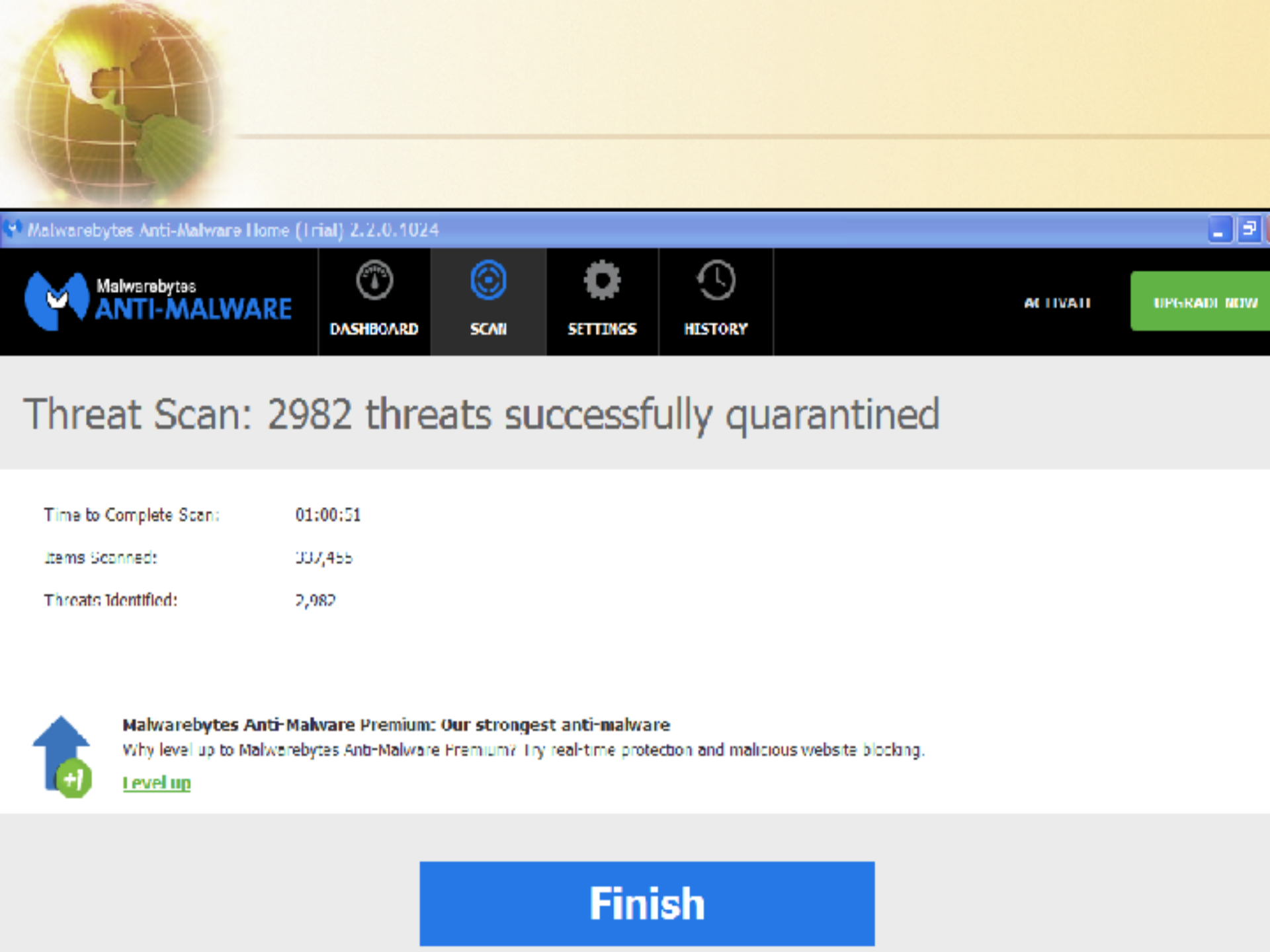
Chapter 3

IT Security and Control

[Laudon] Chap 8

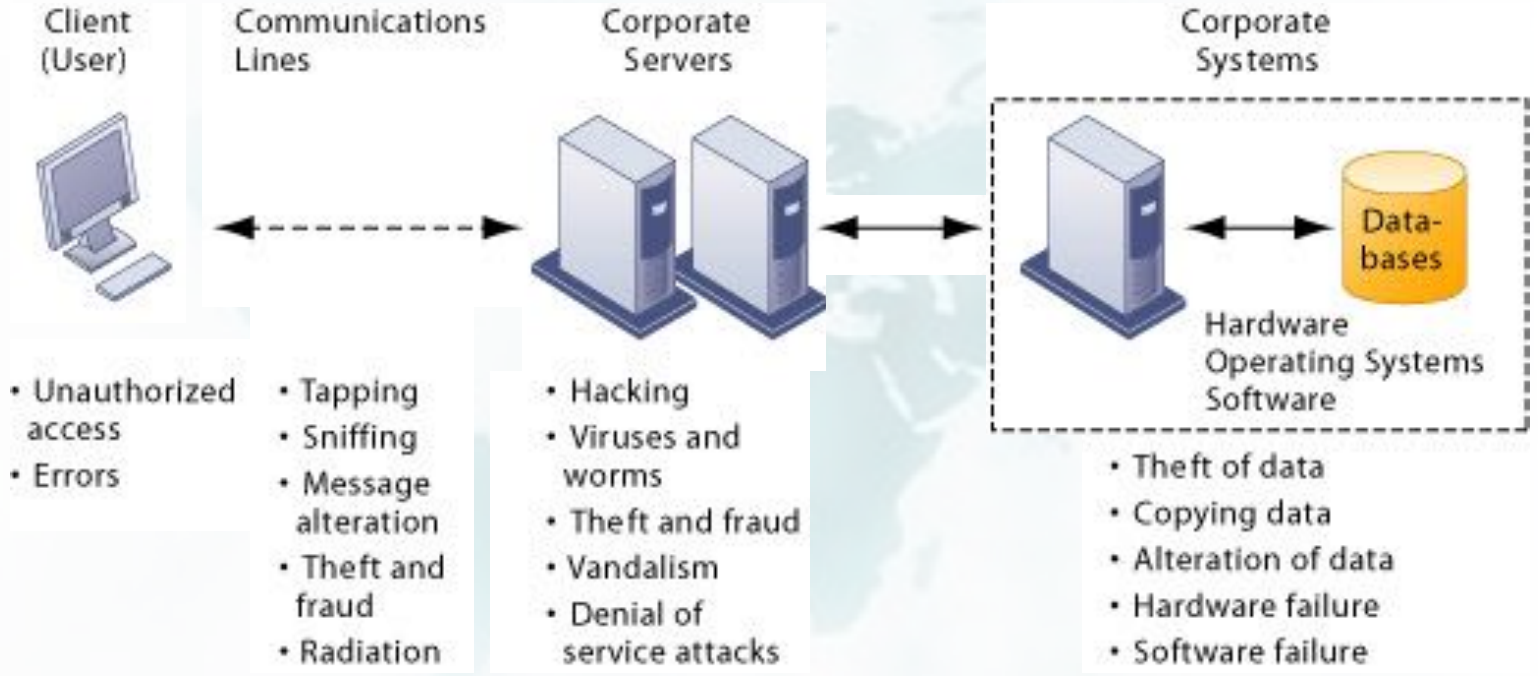
Dr. Yeffry Handoko Putra, M.T
Magister of Information System
Universitas Komputer Indonesia


Malwarebytes Anti-Malware Home (Trial) 2.2.0.1024
Malwarebytes
ANTI-MALWARE
DASHBOARD
SCAN
SETTINGS
HISTORY
ACTIVATE
UPGRADE NOW
Threat Scan: 2982 threats successfully quarantined
Time to Complete Scan:
01:00:51
Items Scanned:
337,455
Threats Identified:
2,982
Malwarebytes Anti-Malware Premium: Our strongest anti-malware
Why level up to Malwarebytes Anti-Malware Premium? Try real-time protection and malicious website blocking.
Level up
Finish

SYSTEM VULNERABILITY AND ABUSE

Why Systems Are Vulnerable

Contemporary Security Challenges and Vulnerabilities



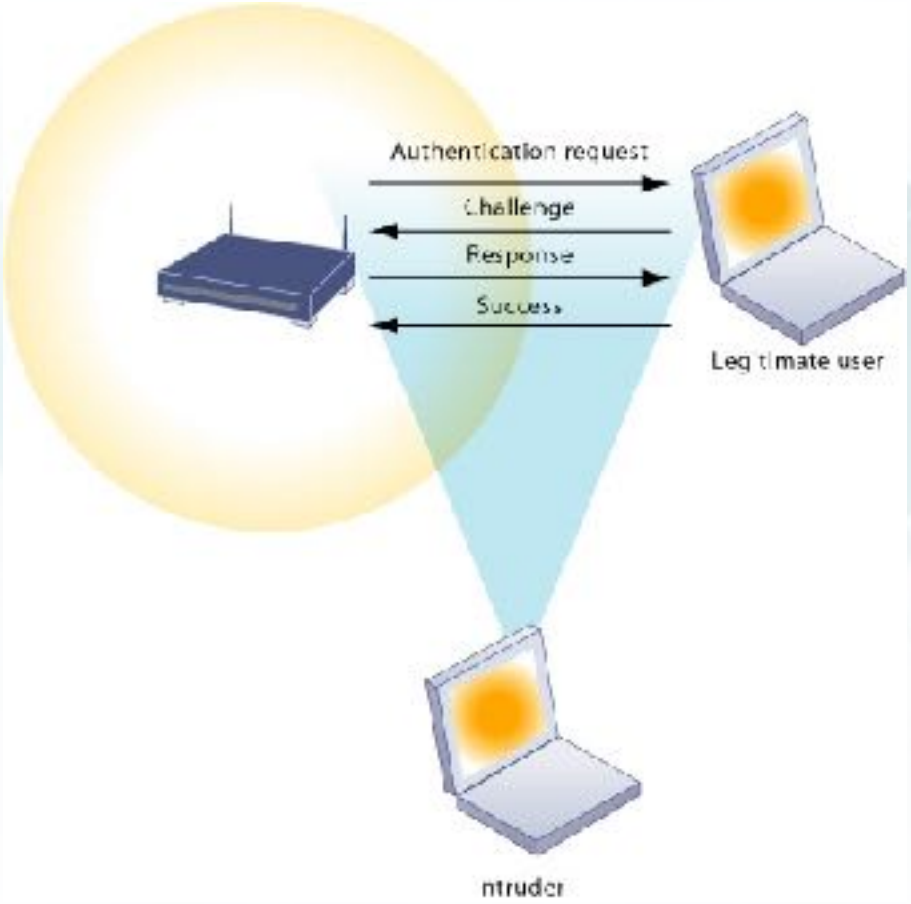
Why Systems Are Vulnerable (Continued)

Internet Vulnerabilities:

- Use of fixed Internet addresses through use of cable modems or DSL
- Lack of encryption with most Voice over IP (VoIP)
- Widespread use of e-mail and instant messaging (IM)

SYSTEM VULNERABILITY AND ABUSE

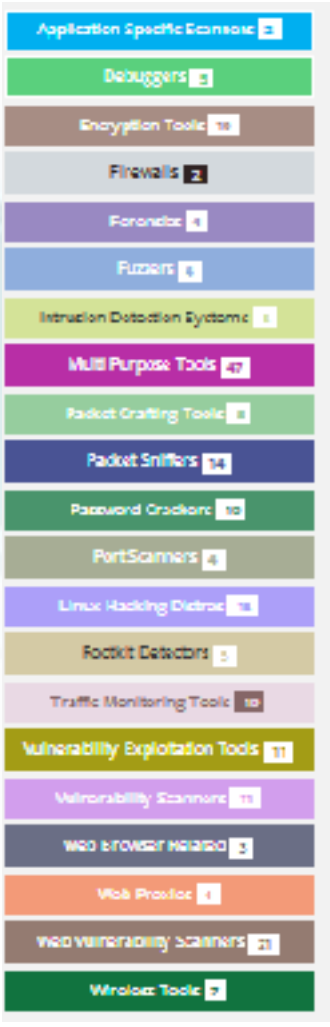
Wi-Fi Security Challenges

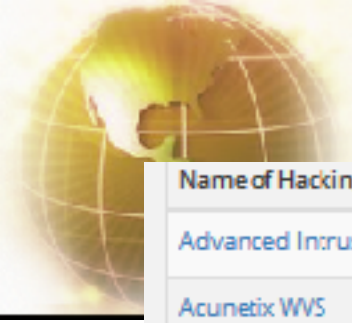


SYSTEM VULNERABILITY AND ABUSE

Malicious Software: Viruses, Worms, Trojan Horses, and Spyware, Hackers and Cybervandalism

- Computer viruses, worms, trojan horses
- Spyware
- Spoofing and Sniffers
- Denial of Service (DoS) Attacks
- Identity theft (e.g. Man in The Middle Attack/ MiTMA)
- Phishing
- Cyberterrorism and Cyberwarfare
- Vulnerabilities from internal threats (employees); software flaws



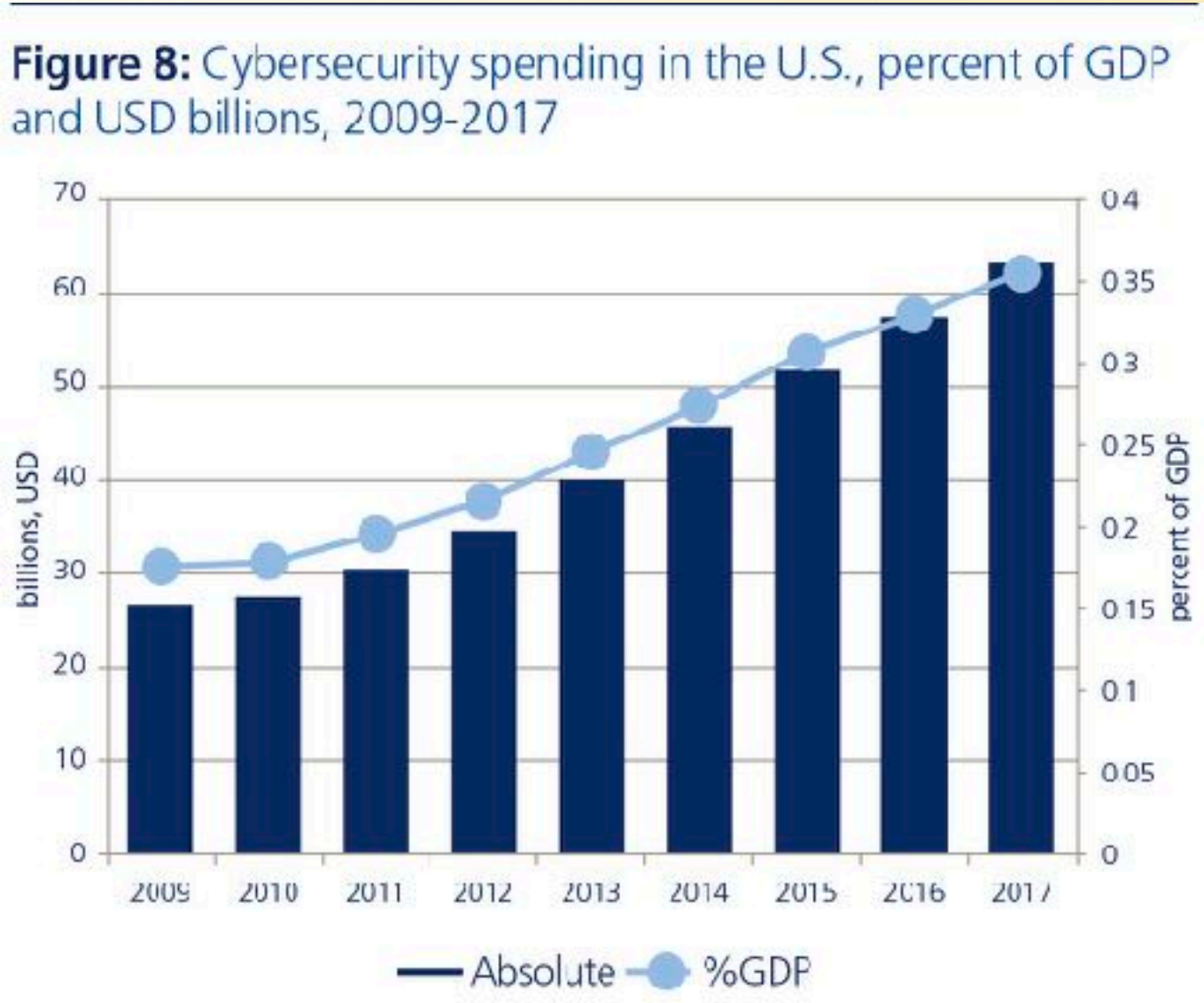


Name of Hacking Tool Name	
Advanced Intrusion Detection Environment	Rootkit Detectors
Acunetix WVS	Web Vulnerability Scanners
Aircrack	Password Crackers
Angry IP Scanner	Port Scanners
AppScan	Web Vulnerability Scanners
ArchAssault	Linux Hacking Distro
Argus	Traffic Monitoring Tools
Autopsy	Forensics
BackBox	Linux Hacking Distro
BeEF	Vulnerability Exploitation Tools
BlackArch Linux	Linux Hacking Distro
Bugtraq	Linux Hacking Distro
Burp Suite	Web Vulnerability Scanners
Cain & Abel	Packet Sniffers
CAINE	Linux Hacking Distro
Core Impact	Vulnerability Exploitation Tools
Core Impact	Vulnerability Scanners
Crowbar	Password Crackers
cURL	General Purpose Tools
DEFT	Linux Hacking Distro
DirBuster	Web Vulnerability Scanners
dradis	Vulnerability Exploitation Tools
dsniff	Packet Sniffers
DumpSec	Rootkit Detectors
EnCase	Forensics
EtherApe	Packet Sniffers
EtherApe	Traffic Monitoring Tools
Ettercap	Packet Sniffers
Ettercap	Traffic Monitoring Tools
Fedora Security Spin	Linux Hacking Distro
Fern WiFi Wireless Cracker	Wireless Tools
Fiddler	Web Proxies
Firebug	Web Vulnerability Scanners
Firebug	Web Browser Related

https://www.concise-courses.com/hacking-tools

Worldwide Damage from Digital Attacks

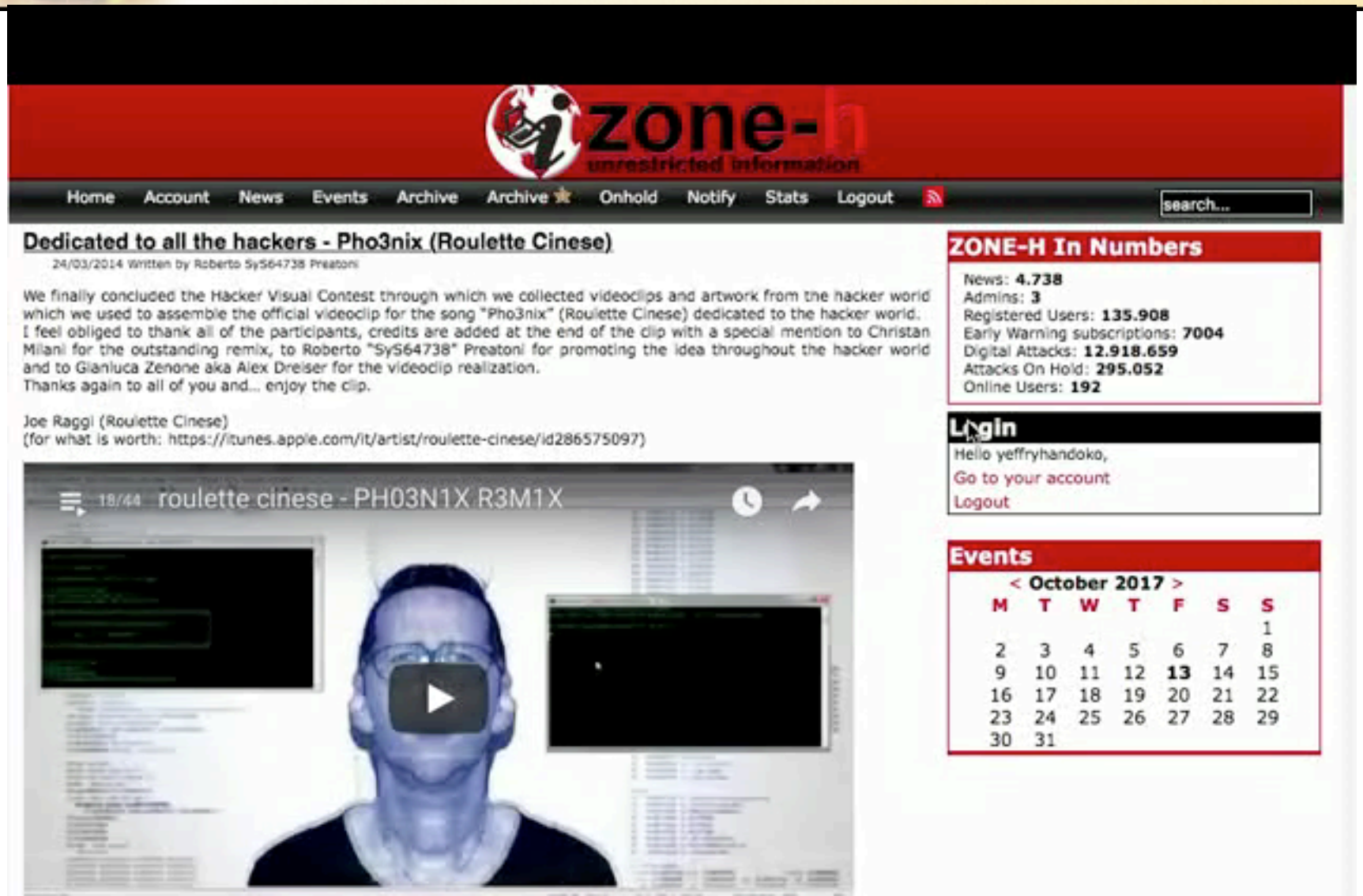
SYSTEM VULNERABILITY AND ABUSE



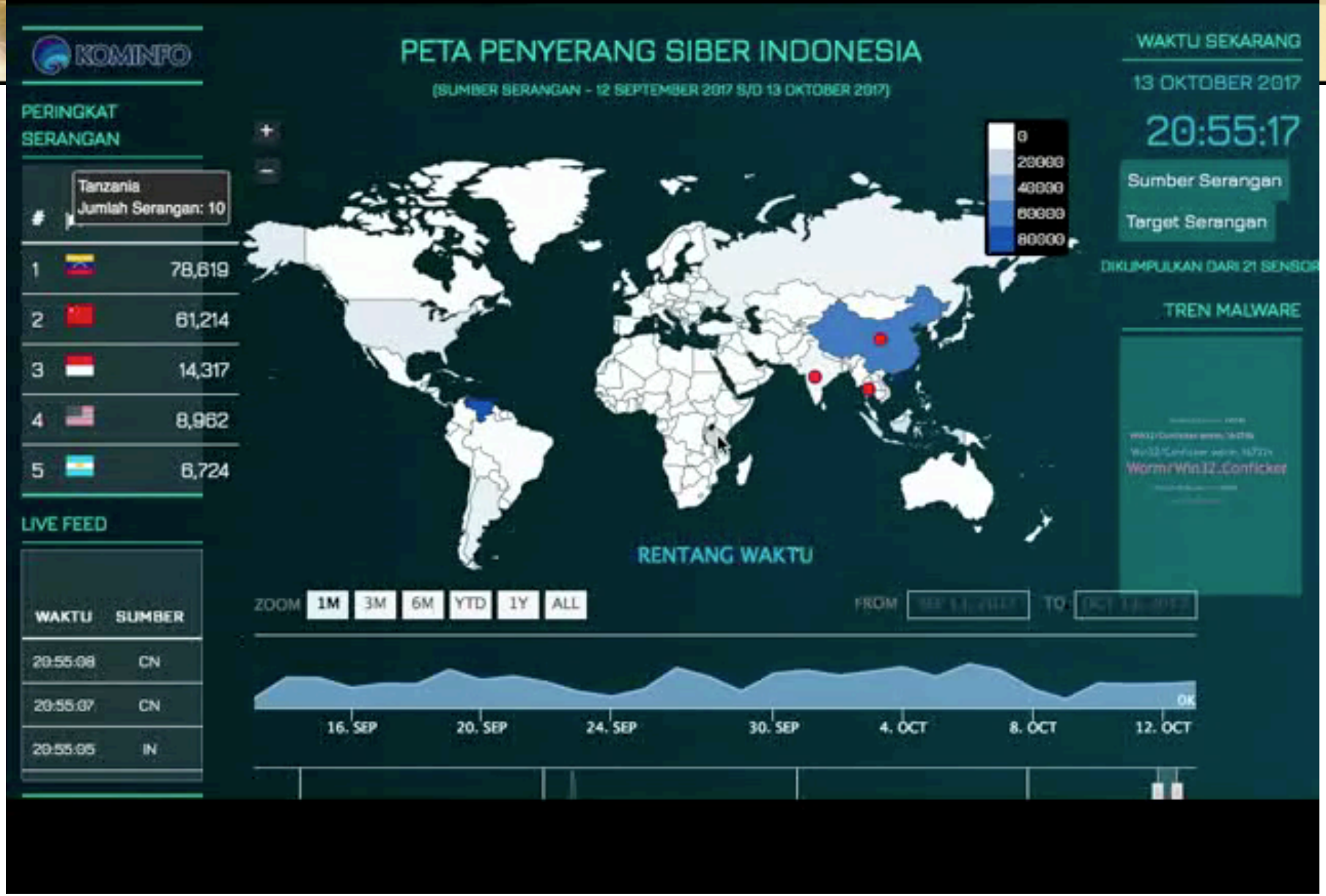
BUSINESS VALUE OF SECURITY AND CONTROL

- Inadequate security and control may create serious legal liability.
- Businesses must protect not only their own information assets but also those of customers, employees, and business partners. Failure to do so can lead to costly litigation for data exposure or theft.
- A sound security and control framework that protects business information assets can thus produce a high return on investment.

BUSINESS VALUE OF SECURITY AND CONTROL



http://public.honeynet.id



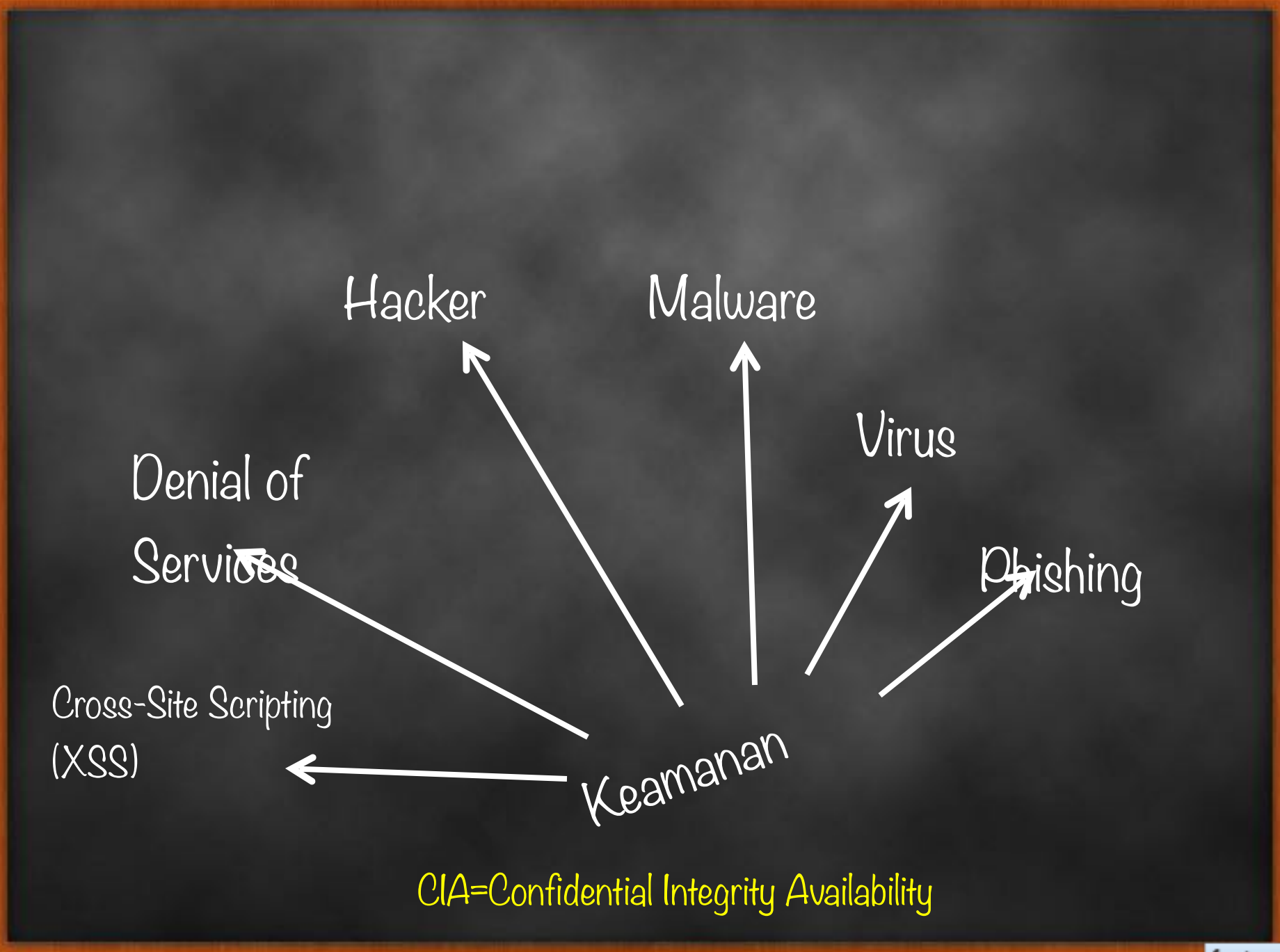
2nd Symposium on Critical Information Infrastructure Protection in Indonesia

Kementerian Kominfo telah mengidentifikasi 8 (delapan) sektor yang tergolong ke dalam sektor strategis nasional, yaitu

1. pemerintahan
2. ketahanan
3. keuangan
4. kesehatan
5. energi dan sumber daya mineral (ESDM)
6. transportasi
7. TIK, serta
8. ketahanan pangan

Penanganan cyber security berskala nasional, yang mencakup 5 (lima) hal:

- **Resilience**, yaitu terselenggaranya infrastruktur informasi yang tetap dapat berjalan melayani publik walaupun terjadi suatu kerusakan atau serangan;
- **Public service**, terbentuknya respon dan langkah penanggulangan pemulihan akibat serangan cyber;
- **Cyber law enforcement**, terbentuknya kerangka kerja dan regulasi yang dapat menciptakan perlindungan yang aman dan kondusif;
- **Cyber culture**, di mana budaya yang dimaksud dalam hal ini adalah kesamaan kerangka berpikir dalam menyikapi keamanan informasi agar terciptanya budaya siber yang mempromosikan keamanan demi penggunaan internet yang sehat dan tepat;
- **Secure market,** terbentuknya profesi dan keahlian keamanan siber yang dapat menciptakan perdagangan elektronik yang aman.


Hacker
Malware
Virus
Denial of Services
Phishing
Cross-Site Scripting (XSS)
Keamanan
CIA=Confidential Integrity Availability

Situs Palsu

Situs Peniru

Phishing

2008 : 55.389 situs phishing hosting di server Indonesia

Sumber: Symantec, Viva.co.id, 2009

21 Desember 2011: ID-CERT mulai mengirimkan feed/berita harian tentang situs pemerintah yang terkena aksi Deface/Phishing.

Situs pemerintah yang diphishing dan di Deface

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM

id.cert

Situs pemerintah yang diphishing dan di Deface

Situs Pemerintah Yang di-Phishing dan di-Deface tahun 2011

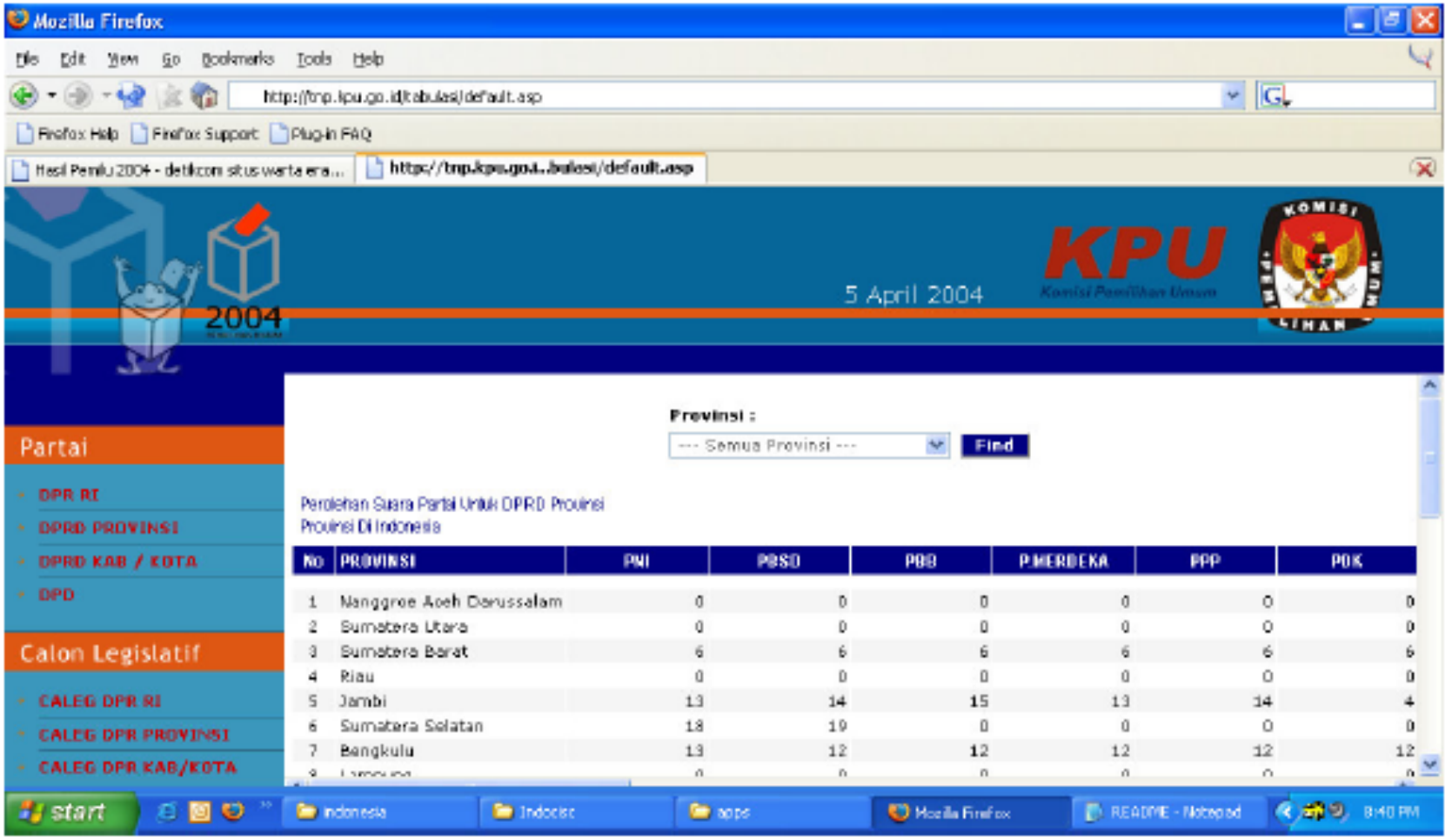
- - http://www.di***s.go.id
- - http://sd*.p*.go.id/
- - http://www.sa***kab.go.id
- - http://www.depk***nfo.go.id
- - http://www.forumbumd***ar.com/bumd/lang/
- - http://www.bapp***-bandung.go.id, terkena Phishing yang disusupi Malware (Trojan) sejak Juni 2011 dan baru tertangani pada 15 September 2011 setelah ID-CERT mendatangi langsung kantor BAP***A BANDUNG.

Situs Palsu Non Finansial: Mafiahukum.org

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM

id.cert

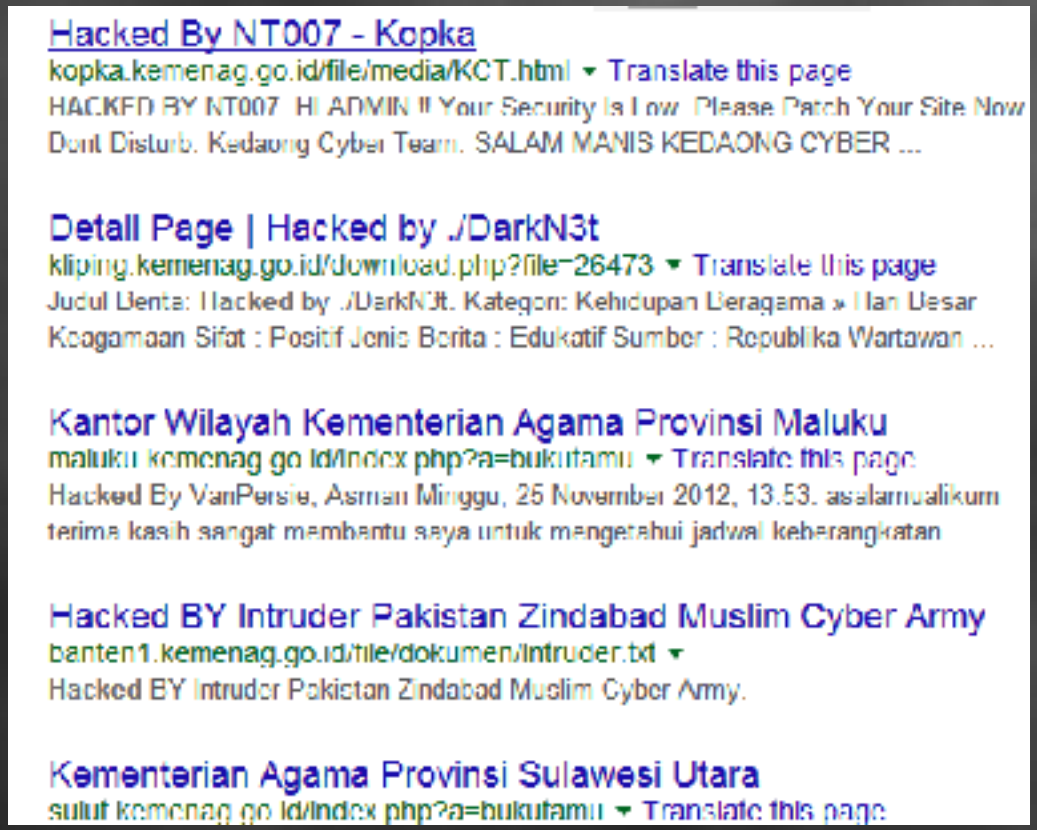
Manipulasi Data



INDONESIA COMPUTER EMERGENCY RESPONSE TEAM

id.cert

Situs Pemerintah yang terkena hack



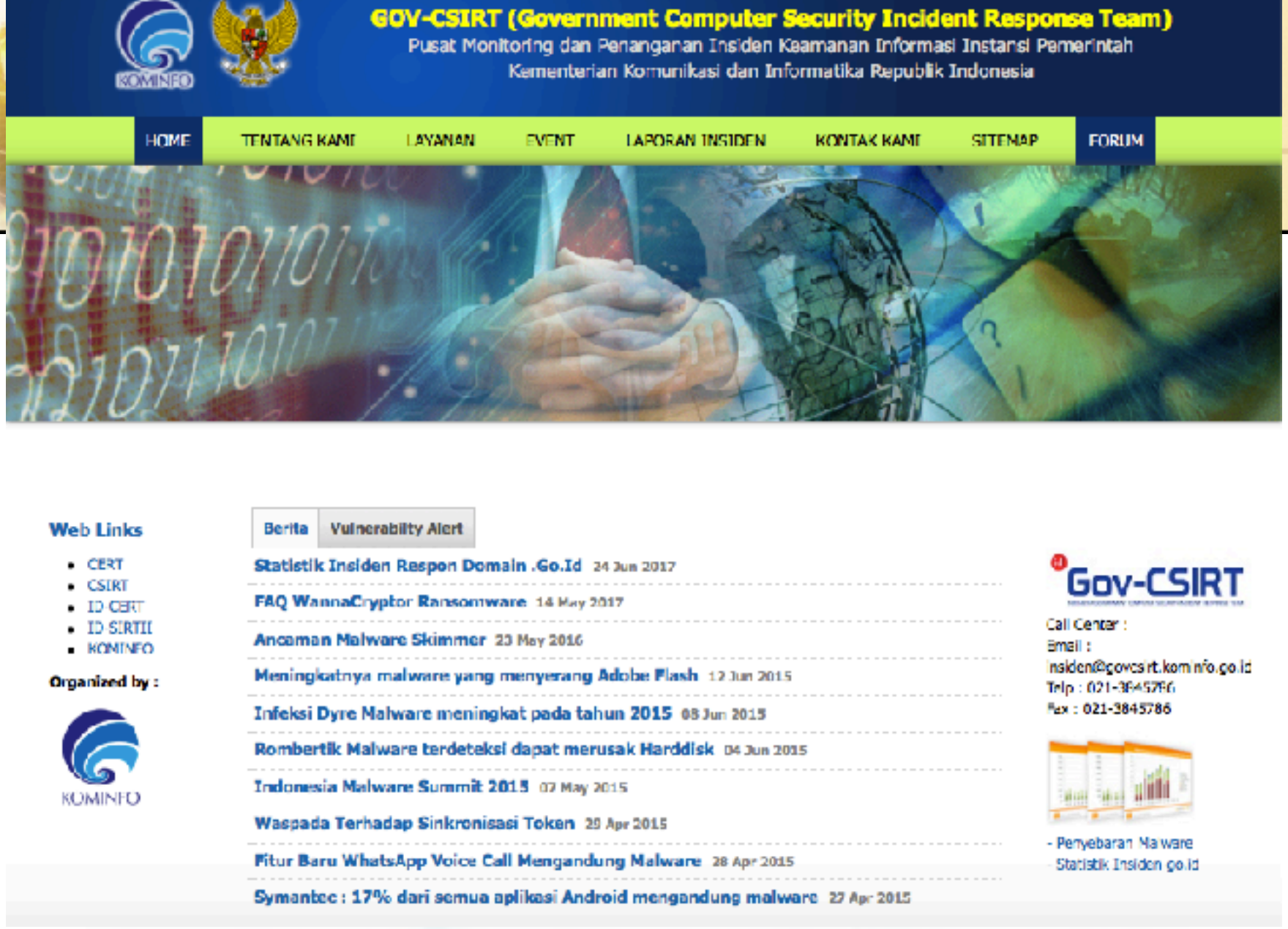
Hacked By NT007 - Kopka
kopka.kemenag.go.id/file/media/KCT.html ▾ Translate this page
HACKED BY NT007 Hi ADMIN !! Your Security Is Low. Please Patch Your Site Now Dont Disturb. Kedaong Cyber Team. SALAM MANIS KEDAONG CYBER ...

Detail Page | Hacked by ./DarkN3t
kliping.kemenag.go.id/download.php?file=26473 ▾ Translate this page
Judul Berita: Hacked by ./DarkN3t. Kategori: Kehidupan Beragama » Hari Besar Keagamaan Sifat : Positif Jenis Berita : Edukatif Sumber : Republika Wartawan ...

Kantor Wilayah Kementerian Agama Provinsi Maluku
maluku.kemenag.go.id/index.php?a=bukutamu ▾ Translate this page
Hacked By VanPersie, Asmat Minggu, 25 November 2012, 13.53. assalamualikum terima kasih sangat membantu saya untuk mengetahui jadwal keberangkatan

Hacked BY Intruder Pakistan Zindabad Muslim Cyber Army
banten1.kemenag.go.id/file/dokumen/intruder.txt ▾
Hacked BY Intruder Pakistan Zindabad Muslim Cyber Army.

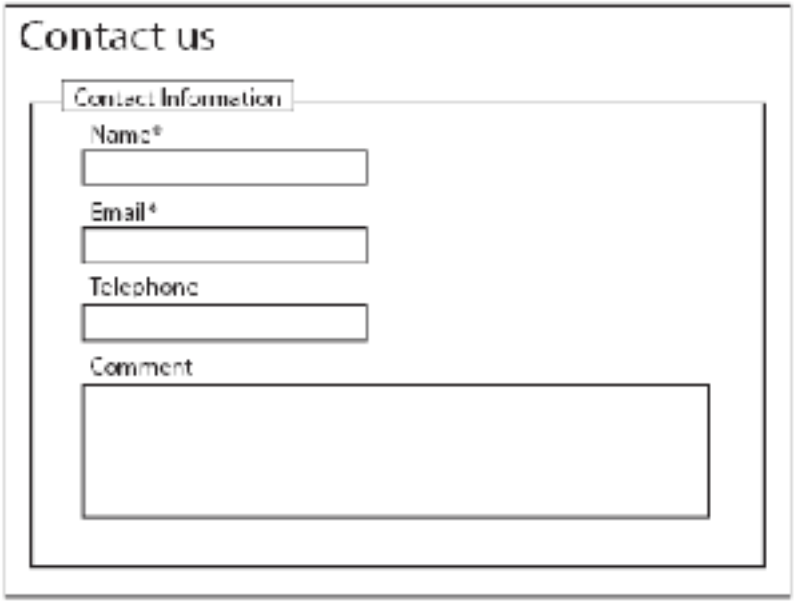
Kementerian Agama Provinsi Sulawesi Utara
sulut.kemenag.go.id/index.php?a=bukutamu ▾ Translate this page



Perlindungan situs e-gov
https://govcsirt.kominfo.go.id

Mengatasi Botnet XSS dengan Captcha

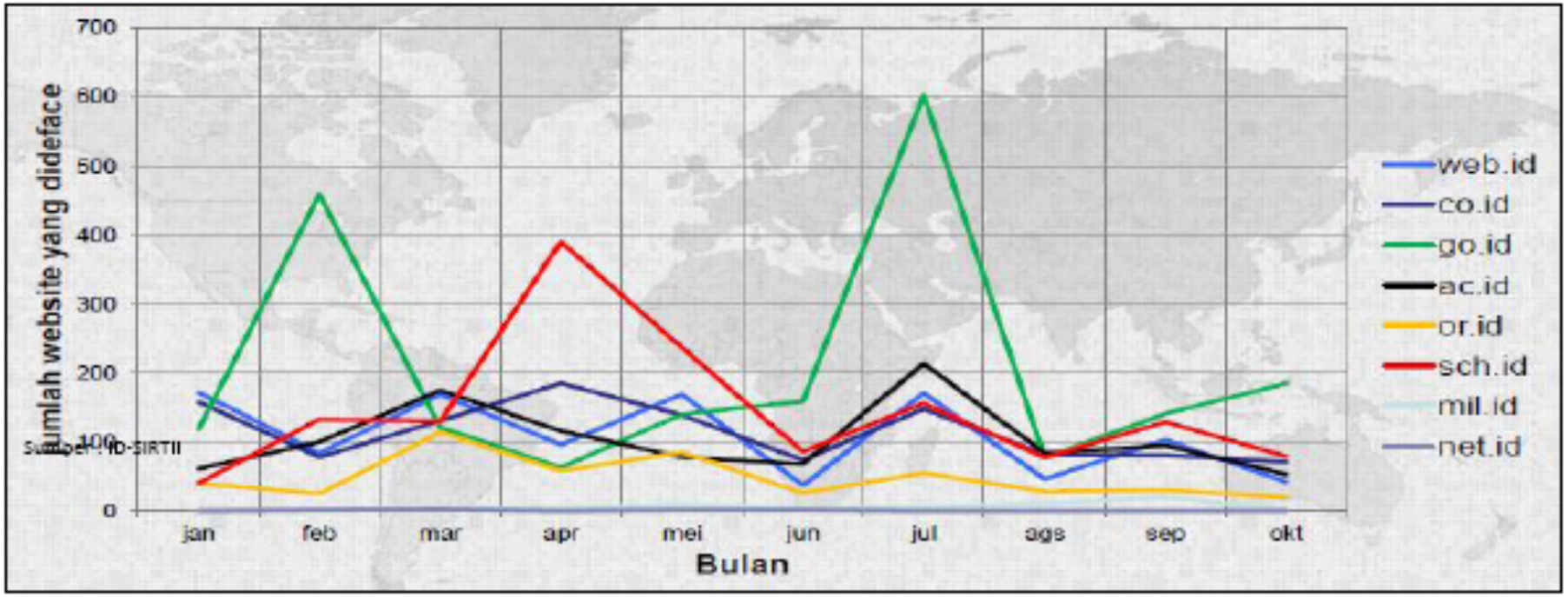
FIGURE 7.4 Using reCAPTCHA for input validation to reduce automated submission



Cross-Site Scri
(XSS)

Botnet = Robot Network

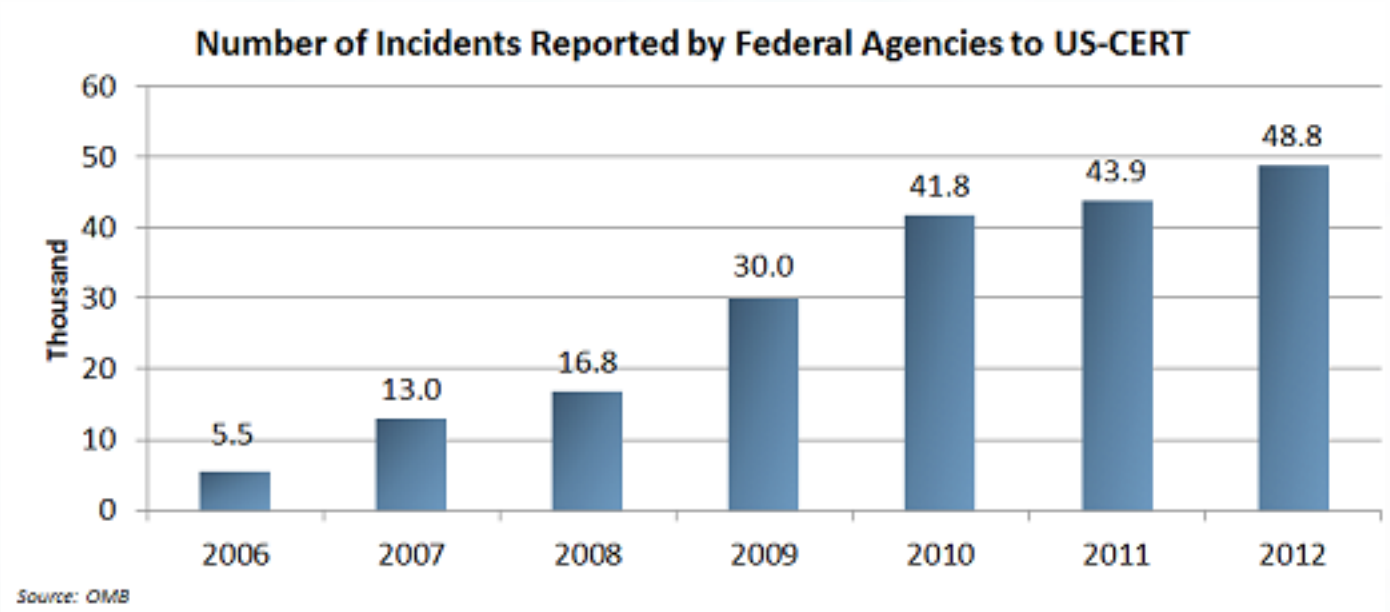
Indonesian Information Security Status



- Internet domain owned by the government is the most frequent attack and uprooted, compared to other sectors.

BUSINESS VALUE OF SECURITY AND CONTROL

Security Incidents Continue to Rise



2016 Cybersecurity Skills Gap

Too Many Threats

$1 BILLION: PERSONALLY IDENTIFIABLE INFORMATION (PII) **RECORDS STOLEN IN 2014**[1]

97% BELIEVE APTs REPRESENT CREDIBLE THREAT TO **NATIONAL SECURITY AND ECONOMIC STABILITY**[2]

MORE THAN 1 IN 4 ORGANIZATIONS HAVE **EXPERIENCED AN APT ATTACK**[3]

$150 MILLION: AVERAGE COST OF A **DATA BREACH BY 2020**[4]

1 IN 2 BELIEVE THE IT DEPARTMENT IS UNAWARE OF ALL OF ORGANIZATION'S **INTERNET OF THINGS (IOT) DEVICES**[5]

74% BELIEVE LIKELIHOOD OF ORGANIZATION BEING **HACKED THROUGH IOT DEVICES IS HIGH OR MEDIUM**[6]

Too Few Professionals

2 MILLION: GLOBAL SHORTAGE OF CYBERSECURITY **PROFESSIONALS BY 2019**[7]

3X **RATE OF CYBERSECURITY JOB GROWTH** VS. IT JOBS OVERALL, 2010-14[8]

84% ORGANIZATIONS BELIEVE HALF OR FEWER OF APPLICANTS FOR **OPEN SECURITY JOBS ARE QUALIFIED**[9]

53% OF ORGANIZATIONS EXPERIENCE DELAYS AS LONG AS **6 MONTHS TO FIND QUALIFIED SECURITY CANDIDATES**[10]

77% OF WOMEN SAID THAT NO HIGH SCHOOL TEACHER OR GUIDANCE COUNSELOR MENTIONED CYBERSECURITY AS CAREER. **FOR MEN, IT IS 67%.**[11]

89% OF U.S. CONSUMERS BELIEVE IT IS IMPORTANT FOR ORGANIZATIONS TO **HAVE CYBERSECURITY-CERTIFIED EMPLOYEES.**[12**]

Cyberattacks are growing, but the talent pool of defenders is not keeping pace.

Although attacks are growing in frequency and sophistication, the availability of sufficiently skilled cybersecurity professionals is falling behind. Cybersecurity Nexus (CSX) is addressing this gap by creating a skilled global cybersecurity workforce. From the Cybersecurity Fundamentals Certificate for university students to CSXP, the first vendor-neutral, performance-based cybersecurity certification, CSX is attracting and enabling cybersecurity professionals at every stage of their careers.

SOURCES: 1. *2015 Cost of Data Breach Study: Global Analysis, IBM and Ponemon Institute, May 2015.* **2.** *ISACA 2015 APT Study, October 2015.* **3.** *ISACA 2015 APT Study.* **4.** *The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation, Juniper Research, May 2015.* **5.** *ISACA 2015 IT Risk/Reward Barometer Member Study, September 2015.* **6.** *ISACA 2015 IT Risk/Reward Barometer Member Study.* **7.** *UK House of Lords Digital Skills Committee.* **8.** *Burning Glass Job Market Intelligence: Cybersecurity Jobs, 2015.* **9.** *State of Cybersecurity: Implications for 2015 ISACA and RSA Conference, April 2015.* **10.** *State of Cybersecurity: Implications for 2015.* **11.** *Securing Our Future: Closing the Cyber Talent Gap, Raytheon and NCSA, October 2015.* **12.** *2015 ISACA Risk/Reward Barometer Consumer Study, September 2015.*

** "Employees" refers to data security professionals at organizations that potentially have access to survey respondents' personal information.

CSX CYBERSECURITY NEXUS

ISACA® Trust in, and value from, information systems

https://cybersecurity.isaca.org January 2016

Data Security and Control Laws:

- The Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act
- Sarbanes-Oxley Act of 2002

Some of IT Audit Regulation in Indonesia

- Undang-undang No. 19 Tahun 2016 perubahan atas UU No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronika
- Permen Kominfo No.4 Tahun 2016 Tentang Sistem Manajemen Pengamanan Sistem Informasi
- Peraturan Pemerintah (PP) No. 82 tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE)

Legal and Regulatory Requirements for Electronic Records Management

1. **Electronic Records Management (ERM):** Policies, procedures and tools for managing the retention, destruction, and storage of electronic records

Electronic Evidence and Computer Forensics

2. **Electronic Evidence:** Computer data stored on disks and drives, e-mail, instant messages, and e-commerce transactions

3. **Computer Forensics:** Scientific collection, examination, authentication, preservation, and analysis of computer data for use as evidence in a court of law

ESTABLISHING A MANAGEMENT FRAMEWORK FOR SECURITY AND CONTROL

Types of Information Systems Controls

1. General controls:

- Software and hardware
- Computer operations
- Data security
- Systems implementation process

ESTABLISHING A MANAGEMENT FRAMEWORK FOR SECURITY AND CONTROL

2. Application controls:

- Input
- Processing
- Output

WHAT TO DO?

- **Risk Assessment**
- **Security Policy**
- **Ensuring Business**
- **Business continuity and disaster recovery planning continuity**

ESTABLISHING A MANAGEMENT FRAMEWORK FOR SECURITY AND CONTROL

Risk Assessment:

- Determines the level of risk to the firm if a specific activity or process is not properly controlled

ESTABLISHING A MANAGEMENT FRAMEWORK FOR SECURITY AND CONTROL

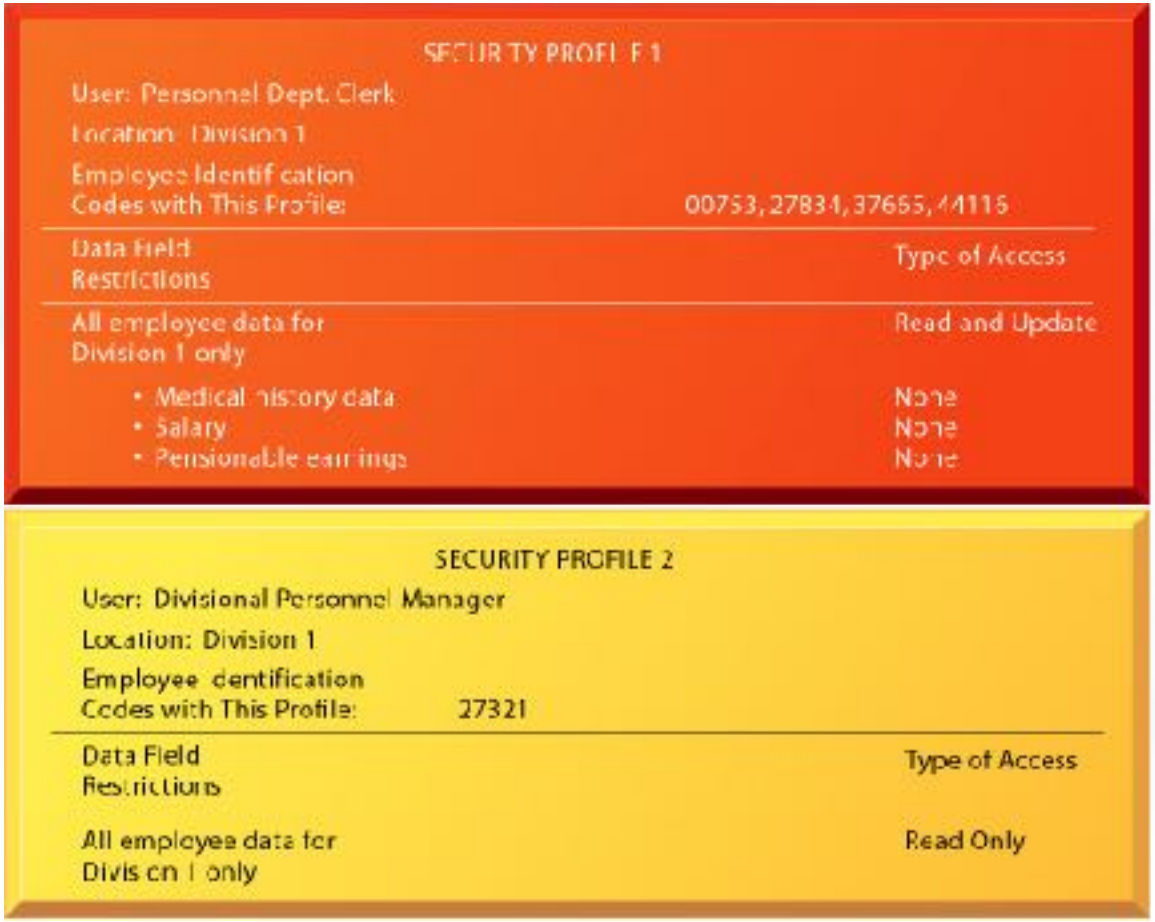
Security Policy:

Policy ranking information risks, identifying acceptable security goals, and identifying the mechanisms for achieving these goals

- **Acceptable Use Policy (AUP)**
- **Authorization policies**

ESTABLISHING A MANAGEMENT FRAMEWORK FOR SECURITY AND CONTROL

Security Profiles for a Personnel System



SECURITY PROFILE 1

User: Personnel Dept. Clerk

Location: Division 1

Employee Identification Codes with This Profile: 00753, 27834, 37665, 44115

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read and Update
• Medical history data	None
• Salary	None
• Pensionable earnings	None

SECURITY PROFILE 2

User: Divisional Personnel Manager

Location: Division 1

Employee identification Codes with This Profile: 27321

Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read Only

ESTABLISHING A MANAGEMENT FRAMEWORK FOR SECURITY AND CONTROL

Ensuring Business Continuity

1. **Downtime:** Period of time in which a system is not operational

2. **Fault-tolerant computer systems:** Redundant hardware, software, and power supply components to provide continuous, uninterrupted service

3. **High-availability computing:** Designing to maximize application and system availability

Ensuring Business Continuity (Continued)

4. **Load balancing:** Distributes access requests across multiple servers

5. **Mirroring:** Backup server that duplicates processes on primary server

6. **Recovery-oriented computing:** Designing computing systems to recover more rapidly from mishaps

Ensuring Business Continuity (Continued)

7. **Disaster recovery planning:** Plans for restoration of computing and communications disrupted by an event such as an earthquake, flood, or terrorist attack

8. **Business continuity planning:** Plans for handling mission-critical functions if systems go down

ESTABLISHING A MANAGEMENT FRAMEWORK FOR SECURITY AND CONTROL

Auditing:

- **MIS audit:** Identifies all of the controls that govern individual information systems and assesses their effectiveness

- **Security audits:** Review technologies, procedures, documentation, training, and personnel

ESTABLISHING A MANAGEMENT FRAMEWORK FOR SECURITY AND CONTROL

Sample Auditor's List of Control Weaknesses

Function: Loans Location: Peoria, IL	Prepared by: J. Ericson Date: June 16, 200/		Received by: T. Benson Review date: June 28, 200/	
Nature of Weakness and Impact	Chance for Error/Abuse		Notification to Management	
	Yes/ No	Justification	Report date	Management response
User accounts with missing passwords	Yes	Leaves system open to unauthorized outsiders or attackers	5/10/07	Eliminate accounts without passwords
Network configured to allow some sharing of system files	Yes	Exposes critical system files to hostile parties connected to the network	5/10/07	Ensure only required directories are shared and that they are protected with strong passwords
Software patches can update production programs without final approval from Standards and Controls group	No	All production programs require management approval; Standards and Controls group assigns such cases to a temporary production status		

Access Control

Access control: Consists of all the policies and procedures a company uses to prevent improper access to systems by unauthorized insiders and outsiders

Authentication:

- Passwords
- Tokens, smart cards
- Biometric authentication

Firewalls, Intrusion Detection Systems, and Antivirus Software

- **Firewalls:** Hardware and software controlling flow of incoming and outgoing network traffic. Firewall Technology: Packet Filtering, Stateful inspection, Network Address Translation, Application Proxy Filtering

- **Intrusion detection systems:** Full-time monitoring tools placed at the most vulnerable points of corporate networks to detect and deter intruders

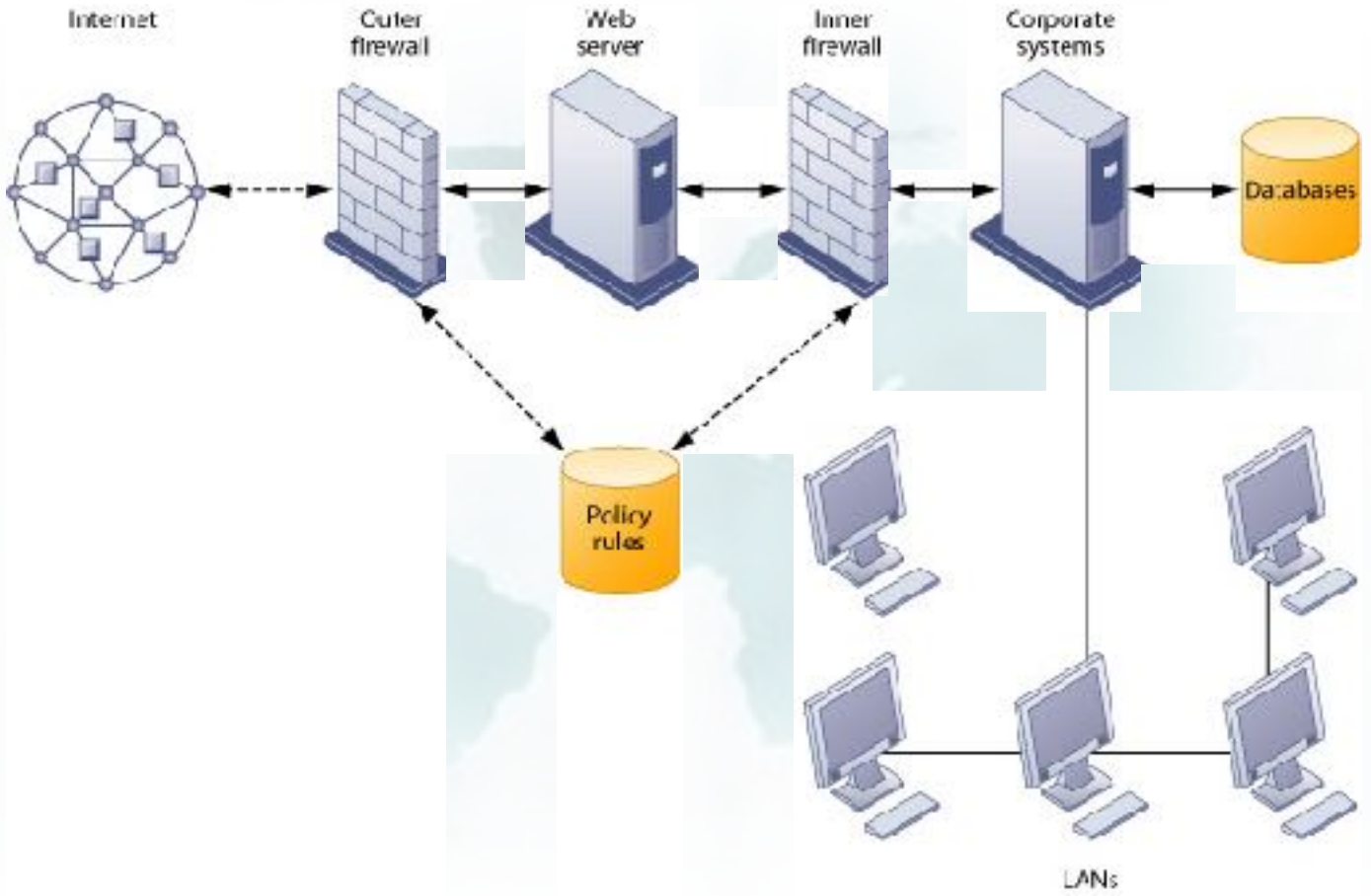
Firewalls, Intrusion Detection Systems, and Antivirus Software (Continued)

- **Antivirus software:** Software that checks computer systems and drives for the presence of computer viruses and can eliminate the virus from the infected area

- Wi-Fi Protected Access specification

TECHNOLOGIES AND TOOLS FOR SECURITY AND CONTROL

A Corporate Firewall



Encryption and Public Key Infrastructure

- **Public key encryption:** Uses two different keys, one private and one public. The keys are mathematically related so that data encrypted with one key can be decrypted using only the other key

- **Message integrity:** The ability to be certain that the message being sent arrives at the proper destination without being copied or changed

Encryption and Public Key Infrastructure (Continued)

- **Digital signature:** A digital code attached to an electronically transmitted message that is used to verify the origin and contents of a message
- **Digital certificates:** Data files used to establish the identity of users and electronic assets for protection of online transactions
- **Public Key Infrastructure (PKI):** Use of public key cryptography working with a certificate authority

TECHNOLOGIES AND TOOLS FOR SECURITY AND CONTROL

Two methods for encrypting network traffic on the Web are:

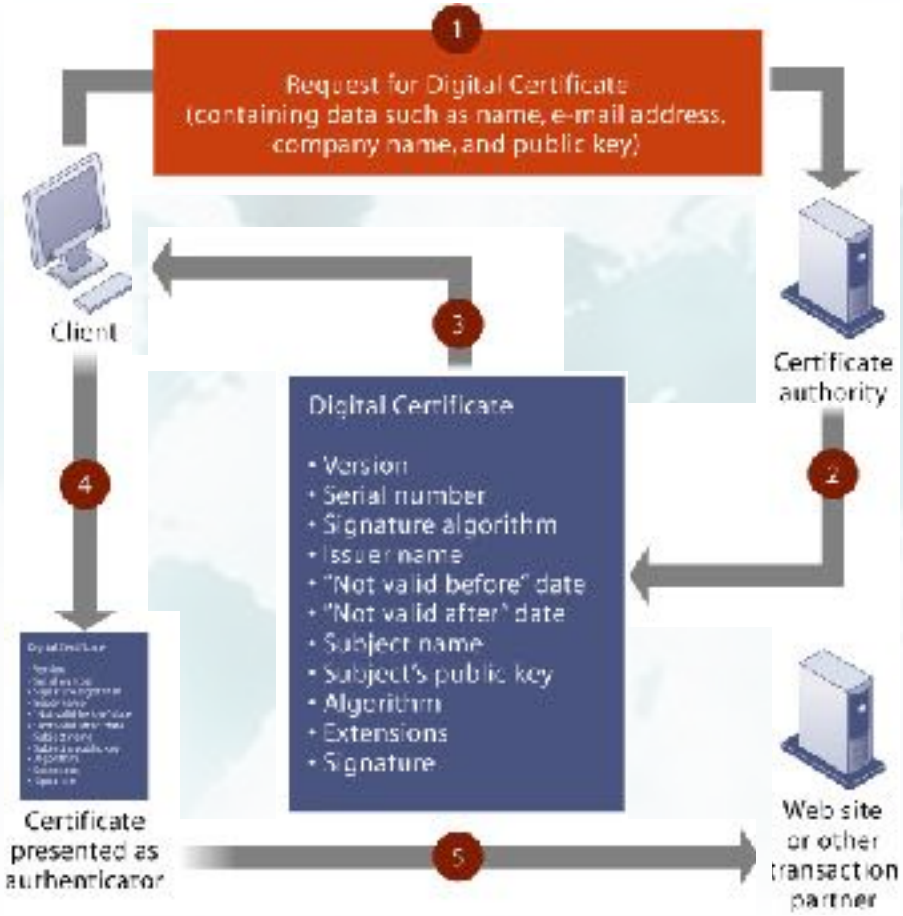
- **Secure Sockets Layer (SSL) and its successor Transport Layer Security (TLS): protocols for secure information transfer over the Internet; enable client and server computer encryption and decryption activities as they communicate during a secure Web session.**
- **Secure Hypertext Transfer Protocol (S-HTTP): used for encrypting data flowing over the Internet; limited to Web documents, whereas SSL and TLS encrypt all data being passed between client and server.**

TECHNOLOGIES AND TOOLS FOR SECURITY AND CONTROL

Public Key Encryption

TECHNOLOGIES AND TOOLS FOR SECURITY AND CONTROL

Digital Certificates



MANAGEMENT OPPORTUNITIES, CHALLENGES AND SOLUTIONS

Management Opportunities:

Creation of secure, reliable Web sites and systems that can support e-commerce and e-business strategies

MANAGEMENT OPPORTUNITIES, CHALLENGES AND SOLUTIONS

Management Challenges:

- Designing systems that are neither overcontrolled nor undercontrolled

- Implementing an effective security policy

Solution Guidelines:

- Security and control must become a more visible and explicit priority and area of information systems investment.
- Support and commitment from top management is required to show that security is indeed a corporate priority and vital to all aspects of the business.
- Security and control should be the responsibility of everyone in the organization.