SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

15 August - 23 October 2020

TOPICAL REPORT

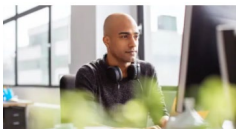
CYBERSECURITY

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 | academic | reports

CYBERSECURITY



How Cybersecurity Threat Intelligence Teams Spot Attacks Before They Start

"When intelligence on threat groups is used to defend clients' networks and drive research, that acts as a force multiplier for organizations, strengthening their security posture with each new insight acquired."
Source: Security Intelligence

Working from home? Slow broadband, remote security remain top issues

"According to Navisite, more than a third (36%) of respondents said they were unprepared for the shift to remote work. And the rush to workers outside the office at unprecedented levels likely resulted in IT teams skipping over normal security protocols."
Source: Computer World

The Important Difference Between Cybersecurity And Cyber Resilience (And Why You Need Both)

"In a nutshell, cybersecurity describes a company's ability to protect against and avoid the increasing threat from cybercrime. Meanwhile, cyber resilience refers to a company's ability to mitigate damage (damage to systems, processes, and reputation),

CYBERSECURITY RISK

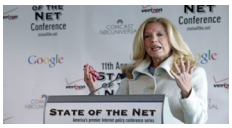
Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management

"We present a decision-analysis-based approach that quantifies threat, vulnerability, and consequences through a set of criteria designed to assess the overall utility of cybersecurity management alternatives. The proposed framework bridges the gap between risk assessment and risk management, allowing an analyst to ensure a structured and transparent process of selecting risk management alternatives. The use of this technique is illustrated for a hypothetical, but realistic, case study exemplifying the process of evaluating and ranking five cybersecurity enhancement strategies."
Source: Wiley Online Library

Public companies' cybersecurity risk disclosures

"Though cybersecurity risks are significant and could materially affect business operations and the integrity of financial reporting, there is limited empirical research on the cybersecurity risk disclosure trends and practices of public companies. In this study, we conduct a longitudinal study of the content and linguistic characteristics of public companies' cybersecurity risk disclosure practices

CYBERSPACE SOLARIUM WHITE PAPER



Cyberspace Solarium Commission White Paper #4: Building a Trusted ICT Supply Chain

"Dependency on China and other adversary countries for some of our most critical supply chains threatens to undermine the trustworthiness of critical technologies and components that constitute and connect to cyberspace. This dependency also risks impairing the availability of these same critical technologies and components and compromises American and partner competitiveness in global markets in the face of Chinese economic aggression.
To address these challenges, the Commission proposes a five-pillar strategy built on the firm foundation of public-private and international partnerships."
Source: Solarium

INSIGHT

State of Cybersecurity Report 2020:

"In the Accenture Third Annual State of Cyber Resilience report we take a deep dive into what sets leaders

and carry on once systems or data have been compromised."
Source: Forbes

CYBER ATTACKS

Office 365: A Treasure Trove for Cybercriminals

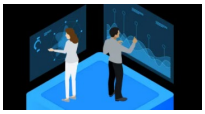
"Office 365 has more than 250 million monthly active users, making it an attractive target for cybercriminals. Recently, a report Vectra revealed that cybercriminals are frequently abusing built-in Office 365 services to launch cyberattacks on enterprises."
Source: Cyware

MOBILE SECURITY

URL address spoofing flaw keeps mobile victims from determining fake, real sites

"If left unpatched, mobile browsers could direct to a fraudulent website where attackers steal account credentials and credit card information."
Source: SC Magazine

CLOUD SECURITY



Modernizing Your Security Operations Center for the Cloud

"Several factors are converging to exert pressure on how security operations centers (SOCs) traditionally function. Evolving information technology (IT) infrastructure, such as cloud migration, serverless services and endpoints being off-network, are straining existing SOC methodologies and tooling. The attack surface is expanding as a result of the distributed workforce and adoption of cloud-based infrastructure and services."
Source: Security Intelligence

DOXING

as well as factors that may drive disclosure trends."
Source: Elsevier

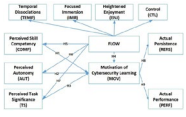
Electricity system resilience in a world of increased climate change and cybersecurity risk

"A growing array of threats now impact the resilience of the electrical network including digitalisation, cybersecurity, technological changes of the power system, and the potential for climate change to expose the system to more extreme weather events. Whether distributed and renewable electricity systems will be more resilient through multiple pathways and redundancy, or less resilient due to greater cybersecurity risks than a conventional centralised electricity system, is the key focus of this paper."
Source: Elsevier

Decision support model for cybersecurity risk planning: A two-stage stochastic programming framework featuring firms, government, and attacker

"We study the decision-making problem in cybersecurity risk planning concerning resource allocation strategies by government and firms. Aiming to minimize the social costs incurred due to cyberattacks, we consider not only the monetary investment costs but also the deprivation costs due to detection and containment delays. We also consider the effect of positive externalities of the overall cybersecurity investment on an individual firm's resource allocation attitude."
Source: Elsevier

CYBERSECURITY LEARNING



Cultivating cybersecurity learning: An integration of self-determination and flow

"We propose motivation as the key to ensuring continuous engagement with and successful learning of such cybersecurity concepts. With a lab-based training program that taught participants about SQL injection attacks, we tested a research model that integrated flow theory and self-determination theory. Within the training program, we captured participants' persistence in attempting and successfully completing the training exercises while also measuring their perceptions of motivation and flow."

apart. Based on our research among 4,644 executives and backed by our knowledge and deep industry expertise, our findings aim to help organizations innovate securely and build cyber resilience to help grow with confidence."
Source: Accenture

Frost Radar™: Global Threat Intelligence Platform Market, 2020

"The growing media attention to cyberattacks and data breaches contributes to raising awareness of cybercrime along with the financial and reputational losses that it causes. Besides, the increasing complexity of cyberattacks highlights the necessity of adopting a proactive, threat intelligence-driven approach to cybersecurity. To secure a modern enterprise, security teams must not only respond to threats but also anticipate and prevent them. Intelligence-led cybersecurity is gaining more traction as organizations not only understand the need for securing their data and infrastructure but also seek the most effective ways to accomplish that goal."
Source: Frost & Sullivan

Integration of Capabilities Transforming the Asia-Pacific Network Security Market, 2020

"The overall APAC network security market is expected to grow at 7.9% CAGR from 2019 to 2024. The wider region was led by the firewall segment due to its popularity in the market, followed by the IDS/IPS segment, and the SSL VPN segment. The network security market is still growing, albeit at a slower rate than in the past 5 years, and with varying contribution from its segments. In the immediate future, the widespread effects of the COVID-19 pandemic will drastically impair the network security market just as it will affect the wider economy. Future growth will also be impacted as the market grapples to recover."
Source: Frost & Sullivan

Cyber Security Report 2020

"Each year, Check Point Research (CPR) reviews previous year cyber incidents to gather key insights about the global cyber threat landscape. In this 2020 Cyber Security Annual Report, we offer a review of 2019's major cyber incidents, suggest predictions for 2020, and recommend best practices to help keep your organization safe from cyber attacks."
Source: Checkpoint

AVIATION

Thinking Outside the Dox: What IT Security Can Learn From Doxing

"Doxing is rightfully regarded as a dangerous threat, potentially exposing personal information where it shouldn't be. But, defenses derived from doxing may strengthen corporate cybersecurity at scale."
Source: Security Intelligence

BIOMETRICS

Dual biometrics for banking: Double trouble or super-secure?

"In an unusual experiment, two European banks (one in Hungary, the other in Spain) are trying to boost security and – nonintuitively – convenience by layering one biometric authentication method on top of another. The two biometrics are facial recognition and palm recognition – both performed via a mobile device"
Source: Computer World

DATA SCIENCE

5 ways to use data science to predict security issues

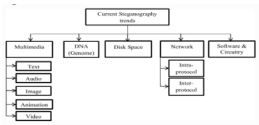
"A key part of digital transformation and the move to digital services is data science. Data science enables people to respond to problems in a better way, and to also understand those problems in a way that would not have been possible 50 years ago. But data science can be just a numbers game if it is not used to its full potential. Utilised properly, data science can help people and decisions to become 'predictive'. In the case of cybersecurity, IT professionals may be able to predict bad events before they occur. Forcepoint's Asia Pacific strategic business director Nick Savvides explains more."
Source: Channel Life

PHISHING

Attackers Increasingly Use Email and Domain Spoofing Attacks, FBI Warns

Source: Elsevier

DIGITAL STUDY



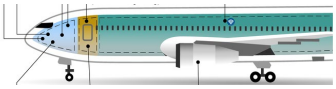
Steganography and Steganalysis (in digital forensics): a Cybersecurity guide

"The state-of-the-art techniques for steganography and steganalysis (image and video) have been deliberated for the last 5 years literature. Further, the paper also takes stock the dataset and tools available for multimedia steganography and steganalysis with the examples where steganography has been used in real-life. It is a corpus of the author's opinion and the viewpoints of different other researchers and practitioners, working in this discipline. Additionally, experiments were done using image steganography techniques to analyse the recent trends. This survey is intended to provide a complete guide for common people and new researchers and scholars approaching this field, sight on the existing and the future of steganography and steganalysis."
Source: Springer Link

DATA SCIENCE

AMSI-Based Detection of Malicious PowerShell Code Using Contextual Embeddings

"In this work, we conduct the first study of malicious PowerShell code detection using the information made available by AMSI. We present several novel deep-learning based detectors of malicious PowerShell code that employ pretrained contextual embeddings of words from the PowerShell "language". A contextual word embedding is able to project semantically-similar words to proximate vectors in the embedding space. A known problem in the cybersecurity domain is that labeled data is relatively scarce, in comparison with unlabeled data, making it difficult to devise effective supervised detection of malicious activity of many types. This is also the case with PowerShell code. Our work shows that this problem can be mitigated by learning a pretrained contextual embedding based on unlabeled data."
Source: ACM Digital Library



FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks

"Modern airplanes are equipped with networks and systems that share data with the pilots, passengers, maintenance crews, other aircraft, and air-traffic controllers in ways that were not previously feasible (see fig. 1). As a result, if avionics systems are not properly protected, they could be at risk of a variety of potential cyberattacks. Vulnerabilities could occur due to (1) not applying modifications (patches) to commercial software, (2) insecure supply chains, (3) malicious software uploads, (4) outdated systems on legacy airplanes, and (5) flight data spoofing. To date, extensive cybersecurity controls have been implemented and there have not been any reports of successful cyberattacks on an airplane's avionics systems."
Source: U.S. Government Accountability Office

RANSOMWARE

FIN11: Widespread Email Campaigns as Precursor for Ransomware and Data Theft

"In some ways, FIN11 is reminiscent of APT1; they are notable not for their sophistication, but for their sheer volume of activity. There are significant gaps in FIN11's phishing operations, but when active, the group conducts up to five high-volume campaigns a week. While many financially motivated threat groups are short lived, FIN11 has been conducting these widespread phishing campaigns since at least 2016. From 2017 through 2018, the threat group primarily targeted organizations in the financial, retail, and hospitality sectors. However, in 2019 FIN11's targeting expanded to include a diverse set of sectors and geographic regions. At this point, it would be difficult to name a client that FIN11 hasn't targeted."
Source: FireEye

SECURITY TOOLS

10 Best Advanced Endpoint Security Tools of 2020

"Email and domain spoofing is a popular practice by cybercriminals to fool recipients to deploy various phishing and malware campaigns. Recently, the FBI has issued a warning about attackers attempting to impersonate the U.S. Census Bureau for phishing and credential theft attacks."
Source: Cyware

Phishing fears cause workers to reject genuine business communications

"Employees are trying to avoid suspicious emails and phone calls, and rightly so, as they can result in malware infections and business email compromise attacks. But hyper-vigilance also has its drawbacks. And it's not just people refusing to respond to calls or emails… The problem is that real communications and fake ones are getting harder to distinguish from each other."
Source: SC Magazine

RANSOMWARE

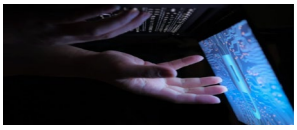
An inside look at how ransomware groups go stealth

"Law enforcement agencies and cybersecurity experts warn that ransomware groups are working harder than ever to leverage tools and techniques that hide their presence from threat detection engines, cover their tracks from investigators and generally make it harder for companies to spot or respond to intrusions until it's too late."
Source: SC Magazine

Queens, rooks and ransomware

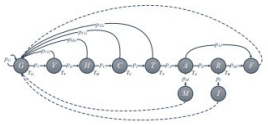
"Cybersecurity is a never-ending chess match requiring a proactive strategy… n cybersecurity, while organizations must be nimble enough to react to the unanticipated and unexpected — such as a ransomware attack, evolving threat tactics, or even a global pandemic shifting business operations — they must also have a robust and comprehensive proactive security strategy moving their metaphorical chess pieces across the board."
Source: Security Magazine

MALWARE



The ABCs of fighting malware

SYSTEMS



An Actuarial Framework for Power System Reliability Considering Cybersecurity Threats

"In this paper, an actuarial framework is established to capture and reduce the riskiness raised by interdependence among cyber risks, with the aim to enhance cyber insurance market for power systems. Absorbing semi-Markov process (SMP) is proposed to model the cyberattacks on the power grid. Also a stochastic model is developed to reflect the correlation of cyber risks across the power system. A sequential Monte Carlo simulations (MCS) framework is developed to evaluate the interruptions of the power system considering both the physical failures of the components and malicious cyberattacks."
Source: IEEE Xplore

Decentralized Consensus Decision-Making for Cybersecurity Protection in Multimicrogrid Systems

"Multimicrogrid (MMG) systems play an increasingly important role in the smart grid. They come with various potential cyberattacks, which may cause power supply interruption or even human casualties. Therefore, decision-making for timely mitigation of cyberattack risks is highly desirable in the security protection of power systems. However, there is a lack of effective decentralized decision-making strategies that are able to deal with MMG scenarios through distributed consensus. To address this issue, a decentralized consensus decision-making (DCDM) approach is proposed in this article for the security of MMG systems. It achieves decentralized consensus without the need of a trusted authority or central server, making it distinct from existing consensus methods."
Source: IEEE Xplore

Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system

"Effective vulnerability management requires the integration of vulnerability information available on multiple sources, including social media. The information could be used to inform common users about impending vulnerabilities and

"Why Endpoint Security Important? You can think of each connecting endpoint as a new gateway for both users and hackers to access your most important digital assets. And not only that, even the endpoints themselves can become the target of various cyber-attacks, including ransomware, cryptojacking, phishing, and fileless malware."
Source: Cyber Security Tools

COVID-19

Pandemic-Driven Change: The Effect of COVID-19 on Incident Response

"Every year, Secureworks releases a report that summarizes findings from our incident response engagements over the past year. Because 2020 has been a year of unprecedented disruption, this year's report approaches incident response through the lens of our changed world." Register to obtain complimentary report.
Source: SecureWorks

"Here are seven tips, from assuming every website is suspect to checking for scams."
Source: Straits Times

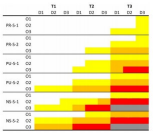
SPYWARE

GravityRAT Gains New Multi-Platform Spyware Capabilities

"GravityRAT operators are constantly working towards advancing this information stealing malware. Recently, Kaspersky researchers have witnessed another enhancement in the tool, allowing it to now target macOS and Android, in addition to existing Windows attacking capabilities, making it a multiplatform tool."
Source: Cyware

countermeasures. First, we present the Cybersecurity Vulnerability Ontology (CVO), a conceptual model for formal knowledge representation of the vulnerability management domain. Second, we utilize the CVO to design a Cyber Intelligence Alert (CIA) system that issues cyber alerts about vulnerabilities and countermeasures."
Source: Elsevier

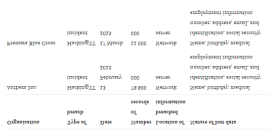
AUTOMATED VEHICLES



New Aspects of Integrity Levels in Automotive Industry-Cybersecurity of Automated Vehicles

"The spread of connected vehicles is expected to multiply the effects of the growing penetration of cyberspace in our life, and with this it remarkably influences the vulnerability of society to cyberattacks in an unfavorable way. Accordingly, ZalalZone - the Hungarian test track - has set up a working group to support the necessary methodological background for cybersecurity-related validation processes for the automotive industry. Therefore the paper aims to reconsider safety integrity levels in the automotive industry related to the field of cybersecurity."
Source: IEEE Xplore

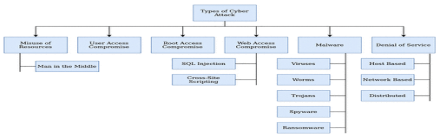
BIOTECHNOLOGY



Cybersecurity in Science and Medicine: Threats and Challenges

"Technology offers opportunities to revolutionize medicine and research but can threaten privacy and patient confidentiality. As the scale of patient data explodes, the safety and integrity of medical information are increasingly at stake. We highlight security and privacy issues associated with genomic research, medical devices, and wearable technology."
Source: Science Direct

MACHINE LEARNING



Machine learning in cybersecurity: a comprehensive survey

"In recent years, machine learning (ML) has been widely employed in cybersecurity, for example, intrusion or malware detection and biometric-based user authentication. However, ML algorithms are vulnerable to attacks both in the training and testing phases, which usually leads to remarkable performance decreases and security breaches. Comparatively, limited studies have been conducted to understand the essence and degree of the vulnerabilities of ML techniques against security threats and their defensive mechanisms. It is imperative to systematize recent works related to cybersecurity using ML to seek the attention of researchers, scientists, and engineers."

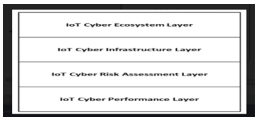
Source: Sage Journals

Teaching Adversarial Machine Learning: Educating the Next Generation of Technical and Security Professionals

"The growth in machine learning has created an opportunity to expand education to include the study of "adversarial" machine learning, specifically in undergraduate and graduate courses for cybersecurity professionals and machine learning experts. This paper presents tools available in teaching these concepts. This information also helps system designers reduce design flaws, as well as design against malicious attacks. This paper recommends using these tools to improve offensive cyber security practices that may harden machine learning systems. These tools include newly developed machine learning libraries that make this approach a practical alternative."

Source: ACM Digital Library

IoT



Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management

"Along with the growing threat of cyberattacks, cybersecurity has become one of the most important areas of the Internet of Things (IoT). The purpose of IoT cybersecurity is to

reduce cybersecurity risk for organizations and users through the protection of IoT assets and privacy. New cybersecurity technologies and tools provide potential for better IoT security management. However, there is a lack of effective IoT cyber risk management frameworks for managers. This paper reviews IoT cybersecurity technologies and cyber risk management frameworks. Then, this paper presents a four-layer IoT cyber risk management framework. This paper also applies a linear programming method for the allocation of financial resources to multiple IoT cybersecurity projects. An illustration is provided as a proof of concept."
Source: MDPI

Cybersecurity Challenges Associated With the Internet of Things in a Post-Quantum World

"In this study, we discuss techniques able to provide security in a post-quantum IoT. Specifically, we examine how the third-generation partnership project (3GPP) IoT security solutions fair in a post-quantum environment. Also, we analyse the security features of fifth-generation (5G) networks, propose improvements and discuss the manner in which a quantum computer can compromise security."
Source: IEEE XPLORE

WORKFORCE

The Cybersecurity Workforce and Skills

"Cyber security is now an essential requirement for modern organisations, but many face a significant constraint in terms of a lack of skilled personnel to support the required roles and responsibilities… This briefing paper examines the nature of the challenge, presenting evidence of the reported skills shortages, and then proceeding to examine the different forms of qualification that are available, and how security practitioners and employers may usefully identify the options that are best suited to their needs."
Source: Elsevier

ETHICS

Ethics in cybersecurity research and practice

"This paper critiques existing governance in cyber-security ethics through providing an overview of some of the ethical issues facing researchers in the cybersecurity community and highlighting shortfalls in governance practice. We separate these issues into those facing the academic research community and those facing the (corporate) practitioner community, drawing on two case studies."

Source: Elsevier

HEALTHCARE

ALICE: a hybrid AI paradigm with enhanced connectivity and cybersecurity for a serendipitous encounter with circulating hybrid cells

"Liquid biopsy in cancer research constitutes a minimally invasive procedure that can be readily carried out with relative ease for sampling one of the most investigated biological materials in body fluids: circulating tumor cells (CTCs) if the body fluid is blood and mobile tumor cells (MTCs) if the body fluid is non-blood. The prevalence and pervasiveness of these rare cancer cells have been demonstrated to correlate well with clinical predictions for diagnosis, prognosis, relapse monitoring and treatment response. However, the adoption of CTCs/MTCs in routine cancer management is still not widespread despite the reported efficacy of its use"

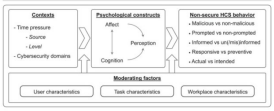
Source: U.S. National Library of Medicine

Cybersecurity Risks in a Pandemic

"This paper outlines why cyberattacks have been particularly problematic during COVID-19 and ways that health care industries can better protect patient data. The Office for Civil Rights has loosened enforcement of the Health Insurance Portability and Accountability Act, which, although useful in using new platforms like Zoom, has also loosened physical and technical safeguards to cyberattacks. This is especially problematic given that 90% of health care providers had already encountered data breaches.

Companies must implement well-defined software upgrade procedures, should use secure networks like virtual local area networks, and conduct regular penetration tests of their systems."
Source: Journal of Medical Internet Research

HUMAN BEHAVIOUR



Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures

"Cybersecurity is a growing concern for private individuals and professional entities. Reports have shown that the majority of cybersecurity incidents occur because users fail to behave securely. Research on human cybersecurity (HCS) behavior suggests that time pressure is one of the important driving factors behind non-secure HCS behavior. However, there is limited conceptual work to guide researchers and practitioners in this regard. Against this backdrop, we investigate how the impact of time pressure on HCS behavior can be conceptualized within an integrative framework and which countermeasures can be used to reduce its negative impact."
Source: Elsevier