Social Networking and Security Risks

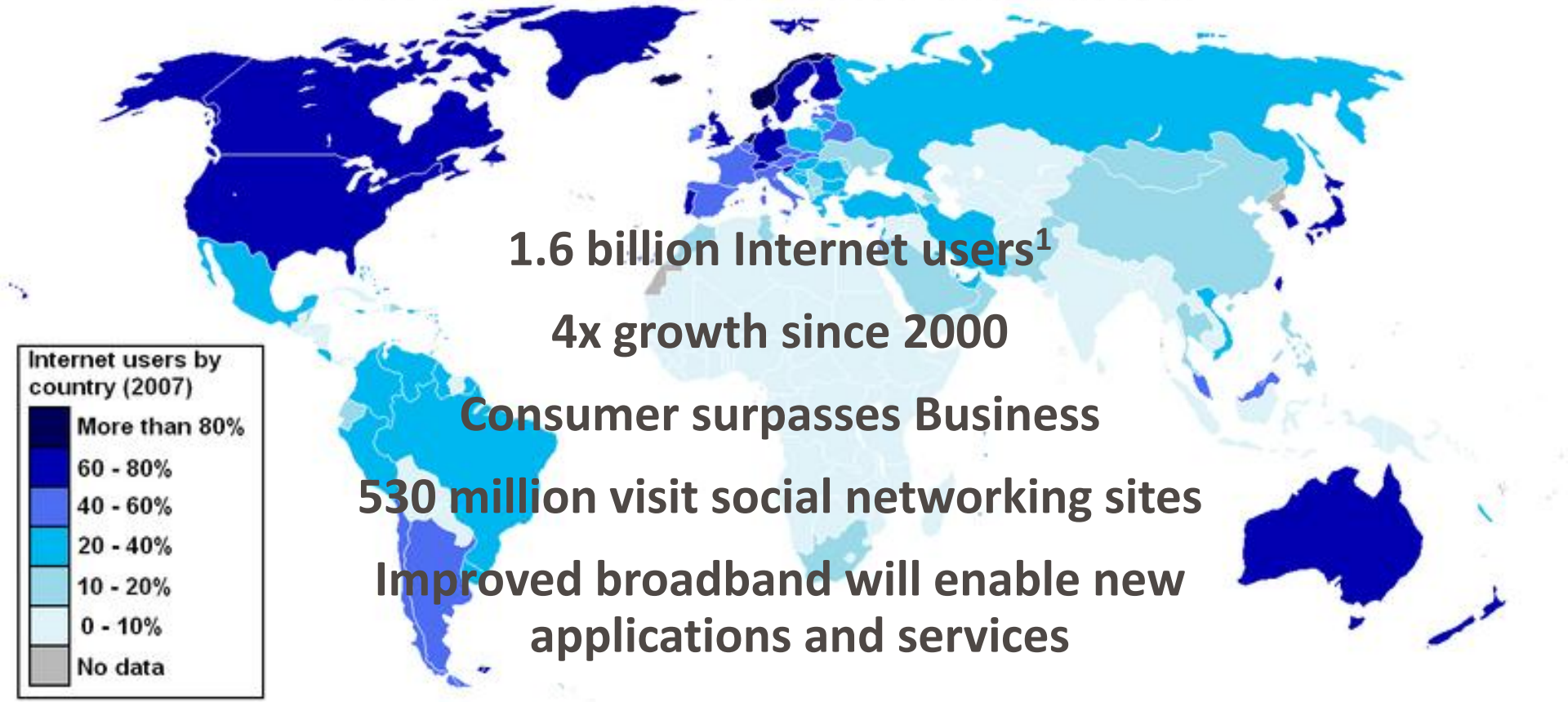
Victor Law

Regional Director, VeriSign User Authentication Services

Asia Pacific

The Online World

Billions of critical Internet interactions occur every day that must be authenticated and trusted.



1.6 billion Internet users[1]

4x growth since 2000

Consumer surpasses Business

530 million visit social networking sites

Improved broadband will enable new applications and services

1: Source world Bank: World Development Indicators 2008

What Are Consumers Feeling?

- Consumers are increasingly IT savvy & security aware
- Over 80% of online shoppers want more assurance that their information is secure[1]

	China	Global
Do NOT expect to be a victim of cybercrime	3%	3%
Victims most likely to ...	1. Change online behaviour (34%) 2. Call their bank (48%)	1. Change online behaviour (51%) 2. Call their bank (48%)
Think cybercriminals will NOT be brought to justice	80%	79%
Average # of days to resolve a cybercrime	23 days and cost US $944.7	28 days and cost US $334

1: Source Javelin strategy March 2009; Table: Source: Symantec CyberCrime The Human Impact Report 2010

Identity Theft And Identity Trading

- Usernames & passwords are easy to steal.
- Extensive use of phishing.
- Increasingly sophisticated malware, web-monitoring and keystroke logging.
  - Zeus trojan targets nearly every form factor even SMS
- There is a rampant trade in stolen identities.
  - Bank identities are breeders of other identities
  - Bank identities are highly valued in the Black Market fetching up to USD $400[1]

Rank	Item	Percentage	Range of prices
1	Credit cards	22%	$0.50-$5
2	Bank accounts	21%	$30-$400
3	Email passwords	8%	$1-$350
4	Mailers	8%	$8-$10
5	Email addresses	6%	$2/MB-$4/MB
6	Proxies	6%	$0.50-$3
7	Full identity	6%	$10-$150
8	Scams	6%	$10/week
9	Social Security numbers	3%	$5-$7
10	Compromised Unix shells	2%	$2-$10

1: Source: Forrester 2008

Identity Theft

- Impersonate at a third party
- Mortgage fraud
- Faked credit cards
- Fake bank accounts
- Account takeovers
- Rampant data-mining and phishing

Social Engineering & Malware Are The Most Common Tools
Worth More Than The Illicit Drug Trade

Social Networking

- Facebook has 500 million accounts.
- Myspace has 100 million accounts.
- Little understanding of ToS or EULA
- Poor understanding of Privacy
- Permanence and persistence of data
- Photos, Comments, Posts

Social Networking Is Unregulated
Social Networking Is A Great Medium For Criminals

Cyberbullying

- Regular bullying does not require an audience
- Cyberbullying generally requires no audience
- Cyberbullying is hard to detect and police
- Legal ground is shaky
- Exclusion of bullies is mostly useless
- Social networks and SMS are the preferred tools

Old Problems, New Mechanism
Rapid And Pervasive Abuse

What Is Social Engineering?

"To manipulate people by deception, into giving out information or performing an action"

Iann Mann

- Two main outcomes
  - Direct loss of information
  - Achievement of some action desired by the attacker
- Attacks can be very simple or very complex
  - Simple questioning over phone
  - Elaborate plans with web sites, phone, email, counterfeit documentation

Common Personality Traits Exploited

- **Diffusion Of Responsibility**
  - The target is made to believe that they are not solely responsible for their actions.
- **Chance For Ingratiation**
  - The target is lead to believe that compliance with the request will enhance their chances of receiving benefit
- **Trust Relationships**
  - The social engineer expends time developing a trust relationship with the intended victim
- **Moral Duty**
  - Encouraging the target to act out of a sense of moral duty or moral outrage.
- **Guilt**
  - Most individuals attempt to avoid the guilt feelings if possible
- **Desire To Help**
  - Social engineers rely on people's desire to be helpful

Common Electronic Types of Social Engineering

- Mail attachments (Trojan & Virus)
  - Programs can and are frequently hidden in email attachments
  - Viruses, Worms, Trojans
- Websites (Drive By & Interactive)
  - A common ploy is to offer something
  - Free chance to win a trip on a website. To register requires an email address and password
  - Free movie tickets, dinner vouchers etc.
  - Free stuff is a very powerful incentive
  - Fake surveys

Phishing

- **What is phishing?**
  - Phishing is the criminally fraudulent process of attempting to acquire sensitive information by masquerading as a trustworthy entity in an electronic communication.
  - Early sites easy to pick, now very hard to pick near-replicas
- **Why does phishing work?**
  - People tend to trust messages that appear to come from an important entity or look important.
  - The attacker can easily manipulate a URL to look very close, fooling the victim to click on it.
  - http://www.company.com looks almost identical to http://www.cornpany.com
  - It is surprisingly successful.

Spear Phishing

- Spear phishing is a highly targeted form of phishing
- Small target size rather than broad based
- Emails sent with information that targets are familiar with
- Emails may appear to come from users or organisations that the targets regularly deal with
- Emails may contain specific, relevant and current information about projects or other tasks that targets are working on
- Attacker has a very specific goal
- These are very, very deceptive

How to Mitigate the Risks?

- Use of corporate or personal IPS, IDS and web & spam filter as first layer of defense
- Make sure your endpoint protection software is up-to-date
- Use of strong password, and preferably make use of the multi-factor authentication if available
- Visit websites that are trusted, by means of inspecting a web seal or SSL certificate
- Do not give out excessive personal information in public forums or social networking sites
- Invite/ accept invitation from people whom you really know

Summary

- Cybercrime is big business, worth more than illicit drugs
- Cybercrime is run by professionals
- IT practitioners need to understand new threats and technologies
- General public needs to be better educated on the threats and privacy
- Technology can mitigate threats but user awareness is the best and last line of defence
- Identity theft and account hijacking are currently the most common threats
- Cyberbullying is hard to police with few laws surrounding it

WHITE PAPER: SYMANTEC REPORT ON ATTACK KITS AND MALICIOUS WEBSITES

Symantec Report on Attack Kits and Malicious Websites

Confidence in a connected world. Symantec.

SYMANTEC ENTERPRISE SECURITY

symantec.

Confidence in a connected world.

Symantec Internet Security Threat Report

April 2010

Regional Data Sheet—Asia-Pacific/Japan

An important note about these statistics

The statistics discussed in this document are based on attacks against an extensive sample of Symantec customers. The attack activity was detected by the Symantec™ Global Intelligence Network, which includes Symantec Managed Security Services and Symantec DeepSight™ Threat Management System, both of which use automated systems to map the IP address of the attacking system to identify where it is located. However, because attackers frequently use compromised systems situated around the world to launch attacks remotely, the location of the attacking system may differ from the location of the attacker.

Introduction

Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec Global Intelligence Network. More than 240,000 sensors in over 200 countries and territories monitor attack activity through a combination of Symantec products and services such as Symantec DeepSight Threat Management System, Symantec Managed Security Services and Norton™ consumer products, as well as additional third-party data sources.

Symantec also gathers malicious code intelligence from more than 133 million client, server, and gateway systems that have deployed its antivirus products. Additionally, Symantec's distributed honeypot network collects data from around the globe, capturing previously unseen threats and attacks and providing valuable insight into attacker methods.

Spam and phishing data is captured through a variety of sources including: the Symantec Probe Network, a system of more than 5 million decoy accounts; MessageLabs Intelligence, a respected source of data and analysis for messaging security issues, trends and statistics; and other Symantec technologies. Data is collected in more than 86 countries. Over 8 billion email messages, as well as over 1 billion Web requests, are processed per day across 16 data centers. Symantec also gathers phishing information through an extensive antifraud community of enterprises, security vendors and more than 50 million consumers.

These resources give Symantec's analysts unparalleled sources of data with which to identify, analyze, and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. The result is the Symantec *Internet Security Threat Report*, which gives enterprises and consumers the essential information to effectively secure their systems now and into the future.

In addition to gathering Internet-wide attack data for the Symantec *Global Internet Security Threat Report*, Symantec also gathers and analyzes attack data that is detected by sensors deployed in specific regions. This regional data sheet will discuss notable aspects of malicious activity Symantec has observed in the Asia-Pacific/Japan (APJ) region for 2009. This is designed to provide a balanced view of the trends in the threat activity landscape that Symantec has observed in the APJ region in comparison to global activity.

Thank you!

Victor Law

Victor_Law@Symantec.com

+852 9471 6062