



# Executive Summary

## e-Security in the Broadband Age

27<sup>th</sup> March 2006

Microsoft Seminar Room  
23<sup>rd</sup> Floor, Three Pacific Place  
1 Queen's Road East, Wan Chai, HK

Microsoft sponsored the following Telecoms InfoTechnology Forum on e-Security in the Broadband Age, a topic of growing concern with the spread of “always-on” wired and wireless broadband networks, and a shift from nuisance spamming and disruptive hacking to more discrete and costly targeted attacks on enterprise networks by organized criminal gangs. How can the enterprise sector protect itself? And given that computer networking and Web-based services have become essential to the daily lives and business of SMEs and citizens, are the problems facing these sectors similar or different from those facing the enterprise sector? And can and should the Government do to help? Is it taking the right steps in the right direction?

### Session One

The first speaker **Dr. Joseph Lee, National Technology Officer, Microsoft**, explores a strategy for addressing the information security risks in the enterprise sector. Dr. Lee commences with a quick review of the threat landscape. The risk factor is increasing due to the heterogeneous nature of the ID/password system, the zero day or ‘almost instantaneous’ exploitation of IT system vulnerabilities, the involvement of organized crime, the involvement of company insiders, leading to more sophisticated, financially motivated attacks on corporate information systems. Dr. Lee then points out the size of the security problem in China. With China’s growing number of Internet users, the proliferation of intelligent mobile devices, the popularity of online gaming (‘a playground for hackers’), Dr. Lee informs the audience that the Chinese Ministry of Public Security announced that 88 per cent of PCs in mainland China are infected with viruses and spyware. Dr. Lee moves on to describing an information security strategy as characterized by policy, culture, and practice. He advocates a proactive *layered* approach to security (as laid out by the ISO1779 standard) to increase an attacker’s chance of detection and use that fear of being caught as a deterrent. Layers include focusing on user education, shoring up physical security, improving perimeter and internal network defenses, down to protecting the OS layer, the application software layer, and the data

layer. As part of this approach, Microsoft has issued the *Trustworthy Computing* initiative which is built around four pillars: security, privacy, business integrity, and reliability. Trust in people and the devices whom you work with (the trust ecosystem) can be achieved through secure code, IPSec, InfoCard, Plug and Play Smartcards, Certificate Lifecycle Manager, through engineering for security or 'security by default' (which means that unused features are turned off by default), through 'security by deployment', and through enhanced security features (IE Protected Mode, Windows Defender, SpyNet, etc.) to be found in Microsoft OS and middleware products. Dr. Lee acknowledges that simplicity is important and that means visibility, control, and context for the end user, consistent and integrated management for the IT professional, and common APIs, tools, and services for the developer. Dr. Lee concludes by stating that security is a shared responsibility along the whole trust ecosystem and this calls for partnership and co-operation amongst law enforcement, industry, public policy, and customer groups to raise awareness.

The second speaker **John Wong, Assistant Hong Kong Government Chief Information Officer (GCIO)**, places special emphasis on the importance of regular *system reviews* and *security risk assessments* to ascertain one's security status. In Hong Kong where ICT usage is high, John Wong acknowledges that there is no foolproof solution (unless you unplug everything) but counters that it is possible to minimise the risk and impact of security incidents by establishing an information security management framework and implementing the necessary measures to safeguard a company's information assets. The key outcome is to get to an *appropriate* level of protection. Monitoring of security measures should be undertaken to insure their effectiveness with a focus on high-risk areas that includes the interfaces of a company's systems to the Internet, the handling of classified information, and the protection of critical information assets and facilities (such as a company's computer centre). John Wong states the point of the review exercise is to avoid having a false sense of security, which is 'more dangerous than having no security', and should concentrate on four elements, those being policy, processes, tools, and people. He concludes with a distinction between threats that impact daily operation and those that affect business strategies, and cites the Cybersecurity review for the WTO Ministerial Conference held in Hong Kong in December 2005 as resulting in the government making a number of improvements to its staff awareness programme, incident handling, business continuity, and disaster recovery plans. An case of Hong Kong government leading by example.

The third speaker **Patrick Lam, Superintendent of the Technology Crime Division, Hong Kong Police Force**, starts out with some practical suggestions. Whereas in a traditional business deal one can make contact with one's counterpart face to face, with e-business, where most dealings are handled via email, has anyone thought of checking the IP address of the email source to verify its origin? Or asked the company's IT administrator to look at the firewall log? There is information readily available that would inform if someone is trying to hack into your system but few people take the time to access it. Patrick Lam cites Zone H, a website for hackers to show off their trophies (sites they have cracked or defaced). It certainly would not do your business any good if your company's website appeared on Zone H. Patrick Lam then proceeds to outline some

of the scams, from the 419 scam moving online which involves a proposition to partake in the inheritance of someone's dead relative (usually a Nigerian general or statesman) to e-shopping frauds. The 419 scam is popular because according to the FBI it is a US\$100 million per annum business (to this day!). To carry off such a scam requires an extensive network of skilled collaborators (and this poses a real challenge for the police), including a mastermind, a programmer, a website developer, a credit card counterfeiter, and a money launderer. Denial of Service (DoS) attacks have increased in frequency, targeting businesses that are heavily reliant on the Internet as a source of income. Patrick Lam emphasizes the need to work through the legal system in addressing these problems. But the issue of jurisdiction can be troublesome as attacks often start outside Hong Kong and can involve servers situated in multiple international jurisdictions. He concludes that the Hong Kong police is actively working with industry, anti-virus vendors, other governments, ISPs, and the public to thwart the new criminality.

The fourth speaker is **KT Yung, GM, Industry Development Division, HK Productivity Council**, and he looks at the issue of information security among HK SMEs, which is marked by a lack of awareness. KT theorizes that SMEs may have a higher ratio of attacks than larger companies simply because they lack the resources to handle security. In a 2003 survey 12 per cent of HK SMEs did not have any anti-virus software installed in their computers, 70 per cent did not employ any security staff due to the expense. Even though SMEs are not viewed as especially reliant on ICT to do business, the email function is becoming increasingly critical and exposing them to security threats. If a crime is committed through the 'hijacking' of your company's server, you can be legally liable for any third party losses. KT outlines some reasonable steps for SMEs to take to shore up their information security, starting out with knowing what kind of information and database should be protected (that which may be accessed remotely), then moving on to reducing risk by better password management (for example, ex-employees who can still access their account with the company), by carrying out regular reviews, by backing up if the email server goes down, by updating security patches. SMEs have gradually become more aware but are still confronted with resource constraints, especially the 'human resource constraint' (i.e. knowledge gap). To address the situation, the Productivity Council runs HKCERT which is active in tracking security incidents in Hong Kong and promoting general awareness.

The final speaker of Session One, **Thomas Parenty, author of *Digital Defense* (Harvard Business School Press)**, has a different focus and priority. He stresses the financial harm done by loss of intellectual property due to corporate espionage. Responsibility is primary due to poor controls within an organization's environment. The financial loss from the disclosure of a small bit of design information can be significantly higher than the losses incurred through PC downtime due to viruses or deleting spam email. A leak caused one automobile company to lose around US\$1 billion. From an organizational perspective, Thomas Parenty sees two problems, one, that companies are restrained from 'doing good' security-wise because this is perceived as slowing down production lines, thereby affecting quarterly results and displeasing Wall Street analysts; two, there is a disconnect between the business people responsible for growing the business and the IT department staff responsible for providing the underlying

infrastructure. Without adequate input from the business side on what they are actually supposed to accomplish, the IT side end up designing poor security systems, ones which do not match the business processes they are intended to secure and in the end just impede doing business. The technological challenge is heightened by the fact that more systems are interconnected and interoperable across organizational boundaries. System integration allows access to a new breed of 'insiders', be it a company's suppliers, software vendors, or government regulators, people over whom one has no organizational control. These people, again from a dollar perspective, cause more harm than any intelligent hacker. Thomas Parenty is critical of third-party security standards, currently in vogue, as being, in some sense, too generic. They are capable of passing an auditor's test but fail to match the actual, specific business processes. This lack of rigor, once again, results in a disconnection when it comes to assessing a company's security, where, when you scratch a little beneath the surface, systems do not gel with policies (for instance, passwords go unencrypted). He concludes that businesses should focus on protecting their information and not just on generic infrastructure. He moves on to address the roles to be played by 'NGOs' (academia, industry associations, etc.) and governments. Industry associations should, one, work on getting better standards in terms of securing inter-operability between systems, leveraging off the work done by the Liberty Alliance and SAML (security assertion markup language), and, two, educate corporations on better ways of controlling access to information by insider populations. As for governments, it is far better for them to impose penalties for failure than to legislate technical requirements, because such legislation is time-consuming, becomes rapidly obsolete, and does not address the fundamental issue of whether or not the information is really protected. He concludes with this aphorism, 'Wonderful technology without policies is not particularly useful, because the technology will not be appropriately employed. Wonderful policies without the appropriate underlying technology is similarly not useful because they don't actually apply to anything real.'

## Discussion

**Alex Yu, HKTUG**, chairs the discussion and shares some of his views with the audience. Alex believes that it is beneficial to push for a *certification process*, led by the government or by security organisations, whereby the certification will be well recognised, well-accepted, and will become part of industry best practice to protect information. On the consumer side, He notes the proliferation of tokens (providing one-time randomized passwords) rather than a single security device to address consumer needs. The result is that 'my choice will come down to one thing, which bank I will trust, number one, and the second is which device I shall carry'. He calls for industry and government to drive common standard.

In response to a question about security analysis, **Thomas Parenty** responds that it is comprised of 4 elements: (i) what is the confidentiality of the information transmitted and stored, (ii) how authentication is done at the user level, then deeper at the application to application level, and finally at the host to host level, (iii) access control, and lastly (iv) accountability. He acknowledges that information security is beyond the knowledge of

any one person. 'It's incredibly difficult to know what the right thing is to do because there are too many moving parts'.

A question is raised about the penalty for failure and who should shoulder it (the organization itself or the vendors to whom it outsources security responsibilities), especially in light of the recent leakage of a confidential police complainant list. **Thomas Parenty** feels that the responsibility resides 100 per cent with the organization regardless of where the data lies. **KT Yung** feels that a penalty cost could affect the business operations of SMEs. **John Wong** points out that Service Level Agreements (SLAs) are part of the Hong Kong government's outsourcing policy and that, in addition to those contractual obligations, there are general laws in place to protect privacy. A hacker runs the risk of breaching criminal law in Hong Kong. **Dr. Lee** mentions that ERP software nowadays operates on the WS star standard which has the sub-standards WS trust, WS policy, and WS reliable messaging. A company must comply with these standards if it wants to transact electronically with Microsoft. **Patrick Lam** observes that the Hong Kong police would take into consideration whether the technology and policies were in place to prevent such a disclosure of confidential information, and that it is important that people rely on the enforcement agencies to catch and prosecute the right people. **A participant** says that the consequences of any loss incurred will be suffered by the affected business or government agency and not by the vendor so that it behoves those organizations to make sure they take the appropriate measures themselves, and be vigilant in their monitoring. **Alex Yu** echoes that comment by finishing off the discussion with the thought that once customers become aware that a service has been compromised and their information exposed their first response is likely to stop doing business with the service provider.

## Session Two

The first speaker of Session Two is **Wilson Cheng, Principle Consultant, OASYS Limited**, and he performs a comprehensive review of the threats and responses in the information security sector. At the outset of his presentation, Wilson Cheng delineates the traditional or 'normal' threats which assail the perimeter of one's hard disk drive as (i) malicious code outbreaks, so viruses, Trojans, and worms, (ii) spam or unsolicited bulk email, and (iii) phishing. According to MessageLabs, an email processor in the UK, an average of one in 30 emails carried a virus in 2005, and spam accounted for nearly three quarters of all emails sent. A reachable email account is so valuable to spammers that often people advocate not to hit the unsubscribe button since this is a sure indicator that the email account is active. The US ranked as the worst country in terms of spam origination, with China in second place, Japan fourth, Taiwan fifth, and South Korea in seventh position. Unfortunately for Hong Kong it came in the ninth spot, indicating that spam is a considerable problem locally. The cost of addressing these threats is spreading, whether it be productivity loss or data loss. That loss is mutating into information theft (in many cases, identity theft), with the thief either coming in through an external broadband connection that is conveniently always-on and taking over a computer remotely (turning it into a zombie) or, in some cases, internally. A man in Hong Kong was recently arrested for hosting copyrighted information on his PC that could be illegally downloaded even though he had no idea how to operate a PC. He had not been

aware of what his two daughters were up to. Phishing plays on the human psyche when one is tempted to click on an official-looking link. To trace down a fake Bank email one would have to go halfway around the world, across multiple domains, to find out where the server is. Even venerable e-commerce sites like eBay are prone to phishing incidents but eBay has the procedures in place that allows them to react quickly and access a customer's account to fix the problem. Ominously, there are new threats emerging, and one of them is spyware. Spyware is when adware takes an evolutionary leap, from a piece of software or freeware that was originally intended to collect demographic information on who was visiting what website to malicious code that sneaks into your PC when you click 'close me' on a popup window and assumes control or surreptitiously collects passwords and usernames. The popularity of devices like the iPod which has a huge amount of storage space (up to 40 Gigs) has led to 'pod slurping' where one simply attaches the iPod to a PC via a USB port and downloads that PC's contents. The proliferation of wireless devices has also lead to new security threats. Bluetooth can let someone synchronize with your PDA and pull your contacts. If a WiFi network is incorrectly configured, freeriders can jump on and surf the Net. Many staff see corporate policies as unnecessarily restrictive and will sneak in a wireless access point inside their cubicle, breaching security, or WiFi in conference rooms is often unsecured. Corporate policies often fail to cover technologies like Instant Messaging which is unencrypted and bypasses an organization's servers or P2P or webmail which can easily leak information into the public domain. With a 2 Gig storage for a Gmail account, that can amount to a lot of lost data. What consumers and small business owners can do to protect themselves is similar, in many ways, to the measures taken by enterprises but on a much smaller scale, such as adopting a layered approach, doing a security background check on your contractor, conducting regular firewall scans, implementing inbound/outbound traffic rules, deciding which ports to block, updating anti-virus software, and using encryption. At home one must also consider a Websurfing policy for children in dealing with inappropriate content. For Wilson, in the end security is as secure as the *weakest link*, often those telecommuting from home, and a lot of security breaches come about because people are not aware what they can and cannot do on the Web.

The second speaker is **Henry Chang, Head of Information and Communications Technology Division, OFTA**, and he outlines the Government's proposal to contain unsolicited electronic messages (UEM) that are commercial in nature. Legislation is not the silver bullet; its only one tool out of a basket of measures against spamming. In February 2005 the Government launched the STEPS campaign which involves strengthening existing regulatory measures, technical solutions, education programmes, international partnership and legislation. The Government is leaning towards adopting an opt out regime in which users decide whether to receive or refuse spam by unsubscribing. This means that e-marketers have the right to send the first electronic message, with the recipient having the right to read the message before deciding if he/she wants to receive more such messages. The second principle the Government has decided to follow is to leave room for the development of e-marketing, which can be a useful business tool for Hong Kong SMEs to reach out to potential customers. This third and the fourth principles are to avoid HK becoming a haven for illicit spammers and not impairing freedom of speech and expression respectively. The last two principles are that penalties and

remedies will be proportionate to offences and enforceable with reasonable effort. The legislation will embrace all existing and future technologies such as telephone, fax, SMS, MMS, email, instant messaging, VoIP (SPIT), and prerecorded messages. Only spam with a HK 'link', those that are sent from Hong Kong, via Hong Kong, or target Hong Kong users, will be targeted. This is the scope of jurisdiction. Exclusions will be made for person-to-person promotional calls (telemarketing) because of the associated high costs and those acts covered by existing TV and radio broadcasting regulations. The Government is contemplating setting up a do-not-call register but there is no current plan to set up a do-not-email list. Such a list would be open to abuse, too valuable for spammers who could not resist the temptation of using such a list illicitly. OFTA will enforce part of the law and will send out notices to those who break the law. An e-marketer would have 10 days (some have called for this being extended to 31 days) to sort out their list of who can/cannot be called. Failing to do so could result in fines being levied. Serious offences involving fraudulent acts, such as hacking, the use of zombies, falsification of registration details and heading information, or any other acts that generally try to conceal or alter sender identification, will be handled by the police. Many of these fraudulent acts are already offences under the present legal framework, with culprits facing the possibility of jail time. This approach of technology neutrality is flexible and the code of practice can be expanded to incorporate new types of spam, with the possibility of exemptions to owners of compromised PCs and exemptions for non-commercial UEM (such as those sent out by charities).

The third speaker is **Yvonne Chia, Partner, Stevenson, Wong & Company** and she addresses Hong Kong's case for setting up a do-not-call registry. Her main criticism is that the current OFTA proposal needs sharper teeth because spammers get away legally with that 1<sup>st</sup> round of spam emails and are 'forever guaranteed to be forgiven'. Two-thirds of the world's anti-spam laws actually adopt the opt out approach, which is quite fitting for HK. A registry (even if it does not include email) would restore the right for recipients to say no. Mobile spam, for instance, is a nuisance because if you answer the call while in China, you will pay HK\$9 for roaming charges. At the moment it is up to OFTA to decide whether or not to set up a registry. Will it put the registry online, so that everyone can see it? Yvonne Chia thinks only telemarketers who have registered and are required to comply with the rules should be allowed to see it and have their own profiles, uploaded so they are more traceable.

## Discussion

The first couple of questions focus on the difficulties of implementing an Opt Out scheme. **Henry Chang** acknowledges that even Australia is having difficulties with an opt in scheme. One problem is that political parties and charities that are supposedly exempt often rely on 3<sup>rd</sup> party 'telemarketers' and this raises the chance of fraudulent messages soliciting for charities (see some of the spam that surfaced after the Asian Tsunami). **Allan Dyer with the IS Division of HKCS** (who joined the panel discussion) argues that the opt-out approach won't work; that HK should be going for an opt-in approach because how can the end users be sure who they are sending the response back to? There's no feasible way to be sure that it's sent back to a responsible telemarketer or an irresponsible

spammer. **Sin Chung Kai of Legco and the Anti Spam Alliance** (who also joined the panel discussion) says that if he were a customer of that particular company -- for example, a bank or a telephone operator, someone with whom he already has a subscription with -- then he may try to unsubscribe that particular mail. **Henry Chang** adds that legislation needs to strike the proper balance. The Australian opt-out regime has demonstrated their SMEs are loosing out in the global market place because they had to be bounded by an opt-in regime while many of their international competitors can operate under an opt-out regime. A participant comments that 15 years after a scheme -- a totally unsuccessful scheme, as it turns out -- was set up to stop fax spamming, why is the onus still being put on the victim, on the recipient, who at the end, in one way or another, is paying for the service to give a spammer a free ride? So, in the end, does it matter whether you go opt in or opt out? **Henry Chang** concludes that if you are a spammer, you are not going to care about whether a jurisdiction is running opt-in or opt-out; you just hit a button.

A question is raised about the TCP Port 25 relay used by spammers.<sup>1</sup> What should ISPs in HK do? A panellist answers that if you want to run an email service, you have to use that port, making it difficult to block outright. Many HK ISPs block that port for consumers who are not likely running an email server (zombie problem). That provision is to be found in the HK ISP code of practice. But **Allan Dyer** points out that HK is ranked quite high on spam list so there is a problem with opening port 25 by default. Letting unauthorised open relays be used is not good practice.

A question is asked about the feasibility of including email in a do-not-call/ email registry? **Yvonne Chia** points out that the FTC (Federal Trade Commission) in the US has done a study and the security concerns outweigh the benefits of amassing such a registry. Millions of valid email addresses would cost millions of US dollars for a marketer to collect and email is seen as more private than a telephone number which after all is readily available through the Yellow Pages. **Sin Chung Kai** adds that do-not-call telephone lists have been around for several years, and at least it is proven in other parts of the world. People in HK are upset, and are calling for legislation now. The anti spam legislation has been two years in the making. If HK tried something as yet not proven that would simply delay legislation even further. If the US are successful in a making a do-not-email list workable, we can amend HK legislation later. Others expressed concerns that cryptographic hash of email addresses wouldn't work and that there are other normal methods for advertisers to get out their messages to a wide audience such as posters, TV

---

<sup>1</sup> 'TCP Port 25 is one of the core interfaces of the Internet, through which Internet mail servers typically send mail to each other. It's normal for users to send data out port 25, but they do so to their own ISP's mail server, from which it is forwarded on to the appropriate location. This is the server identified as the outgoing mail server in the mail client configuration. But if you are infected with a spam zombie—typically, a mail worm with a backdoor used by a spammer to cause your computer to send out massive amounts of spam—the mail does not go through your mail server. It probably goes directly to the server of the target domain for the spam message. The overwhelming majority of users have no need to do this and are perfectly well-served by sending all their mail through the ISP mail servers. It's also worth reiterating that the block need only be put on consumer client systems, not on higher-end services.' Larry Selzer, *Shutting Down the Highway to Internet Hell*, eWeek.com @ <http://www.eweek.com/article2/0,1759,1784276,00.asp>

adverts, and websites on the Internet. **Henry Chang** added that OFTA would be looking at the nature of message, not the organization. So if a charitable organisation wants to sell T-shirts through email or fax or whatever, they will be covered by the legislation, because that is where the money is.

## Conclusions

- There is clearly no one solution to the threat of cyber-crime or indeed cyber-nuisance. What does become clear is that e-security starts with a focus on the problem. Whether it involves an enterprise, an SME or a citizen the principle is the same: study and think about the risks and what is at risk. Since 100 per cent security is an impossibility it is important to judge what needs high security and what can do with lower security because security is costly (time and effort and money) so there have to be trade-offs or cost-benefits. Which information and files can organizations and individuals afford to have 'stolen' or 'lost' and which not? In this sense, the decision is like taking out an insurance policy, where the cost of insurance may not justify insuring everything to its full replacement value. The important thing is that everyone thinks about it and does the calculations.
- The major loss to an enterprise probably lies in its intellectual property. Industrial espionage and cyber-hostage taking, DDOS attacks, etc., are often perpetrated with insider information, so inward security is as important as outward security, and security trails are important. (The likelihood of detection can be a deterrent in cases of opportunistic crime.) The weakest links may also be in ties with third parties and these need especially careful scrutiny.
- SMEs are vulnerable because they often lack the resources (human, financial and technical) to fully understand the nature of the threats and how to deal with them. Apart from the need to 'lock the stable door *before* the horse has bolted' one suggestion that arises from the discussion is assistance through a certification process and the establishment of an industry standard. The HKPC already offer a HKCERT programme, but this could perhaps be extended with Government encouragement to provide security services (in some cases on a cost-recovery basis) for SMEs, possibly outsourced to specialist security companies.
- Citizens are being offered an anti-spam bill with an opt-in provision. This is being justified on the grounds that legitimate tele-marketing business should not be penalized, but for many consumers this will prove frustrating. The proof of the pudding will lie in its eating, but there seems to be sufficient public concern to justify a careful monitoring and revisiting of the legislation within, say, two years to see how effective it has been.
- The advance of technology will always offer the hackers and spammers and criminals (and terrorists) new opportunities to intrude into the private domains of enterprises, SMEs and citizen's lives, and this more or less goes with the territory. Society will learn to live with it and to handle it, but human error and culpability, not technology, will always remain the weakest links in the battle against it. Laws are only helpful up

to a point because it is impossible to legislate against human behaviour. Creating awareness and a systematic mode of thinking about e-security is the key. Government and the private sector should focus some joint effort in discussing how to achieve this. The lessons of the security review of Government ahead of the WTO meeting in December 2005 could be used as a basis for such discussions.