SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

24 APRIL – 19 JUNE 2021

TOPICAL REPORT

CYBERSECURITY

Gain insight and keep up-to-date with the latest publications carefully selected by the library from credible sources in academic publications, industry & market research and scientific & industry news.
If you have any sources to suggest for our report please let us know.

view past reports | subscribe to others | unsubscribe

news

CYBERSECURITY

University of Massachusetts Lowell cancels classes after possible 'cybersecurity incident'

"The University of Massachusetts Lowell canceled all in-person and online classes for the second day following a "cybersecurity incident," the school said.
The public research university has been keeping staff and students updated on the breach on the temporary website UMassLowell.com while the school's main website remains unavailable.
Officials reported the incident Tuesday and said in an online statement that the university, including its Haverhill campus, was closed "due to an IT outage.""
Source: NBC News

The 10 Hottest Cybersecurity Startups Of 2021

"These companies are solving security challenges such as thwarting vulnerabilities early in the development life cycle, protecting SaaS applications regardless of device or location, and managing and securing identities, access and privileges. Here's a look at how the 10 coolest cybersecurity startups have made themselves relevant to partners and customers alike."
Source: CRN

academic

CYBERSECURITY

Cybersecurity Standards in the Context of Operating System: Practical Aspects, Analysis, and Comparisons

"This article presents a detailed literature review, a comprehensive analysis of various cybersecurity standards, and statistics of cyber-attacks related to operating systems (OS). In addition to that, an explicit comparison between the frameworks, tools, and software available for OS compliance testing is provided. An in-depth analysis of the most common software solutions ensuring compliance with certain cybersecurity standards is also presented. Finally, based on the cybersecurity standards under consideration, a comprehensive set of minimum requirements is proposed for OS hardening and a few open research challenges are discussed."
Source: ACM Digital Library

Exploration and Exploitation in Organizational Cybersecurity

"This study examines the cybersecurity responses by organizations to threats. Based on the notions of exploration and exploitation, this study developed a 2 × 2 matrix to characterize organizational actions as Surviving, Investigating, Reinforcing, and Balancing. Using textual data

reports

INDUSTRY REPORT

Why May 2021 Represents a New Chapter in the "Book of Cybersecurity Secrets"

"May 2021 has been an extraordinary month in the cybersecurity world, with the DoD releasing its DoD Zero Trust Reference Architecture (DoDZTRA), the Colonial Pipeline being hit with a ransomware attack, and the White House releasing its Executive Order on Improving the Nation's Cybersecurity (EO). Add to that several major vendors that our government depends on for its critical operations disclosing critical vulnerabilities that could potentially expose our nation's critical infrastructure to even more risk, ranging from compromised email and cloud infrastructures to very sophisticated supply chain attacks like the SolarWinds hack, which could have started as early as 2019."
Source: McAfee

Top Cybersecurity Trends For 2021 and Beyond

"This article provides an overview of the cybersecurity landscape and how it was dramatically shifted due to the COVID-19 pandemic. In addition, it provides a look into the future with the top 10 cybersecurity trends and predictions for 2021 and beyond. The pandemic response caused massive disruptions to the way we live, work, and conduct business. Organizations

New cyber-security and information centre to be set up in S'pore for Asean defence exchanges

"The establishment of the centre was approved at the 15th Asean Defence Ministers' Meeting (ADMM) held virtually on Tuesday (June 15), said the Ministry of Defence.

In its statement, Mindef said the centre will complement the Asean Cyber Defence Network in promoting regional exchanges, interactions and cooperation on cyber-security matters."

Source: Straits Times

The Hottest Cybersecurity Must-Reads for the Busy Security Practitioner

"You're busy. We get that. Let's suppose you're like most of your colleagues in security. In that case, it's almost like Groundhog Day. It starts with chasing the latest threat and protecting your company or agency from attacks. It ends with you wondering where the last eight (or more) hours went. This leaves you little time to do what you really want to do — transform your work into an enabler of growth and innovation. Take a breath. We can help."

Source: Security Intelligence

How Japan Has Prepared For Cybersecurity Threats At The Tokyo 2020

"Japan has faced multiple cyberattacks and threats — the most recent, according to UK National Cyber Security Centre, was an alledged threat from the Russian military during the preparations of Tokyo 2020 Olympics, where journalists, foreign officials, spectators and athletes would add to the 117 million active internet users in Japan."

Source: Forbes

The Changing Trends In Cyber Security

"According to figures released in 2020 by the Department for Digital, Culture, Media and Sport, the UK's cyber security industry is worth £8.3bn. However, the picture isn't as cohesive as you might assume – different areas of the cyber security industry are growing at varying rates and world events continue to shape developing trends.

We've seen, and will continue to see, UK businesses digitising their processes, including the transfer, storage and processing of important data and communication. But we're also seeing more frequent and sophisticated cyber-attacks on enterprise systems. The UK IT security sector is continuing to reshape itself to

gathered from the annual 10–K reports of 87 organizations, this study mapped the explorative and exploitative behaviors of organizations and characterized the cybersecurity responses with the 2 × 2 matrix. This study also identified the changes in cybersecurity responses over multiple time periods, and the patterns of shifts between the quadrants in the 2 × 2 matrix as organizations adapted their cybersecurity responses over time. Several implications for research and practice are discussed."

Source: Taylor & Francis

Leveraging human factors in cybersecurity: an integrated methodological approach

"This paper presents a holistic/Human Factors (HF) approach, where the individual, organisational and technological factors are investigated in pilot healthcare organisations to show how HF vulnerabilities may impact on cybersecurity risks. An overview of current challenges in relation to cybersecurity is first provided, followed by the presentation of an integrated top–down and bottom–up methodology using qualitative and quantitative research methods to assess the level of maturity of the pilot organisations with respect to their capability to face and tackle cyber threats and attacks. This approach adopts a user-centred perspective, involving both the organisations' management and employees, The results show that a better cyber-security culture does not always correspond with more rule compliant behaviour."

Source: Springer Link

Analysis of Cybersecurity-related Incidents in the Process Industry

"The aim of the study is to frame a clear picture of the cyber-attacks on the automated control systems of process facilities and to issue lessons learnt from past incidents. The study is based on the development and analysis of a database of 82 cybersecurity-related incidents gathered from various sources. Time trend, geographical distribution, distribution among the industrial sectors, impacts of the incidents, and nature of the cyber-attacks (attacker, intentional/accidental type, system infected) were investigated. The analysis of a sub-set of more detailed incidents allowed the identification of the general steps of a cyber-attack on automated control systems of a process facility, the main hacking techniques used by the attackers and the more common cybersecurity

rapidly shifted to online operations and remote working to maintain normalcy during the pandemic. These transitions will continue into post-pandemic and beyond as the new normal. Cybercriminals have responded and will use this opportunity to launch a new breed of cyber attacks in 2021. The article outlines the top cybersecurity concerns for 2021 and beyond."

Source: Centre for Homeland Defense and Security

Cybersecurity Services Global Market Report 2021: COVID 19 Growth And Change to 2030

"The global cybersecurity services market is expected grow from $65.41 billion in 2020 to $69.12 billion in 2021 at a compound annual growth rate (CAGR) of 5.7%. The growth is mainly due to the companies resuming their operations and adapting to the new normal while recovering from the COVID-19 impact, which had earlier led to restrictive containment measures involving social distancing, remote working, and the closure of commercial activities that resulted in operational challenges. The market is expected to reach $103.89 billion in 2025 at a CAGR of 11%."

Source: GlobeNewsWire

Frost Radar™: Global Critical Infrastructure Cyber Security Market, 2021

"During the last decade, critical infrastructure organizations (those whose operations are vital to sustaining citizens' lives or national security) have undergone two major transformations: first, the introduction of digital technologies and systems to enable more efficient operations, and second, an exponential rise in their overall risk profile as an attack target for cyber criminals.

The COVID-19 pandemic has presented a pivotal opportunity for critical infrastructure organizations to build out their cyber security operations due to the massive need to enable and safeguard remote access to their facilities and devices, especially during national lockdown or when operating with a reduced staff, and ensure no significant operational downtime occurs."

Source: Frost & Sullivan

Frost Radar™: Security Awareness Training Market

"Companies are facing a substantial threat from social engineering attacks such as phishing, especially because remote working is on the rise due to the COVID-19 pandemic. As a result, businesses of all sizes are realizing the importance of training non-technical employees to become the first line of

meet these evolving threats and the changing demands of organisations. Here are five trends to watch in this space"
Source: Information Security Buzz

CYBER ATTACKS

PNNL's Shadow Figment Technology Foils Cyberattacks

"Scientists have created a cybersecurity technology called Shadow Figment that is designed to lure hackers into an artificial world, then stop them from doing damage by feeding them illusory tidbits of success.
The aim is to sequester bad actors by captivating them with an attractive—but imaginary—world."
Source: Pacific Northwest National Laboratory

Two new attacks break PDF certification

"The World Robotics report shows that Europe is the region with the highest robot density globally, with an average value of 114 units per 10,000 employees in the manufacturing industry. For more facts about robots watch IFR´s video news about Europe in one minute."
Source: RUHR Universitat Bochum

Age of the cyber-attack: US struggles to curb rise of digital destabilization

"Many of the recent attacks have been sourced to operations in Russia and US officials say that Russia's responsibility for ransomware attacks carried out from its territory would be a central issue when Joe Biden meets Vladimir Putin in Geneva next Wednesday.
"One of the things that President Biden will make clear to President Putin, when he sees him, is that states cannot be in the business of harboring those who are engaged in these kinds of attacks," the secretary of state, Tony Blinken, told Congress this week."
Source: The Guardian

Hackers Breached Colonial Pipeline Using Compromised Password

"The hack that took down the largest fuel pipeline in the U.S. and led to shortages across the East Coast was the result of a single compromised password, according to a cybersecurity consultant who responded to the attack.

countermeasures applicable to the prevention of a cyber-attack."
Source: Elsevier

Cybersecurity and Business Continuity in Pandemic Times

"This document is framed in the context of the ongoing research project entitled "Design of a cyber resilience mechanism for business continuity in organizations", having as an objective to present the context of cybersecurity in this time of pandemic, where cybercrime seeks new ways to attack organizations and individuals. Cybersecurity strategies must be adapted to the situational context. Organizational resilience is also present in organizations to ensure business continuity, where the continuity plans of organizations are considering the pandemic as a scenario of disruption that has compromised the internal or external activities of companies."
Source: Annals of the Romanian Society for Cell Biology

Quantifying the Tradeoff Between Cybersecurity and Location Privacy

"This paper tackles this dilemma situation by evaluating the tradeoff between location privacy and security. Specifically, vehicle trips are obfuscated with 2D Laplace noise that meets the requirement of differential privacy. The obfuscated vehicle trips are then fed into a benchmark Recurrent Neural Network (RNN) that is widely used for detecting anomalous trips. This allows us to investigate the influence of the privacy-preservation technique on model performance. The experiment results suggest that applying Laplace mechanism to achieve high-level of differential privacy in the context of location-based vehicle trips will result in low true-positive or high false-negative rate by the RNN, which is reflected in the area under the curve scores (less than 0.7), which diminishes the value of RNN as more anomalous trips will be classified as normal ones."
Source: Cornell University

Training and Embedding Cybersecurity Guardians in Older Communities.

"Older adults can struggle to access relevant community expertise when faced with new situations. One such situation is the number of cyberattacks they may face when interacting online. This paper reports on an initiative which recruited, trained, and supported older adults to become community cybersecurity educators (CyberGuardians), tasked with promoting cybersecurity best practice within their communities to prevent older adults falling victim to

defense for their organizations. The best technological solutions cannot prevent an attack when employees are not aware of security best practices.
The Frost Radar™ reveals the market positioning of companies in the Global Security Awareness Training market using their Growth and Innovation scores as highlighted in the Frost Radar methodology."
Source: Frost & Sullivan

RESEARCH

Check Point Research: Asia Pacific experiencing a 168% year on year increase in cyberattacks in May 2021

"In recent months, the Asia Pacific (APAC) region has seen an increase in the number of cyberattacks. Most recently in Japan, Omiai, the country's most popular dating app, experienced a server hack which exposed the data of over 1.7 million people, including images of driving licenses and passports users submitted to verify their age. Over in India, the data of customers of Domino's India have been found on the Darknet following a cyberattack which exposed the data of 180 million users earlier this year.
Check Point Research (CPR) noticed this trend of cyberattacks happening in the region, and decided to investigate"
Source: CheckPoint

Hackers gained entry into the networks of Colonial Pipeline Co. on April 29 through a virtual private network account, which allowed employees to remotely access the company's computer network, said Charles Carmakal, senior vice president at cybersecurity firm Mandiant, part of FireEye Inc., in an interview. The account was no longer in use at the time of the attack but could still be used to access Colonial's network, he said."
Source: Bloomberg

Biden tells Putin certain cyberattacks should be 'off-limits'

"Biden said the list of organisations that should not be attacked includes the 16 sectors designated by the United States as critical infrastructure. The sectors, based on a description published by the US Homeland Security Department, include telecommunications, healthcare, food and energy.
"We agreed to task experts in both our countries to work on specific understandings about what is off-limits," Biden said. "We'll find out whether we have a cybersecurity arrangement that begins to bring some order.""
Source: Channel News Asia

Cyber Attacks On The Rise

"Cyber attacks are making headlines both nationally and here in the Commonwealth. Last week the Massachusetts Steamship Authority was the target of a cyber attack that brought down its website, causing ferry delays, and today The University of Massachusetts Lowell is canceling its classes while the university investigates a possible cyber security breach. Joining us to discuss how cyber attacks are impacting the Commonwealth is Hiawatha Bray, a technology columnist for The Boston Globe."
Source: WBUR

RISK MANAGEMENT

Reduce the noise to strengthen agency cybersecurity defenses

"Technology advances have given cyber criminals and hostile nation-states more tools to breach networks and gain access to sensitive data, relegating standard perimeter security tools and firewalls to mere first-layer status. Attacks are growing increasingly sophisticated, more devastating and much harder to opportunistic cyberattacks. This initiative utilised an embedded peer-to-peer information dissemination strategy, rather than expert-to-citizen, facilitating the inclusion of individuals who would ordinarily be unlikely to seek cybersecurity information and thus may be vulnerable to cyberattacks."
Source: ACM Digital Library

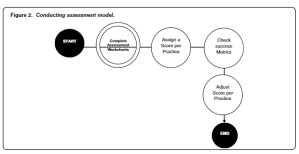
Participatory Threat Modelling: Exploring Paths to Reconfigure Cybersecurity

"We present "participatory threat modelling" as a feminist cybersecurity practice which allows technology research to centre traditionally marginalized and excluded experiences. We facilitated a series of community workshops in which we invited participants to define their own cybersecurity threats, implement changes to defend themselves, and reflect on the role cybersecurity plays in their lives. In doing so, we contest both hierarchical approaches to users in cybersecurity—which seek to 'solve' the problems of human behavior—and a tendency in HCI to equate action research with the development of novel technology solutions."
Source: ACM Digital Library

The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions

"This paper presents an empirical study of the social and cultural aspects of cybersecurity capacity building in 78 nations. While nations within geographically defined regions might be expected to share similar attitudes, values, and practices around cybersecurity, this analysis finds that regional differences can be explained largely by cross-national differences in development and the scale of Internet use. These results question the centrality of regions in shaping social and cultural attributes directly tied to cybersecurity capacity. However, the analysis identifies some countries with greater and some with lesser levels of maturity in capacity building than expected only on the basis of their development and scale of Internet use."
Source: Springer Link

CYBERSECURITY GOVERNANCE



identify and mitigate, especially in vast government agency networks with countless points of entry. Even with aggressive defenses, network perimeter breaches are inevitable."
Source: GCN

Algorithms improve how we protect our data

"Daegu Gyeongbuk Institute of Science and Technology (DGIST) scientists in Korea have developed algorithms that more efficiently measure how difficult it would be for an attacker to guess secret keys for cryptographic systems. The approach they used was described in the journal IEEE Transactions on Information Forensics and Security and could reduce the computational complexity needed to validate encryption security."
Source: Daegu Geongbuk Institute of Science and Technology

Defenseless: UVA Engineering Computer Scientists Discover Vulnerability Affecting Computers Globally

"Researchers named the vulnerability SPECTRE because the flaw was built into modern computer processors that get their speed from a technique called "speculative execution," in which the processor predicts instructions it might end up executing and preps by following the predicted path to pull the instructions from memory. A Spectre attack tricks the processor into executing instructions along the wrong path. Even though the processor recovers and correctly completes its task, hackers can access confidential data while the processor is heading the wrong way."
Source: University of Virginia

Columbia Engineering team builds first hacker-resistant cloud software system

"Columbia Engineering researchers may have solved this security issue. They have developed SeKVM, the first system that guarantees--through a mathematical proof--the security of virtual machines in the cloud. In a new paper to be presented on May 26, 2021, at the 42nd IEEE Symposium on Security & Privacy, the researchers hope to lay the foundation for future innovations in system software verification, leading to a new generation of cyber-resilient system software."
Source: EurekAlert!

Microsoft launches first Asia Pacific Public Sector Cyber Security Executive Council across seven markets in the region

A Maturity Framework For Cybersecurity Governance In Organizations

"Digitalization necessarily leads organizations to rethink their cybersecurity principles in order to counter all the risks inherent in cybercrime. Cybersecurity governance brings together all the essential elements of cyber defense and effective risk management... The aim of this paper is to propose a capability maturity framework to assess and improve cybersecurity governance in organizations. The finding will help organizations to evaluate their cybersecurity governance capabilities."
Source: Taylor & Francis

A Conceptual Model for Cybersecurity Governance

"Cybersecurity is a growing problem associated with everything an individual or an organization does that is facilitated by the Internet. It is a multi-facetted program that can be addressed by cybersecurity governance. However, research has shown that many organizations face at least five basic challenges of cybersecurity. In this study, we developed a model for an effective cybersecurity governance that hopes to address these challenges, conceptualized as factors that must continuously be measured and evaluated. They are: (1) Cybersecurity strategy; (2) Standardized processes, (3) Compliance, (4) Senior leadership oversight, and (5) Resources."
Source: Taylor & Francis

Business, Organisational and governance modalities of collaborative cybersecurity networks

"Starting in the beginning of the centuy, the creation of collaborative networked organisations in other fields demonstrated significant benefits in sharing knowledge, resources, and risk to exploit quickly emerging market opportunities. The major challenge in creating networked organisations is to provide long-term, effective collaboration through adequate governance and management. To support the elaboration of a solid governance model of a cybersecurity competence network in a Horizon 2020 research project, this article presents the results of a study of 92 existing network organisations working in cybersecurity and closely related fields. It presents the implemented methodological approach, the identification of main types of business models depending on funding streams and the degree of

"Cybercrime is globally disruptive and economically damaging, causing trillions of dollars in financial losses and operational impacts to individual and business victims. It threatens national security and diminishes trust in the digital economy and the Internet. Additionally, APAC continues to experience a higher-than-average encounter rate for malware and ransomware attacks – 1.6 and 1.7 times higher respectively than the rest of the world."
Source: Microsoft

From Boardroom To Service Floor: How To Make Cybersecurity An Organizational Priority Now

"The costs and consequences of a data breach or cybersecurity incident have never been more severe. According to the FBI's recently released Internet Crime Report 2020, cybercrime resulted in $4 billion in losses last year, a low estimate that still encapsulates the incredible value lost to threats actors. For small businesses, the costs can be catastrophic. As Vox reports, 60% of small businesses will close after a data breach, underscoring the high-stakes bottom-line nature of cybersecurity."
Source: Forbes

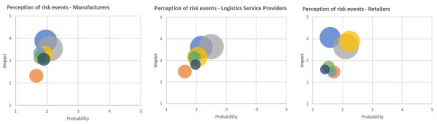
Smarter and safer cities with effective cybersecurity measures

"THE promise of smart cities is clear: a more liveable space for citizens which in turn, fosters a better environment for businesses to flourish and grow, leading to greater economic growth. Governments in South-east Asia have been building up critical infrastructure and rolling out technologies to support their vision of smart cities. Indeed, Singapore is one of the strongest advocates for smart cities, and has been key in proposing the establishment of the Asean Smart Cities Network."
Source: The Business Times

Improving the State of OT Cybersecurity by Sharing Experiences

"The need for significant improvement in the state of OT cybersecurity in critical infrastructures has been broadly acknowledged for almost two decades. Although the subject started to receive significant attention in the early 2000s, the reality is that the protection of operations systems from threats to their integrity and availability has been a concern of asset owners for much longer than that. While the threats and vulnerability components of the risk equation were traditionally physical and safety-related, increased coordination among partners, organisational modalities, and prevailing governance models depending on member representation on senior governance bodies."
Source: Springer Link

RISK MANAGEMENT



Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era

"The purpose of this paper is to explore the perceptions of supply chain managers regarding the elements that make up cyber supply chain risk management (CSCRM) and the related level of alignment, to understand how organizations can deploy a CSCRM strategy that goes beyond the technical, internal functioning of single companies and moves beyond the dyad, to create a better alignment that can ultimately lead to improved cyber supply chain resilience."
Source: Emerald Insight

Centralised IT Structure and Cyber Risk Management

"Against the backdrop of organisational needs to derive value from IT Organisations through agility, efficiencies and cost effectiveness, many organisations have adopted a decentralised IT organisational structure, enabling individual business units the autonomy to implement, operate and govern technology. The increase risk that poses organisations through cyber-attacks, raises the question of how IT security could effectively provide the level of organisations governance to counter cyber threats in a decentralised organisational model. In exploring the challenges in the decentralization of IT security, we highlighted that the accountability of such activities would become diluted, with each business unit managing security in their own methods and practices or lack of, while unable to take full accountability due to the complex independencies of modern system architectures, often resulting in a lack of ownership, accountability and reporting of security at an organisational group level."
Source: Springer Link

CYBER RESILIENCE

network connectivity and the broader use of commercial off-the-shelf (COTS) computer and communications technology inevitably led to increased scrutiny of cybersecurity risks."
Source: ARC Advisory Group

Bank of America spends over $1 billion per year on cybersecurity, CEO Brian Moynihan says

"A series of sweeping cyberattacks have struck private companies and federal government networks over the past year. Two of the most recent were on Colonial Pipeline — the operator of the country's largest fuel pipeline — and JBS, the world's largest meatpacking company.
This has led firms and governments to reassess and modernize their cybersecurity defenses, as these attacks have become a source of economic damage."
Source: CNBC

Small Business Cybersecurity 101: Simple Tips To Protect Your Data

"Smaller organizations are often prime targets for cyberattacks because they aren't protected by the same level of security infrastructure as larger companies — yet they still have valuable data to offer. According to research from the 2020 Verizon Data Breach Investigations Report, 28% of data breach victims were small businesses."
Source: Forbes

Three ways to keep up with cybersecurity demands

"Many organizations are finding it harder to manage the increasing pace and sophistication of security threats these days. But the right technologies and strategies can help, according to security experts who shared their tips at a recent ITWC briefing.
"We're seeing a lot of transformation as organizations adopt more cloud and with people working from home," said Chris Ruetz, AVP and Country Manager at CyberArk. "The complete landscape of cybersecurity has transformed dramatically for a lot of organizations."
Source: IT World

CYBER RESILIENCE

Cyber Resilience and Its Importance for Your Business

"Cybercrimes are rapidly growing both in complexity and frequency. To

Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs

"To aid SMEs in their cyber resilience operationalization, the current literature offers several kinds of solutions, but these solutions are usually targeted for companies with more resources than SMEs and do not aid in the complete process of assessing their current cyber resilience, deciding actions to improve it and prioritizing these actions. To aid companies in this systematic process to operationalize or implement cyber resilience, this article develops and tests an operational web-based tool in which companies can follow the complete process described before. To achieve this, a cyber resilience framework with the essential policies for SMEs, descriptions of their natural progressions in a progression model and a prioritization of these policies have been developed. In this article, this framework, progression model and prioritization are later transformed into one cyber resilience self-assessment tool (CR-SAT) and are tested in three case studies to qualitatively evaluate the tool by trying to ascertain its usefulness and completeness as well as improving it with the feedback from the end-users."
Source: IEEE Xplore

CyRes: towards operational cyber resilience

"Existing approaches to cyber security in the automotive sector are not fit to deliver the resilience required for safe mass deployment of advanced driving functions and intelligent mobility services. This paper promotes an innovative approach to operational cyber resilience, the CyRes methodology, which aims to enable robust and resilient engineering practices in this sector from design to manufacture to operation. CyRes is based on three principles: engineered differences; detecting, understanding and acting on cyber events; and proactive updates. The aim of this short paper is to raise awareness of the problems and the many intellectual challenges in this particular sector."
Source: ACM Digital Library

Cyber resilience during the COVID-19 pandemic crisis: A case study

"The outbreak of the COVID-19 pandemic crisis around the world and the resulting unprecedented

stay competitive in such an unpredictable environment, the security of your organization's data, applications, network and critical business processes should be your top priority. Traditional security solutions and methodologies are no longer enough to combat today's sophisticated cybercrimes. Your business must have a robust cybersecurity resilience strategy in place that will enable you to maintain business continuity before, during and after a cybersecurity incident."
Source: Business to Community

Cyber Resilience Initiative: Monetary Authority of Singapore

"Cyber attacks have become a significant threat to financial stability over the last decade, and the Covid-19 crisis has only heightened the importance of protecting the digital systems of financial services firms. The Monetary Authority of Singapore (MAS) has been a leader in regulatory and supervisory approaches to reducing cyber risks. "We have observed an uptick in Covid-19 themed cyber attacks and scams, where cyber criminals capitalised on the Covid-19 situation," says Vincent Loy."
Source: Central Banking

10 Essential Steps to Cyber Resilience as Hackers Target Critical Infrastructure

"A motivated hacker will break into a system they target. No doubt, no question. Perhaps you have heard that stated less assertively, but the sentiment is the same. Hackers come in all experience levels and sizes, from individual actors to full nation-state forces. Some cybercriminals depend on teams, bots, harvested intelligence, brute force, and relentless targeting. Sometimes, an attacker is fortunate to encounter just dumb luck. Regardless of the skill level or support, a motivated hacker will ultimately succeed in compromising a set of their targets."
Source: Homeland Security Today US

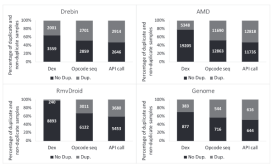
MALWARE

Ransomware is the biggest threat, says GCHQ cybersecurity chief

"The head of the UK's National Cyber Security Centre has warned that ransomware has become the biggest threat to British people and businesses.

measures taken by governments required organizations to quickly adopt new ways of (remotely) working... Three findings stand out. First, the interviews suggest that the organization performed cyber resiliently in the sense that the number of incidents and impact were not significantly higher. Second, the interviews show that all four abilities of resilience were formally developed prior to the COVID-19 outbreak, but rarely resulted in anticipatory adjustment. Third, the interviews indicate that the ability to respond contributed most to the organization's cyber resilience during the pandemic crisis. To conclude, our research note raises the question to what extent the four potentials should be developed beforehand in order to perform resiliently during crises."
Source: Wiley Online Library

MALWARE



On the Impact of Sample Duplication in Machine-Learning-Based Android Malware Detection

"Malware detection at scale in the Android realm is often carried out using machine learning techniques. State-of-the-art approaches such as DREBIN and MaMaDroid are reported to yield high detection rates when assessed against well-known datasets. Unfortunately, such datasets may include a large portion of duplicated samples, which may bias recorded experimental results and insights. In this article, we perform extensive experiments to measure the performance gap that occurs when datasets are de-duplicated. Our experimental results reveal that duplication in published datasets has a limited impact on supervised malware classification models. This observation contrasts with the finding of Allamanis on the general case of machine learning bias for big code."
Source: ACM Digital Library

Initial growth rates of malware epidemics fail to predict their reach

"Empirical studies show that epidemiological models based on an epidemic's initial spread rate often fail to predict the true scale of that epidemic. Most epidemics with a rapid early rise die out before affecting a significant fraction of the population, whereas the early pace of some pandemics is rather modest. Recent models suggest that this could

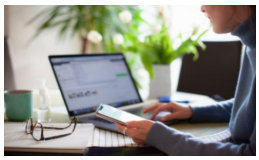
In a speech being given today by Lindy Cameron, chief executive of the NCSC, to the RUSI think tank, she highlights the need for ransomware problem to be taken seriously, and warns of the "cumulative effect" if society fails to properly deal with the rising threat."
Source: Tripwire

PHISHING

Why a Phishing Attack Is Still Profitable — And How To Stop One

"In May 2020, X-Force research uncovered a precision-targeting (or spear phishing) attack on a German multinational corporation connected with a German government-private sector task force in the race to procure personal protective equipment (PPE).
Those threat actors targeted more than one hundred high-ranking executives in management and procurement roles. They reached out within their target group as well as to its third-party partners."
Source: Security Intelligence

REMOTE WORKING



How Cybersecurity Habits Of Returning Remote Workers Can Put Companies At Risk

"The millions of employees who have worked remotely because of Covid and are now returning to the office on a full-time or hybrid-basis could also bring their bad cybersecurity habits, putting companies at greater risk for cyber-related crisis situations."
Source: Forbes

TELECOMMUNICATION

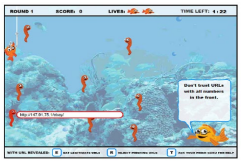
A backdoor in mobile phone encryption from the 90s still exists

"The encryption algorithm GEA-1 was implemented in mobile phones in the 1990s to encrypt data connections. Since then, it has been kept secret. Now, a research team from Ruhr-Universität Bochum (RUB), together be due to the heterogeneity of the target population's susceptibility. We study a computer malware ecosystem exhibiting spread mechanisms resembling those of biological systems while offering details unavailable for human epidemics. Rather than comparing models, we directly estimate reach from a new and vastly more complete data from a parallel domain, that offers superior details and insight as concerns biological outbreaks."
Source: Nature Scientific Reports

Analyzing Machine Learning Approaches for Online Malware Detection in Cloud

"The variety of services and functionality offered by various cloud service providers (CSP) have exploded lately. Utilizing such services has created numerous opportunities for enterprises infrastructure to become cloud-based and, in turn, assisted the enterprises to easily and flexibly offer services to their customers. The practice of renting out access to servers to clients for computing and storage purposes is known as Infrastructure as a Service (IaaS). The popularity of IaaS has led to serious and critical concerns with respect to the cyber security and privacy. In particular, malware is often leveraged by malicious entities against cloud services to compromise sensitive data or to obstruct their functionality. In response to this growing menace, malware detection for cloud environments has become a widely researched topic with numerous methods being proposed and deployed. In this paper, we present online malware detection based on process level performance metrics, and analyze the effectiveness of different baseline machine learning models including, Support Vector Classifier (SVC), Random Forest Classifier (RFC), KNearest Neighbor (KNN), Gradient Boosted Classifier (GBC), Gaussian Naive Bayes (GNB) and Convolutional Neural Networks (CNN)."
Source: Cornell University

CYBERSECURITY AWARENESS



A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education

"We conduct a comprehensive review covering academic

with colleagues from France and Norway, has analysed the algorithm and has come to the following conclusion: GEA-1 is so easy to break that it must be a deliberately weak encryption that was built in as a backdoor. Although the vulnerability is still present in many modern mobile phones, it no longer poses any significant threat to users, according to the researchers."
Source: EurekAlert!

Quantum holds the key to secure conference calls

"The world is one step closer to ultimately secure conference calls, thanks to a collaboration between Quantum Communications Hub researchers and their German colleagues, enabling a quantum-secure conversation to take place between four parties simultaneously.
The demonstration, led by Hub researchers based at Heriot-Watt University and published in Science Advances, is a timely advance, given the global reliance on remote collaborative working, including conference calls, since the start of the C19 pandemic."
Source: EurekAlert!

CLOUD SECURITY

What are cloud security frameworks and how are they useful?

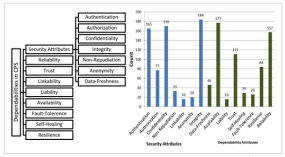
"Ask any security practitioner and they'll say securing cloud environments is challenging for a number of reasons, of which three particularly stand out: First, because of the increased complexity they add to environments. Second, because of their reliance on service providers without direct visibility into day-to-day security operations. Third, due to adoption dynamics that favor rapid and sometimes unplanned incorporation."
Source: Tech Target

NIST Releases New Language To Automate Cloud Security

"A new framework developed by NIST could greatly improve the ability to quickly assess compliance and security in cloud environments, including those used by the Defense Department's JEDI, as well as those used by the Intelligence Community and the defense industrial base.
NIST released the first version of the Open Security Controls Assessment Language (OSCAL) on Thursday."
Source: Breaking Defense

publications and industry products relating to tools for cybersecurity awareness and education aimed at non-expert end-users developed in the past 20 years. Through our search criteria, we identified 119 tools that we cataloged into five broad media categories. We explore current trends, assess their use of relevant instructional design principles, and review empirical evidence of the tools' effectiveness. From our review, we provide an evaluation checklist and suggest that a more systematic approach to the design and evaluation of cybersecurity educational tools would be beneficial."
Source: ACM Digital Library

CYBER PHYSICAL SYSTEMS



Security risks in cyber physical systems—A systematic mapping study

"The increased need for constant connectivity and complete automation of existing systems fuels the popularity of Cyber Physical Systems (CPS) worldwide... Our work aims to form an overview of the security requirements and risks in CPS today and of those published contributions that have been made until now, towards improving the reliability of CPS. The results of this mapping study reveal (i) integrity authentication and confidentiality as the most targeted security attributes in CPS, (ii) model-based techniques as the most used risk identification and assessment and management techniques in CPS, (iii) cyber-security as the most common security risk in CPS, (iv) the notion of "mitigation measures" based on the type of system and the underline internationally recognized standard being the most used risk mitigation technique in CPS, (v) smart grids being the most targeted systems by cyber-attacks and thus being the most explored domain in CPS literature, and (vi) one of the major limitations, according to the selected literature, concerns the use of the fault trees for fault representation, where there is a possibility of runtime system faults not being accounted for."
Source: Wiley Online Library

Understanding the Cyber-Physical System in International Stadiums for Security in the Network from

Cloud-Skilled Cyber Professionals Needed to Secure Organizations Globally

"Cloud security is critically important for organizations across the globe as adoption of cloud infrastructure continues to grow at a rapid clip. The shift toward the cloud is unstoppable, and inevitably, it's driving soaring demand for skilled security professionals. If you want to be at the forefront of this cloud security wave in infosec, GIAC has the cloud security credentials you and your team need for every critical cloud skill set."

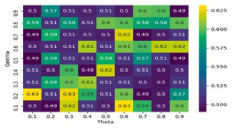
Source: PRN Newswire

Cyber-Attacks and Adversaries using AI

"There is a high demand for advanced stadium security systems because of the large number of sporting events organized. Hence, in this study, an Artificial intelligence assisted Cyber-Physical System (AI-CPS) has been proposed for security in the network to predict cyber attacks and adversaries. The data has been collected and analyzed, and the proposed AI-CPS model predicts anomaly behaviour in the network. This study deals with the subject of how surveillance and security practices at sports events are organized. Advances in Artificial Intelligence (AI) techniques show potential in enabling cybersecurity authorities to counter the ever-evolving attack posed by an adversary. Here, this paper explores AI's potential in enhancing cybersecurity resolutions by determining both its strengths and weaknesses."

Source: Springer Link

ARTIFICIAL INTELLIGENCE



Adversarial attacks on machine learning cybersecurity defences in Industrial Control Systems

"This paper explores how adversarial learning can be used to target supervised models by generating adversarial samples using the Jacobian-based Saliency Map attack and exploring classification behaviours. The analysis also includes the exploration of how such samples can support the robustness of supervised models using adversarial training. An authentic power system dataset was used to support the experiments presented herein. Overall, the classification performance of two widely used classifiers, Random Forest and J48, decreased by 6 and 11 percentage points when adversarial samples were present. Their performances improved following adversarial training, demonstrating their robustness towards such attacks."

Source: Elsevier

Convergence of 5G Technologies, Artificial Intelligence and Cybersecurity of Networked Societies for the Cities of Tomorrow

"To overcome the aforementioned challenges of emerging issues for networks of future, this special issue

focuses on (but are not restricted to) the following topics: Advanced network architecture design for IoT towards 5G; IoT applications to disaster management, smart cities, smart environment, and smart agriculture; Energy-efficiency in 5G for IoT applications; 5G wireless heterogeneous networks: design and optimization; Mobility management of 5G networks for IoT applications; 5G wireless communications and networks for surveillance and management; 5G technologies: NOMA, full-duplex, massive MIMO, network planning, mmWave, URLLC; Big data and IoT data analytics; Security and privacy concerns in 5G wireless communications; Hardware forensics; Deep learning for hardware oriented cybersecurity; Machine learning for resource allocation in wireless networks; Emerging memory and computing technologies for future networks; and Advanced signal processing for future networks."
Source: Springer Link

Enhancing Cybersecurity via Artificial Intelligence: Risks, Rewards, and Frameworks

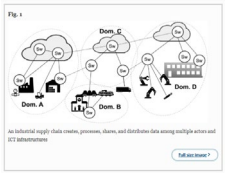
"Recent advances in artificial intelligence challenge classical models of productivity by increasing the scale, complexity, and range of tasks that can be meaningfully automated, including those associated with cybersecurity."
Source: IEEE Xplore

Machine Learning-Based Intrusion Detection for Achieving Cybersecurity in Smart Grids Using IEC 61850 GOOSE Messages

"Increased connectivity is required to implement novel coordination and control schemes. IEC 61850-based communication solutions have become popular due to many reasons—object-oriented modeling capability, interoperable connectivity and strong communication protocols, to name a few. However, communication infrastructure is not well-equipped with cybersecurity mechanisms for secure operation. Unlike online banking systems that have been running such security systems for decades, smart grid cybersecurity is an emerging field. To achieve security at all levels, operational technology-based security is also needed. To address this need, this paper develops an intrusion detection system for smart grids utilizing IEC 61850's Generic Object-Oriented Substation Event (GOOSE) messages. The system is developed with machine learning and is able to monitor the communication traffic of

a given power system and distinguish normal events from abnormal ones, i.e., attacks."
Source: MDPI

DIGITAL ECONOMY



An Autonomous Cybersecurity Framework for Next-generation Digital Service Chains

"Today, the digital economy is pushing new business models, based on the creation of value chains for data processing, through the interconnection of processes, products, services, software, and things across different domains and organizations… In order to fill this gap, this work proposes a new methodological approach to design and implement heterogeneous security services for distributed systems that combine together digital resources and components from multiple domains."
Source: Springer Link

HEALTHCARE

Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review

"The aim of this review was to identify key cybersecurity challenges, solutions adapted by the health sector, and areas of improvement needed to counteract the recent increases in cyberattacks (eg, phishing campaigns and ransomware attacks), which have been used by attackers to exploit vulnerabilities in technology and people introduced through changes to working practices in response to the COVID-19 pandemic… This scoping review identified the most impactful methods of cyberattacks that targeted the health sector during the COVID-19 pandemic, as well as the challenges in cybersecurity, solutions, and areas in need of improvement. We provided useful insights to the health sector on cybersecurity issues during the COVID-19 pandemic as well as other epidemics or pandemics that may materialize in the future."
Source: JMIR Publications