4) Investigative Processes Class: Conduct the Digital Forensic Analysis from LEAs

The fourth and last class of investigative processes develops a likely sequence of events. It includes investigating the incident, analyzing the evidence, interpreting results from the analysis, and reporting on results of the digital evidence. Investigators can examine the pieces of evidence to measure performance against the determined objectives and report the results to the appropriate recipients for review. A singular strategy can not resolve the majority of cybercrime challenges. Technical minds alone cannot solve the issue of prosecuting cybercriminals. Given limited time and resources, it is essential to maximally leverage knowledge, capabilities, and investments in a range of public-private partnerships to improve foundations of trust and enhance agility and resilience.

5) Concurrent Processes Class: Take Place in Company with these Processes Classes

The following concurrent processes class takes place in company with the former processes classes [5, 11, 20].

a) Obtaining Authorization Process

Having authorization from the appropriate authorities makes sure that the appropriate countermeasures are ready to solve it.

b) Documentation Process

Investigators must maintain documentation of digital evidence from the beginning of the e-discovery process until the end.

c) Managing Information Flow Process

Information flow could describe the use of trusted PKI and time stamping to identify the exchange of digital evidence between each of the processes in the same investigation.

d) Preserving Chain of Custody Process

The documentation comprises the chain of custody form and records relating to the evidence analysis.

e) Preserving Digital Evidence Process

In order to preserve the integrity of the digital evidence, investigators should guarantee that the original evidence is not changed.

f) Interaction with Physical Investigation Process

There are some complex interactions with the physical investigation according to the digital investigator's needs and fast adaption to changing boundaries, scope, or investigation objectives. All of the complexities must be simplified to ensure an efficient investigation.

V. *CONCLUSIONS*

ICT innovations are not only set to bring enormous benefits to the general public, but also bring new technological risks to individuals and businesses. Cybercrimes have rapidly evolved for the dissemination of malware. Criminals increasingly use sophisticated tools and methods to commit their cybercrimes. Major information systems of modern society are under the burgeoning attack. Cybersecurity for banking or financial institutions becomes a vital business enabler to enhance customer confidence and bring in more business. It is vital to leverage investments in a range of societies to assure societal services. The ATM withdrawals happened so quickly that none of the commercial banks involved noticed in time to stop the perpetrators. ATM technologies are evolving fast and making payments more convenient. Organizations need a balance between security and functionality in information security. This study outlines a set of profiling cybercrime investigation that aims to identify digital pieces of evidence in the face of increased complexity and vulnerability in hacking activities. It is our sincere hope to bring the technical details to the attention of information security specialists and to minimize risks by preventing information security incidents. A small sacrifice inconvenience can be useful to prevent an attack on the ATM's door. ICT governance should be employed by banks to heist ATM money with more barriers.

REFERENCES

[1] Ablon, L., Libicki, M. C., and Golay, A. A. *Markets for Cybercrime Tools and Stolen Data Hackers' Bazaar*, Rand Corporation, pp. 3-28, 2014.

[2] Akhgar, B., Staniforth, A., and Bosco, F., *Cyber Crime and Cyber Terrorism Investigator's Handbook*, Elsevier Publishing, pp. 88-90, 2014.

[3] Bates, A. and Hassan, W. U., "Can Data Provenance Put an End to the Data Breach? " *IEEE Security & Privacy*, Vol. 17, No. 4, pp. 88-93, July-Aug. 2019.

[4] Bernik, I., *Cybercrime and Cyberwarfare*, John Wiley & Sons Inc., pp. 1-57, 2014.

[5] Brooks, C. L., *CHFI Computer Hacking Forensic Investigator Certification All-in-One Exam Guide (1st Edition)*, McGraw-Hill Education, pp. 13-50, 2015.

[6] Casey, E., *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd Edition)*, Elsevier Inc., pp. 187-306, 2011.

[7] Coburn, A.W., Daffron, J., Smith, A., Bordeau, J., Leverett, É., Sweeney, S., and Harvey, T., "Cyber Risk Outlook 2018, " Centre for Risk Studies, University of Cambridge and Risk Management Solutions, Inc., pp. 2-25, 2018.

[8] Europol and European Cybercrime Center, "Internet Organised Crime Threat Assessment (IOCTA) 2018, " European Union Agency for Law Enforcement Cooperation, pp. 14-65, 2018.

[9] Graves, M. W., *Digital Archaeology: The Art and Science of Digital Forensics*, Addison-Wesley, pp. 91-110, 2014.

[10] Impagliazzo, J. and McGettrick, *A., Information Systems: What Every Business Student Needs to Know*, NW: Taylor & Francis Group, 2016.

[11] International Organization for Standardization (ISO), "ISO/IEC 27043:2015 Information Technology - Security Techniques - Incident Investigation Principles and Processes," ISO Office, 2015.

[12] Jewkes, Y, and Yar, M., *Handbook of Internet crime*, Willan Publishing, pp. 173-193, 2009.

[13] Kao, D. Y., "Exploring the Cybercrime Investigation Framework of ATM Heist from ISO/IEC 27043:2015, " IEEE ICACT 2017 (19th International Conference on Advanced Communications Technology), Pyeong Chaung, South Korea, 2017.

[14] Kao, D. Y., "ATM Heist Threats: a Proposed ICT Governance Strategy," IEEE ICACT 2019 (21th International Conference on Advanced Communications Technology), Pyeong Chaung, South Korea, pp. 610 - 615, 2019.

[15] Law and Regulations Retrieving System, "Criminal Appeals No. 593/106 in Taiwan High Court," Judicial Yuan, May 18, 2017.

[16] Marcella, A. J., Menendez, D., *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes (2nd Edition)*, Auerbach Publications, pp. 1-26, 2008.

[17] Mehan, J. E., *Cyberterror, Cybercrime, and Cyberactivism: An In-Depth Guide to the Role of Security Standards in the Cybersecurity Environment (2nd Edition),* IT Governance Publishing, pp. 25-58, 2014.

[18] Oriyano, S. P., *CEH v9: Certified Ethical Hacker Version 9 Study Guide (3rd Edition)*, John Wiley & Sons, Inc., pp. 1-222, 2016.

[19] Sancho, D., Huq, N., and Michenzi, M., "Cashing in on ATM Malware: A Comprehensive Look at Various Attack Types," Trend

Micro Forward-Looking Threat Research (FTR) Team and Europol's European Cybercrime Centre (EC3), 2017.
[20] Shipley, T. G. and Bowker, A., *Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace*, Elsevier Inc., pp. 21-38, 2014.
[21] Smith, R. G., Cheung, R. C. C., and Lau, L. Y.C., *Cybercrime Risks and Responses Eastern and Western Perspectives*, Macmillan Publishers Limited, pp. 67-211, 2015.
[22] Spitzner, L., *Honeypots Tracking Hackers*, Addison-Wesley, pp. 8-20, 2002.
[23] Stephenson, P., *Official (ISC)²® Guide to the CCFP CBK*, Auerbach Publications, pp. 293-404, 2014.
[24] Walker, M., *CEH Certified Ethical Hacker All-in-One Exam Guide (2nd Edition)*, Graw-Hill Education, pp. 35-198, 2014.

Da-Yu Kao received the B.S. and M.S. degree in Information Management from Central Police University, Taiwan, in 1993 and 2001, the Ph.D. degrees in Crime Prevention and Correction from Central Police University, Taiwan, in 2009, respectively. From 1993 to 1996, he was with Taipei City Police Department, Taiwan, where he was an information technology police officer involved in the development of policing information systems. From 1996 to 2007, he was with Criminal Investigation Bureau, National Police Administration, Taiwan, where he was a detective and forensic police officer in cybercrime investigation and digital forensics. From 2007 to 2013, he was with Maritime Patrol Directorate General, Coast Guard Administration, Taiwan, where he was an information technology section chief in the department of information and communication. Since 2013, he has been with Central Police University, Taiwan, where he is currently an associate professor in the Department of Information Management. His research interests include cybercrime investigation, digital forensics, digital evidence, information management, criminal profiling, and cyber criminology.