The Cybersecurity Renaissance: Security Threats, Risks, and Safeguards

Dr. San Murugesan
Adjunct Professor, Western Sydney University
san@computer.org

We're entering a new digital era driven by significant technological advances and widespread adoption of digital technologies and applications by business, industry, government and individuals. While the new digital era offers us several benefits and presents new opportunities, it faces increased and sophisticated cybersecurity threats and comes with risks. Phishing, ransomware, and other forms of cyberattacks are growing, exposing the personal data of millions of people and costing the economy huge sums of money (billions of dollars) every year. These threats and risks are compounded with newer threats and concerns as we begin to embrace artificial intelligence (AI), machine learning (ML), robo-advisors, and the Internet of Things (IoT) and adopt autonomous systems for a range of tasks that can make and execute decisions with little human intervention.

The cybersecurity landscape continues to change significantly posing major challenges to IT professionals, and businesses. Cybersecurity attacks have increased in number, severity and sophistication, and some of them are often coordinated. Increasing number of cybercriminals and state-sponsored actors target organizations to steal valuable data and disrupt their working and try to sabotage operation of national critical infrastructure. Cyberattackers also monetize their threats. Cyberattacks can be devastating to the affected organizations and individuals. The biggest threat to mankind is cyberthreats, even more so than nuclear weapons threats, cautions multi-billionaire investor Warren Buffett.

There is now growing concern and renewed interest on security of digital systems and their numerous applications on which we highly rely on. It is important that we constantly improve our understanding of how we may detect, respond, learn from security breaches, and develop and implement new security measures. Despite significant research and development, availability of established security practices and techniques, reports on security incidents and failures and information on common known vulnerabilities, security breaches continues occur and securing digital systems and applications remains a key challenge for security professionals and organizations. Besides hardware and software vulnerabilities, human vulnerabilities remain the weakest link in cybersecurity and are hard to mitigate.

To comprehensively and holistically address cybersecurity issues and provide secure and safe applications now and in the future, we need to address several questions such as:

- What can we expect on the cybersecurity front now, and in the near future?
- What are the trends and activities most likely to affect organizations, governments, and individuals?
- Can we secure our growing vast digital landscape, and how? Will our digital assets be safe and secure, and data and information be free from cyberbreaches? What might we need to do safeguard our cybersystems?
- How might we effectively address emerging cyber-threats that automation systems might encounter, including obscure, new, and unknown (future) threats that could be serious or even catastrophic?
- If don't or can't secure them adequately, how might security incidents impact us?
- Are the traditional techniques adequate to address the potential new security threats? If not, what might be new approaches and techniques that we could adopt?

This article examines the looming cyberthreat, examines new cyberthreats and presents a glimpse of cybersecurity renaissance. It also emphasizes that IT professionals, organizations and governments must take adequate steps to bolster security of digital systems and applications that we rely on.

SECURITY THREATS: AN OVERVIEW

Cybercriminals target and attack different types of digital assets – data, infrastructure, and applications and people like IT administrators and users – by several ways. Table 1 presents a brief summary of various threats digital systems and applications face. For a detailed account of potential threats digital systems face, refer to the recent European Union Agency for Network and Information Security (ENISA) Threat Landscape Report 2018 [1]. Security professionals and organisations should examine potential threat they might face, assess impact of those threats and implement adequate measures to address the critical ones.

Table-1: A brief outline of security threats and controls

Asset	Threats	Controls
Data	• Data breach • Misuse or manipulation of information • Corruption of data	• Data protection (encryption) • Boundary defense • Data-recovery capability
Infrastructure	• Denial of service • Manipulation of hardware/software • Botnets • Malware • Network intrusion	• Secure configuration • Network controls (configuration, ports) • Continuous vulnerability assessment • Continuous monitoring of emerging attacks. • Control of privileged access
Applications	• Manipulation of software • Unauthorised installation of software • Misuse of data or applications • Denial of service	• Application software security • Continuous vulnerability assessment • Continuous monitoring of emerging attacks. • Email/browser protection
People	• Identity theft • Abuse of authorisation • Man-in-the-middle • Social engineering	• Controlled access • Account monitoring • Background screening • Security awareness and security skills training
Others (organisation, individuals)	• Ransomware	

Source: McKinsey & Co, The SANS Institute, and ENISA

Threat Agents

Based on their motives, activities and other factors and on the threats faced in 2018, ENISA classified top threat creators, also called threat agents, as [ENISA 2019]:

- Cybercriminals
- Malicious and negligent insiders – users, privileged users and service providers or contractors
- Nation States
- Corporations that try to obtain competitive knowledge from competitors.
- Hacktivists
- Cyberfighters or cyberterrorists
- Script kiddies

Now a days attackers are not just amateurs, they are professionals with high degree of expertise and skills. They are also innovative in advancing threats and use sophisticated tools for launching attacks. Major threats presented by each of these threat agents are highlighted in Table 2, and discussed in detail in [1].

Attack Vectors

An attack vector is a "path or means by which a threat agent can gain access to a computer or network server, abuse weaknesses or vulnerability on assets (including human) in order to achieve a specific outcome." It gives a structured way for threat analysts to describe a threat agent's behaviour and defenders to implement appropriate defences, following a "Course of Action." To understand various tactics, techniques and procedures (TTP) used by threat agents, description of an attack vector is essential. Table 3 provides a categorization of the most predominant and noteworthy attack vectors (observed by ENISA).

Table 2: Top threats and their creators

Threat	Threat creators						
	Cybercri-minals	Insiders	Nation states	Corporati-ons	Hacktivists	Cyber-terrorists	Script kiddies
Malware	√	√	√	√	√	√	√
Web-based attacks	√		√	√	√	√	√
Web application attacks	√		√	√	√	√	√
Denial of Service	√		√	√	√	√	√
Botnets	√		√	√	√	√	√
Phishing	√	√	√	√	√		√
Spam	√	√	√	√			
Ransomware	√	√	√	√			√
Insider threat	√	√	√	√		√	
Physical manipulation, damage, theft, loss	√	√	√	√	√	√	√
Exploit kits	√		√	√			
Data breaches	√	√	√	√	√	√	√
Identity theft	√	√	√	√	√	√	√
Information leakage	√	√	√	√	√	√	√
Cyber espionage		√	√	√			

Source: ENISA Threat Landscape Report 2018

Security Attacks and Failures Are Real and Severe

Cyberattacks and security failures are real. Despite advances in security measures, significant high-profile security attacks and data breaches continue to occur causing major concerns. For example, there were several major security failures - breaches, data exposures, ransomware attacks, state-sponsored campaigns, and general hacks, last year. The following are few of the major failures [2]:

- One of the largest data breaches in history is the Marriot incident in which 500 million travellers who made a reservation at a Starwood hotel since 2014 had their data compromised. Reports say state-sponsored Chinese hackers were behind the attack, this attribution, however, has not been officially confirmed.
- Facebook encountered a data breach in which attackers gained access to 30 million accounts by stealing "user authorization tokens" – essentially stealing access.
- A ransomware attack locked down the City of Atlanta's digital systems, destabilizing municipal operations. The recovery took months and costed millions of dollars. The worldwide WannaCry ransomware cyberattack in 2017 targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. There were a series of successful follow-up ransomware attacks targeting high-profile victims.
- Before the 2018 Winter Olympics opening ceremony, Russian hackers orchestrated a hack that crippled the event's IT infrastructure, knocking out Wi-Fi, the Olympics website, and network devices in the process as retaliation for the country's doping ban from the games.
- A major data breach impacted British Airways reservation system. Names, addresses, email addresses, and sensitive payment card details of 380,000 reservations made between August 21 and September 5 of this year were stolen in the breach. Airline data is a particularly valuable target for hackers, because they hold both personal and financial data, as well as travel data and passport numbers.
- Google discovered a bug in its social network Google+ that had exposed 500,000 users' data for about three years.
- Hackers didn’t spare even small and medium enterprises. SMEs are not only just as vulnerable to a breach; the consequences of an event can be catastrophic. According to data gathered by the Ponemon Institute, in 2017, 61% percent of small businesses have experienced a cyberattack. Verizon's 2018 Data Breach Investigations Report categorises 58% of malware attack victims to small businesses. A representative 2018 survey of 400 senior SME

business and IT leaders in Australia revealed 60% of SMEs have experienced a cyber incident over 12 months and 30% didn't know which data files are affected after a breach [3]. Worryingly, 28% of SMEs took no action following a cyber incident.

- According to the FBI, Russian persistent threat actor Sofacy group, infected more than 500,000 home office routers and network attached to storage devices worldwide to remote control them.

Table 3: Common Attack Vectors

Attacking the human element

- Social engineering
- Phishing/spear-phishing/business email compromise(BEC)/whaling/spam through email/social media/online services
  - Malicious attachments in emails; Malicious URLs in emails and social media; Microsoft office attack vectors (macros etc)
- Social media messaging services
- Scams
  - Customer/tech support scams; Phone scams (Vishing) ; SMS scams (Smishing)

Web and browser based attack vectors

- Drive-by downloads
- Drive-by mining (cryptojacking)
- Malicious scripts/URLs

Exploit-kits

- Malvertising
- Web application attacks (SQL injection)
- Browser based attacks
- Malicious browser add-ons (updates)
- Watering hole attacks
- Mouse hovering

Internet exposed assets

- Unprotected assets exposed on the internet
- Default/weak service credentials
- Password reuse

Exploitation of vulnerabilities/misconfigurations and cryptographic/network/security protocol flaws

Supply-chain attacks

- Software manipulation or third-party API/software
- Hardware manipulation

Network propagation/lateral movement

Active network attacks

- DNS attacks (DNS hijacking/poisoning)

Privilege or user credentials misuse/escalation

- Access token manipulation
- Sticky-keys
- Account manipulation –

Fileless or memory-based attacks

- Malicious PowerShell and XSL scripts

Misinformation/Disinformation

- Online trolling
- Spread of fake news online
- Abuse of social media and search engines algorithms; Illegitimate use of social bots

---

What's Ahead?

What can we expect on the cybersecurity front in 2019 and in the near future? Cyberthreats will be more rampant – several threats will be deployed more aggressively on more fronts. "Target zone" of cyber attacks or threat landscape will be bigger than what is now, as companies increasingly pursue digitization to drive efficiency, reduce costs and build data-driven businesses, and more people use online services. Ransomware attacks will increase. Compounding these is new threats posed by the use cyberphysical system, AI, machine learning, and autonomous systems. Hackers will employ

advanced tools to generate sophisticated security attacks that are new and evade detection, and there will be significant increase in nation-state attacks.

NEWER CYBERTHREATS

The already complex cybersecurity landscape now faces several new threats: those emerging from the IoT, cyber-physical systems and AI and machine learning systems, cryptojacking, formjacking, software update supply chain attacks, rogue robots, and attacks on small clouds and managed IT services. Cyber-defenders should be paying attention to new and known older cyber threats.

The IoT and Cyber Physical Systems

IoT devices have become indispensable, bringing unprecedented levels of convenience and making our lives easier and more enjoyable. In the future it's likely that almost every device in our homes could be equipped with sensors and connected to the internet. Driven by ongoing advances in sensors, the IoT, cloud, fog and edge computing, data storage, (big) data analytics and communications, cyberphysical systems (CPSs) are growing in number and capabilities and are being deployed in several domains offering convenience and several benefits. Within the next three years, 30 billion to 50 billion new IoT devices are estimated to be part of these systems. But CPSs are a major security risk and challenge.

The security landscape of CPSs is vast and more vulnerable to malicious attacks and hacks as these systems use cheap unsecure sensing and communication devices. IoT devices are notorious for their lack of security, leaving these devices exposed to attacks from the outside. Most IoT manufacturers neglect security aspect in the rush to get their products to the market or find implementing strong security features expensive and time-consuming and choose not to implement them. Within the next three years, 30 billion to 50 billion new IoT devices are estimated to be part of these systems. As the number of IoT devices increases, so does the number of cyberattacks directed at them. As communication networks, computing platforms and mobile devices are relatively better protected, cybercriminals are targeting softer targets, like IoT devices.

The IoT is vulnerable to distributed denial-of-service (DDoS) attacks [4]. In 2016, the Mirai attack showed the destructive potential of a botnet on IoT devices and how dangerous unsecured IoT devices can be. In this most disruptive DDoS attack in history, hackers gained control of over 100,000 poorly secured IoT devices and used them to launch a sustained assault on the leading DNS provider Dyn, taking down numerous important websites such as Twitter, Netflix, Amazon and CNN. According to the Nokia's Threat Intelligence Report 2019, in 2018 IoT, botnet caused 78% of malware incidents in communication service provider (CSP) networks in 2018.

Hackers are also increasingly using IOT to attack consumers directly and steal their personal data or use their systems to mine cryptocurrencies. Safety- and mission–critical CPSs raise heightened security and privacy concerns as attackers can compromise or take over portions of the entire system. Exploiting billions of poorly secured IoT devices nation-states attacks will increase.

A new set of approaches, tools, and techniques is needed to secure CPSs that continue to influence us significantly. Governments are considering regulatory measures to address IoT security risks. California recently passed an IoT cybersecurity bill, which will require manufacturers to equip all connected devices with reasonable security features.

Software Update Supply Chain Attacks

'Software update supply chain attack' implants a piece of malware into an otherwise legitimate software package. This can occur during production at the software vendor, at a third-party storage location, or through redirection. This is subversion of software development process. For further information on some recent attacks and how you can manage them, refer to [5].

There has been surge in supply chain attacks in the last two years and this trend will continue as they are attractive to cybercriminals since [5]:

- They allow cyber criminals to infiltrate well-protected organizations by exploiting an already trusted channel.
- The number of infections can grow quickly due to automatic updates.
- They can allow attackers to target specific regions or sectors—as was the case with the well-known Petya/NotPetya attacks. An accounting software that is primarily used in Ukraine was compromised to gain access to victims' machines.
- They can target specific isolated targets, such as those in industrial environments.
- They can also make it more difficult for victims to figure out how attackers got onto their systems as trusted processes are abused.

Cyber-defenders need to anticipate and address adequately software update supply chain attacks.

AI and ML: Solution or Threat?

Artificial intelligence and machine learning are both a saviour and a threat to cybersecurity. They can be used to defend security attacks as well as to create new kinds of attacks and aid cybercriminals and hackers.

A significant feature of a ML algorithm is their ability to quickly find normal patterns across large data sets and detect anomalies or abnormal patterns if any. In its simplest form, it can create a baseline model of what's normal in an environment and then flag and investigate anomalies to that baseline, which could potentially be a threat. This feature can be used in various environments, from individual residence (smart home) with a few IoT devices to a large business. Thus, ML algorithms can be used to learn about potential cyberattacks, and to anticipate and identify them in real time.

They can also be employed to detect fake or edited images and videos as two start-ups have recently demonstrated. A machine learning algorithm uses tweets to spot security flaws [6]. In the coming years, defenders will depend increasingly on AI to counter attacks and identify vulnerabilities.

The Dawn of Adversarial AI

Like defenders, attackers will also exploit AI and ML and use them to aid assaults and create more sophisticated attacks. We are seeing the emergence of a class of attacks known as 'Deep Attacks', which use AI-generated content to evade AI security detection and controls. For example, consider rogue AI-driven chatbot. Cybercriminals and hackers can create a malicious chatbot that tries to socially engineer victims into clicking links, downloading files or sharing private information. Attackers are also likely to leverage web application flaws in legitimate websites to insert a malicious chatbot into a site that doesn't have one.

Consider another example of deep fake. With a typical personal computer and a good graphics card, it's now possible to easily create a fake video or audio message that is incredibly difficult to distinguish from the real thing. Hackers are now able to use a highly realistic fake video and audio, either to reinforce instructions in a phishing e-mail or as a standalone phishing video. Cybercriminals could also use the technology to manipulate stock prices by, say, posting a fake video of a CEO of company announcing that a company is facing a financial problem or some other crisis, or had huge growth and profits. There's also the danger that deepfakes could be used to spread false news in elections. In the future, we'll see deep attacks deployed more commonly in an attempt to evade both human detection and smart defences.

Still worse, cybercriminals could target data sets used to train learning models and poison them — for instance, by switching labels on samples of malicious code to indicate that they are safe rather than suspect [7].

Attacks on Small Cloud Computing Vendors

While big cloud service providers like Amazon, Microsoft and Google can afford to invest heavily in cybersecurity defense and employ some of the best talent in the field, smaller cloud vendors and IT service providers can't afford to implement high security and are vulnerable to security breaches. It's more likely that hackers will target them. In a recent incident, hackers sneaked into the computer systems of a company that managed IT for other firms and were allegedly able to gain access to the computers of 45 companies around the world, in industries from aviation to oil and gas exploration.

Attacks on Robots

While industrial robots boost productivity and efficiency, they're vulnerable to hacks and the risk levels are rising as more robots move from being offline and isolated to being internet-connected machines, often working alongside humans. Factories, hospitals and other robot users often lack sufficient levels of defense against a digital attack, and damage that a hacked robot can cause could be huge and even catastrophic.

Cryptojacking

Cryptojacking is a quiet, more insidious method of steal resources from unsuspecting victims for monetary benefits, and we're likely to see surge in incidences of this type attack.

Formjacking

Formjacking is essentially virtual ATM skimming. In Formjacking cyber criminals inject malicious code into retailers' websites to steal shoppers' payment card details. On average, more than 4,800 unique websites are compromised with formjacking code every month globally. Symantec blocked more than 3.7 million formjacking attacks on endpoints in 2018, with nearly a third of all detections occurring during the busiest online shopping period of the year – November and December [8]. Formjacking is simple and will become more frequent.

Human Error and Human Factors in Cybersecurity

Most organizations tend to focus on external threats, but insider threats are increasingly taking center stage. Insider threats come not only from the malicious insider, but also from infiltrators and unintentional insiders as well.

According to a research study, the majority of information security attacks stem from human error, not from malicious intent. It's imperative that organizations put together a training plan for new employees who are not up to speed on cyber security basics. Employee education and training will help mitigate attacks caused by human error. However, most security awareness training, often conducted by IT, is focused on information security as a topic and doesn't emphasize the human element of the risk sufficiently. Effective training includes content that addresses the threat's psychological, behavioural, and economic aspects, with practical advice on how to spot scams and protect data.

Employee education and applying common sense practices needs to be a priority at companies.

CYBERSECURITY STRATEGY

Organisations should develop and successfully implement an appropriate cybersecurity strategy, which is a good foundational step for obtaining the level of cybersecurity necessary to protect their business, employees, customers and reputation. When done well, it's one of the most worthwhile investments of time, effort and money an organization can make. As the threats will only grow in size, scale and sophistication, with a proactive cybersecurity strategy, businesses can stay one step ahead of attacks.

Cyber resilience is the ability to prepare for, respond to, and recover from cyber security incidents. A cyber-resilient organisation gets protected from cyber risks, defends against and limits the severity of attacks, and ensures that business operations continue to function in the event of a disruption.

In developing a cybersecurity strategy to be cyber-resilient, 1) set out clear objectives, 2) identify your assets to establish cybersecurity priorities, 3) determine where you're vulnerable, 4) examine and plan to put right technology and systems in place, 5) employ right personnel to look after organisation's security needs, and 6) assess the overall organization's cybersecurity awareness and implement requisite awareness and training programs, and periodically reassess and update your cybersecurity strategy. Also consider cyber-insurance, if required.

CYBER-INSURANCE

To protect themselves from financial effects of an attack, businesses can invest in cyber-insurance. Cyberinsurance providers require that companies demonstrate strong cybersecurity to attain cyber-insurance coverage. Businesses use insurance to control risk, and insurers limit their exposure to risk by imposing standards and constraints. Though cyber-insurance has been available since the 1990s, it has not yet taken off and faces some challenges.

As outlined by Nir Kshetri in a recent article [9], "Cyber-insurance provides coverage for the theft or loss of first-party and third-party data, as well as support services. For the loss or theft of first-party data, an insurer may cover expenses related to notifying clients regarding the data breach, extortion, and launching a public relations campaign to restore the company's reputation following a cyberattack-led negative publicity. Third-party cyber-insurance protects a firm from being accused in case of a breach. Third-party coverage includes claims related to unlawful disclosure of a third-party's information and infringement of intellectual property rights. It may also protect if an insurance holder's weak cybersecurity practices result in passing malware or virus to another user. Support services can help limit losses after a cyberattack. They cover expenses such as those related to public relations, IT forensics, and hiring experts in crisis management."

Actuarially estimating the likelihood of cyberattacks and the total anticipated costs of such attacks remains a challenge. The lack of relevant data results in an inaccurate assessment of cyber risks and higher premiums, and stalls adoption and growth of cyber-insurance.

The Way Forward For Secured Future

Cybersecurity will continue to be an ever-growing challenge for professionals, IT industry, businesses and government. Cybercriminals will continue to launch more sophisticated attacks, and cybersecurity incidents and breaches can seriously damage a company. Individuals and enterprises need to be more proactive in their security practice, and security risk management must be integral to corporate governance. It also requires constant evaluation and forward thinking solutions development to advanced solutions.

Security is also a concern for governments that are investing in smart city infrastructure. Without adequate security, innocuous items which generally pose no threat can be transformed into something far more sinister — for example, traffic lights that tell cars and pedestrians to go at the same time or changing tracks to put a commuter train on the wrong course.

A survey of Australia SMEs reveals significant perception gap for cyber awareness and preparedness, and most are not well prepared to navigate and manage cyber risks.

Cybersecurity Education

There is global shortage of skilled cybersecurity professionals, and, the number of vacancies just keeps growing. To take advantage of the opportunities, interested people should upskill in relevant areas. This can be achieved by undertaking certification program, specialised educational programs at colleges and universities or self-learning.

Cybersecurity Research

Cybersecurity is an active area of research and development. In addition to traditional and new technical areas of investigation and development, we need more research into psychology and criminal motivations of hackers and cybercriminals. We need to broaden our research.

The new reality of the digital world is all businesses – from small and medium businesses to big business and corporations, industries of all types and government agencies must place a higher priority on implementing cybersecurity measures to address not only today's threats but tomorrow's as well.

References

1. ENISA Threat Landscape Report 2018. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018
2. Ily Hay Newman, The Worst Hacks of 2018, Wired, 31 December 2018. https://www.wired.com/story/worst-hacks-2018-facebook-marriott-quora/
3. Too Small To Fail?, Australia SME Cyber Preparedness Report, 2019. https://www.chubb.com/au-en/articles/too-small-to-fail.aspx.
4. Natalija Vlajic and Daiwei Zhou, IoT as a Land of Opportunity for DDoS Hackers, Computer, vol. 51 July 2018, pp. 26-34.
5. Software Update Supply Chain Attacks: What You Need to Know, October 2017, https://medium.com/threat-intel/software-update-supply-chain-attacks-what-you-need-to-know-f5bd3ba9718e.
6. Andy Greenberg, Machine Learning Can Use Tweets To Spot Critical Security Flaws. Wired, 7 March 2019, https://www.wired.com/story/machine-learning-tweets-critical-security-flaws.
7. Martin Giles, AI for cybersecurity is a hot new thing—and a dangerous gamble, MIT Technology Review, August 11, 2018 . https://www.technologyreview.com/s/611860/ai-for-cybersecurity-is-a-hot-new-thing-and-a-dangerous-gamble/
8. Cyber Criminals Cash in on Millions with Formjacking: Symantec, 21 February 2019. https://www.dqindia.com/cyber-criminals-cash-millions-formjacking-symantec/
9. Nir Kshetri, The Economics of Cyber-Insurance, IT Professional, vol. 20, no.3, Nov.-Dec. 2018, pp. 9-14. https://www.computer.org/csdl/magazine/it/2018/06/08617758/17D45Xh13rr

For further reading

Special issues on cybersecurity (open access):

1. Security and Privacy, ComputingEdge, Jan 2018, https://ieeecs-media.computer.org/assets/pdf/ce-jan18-final.pdf
2. Cybersecurity, ComputingEdge, Oct 2017, https://ieeecs-media.computer.org/assets/pdf/ce-oct17-final.pdf.
3. Security, ComputingEdge, Feb 2017, https://ieeecs-media.computer.org/assets/pdf/ce-feb17-final.pdf.
4. Security, ComputingEdge, Nov 2016, https://ieeecs-media.computer.org/assets/pdf/ce-nov16-final.pdf.
5. Cybersecurity, Computing Edge, October 2015, https://ieeecs-media.computer.org/assets/pdf/ce-oct15-final.pdf.

About the Author

Dr. San Murugesan is an Adjunct Professor in the School of Computing and Mathematics at Western Sydney University, Australia. He has over four decades of experience in both industry and academia, and his expertise and interests include AI, the Internet of Everything, cloud computing, green computing, and IT applications. He offers certificate training programs on key emerging topics and keynotes.

Dr Murugesan is former Editor-in-Chief of the IEEE's IT *Professional* and coeditor of a few books, including *Encyclopedia of Cloud Computing* and *Harnessing Green IT: Principles and Practices*. He is a member of the COMPSAC Standing Committee, Golden Core member of IEEE and a fellow of the Australian Computer Society. Dr. Murugesan held various senior positions at Southern Cross University, Australia; Western Sydney University; the Indian Space Research Organization, Bangalore, India; and also served as Senior Research Fellow of the US National Research Council at the NASA Ames Research Center. For further information, visit Web page: http://tinyurl.com/sanbio.

Phishing, ransomware and cryptojacking are among the top cyber security threats and trends for 2019.Â A host of new and evolving cybersecurity threats has the information security industry on high alert. Ever-more sophisticated cyberattacks involving malware, phishing, machine learning and artificial intelligence, cryptocurrency and more have placed the data and assets of corporations, governments and individuals at constant risk.Â â€œHonestly, weâ€™re all at risk,â€ Heather Ricciuto of IBM Security told cnbc.com, â€œwhether youâ€™re talking about a large enterprise or an individual.â€ Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks. February 2016. International Journal of Advanced Computer Research 6(23):31-38.Â There are technical and non-technical. safeguards that can be implemented to lower the risk. associated with social engineering to a tolerable. level.Â technology, cybersecurity, physical. security, risk-based security and security technologies. Paul. previously held the position of Director of Corporate. Meeting cybersecurity risks head on. Every new system, application or network service added comes with potential security vulnerabilities, making cyber protection increasingly more difficult and complex. By confronting the serious network security risks pragmatically, you can reap the benefits while minimizing those risks.To accomplish this, you need a solid cybersecurity plan and the resources to execute it. Handling cybersecurity risk reduction up front typically takes less resources than having to clean up after avoidable cyber attacks.Â global IT community to safeguard private and public organizations against cyber threats. However, the threats to national security have now changed rapidly because of the rapid evolution of technology. The threats are no longer confined to just the physical realm, but also extend to the financial system as well as to networks that now maintain communications. There is also an emergence of â€œsubmarineâ€ threats. Submarine threats refer to the planting of devices that remain hidden over a period of time before surfacing later to wreak havoc. Examples of submarine threats would be the Duku malware and the modus operandi for the February 2015 Carbanak malware attacks against banks globa...Â The approach to cybersecurity is no different to how other national security threats in the physical realm are dealt with. For example, if there is credible. 21.