



# Digital War in e-Business

Ricci leong,  
Secretary of ISFS,  
Senior Security Consultant,  
PrivyLink (HK) Ltd.

PrivyLink (Hong Kong) Ltd.

The background of the slide is a collage of three images: on the left, a low-angle shot of modern skyscrapers against a blue sky with clouds; in the center, the PRIVYLINK logo; and on the right, a close-up of a heavy-duty metal padlock.

# Trend in Internet Commerce Market

- More Internet Commerce Market
  - ❑ Increase in Business to Commerce Services
  - ❑ Increase in Business to Business Services
  - ❑ Increase in e-CRM, e-SCM, ERP
  - ❑ Increase in e-Banking
- More Financial transactions on Internet



# Growth in Security Investment

- No of companies spending more than US\$1 million a year has doubled from 1999 to 2000;
- Increment in Security Budget;
- Increase revenue for Security vendors;
- More jobs in computer security market.

The background of the slide features three distinct images: on the left, a low-angle shot of modern skyscrapers against a blue sky with clouds; in the center, the PRIVYLINK logo; and on the right, a close-up of a heavy-duty metal padlock with a keyhole, set against a textured, brownish background.

# Most popular security products

- Prevention Tools
  - ❑ Firewall
  - ❑ VPN
  - ❑ Intrusion Detection Systems
  - ❑ Virus Scanner
  - ❑ Biometrics tools
- Infrastructure
  - ❑ PKI
  - ❑ Smart card
- Services
  - ❑ Security Consultancy

The background of the slide features three distinct images: on the left, a low-angle shot of modern skyscrapers against a blue sky with light clouds; in the center, the PrivyLink logo; and on the right, a close-up of a heavy-duty metal padlock, partially open, set against a textured, brownish background.

## Results: More Hacking

- More than half of the Small and Medium-sized enterprises (SMEs) will be hacked from now to 2003
- More than 80% of companies in Asian region will be attacked from now to 2003.
- According to Gartner Group report





# Hacking Events

- Around 10 - 20 web sites have been defaced daily
- Computer Fraud reported in HK increased from 38 (1999) - 207 (2000)
- More online banks were hacked
  - UK bank Barclays
  - Powergen
  - Bank One Online
- HSBC (UK) web site have been defaced
  - (<http://www.attrition.org/mirror/attrition/2000/09/19/www.banking.hsbc.co.uk/mirror.html>)
- Microsoft was being hacked (not once but twice)



2000年11月8日 星期三

要聞 港聞 社評 論壇 中國 國際 經濟 體育 影視 馬經 副刊 英文

明報新聞網



第二屆 enabler 21 精英培育計劃  
邀請全港七間大學學生參加



---- 中國 ----

友善列印

返回主頁

返回目錄

### 今日相關新聞

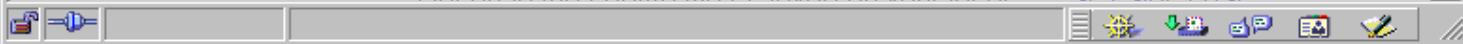
- 黑客擊潰湖北銀行電腦
- 黑客技術一流

### 其他新聞

## 黑客擊潰湖北銀行電腦

### 竊取資料潛逃 上海落網

【明報專訊】湖北省公安廳日前在上海警方的配合下，偵破八月三日中國銀行湖北利川市支行電腦信息系統資源遭黑客破壞而完全癱瘓的案件，上海警



The background of the slide is a collage of three images: on the left, a low-angle shot of modern skyscrapers against a blue sky with clouds; in the center, the PrivyLink logo; and on the right, a close-up of a rusty metal padlock with the word "YALE" embossed on it.

# Why more hacking?

- More targets
- More hackers especially teenage hackers
- More hacking news reported
- Increase in Internet Market
- No enough investment in security
- Improper implementations of security products. Spending more for computer security alone won't protect the network from hackers and cybersaboteurs.





http://www.mingpaonews.com/20001108/\_cca2.htm - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print

Address http://www.mingpaonews.com/20001108/\_cca2.htm

2000年11月8日 星期三 要聞 港聞 社評 論壇 中國 國際 經濟 體育 影視 馬經 副刊 英文

明報新聞網 enabler 21 目標所向 光芒所在

中國

今日相關新聞

- 黑客擊潰湖北銀行電腦
- 黑客技術一流

其他新聞

- 八十萬台幣變白紙

## 黑客技術一流

### 保護措施九流

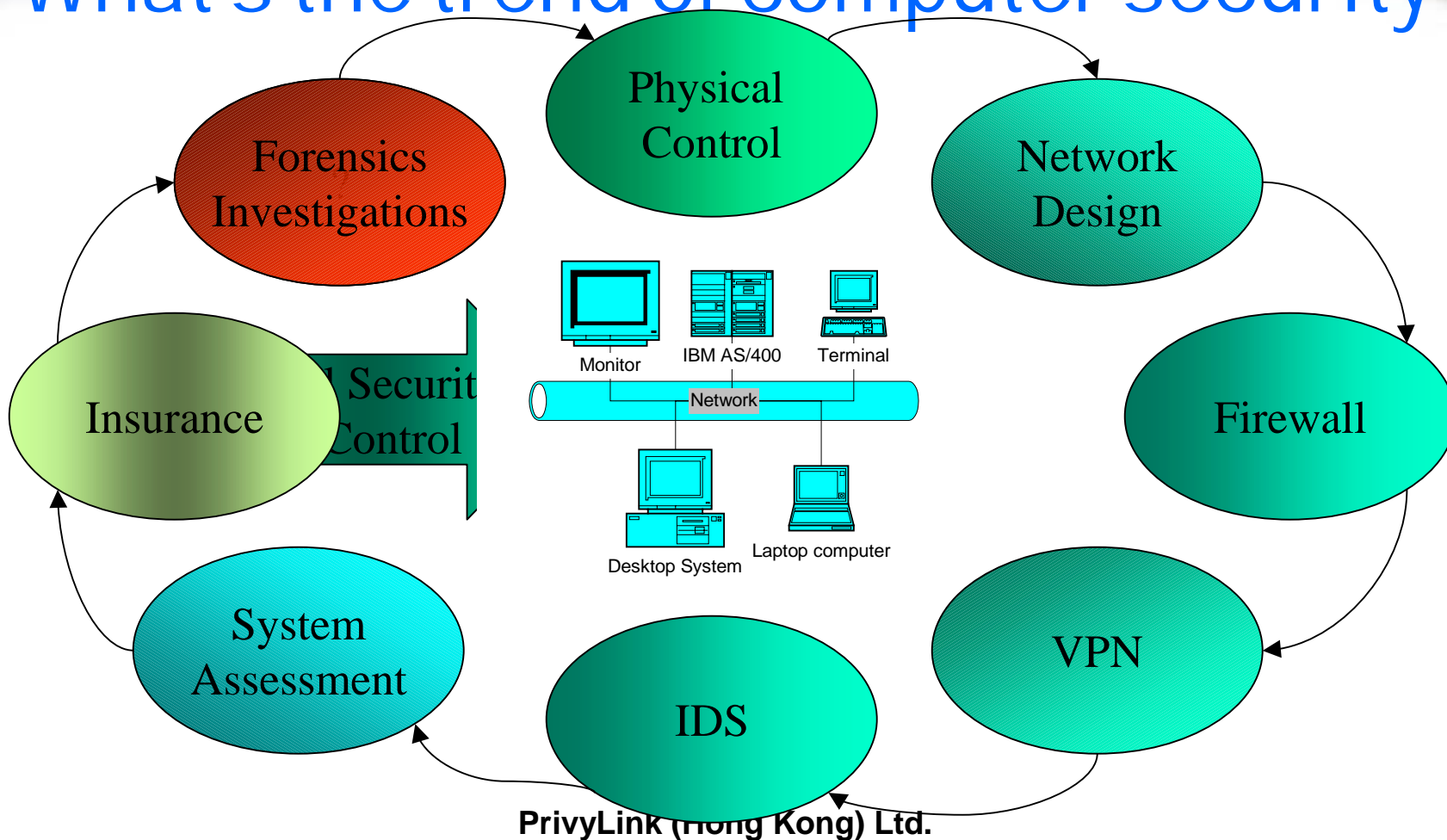
**【明報專訊】**據內地電腦專家表示，內地的網絡設備如擔負內外橋樑和防火牆工作的路由器八成以上來自國外，加上內地以往安全防範意識差，致使絕大多數網站和電子信息系統的安全至保護措施存在大量漏洞，有的系統甚至不堪一擊。

此外，中國的黑客攻擊技術在世界上屬第一流水準，因此，據有關方面統計，包括多個省市政府網站在內的內地六成以上的網站和上網電腦曾被入侵。

Internet



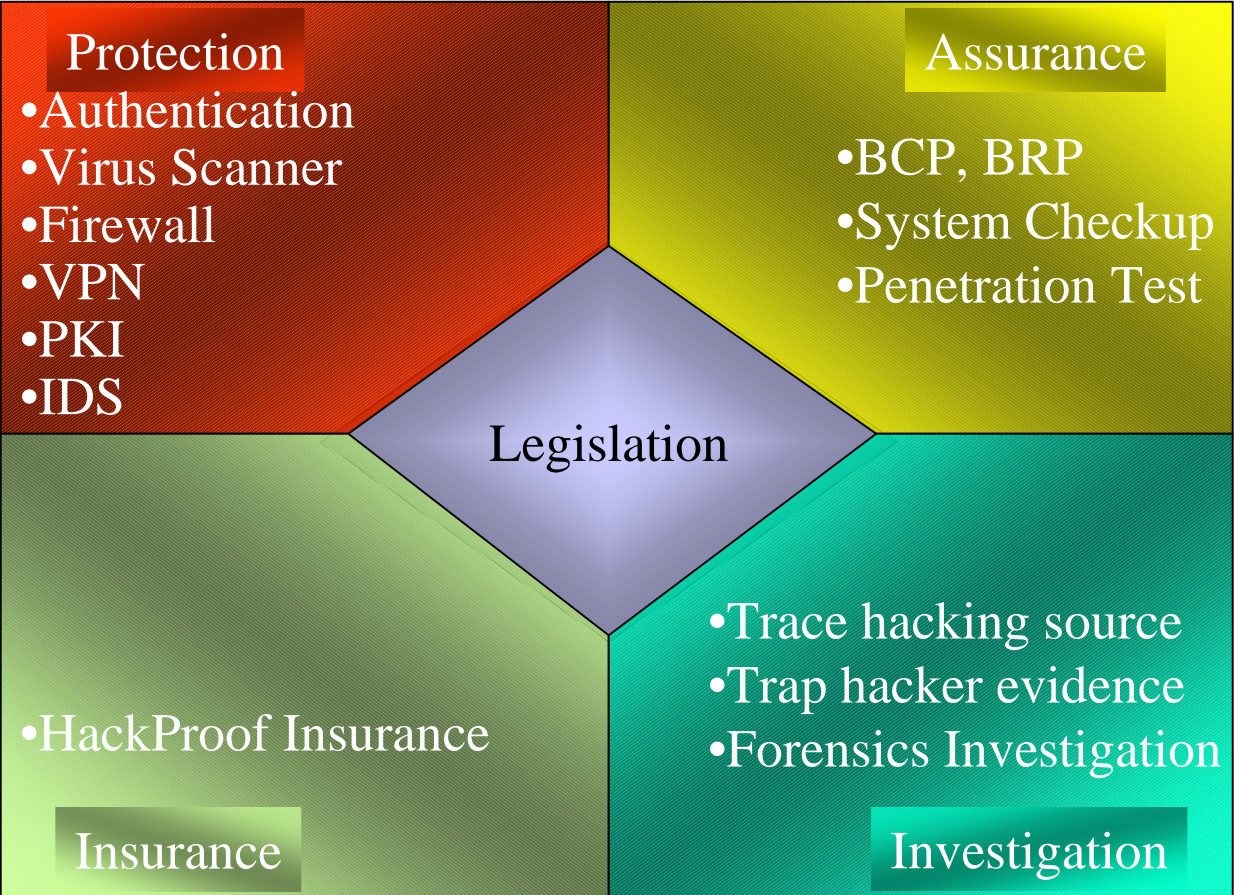
# What's the trend of computer security







# Future picture in security?





# Solution to security problems

- Firewall Configurations
- Boundary Services
- Consolidate and centralized remote access
- Installation of Intrusion Detection Systems
- Assurance Test
- Installation of evidence preserving tools

The background of the slide is a collage of three images: on the left, a low-angle shot of modern skyscrapers against a blue sky with clouds; in the center, the PrivyLink logo; and on the right, a close-up of a heavy-duty metal padlock with a keyhole, set against a textured, brownish background.

# Risk Assessment Strategies

- Systems inventory and definition
- Vulnerability and threat assessment
- Evaluation controls
- Decision
- Communication and monitoring



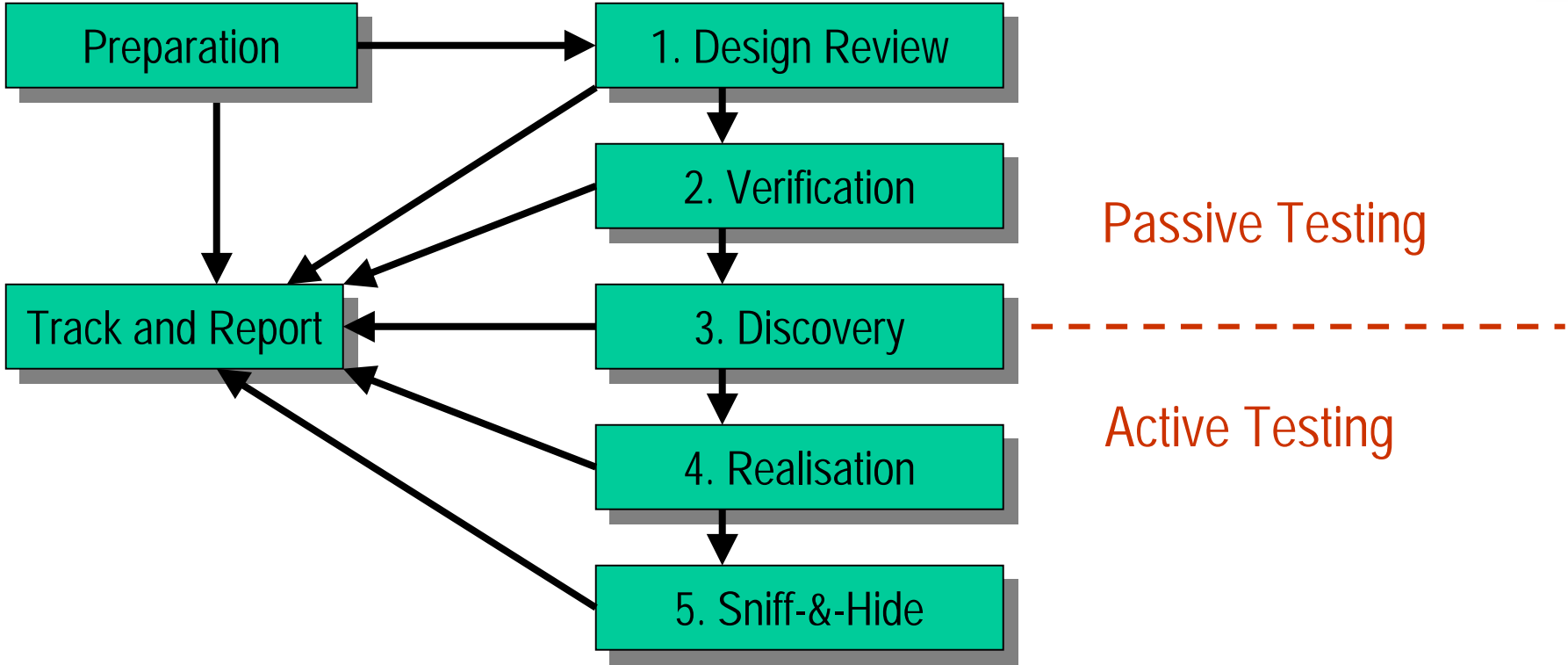
The background of the slide features three distinct images: on the left, a low-angle shot of modern skyscrapers against a blue sky with white clouds; in the center, the PRIVYLINK logo; and on the right, a close-up of a heavy-duty metal padlock with a keyhole, set against a textured, brownish background.

# Assurance Test

- System Checkup
  - ❑ Firewall configuration check
  - ❑ OS System Check
  - ❑ Network Configuration Check
- Penetration Test
  - ❑ Internal Pen Test
  - ❑ External Pen Test



# White-Box Approach



The background of the slide is a collage of three images: a modern glass skyscraper on the left, the PrivyLink logo in the center, and a close-up of a rusty metal padlock on the right.

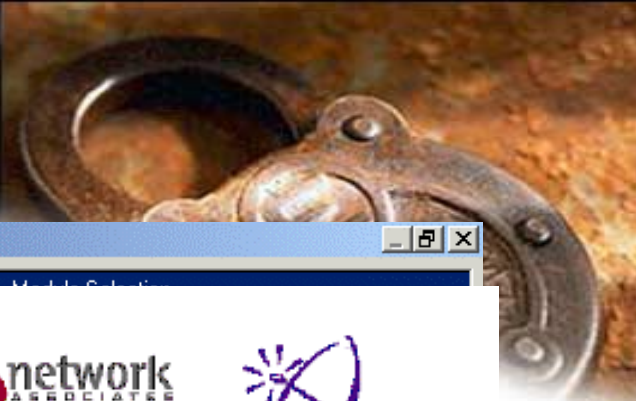
# System Checkup

- Evaluate the each machine on:
  - ❑ System Configurations
  - ❑ Password file protections
  - ❑ Firewall, Router Setting
  - ❑ Ethernet Switch Setting
  - ❑ Database Setting

The background of the slide is a collage of three images: on the left, a low-angle shot of modern skyscrapers against a blue sky with clouds; in the center, the PRIVYLINK logo; on the right, a close-up of a heavy-duty metal padlock with a keyhole, set against a textured, brownish background.

# Penetration Test

- Penetration Test
  - Internal
    - Attack from internal network
    - Attack at machine console
  - External
    - Determine OS type
    - Confirm Patches Version
    - Determine possible vulnerabilities
    - Perform system attack



Module Configuration Dialog

# CyberCop Scanner Results

Report Sorted By Host



 192.168.1.10 4 Vulnerabilities  
192.168.1.10  
OS Type: *unknown*

Scan Performed on 05-Oct-2000 6:51:39PM

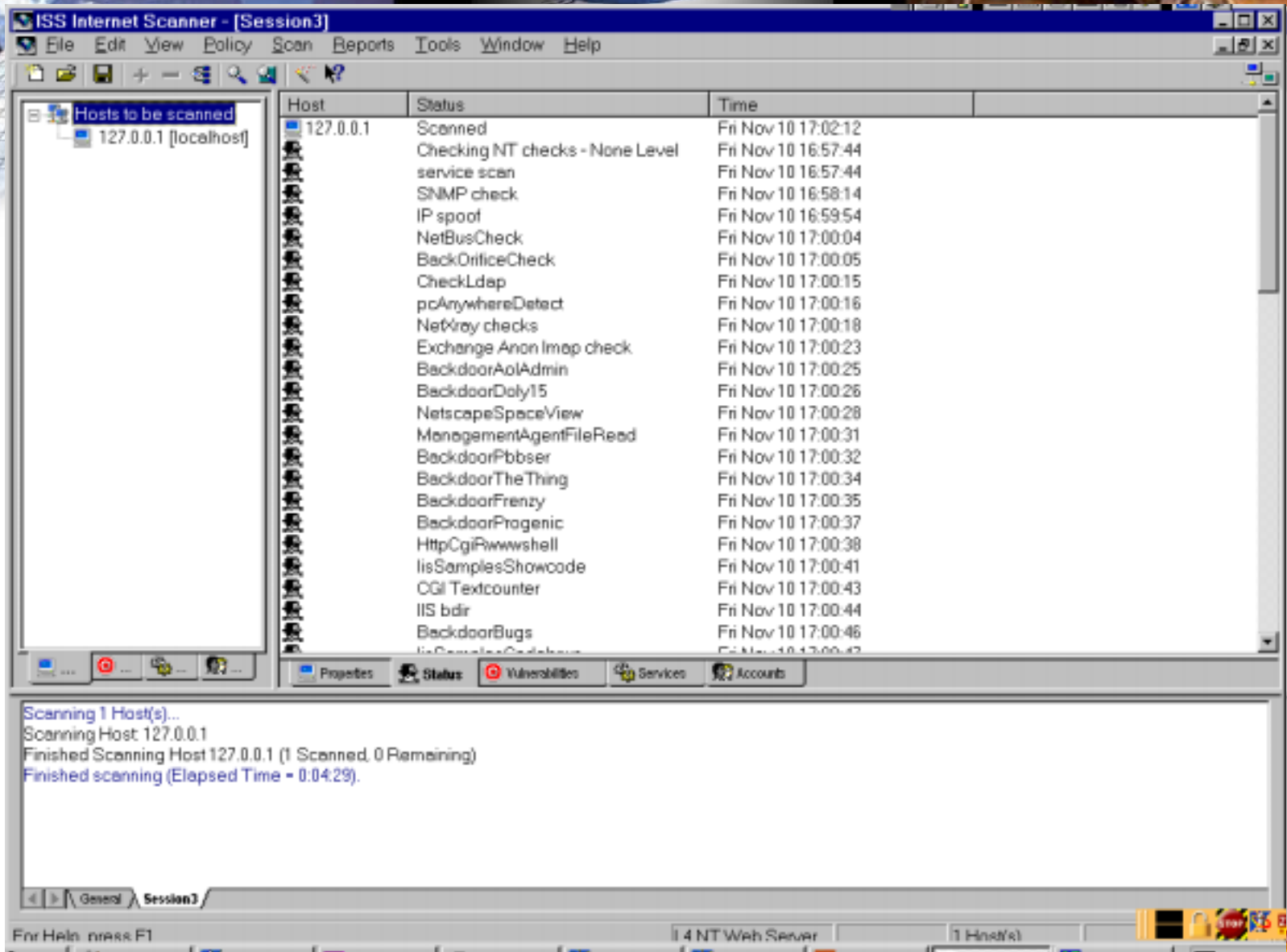
Vulnerability Group 1000 **Information Gathering and Recon**

1032 *ICMP timestamp obtained* 05-Oct-2000 6:51:39PM 

- Risk Factor:** Low
- Complexity:** Medium
- Popularity:** Obscure
- Impact:** Intelligence
- Root Cause:** Insecure Design

Some versions of wu-ftp contained a backdoor. When the string 'NULL' was used as a username the intruder gained root access to the ftp server.





The screenshot shows the ISS Internet Scanner application window. The title bar reads "ISS Internet Scanner - [Session3]". The menu bar includes File, Edit, View, Policy, Scan, Reports, Tools, Window, and Help. The main window is divided into a left sidebar and a main table area. The sidebar shows a tree view with "Hosts to be scanned" and "127.0.0.1 [localhost]". The main table displays scan results for 127.0.0.1, listing various checks and their completion times. At the bottom, a status bar shows "Scanning 1 Host(s)... Scanning Host: 127.0.0.1 Finished Scanning Host 127.0.0.1 (1 Scanned, 0 Remaining) Finished scanning (Elapsed Time - 0:04:29)".

Host	Status	Time
127.0.0.1	Scanned	Fri Nov 10 17:02:12
	Checking NT checks - None Level	Fri Nov 10 16:57:44
	service scan	Fri Nov 10 16:57:44
	SNMP check	Fri Nov 10 16:58:14
	IP spoof	Fri Nov 10 16:59:54
	NetBusCheck	Fri Nov 10 17:00:04
	BackOfficeCheck	Fri Nov 10 17:00:05
	CheckLdap	Fri Nov 10 17:00:15
	pcAnywhereDetect	Fri Nov 10 17:00:16
	NetVray checks	Fri Nov 10 17:00:18
	Exchange Anon Imap check	Fri Nov 10 17:00:23
	BackdoorAolAdmin	Fri Nov 10 17:00:25
	BackdoorDoly15	Fri Nov 10 17:00:26
	NetscapeSpaceView	Fri Nov 10 17:00:28
	ManagementAgentFileRead	Fri Nov 10 17:00:31
	BackdoorPbbser	Fri Nov 10 17:00:32
	BackdoorThe Thing	Fri Nov 10 17:00:34
	BackdoorFrenzy	Fri Nov 10 17:00:35
	BackdoorProgenic	Fri Nov 10 17:00:37
	HttpCgiPwwwshell	Fri Nov 10 17:00:38
	IisSamplesShowcode	Fri Nov 10 17:00:41
	CGI Textcounter	Fri Nov 10 17:00:43
	IIS bdir	Fri Nov 10 17:00:44
	BackdoorBugs	Fri Nov 10 17:00:46
	IisSamplesCodebase	Fri Nov 10 17:00:47



**Report Preview** | 1 of 1+ | 90% | Total:230 100% 230 of 230

---

## Network Vulnerability Assessment Summary

Date: June 23, 1998

**Report Description:**  
 This report summarizes the organization's susceptibility to attack in relation to its policy and vulnerability conditions. Specifically, the summary graphics describe percent of vulnerabilities by severity and number of vulnerabilities by severity. Vulnerabilities are classified as high, medium or low. High risk vulnerabilities are those which provide unauthorized access to the host, and possibly, the network. Medium risk vulnerabilities are those that provide access to sensitive network data that may lead to the exploitation of higher risk vulnerabilities. Low risk vulnerabilities are those which provide access to sensitive, yet non-lethal, network data. It is recommended that all high risk vulnerabilities be corrected as soon as possible.

<b>Session Name:</b> Session1	<b>Session ID:</b> 4
<b>Template:</b> Heavy Scan	<b>Termination Status:</b> Finished
<b>File Name:</b> Session1_980623	

**Scan Summary Information**

<b>Hosts Scanned:</b> 1	<b>Scan Start:</b> 1998/06/23 16:49:06
<b>Hosts Active:</b> 1	<b>Scan End:</b> 1998/06/23 16:55:04
<b>Hosts InActive:</b> 0	<b>Elapsed:</b> 00:05:38

**Number of Vulnerabilities by Severity**

Severity	Count
High	4
Medium	12
Low	45

**Percent of Vulnerabilities by Severity**

Severity	Percentage
High	6.6%
Medium	19.7%
Low	73.8%
<b>Total</b>	<b>100.0%</b>

**Report Preview** | 1 of 1+ | 100% | Total:61 100% 61 of 61

---

## Network Vulnerability Assessment Report

Sorted by Vulnerability Severity and Name

June 23, 1998

**Report Description:**  
 This report displays the organization's susceptibility to attack in relation to its policy and vulnerability conditions. Specifically, this report identifies network vulnerabilities and suggested corrective action. Vulnerabilities are classified as high, medium and low. High risk vulnerabilities are those which provide authorized access to the host, and possibly, the network. Medium risk vulnerabilities are those that provide access to sensitive network data that may lead to the exploitation of higher risk vulnerabilities. Low risk vulnerabilities are those which provide access to sensitive, yet non-lethal, network data. It is recommended that all high risk vulnerabilities be corrected as soon as possible.

<b>Session Name:</b> Session1	<b>Session ID:</b> 4
<b>Template:</b> Heavy Scan	<b>Termination Status:</b> Finished
<b>File Name:</b> Session1_980623	

**Scan Summary Information**

<b>Hosts Scanned:</b> 1	<b>Scan Start:</b> 1998/06/23 16:49:06
<b>Hosts Active:</b> 1	<b>Scan End:</b> 1998/06/23 16:55:04
<b>Hosts InActive:</b> 0	<b>Elapsed:</b> 00:05:38

---

Vulnerability Name:	Severity:		
<b>Getadmin Patch not applied</b>	<b>High</b>		
<b>Description:</b>			
An unpatched version of Windows NT has been found. It is possible for a local user to obtain administrator privileges by running getadmin. See Microsoft Knowledge base article Q146965 for details.			
<b>Fix:</b>			
Apply the post-SP3 getadmin patch, or SP4 when available. For the patch and the Knowledge Base article, see <a href="ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/ntfixes-postSP3/getadmin-fix/">ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/ntfixes-postSP3/getadmin-fix/</a> .			
<b>IP Address</b>	<b>DNS Name</b>	<b>Additional Info</b>	<b>Session ID</b>
127.0.0.1	localhost		4
<b>Vulnerability Name:</b>		<b>Severity:</b>	
<b>Modified teardrop attack blue screens Windows systems.</b>		<b>High</b>	
<b>Description:</b>			
This issue is a modified version of an attack that appeared on the Internet a few months ago called "teardrop." This new issue is caused by a problem with the way the Microsoft TCP/IP stack handles certain exceptions caused by malformed UDP header information. This situation does not occur in properly formed TCP/IP packets and must be generated by a program with malicious intent.			
<b>Fix:</b>			
Obtain patch: <a href="ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/ntfixes-postSP3/teardrop2-fix/">ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/ntfixes-postSP3/teardrop2-fix/</a> for Windows NT 4.0 and <a href="ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT351/ntfixes-postSP3/teardrop2-fix/">ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT351/ntfixes-postSP3/teardrop2-fix/</a> for Windows NT 3.5.1			
<b>IP Address</b>	<b>DNS Name</b>	<b>Additional Info</b>	<b>Session ID</b>
127.0.0.1	localhost		4

The title "Insurance Services" is displayed in a large, blue, sans-serif font, centered on the slide. The background behind the text is a white, glowing circular area that fades into the surrounding images of skyscrapers and a padlock.

# Insurance Services

- Computer Security Insurance
- Hack proof Insurance
- Market players include
  - ICSA Security Services

The background of the slide is a collage of three images: on the left, a low-angle shot of modern skyscrapers against a blue sky with clouds; in the center, the PrivyLink logo; and on the right, a close-up of a heavy-duty metal padlock that is open, set against a textured, brownish background.

# Prepare to be hacked?

- No hack proof system
- Setup Honey pot
- Setup Intrusion Detection System
- Setup proper audit logging system



# Investigation

- Search for evidence from hacked system
- Preserve as much evidence as possible
- Identify hacking source location
- Collect audit logs and trail from all relevant machines



The background of the slide features three distinct images: on the left, a low-angle shot of modern skyscrapers against a blue sky with clouds; in the center, the PRIVYLINK logo; and on the right, a close-up of a heavy-duty metal padlock with a keyhole, set against a textured, brownish background.

# Legislation

- In Hong Kong
  - ❑ No Computer Crime Ordinance
  - ❑ Based on
    - Crimes Ordinance, Cap 200
    - Theft Ordinance, Cap 210
    - Electronic Transactions Ordinance, Cap 553
    - Criminal Jurisdiction Ordinance, Cap 461
- No cross boundary law
- Legal entities have to learn more on security technology trend

The background of the slide is a collage of three images: on the left, a low-angle shot of modern skyscrapers against a blue sky with clouds; in the center, the PRIVYLINK logo; and on the right, a close-up of a heavy-duty metal padlock with a keyhole, set against a textured, brownish background.

## What individual can do?

- Learn to preserve evidence according to industry best practices
- Protect the systems based on security standards
- Conduct Security Awareness Training
- Establish connections with Security Organization Entity
- Perform regular checkup

The background of the slide is a collage of three images: on the left, a low-angle shot of modern skyscrapers against a blue sky with clouds; in the center, the PRIVYLINK logo; and on the right, a close-up of a heavy-duty metal padlock.

## What participants should do?

- No Security at all
- Any machines can be hacked any time
- Can Minimize hacking damage
- Track hacking evidence and identify hacking
- Corporate with Law enforcement entity and HK CERT



*Thank You*

**Tel: (852) 2523 3908  
Fax: (852) 2501 5503  
ricci@privylink.com.hk**

**PrivyLink (HK) Ltd  
Portion B, 38/F  
Bank of China Tower  
1 Garden Road  
Hong Kong**

**PrivyLink (Hong Kong) Ltd.**