Principle of Information Security

Asst. Prof. Kemathat Vibhatavanij Ph.D.

Security Challenges

Compliance to government laws and regulations

Evolution of technology focused on ease of use

Direct impact of security breach on corporate asset base and goodwill

Increased number of network-based applications

It is difficult to centralize security in a distributed computing environment

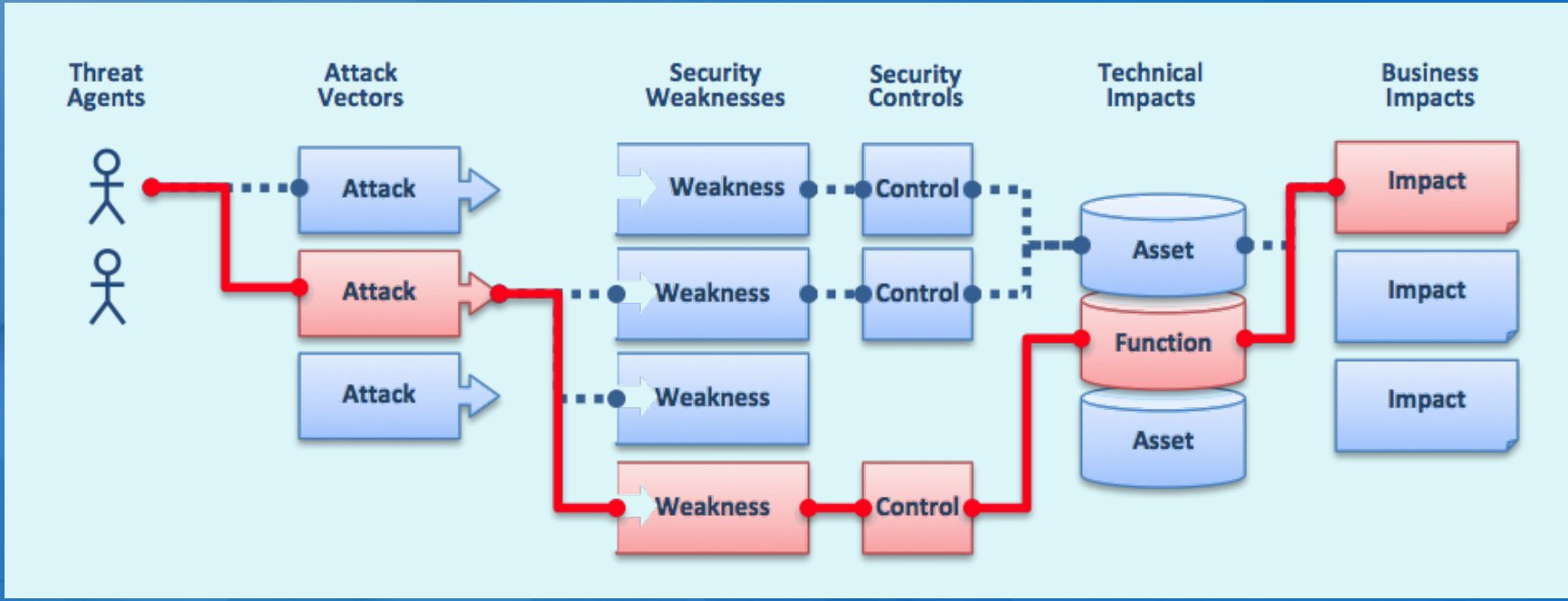
Increasing complexity of computer infrastructure administration and management

Information Security Threats

Threat: A potential cause of an incident that may result in harm of systems and organization

Natural threats	Physical security threats	Human threats
• Natural disasters e.g. floods, earthquakes, hurricanes	• Physical intrusion, loss or damage of system resources, sabotage	• Hackers, insiders, social engineering, lack of knowledge and awareness

Threats to an organization



Who is a hacker ?

Definition

- A person who ILLEGALLY BREAKS into a system or network WITHOUT ANY AUTHORIZATION to destroy, steal or perform malicious attacks

Purpose of breaking systems

- Test his/her skill
- Hobby
- Gain knowledge and poking (intruding)
- Malicious intention

What does a hacker do?

Reconnaissance

The meaning

- (preparatory phase) an attacker seeks to gather info. about a target prior to launching an attack

The type

- Passive reconnaissance
  - Acquire w/o interacting with the target
- Active reconnaissance
  - Involve interacting with the target

Scanning

Pre-attack phase	• Scan the network for specific info.
Port scanner	• Use efficient tools to scan port/vulnerabilities
Extract information	• Extracting information from scanning result

Gaining access

Attacker obtains access to OS DBS or apps.

Escalate privilege to obtain COMPLETE control of the SYSTEM

Maintaining access

Attacker tries to RETAIN his/her ownership of the system

- Prevent attack from other attacker or the REAL system owner

Attacker can upload download or manipulate data, applications or configuration on the owned system

- Use the compromised system to lunch further attack

Covering track

ADVANCED PERSISTENT THREATS

A Symantec Perspective

Introduction to APT

- Threat landscape: an emergence of highly targeted, long-term, int'l espionage and sabotage campaigns be COVERT STATE ACTORS
- APT: is a type of targeted attack
  - An APT is ***always*** a targeted attack **BUT** a targeted attack is ***not necessary*** an APT

Behavior of an APT

- Customized attacks
  - Use highly customized tools and intrusion techniques
  - Developed specifically for the campaign
  - Always launch multiple threats or “kill chainsW simultaneously
- Low and slow
  - Move slow and quietly
  - Continuous monitoring and interaction

Behavior of an APT

- Higher aspirations
  - Aim high, e.g. military, political, economy,, disruption of op., destruction of eq.
- Specific targets
  - Smaller range of targets
  - Intellectual property
  - trade secret

Incursion

- Attackers break into network by using social engineering to deliver targeted malware to vulnerable systems and people
- Reconnaissance
- Social engineering
- Zero-day vulnerabilities
- Manual opeartions

Discovery

- Once in, the attackers stay “low and slow” to avoid detection, then map the organization’s defenses from the inside and create a battle plan and deploy multiple parallel kill chains to ensure success
- Multiple vectors
  - Once malware is present on host systems, additional tools can be downloades as needed
- Run silent, run deep
- Research and analysis
  - Research and analysis on found systems and data including network topology, user IDs, passwd etc.

Capture

- Attackers access unprotected systems and capture information over an extended period. They may also install malware to secretly acquire data or disrupt operations
- Long-term occupancy
  - Ghostnet began capturing data on May 22, 2007 and continued at least through March 12, 2009
- Control
  - Stuxnet went beyond stealing information

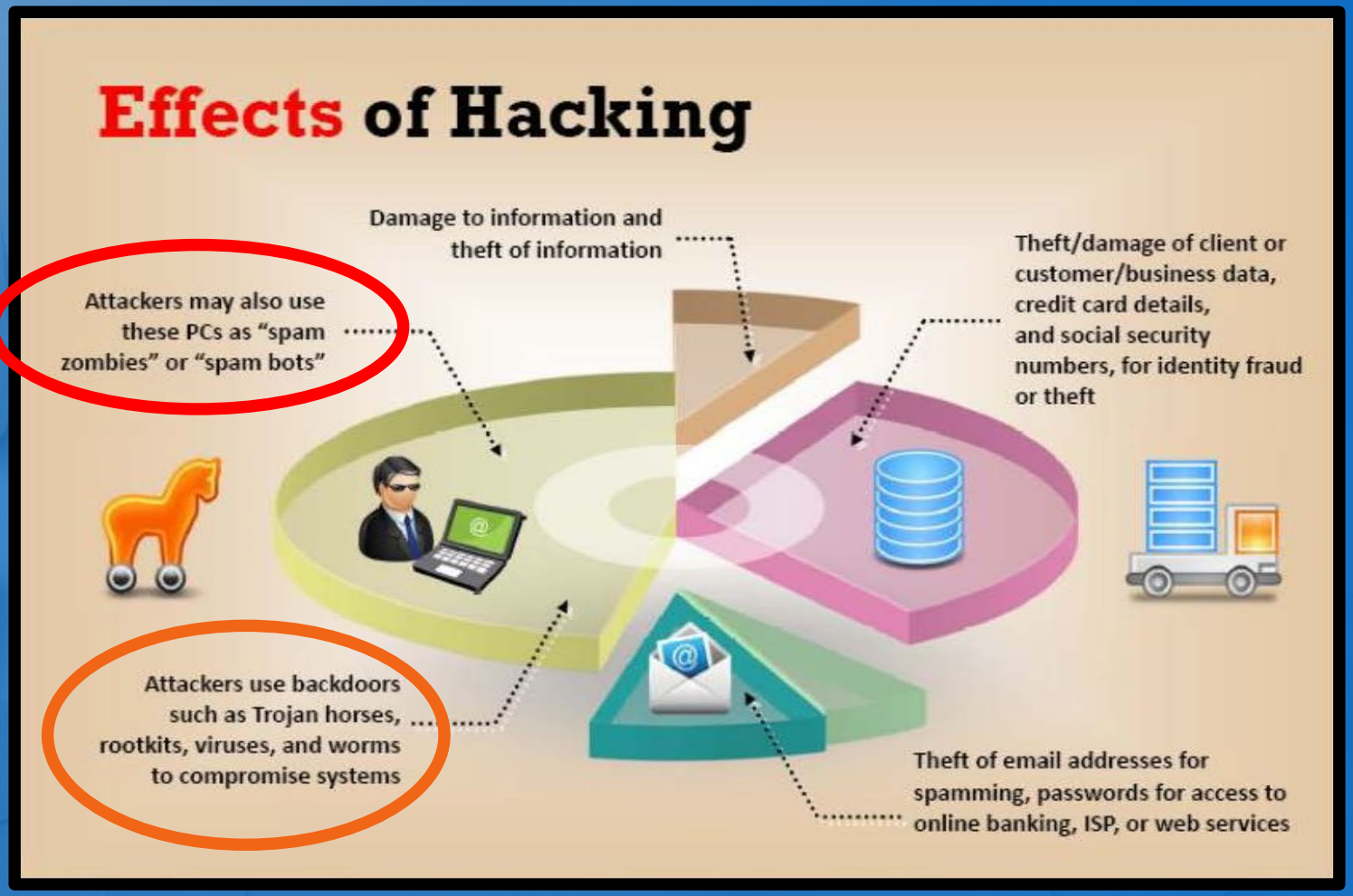
Exfiltration

- Captured information is sent back to attack team's home base for analysis and further exploitation or fraud
- Data transmission
- Ongoing analysis

End of

“A Symantec Perspective”

Effect of hacking, an Example



Secure our information, don’t we?

Info. Sec. is everyone's responsibility

Security Awareness… from Personal

To … Enterprise

Security goals

Protect

- Disclosure
- Modification
- Loss of availability

Critical Element of Information Security Program Success

- Senior Management Commitment to Information Security Initiatives
- Management Understanding of Information Security Issues
- Information Security Planning Prior to Implementation of New Technologies
- Integration Between Business and Information Security
- Alignment of Information Security with the Organization's Objective
- Executive and Line Management Ownership and Accountability for Implementing, Monitoring and Reporting on Information Security

InfoSec and Org.Mgmt.

Strategic management

- Vision, mission, core value
- Strategic and operational plan

Risk management

- Known threats
- Unknown/Incident threats

Business continuity

- Contingency plan

A requirement from professionals

- Information security and risk management
- Access control
- Cryptography
- Physical security
- Security architecture and design
- Business continuity and disaster recovery planning
- Telecommunication and network security
- Application security
- Operation security
- Legal, regulation, compliance and investigation

Types of Hacker

Coders	• The programmers who have the ability to find the unique vulnerability in existing software and to create working exploit codes
Admins	• The computer guys who use the tools and exploits prepared by the coders
Script Kiddies	• The bunnies who use script and programs developed by others to attack computer systems and networks

Types of Hacker

White Hat Hacker

- A computer guy who perform Ethical Hacking

Black Hat Hacker

- A computer guy who performs Unethical Hacking

Grey Hat Hacker

- A computer guy who sometimes acts legally, sometimes in good will, and sometimes not

Types of Hacker

Hacktivist

- A person who try to broadcast political or social messages through their work to raise public awareness of an issue

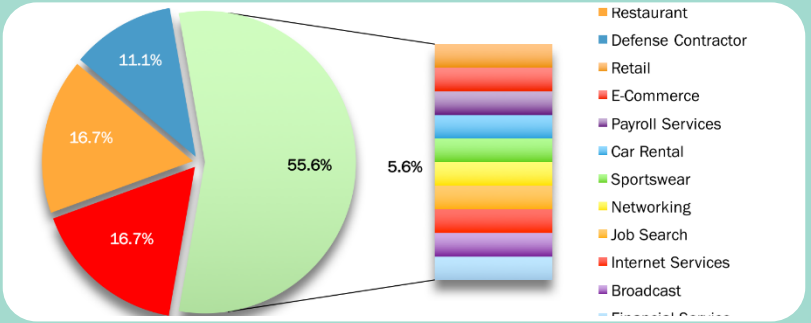
Cyber Terrorist

- A person who attack government computers or public utility infrastructures, crash critical systems or steal classified information.

Cyber Attack

- Norse
- Kaspersky
- FireEye
- Checkpoint
- Fortinet
- …. You name it !!!

Maps of cyber attack



Statistics of cyber attack

- Hackmageddon
- Symantec
- IBM
- Kaspersky
- Etc.

invincea 2016 CYBERTHREAT DEFENSE REPORT

NORTH AMERICA, EUROPE, ASIA PACIFIC, & LATIN AMERICA

SURVEY DEMOGRAPHICS

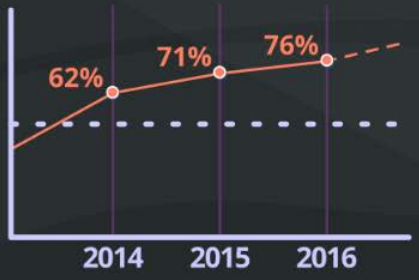
10 Countries represented around the world

20+ Industries represented

1,000 Qualified IT security decision makers & practitioners

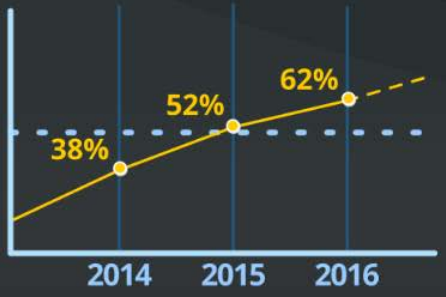
RISING CYBERATTACKS

The percentage of respondents affected by successful attacks is rising each year.



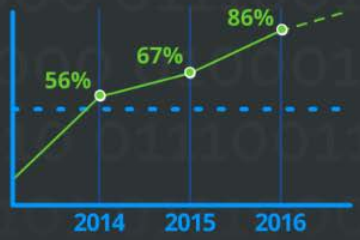
SINKING EXPECTATIONS

Respondents that believe a successful cyberattack is likely in the coming year is skyrocketing.



ENDPOINT PROTECTION REVOLUTION

The percentage of organizations evaluating new endpoint protection solutions to augment or replace their existing investments is skyrocketing.



THE YEAR OF ENDPOINT CONTAINERIZATION

The top four endpoint security technologies targeted for acquisition in 2016 include...

1. CONTAINERIZATION/ MICRO-VIRTUALIZATION
2. SELF-REMEDIATION FOR INFECTED ENDPOINTS
3. DIGITAL FORENSICS/ INCIDENT RESOLUTION
4. DATA LOSS/LEAK PREVENTION (DLP)

SECURITY'S BIGGEST OBSTACLES

These obstacles inhibit IT from defending cyberthreats...

1. LOW SECURITY AWARENESS AMONG EMPLOYEES
2. TOO MUCH DATA TO ANALYZE
3. LACK OF SKILLED PERSONNEL

CYBERTHREAT HEADACHES

Cyberthreats causing the greatest concern include...

1. MALWARE (VIRUSES, WORMS, TROJANS)
2. PHISHING/ SPEAR-PHISHING ATTACKS
3. SSL-ENCRYPTED THREATS

SECURITY'S WEAKEST LINKS

These areas are rated as most difficult to secure...

1. MOBILE DEVICES
2. SOCIAL MEDIA APPLICATIONS
3. LAPTOPS/ NOTEBOOKS

SUSCEPTIBLE NATIONS

The percentage of respondents affected by successful attacks in 2015 varied by nation.

BRAZIL	89%
FRANCE	82%
CANADA	82%
GERMANY	78%
UNITED STATES	75%
JAPAN	75%
MEXICO	74%
SINGAPORE	73%
UNITED KINGDOM	71%
AUSTRALIA	63%

DOWNLOAD THE FULL REPORT AT:
www.invincea.com/cyber-threat-report

CYBEREDGE GROUP

IMPERVA® 2017 CYBERTHREAT DEFENSE REPORT

SURVEY DEMOGRAPHICS

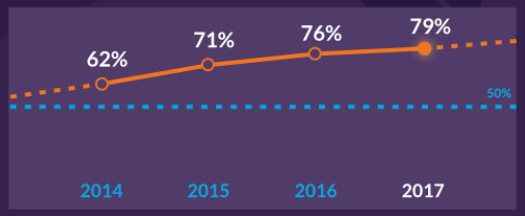
15 Countries represented around the world

19 Industries represented

1,100 Qualified IT security decision makers & practitioners

RISING CYBERATTACKS

The percentage of respondents affected by successful attacks has risen the last three years with no end in sight.



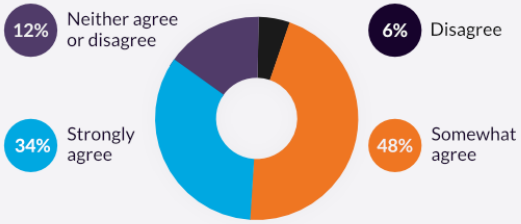
PROCESS INSECURITIES

The IT security processes organizations struggle with the most are ...

1. Application development & testing (SDLC)
2. Attack surface reduction
3. User security awareness/ education

CAUSE FOR CONCERN

Only 34% are confident regarding the ability to monitor privileged users.



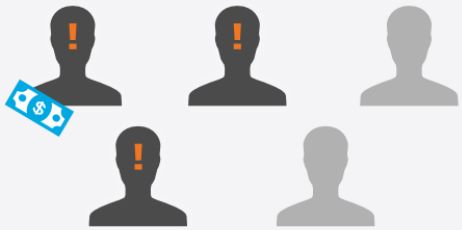
SECURITY'S BIGGEST OBSTACLES

These obstacles inhibit IT from defending cyberthreats...

1. Low security awareness among employees
2. Lack of skilled personnel
3. Too much data to analyze

HELD HOSTAGE BY RANSOMWARE

Three in five respondents indicated their organization was victimized by ransomware last year. One in three victims actually paid the ransom.



APPLICATION & DATA SECURITY DEPLOYMENTS

The most commonly used technologies for protecting applications and data include ...

1. Database Firewall
2. Web application firewall
3. Data encryption/ tokenization

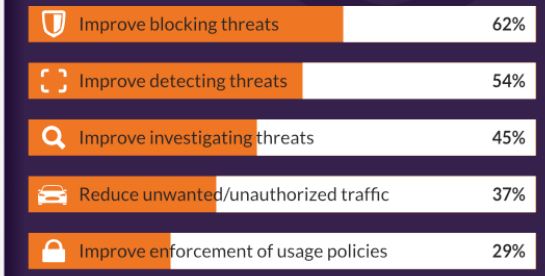
NETWORK SECURITY ACQUISITIONS

The top four network security technologies targeted for acquisition in 2017 are...

1. Honeypots / network deception
2. Next-generation firewall (NGFW)
3. User & entity behavior analytics (UEBA)
4. Threat intelligence service

THREAT INTELLIGENCE BUYING MOTIVATIONS

Organizations integrate third-party threat intelligence for a variety of reasons.



DOWNLOAD THE FULL REPORT AT:
www.imperva.com/go/cdr

CYBEREDGE GROUP

2017 CYBERTHREAT DEFENSE REPORT

CYBEREDGE GROUP

SURVEY DEMOGRAPHICS

15 Countries represented around the world

19 Industries represented

1,100 Qualified IT security decision makers & practitioners

RISING CYBERATTACKS

The percentage of respondents affected by successful attacks has risen the last three years with no end in sight.

SUSCEPTIBLE NATIONS

The percentage of respondents affected by successful attacks in 2016 varied by nation.

China	96%
Mexico	94%
Colombia	87%
South Africa	83%
UK	82%
Turkey	82%
USA	81%
France	79%
Australia	76%
Germany	74%
Canada	74%
Singapore	73%
Saudi Arabia	69%
Japan	66%
Brazil	65%

INCREASING SECURITY BUDGETS

Although three in four IT security budgets are increasing in 2017, the percentage of growing budgets varies by industry.

Retail	83%
Finance	82%
Manufacturing	78%
Health Care	77%
Telecom & Technology	75%
Education	74%
Government	47%

SECURITY'S WEAKEST LINKS

These areas are rated as most difficult to secure...

1. Mobile devices
2. Laptops
3. Desktops

CYBERTHREAT HEADACHES

Cyberthreats causing the greatest concern include...

1. Malware (viruses, worms, Trojans, ransomware)
2. Phishing/ spear-phishing attacks
3. Insider threats/ data exfiltration by employees

HELD HOSTAGE BY RANSOMWARE

Three in five respondents indicated their organization was victimized by ransomware last year. Only one in three victims actually paid the ransom.

SECURITY'S BIGGEST OBSTACLES

These obstacles inhibit IT from defending cyberthreats...

1. Low security awareness among employees
2. Lack of skilled personnel
3. Too much data to analyze

NETWORK SECURITY ACQUISITIONS

The top four network security technologies targeted for acquisition in 2017 are...

1. Honeypots / network deception
2. Next-generation firewall (NGFW)
3. User & entity behavior analytics (UEBA)
4. Threat intelligence service

ENDPOINT SECURITY ACQUISITIONS

The top four endpoint security technologies targeted for acquisition in 2017 include...

1. Containerization/ micro-virtualization
2. Self-remediation for infected endpoints
3. Endpoint deception
4. Digital forensics/ incident resolution

CHALLENGING IT SECURITY FUNCTIONS

The most-challenging internal IT security functions are...

1. Application development & testing (SDLC)
2. Attack surface reduction
3. User security awareness/education

RESEARCH SPONSORS

PLATINUM: CODE42, IMPERVA, SecureWorks, Symantec

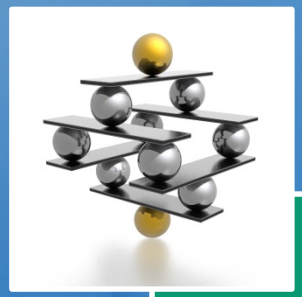
GOLD: bitglass, exabeam, Hewlett Packard Enterprise, WEBROOT Smarter Cybersecurity

SILVER: ENDGAME., foxtechnologies., illusive, Soliton, sumologic

Obstacles to the security

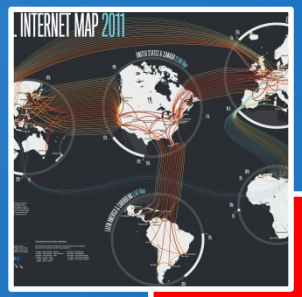
- Security is inconvenient
- Computers are powerful and complex
- Computer users are unsophisticated
- Computers created w/o a thought to security
- Current trend is to share, not protect
- Data accessible from anywhere
- Security is not about HW and SW
- The bad guys are very sophisticated
- Mgmt. sees security as a drain on the bottom line

Two domains of knowledge



Management

- ISMS
- Role and responsibility
- Risk management
- Resources management
  - HR
- Framework, Policy
- Business Continuity Management
- Legal issues



Technics

- Protocol
- Cryptography
- AAA
- IEEE 802.1x
- WPA2
- SSH
- SSL, VPN
- Penetration test
- Network monitoring

ISO 27000 series

- ISO/IEC 27000: Overview and vocabulary
- ISO/IEC 27001: Requirements
- ISO/IEC 27002: Code of practice for ISM
- ISO/IEC 27003: ISMS Implementation guidance
- ISO/IEC 27004: ISM Measurement
- ISO/IEC 27005: Information security risk management
- ISO/IEC 27006: Requirements for bodies providing audit and certification of ISMS
- ISO/IEC 27007: Guidelines for ISMS auditing
- ISO/IEC 27014: Information security governance

ISO 27001 (Information Security Mgmt. System)

Intention

- To harmonize 27001 with other MgmtSysStd
  - ISO/IEC 9000 Quality mgmt. sys.
  - ISO/IEC 14000 Environmental mgmt. sys.

Common model *for*

- Implementing *ISMS*
- Operating *ISMS*
- Monitoring *ISMS operation*
- Improving *ISMS operation*

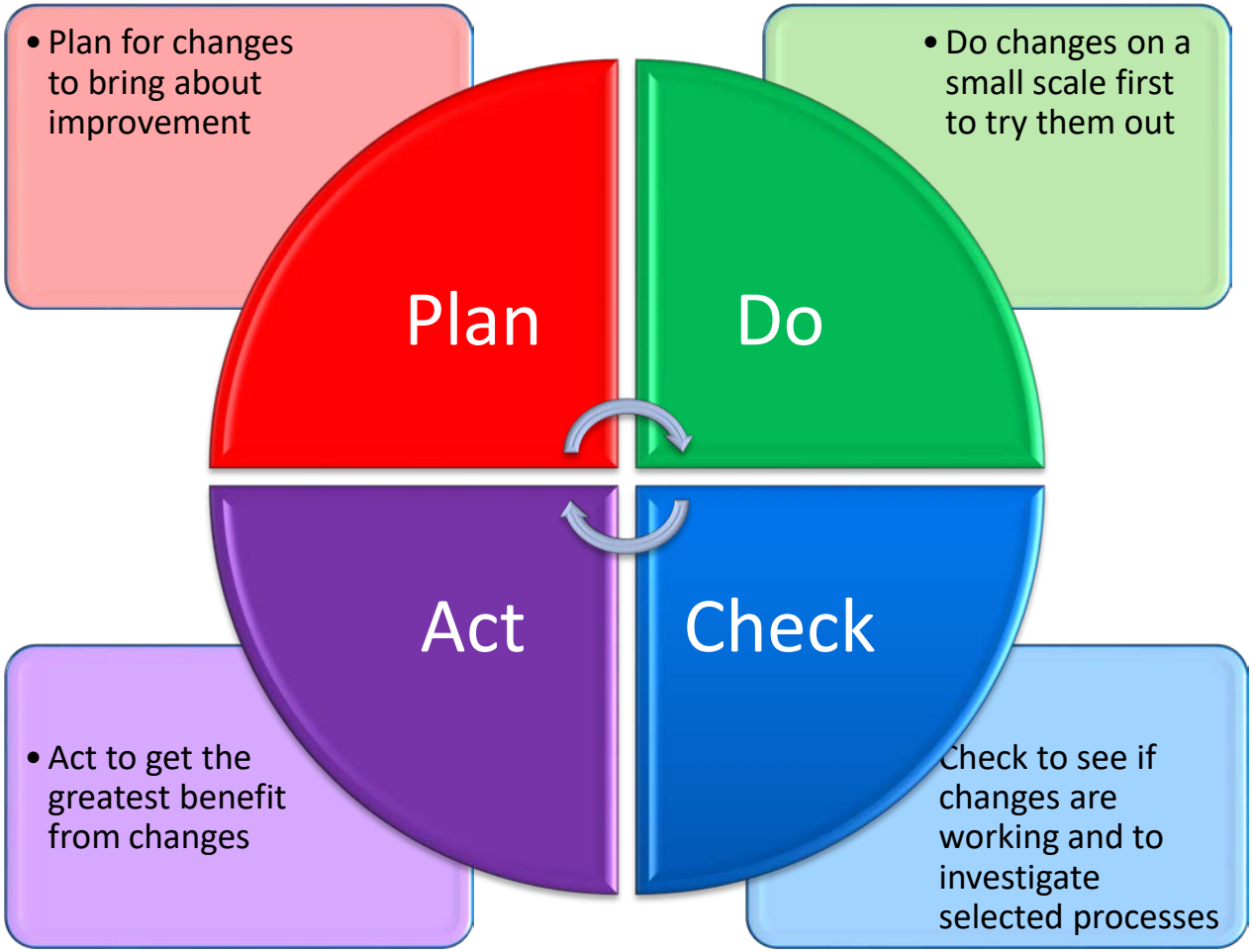
ISO 27002: Code of Practice

- Risk assessment
- Security policy
- Organization of information security
- Asset management
- Human resource security
- Physical and environment security
- Communications and operations mgmt.
- Access control
- Information System acquisition development and maintenance
- Information security incident management
- Business continuity management
- Compliance

Building a secure org.

- Evaluate the risks and threats
- Beware of common misconception
- Provide security training for IT staff
- Think “Outside the box”
- Develop a culture of Security
- Identify and utilize built-in security features of the OS and applications
- Monitor systems
- Hire a third party to audit security
- Don’t forget the basics

PDCA


• Plan for changes to bring about improvement
• Do changes on a small scale first to try them out
Plan
Do
Act
Check
• Act to get the greatest benefit from changes
Check to see if changes are working and to investigate selected processes

Security professionals

Senior management

- **CEO, CRO, CFO, CIO, CISO**

Admin. support and technician

- Champion, team leader, manager
- Security policy developers
- Risk assessment specialists
- Security professionals
- System administrators
- End users

Info. Tech Law

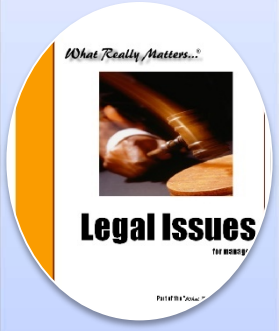
พรบ. ว่าด้วยธุรกรรมทางอิเลคทรอนิกส์ พ.ศ. ๒๕๔๔ และฉบับแก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๕๑

พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

พรฎ. กำหนดประเภทธุรกรรมในทางแพ่งและพาณิชย์ที่ยกเว้นมิให้นำกฎหมายว่าด้วยธุรกรรมทางอิเลคทรอนิกส์มาใช้บังคับ พ.ศ. ๒๕๔๙

พรฎ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเลคทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

พรฎ. ว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเลคทรอนิกส์ พ.ศ. ๒๕๕๑

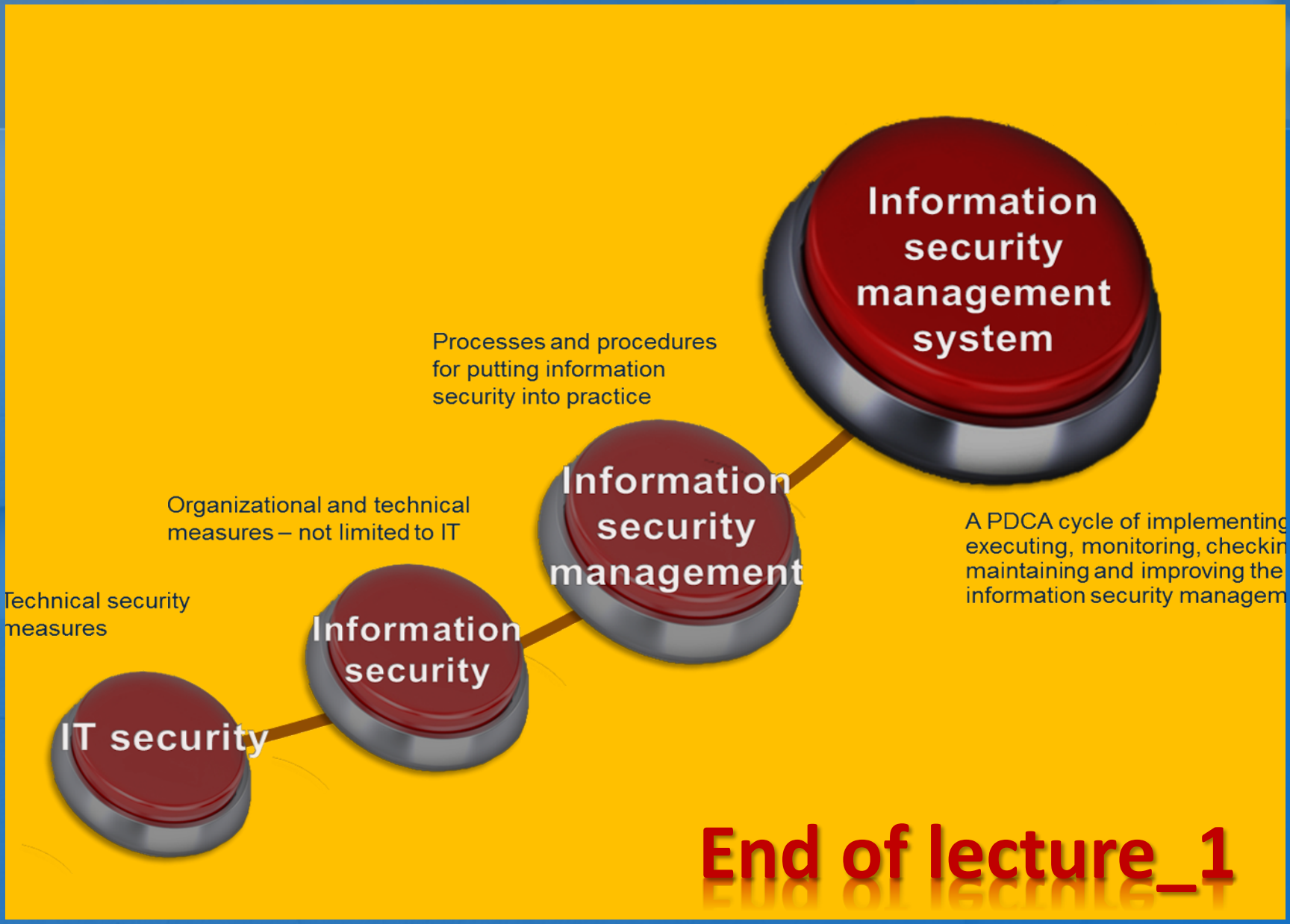


พรฎ. ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเลคทรอนิกส์ พ.ศ. ๒๕๕๓

Community of interest

Group of individuals united by similar interests/values within an organization

- Information security management and professionals
- Information technology management and professionals
- Organizational management and professionals



End of lecture_1