Innovation and Technology Association (ITA)'s response on 2004 DIGITAL 21 Strategy Consultation Paper

1. Wireless Access Point or Wireless network security with IDS/firewall/AV

The potential threats to WLANs are numerous. Denial of Service (DoS), session hijacking, and sniffing are just a small sample of the potential attacks. While many of the attacks against wireless networks are similar to those against wired networks, 802.11 networks are generally subject to more threats. One of the more serious problems is Wired Equivalent Privacy (WEP), the data encryption standard for wireless networks. WEP has been found to have weaknesses and can be "cracked" in as little as a couple of hours. According to IDG, there will be a great growth of wireless LAN users. Therefore IDS, firewall, Anti-virus and VPN are recommended for prevent hacking and protecting the networks in wireless network in the new 2004 DIGITAL 21 Strategy.

2. Policy Enforcement

No matter the system is perfectly designed; there are many possible ways to harm them, e.g. people will make careless mistakes which cause the computer becomes unstable. So, policy enforcement is suggested for in-depth protection of the whole system. For example, Blaster/Code red caused a lot of problems for corporate. Blaster/Code Red caused a lot of problems as many computers are not updated or patched regularly. Policy Enforcement prevents this type of problems, such as normal users cannot modify the configuration of the systems. As most of the virus/worms required computer users with administrator rights modifying computer settings. Policy Enforcement by controlling PC, email or resource usage can prevent this kind of problem occurred. Therefore, we will recommend Policy Enforcement in the new 2004 DIGITAL 21 Strategy.

3. Multifactor Authentication

To authenticate a human user, there are three categories of things an authentication system can depend on:

- Something the user knows (e.g. passwords, PINs)
- Something the user is (e.g. facial recognition, palm line, fingerprints, retinal scans)

Instead of using password-only system, which has caused a lot of weakness (e.g. brute-force attack or weak password) and a lot of overhead (e.g. password management or password revoke) it is recommended to use authentication with

multiple factor, i.e. Multifactor Authentication.

Multifactor Authentication is more secure than simple password security because it forces the user to provide something they know (a password or PIN) along with something they are (face, fingerprint, palm etc.). This ensures a high likelihood that the user is who they claim to be, and not someone who has either snooped the password, or stolen the token.

Multifactor Authentication takes the next step by grading the security associated with specific resources, and enforcing a level of authentication commensurate with the security needs of the resource. For example, a user might be able to log into a standard server from within the network with just a password, but might need their 'face' to come in via VPN, and might need a thumbscan (with a password) to access the Finance server. Therefore, we will recommend Multifactor Authentication in the new 2004 DIGITAL 21 Strategy.

4. Non-intrusive and touch-less biometric solution

Biometric Requirement recognition is a worldwide requirement nowadays, for example USA machine-readable passport with biometric record. It should be traceable and non-intrusive biometric solution. Moreover, according to the experience of SARS, touch-less biometric solution would be recommended for government use.

In the process of screening visas and passports in the United States and abroad, biometrics will be a useful adjunct to existing screening processes that identify individuals who might be terrorists, criminals, or other aliens who might represent a security risk to the United States. There is a growing trend for the deployment of biometric solution. we would recommend non-intrusive and touch-less biometric solution in the new 2004 DIGITAL 21 Strategy.

5. Email Anti-Spam on PC level (together with the gateway)

Nowadays, spam mail becomes a serious problem on internet. It wastes a lot of network resources and manpower to delete/filter spam mails. Furthermore, they may include some virus, which may cause the companies lose a lot of valuable data. Many companies provide gateway anti-spam software to solve this problem. In addition to this, we would recommend to include Email Anti-Spam function on desktop level to provide more customized and effective Email Anti-Spam ability in the new 2004 DIGITAL 21 Strategy.

6. Visible Audit Trail

The term ‘Audit Trail’ is used for an electronic or paper log used to track computer activity. For example, a corporate employee might have access to a section of a network in a corporation such as billing but be unauthorized to access all other sections. If that employee attempts to access an unauthorized section by typing in passwords, this improper activity is recorded in the audit trail.

Audit trails are also used to investigate cybercrimes. In order for investigators to expose a hacker's identity, they can follow the trail the hacker left in cyberspace. Sometimes hackers unknowingly provide audit trails through their Internet service providers' activity logs or through chat room logs.

Security policy nowadays, no matter in government or corporate, usually stress that keeping Audit Trail is a must. **Anyway, existing ‘usage LOG’, ‘access LOG’ or ‘security LOG’ usually only tells the result – system being hacked. It is hard to track back hacker identity. Therefore a new concept about Visible Audit Trail is recommended.**