A Summary of Cyber Security Malaysia Awards, Conference & Exhibition (CSM-ACE) 2014

12 November 2014, Casuarina @ Meru, Ipoh

"Trusted & Secured Ecosystem"

Rapporteurs From
Accounting Research Institute (ARI) & Faculty of Law, UiTM

Associate Professor Dr Zaiton Hamin
Professor Dr Rohana Othman
Saslina Kamaruddin
Muhammad Muaz Abdul Hakim
Hayyum Suleikha Selamat
Siti Saidah Nafisah Omar

12 November 2014

Opening Address at CSM-ACE 2014 (10.00 am – 10.10 am)

Y.B. Datuk Dr. Abu Bakar Mohamad Diah, Deputy Minister of Science, Technology and Innovation

YB Datuk Dr Abu Bakar Mohamad Diah delivered the opening address for YB Datuk Dr. Ewon Ebin, the Minister of Science, Technology, and Innovation. He welcomed the speakers and delegates to the Cyber Security Malaysia's 4th Awards Conference and Exhibition 2014 and also thanked the Chief Minister of Perak and Perak State Government for being the host and co-organiser.

YB Datuk Dr Abu Bakar then expressed his pleasure of hosting the event in Perak and outside Kuala Lumpur and were glad to see a large number of delegates that represented some 30 member countries of the World Trustmark Alliance. He then thanked the experts who were willing to share their expertise and experiences at the conference. Such participation could promote exchange of knowledge among cyber security professionals. Also, it would strengthen the collective cyber security skills, at the time when ICT was being relied upon in all aspects of human activities.

YB Datuk Dr Abu Bakar explained that this CSM-ACE 2014 theme 'Trusted and Secured Ecosystem' was well chosen since the Internet users amongst Malaysians were increasing, and they could be facing some cyber threats. Thus, he believed that the CSM-ACE 2014 was addressing the urgent need to establish a trusted and secured ecosystem.

YB Datuk Dr Abu Bakar then observed that cyber-attacks have become more common and extensive. Its economic effect globally was very huge and today there were many cyberspace threats from criminals around the world.

Turning to the recent statistics in Malaysia, YB Datuk Dr Abu Bakar stated that 10,636 cyber security incidents were reported last year. The police also received 587 reported cases of impersonation with an estimated RM14.9 million losses, while phishing and credit card fraud had resulted in losses amounting to RM845, 000.

YB Datuk Dr Abu Bakar also noted that while the Internet provided considerable opportunities to expand economic and business ventures, the disadvantage with such a medium was its vulnerability to cyber crimes.

YB Datuk Dr Abu Bakar then emphasized that securing cyberspace was a challenge to the national e-sovereignty. In order to achieve self-reliance, cyber security must be determined by a united R&D framework that focused on the technology protecting the Critical National Information Infrastructure (CNII). YB Datuk Dr Abu Bakar urged the audience to protect all critical systems and assets that were vital to the country and also to foster stronger information and communication technologies to enable safer online services for all.

He further explained that with the increasing intensity of cyber crimes and threats, a focused effort from all stakeholders was needed in order to secure cyberspace. Furthermore, cyber security had been identified as one of the priority areas of MOSTI's R, D&C agenda. Hence, enhancing cyber security efforts in R&D was vital to improving the current condition and new capabilities in cyber security.

YB Datuk Dr Abu Bakar stated that an ecosystem that could deal with new complexities was needed. The ecosystem for cyber security and data protection required a dynamic policy framework to adapt, change and respond quickly and efficiently. Moreover, an information security framework should be focused on the basic and the emerging threats. However, some assumption must be made that security breaches would be likely, which eventually required planning and protecting the system.

He then suggested that realistic actions should be taken to ensure all information security measures were executed effectively and were strictly followed. An organization also had to sustain cyber security program, which would keep information security framework effective and up-to-date. The tools in such program would involve compliance measures, self-assessments, continuous learning and improvement measures and follow-up on incidents.

YB Datuk Dr Abu Bakar then expressed his appreciation to all the delegates who were present at the CSM-ACE 2014, He believed that the delegates would give much attention to the issues of cyber threats and risk management in cyberspace. He also hoped that this conference would be

the foundation to work together in the future and to build a safe cyber ecosystem in Malaysia.

In concluding his speech, YB Datuk Dr Abu Bakar promoted the CSM-ACE 2014 as a showcase of the latest information and communication technologies and solutions from the exhibitors. He also encouraged all delegates to visit the exhibition booths and to find out more about the latest cyber security technology and processes. He then concluded his speech by wishing the delegates a productive conference.

Opening Speech of CSM-ACE 2014 by Y.A.B. Dato' Seri Diraja Dr Zambry Bin Abdul Kadir, Chief Minister of Perak (10.10 am – 10.20 am)

On behalf of the State Government of Perak, Y.A.B. Dato' Seri welcomed the guests, speakers and participants to the Cyber Security Malaysia's 4th Awards Conference and Exhibition 2014, held in Ipoh, Perak Darul Ridzuan.

Dato' Seri then stated that the conference was very significant as the participants will learn about numerous cyber security issues, particularly cyber crime. Dato' Seri said that cyber crime was a global concern, requiring more serious, concerted and continuous efforts by global leaders than ever before to curb it.

Dato' Seri further noted that the advent of the Internet has led to a borderless world without any geographical limitations or much regulatory control. He also observed the extensive reliance was being placed on the Internet and electronic gadgets for communication, business, transportation and other necessary services. Such reliance was both a boon and a bane at the same time. Unthinkable harm, losses and a possible collapse of the global economy could occur if cyber world were being compromised by cyber criminals or terrorists.

Citing the Internet Security Forum, a global security think-tank, Dato' Seri observed that cyber crime had been listed among the top 5 security threats this year. He also cited the 2014 McAfee Report on the Global Cost of Cybercrime that the cost of such crime was between USD375 billion to USD575 billion annually. The US Government had estimated the cost at USD1 trillion.

Dato' Seri then turned to the negative consequence of cyber crime - unemployment. More than 350,000 jobs in the USA and Europe have been lost annually because of such crimes. He said that international criminal organizations have continued to abuse the Internet persistently to conduct illegal activities such as drugs and human trafficking, financial fraud and money laundering. On the consequences of cyber crime, he also noted that Malaysians could lose their life savings to online fraudsters. In fact, he stated that such crime had resulted in RM1 billion losses, making the country as the sixth country as being the most vulnerable to cyber-crimes in the region.

Expressing his concern about the risks of cybercrime, Dato' Seri stated that such risks would increase as more people; businesses, institutions and governments conducted their businesses online. Such a situation required a more secure and trusted cyber security eco-system. Dato' Seri noted that governments around the world were spending billions annually on cyber recovery and defence since cyber security had become a global security issue. As the security and integrity of the cyber ecosystem were important, he observed that it was timely that CSM-ACE 2014 addressed these national and global issues.

Dato' Seri proudly stated that ICT was one of the cornerstones of Perak's economic advancement towards a knowledge economy. Perak had been vigorously pursuing five K-initiatives namely, K-Economy, K-Government, K-Infrastructure, K-Society, and K-Worker to transform Perak into a knowledge-based economy by 2020. These initiatives were supported by KPerak INC Corporation and have led to a remarkable digital economic transformation in the State. Dato' Seri cited MSC Cyber centre @ Meru Raya as an example of a world-class ICT hub, which had emerged as a hub for new investments in technology-related industries.

Dato' Seri noted that a cyber-ecosystem would not be fully functional without a safe and secure cyberspace. An effective and efficient cyber ecosystem required responsible and competent digital citizens. The introduction of K-Society and K-Worker initiatives emphasized in technical training, techno-preneurship and instilling knowledge culture from the young. He then urged all ICT professionals in the state to take advantage of the various training programs offered under CSM-ACE 2014 to enhance their skills.

Dato' Seri argued that a trusted, reliable, and secure ecosystem was a safeguard against various and emerging cyber threats. Such a system

would protect business partnerships, shared strategies, digital policies, inter-operable information exchanges and digital players including persons, devices, and processes. Dato' Seri then acknowledged the important and vigilant role of Cyber Security Malaysia in ensuring the security of the country's cyberspace. Dato' Seri gave an assurance that Perak State Government will continue to support and work with Cyber Security Malaysia.

In concluding his speech Dato' Seri thanked the organisers of this conference, and all participants for making the CSM-ACE 2014 conference the best. Dato' Seri hoped that they would take the opportunity to experience and enjoy the diversity of the true Malaysian culture, the beautiful places in Perak, and the amazing warmth and hospitality of the local people. With that Dato' Seri officially declared the CSM-ACE 2014 opened.

Keynote 1: Global Cyber Executive Briefing (11.20 am – 11.50 am)

Speaker: Mr. Mohd Nizar Mohd Najib, Executive Director, Financial Advisory, Deloitte Malaysia

The speaker, Mr. Mohd Nizar Mohd Najib began his presentation by expressing his sincere appreciation to the organisers. He highlighted that the Malaysian Government had taken cyber security very seriously. He said that the Government was doing everything they could to counter the impact of cyber insecurity and the evolving threats. Mr. Nizar then pointed out that the threat of cyber security was very real, albeit in the virtual world. Mr. Nizar argued that some modern CEOs were not taking cyber security seriously, and therefore they did not place high priorities on such issues in their corporate agenda. Mr. Nizar added that the concept of cyber security remained vague and complex. He pointed out that being resilient to cyber security threat, or cyber security awareness started from the awareness of the Board of Directors.

Mr. Nizar then cited Deloitte's Cyber Security best practices. He noted that to be effective and have a well-balanced cyber security defence, all companies must have three characteristics. Firstly, cyber security defences must be secured, i.e., such security must focus on the protection around the company's most valuable assets. Such assets were one that the company or their competitors covered the most, for example, their intellectual property or their trade secrets. Secondly, a company must be vigilant. A company

must develop the capacity to detect any patterns or behaviours that might indicate or even predict or compromise critical assets. Thirdly, a company must be resilient. All companies must rapidly contain the damage or mobilize the diverse resources to mitigate the impact of a cyber security breach. He further stated that all companies must realize that cyber security impact was very grave.

He provided some examples from Deloitte's compilation of case studies to drive up this point. The first case study involved an online media industry that became a launch pad for malware outbreak in the banking sector. The company hosted a news website and was ranked on the top 20 of the most visited website within the country in which they operated. The attackers used the website to spread the malware and gained access to third party with an advertising program. The attackers then used to play the infected advertisement on the news website. When a visitor clicked on this malware advertisement, the attackers were able to hijack his/her banking transactions and to steal credit card payment information.

The complexities of the attacks suggested that the attackers could be organized crime groups and were motivated by financial gain. They used a specific malware to steal money from online banking users in the countries where the website were hosted. To date, law enforcement agencies have no knowledge of how they had gained access to the credential third party system. However, it was clear that the infected advertisement was employed to spread the malware. As a business impact, the company's reputation had been affected by this malware dissemination. Since the company made most of its monies from online media, this incident would be a real challenge for them to regain the trusts and confidence from both the customer-based readers and advertisers.

The second case study cited by Mr. Nizar involved worms that took control of several industrial plants, which were multinational engineering and electronic firms. The attackers used an advanced malware and infected the multiple plants around the world. Once the infection had spread, the attackers then took control of their systems to monitor and control the critical industries such as power plants. He pointed out that such acts were unthinkable, but it had happen.

These types of threats had caused widespread panic to many industries and countries. The level of sophistication of these attacks suggested that the perpetrators could come from state-sponsored groups. The technique used

was the deployment of malware into several industrial plants using infected removable media such as the USB device. It seemed harmless, but such device could hurt the victims if it were to fall into the wrong hands and when it was wrongfully used. Once the infected device became connected to the plants' internal network, the advanced malware would be automatically deployed and grasped control of the plant. Then the malware would run commands to advance the supervisory control, as well as the SCADA system. While the company emphasized that there was no real damage, the incident caused a huge media outcry and significantly damaged the company's reputation. Since the attackers were theoretically able to control the high-value equipment and infrastructure, they could have created considerable havoc in any corporate environment. He concluded the case studies by suggesting that hackers and attackers were getting more sophisticated than ever before. The corporate sector was vulnerable, and no industries would be impervious from these types of threats.

He pointed out that the profile of hackers ranged from teenagers who were operating from their bedrooms to organized crime syndicates and state-sponsored hackers.

Mr. Nizar suggested some solutions to counter the threats by highlighting five questions, which could reflect the secure, vigilant and resilient approach to cyber-security. The first question was whether organizations/companies were focusing on the right area. In order to answer this question, he emphasized that organizations/companies must understand how value was created for their companies in their critical assets and how vulnerable are they to the key threats. He pointed out that organizations/companies must defend their cyber security to the fullest extent.

The second question was whether companies/organizations have the right talent. He stressed quality over quantity. He argued that there might not be enough talent to do everything in-house, and hence, companies should take a strategic approach to out-sourcing. In this context, he suggested that the security teams should also be focused on the real business areas.

The third question was whether organizations/companies were proactive or reactive. He noted that organizations/companies must build security upfront into their management processes, applications, and infrastructure.

The fourth question was whether companies/organizations had the incentive toward openness and collaboration. He noted that they could build strong

relationships with business partners, law enforcement, regulators, and vendors. They could well foster internal co-operation across groups and functions, and ensure that people were not hiding any risks to protect themselves.

The fifth question posed was whether organizations/companies were adapting to change. He suggested that policy reviews, assessments, and rehearsals of crisis response processes should be regularized to establish a culture of perpetual adaptation to the threats and risk landscape.

Mr. Nizar concluded his presentation by reiterating that a well-balanced cyber-defence should be secured, vigilant, and resilient. He admitted that it was not easy to be 100 percent secured, but that it was possible to manage, to reduce the adverse impacts and to minimize the potential for business disruptions. He was proud to state that Deloitte was at the forefront of its cyber security agenda, which had been established in Europe and the United States. The said company was then looking to establish similar agenda in the Asian region or perhaps in Malaysia.

Keynote 2: Cyber Security – Strategy and Approach: Making Cyber Security Part of your Company DNA (11.30pm-12.00pm)

Speaker: David Francis, Cyber Security Officer, Huawei UK

The conference continued with the second keynote address from Mr. David Francis, Cyber Security Officer, Huawei UK. He began his presentation by highlighting the fact that cyber security was not merely an IT issue, but also a national issue, business issue, social issue and also an economic issue. Hence, he believed that it was essential to understand the basic concept in order to address cyber security issues. In this context, he stated that not only were the threats changing, the roles were also changing. The purpose of the attack was changing in terms of the politics, protectionism, monetary gain and hacktivism activities.

He rightly suggested that technology was everywhere and visible, with its massive benefits. Technology had fundamentally helped enhanced mankind for better education, better health, better economic output and better lifestyle choices. Nevertheless, the bad guys have exploited such technology and have enhanced the threats, which were becoming more

sophisticated than before. He said that technological growth has enabled the bad people to buy some technologies to attack the good people. As a double-edge sword, when technology and its uses were advancing at an amazing rate and brought substantial benefits to all, the threats to technology users were also rapidly increasing.

Mr. Francis then explained Huawei's experience in dealing with cyber security. Huawei was a world-class company and a leading global ICT solutions provider. Huawei had been serving for 45 of the world's top 50 carriers, which accounted for 77 percent of Huawei's revenue generated from the carrier network business. In addition, Huawei was also serving for one-third of the world's population. Business areas of Huawei consisted of carrier telecom networks, enterprise networks and easy devices. He also suggested that Malaysia was important to Huawei Technologies Co because the Huawei Southern Pacific Regional HQ was based in Kuala Lumpur. Besides, Huawei was a member of the Multimedia Super Corridor in Malaysia and also a partner with all major telecom operators including TM, Maxis, Celcom, and DiGi. He noted that such relationships have contributed to considerable digital and network development in Malaysia.

He explained that Huawei was very much pushing for strategy and approach in cyber security. Huawei made such security as part of the company and organisational DNA. He believed that such security should also start with the leadership of the company, within the organisations, within the social groups and also within the country. He suggested that similar to Huawei; companies must have the strategy, governance and leadership within the organisations. He observed that Huawei's CEO, Mr. Ken Hu, had shown the leadership standard when he believed that cyber security was not a problem for an IT department only, but rather a business issue.

He said that before 2003, cyber threats were committed by individual script kiddies but nowadays it had expanded to sophisticated expert hackers. It was hard to stop the tide of progress and technology innovation. Threats were increasing every day, and the bad guys were getting significantly more sophisticated. Nevertheless, about 80 percent of cyber security incidents could be addressed if companies and organisations could counter social engineering. He explained social engineering as a non-technical method of intrusion that hacker would use that relied heavily on human interaction and would often involve tricking people into breaking normal security procedures. He noted that such a technique was one of the greatest threats that organisations today would encounter. Mr Francis also highlighted that

the majority of security incidents would usually involve a human error. Many of these successful security attacks were from external attackers who preyed on human weakness in order to lure insiders within organizations to provide them unwittingly with access to sensitive information. These mistakes could be costly as they would involve insiders who often have access to the most sensitive information.

Mr Francis also observed that whatever Huawei had done in Integrated Product Development (IPD) Process was independently tested. He then said that if an organisation had a complex process, the question was whether cyber security was built into that process and whether such security was constantly updated. He later discussed the White Paper published by Huawei that had given some pointers on Huawei's approach to implementing a built-in strategy which embedded the change in the process.

Mr Francis also stated that Huawei had created a virtuous circle of "many eyes and many hands" in ensuring that it would continuously improve its knowledge, technology, people and processes. Such an approach had created a win-win-win process between the customers, the government as well as Huawei.

Mr Francis then observed that Malaysia had developed a clear cyber security policies and comprehensive approaches based on the well-developed ICT infrastructure. The National Cyber Security Policy had been designed to facilitate Malaysia's move towards a knowledge-based economy. Cyber Security Malaysia was established to implement that policy.

The speaker concluded his presentation by highlighting the development of networks that had advanced social progress in Malaysia. He observed that there were various benefits that open networks could reap. Such advantages included encouraging information flow and sharing, providing more opportunities for innovations, lowering the costs of innovation and helping to improve the world's health, wealth and prosperity. He also added that cyber security was not limited to a single country or a specific company. All stakeholders needed to recognize that cyber security was a shared global problem requiring risk-based approaches, best practices and international cooperation to address the challenge. He later noted that as a crucial company strategy, Huawei had established and would constantly optimize an end-to-end cyber security assurance system. Such a system

was a continual effort, and Huawei was committed to providing the best-in-class products and services to meet the needs of its customers.

There was no Q & A session at the end of this presentation.

Keynote 3: Threat Intelligence Driven Environments (12.20pm-12.50pm)

Speaker: James Calder, Client Service Manager, BAE Singapore

Mr Calder began his presentation by highlighting the seriousness of cyber security attacks in which such attacks had been committed on many multinational companies daily. Due to these attacks, he stressed the importance of cyber threat intelligence and how it could be used to prevent digital criminality. Such criminality was seen as a serious threat that led to the resignations of several CEOs who were accountable for the widespread breaches of personal data and credit card information of many customers.

He also noted the evolution of fraud attack methodologies in which cybercrimes and fraud have become more planned, organized and automated than ever before. Technology has been the platform of such crimes. He believed that the leveraging of social engineering and the technical elements had given rise to cyber fraud.

He differentiated between cybercrime, cyber-enabled crime and digital criminals. Whilst referring to cyber-crime as an illegal or damaging act in cyberspace, he defined the cyber-enabled crime as a crime that was facilitated through the use of cyberspace. He defined digital criminal as organized criminals who specialized in stealing money using cyber techniques.

He noted the two types of challenges posed by technological advancement: firstly, the Fraud Challenge and secondly, the Cyber Challenge. He defined the first challenge as an attack on the business process in which the method of the attacks was seeking to create or manipulate transactions. The primary goal of such attacks was financial gain. On the other hand, he stated that Cyber Challenge was an attack against the information technological infrastructure. The methods of such attacks were to steal data, control or disrupt the systems, and the primary goals of such attacks were information theft, system manipulation, espionage and the denial of service.

On the issue of intelligence-led security, he divided the threat intelligence into two types: firstly, the threat data, and secondly, the threat context. Threat data was part of the attacks and was related to the technical part, which could be the malwares, domain blacklists, open source reports and the RSS feeds. On the other hand, he referred to the threat context as identifying the perpetrator, understanding the impact of the breach and the response of the organization to such breach and finally taking informed decisions on the attacks. He believed that an effective threat intelligence management program would span all aspects of business change, people, process and technology. He then identified the following six steps that would enable organizations to develop their threat intelligence. Firstly, performing the threat assessment and secondly, determining the intelligence requirements. Another measure was building the collection resource and fourthly, operationalizing the threat intelligence; fifthly, introducing security analytics and finally, gaining the situational awareness.

Mr Calder then suggested the measures that would make the threat intelligence work. Firstly, the tactical approach to improve the ability of the network operations centre and the corporate security personnel to anticipate, prevent and mitigate cyber-attacks from across a broad spectrum, including amateurs, fraud, APT, DDOS and insiders. Secondly, the operational perspectives in improving the ability of Chief Information Security Officer, Chief Information Officer and Chief Technology Officer to change the use of IT for protection and responses. Thirdly, to engage the top management such as the Chief Risk Officer, the CEO and Board of Directors in making decisions about cyber risks.

Mr. Calder made a particular reference to the Shylock case study, in which the said malware was one of the most sophisticated and fastest growing threats posed by cyber criminals. Its creators have built a platform over the last two years which allowed them to commit large scale targeting and theft of sensitive banking data. The criminals have spread the malware by spreading links that led to downloads of the malware, either via spam e-mail or Skype instant messaging. Also, such malware was used to make fraudulent transactions that were costing the banking industry millions per year. The Shylock code framework was constructed in such a way that enabled more powerful upgrades to be added in the future. It combined various best-of-breed malware techniques for stealth and persistence, resulting in very low detection rates by antivirus products.

In concluding his presentation, Mr Calder remarked that collaboration with the government agencies, law enforcement, group of IT personnel and the academic research was the key concept in preparing and understanding more about the intelligence-led security.

There was no question & answer session at the end of his presentation.

Presentation 1: GRC Topics (2.00 pm- 3.00 pm)

Speakers: Mr. Megat Mohammad Faisal Khir Johari, Director of Risk Consulting of Deloitte, Malaysia

Mr. Megat began the presentation by emphasizing that cyber-security risks and reputational risks were inter-connected. He said that there was always a limitation in a trusted and secure eco-system.

He then proceeded with his presentation by citing Deloitte's 2014 Global Survey on Reputational Risks. The survey involved more than 300 participants particularly in Europe, America and Asia Pacific. The relevant sectors involved were government agencies, banking, and oil and gas companies. He stressed that a company's reputation and financial strength could be threatened by "keyboard warriors" anywhere in the world by defaming the organization and posting about it on social media.

He elaborated further that such cases were common in Malaysia, particularly since the last general election. The attackers could place a simple misrepresentation of an image that could lead to numerous remarks and comments, reputational issues and finally reputational and financial losses to the organization.

He further observed that in terms of business, reputational risk was the top key strategic business risks. The fact that 87 percent of the executives in the above-mentioned survey believed that reputational risk was more important than other strategic risks indicated the challenge of their companies to manage such risk. Moreover, 88 percent of the respondents thought that their companies were focusing on managing such risk. He urged that the company must ensure that all the controls and the efforts needed were placed in the right position when they managed this type of risk.

He argued that other business risks could also drive reputational risk. He stressed that the highest list of the fundamental risks that drove reputational risk were those related to ethics and integrity, such as fraud, bribery, and corruption. It was followed by security risks, including both the real world crime and cyber crime. Next in line were product and service risks involving risks related to safety, health and the environment. Third-party relationship was another emerging risk. Any company involved would also be held accountable for the actions of their suppliers and vendors.

The Deloitte's 2014 Survey also compared such drivers to five industries such as the Consumer and Industrial Products, Life Sciences and Health Care, Technology, Media and Telecommunications, Energy and Resources and Financial Services.

Mr. Megat also noted that the top three drivers of reputational risk today were similar to the top drivers recognized by companies that experienced major reputational risk in the past.

He stressed that in terms of geographical location, the USA was quite balanced. However, in Asia Pacific, product security was always the last. Most companies in Asia viewed security as less priority or were not significant.

He argued that reputational risk was a top management issue. He noted that the respondents in the Deloitte survey believed that the person responsible for such risk should be at the highest level of the organization. Whilst 36 percent believed the CEO was responsible, 21 percent thought the chief risk officer (CRO) should be the one. 14 percent thought the Board of Directors, and 11 percent believed the chief financial officer (CFO) to be responsible.

Mr. Megat stressed that global managing board together with senior leadership team were responsible for managing reputational risks. Close collaboration and with the support of their global governance, risk, and compliance department, corporate audit function, global corporate affairs, the investor relations and marketing officers is crucial.

Pointing out other key findings from the Deloitte survey, he further stated that customers were not the only main stakeholders in reputational risk. Other important stakeholders were the regulators, senior executives, employees, and investors. He observed that in the world of global social media, managing customer expectations and perceptions was an important task. In terms of geographical areas, whilst the companies in the USA were

more customer-centric than those in other regions, companies in the Asia Pacific region placed a strong emphasis on third-party suppliers.

Next, he pointed to the paradox of confidence and capabilities. He argued that the 2014 survey findings showed that companies were both over-confident and under-confident on reputational risk at the same time. He observed that more than 76 per cent view that their reputation was better than average. However, only 39 percent rated their reputational risk programs as “average” or “below average,” and only 19 percent gave themselves an “A” grade for their capabilities at managing reputational risk.

He then suggested that companies were least prepared for risk drivers beyond their direct control. He argued that most companies felt most prepared to manage the risks within their direct control. Most companies disclosed that they were more prepared to bring about reputational risk drivers in which they have direct controls, such as regulatory compliance and employee misconduct. However, they were less organized when the risk drivers were outside their direct control, involving third-party ethics, competitive attacks, hazards or other threats and environmental issues.

Moving on to the implications of reputational risk, Mr. Megat suggested that the loss of revenue and brand value were the key impacts. He argued that when reputational risk was out of control, there could be a wide range of negative impacts. He pointed out that according to the Deloitte’s survey, 41 percent of the respondents who had experienced reputational risk believed that the loss of revenue was the major impact. This loss was most accurate for consumer and energy companies. However, 41 percent believed that the loss of brand value was the main impact, particularly in life sciences and technology companies.

He observed that companies were focusing more attention and resources on reputational risk than ever before. Mr. Megat explained that more than half of the companies in the said survey (57 percent) indicated that they planned to give more attention to reputational risks in the future. The respondents stressed that the areas targeted for future investment and development would be technology and data to people and processes.

Mr. Megat then stated the leading practices and lessons from the front lines. He noted that the respondents offered a number of valuable understandings into how their organizations were tackling the challenge of managing reputational risk. He suggested that companies should identify the available

abilities and technologies, which should then be incorporated into the company's everyday business processes. Such measures could provide the decision makers with sensible ideas to address potential harms before they turn into calamities.

He indicated that reputational risk would become increasingly critical in the future, which meant that companies should continue to improve their capabilities in this area. As such, he argued that crisis management would be a critical capability for handling major reputational problems and an area that more companies should be investing. An effective crisis management approach would certainly benefit companies in avoiding any threats to their business. He suggested that such an approach should begin with identifying and preparing for strategic risks and included a broad portfolio of capabilities such as simulation, monitoring, risk-sensing, response, and communications. He emphasized that risk-sensing was significant because it could identify emerging problems while there was an ample time to avoid any threats. However, all capabilities needed to be in place in countering the crisis because it would be an absolute waste of time to develop a crisis management strategy while the company was running out of options.

In conclusion, Mr. Megat advised that as no company was 100 per cent safe, protecting the company's reputation and brand was a vital obstacle, which could still be manageable. He noted that any company could control its reputational risk if it were able to identify and incorporate such risk into their business strategy and to invest in the right capabilities.

Panel Discussion 1: Trust & Security Challenges in E-commerce (3.00pm – 4.00pm)

Speakers:
Dr. JJ Pan, Chief Privacy Officer & Public Policy Director, Asia Pacific Acxiom Corp.
Eneng Faridah Iskandar, Senior Director of Outreach & Engagement Division, MCMC
Eiichiro Mandai, Director, Overseas/ TradeSafe Corp. & CEO/ODR Room Network INC.

Moderator: Clement Arul, CTO, Principal Technology Architect, Security Consultant, Penetration Tester, Trainer, Chief Architect, Head of R & D, ISO 27001 Lead Auditor

The moderator started the session by highlighting the topic, which was related to the current trend and emerging threats to electronic commerce. He also stressed the importance of gaining trust to e-business and what good practices and good ethics for business order were. Mr Arul then showed a quick demo on what was the real threat in e-commerce by illustrating the Vietnamese online shopping incident. Here, the perpetrators had used technology to purchase anything at whatever price they wanted. Also, they could determine what they wanted to pay and could also change the value of the online selling products, since they had the option of whether to decrease the price or increase the discount. Thus, it emphasized the ease in which the perpetrators could compromise the contents and the privacy involved in e-commerce. In reality, much online shopping had faced this kind of problem. On the other hand, he also suggested that the threats could come not only from the consumer side or merchant side, but also from all angles including the government side.

Dr. JJ Pan, Chief Privacy Officer & Public Policy Director, Asia Pacific Acxiom Corp.

The first speaker, Dr. JJ Pan began her presentation by explaining the contents of her presentation, which was about trust and the secure eco-system, as well as the consumer confidence. She then stated that cyber security itself was already a very successful eco-system. She argued that companies needed the innovation, the Internet, the Internet of things and also a Trustmark. She believed that Trustmark could provide some confidence to customers and indicated to them that it was safe to do online business.

She later discussed the global innovation index, the most influential being the Organization for Economic Cooperation and Development (OECD) Index. A comparative analysis by the OECD of the new generation of national cyber security strategies revealed that cyber security policy making was at a turning point. In many countries, it had become a national policy priority supported by strong leadership. All the new strategies were becoming integrated and comprehensive. Many companies have approached cyber security in a holistic manner, encompassing economic, social, educational, legal, law-enforcement, technical, diplomatic, military and also intelligence-related aspects.

Dr. Pan also explained the Internet of things (IOT), which was a computing concept that described a future in which every day physical objects would be connected to the Internet. With such connection, such objects would be able to identify themselves to other devices, particularly, the mobile devices. Furthermore, the IOT was significant because an object that could represent itself digitally became something greater than the object itself, which

consequently could lead to the creation of more big data than before. Besides, in order to make all data meaningful and useful to individual and organisations, it would depend not only on the data and information, but also on the technology, the management, the process as well as the regulations.

In evaluating e-commerce transaction and interaction, she emphasized that it could be divided into three stages. Firstly, the pre-transaction stage which would involve making information more transparent and more marketing-oriented to consumer. Secondly, the in-transaction stage, which was about making e-commerce transaction more secure, more privacy and more data protected than before. Thirdly, the post-transaction stage, in which handling customer care and complaints would be made more easily and completely. She later explained the new emerging issues involving data protection, which was rather new to some countries. Since data was more utilized in the modern world, there were challenges to the privacy of data itself. Such challenges were not only faced by the government, but also by the private sector and the military.

She later argued that the biggest challenge was the interface between companies and the synchronization of data between country, borders and also organisations. Finally, she concluded her presentation by suggesting that for the public sector, there must be an efficient network with all the stakeholders. She added that whilst for the private sector, there must be a commitment to build and maintain trust and confidence of customers. Also, there must be an independent and fair bridge between the public and the private sectors for the intermediary sector.

Eneng Faridah Iskandar, Senior Director of Outreach & Engagement Division, MCMC

The second speaker, Mrs. Eneng began her presentation by posing the questions about what the government saw in e-commerce and whether computer users could control the technology or vice versa. She explained that under the Communications and Multimedia Act 1998, there were currently over 900 licensees operating as a network facility, survey, application and content application services. She also highlighted the rapid increase of Internet users in Malaysia. For example, in 2009, there were only 31.7 percent of users. However, in 2014, there was an increase to 70 percent of Internet penetration, not only in the urban areas but also in rural areas.

Apart from that, she indicated the statistic from Bank Negara Malaysia in 2014 showed that Malaysia had more than 17 million Internet subscribers. This figure would mean that many Malaysians were doing online transaction and had internet banking capability. However, the question was whether or

not they utilized such transaction. She then quoted the figures from the Department of Statistics Malaysia in 2013, which showed that only 15.3 percent of Internet users were ordering and purchasing goods and services online. The types of goods and services purchased over the Internet were mainly on fashion items such as clothes, bags and shoes.

Mrs. Eneng also pointed out that there were five main reasons for the unwillingness to purchasing or ordering any goods or services over the Internet as below:

No	Reasons for non-participation in E-commerce	Percentage
1	Not interested	69.5
2	Prefer to buy in regular store	49.1
3	Lack of knowledge or skills	41.8
4	Security purposes that concern about privacy and safety	21.4
5	No guarantee for product received	17.6

Source: Department of Statistics Malaysia, 2013

In regulating the communication and multimedia industry, she referred to the objectives provided under the National Policy Objectives of the Communications & Multimedia Act 1998 which included the following:

- to regulate for the long-term benefit of the end user;
- to promote a high level of consumer confidence in service delivery from the industry;
- to ensure an equitable provision of affordable services over ubiquitous national infrastructure;
- to promote the development of capabilities and skills within Malaysia's convergence industries; and
- to ensure information security and network reliability and integrity.

In conclusion, she stressed that we needed success story, and we must highlight the good aspects of e-commerce. Apart from the trust and security issues, the level of awareness and certainty in conducting online transaction must also be examined. As there were challenges for trust and security issues, the initiative for Trustmark was rather important as it could promote consumer confidence. Finally, she advised that in designing e-commerce websites, it should seem legitimate with simple contents and requirements, would build trust and friendly approach to e-commerce.

Eiichiro Mandai, Director for Overseas, TradeSafe Corp. & CEO/ODR Room Network INC.

The third speaker, Mr. Mandai discussed cross-border issues, Trustmark and e-commerce market. He also explained about online dispute resolution (ODR), which was a branch of dispute resolution that employed technology to facilitate the resolution of disputes between the parties. He suggested that efficient mechanisms to resolve online disputes would have an impact on the development of e-commerce. He also stressed that there were two sides or phases for an e-commerce market: the encouraging side and building trust side.

In relation to the encouraging phase, the government and business could encourage consumers to buy goods online and also encourage businesses to sell their products online, and thus it would lead to a competent market. Trustmark worked by promoting increased transactions in order to penetrate the retailers, the logistics and also payment services. On the other hand, relating to phase of building trust, he noted that when e-commerce market had been established, hackers might commit crimes affecting the e-commerce transaction and payment methods. Hence, consumer might lose confidence and, therefore, building trust became important. The ADR, ODR and also Trustmark would protect consumers and build a self-regulation approach by businesses.

He also emphasized that e-commerce was easy to conduct across border. However, he also observed the jurisdictional issues and applicable law problems that would arise from such transactions. For instance, a Japanese consumer purchased a UGG Australian boot on a Japanese language site with Trustmark BBBOnline, US, and pay via a Chinese bank. However, the goods were fake, and when the consumer made a complaint to the shop, there was no response. If the consumer were to send it back for a refund, it would be illegal export of fake goods. Thus, the consumer might lose both the goods and their money.

Mr. Mandai later emphasized that cooperation was the main factor for an e-commerce market: the Trustmark providers' co-operation, TM and ODR co-operation. He also advised on what consumers and businesses should do with the ODR and Trustmark. For the consumers, they must pay attention not to lose money while for businesses; they must keep their reputations in the market and not to be banned from the market.

He ended his presentation by suggesting that Trustmark areas could be improved by making it mandatory for users to participate in the ADR/ODR schemes and to comply with the decisions or recommendations made by the arbitrators. It would be useful for the consumers if an internal complaint handling system were being provided on the Trustmarks' websites and on the traders' websites in which consumers could address their problems with a certified trader.

Question & Answer Session

During this session, the first question posed to the panellists was on the trust being developed between the MCMC and the Internet users. Mrs. Eneng replied to this question by saying that not much the authority such as the MCMC could do because e-commerce trust was built by merchant initiative to encourage people to adopt best practices. Apart from that, MCMC and also Cyber security Malaysia could not give any mandate that the consumer must do certain things because it was a business investment. Besides, she said that e-commerce was a civil transaction and a contractual obligation (based on the willingness of buyer and seller), in which the MCMC as regulator could not enter into such a commercial agreement. She also added that since building trust was a key issue; we must work together with all IT professional in the country in order to ensure Malaysian Trustmark had a global branding and were fully recognized.

The second question posed to the panellists was on the integrity issue and also the concept of community within trust and security of e-commerce. Mrs. Eneng responded that in terms of integrity, the Internet blow up even further because the world has become borderless. Due to this issue, the Malaysian government had established the concept of digital citizenship, which encompassed issues relating to self-governance. She also highlighted that the Communications and Multimedia Act 1998 has an institutional framework for such regulation. She observed that the National Cyber Security Policy also emphasized on the positive use of the Internet and the issue of integrity as well.

The final question posed to the panellists was how Trustmark dealt with competitive intelligence. Dr. JJ Pan replied to this question by saying that Trustmark was a cross function system in which there was a centre or hub between users, businesses, government, as well as a third party. She then suggested that from the competitive intelligence point of view, Trustmark would look to the nature of the data itself in order to make such data more trustworthy, protected and more secure. She suggested that Trustmark should be seen as an eco-system issue. She further explained that Trustmark was not only a mechanism to assist the enforcement of the regulation, but also as a business tool to self-regulate, which would consequently promote further innovation.

Presentation 2: Are the Bad Guys Getting Smarter? (4.15pm- 5.15pm)

Speaker: Mr. Shaharil Abdul Malik, **Chief Technology Officer & Executive Director, SCAN Associates Berhad**

Mr. Shaharil began his presentation by highlighting the categories of bad guys as organized crimes gang, hacktivists, disgruntled staff or ex-staff and finally people from past personal relationship. He was of the view that the primary motivations of the bad guys were monetary gain, personal achievements, and revenge. In addition, he believed that national interest was also part of the motivation for state-sponsored hackers.

Next, Mr. Shaharil emphasized the fact that the cost of cyber crimes was reaching up to RM1 billion. He quoted the Security Threat Report 2013 which indicated that Malaysia as the sixth most vulnerable country in the world to cyber crimes, in the form of malware attacks on computers or smart phones. He stated that cyber crime was a lucrative crime compared to drug trafficking due to the benefits of such crime.

On the new wave or recent trends of cyber threats, Mr. Shaharil pointed out that such threats affecting Malaysia were the ATM skimmer, banking malware, ATM hacking and email interception. The impact of such cyber threats was the lack of trust towards the financial and banking systems in Malaysia.

He emphasized that the trend of future attacks could depend on the near field communication (NFC) and Radio-frequency identification (RFID), which were powerful computing tools for the attacks. Besides, he made a particular reference to the malware called Kasumi that intercepted the 3G/4G telecommunications networks. Also, the Dark Hotel malware and also Wire Lurker malware, which attacked the computing system and telecommunication devices and also were part of the future attacks that need special attention and action.

Mr. Shaharil concluded his presentation by suggesting that organizations and computer users needed to manage their risks properly. Such an approach was necessary because the bad guys or the hackers were always ahead in their technological innovation. Hence, identifying the risks could mitigate the problem caused by the hackers, technology, and the Internet. In addition, the human aspect must be an essential element for consideration in cyber security planning and strategy. Finally, he reminded the audience

not to disclose too much of their personal data over the Internet as it would trigger privacy invasion and the rise of cyber-crimes.

There was no Q & A session after the presentation. The Conference ended at 5.15 pm.