SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

19 December 2020 – 20 FEBRUARY 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

Why 2021 Will Be The Year Of Adaptive Cybersecurity

"96% of enterprise executives say they are adjusting their cybersecurity strategies due to Covid-19 and half are now considering cybersecurity in every business decision.
71% plan to incorporate cybersecurity, including early detection of cyber risks, more into their company-wide enterprise risk management strategies according to PwC."
Source: Forbes

These are the top cybersecurity challenges of 2021

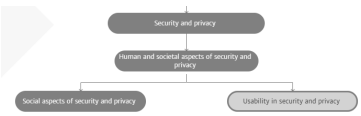
"Looking at the year ahead, it is critical to continue elevating cybersecurity as a strategic business issue and develop more partnerships between industries, business leaders, regulators and policymakers. Just like any other strategic societal challenge, cybersecurity cannot be addressed in silos."
Source: World Economic Forum

Network Security: 5 Fundamentals for 2021

"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

academic

CYBERSECURITY AWARENESS



A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education

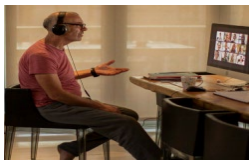
"We conduct a comprehensive review covering academic publications and industry products relating to tools for cybersecurity awareness and education aimed at non-expert end-users developed in the past 20 years. Through our search criteria, we identified 119 tools that we cataloged into five broad media 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

Cybersecurity awareness training programs: a cost–benefit analysis framework

"Employees must receive proper cybersecurity training so that they can recognize the threats to their organizations and take the appropriate actions to reduce cyber risks. However, many cybersecurity awareness training (CSAT) programs

reports

INSIGHT



2021 State of Malware Report

"Through it all, there is one form of business that seems to have thrived in 2020 — the creation and operation of malicious software. The pace of innovation picked up in 2020
as many entirely new malware families emerged. Ransomware gangs continued to learn
from each other too, with successful tactics spreading quickly between them. Perhaps the
most important new tactic that emerged was "double extortion," which saw cybercriminal
groups extorting more money with threats to leak sensitive data than from decrypting compromised computers."
Source: MalwareBytes

IDC's Worldwide Cybersecurity Software and Appliance Taxonomy, 2021

"This IDC study presents IDC's taxonomy of the cybersecurity software and appliance market. It provides definitions of security solutions in five functional markets, four product types, and three deployment types. This taxonomy forms the foundation for IDC's cybersecurity market forecast and market share documents in 2021 and IDC trackers (IDC's Worldwide Semiannual Software Tracker and

industry. For more facts about robots watch IFR´s video news about Europe in one minute."
Source: Security Boulevard

The Top 21 Security Predictions for 2021

"As we recover from the worst pandemic in a century, what will the New Year bring in cyberspace? Here's your annual roundup of security industry forecasts, trends, themes and cybersecurity predictions."
Source: Government Technology

What Will the Cybersecurity Landscape Look Like in 2021?

"The COVID-19 pandemic shifted many enterprises into a new way of working, forcing a fast and swift implementation of new systems and policies to facilitate remote work. In the struggle to adjust and ensure smooth operations, many long-simmering cybersecurity risks and issues have come to the forefront. Our 2021 Security Predictions' report discusses the security challenges brought about by the new workplace environments, migration to cloud applications, and plausible threats that should be anticipated by your organization."
Source: Trend Micro

Cybersecurity after the pandemic

"As the months wore on, new threats emerged and the realization slowly dawned that this was a reality all of us will have to live with for some time. So as we begin 2021, locked down again, what should security leaders' New Year resolutions be?"
Source: TechRadar

Cybersecurity – a collective responsibility and business enabler

"There is no doubt COVID-19 has exponentially increased the speed and magnitude of digital adoption. Globally, six in ten c-suite executives said that their organisations had accelerated their digital transformation due to the pandemic."
Source: Business Times

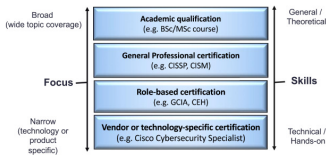
3 ways to fill worrying cybersecurity gaps

"As businesses of the future evolve to be more digital and more shared, the need to prepare to avert a cyber pandemic – with potential even more than the coronavirus to upend our lives – has never been more urgent.
We need to strengthen our strategic response to the risks before we invest in tactics. Our plans must work harder fall short due to their misaligned training focuses. Employees must receive proper cybersecurity training so that they can recognize the threats to their organizations and take the appropriate actions to reduce cyber risks. However, many cybersecurity awareness training (CSAT) programs fall short due to their misaligned training focuses."
Source: Emerald Insight

CyberSecurity Challenges for Software Developer Awareness Training in Industrial Environments

"Awareness of cybersecurity topics facilitates software developers to produce secure code. This awareness is especially important in industrial environments for the products and services in critical infrastructures. In this work, we address how to raise awareness of software developers on the topic of secure coding. We propose the "CyberSecurity Challenges", a serious game designed to be used in an industrial environment and address software developers' needs. Our work distils the experience gained in conducting these CyberSecurity Challenges in an industrial setting. The main contributions are the design of the CyberSecurity Challenges events, the analysis of the perceived benefits, and practical advice for practitioners who wish to design or refine these games."
Source: Cornell University

CYBERSECURITY SKILLS



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. Although numerous related qualifications and certifications are available, it is necessary to understand this landscape in order to make an informed decision about which may signify the skills that are relevant to pursue or recruit. This briefing paper examines the nature of the challenge, presenting evidence of the reported skills shortages."
Source: Elsevier

The Challenges of Software Cybersecurity Certification [Building Security In]

IDC's Worldwide Semiannual Security Products Tracker)."
Source: IDC

Growth Opportunities In Therapeutics, Energy Storage, Millimeter Wave Technology, And Cybersecurity

"This edition of the Inside R&D Technology Opportunity Engine (TOE) features novel innovations related to digital therapeutics, 3D printing for surgery and implantable device for treatment of chronic heart or liver failure. The TOE also features novel algae extract-based active ingredient for cosmetics. The TOE highlights recent innovations related to artificial photosynthesis and flow batteries paving way for a low-carbon economy. The TOE covers an innovative 60 GHz millimeter wave technology as an alternative to fiber optics and novel encryption technology."
Source: Frost & Sullivan

Increasingly Sophisticated Threat Landscape Drives the Uptake of Managed Security Services in APAC

"Managed security service providers (MSSPs) offer managed security services (MSS) that help manage and monitor the security posture of their customers' IT infrastructure. By using these services, client organizations are often able to reduce expenditure on either customer premises equipment (CPE) or in-house security specialists, and receive effective security management…The ASEAN market is expected to maintain its strong growth over the next 5 years. The lack of budget allocated to cybersecurity, specifically to strengthen detection and response capabilities, is one of the reasons why businesses engage MSSPs."
Source: Frost & Sullivan

FORECAST

A Global Reset: Cyber Security Predictions 2021

"While 2020 was filled with great uncertainty, there are still guarantees in the cyber security realm. Threat actors will continue to attack without any regard for the challenges faced by their targets. These actors continue to be motivated by espionage and monetary gain, though their TTPs will always evolve. This means organizations will continue to be breached, resulting in business disruptions, data compromise,

and smarter to address capability gaps.
A common agenda will build the confidence and competence to achieve the resilience we need."
Source: World Economic Forum

Personal data, fodder for cyberwarfare? New models for stepping up cybersecurity

"In today's increasingly digital world, cybersecurity is paramount. The upsurge in cyberattacks has far-reaching effects, from jeopardizing users' private data to sparking all out cyberwar, not to mention threatening private businesses' intellectual property. In such volatile times, the only approach is to adopt new models and applications that can address these problems efficiently."
Source: Universitat Oberta de Catalunya

Why Supply Chains Are Today's Fastest Growing Cybersecurity Threat

"Business ecosystems have expanded over the years owing to the many benefits of diverse, interconnected supply chains, prompting organizations to pursue close, collaborative relationships with their suppliers. However, this has led to increased cyber threats when organizations expose their networks to their supply chain and it only takes one supplier to have cybersecurity vulnerabilities to bring a business to its knees."
Source: Security Boulevard

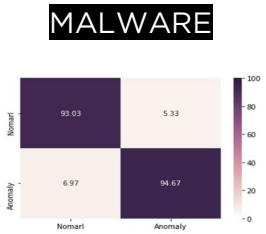
Can your organization obtain reasonable cybersecurity? Yes, and here's how

"An IT axiom, "Do you know where your data is?" has been eclipsed by something more accountable: "Is your data reasonably secure?" That's what companies have to determine to protect themselves in the event of a cybersecurity attack."
Source: Tech Republic

Cybersecurity: Blaming users is not the answer

"Experts are warning, when it comes to cybersecurity, blaming users is a terrible idea. Doing so likely results in creating an even worse situation. "Many organizations have defaulted to a blame culture when it comes to data security," comments Tony Pepper, CEO of Egress Software Technologies, in an email exchange. "They believe actions have consequences and someone has to be responsible."
Source: Tech Republic

"Despite the expected benefits of cybersecurity certification in terms of transparency for end users and the use of best practices, software providers still consider cybersecurity certification to be a costly and complex process. Indeed, certification could cause delays in the launch of new systems, with a significant economic impact.4 So, from the industry's perspective, why should companies invest time and money in certifying ICT components and systems?"
Source: IEEE Xplore



DeepAMD: Detection and identification of Android malware using high-efficient Deep Artificial Neural Network

"In this paper, a novel approach DeepAMD to defend against real-world Android malware using deep Artificial Neural Network (ANN) has been adopted including an efficiency comparison of DeepAMD with conventional machine learning classifiers and state-of-the-art studies based on performance measures such as accuracy, recall, f-score, and precision. As per the experimental analysis, DeepAMD outperforms other approaches in detecting and identifying malware attacks on both Static as well as Dynamic layers."
Source: Elsevier

AI-HydRa: Advanced hybrid approach using random forest and deep learning for malware classification

"In this paper, we propose a machine learning-based hybrid decision model that can achieve a high detection rate with a low false positive rate. This hybrid model combines a random forest and a deep learning model using 12 hidden layers to determine malware and benign files, respectively. This model also includes certain proposed voting rules to make final decisions. In an experiment involving 6,395 atypical samples, this hybrid decision model achieved a higher detection rate (85.1% and standard deviation of 0.006) than that of the prior model (65.5%) without voting rules."
Source: Elsevier

Advanced malware propagation on random complex networks

reputational harm, and almost always a financial loss."
Source: FireEye

134 Cybersecurity Statistics and Trends for 2021

"2020 brought with it several trials and triumphs. COVID-19 has forced companies to create remote workforces and operate off cloud-based platforms. The rollout of 5G has made connected devices, well, more connected than ever. All this to say, the cybersecurity industry has never been more important. These recent events and the below cybersecurity statistics and figures considered, here are some industry trends and also predictions to watch for in 2021 and beyond."
Source: Varonis

2021 Threat Predictions Report

"The December 2020 revelations around the SUNBURST campaigns exploiting the SolarWinds Orion platform have revealed a new attack vector – the supply chain – that will continue to be exploited.
The ever-increasing use of connected devices, apps and web services in our homes will also make us more susceptible to digital home break-ins. This threat is compounded by many individuals continuing to work from home, meaning this threat not only impacts the consumer and their families, but enterprises as well.
Attacks on cloud platforms and users will evolve into a highly polarized state where they are either "mechanized and widespread" or "sophisticated and precisely handcrafted"."
Source: McAfee

Integrated Cybersecurity: Efficiency And Effectiveness in a Challenging Environment

"According to IDC research, 75% of organizations worldwide recognize that a needless lack of integration in a security environment can waste a security team's time.
Organizations are already struggling with two major security challenges:

- A Multifaceted Cyberthreat Landscape
- Outdated Cyber Secruity Software
- A Global Shortage of Security Professionals
- Distributed denial of service (DDoS) attacks"

Source: Tech Republic

CYBER ATTACKS

Fifth-generation cyberattacks are here. How can the IT industry adapt?

"Cyberattacks are continuing to grow in sophistication and scale.
The coronavirus pandemic has increased the attack surface for cybercriminals, leading to a possible cyber-pandemic."
Source: World Economic Forum

Top 5 things to know about adversarial attacks

"Machine learning is being used for a lot of great things, from guiding autonomous cars to creating pictures of cats that don't actually exist. Of course, as with any technology, if it exists someone will want to hack it. Some of those hackers will be malicious. Adversarial attacks use machine learning against machine learning by creating images, text or audio, that thwarts other algorithms from performing as expected."
Source: Tech Republic

'Zoombombing' research shows legitimate meeting attendees cause most attacks

"Cybersecurity experts expressed concerns about the apps' ability to thwart hackers. A new study from researchers at Binghamton University and Boston University, however, shows that most zoombombing incidents are "inside jobs.""
Source: EurekAlert!

Researcher hacks into 35 major technology firms

"A Romanian threat researcher detailed in a published report "In this work a novel model to simulate advanced malware spreading is introduced and analyzed. It is an individual-based model such that the dynamics of the malware outbreak is governed by means of a cellular automaton. The network topologies considered are complex random networks and each device is endowed at every step of time with one of the following possible states: susceptible, infected, attacked and recovered. A study analyzing the influence of topology variability and the structural characteristics of initially infected devices is done."
Source: Elsevier

Towards a systematic description of the field using bibliometric analysis: malware evolution

"This study provides an overview of the articles, productivity, research area, the Web of Science categories, authors, high-cited articles, institutions, and impact journals examining malware. Research activities are continued by placing terms in the classification of malware detection systems that outline important areas in malware research. From the analysis, it can be concluded that the highest number of publications focusing on malware studies came from the continent of Asia. Additionally, this study discusses the challenges of malware studies in the recent research studies as well as the future direction."
Source: Springer Link

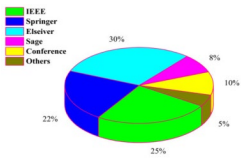
HACKING

$$\ln\left(\sigma^2_{BTC,t}\right) = \omega_{BTC} + \alpha_{BTC}\left|\frac{\epsilon_{BTC,t-1}}{\sigma_{BTC,t-1}}\right| + \beta_{BTC}\ln\left(\sigma^2_{BTC,t-1}\right) + \gamma_{BTC}\frac{\epsilon_{BTC,t-1}}{\sigma_{BTC,t-1}} + \delta_{BTC,0}d_{BTC,0,t} + \sum_{i=1}^{K}\delta_{BTC,i}d_{BTC,i,t}$$

When the blockchain does not block: on hackings and uncertainty in the cryptocurrency market

"A total of 1.1 million bitcoins were stolen in the 2013–2017 period. Noting that the average price for a Bitcoin in 2018 was $7572 the corresponding monetary equivalent of losses is $8.9 billion highlighting the societal impact of this criminal activity. Investigating the response of the uncertainty of Bitcoin returns when hacking incidents occur, the results of this study point toward two different responses."
Source: Taylor & Francis Online

ARTIFICIAL INTELLIGENCE

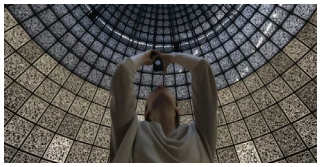


Wednesday how he broke into IT systems belonging to some of the largest corporations in the world. His assaults successfully targeted Apple, Microsoft, Tesla, PayPal, Netflix and more than 30 other corporations."
Source: TechXplore

Tests reveal cybersecurity vulnerabilities of common seismological equipment

"Seismic monitoring devices linked to the internet are vulnerable to cyberattacks that could disrupt data collection and processing, say researchers who have probed the devices for weak points. Common security issues such as non-encrypted data, insecure protocols, and poor user authentication mechanisms are among the biggest culprits that leave seismological networks open to security breaches"
Source: EurekAlert!

MANAGING CYBERSECURITY



4 ways to build resilience to digital risks in the COVID-19 era

"More than ever, companies now must go digital or die. Dependence on cloud computing jumped by a third in 2020. Network operators registered as much as a 70% increase in the demand for internet and mobile data services. Videoconferencing sky-rocketed by 700% last year. Not surprisingly, the valuation of social media and remote conferencing companies soared.
This growing dependence on all things digital has a dark side. Cybercrime, especially ransomware, also increased exponentially."
Source: World Economic Forum

How micro-drilling can enhance your cybersecurity training

"Agile thinking is important in dealing with cyberattacks. Read one psychologist's tips for cybersecurity professionals on how to adapt and stop the attackers."
Source: Tech Republic

Cognitive agility can help solve some "wicked" cybersecurity challenges

"Emergency responders practice continually so that their response during a crisis is inherent and automatic. This approach is also used by many cybersecurity teams, and

Deep Learning Algorithms for Cybersecurity Applications: A Technological and Status Review

"In this survey, we analyzed and reviewed the usage of deep learning algorithms for Cybersecurity applications. Deep learning which is also known as Deep Neural Networks includes machine learning techniques that enable the network to learn from unsupervised data and solve complex problems. Here, 80 papers from 2014 to 2019 have been used and successfully analyzed. Deep learning approaches such as Convolutional Neural Network (CNN), Auto Encoder (AE), Deep Belief Network (DBN), Recurrent Neural Network (RNN), Generative Adversal Network (GAN) and Deep Reinforcement Learning (DIL) are used to categorize the papers referred."
Source: Elsevier

MalNet: A Large-Scale Cybersecurity Image Database of Malicious Software

"Computer vision is playing an increasingly important role in automated malware detection with to the rise of the image-based binary representation... We introduce MalNet, the largest publicly available cybersecurity image database, offering 133x more images and 27x more classes than the only other public binary-image database."
Source: Cornell University

Cybersecurity Enhancement through Blockchain Training (CEBT) – A serious game approach

"Blockchain technology is increasingly finding traction in diverse areas such as finance, supply-chain management, and cloud services because of its ability to provide robust cybersecurity inherent in its system of having decentralized data storage... We propose one of the first such pedagogical tool for training in blockchain using an adversarial sandbox adaptive serious game approach for students and technology professionals. We further propose use of AI to enhance NPC interactivity based on player's responses. We plan to evaluate this serious game on a subjective metrics that is based on a game experience questionnaire."
Source: Elsevier

IoT

with good reason: In an emergency, time to think, gather information, and consider all options is limited. Practice builds in an element of unconscious response, along with the ability to be guided by intuition."
Source: Tech Republic

6 principles to unite business in the fight against cybercrime

"The surge in cybersecurity attacks in 2020 has made boards and CEOs more acutely aware of the risks of inadequately secure technology. Indeed, in the World Economic Forum's COVID-19 Risks Outlook, increases in cyberattacks were among the top three most worrisome risks to leaders around the world. As long as businesses pursue digital growth strategies, cybersecurity is a perennial concern; cybercriminals never sleep – and neither can board or corporate chiefs."
Source: World Economic Forum

We urgently need a new army of digital firefighters. Here's why

"The digital landscape is vast and vulnerable - and we don't have enough cybersecurity professionals to keep it safe.
There is a cyber skills shortfall of around 4 million digital firefighters.
Here's how to find and train a new generation of cybersecurity experts - before it's too late."
Source: World Economic Forum

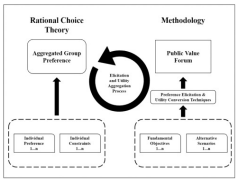
IT leaders see outsourcing cybersecurity as one solution to increased attacks

"IT leaders are turning to outsourced cybersecurity support in response to the spike in cyberattacks since the start of the COVID-19 pandemic. Eighty-three percent of decision-makers with in-house cybersecurity teams are considering outsourcing to a managed service provider (MSP) within the next six months."
Source: Tech Republic

5G adds more concerns: CISOs should build cybersecurity from the ground up

"TechRepublic's Karen Roby spoke with Curtis Simpson, CISO of Armis, an Internet of Things (IoT) security company, about security concerns with 5G. The following is an edited transcript of their conversation."
Source: Tech Republic

MALWARE



User values and the development of a cybersecurity public policy for the IoT

"In this paper we argue that new IoT policy should be guided by key stakeholder values (i.e. what users think to be important). We utilize the Public Value Forum to elicit public values to inform decision-making surrounding IoT policy by public administrators, conceptually informed by Rational choice theory. We use a five-phase process to introduce the decision context (i.e. the policy problem), define fundamental objectives, rank these objectives, identify value-based trade-offs between them and construct a multi-attribute utility model."
Source: Elsevier

A Pragmatic Cybersecurity Strategies for Combating IoT-Cyberattacks

"Massive Cyberattacks, especially Distributed Denial of Service (DDoS), remain an overwhelming threat to new emerging computer paradigms such as Cloud Computing and Internet of Things, deployed within critical infrastructures (healthcare, aviation, energy, industrial control and military). Furthermore, conventional security approaches and strategies are no longer appropriate to deal with this kind of cyberattacks, for the reason that they have major limitations... This paper focuses on DDoS cyberattack detection and mitigation method based on artificial intelligence model affecting IoT network infrastructure."
Source: IEEE Xplore

An IoT-Focused Intrusion Detection System Approach Based on Preprocessing Characterization for Cybersecurity Datasets

"This research proposes the study and evaluation of several preprocessing techniques based on traffic categorization for a machine learning neural network algorithm. This research uses for its evaluation two benchmark datasets, namely UGR16 and the UNSW-NB15, and one of the most used datasets, KDD99… The objective of this research is to evaluate this categorization by using various data preprocessing techniques to obtain the most accurate model. Our proposal shows

State of malware: 3 key findings in the latest Malwarebytes report

"The 2021 State of Malware Report from Malwarebytes found that cybercriminals are learning from the past to build smarter software and starting to modularize their products to make distribution easier. Those are some of the findings in the Malwarebytes report released today. The report examined what malware was most active during 2020, as well as trends in attacks on specific devices such as Android phones and Mac laptops."
Source: Tech Republic

Trickbot's Sibling, Bazarbackdoor, is Hunting Down its Targets Vigorously

"In the fast-paced world of cybersecurity, most malware get a brief period in the spotlight before falling into oblivion. However, this is not the case with TrickBot. Despite the takedown attempt last year, reports suggested that the creators made efforts to reinstate the demolished infrastructure to launch more campaigns. While this struggle continues, a backdoor malware called BazarBackdoor from the same operators has come to the foreground in the threat landscape."
Source: Cyware Social

The first M1 MacBook malware has arrived – here's what you need to know

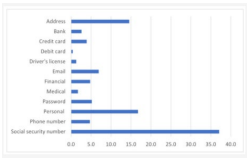
"The first malware native to M1-powered MacBooks has been discovered in the wild, just months after the arrival of the first Apple Silicon devices.
News of the first M1 malware comes via ex-NSA researcher and longtime Mac security researcher Patrick Wardle, who has uncovered the existence of GoSearch22.app, an M1-native version of the longstanding Pirrit virus."
Source: Tech Radar

2021's Most Wanted: Emotet continues reign as top malware threat

"The Emotet trojan continues to reign as top malware in January, despite international law enforcement taking control of its infrastructure resulting in 14% decrease in global impact, says Check Point Research."
Source: IT Brief

that, by applying the categorization of network traffic and several preprocessing techniques,"
Source: MDPI

CYBERSECURITY RISKS IN EDUCATION



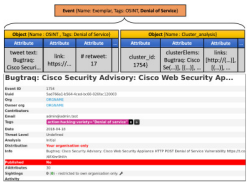
A Systematic Review of Cybersecurity Risks in Higher Education

"The demands for information security in higher education will continue to increase. Serious data breaches have occurred already and are likely to happen again without proper risk management. This paper applies the Comprehensive Literature Review (CLR) Model to synthesize research within cybersecurity risk by reviewing existing literature of known assets, threat events, threat actors, and vulnerabilities in higher education. The review included published studies from the last twelve years and aims to expand our understanding of cybersecurity's critical risk areas."
Source: MDPI

Applying High Impact Practices in an Interdisciplinary Cybersecurity Program

"The Center for Cybersecurity Education and Research at Old Dominion University has expanded its use of high impact practices in the university's undergraduate cybersecurity degree program. Strategies developed to promote student learning included learning communities, undergraduate research, a robust internship program, service learning, and electronic portfolios. This paper reviews the literature on these practices, highlights the way that they were implemented in our cybersecurity program, and discusses some of the challenges encountered with each practice."
Source: Kennesaw State University

THREAT INTELLIGENCE TOOL



Processing tweets for cybersecurity threat awareness

"This work proposes SYNAPSE, a Twitter-based streaming threat

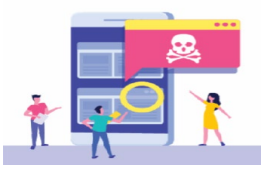
SilentFade malware attacks ramp up in Southeast Asia

"India, Indonesia and Malaysia were among the top 10 countries globally to have been hit by the greatest number of malware attacks by the SilentFade group last month, according to cyber security vendor Kaspersky.

As reported by sister publication CSO, Facebook discovered the SilentFade malware family towards the end of 2018, with its origins traced back to 2016."

Source: Channel Asia

RANSOMWARE



Enterprise ransomware prevention measures to enact in 2021

"Ransomware involves bad actors installing malware within an organization's computer systems and then demanding payment -- typically via bitcoin -- to end the assault. Once the ransom is paid, the hackers then provide the victim organization with codes to decrypt or unlock affected files or systems.

It's a form of extortion and should be labeled as such. "It's going to become the preferred way to monetize cybercrime," said Michael Hamilton, founder and CISO of CI Security, a cybersecurity consulting firm based in Bremerton, Wash., and former CISO for the city of Seattle."

Source: Tech Target

Ransomware 'Brands' Are A Double-Edged Sword — For Threat Hunters And Cybercriminals

"When credit card-stealing malware was at its peak, the perpetrators mainly wanted to be unknowns; they didn't want anyone to know who they were. But, the cyberthreat landscape moves fast, and with ransomware as one of the most prominent cyber threats today, the gangs perpetrating these crimes are taking the complete opposite stance: They want to be public, they want to be known, they want their attacks to make "breaking news" headlines, and they want to get the credit for it."

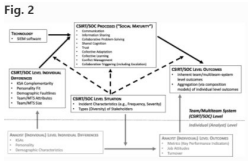
Source: Forbes

Media and Electronic Gaming Companies Prepare for a Jump in Ransomware Attacks in 2021

"It's no surprise that recent surveys highlight ransomware as the top security worry (and highest priority) for monitor that generates a continuously updated summary of the threat landscape related to a monitored infrastructure. SYNAPSE is designed to accurately select any kind of cybersecurity events and summarise them for the convenience of security analysts. Its tweet-processing pipeline is composed of filtering, feature extraction, binary classification, an innovative clustering strategy, and generation of Indicators of Compromise (IoCs)."

Source: Elsevier

ORGANIZATION AND CYBERSECURITY



Organizational science and cybersecurity: abundant opportunities for research at the interface

"We define cybersecurity, provide definitions of key cybersecurity constructs relevant to employee behavior, illuminate the unique opportunities available to organizational scientists in the cybersecurity arena (e.g., publication venues that reach new audiences, novel sources of external funding), and provide overall conceptual frameworks of the antecedents of employees' cybersecurity behavior. In so doing, we emphasize both end-users of cybersecurity in organizations and employees focused specifically on cybersecurity work. We provide an expansive agenda for future organizational science research on cybersecurity—and we describe the benefits such research can provide not only to cybersecurity but also to basic research in organizational science itself."

Source: Springer Link

Assessing the Moderating Effect of Security Technologies on Employees Compliance with Cybersecurity Control Procedures

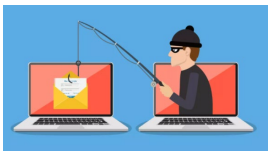
"The increase in cybersecurity threats and the challenges for organisations to protect their information technology assets has made adherence to organisational security control processes and procedures a critical issue that needs to be adequately addressed. Drawing insight from organisational theory literature, we develop a multi-theory model, combining the elements of the theory of planned behaviour, competing value framework, and technology—organisational and

CISOs in 2021. Media and Entertainment organizations, including rapidly growing video game development studios, need to be especially concerned. Sophos' recent State of Ransomware 2020 report noted that the media and entertainment sector was the vertical most targeted by ransomware, with 60% of organizations in the survey experiencing a successful (for the attacker, that is) attack last year."
Source: Security Boulevard

Ransomware Trends You Need to Know in 2021

"It's no secret that cybercriminals continuously test company networks and employees to seek out vulnerabilities. Hackers use every digital trick up their sleeves to steal data and, in some cases, even threaten to publicly release sensitive information. As the world has moved into an increasingly digital direction, ransomware attacks are growing sharply and causing more headaches than ever for companies."
Source: Security Boulevard

PHISHING



This phishing scam lures you in by pretending you've got a bonus

"Security researchers at Fortinet have discovered a new phishing campaign which tries to lure enterprise users with fake customer complaint reports, fake billing statements and even the offer of a phony bonus.
The campaign also uses a new variant of the Bazar trojan, which has been linked to the developers of Trickbot, that comes equipped with anti-analysis techniques to make it more difficult for antivirus software to detect."
Source: Tech Radar

This phishing email promises you a bonus - but actually delivers this Windows trojan malware

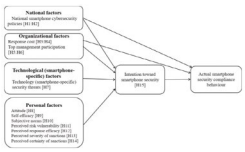
"Researchers at Fortintet identify phishing attacks distributing new variant of Bazar trojan, a malware that creates a full backdoor onto infected Windows PCs."
Source: ZDNet

$62,000 lost in fake Singtel e-mail phishing scams, 22 police reports lodged

"Victims of the phishing fraudsters received e-mails claiming to be from

environmental theory to examine how the organisational mechanisms interact with espoused cultural values and employee cognitive belief to influence cybersecurity control procedures."
Source: ACM DIGITAL LIBRARY

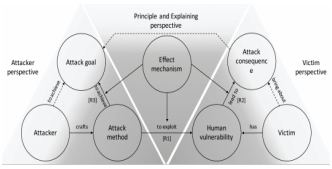
MOBILE DEVICES



Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce

"Employees are increasingly relying on mobile devices. In international organizations, more employees are using their personal smartphones for work purposes. Meanwhile, the number of data breaches is rising and affecting the security of customers' data. However, employees' cybersecurity compliance with cybersecurity policies is poorly understood. Researchers have called for a more holistic approach to information security. We propose an employee smartphone-security compliance (ESSC) model, which deepens understanding of employees' information-security behavior by considering influences on the national, organizational, technological (smartphone-specific), and personal levels."
Source: Elsevier

SOCIAL ENGINEERING IN CYBERSECURITY



Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods

"This paper proposes a conceptual model which provides an integrative and structural perspective to describe how social engineering attacks work. Three core entities (effect mechanism, human vulnerability and attack method) are identified to help the understanding of how social engineering attacks take effect. Then, beyond the familiar scope, we analyze and discuss the effect mechanisms involving 6 aspects (persuasion, social influence, cognition & attitude & behavior, trust and deception, language & thought

the telco saying they had won a cash prize or were eligible to claim cashback or a gift.
People who clicked on the URL link were directed to a fake Singtel webpage which asked for their bank information and one-time passwords (OTPs) in order to claim the prize, cashback or gift."
Source: Straits Times

U.S. Users Targeted with Phishing Scams More than Users in Other Countries

"A new study rolled out by Google, in collaboration with researchers at Stanford University, studied over a billion malicious emails and targets that Google had identified and blocked over a period of five months, to get more intelligence about who was being targeted and how the campaigns were targeting users. The study found that users in the U.S. were targeted more than any others in the world, followed by the United Kingdom and Japan."
Source: National Law Review

CYBERSECURITY INSURANCE

Why cybersecurity insurance may be worth the cost

"Cybersecurity insurance can compensate you in the event of a cyberattack. But how do you determine the right policy for your needs?"
Source: Tech Republic

SECURITY AND VEHICLES

Car Hacking Is Real. Here's How Manufacturers Can Combat It

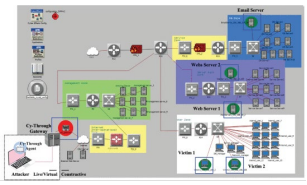
"The thought of a hacker remotely seizing control of your vehicle sounds like something from a science fiction movie. But car hacking is not only possible today; it has been since 2005, according to a computer science researcher from New York University. And many auto manufacturers may not be adequately addressing the growing threat of automotive cyberattacks."
Source: Auth0

& decision, emotion and decision-making) and the human vulnerabilities involving 6 aspects (cognition and knowledge, behavior and habit, emotions and feelings, human nature, personality traits, individual characters) , respectively."
Source: IEEE Xplore

Hacking Humans? Social Engineering and the Construction of the "Deficient User" in Cybersecurity Discourses

"In this paper, we explore how discursive framings of individual versus collective security by cybersecurity experts redefine roles and responsibilities at the digitalized workplace. We will first show how the rhetorical figure of the deficient user is constructed vis-à-vis notions of (in)security in social engineering discourses. Second, we will investigate the normative tensions that these practices create. To do so, we link work in science and technology studies on the politics of deficit construction to recent work in critical security studies on securitization and resilience."
Source: SAGE Journals

CYBERSECURITY SIMULATIONS



Cy-Through: Toward a Cybersecurity Simulation for Supporting Live, Virtual, and Constructive Interoperability

"In this paper, we propose a novel cybersecurity simulation platform, Cy-Through, which enables full interoperability between models with different fidelity levels, live/virtual and constructive models. Through the development and demonstration of a prototype of the platform, we prove the possibility of a Live, Virtual, and Constructive (LVC)-interoperable cybersecurity simulation."
Source: IEEE Xplore

Optimization-Time Analysis for Cybersecurity

"A mathematical framework to reason about time resilience in cybersecurity is introduced. We first consider an attacker who can mount several multi-stage attacks on the organization: the defender's objective is to select an optimal portfolio of security controls, within a given budget, to withstand the highest number of attacks. The

Top 5 security risks to connected cars, according to Trend Micro

"A new report from Trend Micro analyzes a day in the travels of a connected car to identify the cyberattacks most likely to succeed. "Cybersecurity for Connected Cars: Exploring Risks in 5G, Cloud and Other Connected Technologies" puts the overall risk at medium. Among the millions of endpoints in a connected car's ecosystem, analysts found 29 potential cybersecurity attack vectors and ranked five as the highest risks."
Source: Tech Republic

Scientists found a way to maintain the cybersecurity of electronics in vehicles

"Specialists from Peter the Great St. Petersburg Polytechnic University (SPbPU) improved the cybersecurity system mechanism, based on the ECU (Electronic Control Unit) in modern vehicles. The research results were published in the scientific journal Nonlinear Phenomena in Complex Systems."
Source: Tech Xplore

WORK FROM HOME

What you cannot see you cannot secure: Shining a light on cybersecurity threats in a work-from-home environment

"A quick "work from home new normal" search on Google will return results somewhere in the ballpark of 2 billion. On the other hand, searches for "cybersecurity risks work from home" result in far less—around 32 million. While that may seem like a lot of coverage on any scale, it reflects the chasm between what we focus on and what we understand about this new environment as we begin 2021."
Source: Security Magazine

BOOK PUBLISHED

INL researchers publish book to prevent cybersecurity disruptions, train workforce

"Countering Cyber Sabotage: Introducing Consequence-Driven, Cyber-Informed Engineering, written by Andy Bochman and Sarah mathematical model is a Markov chain with an initial state called the safe state, intermediate states for all possible attacks (each attack state denoting a probabilistic attack graph), and a sink state denoting a successful attack."
Source: IEEE Computer Society

REVIEW

The Recent Trends in CyberSecurity: A Review

"During recent years, many researchers and professionals have revealed the endangerment of wireless communication technologies and systems from various cyberattacks... In this conjunction, this paper gives a complete account of survey and review of the various exiting advanced cyber security standards along with challenges faced by the cyber security domain. The new generation attacks are discussed and documented in detail, the advanced key management schemes are also depicted. The quantum cryptography is discussed with its merits and future scope of the same. Overall, the paper would be a kind of technical report to the new researchers to get acquainted with the recent advancements in Cyber security domain."
Source: Science DIrect

A Review on Cybersecurity Vulnerabilities for Urban Air Mobility

"This paper presents a review of several known cybersecurity vulnerabilities and previous attacks associated with UAVs and aircraft's core communication systems. Analyzing current solutions to each threat and incorporating early concepts for UAM, this paper then presents a basic cybersecurity framework featuring a blockchain-based PKI with secondary navigation systems to allow for the development of secure airspace."
Source: Aerospace Research Central

Freeman, details INL's innovative approach to securing critical infrastructure systems like the electric power grid, oil and natural gas refineries and water treatment facilities. Developed in the pre-internet era, much of the technology responsible for controlling operations at many public utilities is often decades-old and lacks modern defense capabilities. This makes them vulnerable to cyberattacks ranging from ransomware threats to significant service disruptions."
Source: Idaho National Laboratory