ร่างพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ....

การประชุมคณะกรรมาธิการวิสามัญ ครั้งที่ ๒

วันพุธที่ ๒๙ พฤศจิกายน พ.ศ. ๒๕๔๙

อาคารรัฐสภา ๒

พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ประมวลกฎหมายอาญา

หลักสิทธิเสรีภาพขั้นพื้นฐานตามรัฐธรรมนูญ

ลักษณะทั่วไปของกฎหมายอาญา

กฎหมายอาญา คือ กฎหมายที่กำหนดฐานความผิดและบทลงโทษ โดยบุคคลจะรับโทษทางอาญาได้ก็ต่อเมื่อ มีกฎหมายในขณะกระทำความผิด กำหนดว่าการกระทำนั้นเป็นความผิดและมีบทลงโทษไว้

- มีลักษณะเป็นกฎระเบียบมุ่งเน้นให้ทุกคนอยู่ร่วมกันอย่างมีความสุข มุ่งเน้นเพื่อความสงบสุขทางสังคม เพื่อเรียบร้อยในบ้านเมือง เช่น ความผิดฐานฆ่าผู้อื่น,ทำร้ายร่างกาย, ลักทรัพย์, ชิงทรัพย์ฉ้อโกง, บุกรุก, ความผิดเกี่ยวกับการปลอมแปลง เป็นต้น

การปรับใช้กฎหมายอาญากับกฎหมายลักษณะอาญาฉบับอื่น

- มาตรา ๑๗ กำหนดว่า บทบัญญัติในภาค ๑ แห่งประมวลกฎหมายนี้ ให้ใช้ในกรณีแห่งความผิดตามกฎหมายอื่นด้วย

เช่น - หลักเจตนา ม. ๕๙

- การพยายามกระทำความผิด ม. ๘๐
- ตัวการ ผู้ใช้ และผู้สนับสนุนการกระทำผิด ม. ๘๓-๘๙ เป็นต้น

<u>ข้อสังเกต</u> จะเห็นได้ว่า ร่างพ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. .... จึงไม่ได้บัญญัติหลักการบางอย่างข้างต้นไว้ เนื่องจากสามารถนำกฎหมายอาญามาปรับใช้ได้อยู่แล้ว

การใช้กฎหมายอาญา

หลักดินแดน มาตรา ๔

- วรรคหนึ่ง การทำผิดในราชอาณาจักร ต้องรับโทษตามกฎหมาย
- วรรคสอง การทำความผิดในเรือไทย หรืออากาศยานไทย ให้ถือว่า เป็นการกระทำความผิดในราชอาณาจักร

หลักดินแดน มาตรา ๕

- วรรคหนึ่ง ความผิดใดที่การกระทำแม้แต่ส่วนหนึ่งส่วนใดได้กระทำในราชอาณาจักร, ผลแห่งการกระทำเกิดขึ้น หรือควรเกิดขึ้นในราชอาณาจักร, หรือย่อมจะเล็งเห็นได้ว่า ผลนั้นจะเกิดในราชอาณาจักร ให้ถือว่าความผิดนั้นได้กระทำในราชอาณาจักร

ประเด็นสำคัญที่มีการตั้งข้อสังเกตอย่างกว้างขวาง

๑) กฎหมายฉบับนี้ มีความทันสมัยสามารถปรับใช้ได้กับความผิดที่เกิดขึ้นในปัจจุบัน และรองรับความผิดในอนาคตที่จะมีความซับซ้อนตามพัฒนาการทางเทคโนโลยีหรือไม่

๒) ฐานความผิดบางมาตรา อาจกระทบต่อสิทธิหรือเสรีภาพขั้นพื้นฐาน เช่น ความเป็นส่วนตัว, การแสดงความคิดเห็น ควรกำหนดฐานความผิดอย่างไรให้เหมาะสม & มีความพอดี

๓) การกำหนดหน้าที่ให้ผู้ให้บริการเก็บ Traffic Data เป็นเวลาไม่น้อยกว่า ๓๐ วัน ก่อให้เกิดภาระมากเกินไปหรือไม่ (มาตรา ๒๔)

๔) ใคร คือ "ผู้ให้บริการ" ซึ่งมีหน้าที่ตามกฎหมายนี้ (มาตรา ๓)

ประเด็นสำคัญที่มีการตั้งข้อสังเกตอย่างกว้างขวาง

๕) บทลงโทษบางมาตรา เช่น โทษสำหรับ hacker น้อยเกินไปหรือไม่ (มาตรา ๕) ส่วนบางมาตรา เช่น หากกระทำผิดแล้วกระทบต่อความมั่นคงปลอดภัย มีโทษสูงสุดถึงขั้นประหารชีวิต (มาตรา ๑๑)

๖) อำนาจของพนักงานเจ้าหน้าที่มีมากจนเกินไปหรือไม่ เพราะอาจเป็นที่มาของการใช้อำนาจในทางมิชอบ (มาตรา ๑๖)

สถิติการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

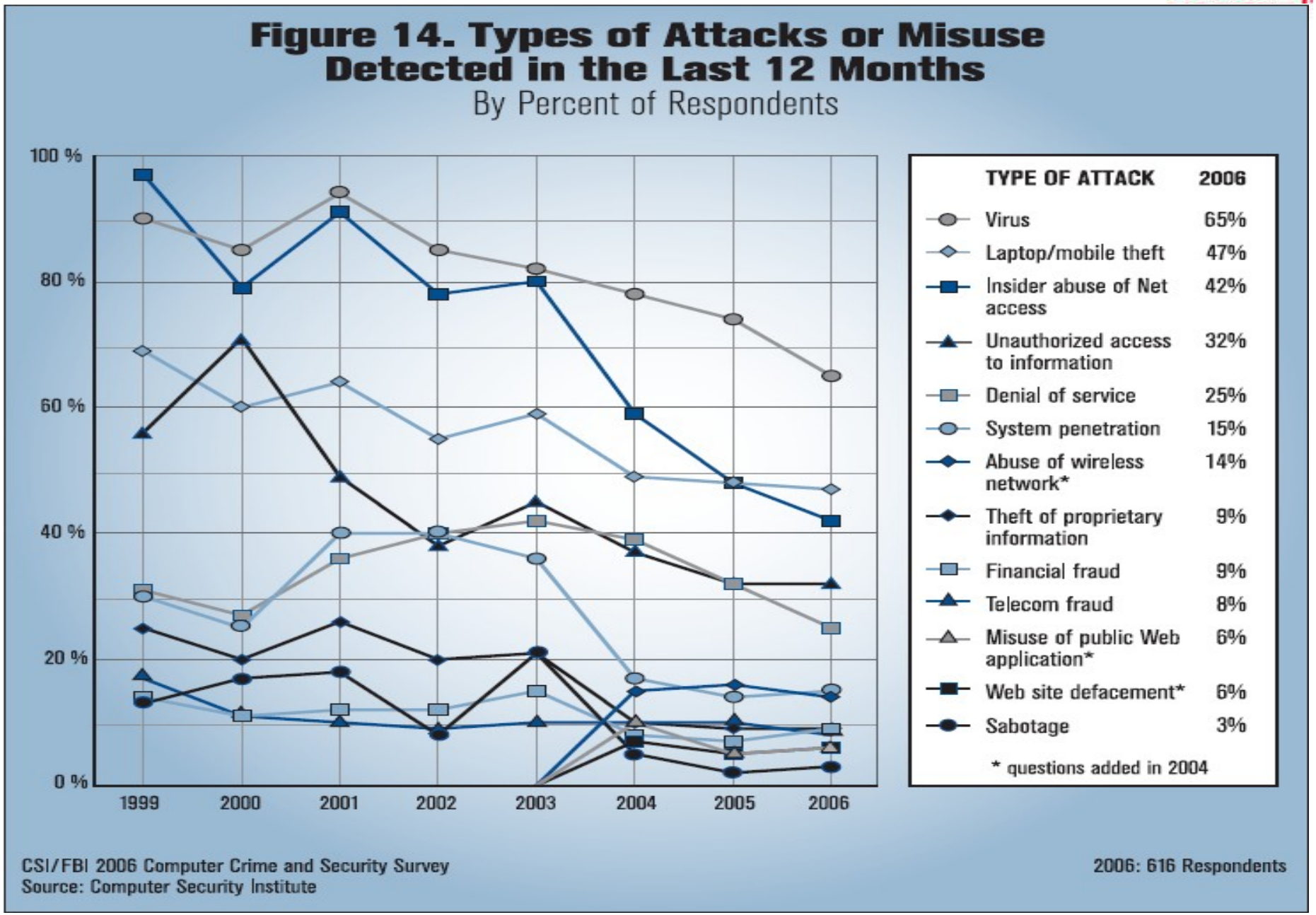


Figure 14. Types of Attacks or Misuse Detected in the Last 12 Months
By Percent of Respondents
100 %
80 %
60 %
40 %
20 %
0 %
1999
2000
2001
2002
2003
2004
2005
2006
TYPE OF ATTACK 2006
Virus 65%
Laptop/mobile theft 47%
Insider abuse of Net access 42%
Unauthorized access to information 32%
Denial of service 25%
System penetration 15%
Abuse of wireless network* 14%
Theft of proprietary information 9%
Financial fraud 9%
Telecom fraud 8%
Misuse of public Web application* 6%
Web site defacement* 6%
Sabotage 3%
* questions added in 2004
CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute
2006: 616 Respondents

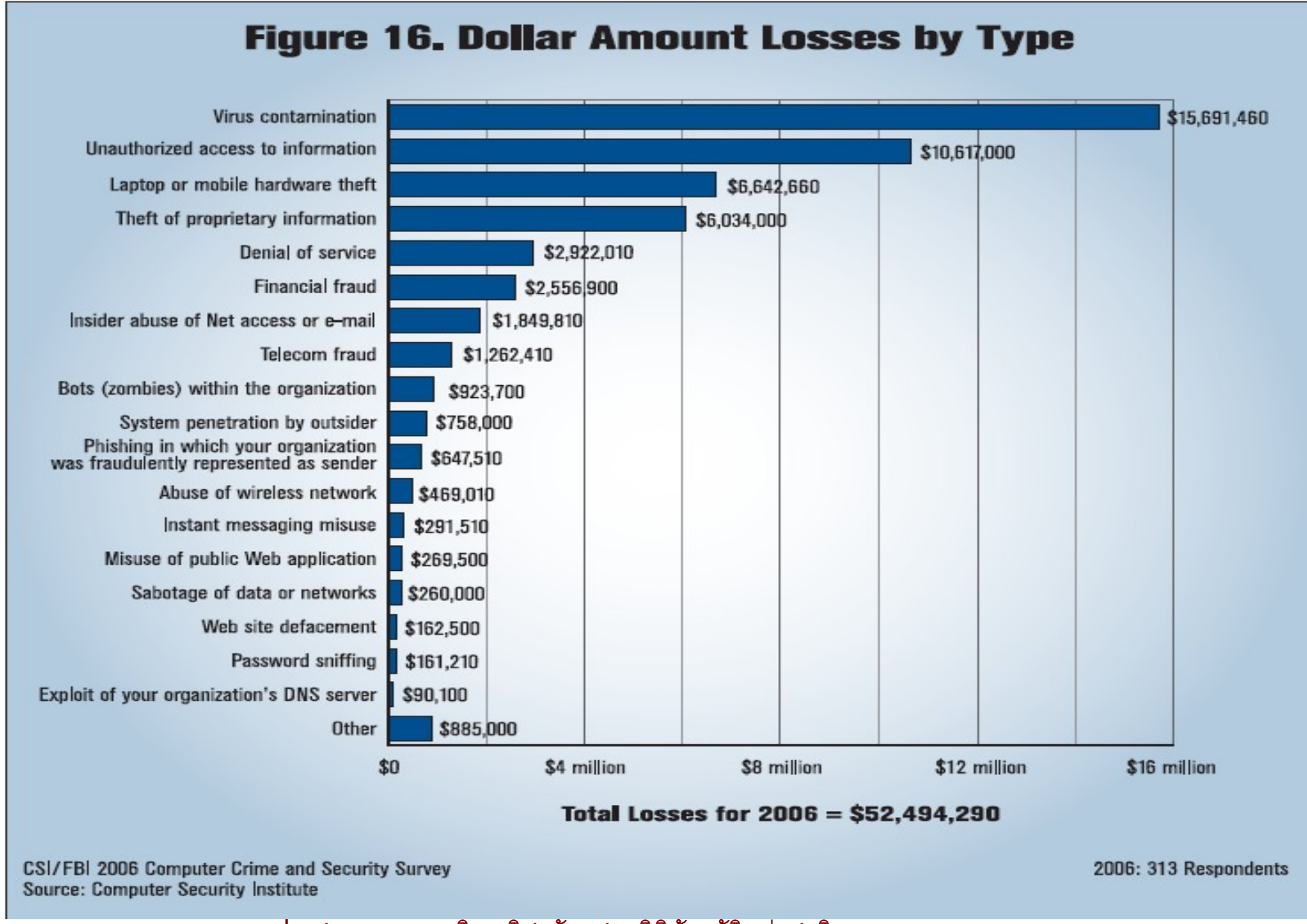
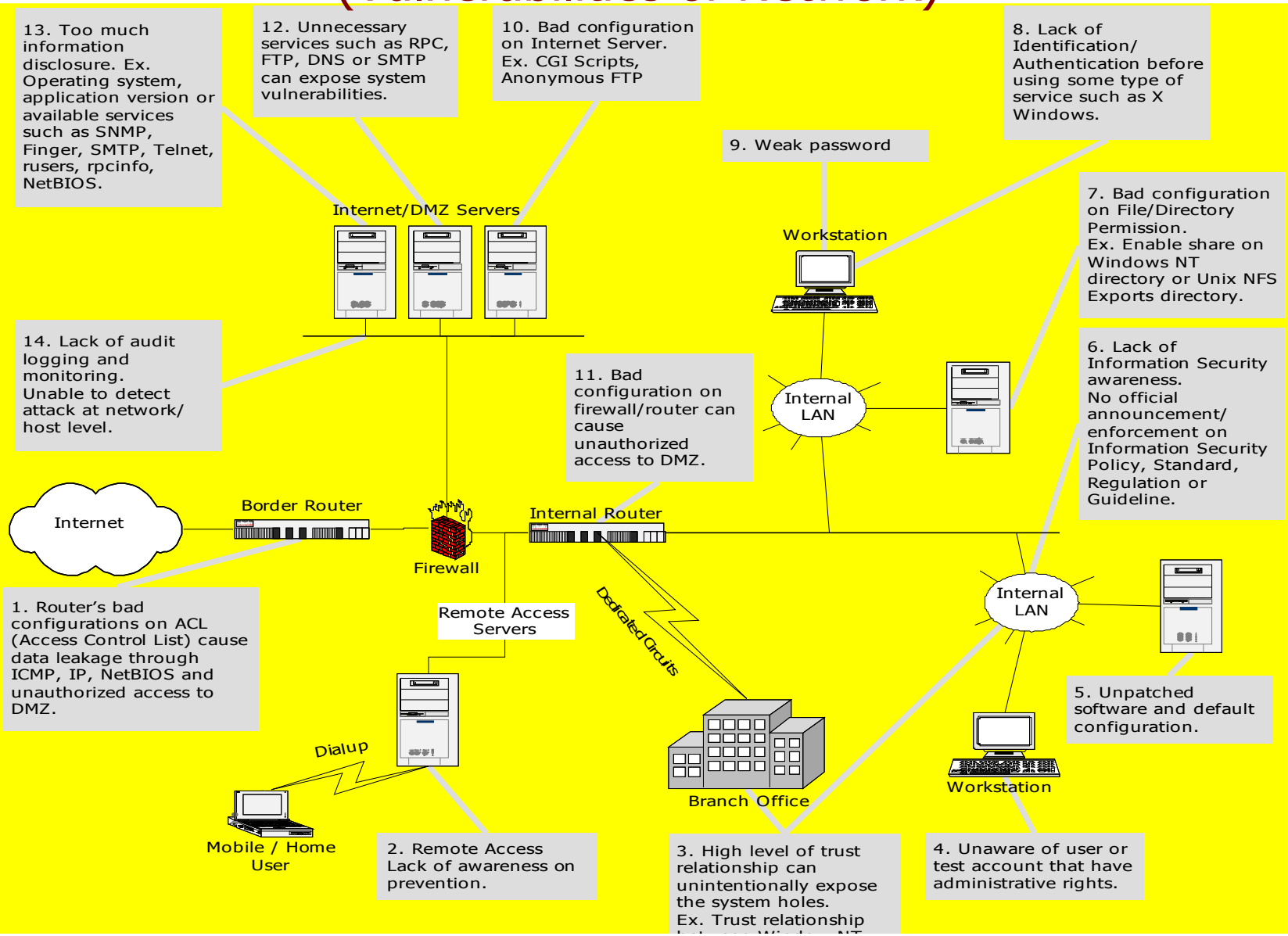


Figure 16. Dollar Amount Losses by Type
Virus contamination
$15,691,460
Unauthorized access to information
$10,617,000
Laptop or mobile hardware theft
$6,642,660
Theft of proprietary information
$6,034,000
Denial of service
$2,922,010
Financial fraud
$2,556,900
Insider abuse of Net access or e-mail
$1,849,810
Telecom fraud
$1,262,410
Bots (zombies) within the organization
$923,700
System penetration by outsider
$758,000
Phishing in which your organization was fraudulently represented as sender
$647,510
Abuse of wireless network
$469,010
Instant messaging misuse
$291,510
Misuse of public Web application
$269,500
Sabotage of data or networks
$260,000
Web site defacement
$162,500
Password sniffing
$161,210
Exploit of your organization's DNS server
$90,100
Other
$885,000
$0
$4 million
$8 million
$12 million
$16 million
Total Losses for 2006 = $52,494,290
CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute
2006: 313 Respondents

จุดอ่อนต่างๆ ของระบบเครือข่าย (Vulnerabilities of Network)



Source : Hacking exposed : Network Security Secrets & Solutions by Joel Scambray, Stuart McClure and George Kurtz

วิธีการ/รูปแบบการกระทำความผิด

การกระทำ	ตัวอย่าง
• ดักข้อมูล (eavesdropping)	Sniffer
• โปรแกรมร้าย (malicious code)	viruses/trojan horses
• โปรแกรมสำเนาตัวเองจำนวนมาก	worm
• โปรแกรมแอบขโมยข้อมูล	spyware/adware
• โปรแกรมแอบแก้ไขข้อมูล (data diddling)	logic bombs
• แปลงหมายเลข/ชื่อ ของต้นทาง (spoofing)	
• ส่ง email หลอกให้ไปเปิดเผยข้อมูลส่วนบุคคล (phishing)	
• สอบถามข้อมูลอย่างถี่ๆจนเครื่องไม่สามารถบริการได้	(denial of service)

การรุมสอบถามข้อมูลจนเครื่องล่ม
(Distributed Denial of Service) (DDoS)

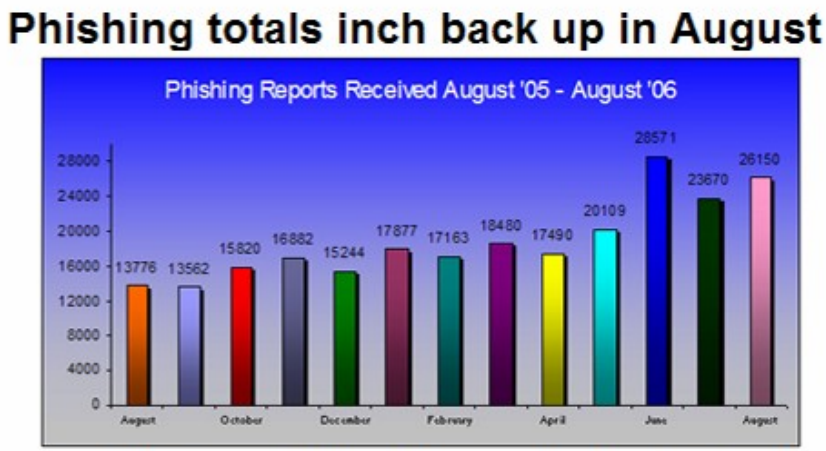
สถิติของ Cybercrime

According to an FBI projection, $67.2 billion a year is taken from U.S. businesses through cybercrime forums.

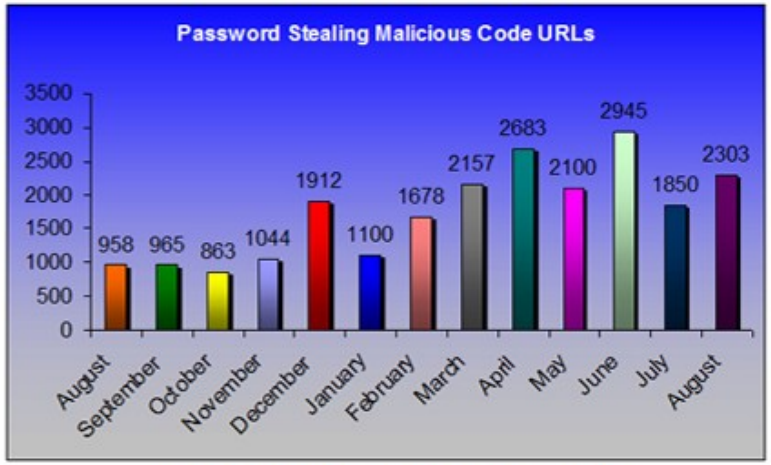
On these forums, hackers sell personal information such as bank account billing data, account numbers, billing addresses, and Social Security numbers, to other criminals. *USA Today* research found that a credit card number and its corresponding PIN typically sells for around $500.

http://www.smartcomputing.com/Editorial/daily/dailyContent.asp?guid=&did=2906875

สถิติ Phishing



Growth of reported phish bounces back up in August



Malicious code also bounces back

What is Phishing and Pharming?
Phishing attacks use both **social engineering** and **technical subterfuge** to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Technical subterfuge schemes plant **crimeware** onto PCs to steal credentials directly, often using Trojan keylogger spyware.

Pharming crimeware misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning.

Source: Anti-Phishing Working Group (http://antiphishing.org/)

ตัวอย่าง **Phishing website/email**

NCUA Home | Search | Privacy Policy & Accessibility | Site Map| Contact Us

National Credit Union Administration

Source: Anti-Phishing Working Group (http://antiphishing.org/)

Share Insurance | Resources for Credit Unions | Resources for Consumers | News | Search

Account Info Verification

Dear FCU holder account,

As part of our security measures, we regularly screen activity in Federal Credit Unions (FCU) network.
We recently noticed the following issue on your account: A recent review of your account determined that we require some additional information from you in order to provide you with secure service. Case ID Number: PP-065-617-349 For your protection, we have limited access to your account until additional security measures can be completed. We apologize for any inconvenience this may cause. Please log in to your FCU account to restore your access as soon as possible.

You must click the link below and fill in the form on the following page to complete the verification process.

Click here to update your account

In accordance with NCUA User Agreement, your account access will remain limited until the issue has been resolved. Unfortunately, if access to your account remains limited for an extended period of time, it may result in further limitations or eventual account closure. We encourage you to log in to your FCU account as soon as possible to help avoid this. We thank you for your prompt

About NCUA

The National Credit Union Administration (NCUA) is the independent federal agency that charters and supervises federal credit unions. NCUA, backed of the full faith and credit of the U.S. government, operates the National Credit Union Share Insurance Fund (NCUSIF) insuring the savings of 80 million account holders in all federal credit unions and many state-chartered credit unions. During the 1990s and into the 21st century, credit unions have been healthy and growing. Credit union failures remain low and the Share Insurance Fund maintains a healthy equity level. The National Credit Union Administration (NCUA) is comitted to maintain a safe environment for over 80 million account holders in all federal credit unions and many state-chartered credit unions. Protecting the security of holders account and of the Federal Credit Unions (FCU) network is our primary concern.

ตัวอย่าง **Phishing website/email**

E-mail

Source: Anti-Phishing Working Group (http://antiphishing.org/)

This phish combines some very dangerous tricks, perfect execution and a flaw in VISA's legitimate site to create the most dangerous phish scam yet.

The email message it is being spreaded with looks perfect:

VISA Verified by Visa

Dear Visa® customer,

Before activating your card, read this important information for cardholders!

You have been sent this invitation because the records of Visa Corporate indicate you are a current or former Visa card holder. To ensure your Visa card's security, it is important that you protect your Visa card online with a personal password. Please take a moment, and activate for Verified by Visa now.

Verified by Visa protects your existing Visa card with a password you create, giving you assurance that only you can use your Visa card online.

Simply activate your card and create your personal password. You'll get the added confidence that your Visa card is safe when you shop at participating online stores.

Activate Now for Verified by Visa

Thank you for your support.
Visa Service Department

It is much more convincing that the usual phish stuff. The sender i spofed, and the link is masked. But even further - if the link is examined, it turns out it leads to the following URL: 'http://usa.visa.com/track/dyredir.jsp?rDirl=http://200.251.251.10/.verified/'. And this is a URL that is really on the visa.com page! It turns out that the phishers have used a redirect page on the visa.com site to redirect to the phish server.

การเรียกค่าไถ่โดยจับข้อมูลเป็นตัวประกัน

Source: The Bangkok Post, May 25, 2005

TECHNOLOGY INTERNET EXTORTION

Now hackers can hold your files hostage

TED BRIDIS

Washington — Computer users already anxious about viruses and identity theft have new reason to worry: Hackers have found a way to lock up the electronic documents on your computer and then demand $200 over the Internet to get them back.

Security researchers at San Diego-based Websense Inc uncovered the unusual extortion plot when a corporate customer they would not identify fell victim to the infection, which encrypted files that included documents, photographs and spreadsheets.

A ransom note left behind included an e-mail address, and the attacker using the address later demanded $200 for the digital keys to unlock the files.

"This is equivalent to someone coming into your home, putting your valuables in a safe and not telling you the combination," said Oliver Friedrichs, a security manager for Symantec Corp.

The FBI said the scheme, which appears isolated, was unlike other Internet extortion crimes. Leading security and anti-virus firms this week were updating protective software for companies and consumers to guard against this type of attack, which experts dubbed "ransom-ware."

"This seems fully malicious," said Joe Stewart, a researcher at Chicago-based Lurhq Corp who studied the attack software. Stewart managed to unlock the infected computer files without paying the extortion, but he worries that improved versions might be more difficult to overcome. Internet attacks commonly become more effective as they evolve over time as hackers learn to avoid the mistakes of earlier infections.

"You would have to pay the guy, or law enforcement would have to get his key to unencrypt the files," Stewart said.

The latest danger adds to the risks facing beleaguered Internet users, who must increasingly deal with categories of threats that include spyware, viruses, worms, phishing e-mail fraud and denial of service attacks.

In the recent case, computer users could be infected by viewing a vandalised website with vulnerable Internet browser software. The infection locked up at least 15 types of data files and left behind a note with instructions to send e-mail to a particular address to purchase unlocking keys. In an e-mail reply, the hacker demanded $200 be wired to an Internet banking account. "I send program to your email," the hacker wrote.

There was no reply to e-mails sent to that address on Monday by the Associated Press.

Experts said there were no widespread reports the new threat was spreading, and the website was already shut down where the infection originally spread. They also said the hacker's demand for payment might be his weakness, since bank transactions can be traced easily.

"The problem is getting away with it — you've got to send the money somewhere," Stewart said. "If it involves some sort of monetary transaction, it's far easier to trace than an e-mail account." AP

คนส่ง spam mail ถูกตัดสินจำคุก 9 ปี ที่ North Carolina (ประกันตัวที่ 1 ล้านเหรียญ)

Address http://www.washingtonpost.com/wp-dyn/content/article/2006/09/05/AR2006090501166.html?referrer=emailarticle

Google Search PageRank 1 blocked Check AutoLink

Pop-up blocked. To see this pop-up or additional options click here...

Source : washingtonpost.com Sept.6,2006)

Print This Article
E-Mail This Article

Advertisement
A.G. EDWARDS.
FULLY INVESTED IN OUR CLIENTS.

QUICK QUOTES

Enter Symbol go
Tables | Portfolio | Index

MOST VIEWED ARTICLES

Technology | On the Site

Updated 10:15 p.m. ET

- Counting the Years, One Device at a Time
- 1,100 Laptops Missing From Commerce Dept.
- New Role Raises Eyebrows
- Access Denied
- Country's Hot, but Big Cities Offer Cold Shoulder

Advertisement
CardScan®

VA. APPEALS COURT

Anti-Spam Conviction Is Upheld

N.C. Man Flooded AOL Customers With Unsolicited E-Mail

By Candace Rondeaux
Washington Post Staff Writer
Wednesday, September 6, 2006; Page B03

The Court of Appeals of Virginia upheld yesterday what is believed to be the first conviction in the nation under a state anti-spamming law that makes it a felony to send unsolicited mass e-mails.

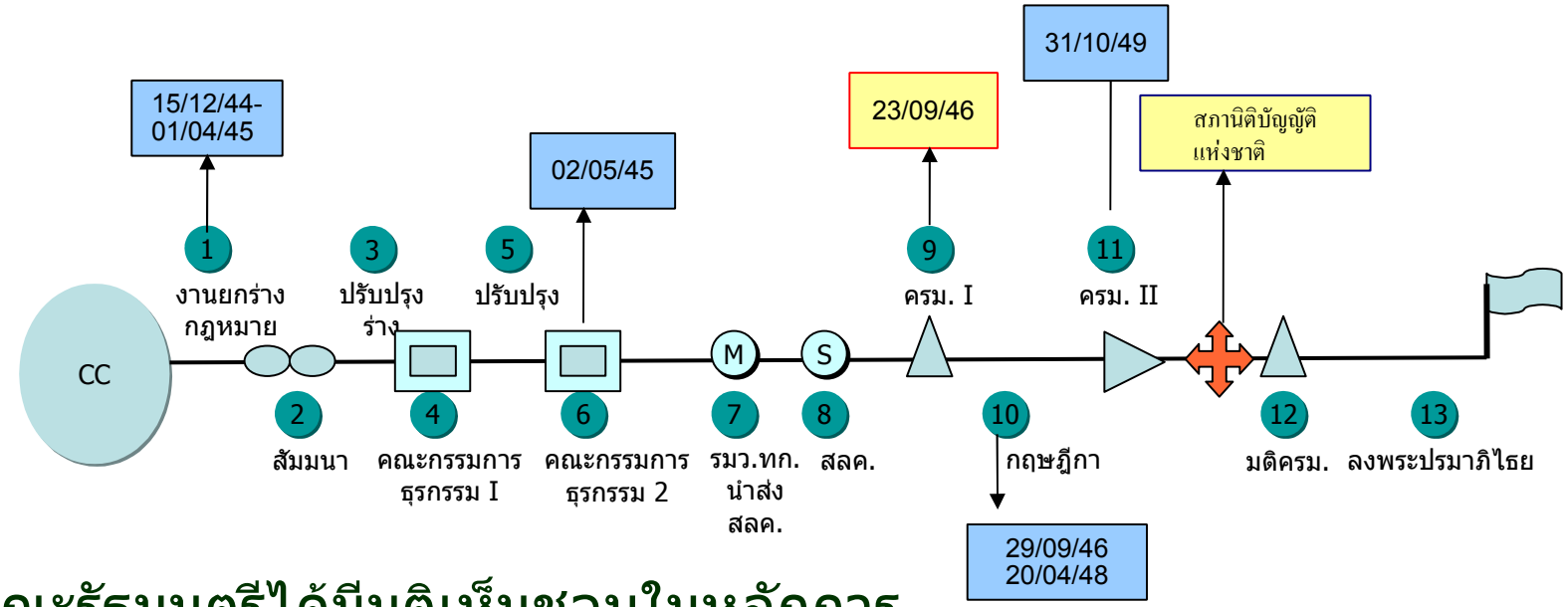
A North Carolina man was convicted in Loudoun County two years ago of illegally sending tens of thousands of e-mails to America Online customers. Prosecutors said Jeremy Jaynes flooded the servers at the Internet company's headquarters in Loudoun with bulk e-mail advertisements for computer programs and stock pickers.

Jaynes was sentenced last year to nine years in prison on three counts of violating the state's anti-spam law and was allowed to remain free on $1 million bond while his case was appealed. Thomas M. Wolf, an attorney for Jaynes, said he plans to appeal yesterday's

Enlarge This Photo

ความเป็นมา

การกระทำความผิดโดยการก่ออาชญากรรมทางคอมพิวเตอร์ อันเป็นการก่ออาชญากรรมรูปแบบใหม่ ยังไม่มีกฎหมายอาญาหรือลักษณะอาญาปัจจุบันฉบับใดรองรับหรือสามารถบังคับใช้ได้



คณะรัฐมนตรีได้มีมติเห็นชอบในหลักการของร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. .... เมื่อวันที่ 23 กันยายน 2546 และส่งร่างพระราชบัญญัติไปยังสำนักงานคณะกรรมการกฤษฎีกาเพื่อให้ตรวจพิจารณา

ความเป็นมา

สำนักงานคณะกรรมการกฤษฎีกา ได้มีคำสั่งแต่งตั้งคณะกรรมการกฤษฎีกา (คณะพิเศษ) คณะหนึ่งขึ้นเพื่อพิจารณาร่างพระราชบัญญัติฯ ดังกล่าว โดยมีศาสตราจารย์มีชัย ฤชุพันธุ์ เป็นประธานคณะกรรมการ

การรับฟังความคิดเห็น ได้มีการรับฟังความคิดเห็นมาโดยตลอดรวม 4 ครั้ง แม้ขณะคณะกรรมการกฤษฎีกา (คณะพิเศษ) พิจารณาแล้วเสร็จในรอบที่สอง และได้จัดบรรยายในรูปแบบการสร้างความรู้ความเข้าใจกว่า 20 ครั้ง

แนวทางในการยกร่างกฎหมาย

Council of Europe: Convention on Cybercrime
ปัจจุบันมีประเทศสมาชิกร่วมลงนาม 32 ประเทศ จาก 46 ประเทศ และประเทศอื่นซึ่งไม่ใช่สมาชิกอีกจำนวน 4 ประเทศ ได้แก่ แคนาดา ญี่ปุ่น แอฟริกาใต้ และสหรัฐอเมริกา

ฟิลิปปินส์: Electronic Commerce Act 2000

มาเลเซีย: Computer Crimes Act 1997

สิงคโปร์: Computer Misuse Act

ญี่ปุ่น: Unauthorized Computer Access Law 2000

อินเดีย: The Information Technology Act 2000

โครงสร้างร่างพระราชบัญญัติ

- บททั่วไป
  ชื่อกฎหมาย วันบังคับใช้ คำนิยาม และ
  ผู้รักษาการตามกฎหมาย

- หมวด 1 ความผิดเกี่ยวกับคอมพิวเตอร์
  (ความผิดเกี่ยวกับการรักษาความลับ ความครบถ้วน และ
  การทำงานของข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ &
  ความผิดเกี่ยวกับคอมพิวเตอร์

- หมวด 2 พนักงานเจ้าหน้าที่

ชื่อร่างพระราชบัญญัติ ฯ

ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ....

เหตุผล ได้มีการเปลี่ยนชื่อร่างกฎหมายจากเดิมว่า "ร่างพระราชบัญญัติว่าด้วยอาชญากรรมทางคอมพิวเตอร์ พ.ศ. ...."

เพราะการกระทำความผิดในบางลักษณะมิได้มีลักษณะเป็นอาชญากรรม เช่น

- ร่างมาตรา 13 การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งมีเนื้อหาอันไม่เหมาะสม
- ร่างมาตรา 14 ผู้ให้บริการซึ่งมิได้ลบเนื้อหาอันไม่เหมาะสมออก

คำนิยามสำคัญ

ร่างเดิม

- มีคำนิยามจำนวน 5 คำ ได้แก่ คำว่า "ระบบคอมพิวเตอร์", "ข้อมูลคอมพิวเตอร์", "ข้อมูลจราจรทางคอมพิวเตอร์", "พนักงานเจ้าหน้าที่" และ "รัฐมนตรี"

ร่างใหม่

- เพิ่มเติมคำนิยามจำนวน 2 คำ ได้แก่ นิยามคำว่า "ผู้ให้บริการ" , "ผู้ใช้บริการ"

<u>เหตุผล</u> เพราะ

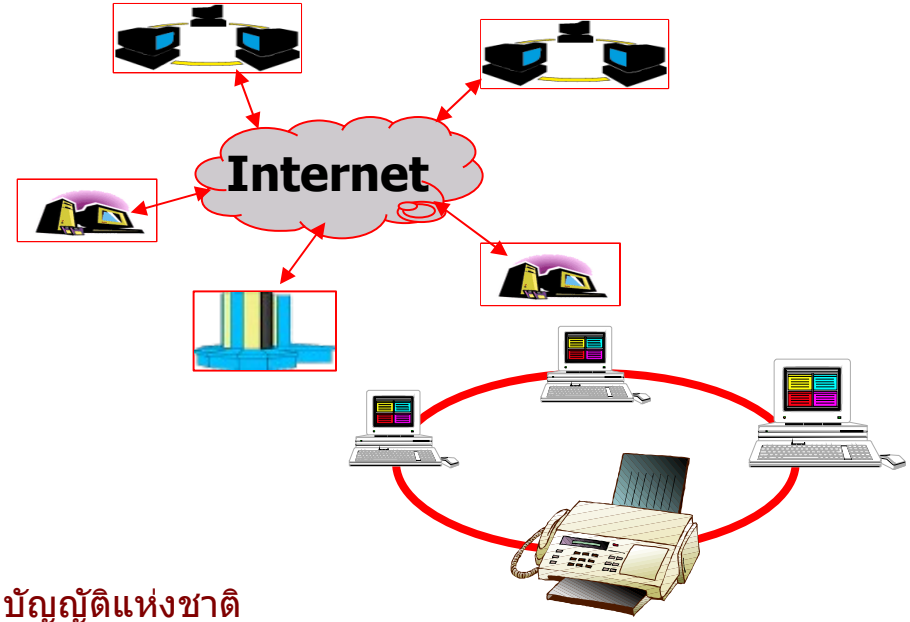
- ได้มีการกำหนดฐานความผิดเพิ่มเติมสำหรับ “ผู้ให้บริการ” ที่ไม่ลบข้อมูลคอมพิวเตอร์อันมีเนื้อหาอันไม่เหมาะสม (ร่างมาตรา 14)
- การกำหนดหน้าที่ของผู้ให้บริการในการเก็บข้อมูลจราจรทางคอมพิวเตอร์อันเป็นพยานหลักฐานสำคัญ (ร่างมาตรา 24)
- การใช้อำนาจพนักงานเจ้าหน้าที่ในการเรียกให้ผู้ให้บริการส่งมอบข้อมูลจราจรของผู้ให้บริการ (ร่างมาตรา 16) และ
- มีการกล่าวถึง “ผู้ใช้บริการ” ในร่างมาตรา 16 และร่างมาตรา 20, 21 และ 22

ระบบคอมพิวเตอร์

"ระบบคอมพิวเตอร์" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดชุดคำสั่งและแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ"

อะไรเป็นระบบคอมพิวเตอร์ได้บ้าง ?

คำนิยามนี้ ต้องไม่ล้าสมัยเมื่อมีความเปลี่ยนแปลงทางเทคโนโลยี



ข้อมูลคอมพิวเตอร์

"ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความ หรือชุดคำสั่ง บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้

ข้อมูลจราจรทางคอมพิวเตอร์

"ข้อมูลจราจรทางคอมพิวเตอร์" หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

ตัวอย่างข้อมูลจราจรของชุมสายโทรศัพท์ (Call detail record)

04151YT2614407110000390010490010000070000300021512890 053304XXX 0002000

- 04 = YTEL
- 1 = Metro
- 5 = YT
- 1 = Normal
- YT = Normal
- 071100= 7/11/00 วันที่
- 003900= 00:39 เวลาเริ่มต้น
- 104900=10:49 เวลาสิ้นสุด
- 100000=10:00:49 ระยะเวลา

ผู้ให้บริการ

"ผู้ให้บริการ" หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น ทั้งนี้โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตาม (๑)

เหตุผล :

(๑) เดิมประสงค์ให้หมายถึงผู้ให้บริการอินเทอร์เน็ตหรือผู้ให้บริการด้านโทรคมนาคมอื่นๆ สำหรับการติดต่อผ่านระบบคอมพิวเตอร์ แต่ต่อมาประสงค์ให้ครอบคลุมถึงเจ้าของเว็บไซต์ด้วย

(๒) บุคคลที่เข้าข่ายตาม (๒) ได้แก่ Web Hosting หรือผู้อยู่เบื้องหลังการให้บริการของบุคคลตาม (๑) รวมทั้งเจ้าหน้าที่/ admin ระบบของหน่วยงาน

ฐานความผิด

มาตรา 5 การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ
มาตรา 6 การเปิดเผยมาตรการป้องกันการเข้าถึง
มาตรา 7 การเข้าถึงข้อมูลคอมพิวเตอร์
มาตรา 8 การดักข้อมูลคอมพิวเตอร์โดยมิชอบ
มาตรา 9 การรบกวนข้อมูลคอมพิวเตอร์
มาตรา 10 การรบกวนระบบคอมพิวเตอร์
มาตรา 11 การกระทำความผิดต่อความมั่นคง
มาตรา 12 การจำหน่าย/เผยแพร่ชุดคำสั่งเพื่อใช้กระทำความผิด
มาตรา 13 การปลอมแปลงข้อมูลคอมพิวเตอร์/เผยแพร่เนื้อหาอันไม่เหมาะสม
มาตรา 14 ความรับผิดของผู้ให้บริการ
มาตรา 15 การเผยแพร่ภาพจากการตัดต่อ ดัดแปลง

การกำหนดฐานความผิด

เจตนารมณ์

- เพื่อกำหนดฐานความผิดและบทลงโทษสำหรับการกระทำความผิดต่อความลับ (Confidentiality) ความครบถ้วน (Integrity) หรือสภาพพร้อมใช้งาน (Availability) ของระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ รวมทั้งความผิดที่เกี่ยวข้องกับการกระทำความผิดทางคอมพิวเตอร์อื่นๆ เช่น การเผยแพร่ภาพอันไม่เหมาะสม และการตัดต่อภาพ เป็นต้น

- เพื่อกำหนดเกี่ยวกับอำนาจหน้าที่ของพนักงานเจ้าหน้าที่

สาระสำคัญของการพิจารณาฐานความผิด

การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ

"มาตรา ๕ ผู้ใดเข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหนึ่งเดือน หรือปรับไม่เกินหนึ่งพันบาท หรือทั้งจำทั้งปรับ

ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้"

<u>เหตุผล</u> เพราะผู้กระทำผิดส่วนใหญ่เป็นเด็กและเยาวชน และมักเป็นการกระทำความผิดในลักษณะกรรมเดียวผิดกฎหมายหลายบท

- กำหนดอัตราโทษน้อยลง จากเดิมจำคุกไม่เกิน 2 ปี ปรับไม่เกิน 4 หมื่นบาท ไปเป็น จำคุกไม่เกิน 1 เดือน หรือปรับไม่เกิน 1 พันบาท
- กำหนดให้เป็นความผิดอันยอมความได้

การเปิดเผยมาตรการป้องกันการเข้าถึง

"มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ"

การพิจารณาฐานความผิด - องค์ประกอบความผิดใกล้เคียงกับเรื่องการขาย/เผยแพร่อุปกรณ์หรือชุดคำสั่งหรือรหัสใช้อุปกรณ์ในทางมิชอบแต่มีขอบเขตการกระทำซึ่งต้องรับผิดแคบกว่า

การเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ

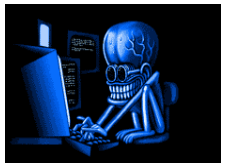
"มาตรา ๗ ผู้ใดเข้าถึงข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้"

การพิจารณาฐานความผิด

- การกระทำซึ่งเป็นความผิดตามมาตรา ๗ อาจต้องมีการกระทำความผิดตามมาตรา ๕ เสียก่อน
- กำหนดอัตราโทษน้อยลง และให้เป็นความผิดอันยอมความได้

การดักข้อมูลคอมพิวเตอร์โดยมิชอบ



ผู้โจมตีระบบ

แอบบันทึก **username & password**

"มาตรา ๘ ผู้ใดกระทำด้วยประการใดด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ความในวรรคหนึ่งไม่ใช้บังคับกับกรณีที่เป็นการดักรับข้อมูลคอมพิวเตอร์ตามคำสั่งเฉพาะของเจ้าของข้อมูลคอมพิวเตอร์"

การพิจารณาฐานความผิด - เหตุที่กำหนดหลักเกณฑ์ในวรรคสองเนื่องจากคำนึงการให้บริการด้าน Security บางประเภทเช่น การสแกนไวรัสคอมพิวเตอร์ที่ส่งจากภายนอกองค์กร เป็นต้น

การรบกวนข้อมูลคอมพิวเตอร์

"มาตรา ๙ ผู้ใดโดยมิชอบทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่น ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้"

การรบกวนระบบคอมพิวเตอร์

"มาตรา ๑๐ ผู้ใดกระทำด้วยประการใด ๆ อันเป็นการทำให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ"

<u>เหตุผล</u> การกำหนดฐานความผิดคำนึงถึงการก่อให้เกิดการปฏิเสธการให้บริการ (Denial of Service) เป็นสำคัญ

การกระทำซึ่งก่อให้เกิดผลกระทบต่อความมั่นคง

"มาตรา ๑๑ ถ้าการกระทำตามมาตรา ๙ หรือมาตรา ๑๐

(๑) ก่อให้เกิดผลอันเป็นความเสียหายแก่ข้อมูลคอมพิวเตอร์ของบุคคลทั่วไปไม่ว่าความเสียหายนั้นจะเกิดขึ้นในทันทีหรือในภายหลังและไม่ว่าจะเกิดขึ้นพร้อมกันหรือไม่ ผู้กระทำต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี และปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท หรือทั้งจำทั้งปรับ

(๒) เป็นการกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำตาม (๒) ก่อให้เกิดอันตรายแก่ร่างกายหรือชีวิตของประชาชน ผู้กระทำต้องระวางโทษประหารชีวิต จำคุกตลอดชีวิต หรือจำคุกตั้งแต่สิบปีถึงยี่สิบปี"

<u>เหตุผล</u> กำหนดโทษหนักขึ้นตามความเสียหายที่เกิดขึ้น

การใช้อุปกรณ์/ชุดคำสั่งในทางมิชอบ

"มาตรา ๑๒ ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นเพื่อใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๕ ถึงมาตรา ๑๐ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ"

<u>เหตุผล</u> จำกัดเฉพาะกรณีโปรแกรมคอมพิวเตอร์เท่านั้น ซึ่งแต่เดิมรวมถึงฮาร์ดแวร์ (อุปกรณ์) ด้วย

การเผยแพร่เนื้อหาอันไม่เหมาะสม

"มาตรา ๑๓ ผู้ใดกระทำด้วยประการใดๆ ดังต่อไปนี้

(๑) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์เพื่อให้ผู้อื่นเชื่อว่าข้อมูลคอมพิวเตอร์นั้นเป็นของบุคคลที่สามหรือจัดทำโดยบุคคลที่สาม โดยประการที่น่าจะทำให้บุคคลที่สามนั้นหรือประชาชนเสียหาย

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกกับประชาชน

(๒ทวิ) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรตามประมวลกฎหมายอาญา และข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

การเผยแพร่เนื้อหาอันไม่เหมาะสม (ต่อ)

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันมีลักษณะอันลามก และข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๔) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑) (๒) หรือ (๓) ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

ถ้าข้อมูลคอมพิวเตอร์อันลามกตาม (๓) เป็นภาพของบุคคลอายุไม่เกินสิบแปดปี ต้องระวางโทษจำคุกตั้งแต่สองปีถึงห้าปี หรือปรับตั้งแต่สี่หมื่นบาทถึงหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”

การกำหนดบทลงโทษผู้ให้บริการซึ่งมิได้ลบเนื้อหาอันไม่เหมาะสม

"มาตรา ๑๔ ผู้ให้บริการผู้ใดรู้ถึงการกระทำตามมาตรา ๑๓ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน มิได้จัดการลบข้อมูลคอมพิวเตอร์นั้นในทันที ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๓"

<u>เหตุผล</u> ผู้ให้บริการในที่นี้มุ่งประสงค์ถึงเจ้าของเว็บไซต์ซึ่งมีการพิจารณาว่าควรต้องมีหน้าที่ลบเนื้อหาอันไม่เหมาะสมด้วย

การเผยแพร่ภาพซึ่งตัดต่อในลักษณะหมิ่นประมาท

"มาตรา ๑๕ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้"

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย"

โทษ

ฐานความผิด	โทษจำคุก/ประหารชีวิต	โทษปรับ
มาตรา 5 เข้าถึงคอมพิวเตอร์โดยมิชอบ	<=1 เดือน	<=1,000 บาท
มาตรา 6 ล่วงรู้มาตรการป้องกัน	<=6 เดือน	<=10,000 บาท
มาตรา 7 เข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ	<=1 ปี	<=20,000 บาท
มาตรา 8 การดักข้อมูลคอมพิวเตอร์	<=3 ปี	<=60,000 บาท
มาตรา 9 การรบกวนข้อมูลคอมพิวเตอร์	<=5 ปี	<=100,000 บาท
มาตรา 10 การรบกวนระบบคอมพิวเตอร์	<=5 ปี	<=100,000 บาท
มาตรา 11 การกระทำต่อความมั่นคง - ก่อความเสียหายแก่ข้อมูลคอมพิวเตอร์ - กระทบต่อความมั่นคง - อันตรายแก่กายหรือชีวิต	 1 ปี – 10 ปี 3 ปี – 15 ปี ประหารชีวิต/จำคุกตลอดชีวิต 10 ปี – 20 ปี	 20,000 -200,000 บาท 60,000 -300,000 บาท
มาตรา 12 การจำหน่าย/เผยแพร่ชุดคำสั่ง	<=1 ปี	<=20,000 บาท
มาตรา 13 การเผยแพร่เนื้อหาอันไม่เหมาะสม	2 ปี – 5 ปี	40,000-100,000 บาท
มาตรา 14 ความรับผิดของ ISP	2 ปี – 5 ปี	40,000-100,000 บาท
มาตรา 15 การตัดต่อภาพผู้อื่น	<=3 ปี	<=60,000 บาท

หมวด 2 พนักงานเจ้าหน้าที่

มาตรา 16 อำนาจทั่วไปของพนักงานเจ้าหน้าที่ที่ได้รับการแต่งตั้ง

- เข้าถึงระบบคอมพิวเตอร์/ข้อมูลคอมพิวเตอร์
- ถอดรหัสลับ
- เรียกข้อมูลจราจรคอมพิวเตอร์
- ยึดอายัดระบบคอมพิวเตอร์

มาตรา 17 ระยะเวลาในการยึด/อายัดระบบคอมพิวเตอร์

30 วัน หรือ 60 วัน

มาตรา 18 เงื่อนไขการใช้อำนาจตามมาตรา 16

- ต้องไม่เป็นอุปสรรค/เกินจำเป็น
- รายงานต่อศาลจังหวัดที่มีเขตอำนาจ/ศาลอาญา

หมวด 2 พนักงานเจ้าหน้าที่

มาตรา 19 ข้อยกเว้นเกี่ยวกับชุดคำสั่งที่ไม่พึงประสงค์

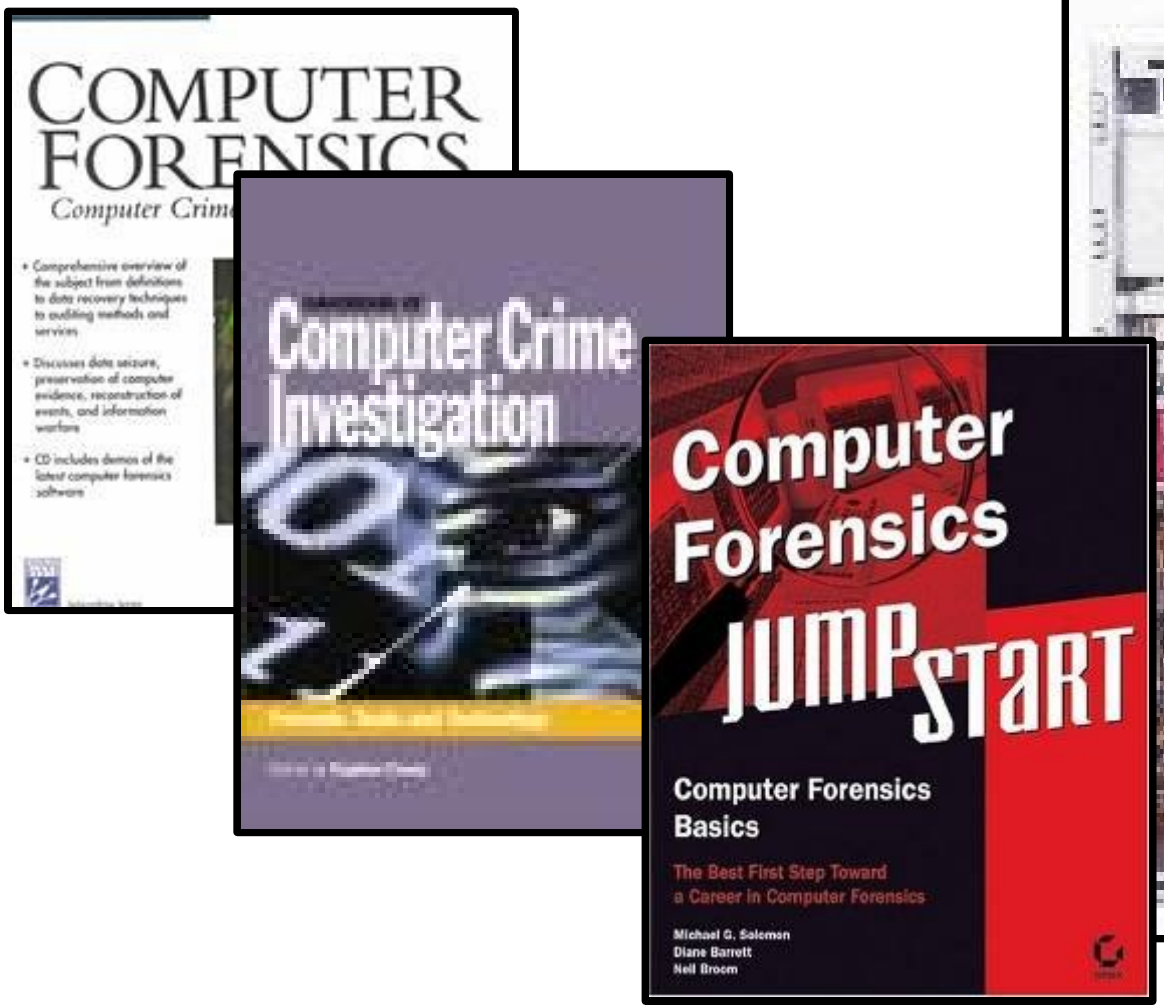
มาตรา 20 ถึงมาตรา 23
ข้อห้ามเกี่ยวกับการเปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ และกรณีฝ่าฝืน

มาตรา 24 หน้าที่ในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (30 วัน โทษปรับไม่เกิน 500,000 บาท)

มาตรา 25 การขัดขวางการปฏิบัติหน้าที่/ไม่ปฏิบัติตามคำสั่ง และค่าปรับทางปกครอง

มาตรา 26 ถึงมาตรา 28
การแต่งตั้งพนักงานเจ้าหน้าที่ การแสดงบัตรเมื่อปฏิบัติหน้าที่ และการปฏิบัติหน้าที่

Computer Forensics



อำนาจของพนักงานเจ้าหน้าที่ (1)

พ.ร.บ.ให้อำนาจแก่พนักงานแก่พนักงานเจ้าหน้าที่ ดังนี้

- เรียกให้ส่งมอบข้อมูล/อุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์
- ทำสำเนาข้อมูลคอมพิวเตอร์
- ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์
- เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารบนระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง
- ถอดรหัส/สั่งให้บุคคลที่เกี่ยวข้องกับข้อมูลคอมพิวเตอร์ทำการถอดรหัสลับ
- มีหนังสือสอบถามหรือเรียกบุคคลใดๆ ที่เกี่ยวข้องกับการกระทำดังกล่าวมาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ เอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

อำนาจของพนักงานเจ้าหน้าที่ (2)

อำนาจในการตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์

- การดักข้อมูลจราจรทางคอมพิวเตอร์แบบ Real-time
- การเคลื่อนย้ายข้อมูลคอมพิวเตอร์ต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์

การใช้อำนาจในการรวบรวมพยานหลักฐาน ให้พนักงานเจ้าหน้าที่ดำเนินการเฉพาะเท่าที่จำเป็นเพื่อประโยชน์ในการป้องกันและปราบปรามการกระทำความผิด

อำนาจหน้าที่ของพนักงานเจ้าหน้าที่ (3)

ความผิดเพื่อลงโทษแก่บุคคลผู้นำพยานหลักฐานที่ได้จากการสอบสวนตามร่างพระราชบัญญัตินี้ไปใช้ในทางมิชอบ

มาตรา 20 ห้ามพนักงานเจ้าหน้าที่เปิดเผยมอบข้อมูลที่ได้จากการสอบสวนไปใช้ประโยชน์อื่นใดนอกเหนือจากการดำเนินคดีอาชญากรรมทางคอมพิวเตอร์ (เพราะพนักงานเจ้าหน้าที่ตามร่างกฎหมายมีอำนาจค่อนข้างมาก อาจเป็นที่มาของการใช้อำนาจในทางมิชอบ)

มาตรา 21 พนักงานเจ้าหน้าที่กระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลที่ได้จากการสอบสวน

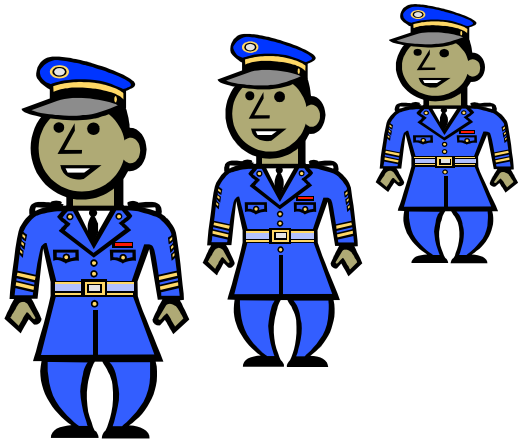
มาตรา 22 กำหนดบทลงโทษบุคคลอื่นซึ่งล่วงรู้พยานหลักฐานที่พนักงานเจ้าหน้าที่รวบรวมได้

มาตรา 23 ห้ามมิให้รับฟังการอ้างหรือใช้ประโยชน์ในข้อมูลที่ได้มาโดยมิชอบ

พนักงานเจ้าหน้าที่

การแต่งตั้งพนักงานเจ้าหน้าที่

"มาตรา ๒๖ การแต่งตั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ ให้รัฐมนตรีแต่งตั้งจากเจ้าหน้าที่ของรัฐซึ่งมีความรู้และความชำนาญเกี่ยวกับระบบคอมพิวเตอร์และผ่านการอบรมหลักสูตรตามที่รัฐมนตรีกำหนด"



การปฏิบัติหน้าที่ของพนักงานเจ้าหน้าที่

"มาตรา ๒๗ ในการปฏิบัติหน้าที่พนักงานเจ้าหน้าที่ต้องแสดงบัตรประจำตัวต่อบุคคลซึ่งเกี่ยวข้อง

บัตรประจำตัวให้เป็นไปตามแบบที่รัฐมนตรีกำหนดโดยประกาศในราชกิจจานุเบกษา"

พนักงานเจ้าหน้าที่

"มาตรา ๒๘ ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่ที่รัฐมนตรีกำหนด เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ ตามประมวลกฎหมายวิธีพิจารณาความอาญา

ในการจับ ควบคุม ค้น สอบสวน และดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจ พนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานฝ่ายปกครองหรือตำรวจ พนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวน ดำเนินการได้เฉพาะตามที่ได้รับการร้องขอจากพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้

ให้นายกรัฐมนตรีในฐานะผู้กำกับดูแลสำนักงานตำรวจแห่งชาติและรัฐมนตรีมีอำนาจร่วมกันกำหนดระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการดำเนินการตามวรรคสอง"

หน้าที่ของผู้ให้บริการ (1)

- ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ไว้ไม่น้อยกว่าสามสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ (มาตรา 24)
- ในกรณีที่ผู้ใช้บริการมีสัญญาหรือข้อตกลงในการใช้บริการกับผู้ให้บริการ ผู้ให้บริการต้องเก็บข้อมูลของผู้ใช้บริการที่ปรากฏในสัญญาหรือข้อตกลงนั้นไว้เป็นเวลาไม่น้อยกว่าสามสิบวันนับแต่วันที่สัญญาหรือข้อตกลงนั้นสิ้นอายุ (มาตรา 24)
- ในกรณีที่มีเหตุอันควรสงสัยว่ามีผู้กระทำความผิด พนักงานเจ้าหน้าที่ มีอำนาจยึดหรืออายัดระบบคอมพิวเตอร์ที่ต้องสงสัยได้รวม 90 วัน (มาตรา 17)

ข้อสังเกต ในทางปฏิบัติการทำ Computer Forensics บางครั้งเกิด 90 วัน ระยะเวลาที่กำหนดในร่างกฎหมายจึงอาจไม่เพียงพอ

หน้าที่ของผู้ให้บริการ (2)

- ผู้ให้บริการมีหน้าที่เก็บข้อมูลจราจรไม่เกิน 90 วัน
- หลักเกณฑ์ต่างๆ ข้างต้นจะใช้กับผู้ให้บริการประเภทใด และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา
- หากผู้ให้บริการไม่ปฏิบัติตาม มีโทษปรับไม่เกิน 500,000 บาท (ม.24)

ข้อสังเกต ผู้ให้บริการรายเล็กค่อนข้างไม่เห็นด้วยกับค่าปรับที่มีอัตราสูง หากแต่ก็ได้มีการชี้แจงเรื่องค่าของเงินที่จะมีการเปลี่ยนแปลงในอนาคต และ

ข้อน่าสนใจ คือ หากผู้ให้บริการไม่ยอมปฏิบัติตาม ก็เพียงจ่ายค่าปรับเท่านั้น แต่ผลที่ได้รับ คือ จะไม่มีข้อมูลจราจรคอมพิวเตอร์อันสามารถนำไปใช้เป็นพยานหลักฐานสำคัญในการดำเนินคดี

ระหว่างภัยจากการก่อการร้าย และ ความสะดวกสบาย เราจะเลือกอะไร? รัฐจะคุ้มครองอย่างไร?

หนังสือพิมพ์นิวยอร์คไทมส์

• สำรวจ เมื่อ 10 ก.ย. 49 พบว่า 69% ยังหวาดผวากับ 11 ก.ย.โดย 1/3 ยังคิดถึง 11 ก.ย.

56% ไม่ต้องการทำงานบนตึกสูง 58% คิดว่ารัฐบาลสหรัฐยังทำไม่เพียงพอในการป้องกันเหตุร้าย

ขณะที่ 34% เห็นว่าทำดีแล้ว 57% เชื่อว่าผู้ก่อการร้ายจะก่อเหตุร้ายกับนิวยอร์คอีก 35% เชื่อว่าไม่น่าจะเกิดแล้ว

สถานีซีบีเอส สำรวจพบว่า

70% เชื่อมั่นในความสามารถของรัฐบาลในการป้องกันเหตุร้าย

68% เห็นด้วยกับการสูญเสียอิสรภาพบางอย่าง เพื่อให้รัฐปกป้อง

59% ไม่เต็มใจให้รัฐตรวจสอบการใช้โทรศัพท์หรืออีเมล

http://www.msnth.com/msn/news/foreigndaily/article5.asp
สำนักข่าวไทย MCOT.net