


Securing your data

The recent slew of data leakages highlights the importance of data protection but fear not – accountants have a few tips to share, writes *John Ryan*



During a branch renovation, banking giant HSBC lost a server, and the customer transaction data that went with it. The Hong Kong police discovered complaints made against its officers on a public website, and the Immigration Department found some of its confidential files on the Internet. And then, the files of 10,000 patients from the Prince of Wales Hospital got lost when an employee left a USB in a taxi.

John Chiu, chief financial officer of the Hong Kong Institute of CPAs, thinks these cases are just the tip of the iceberg, not to mention phishing scams or identity theft. “There’s a lot more unreported (data loss) in my view.”

Hong Kong is becoming a place where worries about data security are moving from the information technology department to the offices of top management. “Every company should really look at the data they have – in hard copy or soft copy – to protect against instances of loss or misplacing, whether intentionally or accidentally,” Chiu says.

Even the wary can be trapped. At a secret meeting of computer security experts in March at Microsoft headquarters, experts laid out a potentially dangerous flaw in the Domain Name System. The system assigns web addresses to the numerical underpinnings (like postcodes) of the Internet. They look like a series of numbers, for example, 192.168.0.1, on your wireless router, which in turn gives

addresses to the computers and other equipment attached to it.

The DNS flaw, could, for example, allow criminals to redirect typed-in web addresses to their own sites, unbeknown to innocent users who could then unknowingly type in sensitive log-in and password data on a website they think belongs to their bank but instead is owned by thieves.

Using this flaw, hackers can trick almost any DNS server into associating malicious Internet Protocol addresses with legitimate domains. Security expert Dan Kaminsky, who discovered the flaw, estimates that 41 percent of DNS servers are still vulnerable, more than half a year after the Microsoft meeting.

“The control of DNS services lies with Internet service providers, so it’s basically their responsibility,” says Roy Ko, manager at the Hong Kong Computer Emergency Response Team Coordination Centre, which was set up in 2001 with government funding and operates under the Hong Kong Productivity Council.

Hong Kong ranks top in malicious websites survey

McAfee, a maker of anti-virus, security and encryption software, in June released its second “comprehensive map of malicious websites across the world” and it draws a disquieting picture. Hong Kong (.hk) earns the unenviable distinction of being the riskiest country domain (like .uk, .cn and so on), with 19.2 percent of all sites tested earning a red or yellow warning label, the first and second-highest risk categories, respectively.

Lest our mainland colleagues rest smug, .cn is the second-riskiest, with

“Hong Kong earns the unenviable distinction of being the riskiest country domain with 19.2 percent of all sites tested earning a red or yellow warning label, the first and second-highest risk categories.”

11.8 percent of sites labelled red or yellow. Russia, often regarded as a haven for cybercrime, compares well with Hong Kong with a risk rating of just 6 percent, not much worse than the 5.3 percent recorded by the common commercial .com top-level domain.

Using encryption can protect a laptop from accidental leakages, according to Chiu, who notes that securely encrypted data left in a taxi is more of a survivable embarrassment than a security danger.

Then, of course, there’s the situation when you’ve lost data and you don’t even know it – until you read about it in the newspaper.

“There have been many instances of leakage through popular file-sharing software called Foxy in the past few months,” says Ko.

Commonly used to share music and video files, Foxy can make all the data on a given computer available over the Internet to any other Foxy user if its installation parameters are configured – intentionally or unintentionally – to allow it.

The software is the culprit behind the leakage of a large number of sensitive government departmental documents, according to a recent report from the

University of Hong Kong’s Centre for Information Security and Cryptography.

Departments that have seen their supposedly safe documents posted on the Internet include the Civil Aviation Department, the Immigration Department, the Hong Kong Police Force and the Customs and Excise Department, the report says.

Ignorance and carelessness

Ko says there are two ways sensitive data leaks into the public sphere: ignorance and carelessness.

Ignorance, or not understanding crucial features of a technology that is new to you, “like in the case of Foxy and Google, where there can be hidden features you’re not aware of with the result that information is leaked accidentally,” he says.

“Second, we’re not sensitive enough about the information we handle and it gets published as a result,” he warns. “If you treat the data as sensitive, critical and important, you’ll handle it with good care: You won’t bring it home as you’ll consider it’s something not to take away from the office.”

What can you do to protect data? As in medicine, an ounce of prevention

+30



Photo: Thomas Jackson/Getty Images

is worth a pound of cure. Update all software all the time. Microsoft issues monthly updates, generally on a Tuesday and also rushes out patches off schedule when particularly severe threats surface. But it's not just operating systems and web browsers (like Internet Explorer, Firefox or Safari) – it's everything.

"In one recent attack, hackers used Adobe Flash Player to break into computers," Ko says. "This is another product that works as an add-on to your browser, and it's not part of the regular updates from Microsoft, so you have to keep track of updating it separately."

Watch out for malware

Apart from seeking out and installing updates regularly, backing up important data is your best insurance policy. And anti-malware software, like McAfee or Symantec products, is a must.

"The anti-malware can check files copied or transferred to your machine for malware, real-time. You can also use

tools to scan your computer on a regular basis," says Ko.

Malware is cropping up in mobile phones, particularly smart phones, such as the iPhone from Apple or Nokia's N-Series phones. All of these can surf the Internet over Wi-Fi or cellular networks, and all are vulnerable.

"With the increasing power of mobile phones and increasing similarity of mobile phones to computers, there's increasing risk," says Ko.

How accountants curb cyber threats

The accounting profession has been quick off the mark responding to cyber threats. Accounting firms have offered cyber security services for years since these services logically build on their expertise with financial reporting systems.

The American Institute of CPAs and the Canadian Institute of Chartered Accountants developed two services – SysTrust and WebTrust – in the late

1990s to allow auditors to issue opinions on technologies used in electronic commerce and IT systems.

Under a SysTrust examination, a CPA tests system controls during a specified period and delivers an attestation report for controls that operated effectively.

WebTrust is similar to SysTrust, but covers e-commerce. While SysTrust only delivers a report, WebTrust awards clients who pass its examination (an independent verification or audit is required) with a seal of assurance that they can then display on their websites.

However, there is no panacea. No single software audit, tool or patch can act as a one-size-fits-all security system in our increasingly networked world. There are many unknown unknowns.

"We have a lot to do. We don't know what's going to happen tomorrow," Ko warns. "It might be a quiet day, or we might have a major problem." **A+**