YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Yui Kee Computing Ltd.

Newsletter

July 2009

Contents

Intel Claims Buying a New PC Prevents Virus Incidents

<web-link for this article>

A study performed by Techaisle.com and widely publicised by Intel has found that PCs older than 3 years have greater maintenance and support costs, including a higher number of virus incidents. Not surprisingly, Intel is using the report to promote PC sales, in a blog posting, Intel spokesperson Scott Smith says, "A new PC can have other benefits – reduced downtime from viruses".

This has important implications, it claims there is a casual link between buying a new PC and reducing virus incidents. If the claim is true, it could revolutionise the Anti-Virus industry. Perhaps we can buy a new PC every week and stop paying for anti-virus software. Or perhaps we can study what it is about buying a new PC that reduces virus incidents, and get the same effect in a different way.

Examining the study report, the picture becomes clearer. The study looked at two categories of businesses, small (<100 employees) and medium (>=100 employees). The figure used for demonstrating the higher number of virus incidents is described in the report as, "Email borne virus attacks", but there are other malware categories, these are the figures for the number of security incidents:

Incident	Small Buisnesses		Medium Businesses	
	PCs>3yrs old	PCs<3yrs old	PCs>3yrs old	PCs<3yrs old
Email borne virus attacks	3.2	2.6	5.3	2.7
Denial of service/phishing attacks	1.7	1.6	2.3	1.3

Viruses resulting from visiting websites	1.6	2.1	2.6	1.8
Adware and spyware infections	1.4	1.2	2.3	1.7
Theft of data by others	1.2	1.0	0.0	1.0
Theft of data by employees	1.0	1.0	0.0	1.4
PC downtime resulting from network intrusions (hacking)	1.0	1.2	1.0	1.3
Theft of PCs (eg: at airports)	1.0	1.1	0.0	1.4
Total	12.1	11.8	13.5	12.6

So, the number of security incidents is still higher for the older PCs, but the difference is less dramatic than the 28-58% change for email borne virus attacks. What might the causes of the difference in malware incidents? Here are some guesses, with speculation by our Chief Consultant, Allan Dyer:

- New hardware is more secure. *Highly Unlikely - malware is a software issue.*
- New hardware comes with new software. *Likely. But why is new software significant?*
    - New software is more secure. *Debatable.*
    - Less malware exists for new software. *Possible. Some malware is dependant on particular software versions, there will have been less time for development on new software, and malware authors tend to target mainstream versions, new software might be less common and therefore less targetted.*
    - New software often has bundled 1 year anti-virus. *Possible. This would suggest that some companies are not renewing or replacing the bundled solutions when they expire.*
- Regular hardware replacement is an indicator for strong PC management, including good security measures. *Likely. In this case, companies are providing resources to maximise the benefits from their IT systems, and this manifests as both regular PC replacement, and strong malware protection. If this is the case, then companies could benefit from reduced security incidents by strengthening malware protection instead of buying new PCs, but Intel might not want to emphasise that.*

Further study is required before we can safely move to a "PC a week" regime.

More Information

Techaisle Global Small Business Economic Impact Study 2009
To Chuck or Not To Chuck that Old Computer…
Intel pro-tip: replace PCs within 3 years to keep costs down
Intel to SMBs: Don't hold off PC refresh
Delaying PC refresh will cost SMBs money: Intel
SMB strategies from Intel, ASUS and Gigabyte

“‘.hk’ for Everyone” is not a Communications Panacea

<web-link for this article>

Allan Dyer

In the June 2009 issue of his corporation's newsletter, Jonathan SHEA (CEO of the Hong Kong Internet Registration Corporation Limited (HKIRC)) advocates every Hong Kong person being given an online identifier that includes access to a virtual file folder and a personal email address in the .idv.hk domain, and linked to their mobile phone number. He envisages that it could be used as an instant notification system during an emergency, such as a typhoon, without extra effort in collecting personal data or email addresses. He writes, "Whenever an incident occurs, all government departments, public or private organisations or institutions, and schools, could send their messages to everybody's virtual file folders. Messages would then be instantly broadcasted*sic* via mobile phone text message reminders."

Although such a scheme would be immensely beneficial to the HKIRC (full disclosure: I am the voting representative of Yui Kee Computing, which is a Member of the HKIRC in the Demand class), as it would guarantee a large number (about 7 million) of domain registrations and make necessary Government expenditure to support HKIRC in the management of those domains, the benefits for Hong Kong are less clear. Some points that should be more fully discussed are:

- Registration.
  - Which department would be responsible for allocating the domains? The Immigration Department would be the obvious choice, as only they have a complete list of Hong Kong people.
  - How would domain names be chosen or allocated? Mr. Shea gives the example of "me@sammy.idv.hk", but Sammy is a common name, so there would be a lot of competition for it. Using ID card numbers would be reusing an identifier that is already over-used (inadvisedly) as a supposed "shared secret".
  - Who would be responsible for ensuring that the phone numbers are up-to-date?
- Text Messaging
  - Capacity. Can the mobile phone providers cope with 7 million simultaneous messages?
  - Timeliness. On occasion (though not recently - I changed service provider) SMS messages to me took four days to arrive. Even a delay of four hours could make an emergency message redundant.
  - Charging. Who pays for the messages? Who pays for roaming charges when recipients are overseas?
- Access and Applicability. Who decides which, "government departments, public or private organisations or institutions, and schools" are permitted to send messages to everyone? Does one school have any message that *should* be broadcast to every Hong Kong person? The obvious solution would be to create a list of affiliations, but who collects and updates the list, and where is is stored?
- Security.
  - How will the vast amount of personal data needed for the scheme to be effective be protected? It will be a very attractive target for marketers, but many organisations will need access to update their part of it.
  - If the email addresses are predictable, they will be an easy target for spammers, if they are unpredictable they will be difficult for people to remember and use.
  - The virtual file folders provided for each person will be another attractive target for data thieves. If the security is made strong, then it will be difficult for the digitally-inexperienced, the main target of the scheme, to use.

There is merit in encouraging more people to benefit from using digital communications, and there is merit in utilising digital communications to disseminate emergency communications. However, combining the two ideas in this massive scheme generates a host of difficulties and inefficiencies. We are better served by *ad hoc* alert mechanisms for different incidents, that we can choose to subscribe to with the relevant organisation.

More Information

HKIRC Newsletter 2009
"'.hk' for Everyone" Makes Hong Kong a Digital City

Hong Kong Monetary Authority Requires Banks to Combat Internet Banking Fraud

<web-link for this article>

The Hong Kong Monetary Authority (HKMA) has issued a circular requiring banks to step up security controls for their internet banking services after recent online fraud cases. Between April and June, eight banks discovered attempts to steal login credentials of customers.

Hong Kong banks already have a number of controls in place to prevent online fraud, including tokens providing one-time passwords for two-factor authentication, but the attacks are using trojan keyloggers to capture the login credentials, including the one-time passwords. The stolen credentials are used to make unauthorised fund transfers.

One of the security measures is that banks are required to notify their customers immediately via a SMS message after completing an online high-risk transaction, such as transferring fund to an unregistered third-party account. Customers are advised to check such notifications carefully, and notify their bank if there is a problem.

Roy Ko Wai-tak, manager of the Hong Kong Computer Emergency Response Team Co-ordination Centre (HKCERT), said that the onus was on online banking customers to protect their accounts, "The banks have already adopted security measures like two-factor authentication. The key issue now is whether the customers' computers are clear [of malware] ... if they've been infected, it's like they are leaving their front doors unlocked."

Yui Kee Chief Consultant Allan Dyer commented, "You should only operate your online bank account from a computer you really trust: probably your personal laptop or home computer, running only the software you approve. Online banking without anti-virus software is like lending your chequebook to Mr. A. Thief."

More Information

Banks told to bolster security after online fraud
Strengthening Security Controls for Internet Banking Services

Sophos Sit-Com

<web-link for this article>

Unsatisfied with their success as a leading anti-virus company, Sophos has decided to diversify into comedy with "The IT Vigilante". The bodysuit is very orange and may disturb those of a nervous disposition. Connoisseurs of IT Security fashion may also remember "Captain F-Secure" and Symantec's men in yellow suits.

Don't give up the day-job, guys.

More Information

The IT Vigilante

Sophos's CTO Criticises Windows 7 Security

<web-link for this article>

Sophos's Chief Technology Officer Richard Jacobs asserts that security is not Microsoft's first prioty in a blog posting. He explains how Windows 7's XP mode will, effectively, double the number of PCs organisations need to manage - including for security software, security settings and patches, without providing a built-in way to manage the complexity.

More Information

Guest blog: XP mode - demonstrating that security is never Microsoft's first priority

Facebook, Advertising and Privacy

<web-link for this article>

The implications of scoial networking in general, and Facebook in particular, are under renewed scruitiny after a man with a Facebook account saw an ad for a singles Web site appear on his page accompanied by his wife's photo. The man's wife had not become a member of the site in question, but the third-party advertiser used the photo from her Facebook profile anyway. Facebook says it was a violation of the site privacy policy and banned the advertiser.

However, the incidents highlight the fact that not all advertisers obey the rules, and might get away with it for some time before being reported. Facebook does have a wide range of options for users to control how their information is used, perhaps too many separate controls and it is often unclear what each option affects. Facebook applications also take advantage of social pressure - friends 'invite' you to join them in using new applications, each of which requires access to your personal information, and it feels like insulting a friend to reject the requests.

Facebook and other social networking sites have grown enormously by playing on people's dislike of appearing anti-social, but will they face a downturn as people become more aware of how their information is misused?

More Information

Facebook slaps faces on ads
Facebook photo marketing privacy issue is drawing attention
Oh, you obviously didn't check Google then..

BIND vulnerability allows DNS DOS

<web-link for this article>

System administrators have been urged to update their BIND (Berkeley Internet Name Domain Server) installations because of a vulnerability that can allow an attacker to crash master servers by submitting a malformed update message. Slave servers are not vulnerable. BIND is the most common DNS software on the internet. The newly-released versions, 9.4.3-P3, 9.5.1-P3 or 9.6.1-P1, which defend against the flaw are available from the Internet Systems Consortium, the developers of BIND.

Exploits are already in circulation.

More Information

BIND crash bug prompts urgent update call
Internet Systems Consortium
BIND Dynamic Update DoS

Red Faces for Security Gurus

<web-link for this article>

Prominent security gurus, including Kevin Mitnick and Dan Kaminsky, have had weaknesses in their online security publicised in a 29,000 line text file posted by "Headenson John" on SecLists.org. The attacks, published on the eve of the Black Hat conference, highlight the fact that no-one is invulnerable.

More Information

Security elite pwned on Black Hat eve
ZF05 Released

McAfee Leaks Customer Details

<web-link for this article>

McAfee joins Baptist University as an organisation that accidentally attached an address list to the email they were sending. The security company's mistake occurred after a Strategic Security Summit held at the Sydney Convention Centre held on 17th July. They sent out a email thanking attendees, and attached a spreadsheet containing the names, numbers, e-mail addresses, employment details, and dietary requirements of over 1400 people. McAfee downplayed the incident, stating that it had interrupted the message before completion, sent a follow-up message instructing recipients to delete it, and put in place measures to prevent a repetition.

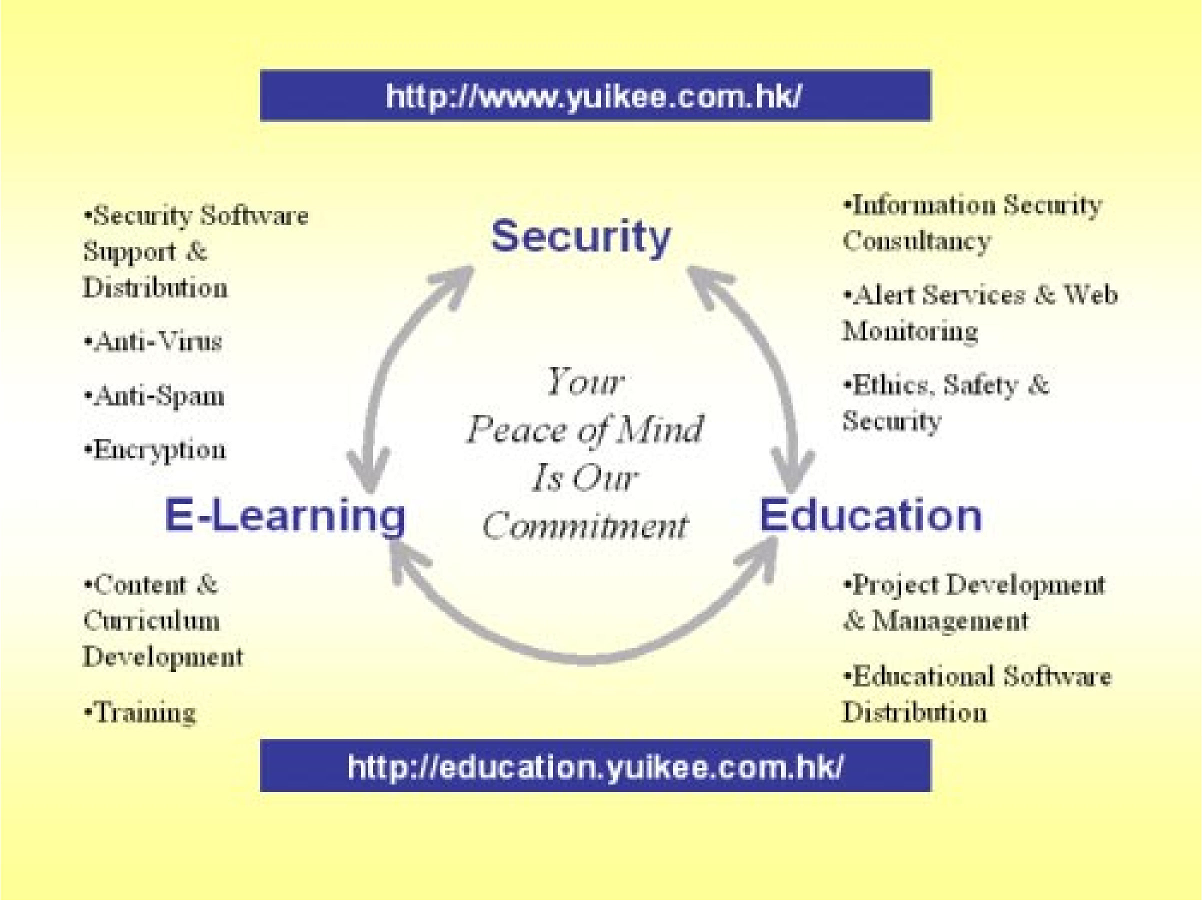
McAfee claims that its Total Protection for Internet Gateways product helps you protect against malware attacks and keep sensitive information secure, but they might not be using it themselves.

More Information

Security vendor McAfee spills 1,400 customer names
McAfee keeps leaked details to itself
McAfee sends out personal details in email
FW: McAfee Strategic Security Summit 09 — Inbox
Baptist University Applicant Data Leak
Data Leak Disease Spreads to Police?

YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/



http://www.yuikee.com.hk/

- Security Software Support & Distribution
- Anti-Virus
- Anti-Spam
- Encryption

Security

- Information Security Consultancy
- Alert Services & Web Monitoring
- Ethics, Safety & Security

Your Peace of Mind Is Our Commitment

E-Learning

- Content & Curriculum Development
- Training

Education

- Project Development & Management
- Educational Software Distribution

http://education.yuikee.com.hk/