



INFORMATION SECURITY

AN INTRODUCTION

IC-SIRTII

THE ATTACKER PERSPECTIVE

- Individual computer experts ("hackers")
- Political issues, ICT supremacy, just for fun
- Intelligence agencies including cyber spy
- Criminals, cyber mafia, underground economy
- Businesses rivalry, trade secrets stealing
- Disgruntled employees, retired personnel
- Other parties may all seek to breach infosec

TYPE OF INFRASTRUCTURE ATTACK

- Hijacking, to intercept & to take over ICT resources
- Interruption, disrupting & to take down infrastructure
- Modification, change the contents into destructive materials, propaganda etc.
- Fabrication, spreading damages, well planned & or sophistication of targetted attack
- Using techniques: DDoS, DNS/route poison, scam, SPAM, phishing, identity theft, malware (virus, trojan, botnet, rootkit, backdoor)

DEFENSE & COUNTERMEASURE

- Conduct cyber defense (monitor, detect, prevent, anticipate, mitigate, recover) infrastructure
- Organize National CyberSec framework to assure & evaluate periodic intelligence & proactive defense initiatives incl best practices of infosec deployment
- Build national secure data center, backup (DRC) & rehabilitation capability, provide secure emergency channel & resources to establish & maintain critical infrastructure during the hard events
- Perform CERT/CSIRT/CC to coordinate incident response handling & international collaboration

INFOSEC BASIC THEORY

- Protect information & systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction
- Protect the confidentiality, integrity and availability of information: electronic, print, & or other forms
- Non repudiation, in digital terms is a service:
 - Provides proof of the integrity & origin of data i.e encryption
 - An authentication that with high assurance can be asserted to be genuine
- Packerian hexad model: confidentiality, possession, integrity, authenticity, availability & utility(debatale)

INFORMATION SECURITY BREACH

- Interception of messages and theft of stored data
- Information sabotage (i.e., alteration or destruction of data belonging to another party)
- Spoofing (i.e., using stolen information to pose as somebody else); and
- Denial of service (i.e., deliberate shutdown of cash machines, electric-supply grids, air-traffic control networks, or the like)

RISK MANAGEMENT

- Assets identification, valuation. Incl.: people, buildings, hardware, software, data (electronic, print, other), supplies
- Conduct threat assessment. Incl.: Acts of nature, acts of war, accidents, malicious acts originating from inside/outside orgz
- Conduct a vulnerability assessment, & for each vulnerability, calculate the probability that it will be exploited. Evaluate policies, procedures, standards, training, physical security, quality control, technical security
- Calculate the impact that each threat would have on each asset. Use qualitative analysis or quantitative analysis
- Identify, select, implement appropriate controls. Provide proportional response. Consider productivity, cost effectiveness, & value of the asset
- Evaluate the effectiveness of the control measures. Ensure the controls provide the required cost effective protection without discernible loss of productivity

ISO/IEC STANDARD SERIES

- ISO 15443: "Information technology - Security techniques - A framework for IT security assurance"
- ISO/IEC 27002: "Information technology - Security techniques - Code of practice for information security management"
- ISO-20000: "Information technology - Service management", and
- ISO/IEC27001: "Information technology - Security techniques - Information security management systems - Requirements" are of particular interest to information security professionals

STANDARD: ISO/IEC 27002:2005

- Security policy, Access control,
- Organization of information security,
- Human resources security, Asset management,
- Physical and environmental security,
- Communications and operations management,
- Systems acquisition, development & maintenance,
- Information security incident management,
- BCP, and Regulatory compliance

MANAGEMENT & CONTROL

- Physical: doors, locks, heating, aircon, smoke & fire alarms, fire suppression systems, cameras, fencing, barricades, security guards, cable locks, etc.
- Physical segregation: separating network & work space & places into functional areas
- Logical: passwords, network and host based firewalls, network intrusion detection systems, access control lists, & data encryption

OTHERS MANAGEMENT & CONTROL

- Defense in depth: to fully protect the information during its lifetime, each component of information processing system must have its own protection mechanisms. Building up, layering on overlapping of security measures is called defense in depth
- Process: reasonable, prudent, due care/diligence
- Compliance to existing laws & regulation
- Professionalism of the human resource

INFORMATION CLASSIFICATIONS

- Label in business sector: Public, Sensitive, Private, Confidential, Unclassified
- Label in government sector: Unclassified, Sensitive, Restricted, Confidential, Secret, Top Secret
- In cross-sectoral formations, the Traffic Light Protocol, consists of: White, Green, Amber & Red

MILITARY CLASSIFICATIONS

- Top Secret (TS), material would cause "exceptionally grave damage" to national security if made publicly
- Secret, material would cause "grave damage" to national security if it were publicly available
- Confidential, material would cause "damage" or be "prejudicial" to national security if publicly available
- Restricted, material would cause "undesirable effects" if publicly available
- Unclassified, used for documents that do not have a classification listed above & sometimes can be viewed by those without security clearance

CRYPTOGRAPHY

- To transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption
- Information encrypted (rendered unusable) can be transformed back by authorized user, who possesses the cryptographic key, through decryption process
- Protect information from unauthorized accidental disclosure while is in transit & while is in storage
- Provides other useful apps: improved authentication methods, message digests, digital signatures, non-repudiation & encrypted network communications

ACCESS CONTROL

- Non-discretionary approach consolidates all access control under a centralized administration
- Usually based on individuals function (role) within the orgz or individual task/role
- Gives the creator or owner of the information resource ability to control access
- In the Mandatory access control approach, access is granted or denied basing upon the classification assigned to the information resource
- Access control key: identification, authentication

AUTHENTICATION

- 3 types of authentication information: something you know, something you have, something you are
- You know: PIN, password, mother's maiden name
- You have: driver's license or a magnetic swipe card
- You are: palm/finger prints, voice, retina (eye) scans
- Strong authentication requires providing information from 2/3 different types of auth information. For example, something you know plus something you have. This is called two factor authentication

AUTHORIZATION

- After a person, program, computer has successfully been identified & authenticated then it must be determined what informational resources permitted to access & what actions they will be allowed to perform (run, view, create, delete, or change)
- Authorization to access begins with administrative policies & procedures
- The policies prescribe what can be accessed, by whom, & under what conditions
- The access control mechanisms then configured to enforce these policies

SECURITY GOVERNANCE

- An enterprise-wide issue
- Leaders are accountable, staff aware & trained
- Viewed as a business requirement
- Roles, responsibilities, segregation of duties defined
- Addressed & enforced in policy
- Adequate resources committed
- A development life cycle requirement
- Planned, managed, measurable, and measured
- Risk-based, reviewed and audited

INCIDENT RESPONSE

- Selecting team members, training, drills
- Define roles, responsibilities and lines of authority
- Define a security incident & reportable incident
- Mitigation: Detection, Classification, Escalation, Containment, Eradication, Documentation

BCP AND DRP

- “Mechanism by which an organization continues to operate its critical business units, during planned or unplanned disruptions that affect normal operations by invoking planned & managed procedures.”

BUSINESS CONTINUITY PLAN

- Most of BCP's structure is to prepare emergency procedures in every stages to fulfil many questions related to “what should do if situations happen”
- If disaster strike, what are first few things should do? ER services help take the first hit when disaster strikes & if disaster is serious enough ERT need to quickly get a Crisis Management team in place

DECISION TO MAKE

- What parts of business should recover first? The one that brings most revenue or the one where spend the most or the one that will ensure sustained future growth? The identified sections are the critical business units. There is no magic bullet here, no one answer satisfies all. Businesses need to find answers that meet business requirements

RECOVERY CONSIDERATIONS

- How soon is target to recover critical business units? Technical is called Recovery Time Objective (RTO). Define what costs the business will need to spend to recover from a disruption. For example, it is cheaper to recover a business in 1 day than in 1 hour
- What all needed to recover the business? IT, record, machinery, food, water, people, supplies, many aspects to dwell upon. The leaders need to drive business continuity and make clearer decision

RECOVERY PROCESS

- Where we recover business from? Will emergency business center give enough space & facility to work or would it be flooded many people queuing up for the same reasons: no place to go
- How long can we survive after recovery without original sites, systems, capacity, people? this defines the amount of business resilience may have
- How to make sure the plan works? Most BCP pundits would recommend testing the plan at least once a year, reviewing it for adequacy & rewriting updating plans either annually or when businesses change

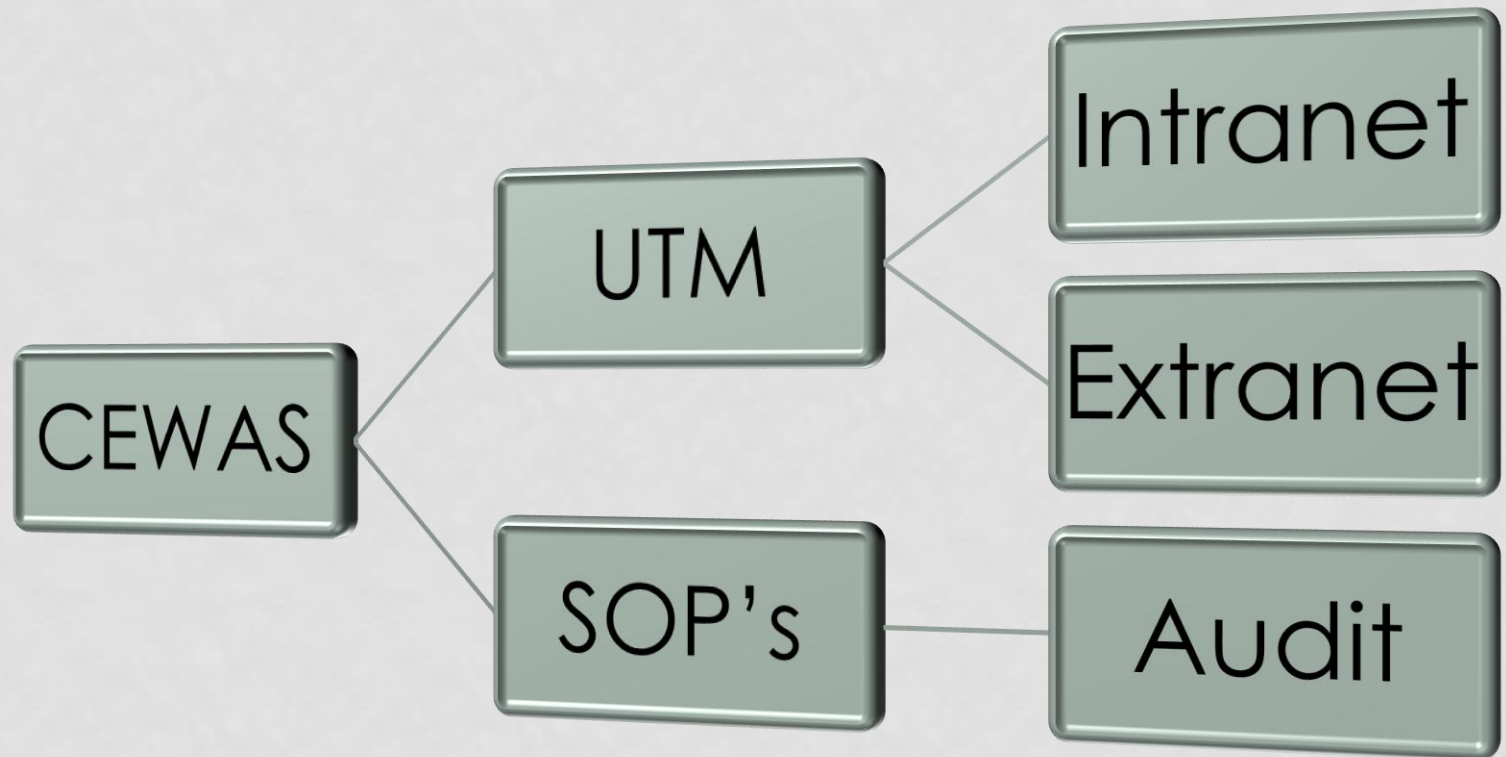
DISASTER RECOVERY PLAN

- While a BCP takes a broad approach to dealing with organizational-wide effects of a disaster, a disaster recovery plan (DRP), which is a subset of BCP, is instead focused on taking the necessary steps to resume normal business operations ASAP
- A DRP is executed immediately after the disaster occurs & details what steps to be taken in order to recover critical infotech infrastructure

INTERNAL DEFENSE

- “Your security is my security. Ensuring self defense.”

CEWAS (IN HOUSE)



UNDETECTED THREAT

- Sophistication/targetted attack
- Personal information stealing
- Account hijacking & fraud crime
- Lack of awareness, user behaviour
- Mostly caused by data over exposure
- Social engineering techniques
- Phising & malicious code as tools
- Human, the weakest security link

INSIDER THREAT

- Trojans and backdoor
- Unsecure programming
- Counterfeit equipment
- Data/information misuse
- Level of access policy breach
- Physical security perimeter breach
- Inappropriate disposal procedures

REAL STRENGHT

- Professional certified human resources
- Skill improvement (training, drill)
- Continuous research and development
- Updated data and base of knowledge
- Log management and correlation analysis
- Periodic security assesment and audit (CIA)

COMPUTER PROTECTION

- Use updated legal Operating System (OS) & apps
- Updated legal Anti Virus/Malware/Firewall is a must
- Periodically updated, cleaning apps trash, backup (settings, OS & application configuration, data)
- Do backup 3 times with different external media & keep it safe at several places. Backup cost is always cheaper than recovery cost
- Use protection tools (Deep Freeze, Windows Steady State etc.) & never log in as Administrator level users
- Never trust any external devices/media/files/apps

PUBLIC ACCESS PROTECTION

- Make sure cold boot the computer before use it
- Takes several minutes to check any suspicious or hidden activity at Task Manager, do quick virus & malware scanning check with your own trusted & secure protected portable tools
- Beware of hijacking tools (keylog, remote access)
- Never use public access terminal for critical transaction i.e. email (private), internet banking, e-commerce, company data transfer
- Don't leave terminal unattended & unprotected, not a second

WIRELESS ACCESS PROTECTION

- Always ask Wireless SSID's & never trust "Free WiFi Access" alike SSID's. Could be attacker/fake AP
- Wireless is open network, important to know about sniffing, side jacking, MITM, hidden camera
- Never open network sharing, make sure always turn off others wireless data connection i.e. bluetooth
- Never use public access terminal for critical transaction i.e. email (private), internet banking, e-commerce, company data transfer
- Don't leave terminal unattended & unprotected, not a second

SURFING PROTECTION

- Use only HTTPS, check validity of CA
- No script, no pop up, read before click! You can click NO/CANCEL, pay attention in every warning
- Always use parental control for your kids (default features in every latest browser), beware of phishing site, use DNS filter, never trust downloadable materials, use “open in a new tab” features not “new windows”, employ any useful add on
- Make sure clean log out, clear & clean up swap, cache, cookies, history, bookmark (use private browsing features), don't save username passwords

EMAIL PROTECTION

- Always use plain text not rich text (HTML, MIME etc.)
- Turn off auto open files (attachment, HTML) mode & always use latest & updated email anti virus/SPAM
- Never trust any attachment files, scan it, always ask confirmation from the sender before you open it
- Always use email client at own trusted computer or use portable email client with portable device
- Use PKI (i.e. GPG) to make sure email authorization
- Use secure encrypted protocol (POP, IMAP, SMTP)

MESSAGING PROTECTION

- Use latest most secure updated messaging apps & never spread ID to others peers that you're not trust
- Never trust unknown new friends, always double check, ask first to make sure & to identify who they really are. Stranger background check necessary
- Never trust DCC files/materials/links, double check it
- If you should download files/materials: scan it with latest anti virus & anti malware before you open it
- Use DNS filtering services to protect most phishing sites, ads, SPAM, malware spreading sites & any others untrusted content

E-COMMERCE PROTECTION

- Never use unsecured/public access terminal. If you should make sure it safe & clean before transaction
- Make sure always connected in secure (HTTPS) & always check CA validity, the expiry date etc.
- Make sure that access to real official web site not a fake, beware of phishing attack. Never click external links from email, chat, any others pops up
- Always use DNS filtering protection, latest anti virus, anti SPAM, anti malware, anti phishing. Make it double if necessary because it will never enough to prevent any such incident possible & losses

SOCIAL NETWORK PROTECTION

- Never add unknown new friends. Always ask for confirmation to mutual friends. Leave direct basic questions message to the suspicious account
- Be conservative. Limiting privacy exposure, decide how much to share. Not everybody needs yours
- Never use free mail. Use private domain & email addresses or corporate account (if it's allowed)
- If something happens, report to admin, broadcast alert to all of your friends, hope you have backup, make new account & tag your old account as impersonating & fraud. Ask everybody to do it

ATM & SMS PROTECTION

- Knowing latest updated technology & procedures to understand weakness, loop holes, fraud tech, detect unusual process, using PIN management & one time token. Ask your banks about latest update
- Knowing card types (magnetic stripes, chip, RFID) & kind of services (debit/credit, ecash). Protect card physically, hiding CVV2 code, anti magnetic sleeve
- Never trust. Double check in any transaction careful while in the middle of transaction, watch the EDC
- Look physical environment, consider all possibilities: skimming, hidden camera, unauthorized assistance

PASSWORD PROTECTION

- Change password periodically, more often better & never share password to anybody for any reasons
- Longer complicated combination is more stronger. Not easy to remember/reveal. Unpredicted phrase
- Keep in safe secret places. Nobody's know. Ever
- Use password management application or services or one time token password services. The problem is how to make sure & to secure the token delivery channel from the system to the end user. Most of delivery channel is open public network i.e. SMS
- Don't use one for all password, use different each

PORTABLE DEVICES PROTECTION

- Password protected any of your rewritable portable devices (flash disk, external drive, gadget, ipod etc.). Consider to use encryption
- Use the most possible, secure, limited sophisticated file system NTFS, HFS+ (MacOS), Ext2/Ext3 (Linux) etc.
- Always make 3 backup, latest Anti Virus & Malware
- Keep devices with you, never lend it to anybody
- Beware safety surroundings physical environment
- Do highest secure wiping procedures for disposal

THANK YOU

- Ravindo Tower 17th Floor
- Kebon Sirih Raya, Kav. 75
- Central Jakarta, 10340
- Phone +62 21 3192 5551 ; Fax +62 21 3193 5556
- office@idsirtii.or.id ; www.idsirtii.or.id