DR. RICCI IEONG *Founder, eWalker Consulting (HK) Ltd.*
www.ewalker.com.hk

Ricci has over 20 years experience in the IT Security area; specialising in Security Risk Assessment, IT Audit, Ethical Hacking and Penetration Test, Smart Card and Biometrics System deployment and Computer Forensics Investigation. He is the founder and Principal Consultant of eWalker Consulting (HK) Ltd. He was the Security Lead of HPS Consulting & Integration in Hong Kong, Deputy Manager of ITPSA Security Services in HP and founded the first e-Security centre within Hewlett Packard. He is the founding member of Information Security and Forensics Society (HK) and the founding member of Cloud Security Alliance (HK and Macau Chapter). He actively participates in the cyber security community in Hong Kong. He is also an educator in a number of Universities in Hong Kong. He is also one of the first Certificate of Cloud Security Knowledge v4.0 (CCSK v4) Trainers within Asia Pacific Region, (ISC)2 Authorised Certified Cloud Security Professional (CCSP) in Hong Kong, APMG Accredited Trainer of Certificate of Cloud Auditing Knowledge (CCAK) in Asia Pacific Region.

TIP 1. BEGIN WITH THREAT MODEL

Before, when we considered cyber security review, we started by conducting security audit and security assessments. When we entered the new age, with more cloud environment, different varieties of applications, and more automation, traditional security review methodology had to be enhanced. By performing threat modelling at the beginning, system and data owners can determine the most concerning threats to their organisation before performing a relevant security review. We should always develop a threat model of our system.

TIP 2. DATA IS THE CORE TO CYBER SECURITY

We understand cyber security starts by enforcing security protection to servers and storages. Firewall encryption and different kinds of defensive security tools have been implemented in companies' data centres. Focuses should be brought back to the core – data. Data should be the focus of all cyber security issues. Top risk to most companies is data leakage during a cyber attack. We should ensure that cyber security reviews should start from data security.

TIP 3. ATTACKER STARTS FROM ACCOUNTS

Data is the target of most attackers, the user's account is one of the most important keys to attack. All attacks will link up with accounts associated with processes or programs being compromised. So attackers normally start by compromising systems with weak passwords, or previously stolen passwords. Then, through the compromised accounts, attackers will further explore to obtain privilege accounts in the system, or the entire environment. We should define monitoring mechanisms of use of seldom used accounts and privilege accounts.

TIP 4. STRONG PASSWORD IS MORE IMPORTANT THAN PASSWORD AGING

Traditionally, we emphasise the importance of defining password policies, including strong passwords and password aging policies. However, in recent years, we are already aware that frequently changing passwords, together with preventing use of previous passwords, will bring users to adopt less secure and patterned passwords. In fact, a strong and difficult to guess password is a much better option to use. We should revise our policy to encourage use of strong passwords; with password changes whenever required.

TIP 5. PASSWORD MANAGER IS YOUR GUARD

How many passwords can you remember? There is always a debate between experts:- should we use a single password, or multiple passwords for different applications? History tells us that we should use different passwords for different applications. A password manager becomes our necessary component to handle all those passwords. A good password manager will also help us to check and match the applications that pop up for passwords. Phishing sites can also be prevented from obtaining passwords. We should adopt using a password manager to protect our passwords.

TIP 6. MORE ATTACK IN THE CLOUD ENVIRONMENT

Use of a cloud computing environment is already becoming the norm for most IT application development. Both SME and large enterprises are moving to a cloud computing environment. Cloud Security is considered to be one of the most critical concerns to many companies. In fact, according to honey pot analysis and research, more attackers move to target IP addresses owned by cloud service providers. We should ensure that instances have minimal services reachable from the Internet.

TIP 7. MORE SECURITY IN A CLOUD ENVIRONMENT

Are systems in a cloud computing environment really less secure than an on-premises environment? It depends. Depending on whether the cloud user is mature in using a cloud environment, understanding the requirement of a Shared Responsibility Model and able to utilise the security features and functions provided by the service provider. In fact, many Cloud Service Providers were equipped with the latest cyber security solutions which used to be enabled for enterprise customers only. We should utilise security features provided by CSP for monitoring of our cloud environment that aligns with the Shared Responsibility Model.

TIP 8. TRUST MORE IN ZERO TRUST

With the use of a cloud computing environment, perimeter defence mechanism is no longer considered as a unique and sound defence solution. Internal and external environments could not be clearly defined. In order to strengthen the network defence mechanism, companies started to adopt the use of a Zero Trust network segmentation scheme to separate the computing environment with an additional layer of defence – Identity Access Management solution. An unauthenticated system would not be authorised to have network access to the targeted environment. We should adopt a Zero Trust network segment as part of the network defence mechanism.

TIP 9. SIEM IS MORE THAN LOG CONSOLIDATION

If more network devices, more defence solutions, more use of host and server based security solutions are used, more logs would be generated. Logs are sets of big data. Without categorisation and consolidation, they are sets of unstructured raw data. If we can categorise them, they are useful valuable resources. So log consolidation would be necessary - and consolidated logs are better to be transferred to Security Incident Event Management (SIEM) tools for instant correlation of related logs. We should implement SIEM to handle logs centrally with meaningful categorisation.

TIP 10. COMPUTER FORENSICS IS PART OF THE PUZZLE

Logs become useful when we need to investigate an incident. Most of the time, we would not expect to be compromised, but when compromised, we would like to determine how the system could be compromised? What is the coverage of the attack? How can the attacker first enter into the environment? What has been damaged by the attacker? Has any information leakage happened? In order to get the answers to these questions, forensics investigation would have to be performed based on the collected logs and acquired computers. We should incorporate forensics investigation procedures into the overall incident management procedures.