SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

17 June - 14 August 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

NETWORK SECURITY

Critical Bugs in Utilities VPNs Could Cause Physical Damage

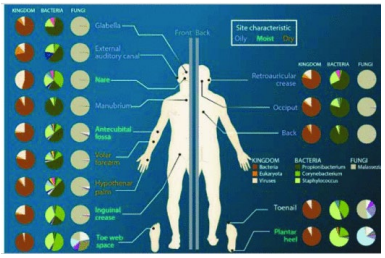
"Remote code-execution vulnerabilities in virtual private network (VPN) products could impact the physical functioning of critical infrastructure in the oil and gas, water and electric utilities space, according to researchers. Researchers at Claroty found that VPNs used to provide remote access to operational technology (OT) networks in industrial systems are vulnerable to an array of security bugs, which could give an attacker direct access to field devices and cause physical damage or shut-downs."

Source: Cyber Security Review

RANSOMWARE

Garmin obtains decryption key after ransomware attack

HEALTHCARE

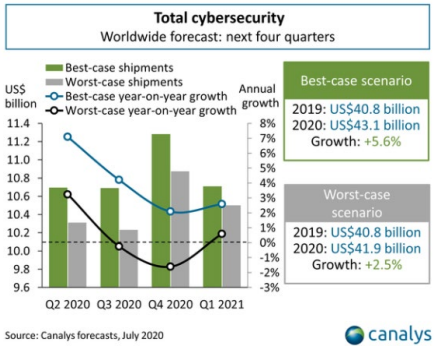


Cyber Threat Intelligence and the Cyber Meta-Reality and Cyber Microbiome

"In a cyber meta-reality filled with zero day exploits, autonomous code, Worms modeled from Stuxnet, and the coming onslaught of AI enabled malware, the need for actionable, virtually prescient threat intelligence is paramount. It is almost uniformly recognized that the current reactionary paradigm concerning cyber threats is severely lacking. Cyber threat analysts desperately need a systematic approach to cyber threat characterization and how cyber threats evolve within a greater construct defined here as the cyber microbiome. This paper will first define the concept of the cyber microbiome and its place in what has become the cyber meta-reality. Cyber threats will then be examined in relation to this paradigm and recommendations will be made regarding how threat characterization and genetic mutation can be examined in light of this new, techno-biological understanding."

Source: IEEE Xplore

COVID 19



Global cybersecurity 2020 forecast

"Canalys forecasts that worldwide cybersecurity spending will grow 5.6% in its best-case scenario, where investment continues to outpace the economy. The overall shipment value, covering endpoint security, network security, web and email security, data security, and vulnerability and security analytics, is expected to reach US$43.1 billion. Even in Canalys' worst-case scenario, if IT budgets come under serious pressure, the global cybersecurity market is still forecast to grow 2.5% in 2020. This assumes the maximum level of negative economic impact and duration of the COVID-19 pandemic."

Source: Canalys

Check Point Research: COVID-19 Pandemic Drives Criminal

"Cyber Attack Trends: 2020 Mid-Year Report' reveals how criminals have targeted all sectors with pandemic-themed attacks, and highlights surge in nation-state cyber activity."

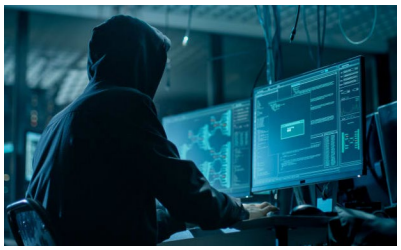
Source: Globenewswire

"Smartwatch maker Garmin has obtained the decryption key to recover its computer files from a ransomware attack last Thursday, Sky News has learned. Last week, Garmin's services were taken offline after hackers infected the company's networks with a ransomware virus known as WastedLocker."
Source: Cyber Security Review

Has Canon Suffered A Ransomware Attack? 10TB Of Data Alleged Stolen: Report

"Canon suffered an outage impacting users of the image canon photo storage site. Now, it has been reported that it may have been hit by a ransomware attack involving the theft of 10TB of data across multiple services."
Source: Forbes

COVID-19



Cybercrime ramps up amid coronavirus chaos

"Data breaches have grown in intensity and frequency in recent months as cybercriminals take advantage of coronavirus confusion. Among the most common types of attacks are ransomware, destructive attacks and island hopping."
Source: CNBC

Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since Covid-19

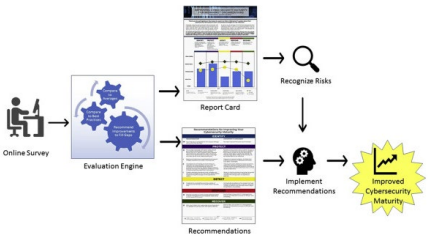
"The World Robotics report shows that Europe is the region with the highest robot density globally, with an average value of 114 units per 10,000 employees in the manufacturing industry. For more facts about robots watch IFR´s video news about Europe in one minute."
Source: PRnewswire

INTERPOL report shows alarming rate of cyberattacks during Covid-19

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

RISK MANAGEMENT



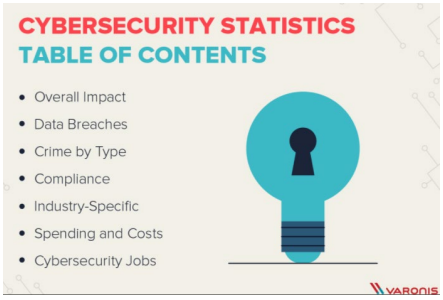
Calculated risk? A cybersecurity evaluation tool for SMEs

"Small and medium-sized enterprises (SMEs) are among the least mature and most vulnerable in terms of their cybersecurity risk and resilience. In this article, we describe a methodology developed using the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) as a starting point. The NIST CSF does not meet all the needs of the SME IT leader, but it offers a solid foundation for a useful evaluation and recommendation methodology. We propose an SME cybersecurity evaluation tool (CET) that consists of a 35-question online survey to be completed by IT leaders to self-rate their maturity within the five NIST framework categories: identify, protect, detect, respond, and recover. We outline this approach to cybersecurity risk management before discussing its effectiveness and implications for practitioners."
Source: Business Horizons

Risk based approach in scope of cybersecurity threats and requirements

"Paper is focused on theoretical and practical considerations related to risk management and cyber security based on the cyber kill chain concept introduced by Lockheed Martin. Proposed approach of cyber risk management embedded on the cyber kill chain is new and not reflected in the available literature. Proposed risk management process of identifying, analyzing, evaluating, assessing and ultimately responding to cyber threats and monitoring risks in

CYBER AWARENESS



110 Must-Know Cybersecurity Statistics for 2020

"Cybersecurity issues are becoming a day-to-day struggle for businesses. Recent trends and cybersecurity statistics reveal a huge increase in hacked and breached data from sources that are increasingly common in the workplace, like mobile and IoT devices.
Additionally, recent security research suggests that most companies have unprotected data and poor cybersecurity practices in place, making them vulnerable to data loss. To successfully fight against malicious intent, it's imperative that companies make cybersecurity awareness, prevention and security best practices a part of their culture."
Source: Varonis

IBM: 2020 Cyber Resilient Organisation Report

"Being the target of a cyber attack is a statistical certainty for enterprises of all sizes. Most people understand this now and organisations have, for the most part, become more effective and diligent about planning for attacks and detecting them when they happen. But according to this survey-based report, conducted by the Ponemon Institute, the past five years have actually seen a reduction in organisations' ability to contain attacks while they're happening."
Source: Science Direct

MALWARE AND RANSOMWARE

Fidelis Threat Intelligence Report

"The Fidelis Threat Research Team (TRT) collects a wealth of security and threat intelligence information for security professionals interested in the

"An INTERPOL assessment of the impact of COVID-19 on cybercrime has shown a significant target shift from individuals and small businesses to major corporations, governments and critical infrastructure.

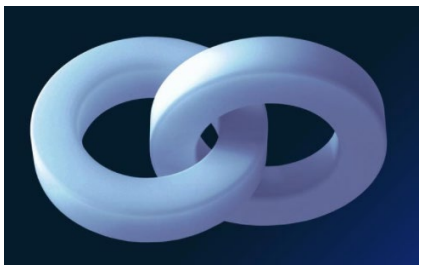
With organizations and businesses rapidly deploying remote systems and networks to support staff working from home, criminals are also taking advantage of increased security vulnerabilities to steal data, generate profits and cause disruption."
Source: Interpol

How to approach cybersecurity in the post-COVID-19 world

"COVID-19 is changing everything. Along with social distancing, obsessive sanitisation, broken supply chains, fragmented workforces and the rise of video meetings, the pandemic is driving acute systemic changes in consumer and business behavior. These changes are causing an outbreak of new and unanticipated business moments. The resolve to transform is palpable.

Businesses know they must rapidly innovate, take advantage of new digital tools and leverage cloud services to emerge from the crisis ahead of their competitors with momentum for the long-term transformation of their business in the altered global landscape.

This innovation is good news, but it is coming at a cost. As digital spreads its roots deeper, it also increases the risk and impact of cyberattacks."
Source: World Economic Forum



A dual cybersecurity mindset for the next normal

"As companies extend commitments to remote workforces, cybersecurity teams need to address new risks while helping create business value in the next normal."
Source: McKinsey

A 10-point plan for addressing WFH cybersecurity challenges

"Back in early Spring, ensuring users could access the necessary applications securely from home was priority No. 1. Now, 3-4 months later, work from home looks like it's here to stay … for a while, at least. Here's your

each stage of the cyber kill chain is the heart of proposed approach. The approach may be used in organizations which are going to implement security mechanisms to align with the in-force requirements or to reduce cyber risks to accepted level. The process of the risk assessment introduced by the authors follows with the description of the example risk evaluation method based on a continuous-time Markov chain as a model of the cyber kill chain."
Source: Science Direct

CYBER AWARENESS

Riskio: A Serious Game for Cyber Security Awareness and Education

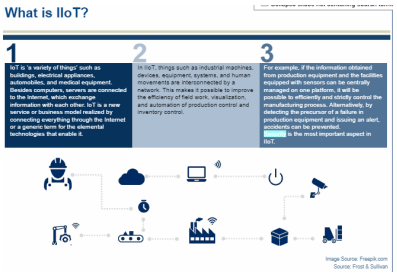
"Cyber attacks are increasing in number and sophistication, causing organisations to continuously adapt management strategies for cyber security risks. As a key risk mitigation policy, organisations are investing in professional training courses for their employees to raise awareness on cyber attacks and related defences. Serious games have emerged as a new approach that can complement instruction-led or computer-based security training by providing a fun environment where players learn and practice cyber security concepts through the game. In this paper we propose Riskio, a tabletop game to increase cyber security awareness for people with no-technical background working in organisations. Riskio provides an active learning environment where players build knowledge on cyber security attacks and defences by playing both the role of the attacker and the defender of critical assets in a fictitious organisation."
Source: Science Direct

When believing in technology leads to poor cyber security: Development of a Trust in Technical Controls Scale

"While technical controls can reduce vulnerabilities to cyber threats, no technology
provides absolute protection and we hypothesised that people may act less securely if

state of global cybersecurity. The report gives insights into malware, ransomware, and other cyber threats, as well as recommendations from the Fidelis TRT."
Source: Fidelis Security

IoT



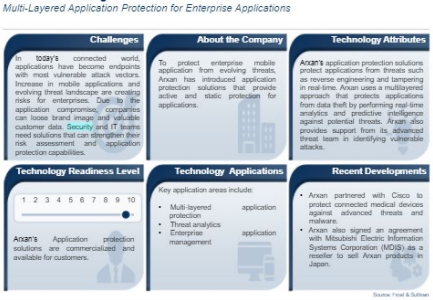
Industrial Internet of Things (IIoT) in Cyber Security in Japan, 2020

"Of late, cyber space has been driving socio-economic activities, as a fall-out of the unification of cyber space and real space including entire industries, especially manufacturing industries, which is termed Industrial Internet of Things (IIoT).

The vast amount of data produced by sensors and devices every second from all over the world is being stored and analyzed in cyber space globally. In addition, real-time delivery of new products and services that use data to provide added value is evolving in a number of domains. In such circumstances, cyber space and real space can no longer be considered separately.

Modern operations spread across complex information technology (IT) and operational technology (OT) infrastructures. These include several devices connected via IIoT. This leads to new challenges in protecting the industrial environment. To protect this complex attack surface, many industrial organizations are trying to integrate IT and OT operations."
Source: Frost & Sullivan

CYBER SECURITY TECHNOLOGY



Recent Innovations in Cyber Security Technology

"This Cyber Security TechVision Opportunity Engine (TOE) provides a snapshot on emerging cyber security solutions powered by artificial

to-do list for the next 6 months and beyond."
Source: CIO

IoT

Are newer medical IoT devices less secure than old ones?

"Legacy medical IoT devices may lack security features, but newer ones built around commodity components can have a whole different set of vulnerabilities that are better understood by attackers."
Source: Network World

New method to defend against smart home cyber attacks developed by Ben-Gurion University researchers

"Instead of relying on customers to protect their vulnerable smart home devices from being used in cyberattacks, Ben-Gurion University of the Negev (BGU) and National University of Singapore (NUS) researchers have developed a new method that enables telecommunications and internet service providers to monitor these devices."
Source: EurekaAlert!

IoT roundup: A wide-scale security flaw and energy-sector botnets

"One of the most fascinating parts of the IoT space is seeing new applications for what is, at core, a fairly simple technology spring up every week. Everything from rat traps to race cars to smart buildings to wildlife photography can fall, in some way, into the general category of IoT.

A new report from UK-based IDTechEx details one such growing market – the monitoring and measurement of water quality and delivery systems. The research firm said that the market just for sensors in water pipes is set to reach $3.5 billion in revenues in the next decade, and that the technology to help keep drinking water safe and available is relatively mature already."
Source: Insider Pro

they place unwarranted trust in these automated systems. This paper describes the
development of a Trust in Technical Controls Scale (TTCS) that measures people's faith
in four of these technical controls."
Source: Computers and Security

Developing Cybersecurity Culture to Influence Employees Behavior: A Practice Perspective

"This paper identifies and explains five key initiatives which three Australian organizations have implemented to improve their respective cyber security cultures. The five key initiatives include: identifying key cyber security behaviors, establishing a 'cyber security champion' network, developing a brand for the cyber team, building a cyber security hub, and aligning security awareness activities with internal and external campaigns. These key initiatives have helped organizations exceed minimal standards-compliance to create functional cyber security cultures. This paper discusses why these initiatives have been effective and provide practical guidance on their integration into organizational security program."
Source: Computers and Security

NETWORK SECURITY

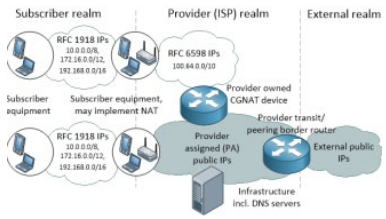


Fig. 1. *Classification of IP addresses*

Cyber-security research by ISPs: A NetFlow and DNS Anonymization Policy

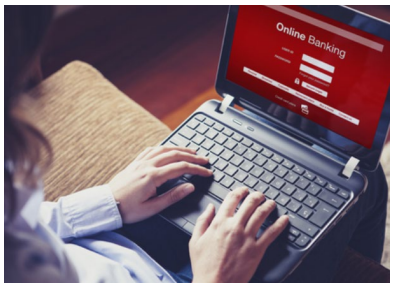
"Internet Service Providers (ISPs) have an economic and operational interest in detecting malicious network activity relating to their subscribers. However, it is unclear what kind of traffic data an ISP has available for cyber-security research, and under which legal conditions it can be used. This paper gives an overview of the challenges posed by legislation and of the data sources available to a European ISP. DNS and NetFlow logs are identified as relevant data sources and the state of the art in anonymization and fingerprinting techniques is discussed. Based on legislation, data availability and privacy considerations, a practically applicable anonymization policy is presented."
Source: IEEE Xplore

intelligence, cloud, machine learning, and IoT innovations that help companies protect from threats, data breaches, phishing attacks, and defend against modern attacks residing within cloud, endpoints, and various network layers."
Source: Frost & Sullivan

Global; Technology Innovation Leadership Award - Cyber Risk Modeling Industry

"Companies need to protect their digital ecosystem against multiple threats, and while attackers need to find only one security flaw, companies must conduct an effective, consistent data-driven security program to prevent a cyber disaster. Small and large companies suffer from cybersecurity damages, and the financial impact of such incidents may cause business operations to cease. Cyber damages have grown exponentially in the last decade as a broadening digital and Internet-connected ecosystem raises a business's cyber risk. Even in cases where protection measures and mechanisms are deployed, the ever-evolving cyber risk posed to information technology (IT) systems, employees, and third-party vendors threaten an organization's business operations. Ultimately, a business is the custodian of its data and the data of its customers. Losing such data may result in financial fines, loss of business, and, in some cases, business closure."
Source: Frost & Sullivan

DATA SECURITY



Emotet Surfaces With 'Red Dawn' Threat| Cyware Alerts - Hacker News

"Emotet malware operators are apparently on a continuous mission of enhancing the notorious malware family. They have recently come up with a new way to target their victims into opening up malicious documents."
Source: Cyware

What is doxing? Weaponizing personal information

"Doxing victims find their home address, social security number, and more posted online, typically because someone wanted to intimidate, humiliate, or harass them. Here's what you need to know."
Source: CSO

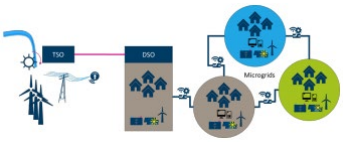
Phishing Attack Used Box to Land in Victim Inboxes

"A phishing attack targeting government and security organizations used a legitimate Box page with Microsoft 365 branding to trick victims."
Source: Cyware

Twitter: Android users' direct messages may have been exposed

"Twitter disclosed a new security vulnerability that may have exposed the direct messages of users who access the service using Android devices. Specifically, the vulnerability could have exposed the private data of Twitter users running devices with Android OS versions 8 and 9."
Source: CNBC

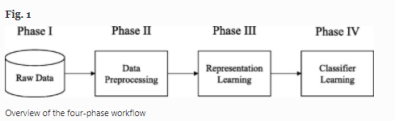
OUTLOOK



What Could Possibly Go Wrong? Smart Grid Misuse Case Scenarios

"The modernisation of the power grid is ongoing, and the level of digitalisation of the power grid in, say, ten years may be quite different than today. Cyber security needs will change correspondingly. In this paper we utilise a qualitative research approach to explore misuse cases related to three main areas of modernisation that we envision for the next ten year period: 1) managing flexibility in the TSO-DSO relation, 2) smart distribution grids, and 3) microgrids. The misuse cases represent potential security challenges to be considered when working on modernising the grid, however they are not exhaustive. The misuse cases presented in this paper can contribute to identifying security requirements, thus reducing associated cyber risks, and assist in development of new cyber security mechanisms for the next-generation power grid employing digitally-connected, self-healing, and automation characteristics."
Source: 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)

DEEP LEARNING



Using deep learning to solve computer security challenges: a survey

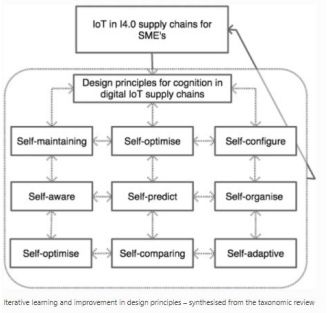
"Although using machine learning techniques to solve computer security challenges is not a new idea, the rapidly emerging Deep Learning technology has recently triggered a substantial amount of interests in the computer security community. This paper seeks to provide a dedicated review of the very recent research works on using Deep Learning techniques to solve computer security challenges. In particular, the review covers eight computer security problems being solved by applications of Deep Learning: security-oriented program analysis, defending return-oriented programming (ROP) attacks, achieving control-flow integrity (CFI),

defending network attacks, malware classification, system-event-based anomaly detection, memory forensics, and fuzzing for software security."
Source: Cyber Security

Conceptualisation of Cyberattack prediction with deep learning

"The state of the cyberspace portends uncertainty for the future Internet and its accelerated number of users. New paradigms add more concerns with big data collected through device sensors divulging large amounts of information, which can be used for targeted attacks. Though a plethora of extant approaches, models and algorithms have provided the basis for cyberattack predictions, there is the need to consider new models and algorithms, which are based on data representations other than task-specific techniques. Deep learning, which is underpinned by representation learning, has found widespread relevance in computer vision, speech recognition, natural language processing, audio recognition, and drug design. However, its non-linear information processing architecture can be adapted towards learning the different data representations of network traffic to classify benign and malicious network packets."
Source: Cyber Security

SECURITY ANALYTICS



Iterative learning and improvement in design principles – synthesised from the taxonomic review

Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains

"Digital technologies have changed the way supply chain operations are structured. In this article, we conduct systematic syntheses of literature on the impact of new technologies on supply chains and the related cyber risks. A taxonomic/cladistic approach is used for the evaluations of progress in the area of supply chain integration in the Industrial Internet of Things and Industry 4.0, with a specific focus on the mitigation of cyber risks."

Source: Cyber Security