LEISURE SUMMER

Willis NEWSLETTER

2011 www.willis.com

DATA, DATA EVERYWHERE! 'PROTECTION IS A NECESSITY'

TOO MUCH INFORMATION?

- Wallmart the USA retail chain handles more than 1,000,000 customer transactions per hour feeding databases containing 2.5 petabytes of data
- Facebook has 40,000,000,000 photos stored on its website
- You Tube claim to receive 24 hours of video, every minute
- The International Data corporation predict that by the end 2011 mankind will generate 1,200 exabytes of data

Data Inflation

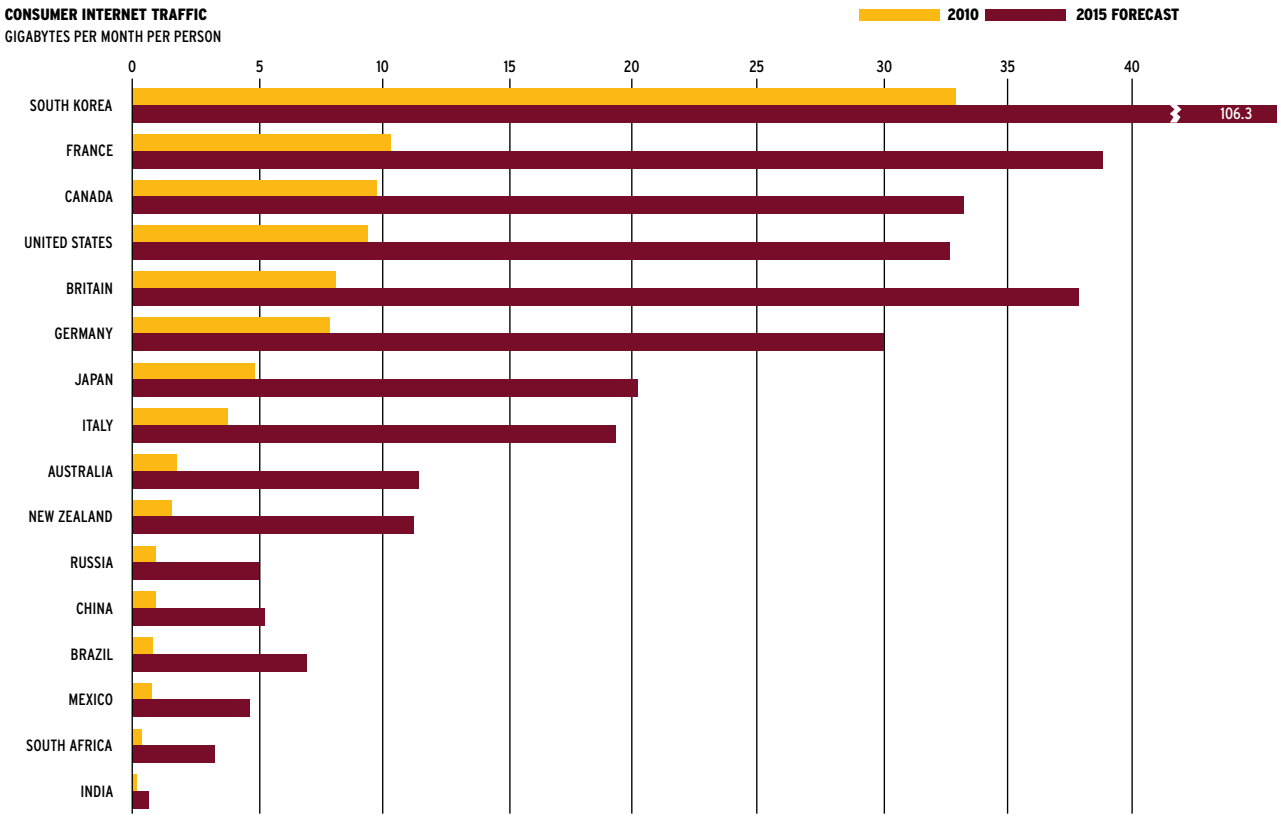
UNIT	SIZE	WHAT IT MEANS
Bit (b)	1 or 0	Short for 'binary digit', after the binary code (1 or 0) computers use to store and process data
Byte (B)	8 bits	Enough information to create an English letter or number in computer code. It is the basic unit of computing
Kilobyte (KB)	1,000 or 2^{10}, bytes	From 'thousand' in Greek. One page of typed text is 2KB
Megabyte (MB)	1,000KB; 2^{20} bytes	From 'large' in Greek. The complete works of Shakespeare total 5MB. A typical pop song is about 4MB
Gigabyte (GB)	1,000MB; 2^{30} bytes	From 'giant' in Greek. A two-hour film can be compressed into 1-2GB
Terabyte (TB)	1,000GB; 2^{40} bytes	From 'monster' in Greek. All the catalogued books in America's Library of Congress total 15TB
Petabyte (PB)	1,000TB; 2^{50} bytes	All letters delivered by America's postal service this year will amount to around 5PB. Google processes around 1PB every hour
Exabyte (EB)	1,000PB; 2^{60} bytes	Equivalent to 10 billion copies of **The Economist**
Zettabyte (ZB)	1,000EB; 2^{70} bytes	The total amount of information in existence this year is forecast to be around 1.2ZB
Yottabyte (YB)	1,000ZB; 2^{80} bytes	Currently too big to imagine

The prefixes are set by an intergovernmental group, the International Bureau of Weights and Measures. Yotta and Zetta were added in 1991; terms for larger amounts have yet to be established.

Source: **The Economist**

Data production is growing at an exponential rate (currently compound annual 60%)[1]. This data expansion does not just apply to the generation 'net' demographical group and their social media postings. A recent press release from IHG announced that during the past 28 years they had signed up 56,000,000 loyalty card members[2]. McKinsey Global Institute in their May 2011 publication on Big Data consider companies who can harness big data will out-perform companies who are data- incompetent. McKinsey suggest that the accommodation and food sector can derive significant value from big data. (Big data is defined as datasets whose size is beyond the ability of typical database tools to capture, store, manage and analyse.)

[1] Economist February 25, 2011
[2] IHG

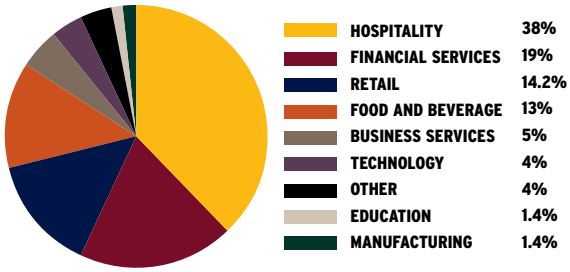


Sources: Cisco; UN; **The Economist**

Consumers will increasingly generate more data as shown by this Cisco survey of growing internet usage. Globalization and the commoditization of information technology have driven businesses to also collect and store increasing amounts of data. These data are attractive to cyber criminals and hackers. In 2010 the Assistant for the Federal Bureau of Investigation testified (before the House Judiciary subcommittee on Crime, Terrorism and Homeland Security) that **'The impact of cyber crime on individuals and commerce can be substantial with the consequences ranging from a mere inconvenience to financial ruin'**[3].

DATA LOSS

The Ponemon Institute lists three root causes of data breach. These are categorised as: third party mistakes; malicious attacks or a negligent insider or a systems glitch. In 2010, businesses suffered 29% of all malicious attacks recorded.



Source: Trustwave Spider Labs

Hackers steal data from the hospitality industry more than any other industry. From the 218 data-breach investigations in 24 countries a majority 38% applies to hospitality. The Ernst & Young 2010 Global Information Security Survey indicates that 81% of the executives interviewed considered managing privacy and protecting personal data as very important. Immediately following their recent attack, a major electronic components manufacturer brought in outside experts to assess the situation. They advised that the five day delay in announcing the data loss was attributable to extensive forensic analysis by outside experts. This was required to determine the scope of the malicious attack that had occurred[4].

Research performed by the Ponemon Institute in 2010 confirmed that recovery from a cyber attack can require between one week and one month, with financial costs ranging between US$100,000 to US$1,000,000. The more common successful spear phishing attack generally takes between two days to one week and incurs costs between US$100,000 to US$1,000,000 for the business victim.

WHO IS NOW THE TARGET?

A major electronic components manufacturer had encrypted all credit card numbers making it difficult for hackers to access the datum. However, personal information not encrypted is useful to hackers. Using stolen e-mail addresses to send carefully crafted e-mails allows the hacker to trick the target victim into clicking on an attachment. A spear 'phishing 'attack allows the hacker to download malicious software into the victim's computer. This targets passwords, account numbers, user IDs, access codes, PIN numbers or other pertinent information allowing the hacker to access the victim's financial resources[5].

[3] McAfee/SAIC
[4] Insurance Day June 7, 2011
[5] FBI

SOLUTIONS

Recent malicious attacks affecting brand name organisations indicate that the hackers specifically targeted personal data[6]. Criminals use personal data to launch spear 'phishing' attacks on those individuals[7]. Threats exist not only from external sources, there is the insider threat. Ernst & Young report that individuals who are authorised to access and use information are increasingly found at the centre of high-profile incidents[8]. Ernst & Young identifies 11 trends in privacy protection for 2011; regulation; breach notification; governance; cloud computing; mobile devices; increased investment; privacy assessments; service provider standards; privacy by design; social networking and evolving privacy professional expectations.

Protection against loss of data operates in two sectors; risk management and/or risk transfer.

RISK MANAGEMENT

Specific actions that can be implemented to improve your current cyber security and protection are:[9]

- Elevate cybersecurity issues to the Chief Executive
- Conduct regular security audits
- Assume that if you have not been hacked you will be
- Identify your most critical digital assets and isolate them
- Acknowledge the death of the perimeter defence (employees now bring in portable miniature drives that connect to your networked machines)
- Use active gateway protection to block access to insecure websites
- Deploy software that can check websites for bad code
- Exercise caution with mobile and remote access
- Train your workforce in cyber security (including senior management)
- Patch your systems immediately the software manufacturer releases this
- Minimise the amount of power that employee machines have and the data they retain

RISK TRANSFER

Although cyber liability insurance has been in existence during the last 10 years, there has now been recognition by insurers that this risk transfer needs to reflect current environment[10].

This now means complying with regulatory as well as individual operational requirements. The 2011 privacy protection trends show how data protection needs constant evolution to stay relevant. The risk transfer insurance market provides insurance specifically to meet these growing needs of business.

For more information contact:
Laurie Fraser
Global Markets Leisure Practice Leader
Email: fraserl@willis.com

Pedro Sarrion
Leisure Practice International
Email: pedro.sarrion@willis.com

[6] FT Cybersecurity June 2, 2011
[7] Reuters, April 29, 2011
[8] Insights in IT, January, 2011
[9] FT Cybersecurity June 2, 2011
[10] Insurance Day June 7, 2011

9771/07/11