Technical Education and Skills Development Authority

LABOR MARKET INTELLIGENCE REPORT

ISSUE NO. 4 | SERIES OF 2020

LABOR MARKET
INTELLIGENCE REPORT

CYBERSECURITY

Protecting the Philippines' Digital Future

Issue no. 4 | Series of 2020
Technical Education and Skills
Development Authority (TESDA)

EXECUTIVE SUMMARY

Cybersecurity is a crucial component in today's activities that rely on Information and Communications Technology (ICT). The need to protect one's private information has grown significantly in recent years, not only due to the advances made in ICTs across the globe, but also due to the ongoing COVID-19 Pandemic that has forced virtually everyone to use the online space for most of their activities. Various governments have also passed laws and regulations, further highlighting the demand for competent cybersecurity across the world.

As a skills need, however, cybersecurity is rather unique in that it often revolves around certifications on different types of cybersecurity systems and approaches. The skills imparted are vendor-based as a result, leading to varying levels of competence among prospective cybersecurity professionals rather than a more unified one. Furthermore, the importance placed by countries to cybersecurity also tend to vary, with the Philippines lagging behind the likes of Malaysia and Singapore, for example, in terms of training cybersecurity experts.

TESDA also currently lacks the specific training regulations that can be used to teach cybersecurity skills through a technical-vocational approach, but this is mitigated by the presence of other ICT-related courses that should be used as a baseline for more specialized skills. All in all, Philippine cybersecurity is in its infancy compared to its contemporaries in the world. However, with further research and partnerships with other stakeholders, the Philippines will have the means to meet this skills gap in ICT and be more prepared to face the rigors of a growing computerized and Internet-reliant world.

I. BACKGROUND

The world relies on technology more than ever before, resulting in a surge of digital data creation, transactions, and the like. Today, businesses and governments store a great deal of that data on computers and transmit it across networks to other computers. Devices and their underlying systems have vulnerabilities that, when exploited, undermine the health and objectives of an organization. Thus, the concept of cybersecurity was born.

Technology research and advisory company Gartner defined Cybersecurity as "the combination of people, policies, processes and technologies employed by an enterprise to protect its cyber assets." Subsets of cybersecurity include, but are not limited to:

- Information and Communications Technology (ICT)
- Internet of Things (IoT)
- Information Security
- Operational Technology (OT)

A successful cybersecurity approach has multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe. In an organization, the people, processes, and technology must all complement one another to create an effective defense from cyberattacks.

Cybersecurity has always been a major concern for business and consumer protection, but the need for cybersecurity was made even more apparent during the COVID-19 Pandemic. Coalition, a cyber insurance and security company, saw a 47% increase in "ransomware" attacks and 35% in funds transfer scams, and 19% in email theft, just to name a few. It is believed that this uptick of cybercrimes are mainly due to the transition of work-from-home arrangements across the globe, which logically leads to an increase in the number of prospective victims for hackers and malicious groups.

(Image Source: Techspot.com)

Common Types of Cyber Threats

- Malware – general term for any malicious software, such as computer viruses, spyware, Trojan horses, and keyloggers.
- Ransomware – specific type of malware that locks or encrypts the victim's data until a ransom is paid.
- Phishing Attacks – use malware to obtain sensitive information (e.g., passwords, credit card information) through a disguised email, phone call, or text message.
- Social engineering - The psychological manipulation of individuals to obtain confidential information; often overlaps with phishing.
- Advanced Persistent Threat – occurs where an unauthorized user gains access to a system or network and remains there for an extended time without being detected.
- Cybercrime - includes single actors or groups targeting systems for financial gain or to cause disruption.
- Cyberattack - often involves politically motivated information gathering.
- Cyberterrorism - intends to undermine electronic systems to cause panic or fear.

Sources of Threats

- Cyber criminals - individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data, and generating profit. Cybercriminals are unlikely to focus on a single entity, but conduct operations on broad masses of victims defined only by similar platform types, online behavior, or programs used. Secondly, they differ in the way that they conduct their operations.
- Cyber-enabled criminals – commit traditional crimes, only this time these are perpetuated, magnified and increased in scale/reach through the use of ICTs.
- Hacktivist - someone who uses hacking to bring about political and social change. The term "hacktivist" traces back to 1994, originating from the hacker group "Cult of the Dead Cow".
- Script kiddies – term for those who lack the skills and infrastructure to launch an attack, yet commit cybercrimes anyway. A script kiddie will use these programs without even knowing how they work or what they do.
- Terrorist – terrorists operate with specific intent and motive and that is to create chaos and terror to the public. Terrorists use the internet for recruitment and propaganda for vulnerable target groups or individuals.
- Insiders - also known as a turn cloaks, they refer to malicious insider actors intentionally targeting systems and abuse privileges to gain access to sensitive information. A turn cloak will have an upper hand as he or she is familiar with the system and can easily navigate through without detection.
- Social engineering - Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

- Non-State and State sponsored threats – countries with technical capabilities to attack other state. Other countries like the Philippines are used as launch pads to attack other states or through state-sponsored attacks.

Common Types of Cybersecurity

- Network Security – seeks to protect network traffic by controlling all incoming and outgoing connections, preventing threats from entering or spreading to the rest of the network.
- Data Loss Prevention (DLP) - protects data integrity, specifically y focusing on the location, classification and monitoring of data, whether if it's at rest, in use or in motion.
- Cloud Security - provides protection for data used in cloud-based services and applications.
- Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) - work to actively identify potentially hostile cyber activity.
- Identity and Access Management (IAM) - use authentication services to limit and track employee access to protect internal systems from malicious entities.
- Encryption - is the process of encoding data to render it unintelligible, and is often used during data transfer to prevent theft in transit.
- Antivirus/anti-malware solutions - scan computer systems for known threats and initiates actions to resolve them. Modern antivirus/malware solutions are even able to detect previously unknown threats and react accordingly based on their behavior.

Examples of Cybersecurity Certifications

As the importance of cybersecurity is made apparent to all, security firms and consultants have seen fit to formalize the training of cybersecurity professionals by creating the following certifications.

- Certified Ethical Hacker (CEH) - a certification program for an information security professional, also referred to as a "white-hat hacker", who systematically attempts to inspect network infrastructure with the consent of its owner to find security vulnerabilities which a malicious hacker could potentially exploit.
- CompTIA Security+ - a global certification that validates the baseline skills students need to perform core security functions and pursue an IT security career.
- Certified Information System Security Professional (CISSP) - an independent information security certification granted by the International Information System Security Certification Consortium, also known as (ISC)².
- Certified Information Security Manager (CISM) - certification that indicates expertise in information security governance, program development and management, incident management and risk management.

- Certified Information Systems Auditor (CISA) - a standard of achievement for those who audit, control, monitor and assess an organization's information technology and business systems.
- NIST Cybersecurity Framework (NCSF) – a collection of qualifications that teach the knowledge, skills and abilities to assess, design, implement, operationalize and continually improve the cybersecurity controls & management systems associated with a NIST Cybersecurity Framework program. The NIST Cybersecurity certification training programs teach organizations how to design and operationalize a NIST/COSO cybersecurity practice capable of Identifying, Protecting, Detecting, Responding and Recovering from cyberattacks.
- Certified Cloud Security Professional (CCSP) – certification for advanced technical skills and knowledge to design, manage and secure data, applications and infrastructure in the cloud using best practices, policies and procedures established by the cybersecurity experts at the International Information System Security Certification Consortium or $(ISC)^2$.
- Computer Hacking Forensic Investigator (CHFI) – certification for conducting computer investigations using ground-breaking digital forensics technologies.
- GIAC Certifications - provide the highest and most rigorous assurance of cyber security knowledge and skill available to industry, government, and military clients.
- Cisco Certified Network Associate (CCNA) Security - CCNA Security validates knowledge of security infrastructure, threats, and vulnerabilities to networks and threat mitigation. Required skills include installation, troubleshooting and monitoring of network devices to maintain the integrity, confidentiality, and availability of data and devices.

Note: Except for CISCO CCNA Security, the certifications listed above are vendor neutral. There are certifications and training for cybersecurity that are vendor- specific; those trainings are designed to configure, use and design security systems around specific vendor technology ecosystems (software and hardware).

Cybersecurity in Other Countries

- ❑ Australia

In Australia, two academic centers of cybersecurity excellence (ACCSEs) were established at the University of Melbourne and Edith Cowan University in 2017. As part of the Australian cybersecurity strategy, the establishment of the two ACCSEs directly supports one of the key themes (building 'A cyber smart nation') of the country's strategic vision and follows an investment of AUD 1.9 million over 4 years by the government. This initiative is also aligned

with the Cyber Security Science and Research Priorities, which aim to enhance Australian leadership in innovative cybersecurity research and innovation. The applications to become ACCSEs were assessed by a working group appointed by the Minister for Education and Training.

Overall, ACCSEs target the national skills shortage of both technical and nontechnical cybersecurity expertise, and their intended impact is to:

- Encourage more students to study cybersecurity as an academic discipline;
- Increase the number of cybersecurity graduates with skills ready to be deployed in Australia's industry;
- Support cybersecurity research addressing key cybersecurity issues.

The Australian government also set short- and long-term outcomes that should be achieved with this policy. Among the short-term results, ACCSEs are expected to:

- Advance collaboration with other universities, businesses and the government;
- Increase interest in their own programs and activities;
- Have more internships supported by the private sector.

In the long term, the government expects ACCSEs to:

- Increase the number of skilled cybersecurity graduates entering the workforce and improve the basic cybersecurity knowledge of non-cybersecurity graduates;
- Promote the provision of professional executive training;
- increase the number of cybersecurity professionals coming from under-represented segments of society;
- Conduct research projects that contribute to the cybersecurity strategy and the Science and Research Priorities and to increase commercialization outputs.

❑ United Kingdom (UK)

The United Kingdom has acknowledged that their cybersecurity skills needs go beyond the lack of qualified individuals they have available; the capability of UK businesses and companies to enforce cybersecurity is also an issue. So far, it is only the National Cyber Security Centre (NSCS) that certifies bachelors', integrated masters' and masters' degrees, and apprenticeships related to this industry. This initiative directly stems from the UK Cyber Security Strategy 2016-21, which states that 'the UK requires more talented and qualified cybersecurity professionals'. Businesses believe that the shortage has its origins in the novelty and immaturity of cybersecurity as a profession, the lack of graduates in science, technology, engineering and mathematics (STEM)-related disciplines, and the poor awareness of cybersecurity as a career option.

Prior to this, only 'centres for doctoral training (CDTs)' in cybersecurity, which were established in 2013 as a part of the 2011 national cybersecurity programme, provide tutelage for cybersecurity in the UK. A CDT in cybersecurity provides a 4-year programme: enrolled doctoral students attend a taught component in their first year and undertake a specific research project with a clear focus on cybersecurity in the remaining 3 years. The taught component should account for 25 % of the doctoral programme, enhance students' technical knowledge across all areas of cybersecurity, be relevant to business demands, expose students to activities other than research (for example public engagement).

Businesses believe that the shortage has its origins in the novelty and immaturity of cybersecurity as a profession, the lack of graduates in science, technology, engineering and mathematics (STEM)-related disciplines, and the poor awareness of cybersecurity as a career option.

❑ United States (US)

In the US, the National Security Agency (NSA) sponsors centers of academic excellence (CAEs) in cybersecurity. There are two types of CAE: cyberdefence and cyber operations. The Department of Homeland Security and the NSA jointly sponsor the CAE in cyberdefence (CAE-CD) program in 1999, which had the declared scope of reducing US vulnerabilities through the promotion of cybersecurity higher education and research. As of December 2019, there are 272 institutions in the United States recognized as CAEs-CD. Regionally accredited 2-year, 4-year and graduate-level institutions in the United States could become CAEs. These institutions are formally recognized by the US government, but they do not receive direct funding from it.

The CAE in cyber operations (CAE-CO) program is complementary to the CAE-CD, with the aim of supporting the National Initiative for Cybersecurity Education (NICE) and increasing the pipeline of cybersecurity professionals. This program has a strong foundation in computer science, computer engineering and electrical engineering, and is particularly devoted to the study of technologies and tools enabling cyber operations such as collection, exploitation and response.

Cybersecurity in the Philippines

❑ Philippine Electronic Commerce Act of 2000

The Philippines already has taken steps to quell cybercrimes even before the Pandemic's onset. On 14 June 2000, then-President Joseph E. Estrada signed into law Republic Act 8792

"An Act Providing for the Recognition and Use of Electronic Commercial and Non-Commercial Transactions, Penalties for Unlawful Use Thereof, And Other Purposes, also known as the "Electronic Commerce Act."

The Objective and Sphere of Application of the new law were stated as such:

> Sec. 3. Objective - This Act aims to facilitate domestic and international dealings, transactions, arrangements, agreements, contracts and exchanges and storage of information through the utilization of electronic, optical and similar medium, mode, instrumentality and technology to recognize the authenticity and reliability of electronic data messages or electronic documents related to such activities and to promote the universal use of electronic transactions in the government and by the general public. Sec. 4. Sphere of Application - This Act shall apply to any kind of electronic data message and electronic document used in the context of commercial and non-commercial activities to include domestic and international dealings, transactions, arrangements, agreements, contracts and exchanges and storage of information.

To protect internet users, consumers and owners of computer systems / servers and copyright owners, the new law defines what constitutes illegal activities and provides penalties thereof. Thus:

> Sec. 33. Penalties. – The following Acts shall be penalized by fine and/or imprisonment, as follows:
>
> Hacking or cracking which refers to unauthorized access into or interference in a computer system/server or information and communication system; or any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communications system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic documents shall be punished by a minimum fine of One Hundred Thousand Pesos (P100,000.00) and a maximum commensurate to the damage incurred and a mandatory imprisonment of six (6) months to three (3) years;
>
> Piracy or the unauthorized copying, reproduction, dissemination, distribution, importation, use, removal, alteration, substitution, modification, storage, uploading, downloading, communication, making available to the public, or broadcasting of protected material, electronic signature or copyrighted works including legally protected sound recording or phonograms or information material on protected works, through the use of telecommunication networks, such as, but not limited to, the internet, in a manner that infringes intellectual property rights shall be punished by a minimum fine of One Hundred Thousand Pesos (P100,000.00) and a maximum

commensurate to the damage incurred and a mandatory imprisonment of six (6) months to three (3) years;

Violation of the Consumer Act or Republic Act No. 7394 and other relevant or pertinent laws through transactions covered by or using electronic data messages or electronic documents, shall be penalized with the same penalties as provided in those laws;

Other violations of the provisions of this Act, shall be penalized with a maximum penalty of One Million Pesos (P1,000,000.00) or six (6) years imprisonment.

- **National CyberSecurity Plan 2022**

On May 2, 2017 Department of Information Communication and Technology (DICT) unveiled The National CyberSecurity Plan 2022, intended to provide a roadmap to make a coherent and cohesive strategy for cybersecurity. The primary goals of this Plan are as follows:

- assure the continuous operation of our nation's critical infostructures, public and military networks
- implement cyber resiliency measures to enhance our ability to respond to threats before, during and after attacks
- Facilitate effective coordination with law enforcement agencies
- Create a cybersecurity educated society

Under the plan an Accelerate Learning Skills and Development is to be implemented. To implement the strategy there are four (4) objectives:

- Stimulate the development of approaches and techniques that can rapidly increase the supply of qualified cybersecurity professional
    - Integration of subjects on cybersecurity in higher learning curriculum
    - Integration of cybersecurity in ladderized programs offered by Technical Education and Skills Development Authority TESDA
- Promote advance programs and specialized courses that reduce the time and cost for obtaining knowledge, skills, and abilities for in demand work roles.
- Encourage the adoption of apprenticeships and cooperative education programs to provide an immediate workforce that can earn a salary while they learn the necessary skill
- Promote efforts to identify gaps in cybersecurity skills and raise awareness of training that addresses identified workforce.

❑ Other Measures in the Philippines

The National Privacy Commission (NPC) requires certain companies to assign data protection officers, primarily to allow the public to access these companies' websites through the NPC in the event of a shutdown. Data protection officers are mandatory for companies that process personal information of at least 1,000 records and employ at least 250 workers.

It is for this reason why Cybersecurity Philippines CERT (CPC) consulted with TESDA on September 9, 2020 for the creation of training competencies for Cybersecurity (NCI and NCII). The organization wished to explore the possibility of Philippine and Philippines-based businesses to create their own "defensive" cybersecurity emergency response teams (CERTs), instead of relying on vendors who provide them with "offensive" security solutions like ethical hackers. According to CPC, a CERT could be drawn from a company's existing IT personnel, which means that a 100-man workforce can have only one or two professionals engaged in cybersecurity. The need for CERTs are especially pronounced with the on-going COVID-19 Pandemic that is forcing businesses, schools, and individuals to engage in online activities far more than usual.

(Image Source: Pegasustechnologies.com)

II. TVET CAPACITY

In terms of human resources, the Philippines is sorely lacking in order to provide its people with top-notch cybersecurity and protection. In 2016 alone, the country only had 84 Certified Information Systems Security Professionals, which pale in comparison to Singapore's 1,000+ and Malaysia's 275. Experts have since urged stronger collaboration between security groups and the government to fill this gap. Not only is cybersecurity integral to the well-being of Filipinos in the online space, it is also a very lucrative career choice as seen in Table 1.

Table 1. Salary of Cybersecurity Professionals in the Philippines

Job Title	Description	Salary
Information Security Analyst	Information security analysts are responsible for providing security solutions for their companies. Their main duties include doing research, collecting data, developing secure strategies and maximizing productivity. They also are in charge of implementing security principles while following strict privacy policies.	₱507,131
Security Analyst	as security analysts work to maintain the integrity of company networks, as well as diagnose and quickly resolve network problems as they arise. They must be able to proactively identify risks to the network and promptly address and neutralize these threats, and knowledge of security log fundamentals is essential. Prior experience with escalation patterns, hardening systems, firewalls, anti-virus, anti-spam, secure electronic data transmission, and anti-malware is also important.	₱675,000
Cyber Security Analyst		₱300,000
Security Engineer	Security engineers are responsible for developing effective computing solutions to increase the security of their company's systems and projects. They are in charge of creating new ways to solve existing production security issues and must possess an advanced understanding of intrusion detection and prevention protocols.	₱501,430
Cyber Security Engineer		₱480,000
Security Consultant, (Computing / Networking / Information Technology)	Security consultants (computing/networking/information technology) often work in large organizations and educational institutions that have large digitized databases. Security consultants must be adaptable to each industry they may specifically cater to. They must have good organization and communication skills.	₱650,000
Chief Information Security Officer	is the senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.	₱3,000,000
Senior Information Technology (IT) Manager	No description	₱1,320,000
Information Systems Auditor	No description	₱416,400
Director, Computing/Networking /Information Technology (IT) Security	No description	₱4,200,000

Among such cybersecurity professions that the Philippines currently needs is Computer Security Incident Handling, which deals with resolving security issues that occur online, such as data breaches. At least one consultancy group in the country has proposed the creation of organic computer emergency response teams in companies, given the greater prevalence of online transactions in the country due to the COVID-19 Pandemic. Other professions include:

- Certified Ethical Hacker
- Computer Hacking Forensics Investigator
- Certified Security Analyst

❑ Training Regulations

TESDA currently has no training regulations that are directly related to cybersecurity. However, certain courses related to ICT, such as Web Development NC III, have knowledge requirements in cybersecurity laws. As such, it is reasonable to surmise that ICT courses can be used as a baseline to gauge TVET capacity in cybersecurity, given how they encompass the basics of cybersecurity to begin with. Table 2 lists these courses that have some element of cybersecurity (i.e. data security, security configuration and security measures) included in their curricula:

Table 2. Information and Communication Technology Qualifications with Cybersecurity Elements

ICT Qualifiactions	
Contact Center Services NC II	2D Game Art Development NC III
Medical Transcription NC II	3D Game Art Development NC III
2D Animation NC III	Game Programming NC III
3D Animation NC III	Programming (.Net Technology) NC III
Animation NC II	Programming (Java) NC III
Visual Graphic Design NC III	Programming (Oracle Database) NC III
Web Development NC III	Medical Coding and Claims Processing NC III
Broadband Installation (Fixed Wireless Systems) NC II	

❑ Enrolled, Graduated, Assessed, and Certified Students

As seen in Table 3, the number of TVET students in ICT-related courses have been gradually decreasing since at least 2018. From 118,308 graduates in 2018, ICT courses have only reported 71,119 in 2019. Interestingly, there are more female enrollees and graduates than males, though there are more male assessed and certified graduates, indicating that ICT seems to be more attractive to female students. 2020 data is not yet complete enough to provide any insights in this regard.

Table 3. TVET Students in ICT-Related Courses (2018-2020)

Year/Sex	Enrolled			Graduated			Assessed			Certified		
	Male	Female	Total	Male	Female	Total	Male	Female	Total	Male	Female	Total
2018	56,982	66,040	123,022	54,374	63,934	118,308	16,182	14,814	30,996	12,951	11,925	24,876
2019	34,636	44,246	78,882	31,317	39,802	71,119	10,169	8,017	18,186	8,625	6,858	15,483
2020*	11,379	16,069	27,448	750	998	1,748	1,789	1,371	3,160	1,514	1,133	2,647

*Latest data as of August 2020

Table 4 shows the distribution of ICT students as of August 2020. While this data is still being updated, a vast majority of students have been reported to have enrolled and graduated from Contact Center Services II. Part of this course's requirements is knowledge on data security guidelines, which is a key aspect of cybersecurity. This is can be seen as a positive, as majority of ICT qualifications contains guidelines and procedures on data security and malware avoidance anyway. Web Development NC III also includes knowledge of cybersecurity laws and data privacy, as well as web security concepts and best practices as part of its basic and core competencies.

Table 4. Enrollment and Graduates in the Information and Communication Technology Sector, under Program Registration, Qualification, and Sex (as of August 2020)

Program Registration	Qualification	Enrolled			Graduates		
		Female	Male	Total	Female	Male	Total
With Training Regulation (WTR)	2D Animation III	13	19	32	0	0	0
	3D Animation III	5	6	11	0	1	1
	Animation II	17	13	30	17	13	30
	Broadband Installation (Fixed Wireless Systems) II	12	17	29	0	0	0
	Contact Center Services II	1,043	614	1657	713	445	1158
	Medical Transcription II	18	13	31	0	0	0
	Telecom OSP Installation (Fiber Optic Cable) II		20	20		0	0
	Visual Graphic Design III	61	97	158	22	33	55

❑ Competency Assessors and Assessment Centers

The number of competency assessors and assessment centers for ICT-related courses seem to fluctuate. As seen in Table 5, there were 233 assessors and 188 assessment centers, which increased to 274 and 228 (respectively) the following year. However, these numbers slightly decreased in 2019, reporting 265 competency assessors and 207 assessment centers. No numbers for 2020 have yet been reported.

Table 5. Information and Communication Technology Sector Number of Competency Assessors and Assessment Centers: 2017-2019

Year	No. of Competency Assessors	No. of Assessment Centers
2017	233	188
2018	274	228
2019	265	207

III. RECOMMENDATIONS

- As today's cyberattacks are highly sophisticated, organized and exploit vulnerabilities of technology and social engineering, professionals need specific skills and specialized knowledge to meet multiple, varied threats. Even the DICT Cybersecurity Plan 2022 strategized the strengthening and development of cybersecurity training as a key part of the Philippine government's mission to ensure public safety and welfare in the digital age. Cybersecurity is arguably even more important now more than ever, as the COVID-19 Pandemic has forced people and businesses to engage in online activities much more frequently. However, **TESDA do not have corresponding TVET programs that can support the capability building/training of human resource**. TESDA's current training regulations in ICT do not include programs explicitly for Cybersecurity, thus it is recommended that TESDA consults with the DICT, the academe and industry stakeholders to develop relevant training programs to meet this skills gap.
- The National CyberSecurity Plan indicates as one of its strategies is the "Encourage the adoption of apprenticeships and cooperative education programs to provide an immediate workforce that can earn a salary while they learn the necessary skill." Given this, TESDA through its ROPOTIs must work out on the implementation of the Enterprise-Based Training for the related programs that will be developed for the budding Cybersecurity industry.
- Other than training, TESDA has to consider that existing licensure for the cybersecurity. The said certification can be considered in the development of the relevant assessment tool or the possible adoption of the cybersecurity certification.

(Image Source: Techspot.com)

REFERENCES:

CompTIA. (n.d.). *CompTIA Security+ Certification*. Retrieved from: https://www.comptia.org/certifications/security

Cybersecurity. (n.d.). In *Gartner.com Glossary*. Retrieved from: https://www.gartner.com/en/information-technology/glossary/cybersecurity

Data Privacy Philippines. (June 29, 2017). *Select PH Companies Required by NPC to Submit Security Officer Info*. Retrieved from: https://privacy.com.ph/news-article/select-ph-companies-required-npc-submit-security-officer-info/

Department of Information and Communications Technology. (2017). *National Cybersecurity Plan 2022*. Retrieved from: https://dict.gov.ph/national-cybersecurity-plan-2022/

EC-Council. (n.d.). *Certified Ethical Hacker*. Retrieved from: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

ENISA. December 2019. *Cybersecurity Skills Development in the EU: The certification of cybersecurity degrees and ENISA's Higher Education Database*. Retrieved from: https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union/at_download/fullReport

Furminger, M. (n.d.). *CCNA Security Hungarian Event*. Retrieved from: https://www.cisco.com/web/offer/emea/4867/docs/CCNASecurityOverview_Hungary.pdf

ISACA. (n.d.). *Certified Information Systems Auditor*. Retrieved from: https://www.isaca.org/credentialing/cisa

Parcon, R.J.M.L. (February 2017). *Addressing Cyberspace Vulnerability: The ASEAN and the Philippines*. Center for International Relations and Strategic Studies. Retrieved from: http://www.fsi.gov.ph/addressing-cyberspace-vulnerability-the-asean-and-the-philippines/

SecurityMagazine. (September 11, 2020). *Cybersecurity claims trends amid COVID-19*. Retrieved from: https://www.securitymagazine.com/articles/93322-cybersecurity-claims-trends-amid-covid-19

Labor Market Information Division and Policy Research and Evaluation Division
Planning Office
Office of the Deputy Director General for Policies and Planning
Technical Education and Skills Development Authority
TESDA Complex, East Service Road, South Luzon Expressway (SLEX)
Fort Bonifacio, Taguig City 1630, Metro Manila