



Chapter 3

IT Security and Control

[Laudon] Chap 8

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



 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



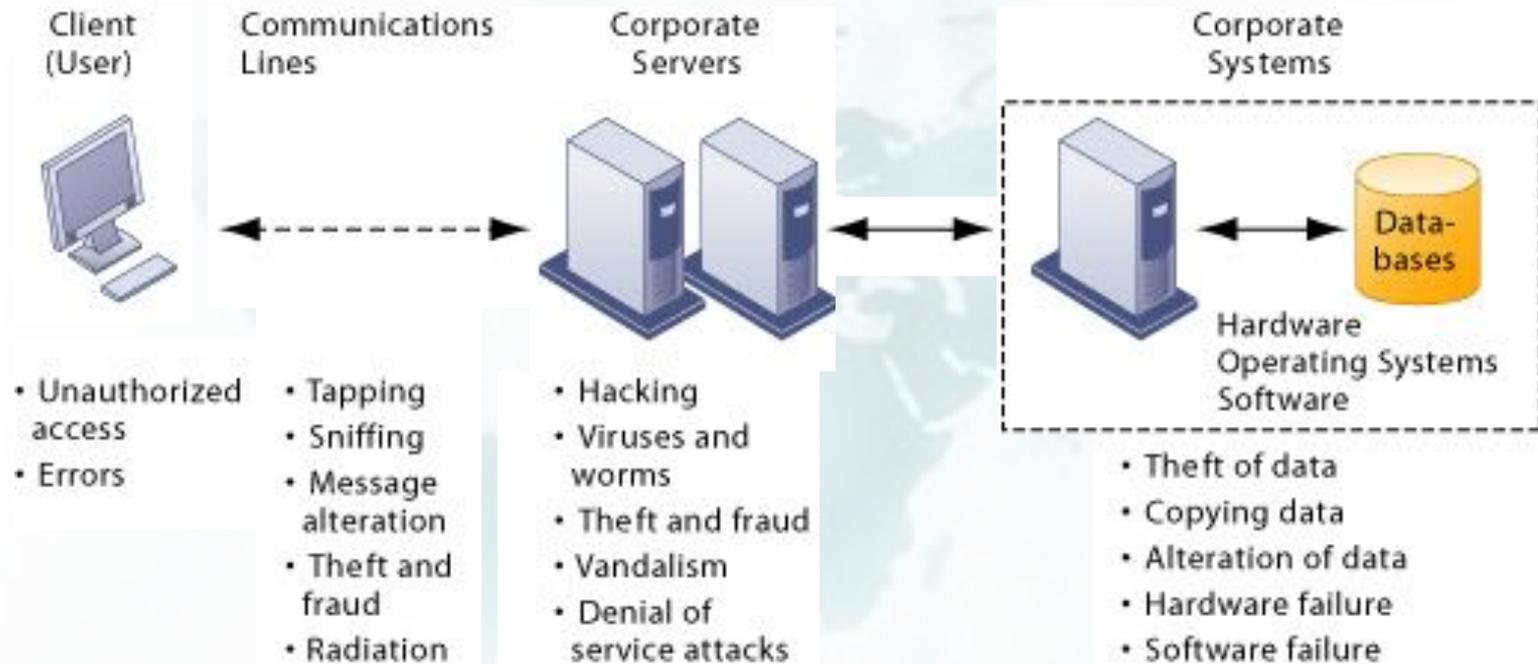
Information System Managements

Chapter 4 Security and Control

SYSTEM VULNERABILITY AND ABUSE

Why Systems Are Vulnerable

Contemporary Security Challenges and Vulnerabilities





Information System Managements

Chapter 4 Security and Control

SYSTEM VULNERABILITY AND ABUSE

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)**

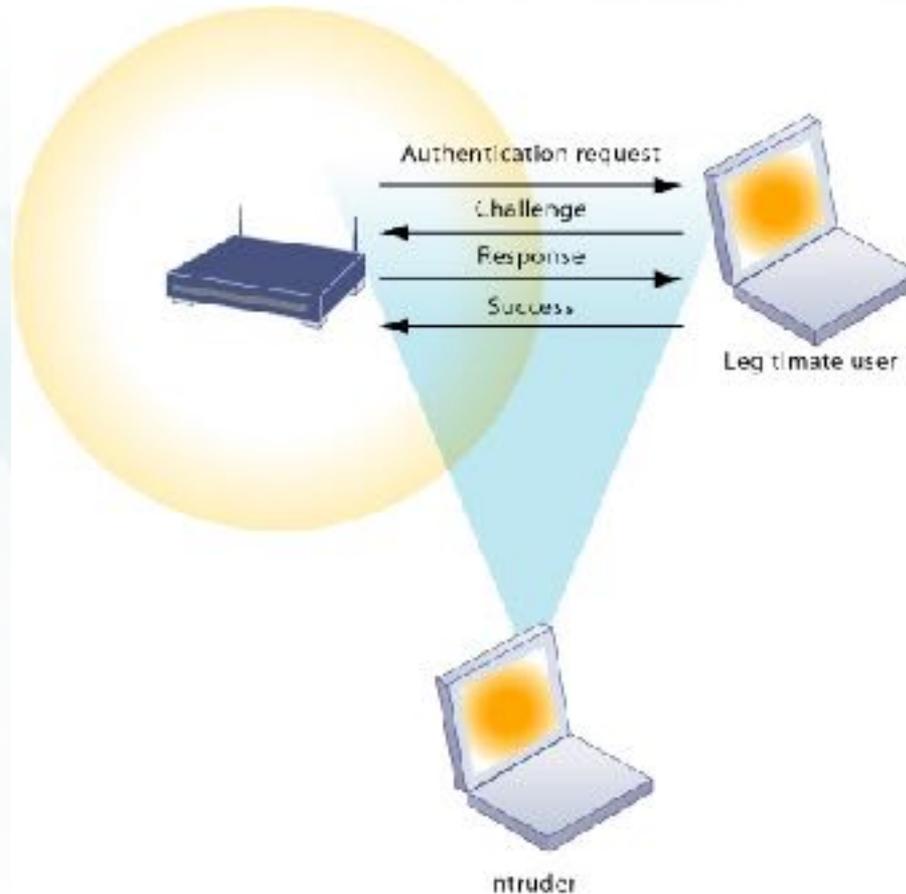


Information System Managements

Chapter 4 Security and Control

SYSTEM VULNERABILITY AND ABUSE

Wi-Fi Security Challenges





Information System Managements

Chapter 4 Security and Control

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

Application Specific Economic	3
Debuggers	3
Encryption Tools	10
Firewalls	2
Forensic	1
Fuzzers	4
Intrusion Detection Systems	1
Multi Purpose Tools	47
Packet Crafting Tools	2
Packet Sniffers	24
Password Crackers	10
PortScanners	4
Linux Hacking Distro	1
Rootkit Detectors	2
Traffic Monitoring Tools	10
Vulnerability Exploitation Tools	11
Vulnerability Scanners	11
Web browser Hijack	2
Web Proxy	1
Web vulnerability scanners	11
Wireless Tools	2



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

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



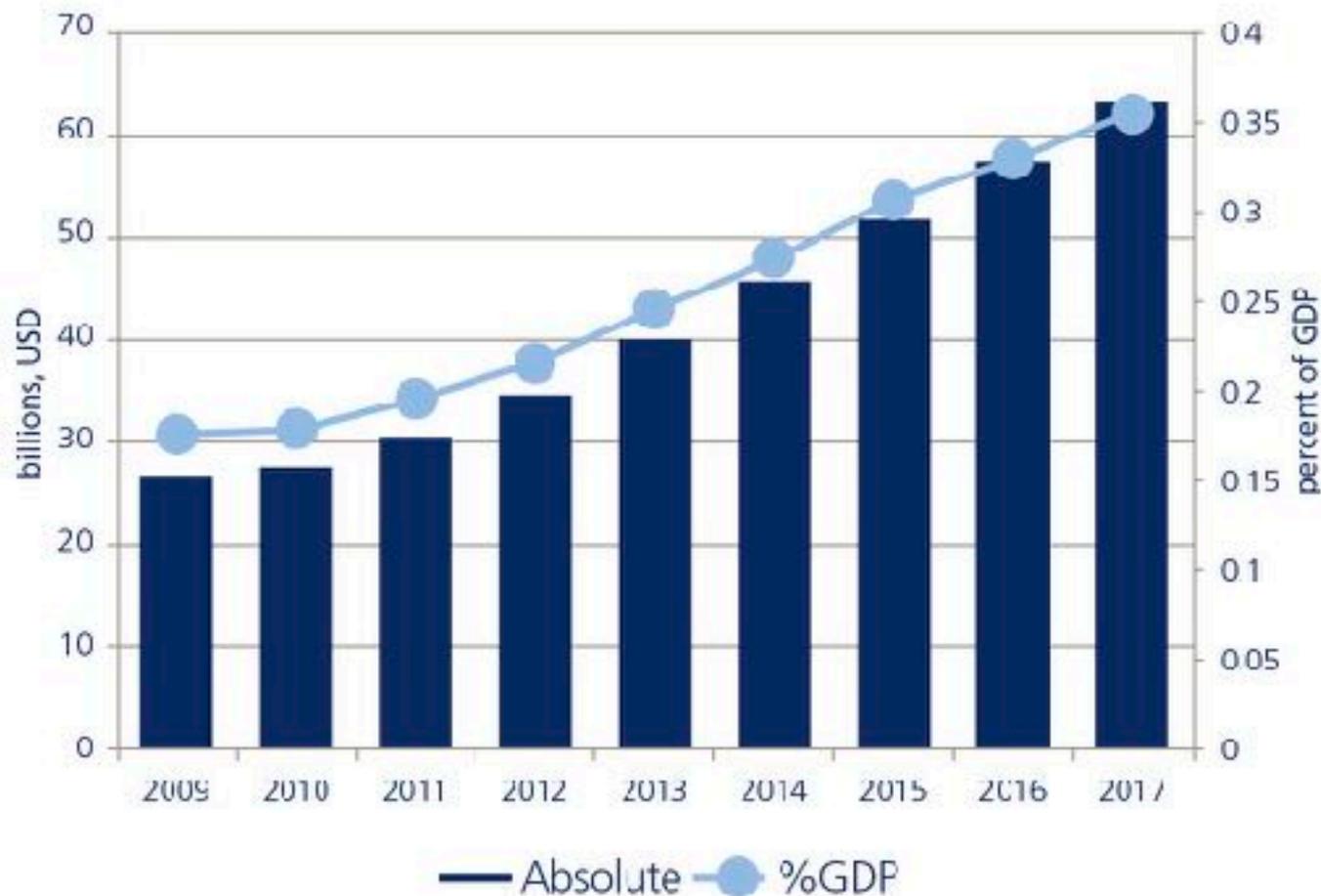
Information System Managements

Chapter 4 Security and Control

Worldwide Damage from Digital Attacks

SYSTEM VULNERABILITY AND ABUSE

Figure 8: Cybersecurity spending in the U.S., percent of GDP and USD billions, 2009-2017





Information System Managements

Chapter 4 Security and Control

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.**



Information System Managements

Chapter 4 Security and Control

BUSINESS VALUE OF SECURITY AND CONTROL

zone-h
unrestricted information

Home Account News Events Archive Archive★ Onhold Notify Stats Logout

Dedicated to all the hackers - Pho3nix (Roulette Cinese)

24/03/2014 Written by Roberto Sy564738 Preatoni

We finally concluded the Hacker Visual Contest through which we collected videoclips and artwork from the hacker world which we used to assemble the official videoclip for the song "Pho3nix" (Roulette Cinese) dedicated to the hacker world. I feel obliged to thank all of the participants, credits are added at the end of the clip with a special mention to Christian Milani for the outstanding remix, to Roberto "Sy564738" Preatoni for promoting the idea throughout the hacker world and to Gianluca Zenone aka Alex Dreiser for the videoclip realization. Thanks again to all of you and... enjoy the clip.

Joe Raggi (Roulette Cinese)
(for what is worth: <https://itunes.apple.com/it/artist/roulette-cinese/id286575097>)

18/44 roulette cinese - PH03N1X R3M1X

ZONE-H In Numbers

News: **4.738**
Admins: **3**
Registered Users: **135.908**
Early Warning subscriptions: **7004**
Digital Attacks: **12.918.659**
Attacks On Hold: **295.052**
Online Users: **192**

Login

Hello jeffryhandoko,
[Go to your account](#)
[Logout](#)

Events

< **October 2017** >

M	T	W	T	F	S	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

<http://public.honeynet.id>



PETA PENYERANG SIBER INDONESIA

(SUMBER SERANGAN - 12 SEPTEMBER 2017 S/D 13 OKTOBER 2017)

WAKTU SEKARANG

13 OKTOBER 2017

20:55:17

Sumber Serangan

Target Serangan

DIKUMPULKAN DARI 21 SENSOR

TREN MALWARE

Worm:Win32.Conficker
Worm:Win32.Conficker
Worm:Win32.Conficker

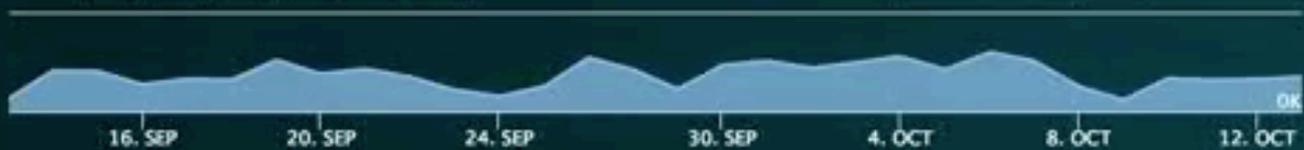
PERINGKAT SERANGAN

#	Tanzania	Jumlah Serangan: 10
1		78,619
2		61,214
3		14,317
4		8,962
5		6,724



RENTANG WAKTU

ZOOM **1M** 3M 6M YTD 1Y ALL FROM TO



LIVE FEED

WAKTU	SUMBER
20:55:08	CN
20:55:07	CN
20:55:05	IN

2nd Symposium on Critical Information Infrastructure Protection in Indonesia

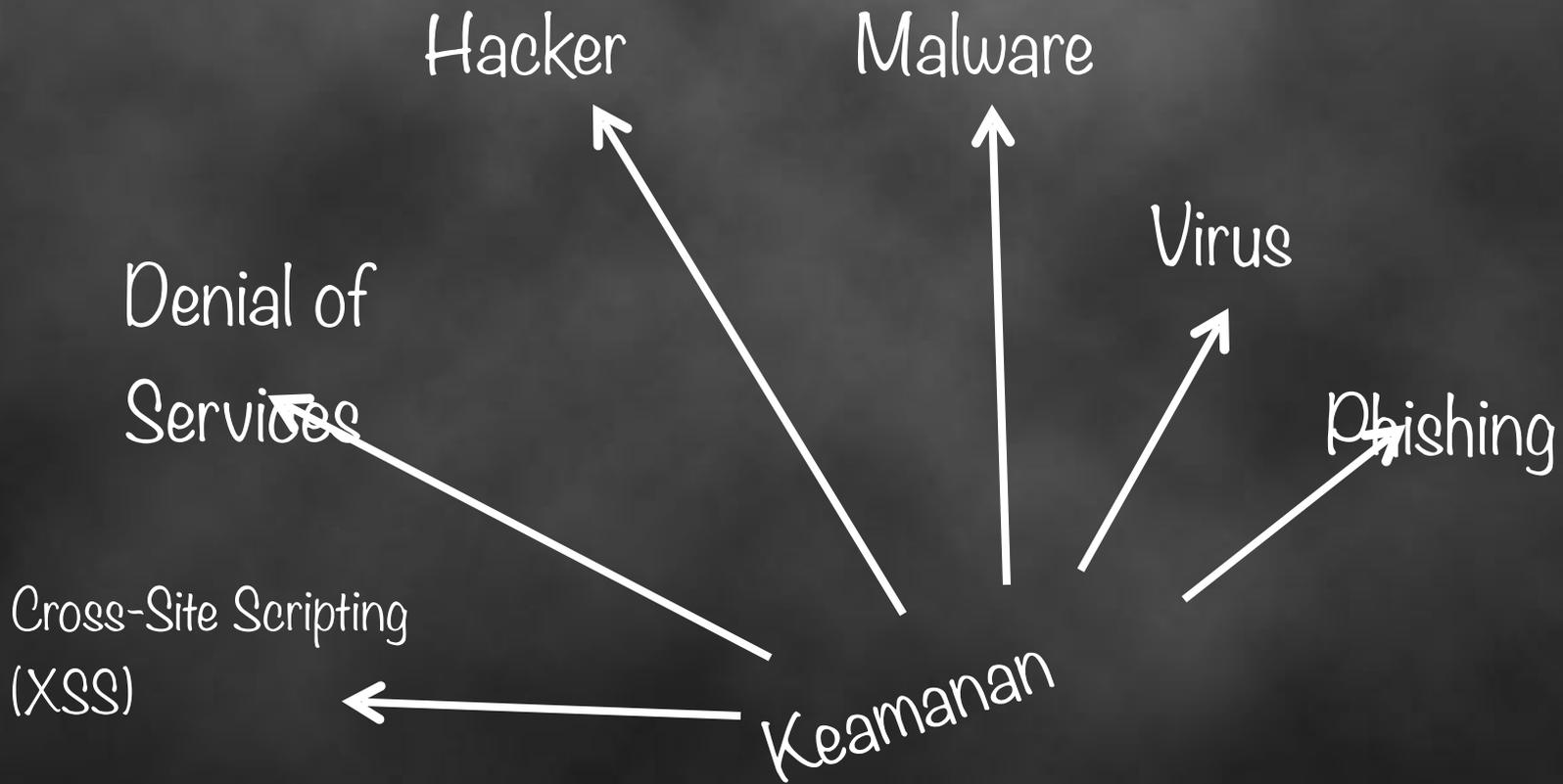


Kementerian Kominfo telah mengidentifikasi 8 (delapan) sektor yang tergolong ke dalam sektor strategis nasional, yaitu

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.

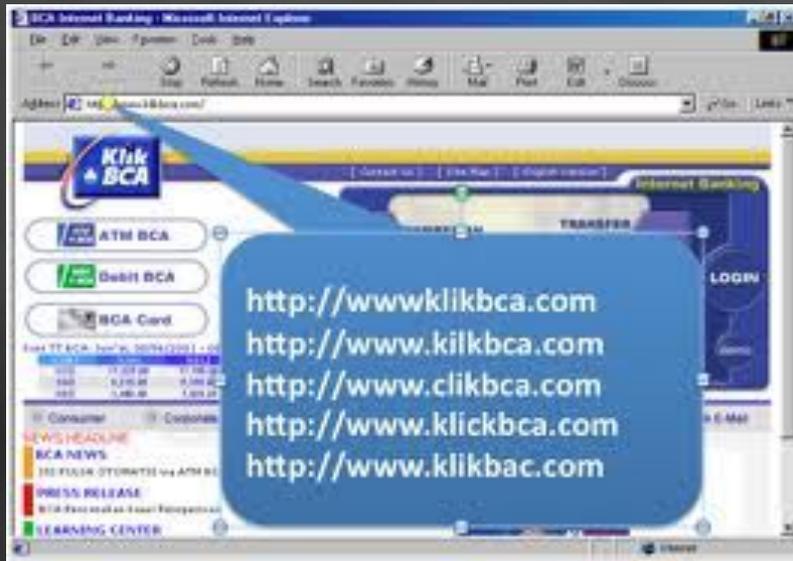


CIA=Confidential Integrity Availability

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



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

The screenshot shows a web browser window displaying the website mafiahukum.com. The page layout includes a main banner with the organization's logo and name, a navigation bar with links for HOME, NEWS, PARTNER, BUNU TAMU, PENGADUAN, and KONTAK KAMI, and a search bar. The main content area is divided into several sections:

- Beranda**: A sidebar with links for Tentang LIAMH, Sejarah LIAMH, Login E-mail, and Partner.
- Interaktif**: A sidebar with links for Contact Us, Guestbook, Album Photo, Statistik Website, and Forum diskusi.
- Jasa Analog**: A sidebar with a link for Jasa Analog.
- News**: A central article titled "MA KABULKAN PERMOHONAN KASASI AAN" with a sub-headline "Majelis Agung (MA) mengabulkan permohonan kasasi Susandi alias Aan terkait kasus tuduhan kepemilikan satu butir bktadi. Aan sebelumnya divonis 4 tahun penjara dan denda Rp 800 juta oleh Pengadilan Tinggi DKI Jakarta." Below the article are three smaller news items: "Kalapas Jangan Jadi Pelindung Mafia Narkoba", "MA Bebaskan Korban Rekayasa Kasus", and "Kuntoro Malu Ranking Penegakan Hukum HJ BURUK".
- Polling**: A poll titled "Bagaimana Menurut anda tentang Website ini?" with options: Bagus, Biasa Saja, and No Comment. Buttons for "PEB" and "Lihat Hasil" are visible.
- Login**: A login form with fields for "Username" and "Password", and a "Login" button.

At the bottom of the page, there is a yellow banner with the text "STRUKTUR LEMBAGA INDEPENDEN ANTI MAFIA HUKUM". Below this, a dark blue banner contains the text "Kasasi narkoba di tempat-tempat ini. Kalapas pun diminta terbuka melapor ke Badan Narkotika Nasional (BNN) jika menemukan peredaran Narkoba, [Baca Selengkapnya](#) M".

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM

id.cert

Manipulasi Data

The screenshot shows a Mozilla Firefox browser window displaying the KPU (Komisi Pemilihan Umum) website. The address bar shows the URL <http://tnp.kpu.go.id/keputusan/default.asp>. The page header includes the KPU logo, the date "5 April 2004", and the text "Komisi Pemilihan Umum".

On the left side, there is a navigation menu with the following items:

- Partai
 - DPR RI
 - DPRD PROVINSI
 - DPRD KAB / KOTA
 - OPD
- Calon Legislatif
 - CALEG DPR RI
 - CALEG DPR PROVINSI
 - CALEG DPR KAB/KOTA

The main content area features a search form for "Provinsi" with a dropdown menu set to "--- Semua Provinsi ---" and a "Find" button. Below the search form is the title "Perolehan Suara Partai Untuk DPRD Provinsi Provinsi Di Indonesia".

No	PROVINSI	PMI	PBSD	PBB	P.MERDEKA	PPP	PKK
1	Nanggroe Aceh Darussalam	0	0	0	0	0	0
2	Sumatera Utara	0	0	0	0	0	0
3	Sumatera Barat	6	6	6	6	6	6
4	Riau	0	0	0	0	0	0
5	Jambi	13	14	15	13	14	4
6	Sumatera Selatan	18	19	0	0	0	0
7	Bengkulu	13	12	12	12	12	12
8	Lampung	0	0	0	0	0	0

The Windows taskbar at the bottom shows the Start button, several open applications (Indonesia, Indocirc, apps), Mozilla Firefox, and the system tray with the time 8:40 PM.

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 Denta: Hacked by ./DarkN3t. Kategori: Kehidupan Beragama > Ilan Uasar
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, Asman Minggu, 25 November 2012, 13.53. asalammualikum
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](#)



GOV-CSIRT (Government Computer Security Incident Response Team)

Pusat Monitoring dan Penanganan Insiden Keamanan Informasi Instansi Pemerintah
Kementerian Komunikasi dan Informatika Republik Indonesia

[HOME](#)[TENTANG KAMI](#)[LAYANAN](#)[EVENT](#)[LAPORAN INSIDEN](#)[KONTAK KAMI](#)[SITEMAP](#)[FORUM](#)

Web Links

- CERT
- CSIRT
- ID CERT
- ID SIRTII
- KOMINFO

Organized by :

[Berita](#)[Vulnerability Alert](#)

[Statistik Insiden Respon Domain .Go.Id](#) 24 Jun 2017

[FAQ WannaCryptor Ransomware](#) 14 May 2017

[Ancaman Malware Skimmer](#) 23 May 2016

[Meningkatnya malware yang menyerang Adobe Flash](#) 12 Jun 2015

[Infeksi Dyrer Malware meningkat pada tahun 2015](#) 08 Jun 2015

[Rombentik Malware terdeteksi dapat merusak Harddisk](#) 04 Jun 2015

[Indonesia Malware Summit 2015](#) 07 May 2015

[Waspada Terhadap Sinkronisasi Token](#) 25 Apr 2015

[Fitur Baru WhatsApp Voice Call Mengandung Malware](#) 28 Apr 2015

[Symantec : 17% dari semua aplikasi Android mengandung malware](#) 27 Apr 2015



Call Center :

Email :

insiden@govcsirt.kominfo.go.id

Telp : 021-3645786

Fax : 021-3645786



- Penyebaran Malware
- Statistik Insiden go.id

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

Contact us

Contact Information

Name*

Email*

Telephone

Comment

Recaptcha

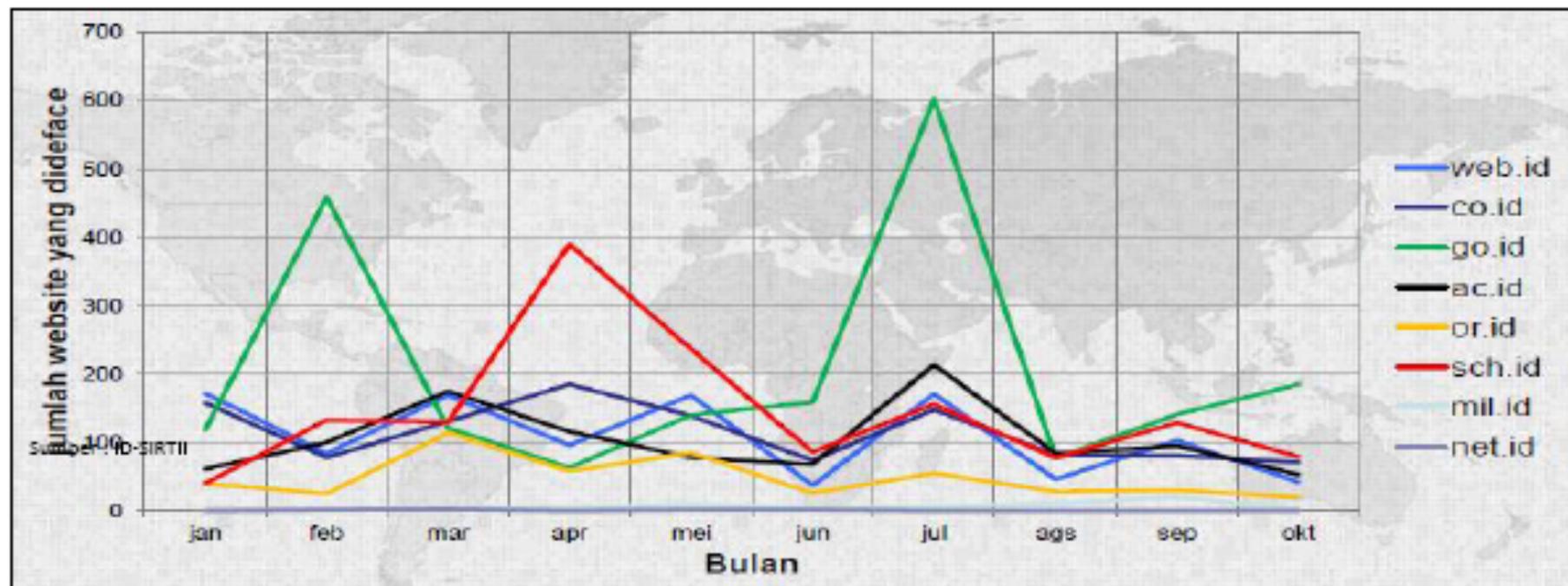
overlooks inquiry ? 10 ?

Enter the words above:

Cross-Site Scripting (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.

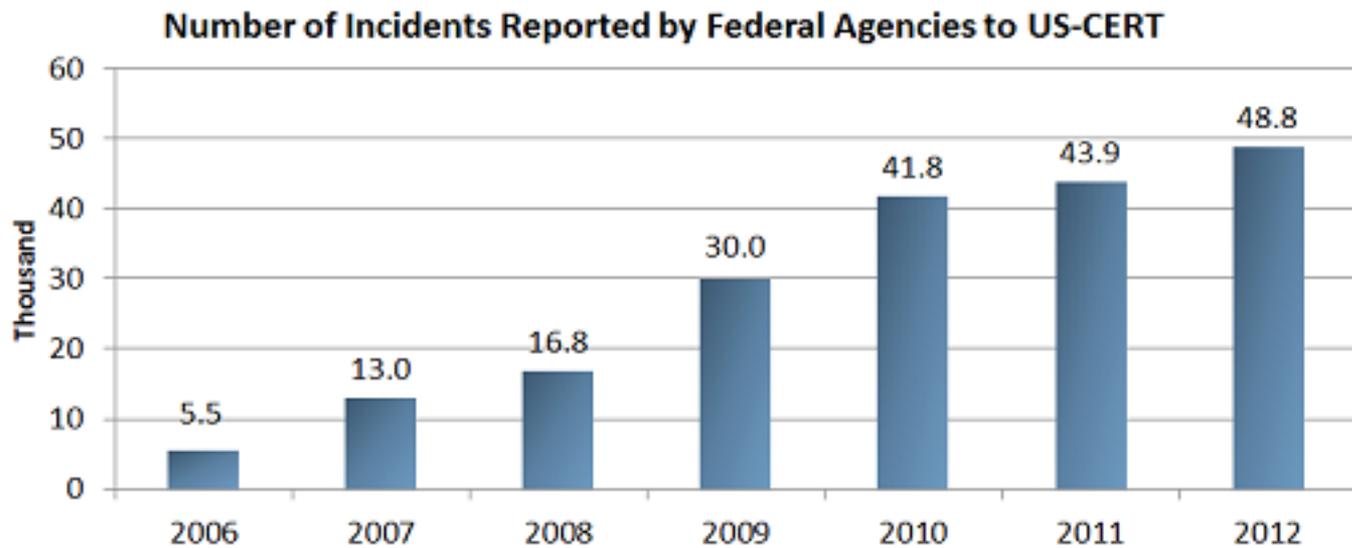


Information System Managements

Chapter 4 Security and Control

BUSINESS VALUE OF SECURITY AND CONTROL

Security Incidents Continue to Rise



Source: OMB

2016 Cybersecurity Skills Gap

Too Many Threats

\$1 BILLION: PERSONALLY IDENTIFIABLE INFORMATION (PII) RECORDS STOLEN IN 2014¹

97% BELIEVE APTs REPRESENT CREDIBLE THREAT TO NATIONAL SECURITY AND ECONOMIC STABILITY²

MORE THAN 1 IN 4 ORGANIZATIONS HAVE EXPERIENCED AN APT ATTACK³

\$150 MILLION: AVERAGE COST OF A DATA BREACH BY 2020⁴

1 IN 2 BELIEVE THE IT DEPARTMENT IS UNAWARE OF ALL OF ORGANIZATION'S INTERNET OF THINGS (IOT) DEVICES⁵

74% BELIEVE LIKELIHOOD OF ORGANIZATION BEING HACKED THROUGH IOT DEVICES IS HIGH OR MEDIUM⁶

Too Few Professionals

2 MILLION: GLOBAL SHORTAGE OF CYBERSECURITY PROFESSIONALS BY 2019⁷

3X RATE OF CYBERSECURITY JOB GROWTH VS. IT JOBS OVERALL, 2010-14⁸

84% ORGANIZATIONS BELIEVE HALF OR FEWER OF APPLICANTS FOR OPEN SECURITY JOBS ARE QUALIFIED⁹

53% OF ORGANIZATIONS EXPERIENCE DELAYS AS LONG AS 6 MONTHS TO FIND QUALIFIED SECURITY CANDIDATES¹⁰

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. SICA 2015 IT Risk/Reward Barometer-Member Study, September 2015. 6. ISACA 2015 IT Risk/Reward Barometer-Member Study. 7. U.S. HOUSE OF REPRESENTATIVES COMMITTEE. 8. Burning Glass Job Market Intelligence: Cybersecurity Jobs, 2010-14. 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.





Information System Managements

Chapter 4 Security and Control

BUSINESS VALUE OF SECURITY AND CONTROL

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 Elektronik
- 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)



Information System Managements

Chapter 4 Security and Control

BUSINESS VALUE OF SECURITY AND CONTROL

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



Information System Managements

Chapter 4 Security and Control

BUSINESS VALUE OF SECURITY AND CONTROL

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



Information System Managements

Chapter 4 Security and Control

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**



Information System Managements

Chapter 4 Security and Control

ESTABLISHING A MANAGEMENT FRAMEWORK FOR SECURITY AND CONTROL

2. Application controls:

- **Input**
- **Processing**
- **Output**





Information System Managements

Chapter 4 Security and Control

WHAT TO DO?

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



Information System Managements

Chapter 4 Security and Control

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**



Information System Managements

Chapter 4 Security and Control

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**



Information System Managements

Chapter 4 Security and Control

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, 37655, 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



Information System Managements

Chapter 4 Security and Control

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



Information System Managements

Chapter 4 Security and Control

ESTABLISHING A MANAGEMENT FRAMEWORK FOR SECURITY AND CONTROL

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



Information System Managements

Chapter 4 Security and Control

ESTABLISHING A MANAGEMENT FRAMEWORK FOR SECURITY AND CONTROL

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



Information System Managements

Chapter 4 Security and Control

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



Information System Managements

Chapter 4 Security and Control

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, 2007		Received by: T. Benson Review date: June 28, 2007	
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			



Information System Managements

Chapter 4 Security and Control

TECHNOLOGIES AND TOOLS FOR SECURITY AND CONTROL

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



Information System Managements

Chapter 4 Security and Control

TECHNOLOGIES AND TOOLS FOR SECURITY AND CONTROL

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



Information System Managements

Chapter 4 Security and Control

TECHNOLOGIES AND TOOLS FOR SECURITY AND CONTROL

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**

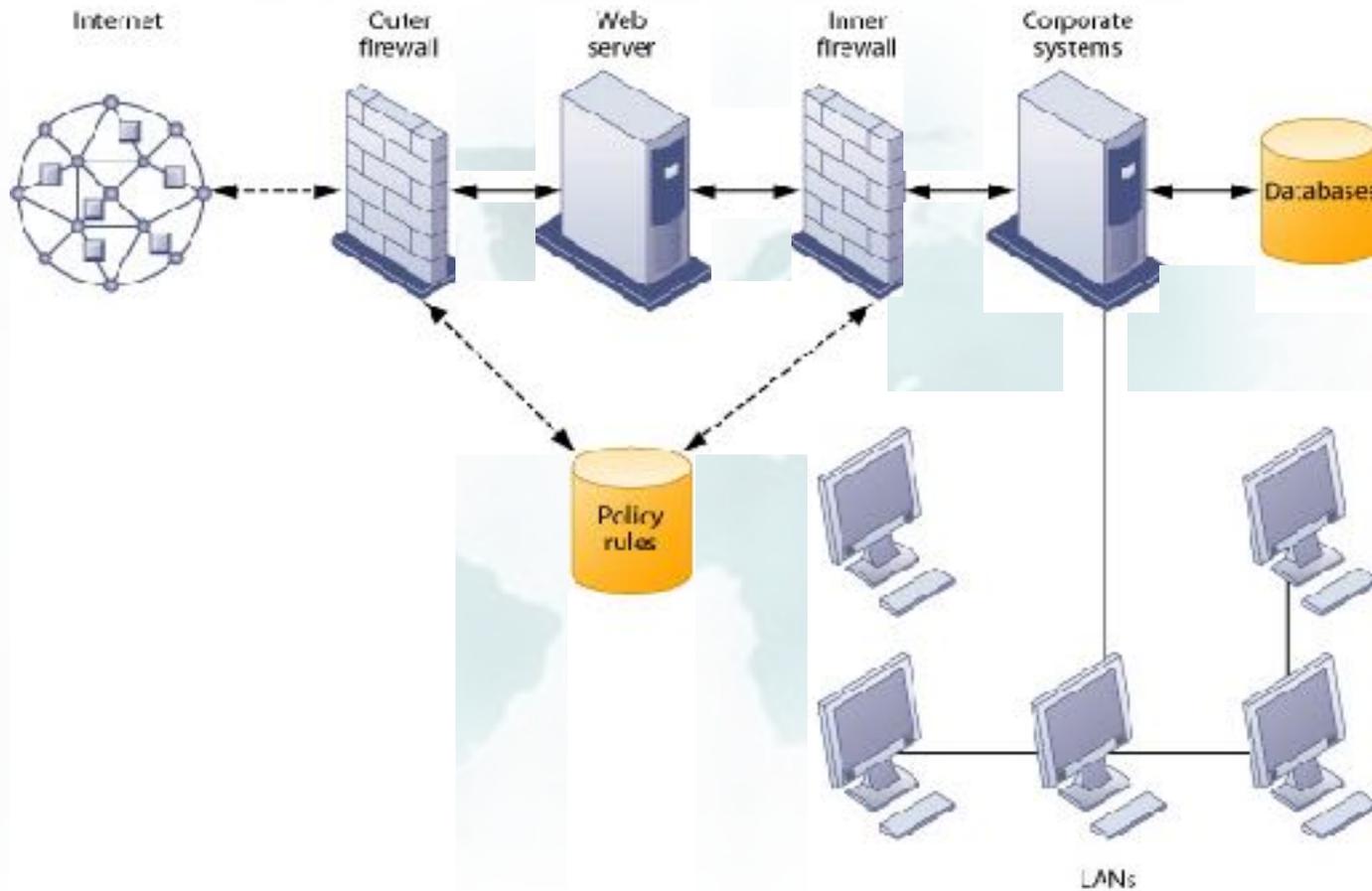


Information System Managements

Chapter 4 Security and Control

TECHNOLOGIES AND TOOLS FOR SECURITY AND CONTROL

A Corporate Firewall





Information System Managements

Chapter 4 Security and Control

TECHNOLOGIES AND TOOLS FOR SECURITY AND CONTROL

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



Information System Managements

Chapter 4 Security and Control

TECHNOLOGIES AND TOOLS FOR SECURITY AND CONTROL

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



Information System Managements

Chapter 4 Security and Control

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.

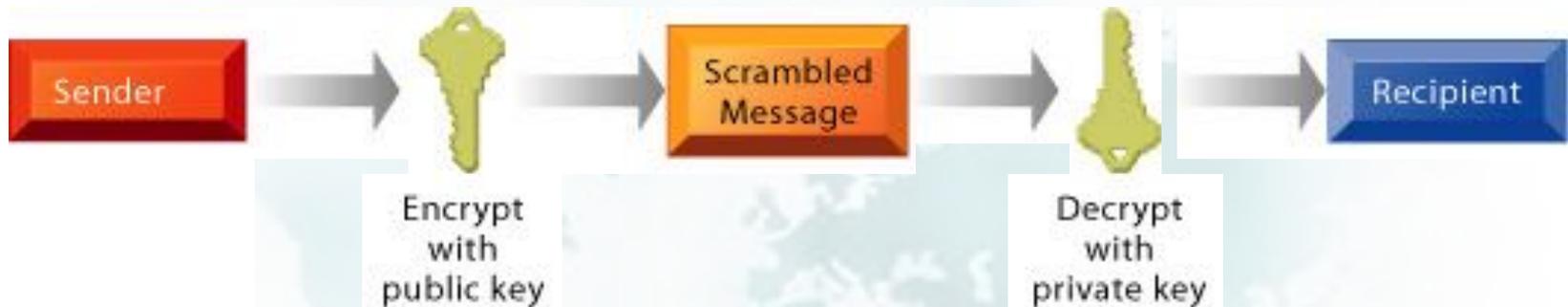


Information System Managements

Chapter 4 Security and Control

TECHNOLOGIES AND TOOLS FOR SECURITY AND CONTROL

Public Key Encryption



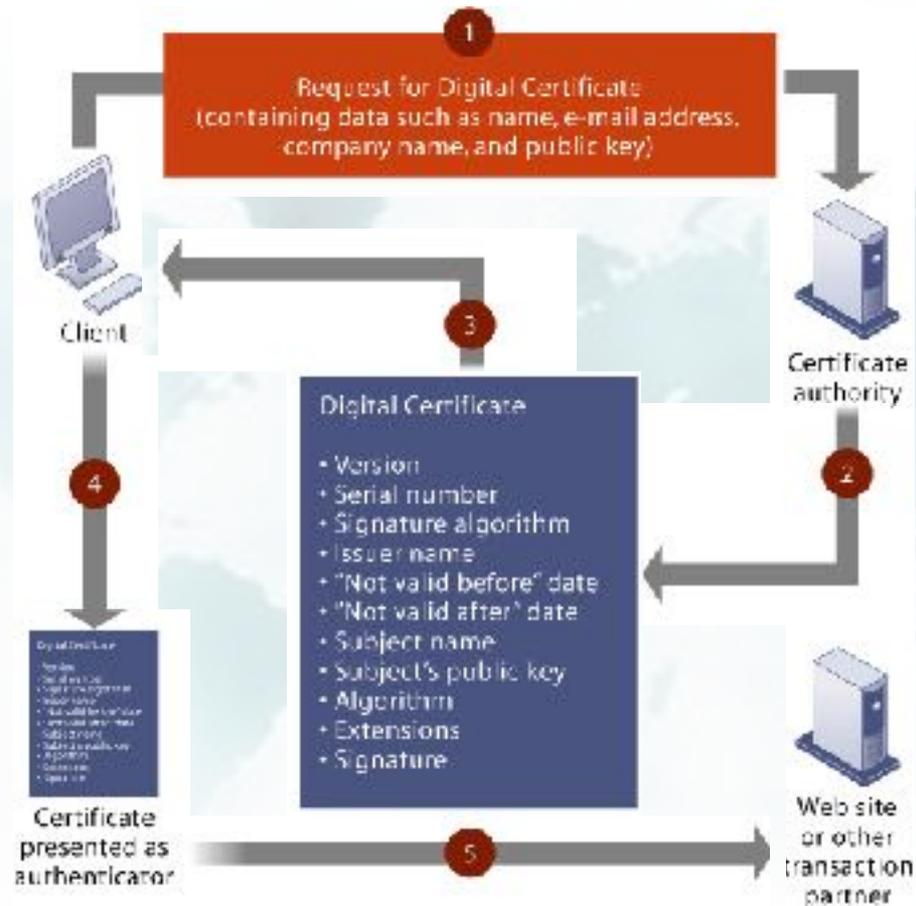


Information System Managements

Chapter 4 Security and Control

TECHNOLOGIES AND TOOLS FOR SECURITY AND CONTROL

Digital Certificates





Information System Managements

Chapter 4 Security and Control

MANAGEMENT OPPORTUNITIES, CHALLENGES AND SOLUTIONS

Management Opportunities:

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





Information System Managements

Chapter 4 Security and Control

MANAGEMENT OPPORTUNITIES, CHALLENGES AND SOLUTIONS

Management Challenges:

- **Designing systems that are neither overcontrolled nor undercontrolled**
- **Implementing an effective security policy**



Information System Managements

Chapter 4 Security and Control

MANAGEMENT OPPORTUNITIES, CHALLENGES AND SOLUTIONS

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.**