.co/wordpress/128322/apt/equation-group-bvp47-backdoor.html

https://www.cyberscoop.com/chinese-researchers-nsa-exploit-pangu-lab/

https://www.securityweek.com/chinese-researchers-detail-linux-backdoor-nsa-linked-equation-group

https://www.theregister.com/2022/02/23/chinese_nsa_linux/

CISA Warns of New Malware Framework Used by Russian 'Sandworm' Hacking Team

From the article: "Russian General Staff Main Intelligence Directorate (GRU) hacking team appears to have swapped its VPNFilter malware platform for the so-called Cyclops Blink malware framework."

Source: https://www.darkreading.com/vulnerabilities-threats/cisa-warns-of-new-malware-framework-employed-by-infamous-sandworm-hacking-team

Additional sources:
https://www.cyberscoop.com/sandworm-new-malware-cyclops-blink/

https://www.bleepingcomputer.com/news/security/us-uk-link-new-cyclops-blink-malware-to-russian-state-hackers/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

https://www.securityweek.com/new-cyclops-blink-malware-linked-russian-state-hackers-targets-firewalls

https://securityaffairs.co/wordpress/128340/malware/cyclops-blink-sandworm-malware.html

FBI, CISA, Cyber Command take aim at cyber-espionage by Iran's MuddyWater group

From the article: "U.S. and U.K. government agencies called out Iranian government-affiliated hackers Thursday, accusing them of being behind cyber-espionage targeting the defense, local government, oil and natural gas and telecommunications sectors across the globe."

Source: https://www.cyberscoop.com/alert-fbi-cisa-cyber-command-iran-muddywater/

Additional sources:
https://www.bleepingcomputer.com/news/security/us-and-uk-expose-new-malware-used-by-muddywater-hackers/

https://cyberintelmag.com/malware-viruses/new-malware-employed-by-muddywater-hackers-discovered-in-us-and-uk/

https://www.securityweek.com/us-uk-warn-iranian-cyberattacks-government-commercial-networks

https://securityaffairs.co/wordpress/128383/apt/muddywater-apt-python-backdoor.html

DeadBolt ransomware now targets ASUSTOR devices, asks 50 BTC for master key

From the article: "The DeadBolt ransomware is now targeting ASUSTOR NAS devices by encrypting files and demanding a $1,150 ransom in bitcoins."

Source: https://www.bleepingcomputer.com/news/security/deadbolt-ransomware-now-targets-asustor-devices-asks-50-btc-for-master-key/

Additional sources:
https://cyberintelmag.com/iot/deadbolt-ransomware-attack-impacts-asustor-nas-users/

Link back to Table of Contents

https://securityaffairs.co/wordpress/128356/hacking/deadbolt-ransomware-asustor-nas.html

https://www.securityweek.com/deadbolt-ransomware-targeting-asustor-nas-devices

Ransomware is top cyberattack type, as manufacturing gets hit hardest

From the article: "The report, which covers 2021, reported ransomware as the top attack type; phishing and unpatched vulnerabilities as leading infection vectors; cloud, open-source, and Docker environments as the biggest areas of focus for malware; manufacturing the most attacked industry; and Asia the most attacked region."

Source: https://www.csoonline.com/article/3651489/ransomware-is-top-cyberattack-type-as-manufacturing-gets-hit-hardest.html

Additional sources:
https://www.tripwire.com/state-of-security/security-data-protection/manufacturing-was-the-top-industry-targeted-by-ransomware-last-year/

https://www.zdnet.com/article/hackers-tried-to-shatter-the-spine-of-global-supply-chains-in-2021/

https://www.darkreading.com/attacks-breaches/ransomware-trained-on-manufacturing-firms-led-cyberattacks-in-industrial-sector

Microsoft Exchange servers hacked to deploy Cuba ransomware

From the article: "The Cuba ransomware operation is exploiting Microsoft Exchange vulnerabilities to gain initial access to corporate networks and encrypt devices."

Source: https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-hacked-to-deploy-cuba-ransomware/

Additional sources:
https://threatpost.com/microsoft-exchange-exploited-cuba-ransomware/178665/

https://cyberintelmag.com/attacks-data-breaches/cuba-ransomware-installed-on-

Link back to Table of Contents

microsoft-exchange-servers-once-they-were-hijacked/

UpdraftPlus WordPress plugin update forced for million sites

From the article: "WordPress forces the update of the UpdraftPlus plugin patch on 3 million sites to fix a high-severity vulnerability."

Source: https://securityaffairs.co/wordpress/128170/hacking/updraftplus-forced-update.html

Additional sources:
https://www.theregister.com/2022/02/21/in_brief_security/

https://www.securityweek.com/vulnerability-updraftplus-plugin-exposed-millions-wordpress-site-backups

OpenSea users lose $2 million worth of NFTs in phishing attack

From the article: "The non-fungible token (NFT) marketplace OpenSea is investigating a phishing attack that left 17 of its users without more than 250 NFTs worth around $2 million."

Source: https://www.bleepingcomputer.com/news/security/opensea-users-lose-2-million-worth-of-nfts-in-phishing-attack/

Additional sources:
https://securityaffairs.co/wordpress/128207/breaking-news/opensea-nft-marketplace-hacked.html

https://www.zdnet.com/article/opensea-scam-artists-swindle-nfts-worth-millions-in-phishing-attack/

Nigerian hacker pleads guilty to stealing payroll deposits

From the article: "A Nigerian national named Charles Onus has pled guilty in the District Court of the Southern District of New York to hacking into a payroll company's user

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

accounts and stealing payroll deposits."

Source: https://www.bleepingcomputer.com/news/security/nigerian-hacker-pleads-guilty-to-stealing-payroll-deposits/

Additional sources:
https://www.securityweek.com/nigerian-admits-us-court-hacking-payroll-company

https://cyberintelmag.com/attacks-data-breaches/in-new-york-nigerian-hacker-admits-stealing-payroll-payments-enters-guilty-plea/

Microsoft adds GCP to Defender for Cloud

From the article: "Microsoft Defender's tentacles have spread to include the Google Cloud Platform (GCP) – and beefed up visibility with a public preview of CloudKnox Permissions.…"

Source: https://www.theregister.com/2022/02/23/microsoft_defender_cloud_gcp/

Additional sources:
https://www.bleepingcomputer.com/news/microsoft/microsoft-defender-for-cloud-can-now-protect-google-cloud-resources/

https://www.csoonline.com/article/3651110/microsoft-updates-security-applications-for-multicloud-environments.html

Popular e-cigarette store was compromised to steal credit cards

From the article: "BleepingComputer has confirmed Element Vape, a prominent online seller of e-cigarettes and vaping kits was serving a credit card skimmer on its live site, likely after getting hacked."

Source: https://www.bleepingcomputer.com/news/security/popular-e-cigarette-store-was-compromised-to-steal-credit-cards/

Additional sources:
https://cyberintelmag.com/attacks-data-breaches/leading-e-cigarette-retailer-hacked-to-steal-credit-cards/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Hive Ransomware's Master Key Recovered Using Weakness in Its Encryption Algorithm

From the article: "Researchers have described the "first successful attempt" at decrypting Hive ransomware-infected data without depending on the private key that was used to limit access to the material."

Source: https://cyberintelmag.com/malware-viruses/hive-ransomwares-master-key-recovered-using-weakness-in-its-encryption-algorithm/

Additional sources: https://securityaffairs.co/wordpress/128232/security/recover-files-hive-ransomware.html

CISA Warns Critical Infrastructure Organizations of Foreign Influence Operations

From the article: "Newly published guidance from the United States Cybersecurity and Infrastructure Security Agency (CISA) provides critical infrastructure organizations with instructions on how to prepare for and mitigate foreign influence operations."

Source: https://www.securityweek.com/cisa-warns-critical-infrastructure-organizations-foreign-influence-operations

Additional sources:
https://www.bleepingcomputer.com/news/security/cisa-warns-of-hybrid-operations-threat-to-us-critical-infrastructure/

Toyota forced to suspend operations after domestic supplier hit by cyberattack

Summary: Toyota had to suspend operations all all plants in Japan as a supplier was hit by a suspected Cyberattack. The supplier was Kojima Industries Corporation

Source: https://industrialcyber.co/threats-attacks/toyota-forced-to-suspend-operations-after-domestic-supplier-hit-by-cyberattack/

Additional sources: https://www.bleepingcomputer.com/news/security/toyota-halts-production-after-reported-cyberattack-on-supplier/

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Expeditors shuts down global operations after likely ransomware attack

From the article: "Seattle-based logistics and freight forwarding company Expeditors International has been targeted in a cyberattack over the weekend that forced the organization to shut down most of its operations worldwide."

Source: https://www.bleepingcomputer.com/news/security/expeditors-shuts-down-global-operations-after-likely-ransomware-attack/

Additional sources:
https://www.bleepingcomputer.com/news/security/expeditors-shuts-down-global-operations-after-likely-ransomware-attack/

LockBit, Conti most active ransomware targeting industrial sector

From the article: "Ransomware attacks extended into the industrial sector last year to such a degree that this type of incident became the number one threat in the industrial sector."

Source: https://www.bleepingcomputer.com/news/security/lockbit-conti-most-active-ransomware-targeting-industrial-sector/

Additional sources:
https://www.bleepingcomputer.com/news/security/conti-lockbit-most-active-ransomware-targeting-industrial-sector/

NSA Notifies Cisco of Vulnerability That Exposes Nexus Switches to DoS Attacks

From the article: "The flaw arises because user-supplied data isn't properly checked, allowing an attacker to execute instructions on the operating system by sending a forged HTTP POST request to the NX-API function on the vulnerable device."

Source: https://cyberintelmag.com/cloud-security/nsa-notifies-cisco-of-vulnerability-that-exposes-nexus-switches-to-dos-attacks/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Additional sources:
https://www.securityweek.com/nsa-informs-cisco-vulnerability-exposing-nexus-switches-dos-attacks

New York Opens Joint Security Operations Center in NYC

From the article: "The "first-in-nation" cyber command center will provide municipal and local governments with threat intelligence and resources to defend themselves against cyberattacks."

Source: https://www.darkreading.com/threat-intelligence/new-york-opens-joint-security-operations-center-in-nyc

Additional sources:
https://www.securityweek.com/new-york-plans-cybersecurity-hub-coordinate-responses

Linux Snap package tool fixes make-me-root bugs

From the article: "The snap-confine tool in the Linux world's Snap software packaging system can be potentially exploited by ordinary users to gain root powers, says Qualys."

Source: https://www.theregister.com/2022/02/19/linux_snap_ubuntu/

House Bill Would Create FTC Bureau to Oversee Online Platforms

From the article: “House Democrats introduced new legislation this week that they believe would hold big tech companies—and their widely used internet platforms—accountable to users and regulators.
The Digital Services Oversight and Safety Act of 2022 would create a Bureau of Digital Services, Oversight and Safety within the Federal Trade Commission that would investigate systemic risks on online platforms and issue transparency requirements and guidance.”

Source: https://www.nextgov.com/policy/2022/02/house-bill-would-create-ftc-bureau-oversee-online-platforms/362327/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Lawmakers Question When Discarded U.S. Military Equipment is Used in Terror Attacks

From the article: “Legislation introduced by a group of almost a dozen Republican senators on Wednesday would require the national security director to report any time U.S. military equipment ditched in Afghanistan, Iraq or Syria is used in terrorist attacks against Americans and allies—or deployed in nearby places.”

Source: https://www.nextgov.com/policy/2022/02/lawmakers-question-when-discarded-us-military-equipment-used-terror-attacks/362146/

"Better Late Than Never" No Longer a Cybersecurity Option: Prepare Now for the Current Threat

From the article: “The United States is facing a very real cybersecurity threat. As Russia intensifies actions in Ukraine, economic sanctions are sure to follow. In response, experts expect Russia to launch cyberattacks against high-value targets in the West, including vital infrastructure. For owners and operators of critical infrastructure resources, it is important to take action to prevent serious impacts. We recommend reviewing the Cyber and Infrastructure Security Agency’s (CISA) guidelines.”

Source: https://www.jdsupra.com/legalnews/better-late-than-never-no-longer-a-2837807/

Cybersecurity: Board of Director Litigation Risk

From the article: “With the surge of data and cybersecurity breaches, corporate directors and officers have become targets for shareholder derivative lawsuits. Fortunately, there are procedural measures that directors and officers can put in place in order to mitigate the risk of litigation.”

Source: https://www.jdsupra.com/legalnews/cybersecurity-board-of-director-4722584/

The Price set on Ransomware – Avoiding the Cyber Sucker Punch

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the article: “Most businesses today understand that the internet can be a dangerous place. As an organization grows beyond the very early stage of one or two employees and a few thousand dollars in sales, the cyber strategy of “security by obscurity” must give way to a balanced and nuanced approach to mitigating the risks posed by the dark web.”

Source: https://www.jdsupra.com/legalnews/the-price-set-on-ransomware-avoiding-8900177

Practical Strategies to Combat Common Cybersecurity Threats and Mitigate Risk

From the article: “What would you do if you woke up tomorrow and your company was experiencing a cybersecurity incident? What if IT systems were completely locked down? What if you could not use phones, check emails, or receive orders? What if you could not operate machinery or pay payroll? ”

Source: https://www.jdsupra.com/legalnews/practical-strategies-to-combat-common-7256004/

Russian hackers raided defense contractors for two years, stole sensitive info: US

From the article: “For the last two years hackers backed by the Russian government worked to infiltrate American defense contractor systems, sometimes raiding the companies for months at a time, to steal sensitive, unclassified information, the US government warned today.”

Source: https://breakingdefense.com/2022/02/russian-hackers-raided-defense-contractors-for-two-years-stole-sensitive-info/

Iran-Linked Hackers Conducting Operations Against Government Networks, Intel Agencies Warn

From the article: “With the world’s eyes on Russia’s multipronged attack on Ukraine—including hackers attacking and disabling Ukrainian government and financial websites—the U.S. government issued a warning Thursday that Iranian government-

sponsored hackers are conducting active “cyber operations against government and commercial networks.””

Source: https://www.nextgov.com/cybersecurity/2022/02/iran-linked-hackers-conducting-operations-against-government-networks-intel-agencies-warn/362391/

War Exclusion Does Not Bar Recovery for Losses from a Nation-State Cyber Attack on Pharma Giant and the Effects on Insurance Policies from Increased Globalized Threats of Ransomware

From the article: “The Cybersecurity & Infrastructure Security Agency noted that cybersecurity authorities in the United States, Australia, and the United Kingdom assess that “if the ransomware criminal business model continues to yield financial returns for ransomware actors, ransomware incidents will become more frequent. Every time a ransom is paid, it confirms the viability and financial attractiveness of the ransomware criminal business model.””

Source: https://www.jdsupra.com/legalnews/war-exclusion-does-not-bar-recovery-for-5565158/

A Prelude to Enforcement: Colorado AG Issues Remarks Opining on What Constitutes Reasonable Security Measures

From the article: “Last month, on Data Privacy Day, Colorado’s Attorney General Philip Weiser released prepared remarks entitled “The Way Forward on Data Privacy and Data Security” that shed some light on his approach to enforcing Colorado’s existing data security law, and the Colorado Privacy Act (“CPA”) once it comes into effect in 2023.”

Source: https://www.jdsupra.com/legalnews/a-prelude-to-enforcement-colorado-ag-2772233/

FTC emphasizes expectations around the health breach notification rule

From the article: “The Federal Trade Commission (FTC) recently has signaled its intent to inject new life into a longstanding but rarely triggered rule governing health breach

notifications for non-HIPAA-covered health records. ”

Source: https://www.jdsupra.com/legalnews/ftc-emphasizes-expectations-around-the-9607643/

Capital One Reaches $190 Million Settlement In Connection with 2019 Data Breach

From the article: “The saga of the Capital One data breach, which impacted an estimated 106 million individuals in the U.S. and Canada, may soon be coming to an end. After more than two years of litigation, the parties have reached a settlement that would resolve existing and future consumer claims arising out of the 2019 breach which impacted Capital One customer information stored in the Amazon Web Services (AWS) cloud environment. ”

Source: https://www.jdsupra.com/legalnews/capital-one-reaches-190-million-5708035/

Top 5 Cyber Security Threats the Manufacturing Industry Should Watch in 2022

From the article: “Companies continue to see headlines about cyberattacks, but manufacturing companies, specifically, have become more targeted in the last few years. In the most recent issue of The Illinois Manufacturer, Molly Arranz and Sofia Valdivia’s article, “Top 5 Cyber Security Threats the Manufacturing Industry Should Watch in 2022,” helps companies learn more about what they are facing, and where they can go from here.”

Source: https://www.jdsupra.com/legalnews/top-5-cyber-security-threats-the-8905204/

Ransomware attacks rise almost 93% in 2021, according to NCC Group Annual Threat Monitor

From the article: “Global cyber security and risk mitigation expert NCC Group has revealed that ransomware attacks almost doubled in 2021, rising 92.7% year-on-year, according to its 2021 Annual Threat Monitor.”

Source: https://www.jdsupra.com/legalnews/ransomware-attacks-rise-almost-93-in-8714706/

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Owners of Bricked Jeep Grand Cherokee L's Blame Faulty Key Fob Electronics

From the article: "This seems to not be software-related, but hardware-related, perhaps to do specifically with an in-vehicle "antenna or module," according to the forum thread. We've reached out to Jeep for comment on the situation, though we've yet to receive one at the time of publishing. These bricked trucks are still sitting at dealerships, and nobody knows yet when a fix will arrive."

Source: https://www.thedrive.com/news/44410/owners-of-bricked-jeep-grand-cherokee-ls-blame-faulty-key-fob-electronics

2022 Jeep Grand Cherokee Hit With Stop-Sale After Owners Stranded by Faulty Electronics

Summary: More information on the Jeep Grand Cherokee L key fob fault issue. There is now a 'stop sale' on the vehicles. The source is a 'Radio Frequency Hub Module' causing issues between the car and the key fob

Source: https://www.thedrive.com/tech/44438/2022-jeep-grand-cherokee-hit-with-stop-sale-after-owners-stranded-by-faulty-electronics

Much-Anticipated Crypto Unlock For Nvidia Graphic Cards Installs Malware

Summary: LHR - Light Hash Rate limiter for GPU cards was hailed as a solution to enable crypto mining on the popular Nvidia cards; however a utility actually contained a trojan which attempted to construct an extensive botnet.

Source: https://cyberintelmag.com/malware-viruses/much-anticipated-crypto-unlock-for-nvidia-graphic-cards-installs-malware/

Dragos detects three new threat activity groups with interest in targeting ICS/OT environments in 2021

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Summary: Kostovite, Petrovite, Erythrite are threat actors identified in the Dragos report that have significant impact in 2021

Source: https://industrialcyber.co/threats-attacks/dragos-detects-three-new-threat-activity-groups-with-interest-in-targeting-ics-ot-environments-in-2021/

Unit 42: SockDetour Backdoor Employed in Cyberattacks Against Defense Firms

From the article: "Considering the telemetry data obtained by Unit 42 and the analysis of the samples collected, they think the threat actor behind SockDetour has been employing the tools to target US-based defense businesses. According to Unit 42, at least four defense contractors have been targeted by this effort, with at least one of them compromised. By loading filelessly in genuine service processes and exploiting legitimate processes' network ports to construct its own encrypted C2 channel, SockDetour helps attackers to remain undetected on infected Windows servers. There were no more SockDetour samples found in public sources, and the plugin DLL is still unknown. They further said it's being supplied using SockDetour's encrypted route and communicating through hijacked sockets."

Source: https://cyberintelmag.com/attacks-data-breaches/unit-42-sockdetour-backdoor-employed-in-cyberattacks-against-defense-firms/

GE SCADA Product Vulnerabilities Show Importance of Secure Configurations

Summary: SecurityWeek summary of the Cimplicity vulnerabilities disclosed on the GE SCADA product.

Source: https://www.securityweek.com/ge-scada-product-vulnerabilities-show-importance-secure-configurations

CISA, FBI Issue Warnings on WhisperGate, HermeticWiper Attacks

Summary: Update and warnings on the WhisperGate and HerememticWiper attacks. Both deserve special attention in light of current world events.

Link back to Table of Contents

Source: https://www.securityweek.com/cisa-fbi-issue-warnings-whispergate-hermeticwiper-attacks

Nvidia confirms it's investigating an "incident," reportedly a huge cyberattack

From the article: "Early Saturday morning, the dark web intelligence firm DarkTracer tweeted that Lapsus$, a ransomware gang recently linked to an attack on Portugal's largest TV channel, has claimed responsibility, leaking what it says are the password hashes for Nvidia employees, and indicating it has other data including source code and information related to RTX GPUs."

Source: https://www.theverge.com/2022/2/25/22951376/nvidia-incident-alleged-cyberattack-february-2022

Symantec: Super-Stealthy 'Daxin' Backdoor Linked to Chinese Threat Actor

Summary: Daxin malware linked to Chinese ThreatActor; enables tunneling via hard to detect TCP traffic to and from secure networks

Source: https://www.securityweek.com/symantec-super-stealthy-daxin-backdoor-linked-chinese-threat-actor

Bridgestone Americas Has Disconnected Production Facilities After 'Security Incident'

From the article: "After a possible cyber-attack yesterday morning (February 27), Bridgestone Americas apparently "disconnected" several of its production and retreading operations. According to the reports, the tiremaker stated that it is unable to establish with certainty the scale or type of any possible event at this time.

Source: https://cyberintelmag.com/attacks-data-breaches/bridgestone-americas-has-disconnected-production-facilities-after-security-incident/

New EU Data Act to Extend Protections to Non-Personal Data

Link back to Table of Contents

Summary: EU Drafted a new Data Law allowing stakeholders greater control over industrial data.

Source: https://www.jdsupra.com/legalnews/new-eu-data-act-to-extend-protections-7404421/

Satellite Outage Knocks Out Thousands of Enercon's Wind Turbines - Slashdot

Summary: Enercon lost 11GW of wind turbine generation capability due to a massive satellite disruption. Viasat (the provider) is investigating a loss of service to business and residential customers late last week.

Source: https://hardware.slashdot.org/story/22/02/28/2159258/satellite-outage-knocks-out-thousands-of-enercons-wind-turbines

Multiple Flaws Discovered in Snap-Confine Function on Linux Platforms

From the article: "Qualys security researchers have uncovered several flaws in Canonical's Snap software packaging and deployment system."

Source: https://cyberintelmag.com/cloud-security/multiple-flaws-discovered-in-snap-confine-function-on-linux-platforms/

Software and Firmware Updates From Intel Patch 18 High-Severity Flaws

From the article: "Intel has provided software and firmware patches to address several security flaws discovered in its devices."

Source: https://cyberintelmag.com/cloud-security/software-and-firmware-updates-from-intel-patch-18-high-severity-flaws/

Microsphere-assisted, nanospot, non-destructive metrology for semiconductor devices

Link back to Table of Contents

From the article: "However, there has been an increasing demand for a significant reduction in the physical spot diameter used in the SE technique; the spot diameter should be at least 10 times smaller than the cell dimension (~30 × 40 μm2) of typical dynamic random-access memory to be able to measure in-cell critical dimension (CD) variations."

Source: https://semiengineering.com/microsphere-assisted-nanospot-non-destructive-metrology-for-semiconductor-devices/

The Wiretap Channel for Capacitive PUF-Based Security Enclosures

From the article: “In order to protect devices from physical manipulations, protective security enclosures were developed. However, these battery-backed solutions come with a reduced lifetime, and have to be actively and continuously monitored."

Source: https://semiengineering.com/the-wiretap-channel-for-capacitive-puf-based-security-enclosures/

Closer look at Windows 11's new Task Manager

From the article: "Microsoft has finally started testing a new version of Task Manager with users in the Windows Insider Program."

Source: https://www.bleepingcomputer.com/news/microsoft/closer-look-at-windows-11s-new-task-manager/

BEC scammers impersonate CEOs on virtual meeting platforms

From the article: "The FBI warned US organizations and individuals are being increasingly targeted in BECattacks on virtual meeting platforms."

Source: https://securityaffairs.co/wordpress/128206/hacking/fbi-bec-virtual-meeting-platforms.html

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Top chipmakers ignore India's semiconductor factory subsidies

From the article: "India has revealed the identities of companies that have applied to build semiconductor manufacturing facilities on its soil under a $10 billion subsidy scheme – and none are substantial chipmakers."

Source: https://www.theregister.com/2022/02/21/india_semiconductor_subsidies/

US to attack cyber criminals first, ask questions later – if it protects victims

From the article: "The United States Department of Justice (DoJ) has revealed new policies that may see it undertake pre-emptive action against cyber threats.…"

Source: https://www.theregister.com/2022/02/21/doj_cyber_offensive_policy/

Motorola case shows importance of detecting insider IP theft quickly

From the article: "The Department of Justice (DOJ) announced on February 7, 2022, the unsealing of an indictment that charged Chinese telecommunications company Hytera Communications with conspiring with former Motorola Solutions employees to “steal digital mobile radio (DMR) technology from Motorola.”

Source: https://www.csoonline.com/article/3649753/motorola-case-shows-importance-of-detecting-insider-ip-theft-quickly.html

Shifting security left at WGU

From the article: "James Chandler, vice president of security for Western Governors University, has successfully moved security left by implementing a scorecard system that requires devops teams to meet certain standards and enforcing those expectations through business processes."

Source: https://www.csoonline.com/article/3649772/shifting-security-left-at-wgu.html

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Cybersecurity Tools Lie Unused in Federal Agencies' Toolboxes

From the article: "Concerns over the possible Russian use of cyber weapons against U.S. domestic critical infrastructure in connection with the Ukraine crisis—warnings renewed on Feb. 11—should prompt reconsideration of the still-deferential posture of U.S. cybersecurity policy toward much of the private sector. Once again, though, complaints against "government mandates" may block action."

Source: https://www.lawfareblog.com/cybersecurity-tools-lie-unused-federal-agencies-toolboxes

How much can you trust your printer?

From the article: "In this interview with Help Net Security, Scott Best, Director of anti-tamper security technology at Rambus, talks about what organizations should be aware of when it comes to printer security and what they should do to remain secure."

Source: https://www.helpnetsecurity.com/2022/02/22/printer-security/

CMMC Accreditation Body looks ahead to voluntary assessments, growing 'ecosystem'

From the article: "The Cybersecurity Maturity Model Certification is at least months away from showing up as a requirement in defense contracts, but the CMMC Accreditation Body is gearing up for voluntary assessments and is also looking to recruit more cybersecurity assessors."

Source: https://federalnewsnetwork.com/defense-news/2022/02/cmmc-accreditation-body-looks-ahead-to-voluntary-assessments-growing-ecosystem/

How the US Can Reshore Semiconductor Manufacturing

From the article: "If the United States develops the most innovative semiconductor designs in the world, but can't manufacture the less complicated chips that its electronics and automobile industries require, is it a case of penny wise, pound foolish?"

Link back to Table of Contents

Source: https://www.industryweek.com/supply-chain/article/21234163/how-the-us-can-reshore-semiconductor-manufacturing

Navy thinks it has some specific answers to the 'fix our computers' complaint

From the article: "The reasons behind the "fix our computers" problem are fairly complex, but I thought one of the most salient points the post's author, Michael Kanaan, the operations director at that Air Force/MIT AI Accelerator made was the portion that pointed out the endpoint security bits. If two or five different malware scanners are running at all times, often fighting against one another, your desktop or laptop is spending more hardware resources toward looking for threats than doing its actual job. Opening that Excel sheet is going to take a while."

Source: https://federalnewsnetwork.com/dod-reporters-notebook-jared-serbu/2022/02/navy-thinks-it-has-some-specific-answers-to-the-fix-our-computers-complaint/?amp=1

ECIA and Texas A&M University Launch Major Research Project Quantifying Value of Authorized Distribution

From the article: "In 2001-2002, the Industrial Distribution Program at Texas A&M University conducted the ground-breaking study entitled 'Quantifying the Value of Authorized Electronic Distributors.' The results showed that using the Distribution channel resulted in savings ranging from 15-50% for customers and suppliers. These results were widely presented, published as a report and as an online Value Calculator."

Source: https://www.ecianow.org/index.php?option=com_content&view=article&id=435:ecia-and-texas-a-m-university-launch-research-project-quantifying-value-of-authorized-distribution&catid=23:news&Itemid=145

White House invests $35M to tackle rare earth supply vulnerabilities

From the article: "Higher amounts of rare earth metals are required in the production of electric vehicles, advanced batteries, wind turbines and other renewable products. An

average electric car requires six times the mineral inputs of a conventional car, while an onshore wind plant needs nine times more mineral resources than a gas-fired plant, according to a May report from the International Energy Agency."

Source: https://www.supplychaindive.com/news/white-house-critical-minerals-supply-chain-investment/619231/

ATT&CK for Mobile: Reintroduction and 2022 Goals

From the article: "With the huge rise in critical work data on smartphones over the past couple of years, mobile security is more important than ever before. With this in mind, since early 2021 we've been re-designing and rewriting the entirety of ATT&CK for Mobile. We've also spent a lot of time considering how we want to continue to enhance Mobile moving forward, including increasing community understanding of the mobile threat landscape."

Source: https://medium.com/mitre-attack/attack-for-mobile-2022-roadmap-4fdb40a88a48

CISA Alerts on Actively Exploited Flaws in Zabbix Network Monitoring Platform

From the article: "The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has warned of active exploitation of two security flaws impacting Zabbix open-source enterprise monitoring platform, adding them to its Known Exploited Vulnerabilities Catalog."

Source: https://thehackernews.com/2022/02/cisa-alerts-on-actively-exploited-flaws.html

Intel Bets on Blockchain

From the article: "Does blockchain have a future beyond selling digital NFT trinkets like Melania Trump's watercolors and short video clips of great moments in sports? Intel says yes. In his recent online editorial titled "Blockchain and the New Custom Compute Group," Intel's senior vice president and general manager of the Accelerated Computing Systems and Graphics Group, Raja Koduri, announced that Intel has created a new accelerator group called the "Custom Compute Group" and will be shipping a custom

Link back to Table of Contents

blockchain accelerator designed by this group later this year."

Source: https://www.eetimes.com/intel-bets-on-blockchain/

AnandTech interview with Dr. Ann Kelleher: EVP and GM of Intel's Technology Development

From the article: "It's somewhat of an understatement to say that Intel's future roadmap on its process node development is one of the most aggressive in the history of semiconductor design. The company is promising to pump out process nodes quicker than we've ever seen, despite having gone through a recent development struggle. Even with CEO Pat Gelsinger promising more than ever before, it's up to Intel's Technology Development (TD) team to pick up the ball and run with it in innovative ways to make that happen"

Source: https://www.anandtech.com/show/17243/anandtech-interview-with-dr-ann-kelleher

Why DevOps pipelines are under attack and how to fight back

From the article: "In mid-2017, Russian state-sponsored attackers installed a malicious worm in a Ukrainian financial software package. When businesses updated their software, it became infected. The worm, NotPetya, spread quickly, doing billions of dollars of damage around the world. The White House called it "the most destructive and costly cyberattack in history.""

Source: https://www.csoonline.com/article/3649798/why-devops-pipelines-are-under-attack-and-how-to-fight-back.html

It's Time for Just-in-Case

From the article: "Can we now admit that just-in-time production systems dependent on far-flung suppliers involves great risk?"

Source: https://www.assemblymag.com/blogs/14-assembly-blog/post/96904-its-time-for-just-in-case

Link back to Table of Contents

North American PCB Sales Up 7.7% in January

From the article: “Sales at North American printed circuit board fabricators were up 7.7% compared to the same month last year.
On a sequential basis, shipments fell 22.1%, IPC announced today.”

Source: https://www.pcdandf.com/pcdesign/index.php/editorial/menu-news/fab-news/16395-north-american-pcb-sales-up-7-7-in-january

Iran's MuddyWater Hacker Group Using New Malware in Worldwide Cyber Attacks

From the article: “Cybersecurity agencies from the U.K. and the U.S. have laid bare a new malware used by the Iranian government-sponsored advanced persistent threat (APT) group in attacks targeting government and commercial networks worldwide.”

Source: https://thehackernews.com/2022/02/irans-muddywater-hacker-group-using-new.html

How Manufacturers Can Best Mitigate And Navigate Risk

From the article: “In recent years, many organisations have started to adopt a broader perspective when it comes to risk-based thinking. Much of this can be attributed to the ever-increasing requirements of regulatory compliance as well as unexpected macro factors that have impacted operations.”

Source: https://www.emsnow.com/28393-2/

U.S. governors urge swift action on $52 billion chip funding bill

From the article: “A bipartisan group of 22 governors Thursday urged leaders in Congress to move quickly to finalize $52 billion in government funding to subsidize the production of semiconductor chips.”

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.reuters.com/world/us/us-governors-urge-swift-action-52-billion-chip-funding-bill-2022-02-24/

Taiwan's TSMC says to comply with export control rules on Russia

From the article: “Chipmaker TSMC is fully committed to complying with new export control rules, the company said on Friday, after Taiwan's government said it would join international sanctions on Russia for invading Ukraine.”

Source: https://www.reuters.com/technology/taiwans-tsmc-says-comply-with-export-control-rules-russia-2022-02-25/

Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks

From the article: “The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Cyber Command Cyber National Mission Force (CNMF), and the United Kingdom’s National Cyber Security Centre (NCSC-UK) have observed a group of Iranian government-sponsored advanced persistent threat (APT) actors, known as MuddyWater, conducting cyber espionage and other malicious cyber operations targeting a range of government and private-sector organizations across sectors—including telecommunications, defense, local government, and oil and natural gas—in Asia, Africa, Europe, and North America. Note: MuddyWater is also known as Earth Vetala, MERCURY, Static Kitten, Seedworm, and TEMP.Zagros.”

Source: https://www.cisa.gov/uscert/ncas/alerts/aa22-055a

Exclusive: Intel Reveals Plans for Massive New Ohio Factory, Fighting the Chip Shortage Stateside

From the article: “As part of an effort to regain its position as a leading maker of semiconductors amidst a global chip shortage, Intel is committing $20 billion to build a manufacturing mega-site in New Albany, on the outskirts of Columbus, Ohio, the company exclusively confirmed to TIME.”

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://time.com/6140476/intel-building-factory-ohio/

Why vendors can't wait for CMMC to raise their cyber standards

From the article: “”The current geopolitical climate...should have companies thinking about how they are currently defending themselves against cyber attacks," a defense official said on Thursday.”

Source: https://fcw.com/defense/2022/02/why-vendors-cant-wait-cmmc-raise-their-cyber-standards/362454/

How Congress Can Ensure CHIPS Act Funding Advances National Security Interests

From the article: “But as Congress leans into industrial policy, it has a responsibility to ensure that taxpayer dollars are spent strategically to advance U.S. interests, not amounting to a blank check untethered to U.S. strategic objectives. CHIPS Act investment must tilt the geopolitical scales strongly toward the U.S. side and, along with other proposals under consideration, advance U.S. leadership in the chips race vis-a-vis China. ”

Includes links to many references and reports

Source: https://www.lawfareblog.com/how-congress-can-ensure-chips-act-funding-advances-national-security-interests

Koreans Targeted by PseudoManuscrypt Malware Spreading Like CryptBot

From the article: "A botnet known as PseudoManuscrypt has been targeting Windows workstations in South Korea since at least May 2021. It uses the same distribution methods as another malware known as CryptBot."

Source: https://cyberintelmag.com/malware-viruses/koreans-targeted-by-pseudomanuscrypt-malware-spreading-like-cryptbot/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Customers of Monzo Online Banking Targeted Through New Phishing Attack

From the article: "Phishing messages sponsored by a growing network of rogue websites are targeting users of Monzo, the UK's popular digital-only banking services."

Source: https://cyberintelmag.com/attacks-data-breaches/customers-of-monzo-online-banking-targeted-through-new-phishing-attack/

Stealing Bicycles by Swapping QR Codes

From the article: "They're stealing Citi Bikes by switching the QR scan codes on two bicycles near each other at a docking station, then waiting for an unsuspecting cyclist to try to unlock a bike with his or her smartphone app."

Source: https://www.schneier.com/blog/archives/2022/02/stealing-bicycles-by-swapping-qr-codes.html

Your Low-Power Wide-Area Network: Selecting The Best Location Positioning Option

From the article: "LPWANs have use cases including asset tracking solutions, smart city infrastructure, and smart metering. In many of these use cases, performance is dependent on accurate location capabilities."

Source: https://www.iotforall.com/?p=162381

NIST proposes model to assess cybersecurity investment strategies in network security

From the article: "The larger the network, the larger the attack surface. Computational models may pinpoint the best places for investment."

Source: https://www.zdnet.com/article/nist-proposes-model-to-assess-cybersecurity-investment-strategies-in-network-security/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

At Olympics, Cybersecurity Worries Linger in Background

From the article: "Warnings to use disposable “burner” phones and laptops. Privacy-protecting software. Concerns about a security flaw in an official Games smartphone app."

Source: https://www.securityweek.com/olympics-cybersecurity-worries-linger-background

Open Source Code: The Next Major Wave of Cyberattacks

From the article: "The ubiquity of open source software presents a significant security risk, as it opens the door for vulnerabilities to be introduced (intentionally or inadvertently) to those who use it."

Source: https://www.darkreading.com/vulnerabilities-threats/open-source-code-the-next-major-wave-of-cyberattacks

SaaS and Paas: Selecting an IoT Platform

From the article: "SaaS or PaaS? The best IoT platform option for your business depends on your business's needs and stage in the IoT journey."

Source: https://www.iotforall.com/?p=155664

New Xenomorph Android malware targets customers of 56 banks

From the article: "A new malware called Xenomorph distributed through Google Play Store has infected more than 50,000 Android devices to steal banking information."

Source: https://www.bleepingcomputer.com/news/security/new-xenomorph-android-malware-targets-customers-of-56-banks/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Cookware giant Meyer discloses cyberattack that impacted employees

From the article: "Meyer Corporation, the largest cookware distributor in the U.S., and the second-largest globally, has informed U.S. Attorney General offices of a data breach affecting thousands of its employees."

Source: https://www.bleepingcomputer.com/news/security/cookware-giant-meyer-discloses-cyberattack-that-impacted-employees/

Revamped CryptBot malware spread by pirated software sites

From the article: "A new version of the CryptBot info stealer was seen in distribution via multiple websites that offer free downloads of cracks for games and pro-grade software."

Source: https://www.bleepingcomputer.com/news/security/revamped-cryptbot-malware-spread-by-pirated-software-sites/

Researchers Devise Method to Decrypt Hive Ransomware-Encrypted Data

From the article: "A group of academic researchers has found a way to exploit a security flaw in the encryption algorithm used by the Hive ransomware to recover hijacked and encrypted data."

Source: https://www.securityweek.com/researchers-devise-method-decrypt-hive-ransomware-encrypted-data

How SMS PVA services could undermine SMS-based verification

From the article: "Crooks abuse some SMS PVA services that allow their customers to create disposable user accounts to conduct malicious activities."

Source: https://securityaffairs.co/wordpress/128242/cyber-crime/sms-pva-services.html

Link back to Table of Contents

Coinbase Pays $250K for 'Market-Nuking' Security Flaw

From the article: "Cryptocurrency exchange Coinbase has shelled out its largest ever bug bounty payment -- a quarter of a million dollars -- for what was described as a “market-nuking” security flaw that could have allowed users to sell bitcoins they didn’t own."

Source: https://www.securityweek.com/coinbase-pays-250k-market-nuking-security-flaw

New phishing campaign targets Monzo online-banking customers

From the article: "Users of Monzo, one of the UK's most popular digital-only banking platforms, are being targeted by phishing messages supported by a growing network of malicious websites."

Source: https://www.bleepingcomputer.com/news/security/new-phishing-campaign-targets-monzo-online-banking-customers/

Panelists Challenge U.S. Navy's Strategic Thinking

From the article: "A WEST conference and exhibition panel discussion designed deliberately to be provocative questioned whether the U.S. Navy’s strategy permits the kind of innovation necessary to vie with peer competitors such as China."

Source: https://www.afcea.org/content/panelists-challenge-us-navys-strategic-thinking

Intel’s plans for a manufacturing turnaround

From the article: "Hello and welcome to Protocol Enterprise! Today: Intel is playing catch-up, the Pentagon is going after AI, and here’s what’s coming next week in enterprise tech."

Source: https://www.protocol.com/newsletters/protocol-enterprise/intel-manufacturing-pentagon-ai

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Wiper Used in Attack on Iran National Media Network

From the article: "An analysis of a January attack targeting Iran's national media corporation has found the use of multiple malware families, including a data-wiper and custom backdoors."

Source: https://www.securityweek.com/wiper-used-attack-iran-national-media-network

Automakers Need to Lock Their Doors Against Ransomware

From the article: "Issues with patch management and other security practices leave auto manufacturers open to attacks."

Source: https://www.darkreading.com/tech-trends/automakers-need-to-lock-their-doors

DOJ drops Trump-era 'China Initiative' but remains focused on nation-state threats

From the article: "The U.S. Department of Justice is closing down its controversial "China Initiative," instead launching a broader strategy toward countering multiple threats from several countries, a senior department official said Wednesday."

Source: https://www.cyberscoop.com/china-initiative-dropped-doj-nation-state-threats/

Millions of dollars pour into security compliance startups amid pressure on business

From the article: "Government agencies and industry groups are putting increasing pressure on enterprises to ensure their systems, and the vast amounts of data they are holding, are protected against the growing threat of ransomware and others cyber-attacks…."

Source:
https://www.theregister.com/2022/02/23/secureframe_security_compliance_investment/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Samsung Shattered Encryption on 100M Phones

From the article: "One cryptography expert said that 'serious flaws' in the way Samsung phones encrypt sensitive material, as revealed by academics, are 'embarrassingly bad.'"

Source: https://threatpost.com/samsung-shattered-encryption-on-100m-phones/178606/

Dridex Malware Downloader Connected to Entropy Ransomware

From the article: "The newly discovered Entropy ransomware shares coding similarities with the general-purpose Dridex malware, which began as a banking trojan."

Source: https://cyberintelmag.com/malware-viruses/dridex-malware-downloader-connected-to-entropy-ransomware/

Horde Webmail Software Has 9-Year-Old Unfixed Email Hacking Vulnerability

From the article: "Horde Webmail users are being asked to disable a feature in order to protect themselves from a nine-year-old unpatched security flaw in the program that may be used to acquire total access to email accounts merely by previewing an attachment."

Source: https://cyberintelmag.com/cloud-security/horde-webmail-software-has-9-year-old-unfixed-email-hacking-vulnerability/

What Does Least Privilege Access Mean for Cloud Security?

From the article: "While traditional security controls are necessary at the perimeter, organizations also need to prevent malicious privileged access."

Source: https://www.darkreading.com/edge-ask-the-experts/what-role-will-least-privilege-access-play-in-cloud-security-strategy-

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Ransomware extortion doesn't stop after paying the ransom

From the article: "A global survey that looked into the experience of ransomware victims highlights the lack of trustworthiness of ransomware actors, as in most cases of paying the ransom, the extortion simply continues."

Source: https://www.bleepingcomputer.com/news/security/ransomware-extortion-doesnt-stop-after-paying-the-ransom/

Tales from the Dark Web, Part 3: How Criminals Monetize Ransomware

From the article: "Ransomware operators rely on cryptocurrency and other payment schemes to keep their activities under the radar and harder to trace."

Source: https://www.darkreading.com/crowdstrike/tales-from-the-dark-web-part-3-how-criminals-monetize-ransomware

Forcepoint One combines zero trust and SASE under a single umbrella

From the article: "Its Forcepoint One is an all-in-one cloud platform that simplifies enterprise security by integrating zero trust and secure access service edge (SASE) technologies so security teams can manage one set of policies through a single console."

Source: https://www.csoonline.com/article/3651328/forcepoint-one-combines-zero-trust-and-sase-under-a-single-umbrella.html

Microsoft Debuts Unified Service for Multicloud ID Management

From the article: "With nine in 10 companies adopting a multicloud strategy, service providers are focused on finding ways to support the management and security efforts of businesses that rely on multiple cloud resources."

Link back to Table of Contents

Source: https://www.darkreading.com/cloud/microsoft-debuts-unified-service-for-multi-cloud-id-management

Sextortion Rears Its Ugly Head Again

From the article: "Attackers are sending email blasts with malware links in embedded PDFs as a way to evade email filters, lying about having fictional "video evidence.""

Source: https://threatpost.com/sextortion-rears-its-ugly-head-again/178595/

IoT Congestion Is Challenging Engineers to a 'Dual'

From the article: "This white paper provides an overview of the role that dual-band Wi-Fi can play in IoT deployments & provides a number of practical design considerations for engineers."

Source: https://www.iotforall.com/white-paper/iot-congestion-is-challenging-engineers-to-a-dual

Redstor extends protection of Kubernetes in AWS, unifies container backups

From the article: "The firm has added support for Amazon Elastic Kubernetes (Amazon EKS), a managed container service for handling applications in the cloud or on-premises, giving partners the ability to scale customer backups and removing the need to rely on disparate, ununified solutions."

Source: https://www.csoonline.com/article/3651054/redstor-extends-protection-of-kubernetes-in-aws-unifies-container-backups.html

Private vs. Public Fixed IP IoT SIM

From the article: "The overall benefits and downfalls of the public vs. private fixed IP SIM must be analyzed closely to meet your specific IoT business needs."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.iotforall.com/?p=146384

Creaky Old WannaCry, GandCrab Top the Ransomware Scene

From the article: "Nothing like zombie campaigns: WannaCry's old as dirt, and GandCrab threw in the towel years ago. They're on auto-pilot at this point, researchers say."

Source: https://threatpost.com/wannacry-gandcrab-top-ransomware-scene/178589/

Ubuntu applies security fixes for all versions back to 14.04

From the article: "Ubuntu has issued a batch of updates that cover the default as well as the AWS and KVM flavours for the current short-term release 21.10, both the original 5.04 and OEM 5.14 builds for the current 20.04 LTS release, as well as 18.04, and, surprisingly, even 16.04 and 14.04."

Source: https://www.theregister.com/2022/02/23/ubuntu_kernel_updates/

Why Passwordless Is at an Impasse

From the article: "Many widely used business applications aren't built to support passwordless login because identity and authentication remain siloed."

Source: https://www.darkreading.com/operations/why-passwordless-is-at-an-impasse

Astrix Security Nabs $15M to Tackle Attack Surface Sprawl

From the article: "Israeli startup Astrix Security has banked $15 million in early stage venture capital investment to build technology to help organizations secure third-party app integrations."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.securityweek.com/astrix-security-nabs-15m-tackle-attack-surface-sprawl

Shadowserver Starts Conducting Daily Scans to Help Secure ICS

From the article: "The Shadowserver Foundation this week announced that it has started conducting daily internet scans in an effort to identify exposed industrial control systems (ICS) and help organizations reduce their exposure to attacks."

Source: https://www.securityweek.com/shadowserver-starts-conducting-daily-scans-help-secure-ics

Sway AI Announces No-Code Artificial Intelligence (AI) Platform to Accelerate AI Adoption in Every Enterprise

From the article: "Sway AI announced its no-code AI platform for enterprise users and data scientists, allowing enterprises to build and deploy AI solutions."

Source: https://www.iotforall.com/?post_type=press-releases&p=164692

mPERS Wearables: Benefits of Hybrid Location for the Emergency Device

From the article: "Maintaining quality of life has more recently become a growing challenge. mPERS can help caregivers ensure their loved one's safety."

Source: https://www.iotforall.com/?p=162385

CISA Warns of Attacks Exploiting Recent Vulnerabilities in Zabbix Monitoring Tool

From the article: "The United States Cybersecurity and Infrastructure Security Agency (CISA) this week expanded its Known Exploited Vulnerabilities Catalog with two critical flaws in the Zabbix enterprise monitoring solution."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.securityweek.com/cisa-warns-attacks-exploiting-recent-vulnerabilities-zabbix-monitoring-tool

Bypassing Apple's AirTag Security

From the article: "A Berlin-based company has developed an AirTag clone that bypasses Apple's anti-stalker security systems. Source code for these AirTag clones is available online."

Source: https://www.schneier.com/blog/archives/2022/02/bypassing-apples-airtag-security.html

Empire State Development Announces KORE Expands Operations in Monroe County

From the article: "Empire State Development (ESD) announced KORE will expand its operations in Monroe County, moving to a new, larger location of in the Town of Pittsford."

Source: https://www.iotforall.com/?post_type=press-releases&p=163196

Dutch govt issues data protection report card for Microsoft

From the article: "A Data Protection Impact Assessment (DPIA) has been published by a Dutch ministry, noting that Microsoft still has work to do if the country's institutions are to use the company's products without all manner of mitigations."

Source: https://www.theregister.com/2022/02/23/dpia_microsoft/

Horde Webmail Software is affected by a dangerous bug since 2012

From the article: "Experts found a nine-year-old unpatched flaw in the Horde Webmail software that could allow access to email accounts."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://securityaffairs.co/wordpress/128314/hacking/horde-webmail-xss.html

Malware authors target rivals with malicious npm packages

From the article: "Trojan packages reveal what could be internal rivalry between cybercriminals."

Source: https://www.zdnet.com/article/malware-authors-target-rivals-with-malicious-npm-packages/

These new hacking groups are striking industrial, operational tech targets

From the article: "Two of the new groups are sophisticated enough to reach ICS/OT networks directly."

Source: https://www.zdnet.com/article/these-new-hacking-groups-are-striking-industrial-operational-tech-targets/

Microsoft changes default settings to improve network security

From the article: "Microsoft changes default settings for a variety of reasons, but some recent key changes will keep us safer from attacks, specifically ransomware."

Source: https://www.csoonline.com/article/3650670/microsoft-changes-default-settings-to-improve-network-security.html

Sophisticated Phishing Tactic Circumvents MFA Using Remote Access Software

From the article: "According to a new phishing tactic, adversaries can defeat multi-factor authentication (MFA) by having victims connect to their accounts directly on attacker-controlled servers using the VNC screen sharing system."

Source: https://cyberintelmag.com/attacks-data-breaches/sophisticated-phishing-tactic-

circumvents-mfa-using-remote-access-software/

Extensis Portfolio Contains Multiple Vulnerabilities, Including Zero-Day RCE

From the article: "On February 17, White Oak Security researchers Michael Rand and Talis Ozols publicly reported that Extensis Portfolio has serious vulnerabilities, including an unpatched zero-day bug."

Source: https://cyberintelmag.com/cloud-security/extensis-portfolio-contains-multiple-vulnerabilities-including-zero-day-rce/

Cisco warns firewall customers of four-day window for urgent updates

From the article: "Cisco has warned users of its Firepower firewalls – physical and virtual – that they may need to upgrade their kit within a four-day window or miss out on security intelligence updates."

Source:
https://www.theregister.com/2022/02/23/cisco_firepower_rapid_update_required/

Iranian Broadcaster IRIB hit by wiper malware

From the article: "An investigation into the attack that hit the Islamic Republic of Iran Broadcasting (IRIB) in late January, revealed the involvement of a disruptive wiper malware along with other custom-made backdoors, and scripts and configuration files used to install and configure the malicious executables."

Source: https://securityaffairs.co/wordpress/128309/hacking/irib-hit-by-wiper-malware.html

Addressing Library Characterization And Verification Challenges Using ML

From the article: "At advanced process nodes, Liberty or library (.lib) requirements are

more demanding due to design complexities, increased number of corners required for timing signoff, and the need for statistical variation modeling."

Source: https://semiengineering.com/addressing-library-characterization-and-verification-challenges-using-ml-2/

Transistors Reach Tipping Point At 3nm

From the article: "The semiconductor industry is making its first major change in a new transistor type in more than a decade, moving toward a next-generation structure called gate-all-around (GAA) FETs."

Source: https://semiengineering.com/transistors-reach-tipping-point-at-3nm/

Achieving C-V2X Compliance

From the article: "Testing the performance of cellular vehicle-to-everything (C-V2X) components and subsystems to achieve compliance against evolving 5G test requirements is an ongoing challenge for the connected vehicle market."

Source: https://semiengineering.com/achieving-c-v2x-compliance/

Fuzz Testing Software-Defined Vehicles Using Agent Instrumentation

From the article: "Cybersecurity has become intertwined into each step of the automotive development process. In particular, fuzz testing has proven to be a powerful approach to detect unknown vulnerabilities in automotive systems."

Source: https://semiengineering.com/fuzz-testing-software-defined-vehicles-using-agent-instrumentation/

RF To mmWave Design For Systems

Link back to Table of Contents

From the article: "RF-enabled next-generation communication systems and connected devices are differentiated by their performance, size, and cost. "

Source: https://semiengineering.com/rf-to-mmwave-design-for-systems/

Image Processing For Vision AI

From the article: "DRP-AI is an AI accelerator highly rated for its superior power efficiency, providing optimal image processing for Vision AI. RZ/V2M is equipped with a dedicated hardware ISP (Image Signal Processor) which is tuned to match the unique characteristics of the Renesas-selected CMOS sensor."

Source: https://semiengineering.com/image-processing-for-vision-ai/

Blog Review: Feb. 23

From the article: "Synopsys' Varun Agrawal looks at four new technologies have emerged to support the demands on 5G networks and applications, the challenges in validating all of those technologies together, and what's needed to perform end-to-end testing effectively for 5G O-RAN SoCs."

Source: https://semiengineering.com/blog-review-feb-23/

China's APT10 cyber-spies 'targeted Taiwanese financial firms'

From the article: "China's state-sponsored snoops conducted a two-month campaign against Taiwanese financial services firms, according to CyCraft, a security consultancy from the island nation.…"

Source:
https://www.theregister.com/2022/02/23/apt10_operation_cache_panda_taiwan/

Samsung shipped '100 million' phones with flawed encryption

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the article: "Academics at Tel Aviv University in Israel have found that recent Android-based Samsung phones shipped with design flaws that allow the extraction of secret cryptographic keys.…"

Source: https://www.theregister.com/2022/02/23/samsung_encryption_phones/

Teenage cybercrime: How to stop kids from taking the wrong path

From the article: "It's never too late to prevent children from being dragged to the dark side and to ensure their skills are a force for good."

Source: https://www.welivesecurity.com/2022/02/22/teenage-cybercrime-stop-kids-wrong-path/

Log4j Remediation Took Weeks or More for Over 50% of Organizations

From the article: "(ISC)² survey also found that half of cybersecurity teams worldwide worked on fixing Log4j issues on weekends and during time off."

Source: https://www.darkreading.com/attacks-breaches/log4j-remediation-took-weeks-or-more-for-more-than-50-of-organizations

Hikvision Network Cyber-Protect Helps Ensure Physical Cybersecurity Protection

From the article: "Combines technology, education and tools to help dealers protect networked security systems."

Source: https://www.darkreading.com/physical-security/hikvision-network-cyber-protect-helps-ensure-physical-cybersecurity-protection

Palo Alto Networks Introduces the Autonomous Security Platform, Cortex XSIAM

Link back to Table of Contents

From the article: "The new AI-driven platform brings threat response times from days to minutes and provides a modern alternative to SIEM. Cortex XSIAM is currently available to a limited set of customers with general availability expected later this year."

Source: https://www.darkreading.com/operations/palo-alto-networks-introduces-the-autonomous-security-platform-cortex-xsiam

GitHub Opens Security Database to Community Contributions

From the article: "The Microsoft company will allow community members to add information and code samples to security advisories using the standard pull request to change the document."

Source: https://www.darkreading.com/application-security/github-opens-security-database-to-community-contributions

Network hackers focus on selling high-value targets in the U.S.

From the article: "A Crowdstrike report looking into access brokers' advertisements since 2019 has identified a preference in academic, government, and technology entities based in the United States."

Source: https://www.bleepingcomputer.com/news/security/network-hackers-focus-on-selling-high-value-targets-in-the-us/

Entropy ransomware linked to Dridex malware downloader

From the article: "Analysis of the recently-emerged Entropy ransomware reveals code-level similarities with the general purpose Dridex malware that started as a banking trojan."

Source: https://www.bleepingcomputer.com/news/security/entropy-ransomware-linked-to-dridex-malware-downloader/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Apple's Tracking-Protection Mechanisms Surpassed by AirTag Clone

From the article: "With a custom-made AirTag clone, a security researcher claims to have defeated the tracking protection mechanisms embedded into Apple's Find My app and AirTag tracking devices."

Source: https://cyberintelmag.com/iot/apples-tracking-protection-mechanisms-surpassed-by-airtag-clone/

Darktrace Acquires Attack Surface Management Company Cybersprint

From the article: "Through this acquisition, Darktrace gains a second European R&D centre in The Hague, Netherlands."

Source: https://www.darkreading.com/threat-intelligence/darktrace-acquires-attack-surface-management-company-cybersprint

Cloud Storage Leaks Grew by 150% in 2021, New CybelAngel Report Reveals

From the article: "An increase in outsourced development projects also led to a 66% increase in source code leaks."

Source: https://www.darkreading.com/cloud/cloud-storage-leaks-grew-by-150-in-2021-new-cybelangel-report-reveals

NetSPI Launches New Attack Surface Management Platform

From the article: "The offering leverages innovative technology and expert pentesters to help organizations discover and secure all assets on the external attack surface."

Source: https://www.darkreading.com/vulnerabilities-threats/netspi-launches-new-attack-surface-management-platform

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Sophos linked Entropy ransomware to Dridex malware. Are both linked to Evil Corp?

From the article: "The code of the recently-emerged Entropy ransomware has similarities with the one of the infamous Dridex malware."

Source: https://securityaffairs.co/wordpress/128323/cyber-crime/entropy-ransomware-dridex-link.html

Ransomware Resilience Tops Findings in X-Force Threat Intelligence Index 2022

From the article: "For the third year in a row, ransomware was the top attack type globally in 2021, despite some successes last year by law enforcement to take down ransomware groups."

Source: https://securityintelligence.com/posts/2022-x-force-threat-intelligence-index-ransomware-resilience-tops-findings/

Increasing Number of Threat Groups Targeting OT Systems in North America

From the article: "An increasing number of threat groups have been targeting organizations with industrial control system (ICS) or other operational technology (OT) environments, according to a new report from industrial cybersecurity company Dragos."

Source: https://www.securityweek.com/increasing-number-threat-groups-targeting-ot-systems-north-america

Counterfeit parts found in U.S. nuclear plants -inspector general

From the article: "Counterfeit parts have been discovered in U.S. nuclear plants, potentially increasing the risk of a safety failure, the inspector general of the federal nuclear industry regulator said in a report released on Thursday."

Source: https://www.reuters.com/business/energy/counterfeit-parts-present-many-us-nuclear-power-plants-inspector-general-2022-02-10/

Link back to Table of Contents

Technology, Progress, and Climate

From the article: "The climate solutions we need to transform every sector are here. The question is: what role will you play in this transformation? You, your community, your business, your government?"

Source: https://www.welivesecurity.com/2022/02/23/technology-progress-climate/

CISA adds two Zabbix flaws to its Known Exploited Vulnerabilities Catalog

From the article: "US CISA added two flaws impacting Zabbix infrastructure monitoring tool to its Known Exploited Vulnerabilities Catalog."

Source: https://securityaffairs.co/wordpress/128374/hacking/cisa-zabbix-flaws.html

The Harsh Truths of Cybersecurity in 2022, Part II

From the article: "Sonya Duffin, ransomware and data-protection expert at Veritas Technologies, shares three steps organizations can take today to reduce cyberattack fallout."

Source: https://threatpost.com/harsh-truths-cybersecurity-part-two/178447/

Insider Threats Are More Than Just Malicious Employees

From the article: "Humans are unpredictable and may make mistakes that could result in a security incident."

Source: https://www.darkreading.com/dr-tech/insider-threats-are-more-than-just-malicious-employees

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

How to improve threat detection in ICS environments

From the article: "A challenge in industrial control systems (ICS) cybersecurity is the lack of detection and collection capability within most ICS environments. Security leaders can struggle to piece together the complete attack chain in actual ICS incidents because the environments cannot collect the required evidence."

Source: https://www.cyberscoop.com/how-to-improve-threat-detection-in-ics-environments/

Why Developers Should Care About Log4j

From the article: "Unless you can gain full visibility into how data flows to and through your dependencies, you can't be sure if you are affected by this vulnerability."

Source: https://www.darkreading.com/edge-articles/why-developers-should-care-about-log4j

Zenly Social-Media App Bugs Allow Account Takeover

From the article: "A pair of bugs in the Snap-owned tracking app reveal phone numbers and allow account hijacking."

Source: https://threatpost.com/zenly-bugs-account-takeover/178646/

Ransomware is top attack vector on critical infrastructure

From the article: "Ransomware was the number one attack vector on critical infrastructure in 2021, according to a report by Dragos, a leading company in industrial cybersecurity."

Source: https://www.csoonline.com/article/3651370/ransomware-is-top-attack-vector-on-critical-infrastructure.html

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

4 Simple Steps to a Modernized Threat Intelligence Approach

From the article: "As cybersecurity strategies continuously evolve to keep pace with attackers, the relevance of the traditional model is in need of an automation upgrade."

Source: https://www.darkreading.com/threat-intelligence/4-simple-steps-to-a-modernized-threat-intelligence-approach

Microsoft App Store Sizzling with New 'Electron Bot' Malware

From the article: "The SEO poisoning bot, capable of full system takeover, is actively taking over social media accounts, masquerading as popular games like Temple Run."

Source: https://threatpost.com/microsoft-app-store-electron-bot-malware/178629/

Wireless Logic Extends International Reach With Major US Partnerships

From the article: "Wireless Logic announces new partnerships that enable customers to localize through major cellular networks in the US."

Source: https://www.iotforall.com/press-releases/wireless-logic-us-partnership-announcement

Businesses Are at Significant Risk of Cybersecurity Breaches Due to Immature Security Hygiene and Posture Management Practices

From the article: "Seven out of 10 organizations experienced a cyberattack that started through the exploit of unknown or poorly managed technology assets, according to Enterprise Strategy Group research."

Source: https://www.darkreading.com/risk/businesses-are-at-significant-risk-of-cybersecurity-breaches-due-to-immature-security-hygiene-and-posture-management-practices

Link back to Table of Contents

Defense contractors hit by stealthy SockDetour Windows backdoor

From the article: "A new custom malware dubbed SockDetour found on systems belonging to US defense contractors has been used as a backup backdoor to maintain access to compromised networks."

Source: https://www.bleepingcomputer.com/news/security/defense-contractors-hit-by-stealthy-sockdetour-windows-backdoor/

Web Filtering and Compliances for Wi-Fi Providers

From the article: "Demand for public Wi-Fi is on the rise. Usually free of charge, but there is a risk of expensive losses. Learn ways to protect yourself from cyber-threats."

Source: https://threatpost.com/web-filtering-and-compliances-for-wi-fi-providers/178532/

How Computer Vision is Powering Marketing Strategies in 2022

From the article: "Computer vision is helping brands transform and improve their marketing practices by providing a more personalized brand experience to the consumers, ensuring they will come back again."

Source: https://www.iotforall.com/?p=160804

3 Steps Security Leaders Can Take Toward Closing the Skills Gap

From the article: "Much has been written about the Great Resignation as its impact is widespread. Sectors including hospitality, food, retail, manufacturing and healthcare have all been affected, making access to goods and services we took for granted hard to come by."

Source: https://www.securityweek.com/3-steps-security-leaders-can-take-toward-closing-skills-gap

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

JupiterOne Unveils Starbase for Graph-Based Security

From the article: "The open source asset management tool lets security analysts collect asset information all across the organization's digital operations and run queries to understand their relationships."

Source: https://www.darkreading.com/dr-tech/jupiterone-unveils-starbase-for-graph-based-security

Cyberattackers Leverage DocuSign to Steal Microsoft Outlook Logins

From the article: "A targeted phishing attack takes aim at a major U.S. payments company."

Source: https://threatpost.com/cyberattackers-docusign-steal-microsoft-outlook-logins/178613/

SaaS in the Enterprise: The Good, the Bad, and the Unknown

From the article: "SaaS offers many benefits to the enterprise, but security issues left unchecked can mitigate value."

Source: https://www.darkreading.com/cloud/saas-in-the-enterprise-the-good-the-bad-and-the-unknown

Entropy ransomware linked to Evil Corp's Dridex malware

From the article: "Analysis of the recently-emerged Entropy ransomware reveals code-level similarities with the general purpose Dridex malware that started as a banking trojan."

Source: https://www.bleepingcomputer.com/news/security/entropy-ransomware-linked-to-evil-corps-dridex-malware/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

The Art of Non-boring Cybersec Training–Podcast

From the article: "With human error being the common factor in most cyberattacks, employee training has got to get better. To that end, Trustwave cybersec training expert Darren Van Booven explains the importance of fish stress balls and management buy-in."

Source: https://threatpost.com/the-art-of-non-boring-cybersec-training-podcast/178594/

Citibank phishing baits customers with fake suspension alerts

From the article: "An ongoing large-scale phishing campaign is targeting customers of Citibank, requesting recipients to disclose sensitive personal details to lift alleged account holds."

Source: https://www.bleepingcomputer.com/news/security/citibank-phishing-baits-customers-with-fake-suspension-alerts/

How Smart Restrooms Help Buildings Adapt to Pandemic Disruptions

From the article: "Smart restroom technology is helping building managers keep up with the higher demands for cleanliness in response to the pandemic."

Source: https://www.iotforall.com/?p=162454

An Elaborate Employment Con in the Internet Age

From the article: "Gemma Brett, a 27-year-old designer from west London, had only been working at Madbird for two weeks when she spotted something strange."

Source: https://www.schneier.com/blog/archives/2022/02/an-elaborate-employment-con-in-the-internet-age.html

Link back to Table of Contents

Salesforce Paid Out $12.2 Million in Bug Bounty Rewards to Date

From the article: "Customer relationship management services provider Salesforce says it has handed out more than $12.2 million in payouts to the ethical hackers who reported vulnerabilities as part of its bug bounty program."

Source: https://www.securityweek.com/salesforce-paid-out-122-million-bug-bounty-rewards-date

Extortion Through Ransomware Does Not End When Ransom is Paid

From the article: "The lack of trustworthiness of ransomware operators was highlighted in a global study of ransomware victims."

Source: https://cyberintelmag.com/attacks-data-breaches/extortion-through-ransomware-does-not-end-when-ransom-is-paid/

CISA Announces Attacks Abusing Recent Flaws in Zabbix Monitoring Tool

From the article: "The US Cybersecurity and Infrastructure Security Agency (CISA) included two severe flaws of the Zabbix corporate monitoring tool to its Known Exploited Vulnerabilities Catalog."

Source: https://cyberintelmag.com/attacks-data-breaches/cisa-announces-attacks-abusing-recent-flaws-in-zabbix-monitoring-tool/

CISOs, beware of spyware tools for illicit competitive intelligence

From the article: "The U.S. Department of Justice (DOJ) released information surrounding the guilty plea of Mexican businessman Carlos Guerrero and his conspiracy to sell and use hacking tools that were manufactured by companies in Italy, Israel, and elsewhere."

Source: https://www.csoonline.com/article/3650537/cisos-beware-of-spyware-tools-for-illicit-competitive-intelligence.html

Link back to Table of Contents

The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Data Center Architectures In Flux

From the article: "Data center architectures are becoming increasingly customized and heterogeneous, shifting from processors made by a single vendor to a mix of processors and accelerators made by multiple vendors — including system companies' own design teams."

Source: https://semiengineering.com/data-center-architectures-in-flux/

Why RISC-V Is Succeeding

From the article: "There is no disputing the excitement surround the introduction of the RISC-V processor architecture. Yet while many have called it a harbinger of a much broader open-source hardware movement, the reasons behind its success are not obvious, and the implications for an expansion of more open-source cores is far from certain."

Source: https://semiengineering.com/why-risc-v-is-succeeding/

Unintended Coupling Issues Grow

From the article: "The number of indirect and often unexpected ways in which one design element may be affected by another is growing, making it more difficult to ensure a chip — or multiple chips in a package — will perform reliably."

Source: https://semiengineering.com/unintended-coupling-issues-grow/

Does EDA Sell Fear?

From the article: "I worked in the EDA industry for over 30 years and a common lament I heard was that the EDA industry survived by selling fear. Your new chip will fail if you do not buy the latest tool offering."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://semiengineering.com/does-eda-sell-fear/

Dissolving The Barriers In Multi-Substrate 3D-IC Assembly Design

From the article: "Advanced packaging continues to promise improved form factor, cost, performance, and functionality compared to the traditional transistor scaling on SoCs."

Source: https://semiengineering.com/dissolving-the-barriers-in-multi-substrate-3d-ic-assembly-design/

Are Sustainability And Safety Gen Z's Top Requirements In 2031?

From the article: "For this anniversary, I am looking forward ten years to 2031 and how generational changes of the end customer base may or may not impact requirements in electronics and its enabling ecosystems to which electronic design automation (EDA) and computational software belong."

Source: https://semiengineering.com/are-sustainability-and-safety-gen-zs-top-requirements-in-2031/

Intelligent Waveform Replay For Efficient Debug

From the article: "There is no doubt that design reuse is essential for today's massive system on chip (SoC) projects. No team, no matter how large or how talented, can design billions of gates from scratch for each new chip."

Source: https://semiengineering.com/intelligent-waveform-replay-for-efficient-debug/

How To Extend The 'Unscalable' RISC Architectures

From the article: "A couple of years ago, Erik McClure (a Microsoft software developer, at the time) published a blog entitled RISC Is Fundamentally Unscalable. "

Link back to Table of Contents

Source: https://codasip.com/2022/02/18/how-to-extend-the-unscalable-risc-architectures/

US winds up national security team dedicated to Chinese espionage

From the article: "The United States' National Security Division will wind up its "China Initiative" – an effort to combat what then-attorney general Jeff Sessions described in 2018 as "systematic and calculated threats" posed by Beijing-backed economic espionage."

Source: https://www.theregister.com/2022/02/24/us_china_initiative_ended/

Malware infiltrates Microsoft Store via clones of popular games

From the article: "A malware named Electron Bot has found its way into Microsoft's Official Store through clones of popular games such as Subway Surfer and Temple Run, leading to the infection of 5,000 computers in Sweden, Israel, Spain, and Bermuda."

Source: https://www.bleepingcomputer.com/news/security/malware-infiltrates-microsoft-store-via-clones-of-popular-games/

Additional sources:
https://cyberintelmag.com/malware-viruses/malware-penetrates-microsoft-store-through-famous-game-clones/

GPU giant Nvidia is investigating a potential cyberattack

From the article: "US chipmaker giant Nvidia confirmed today it's currently investigating an "incident" that reportedly took down some of its systems for two days."

Source: https://www.bleepingcomputer.com/news/security/gpu-giant-nvidia-is-investigating-a-potential-cyberattack/

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

NHS urges orgs to apply security update for Okta Client RCE bug

From the article: "The UK's NHS Digital agency is warning organizations to apply new security updates for a remote code execution vulnerability in the Windows client for the Okta Advanced Server Access authentication management platform."

Source: https://www.bleepingcomputer.com/news/security/nhs-urges-orgs-to-apply-security-update-for-okta-client-rce-bug/

6 Cyber-Defense Steps to Take Now to Protect Your Company

From the article: "Ransomware is getting worse, but Daniel Spicer, chief security officer at Ivanti, offers a checklist for choosing defense solutions to meet the challenge."

Source: https://threatpost.com/latest-insights-ransomware-threats/178391/

Visual Voice Mail on Android may be vulnerable to eavesdropping

From the article: "A security analyst has devised a way to capture Visual Voice Mail (VVM) credentials on Android devices and then remotely listen to voicemail messages without the victim's knowledge."

Source: https://www.bleepingcomputer.com/news/security/visual-voice-mail-on-android-may-be-vulnerable-to-eavesdropping/

Mandiant adds ransomware defense validation to XDR security platform

From the article: "Cyberdefense and response company Mandiant is offering a new Ransomware Defense Validation service for its SaaS-based XDR (extended detection and response) platform, Mandiant Advantage, to help organizations measure the ability of their security systems to prevent ransomware attacks."

Source: https://www.csoonline.com/article/3651510/mandiant-adds-ransomware-defense-validation-to-xdr-security-platform.html

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Much-Anticipated Crypto Unlock For Nvidia Graphic Cards Installs Malware

From the article: "Faced with high demand from cryptocurrency miners, scalpers, and even regular individuals looking to play video games, Nvidia introduced the “Lite Hash Rate” limiter, which artificially restricts the amount of Ethereum that can be mined on recently released GeForce RTX 30-series graphics cards."

Source: https://cyberintelmag.com/malware-viruses/much-anticipated-crypto-unlock-for-nvidia-graphic-cards-installs-malware/

Top 5 Interview Questions to Ask DevOps Candidates in 2022

From the article: "It's worthwhile to find candidates who have experience with models that embed security into their processes."

Source: https://www.darkreading.com/edge-articles/top-5-interview-questions-to-ask-devops-candidates-in-2022

Jester Stealer malware adds more capabilities to entice hackers

From the article: "An infostealing piece of malware called Jester Stealer has been gaining popularity in the underground cybercrime community for its functionality and affordable prices."

Source: https://www.bleepingcomputer.com/news/security/jester-stealer-malware-adds-more-capabilities-to-entice-hackers/

Six Benefits of an Effective Cloud Migration Strategy for Your Business

From the article: "Businesses need data to compete with the market. Nowadays, more businesses are shifting to the cloud, but it is not as easy as you think. Learn the essentials here and know what benefits you will get if you shift to a cloud data warehouse."

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Source: https://www.iotforall.com/?p=160865

The Future of Cyber Insurance

From the article: "Having cyber insurance is a good idea if the costs make sense — it could be the difference between going out of business and staying afloat. But it shouldn't be your first course of action."

Source: https://www.darkreading.com/risk/the-future-of-cyber-insurance

Putting the X Factor in XDR

From the article: "While extended detection and response (XDR) is effectively considered an upgrade from endpoint detection and response, enterprises must still begin with a strong EDR foundation."

Source: https://www.darkreading.com/crowdstrike/putting-the-x-factor-in-xdr

Why Are Pharmacies Deploying IoT Cold Chain Monitoring Solutions?

From the article: "IoT cold chain monitoring will allow the automation of sensors used to track the condition of perishable items while in transport."

Source: https://www.iotforall.com/?p=162444

Microsoft: January Windows Server updates cause Netlogon issues

From the article: "Microsoft says Windows Server security updates released on and since the January 2022 Patch Tuesday might prevent applications and network appliances from creating Netlogon secure channels if installed on domain controllers."

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-january-windows-

server-updates-cause-netlogon-issues/

Privacy Violating COVID Tests

From the article: "Cignpost Diagnostics, which trades as ExpressTest and offers £35 tests for holidaymakers, said it holds the right to analyse samples from seals to “learn more about human health” — and sell information on to third parties."

Source: https://www.schneier.com/blog/archives/2022/02/privacy-violating-covid-tests.html

US defense contractors hit by stealthy SockDetour Windows backdoor

From the article: "A new custom malware dubbed SockDetour found on systems belonging to US defense contractors has been used as a backup backdoor to maintain access to compromised networks."

Source: https://www.bleepingcomputer.com/news/security/us-defense-contractors-hit-by-stealthy-sockdetour-windows-backdoor/

Microsoft: Resetting Windows devices might not wipe all data

From the article: "Microsoft says Windows customers might find that some of their files are not deleted after resetting their Windows devices with the "Remove everything" option."

Source: https://www.bleepingcomputer.com/news/microsoft/microsoft-resetting-windows-devices-might-not-wipe-all-data/

CISA warns of actively exploited vulnerabilities in Zabbix servers

From the article: "A notification from the U.S. Cybersecurity Infrastructure and Security

Agency (CISA) warns that threat actors are exploiting vulnerabilities in the Zabbix open-source tool for monitoring networks, servers, virtual machines, and cloud services."

Source: https://www.bleepingcomputer.com/news/security/cisa-warns-of-actively-exploited-vulnerabilities-in-zabbix-servers/

KORE, Kigen & Energy Web Collaborate To Provide eSIM Based Trusted Identity System for Smart Grid

From the article: "KORE, Kigen and Energy Web collaborate for an integrated, eSIM-based, trusted identity system for smart grid applications."

Source: https://www.iotforall.com/?post_type=press-releases&p=165851

UK Computer Misuse Act reformers visit Parliament

From the article: "Infosec researcher Rob Dyke, best known to Reg readers for fending off legal threats from not-for-profit open-source foundation Apperta after finding a data breach, has visited Parliament to demand Computer Misuse Act reform."

Source: https://www.theregister.com/2022/02/25/cyberup_parliament_rob_dyke/

Conti Ransomware Attack on Ireland's Healthcare Sector Expected to Cost More Than $100 Million

From the article: "According to an Irish news outlet report, the country's healthcare sector would have to pay more than $48 million to recover from last year's massive ransomware attack by the Conti gang."

Source: https://cyberintelmag.com/attacks-data-breaches/conti-ransomware-attack-on-irelands-healthcare-sector-expected-to-cost-more-than-100-million/

GE SCADA Product Vulnerabilities Show Importance of Secure Configurations

Link back to Table of Contents

From the article: "GE Digital has released patches and mitigations for two high-severity vulnerabilities affecting its Proficy CIMPLICITY HMI/SCADA software, which is used by plants around the world to monitor and control operations."

Source: https://www.securityweek.com/ge-scada-product-vulnerabilities-show-importance-secure-configurations

Unit 42: SockDetour Backdoor Employed in Cyberattacks Against Defense Firms

From the article: “One of the command and control (C2) infrastructures that the threat actor used for malware distribution for the TiltedTemple campaign hosted SockDetour along with other miscellaneous tools such as a memory dumping tool and several webshells."

Source: https://cyberintelmag.com/attacks-data-breaches/unit-42-sockdetour-backdoor-employed-in-cyberattacks-against-defense-firms/

Nvidia probes cyberattack on internal systems

From the article: "In brief Nvidia is probing what may be a ransomware infection that caused outages within its internal network.…"

Source: https://www.theregister.com/2022/02/26/in_brief_security/

Subscription

Japan's inflation spreads to tuna and beef bowls, slamming households

From the article: “Having suffered from decades of deflation, Japan is now seeing price hikes spread to a range of items, from electricity to mayonnaise, squeezing household budgets by raising costs for basic necessities and services.”

Source: https://asia.nikkei.com/Economy/Japan-s-inflation-spreads-to-tuna-and-beef-

Link back to Table of Contents

bowls-slamming-households

Anticipating retaliation, Japan scrambles to review Russian imports

From the article: "From chipmaking materials to energy, Japan this month launched efforts to identify critical imports from Russia and make contingency plans for potential disruptions to its supply chains as Moscow is expected to halt shipments in retaliation against economic sanctions."

Source: https://asia.nikkei.com/Politics/Ukraine-conflict/Anticipating-retaliation-Japan-scrambles-to-review-Russian-imports

BYD zooms past Tesla in China's electric-car market

From the article: "Chinese automaker BYD sold more electric and hybrid vehicles in China last year than Tesla, new industry figures show, with a surge of growth that puts it on track to doubling sales in 2022."

Source: https://asia.nikkei.com/Spotlight/Electric-cars-in-China/BYD-zooms-past-Tesla-in-China-s-electric-car-market

Global chip shortage may soon turn into an oversupply crisis

From the article: "From supply chain bottlenecks to rising inflation, an important question for all stakeholders is whether we are going to see an end to the chip shortage crisis. While the limited supply of chips has resulted in higher prices for consumers, other repercussions include the disruption of industrial activities and supply chain security."

Source: https://asia.nikkei.com/Opinion/Global-chip-shortage-may-soon-turn-into-an-oversupply-crisis

Taiwan's UMC to build $5bn chip plant in Singapore

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

From the article: "Taiwan's United Microelectronics Corp. on Thursday announced plans to spend $5 billion to expand its chip production capacity in Singapore as the world's fourth largest contract chipmaker looks to help clients overcome the ongoing global chip crunch."

Source: https://asia.nikkei.com/Business/Tech/Semiconductors/Taiwan-s-UMC-to-build-5bn-chip-plant-in-Singapore

China's Oppo aims to double high-end phone sales despite chip crunch

From the article: "Chinese smartphone maker Oppo plans to double its shipments of high-end devices this year despite chip shortages as the company seeks to expand in Europe and the Americas, an executive told Nikkei Asia."

Source: https://asia.nikkei.com/Business/Technology/China-s-Oppo-aims-to-double-high-end-phone-sales-despite-chip-crunch

Toshiba, Rohm pursue power chip tech to cut energy loss in half

From the article: "Japanese manufacturers Toshiba, Denso and Rohm have begun developing power chip technology that will cut electricity loss in half, seeking to put the products on the market by the end of the decade."

Source: https://asia.nikkei.com/Business/Tech/Semiconductors/Toshiba-Rohm-pursue-power-chip-tech-to-cut-energy-loss-in-half

G-7 leaders condemn Ukraine invasion and announce Russia sanctions

From the article: "Leaders from the Group of Seven advanced economies held an emergency virtual meeting Thursday, agreeing to bring forward "severe and coordinated economic and financial sanctions" against Russia over its invasion of Ukraine."

Source: https://asia.nikkei.com/Politics/Ukraine-conflict/G-7-leaders-condemn-Ukraine-invasion-and-announce-Russia-sanctions

Link back to Table of Contents
The articles have been curated by an independent team of subject matter experts to raise awareness of contemporary cyber-physical security issues with systems, software and hardware assurance.

Turkey car sales drop as inflation puts them out of reach for many

From the article: "Turkey's soaring prices are putting the brakes on domestic car sales. Unit sales of new autos fell in 2021 versus the previous year, while output declined for the fourth year in a row."

Source: https://asia.nikkei.com/Business/Automobiles/Turkey-car-sales-drop-as-inflation-puts-them-out-of-reach-for-many

Ukraine conflict puts chipmakers on alert over supply of key gases

From the article: "Top chipmakers in Taiwan and South Korea are closely reviewing their stockpiles of critical industrial gases after Russia's invasion of Ukraine sparked fears of supply disruption that could exacerbate a global chip shortage."

Source: https://asia.nikkei.com/Business/Tech/Semiconductors/Ukraine-conflict-puts-chipmakers-on-alert-over-supply-of-key-gases

Suzuki, Japan Tobacco caught up in Ukraine's economic shutdown

From the article: "The advance of Russian troops and fighting through Ukraine has prompted Suzuki Motor, Japan Tobacco and other global multinationals to halt operations inside the country to ensure the safety of workers."

Source: https://asia.nikkei.com/Politics/Ukraine-conflict/Suzuki-Japan-Tobacco-caught-up-in-Ukraine-s-economic-shutdown

The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict

From the article: “As warnings of an imminent Russian attack on Ukraine proliferate, news networks and social media have featured clips of Russian armed forces training, exercising, and preparing to fight. Less visible are Russia’s formidable cyber forces that would be preparing to unleash a new wave of cyber-attacks on Ukrainian and western

energy, finance, and communications infrastructure. ”

Source: https://hbr.org/2022/02/the-cybersecurity-risks-of-an-escalating-russia-ukraine-conflict

Toyota to halt operations at all Japan plants due to cyberattack

From the article: “Toyota Motor announced Monday that it will halt operations at all of its plants in Japan on Tuesday, as a major supplier was hit by a suspected cyberattack. The decision to suspend 28 lines at 14 plants came after the supplier was hit by the attack, bringing a parts supply management system to a halt.”

Source:https://asia.nikkei.com/Business/Automobiles/Toyota-to-halt-operations-at-all-Japan-plants-due-to-cyberattack

U.S. Banks Are Prepared for Russia Sanctions, but Concerns Grow About Potential Hacks

From the article: “U.S. financial institutions are largely prepared to handle a new round of Russia-related sanctions in the wake of the invasion of Ukraine, given the steady ratcheting up of pressure against Russia over the past eight years and recent warnings of such measures from the Biden administration, according to experts with knowledge of the U.S. banking sector.”

Source: https://www.wsj.com/articles/u-s-banks-are-prepared-for-russia-sanctions-but-concerns-grow-about-potential-hacks-11645743246

Will war in Ukraine lead to a wider cyber-conflict?

From the article: “Russian missiles slammed into Kyiv on the morning of February 24th. But its computer networks were already long under attack. On February 23rd, as the country was still bracing for an invasion that was expected to be imminent, the websites of Ukraine’s parliament and several government agencies were put out of action. A similar digital assault on Ukrainian government websites and banks on February 15th and 16th was quickly attributed by America, Britain and other governments to the gru, Russia’s military-intelligence agency. Last month the websites of several government

ministries were defaced with the message, “Be afraid and expect the worst.””

Source:
https://amp.economist.com/europe/2022/02/23/will-war-in-ukraine-lead-to-a-wider-cyber-conflict

NIST’s Stine says ‘CSF 2.0’ process will ‘maximize’ engagement with array of stakeholders, align with other initiatives

From the article: “The National Institute of Standards and Technology has launched its “CSF 2.0” process to update the cybersecurity framework and is planning for “a tremendous amount of stakeholder engagement” in the coming months, according to NIST’s Kevin Stine, who said the effort will be complementary to ongoing work on the 2021 cyber executive order and other initiatives.”

Source: https://insidecybersecurity.com/share/13225

Link back to Table of Contents