# Techniques & Strategies to Empower Cyber Security

by
(alphabetical order)

Abraham Ferdinand
Andy Minar Widjaja
Aris Budiman Hartono
Dicky Prasetia
Gildas Deograt
Kalpin E. Silaen
Onno W. Purbo

XECUREIT.id

# Table of Contents

# CHAPTER 1 Cyber Security Empowerment Essentials

## Focus on Cyber Security Empowerment

XECUREIT (xecureit.id) is an Indonesian company with more than twenty years' experience in cyber / computer security. It includes experiences in creating applications and appliances for cyber / computer security. These products then are used for government agencies as well as large private companies, including several major banks, in Indonesia.

In the process of implementing cyber security in various agencies, we allocate considerable time to empower partners and clients in the field of cyber / computer security, including training and certification of Computer Security Certified Professional (CSCP). CSCP is a professional certification that is open to the public.

One of the authors, Onno W. Purbo, coincidentally is also one of the advisors in Internet Sehat (Internet Safety) community (internetsehat.id). Internet Safety is a community movement to empower safe Internet for the general public / end user.

This book will discuss the experiences and tactics / strategies that need to be developed in teaching cyber / computer security both at the end user level, administrators and regulators / decision makers.

### The Book Objectives

- Sharing patterns / strategies in the field of cyber / computer security.
- Sharing cyber / computer security teaching experience and techniques.
- Foundation for discussion on teaching techniques in cyber / computer security.

### Basic Condition of The Public

Patterns used in teaching / empowerment will vary from one place to another, from one country to another  as it depends on the knowledge background of the public. This book will use mainly the Indonesian condition as reference. At the momet, the common is,

- Most think that IT is sophisticated. All problems can be solved by pressing the button.
- Everyone on the Internet is educated and well-behave. Everyone on the Internet can be trusted.
- Most are ordinary IT users, not administrators, not regulators.
- Most users are very naïve about IT operational backend.

## Cyber Security Strategies

In general to strengthen the cyber security, we must focus on three (3) targets, namely,

- End user
- Administrator
- Government / Regulator

Some general strategies,

- Empowerment - This is the most important strategy as most problems happen because of a lack of knowledge about the dangers that exist on the Internet.

- Cooperation / coordination with private sector - this becomes very important to do because most of the network in Indonesia operated by private sector. A good cooperation may happen mainly due to personal networking. Therefore it is very important to establish a forum / place to meet / discuss among stake holders.
- Information sharing and coordination - At this moment, coordination and sharing of information is rare. In Indonesia case, hopefully with the establishment of the Cyber and Crypto State Agency (Badan Siber Sandi Negara / BSSN ) the process of coordination and information sharing can be more easily done.
- Implementation and make own equipment - especially in strategic state institutions / installations, it is necessary to develop the ability to build and implement own cyber security equipment.

## Cyber Security, the End User Side

At the end user side, the main focuses are,

- Empowerment on cyber security.
- Technical skills on how to do self-protection and Internet safety.
- Safe behavior on the Internet, such as not doing any unresponsible posting  etc.

Some of the main problems,

- Reading culture, especially English text is quite low.
- A huge amount to be empowered, Indonesian Internet users reach 80 ++ million people.
- Since 2013, ICT have been removed from the school curriculum, making it difficult to include cyber security into the school curriculum.

## Cyber Security, the Operator Side

On the network administrator / operator side, there are some main focus that need to be performed, among others,

- Skill to secure the network from attack.
- Skill to monitor the attacks.
- Understanding Information Security Management, and able to escalate in the event of a problem.
- Can help the user in the event of a problem.
- At the private sector management level, it needs the ability to integrate information security as part of the corporate culture.

Some of the main problems,

- English is the main problem, as most of the materials, manuals, error message is in English.
- Most campuses do not teach skilll / practical knowledge on network attack techniques, attack monitoring techniques or network security techniques.
- The network knowledge provided is largely limited to clients side, not much on networking or server management.

## Cyber Security, the Goverment / Regulator Side

On the government / regulator side, there are some main focus that need to be considered, some of them are,

- Ability to coordinate and share information among institutions. At the moment, most of the process of coordination and information sharing is done through a formal process that is usually slow.

- Establishment of rules and procedures. This may be difficult, if the regulators do not have understanding on how the cyber network works.

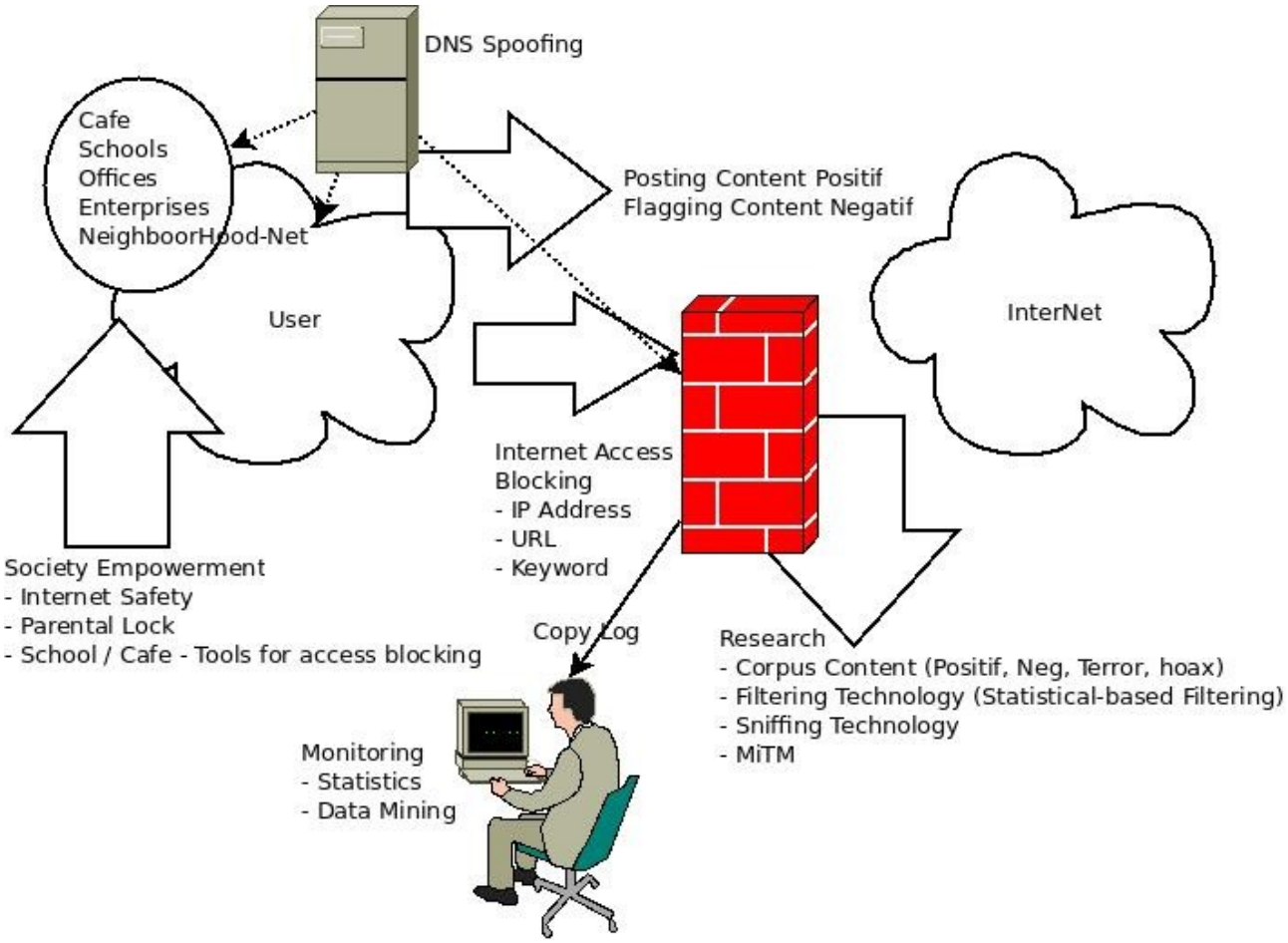
Some of the main problems,

- Accelerate the coordination and information sharing processes. This can be done easily if one personally knows each other.
- The rules and procedures may only be effectively drafted by those who understand of the technology works.
- Understand the priorities / staging of technology implementation. Technology can be applied gradually / staging based on the priority sets. It needs the knowledge of technology and its stages to be able to set in accordance to human resource and budget capacity.

# CHAPTER 2 Cyber Security for the End Users

## Global Strategies

An overview of the implementation strategies is shown in the figure below.




In general, the important strategy components are as follows,

- Society empowerment. It will be more effective through schools and young generation crowds.
- Flooding positive content to the Internet - this will only be effective if the Internet Safety / Internet Sehat movement can be incorporated into the school curriculum.
- Blocking illegal content via firewalls / routers at public facilities - this will only be effective if there is research on filtering techniques as well as free distribution of results to the Community.
- Government rules / policies - the Indonesians will normally move quickly after a government policy for the required implementation. Of course, a policy must be supported by a right ecosystem that is well-planned staging, in order to be implemented well.

## Internet Safety

Community empowerment on Internet Safety is one of the most important empowerment component.

- Providing an understanding of Internet safety should be a movement at the community level.
- Internet Safety - has been started in the early 2000s by InternetSehat.id. They generate the required resources. The primarily activities are based on resources that can be freely taken / downloaded, such as,
  - e-books, booklet, comics.
  - Some films
- Organized events,
  - Seminar
  - Workshop
  - Talkshow

Actually it would be better if we could,

- Integrate Internet Safety movement into school curriculum. Strategically, this can only be implemented if ICT clas is included in the school curriculum. This will require the provision of educational resources, teacher training to be ready to implement ICT classes in schools.
- Connecting all schools to the Internet using Universal Service Obligation (USO) held by telecom operators. USO financing may be provided as a deduction for schools in connecting to the Internet, and for remote areas can be a full donation for the required Internet access or equipments.

## Illegal Content Blocking, Positif Content Flooding

Since most Internet users, especially in Indonesia, are still very new to the Internet with a mostly conservative in culture, one of the fastest solutions to make Internet safer for most people is to block illegal content on the Indonesian Internet. For that purpose, the Electronic Information and Transaction Act (UU ITE) is made. In the revision of the ITE Law, it is explicitly mandated that the government must block illegal content on the Internet accessed by Indonesians. Unfortunately, blocking content (URL) is not technically easy especially if access is done using HTTPS.

Another alternative for a more positive Internet, is to flood the Internet with positve contents. The consequence is if someone search through a keyword in search engines, then the probability to obtain negative contents will become lowert. To be able to flood the Internet with positive content, inevitably have to mobilize resources in Indonesia to post good content as much as possible on the Internet. It would be much easier to mobilize schools and teachers to encourage students to about anythings around them on the Internet. Activities to flood the Internet with positive content can be included as part of the ICT / Internet Safety curriculum in schools.

## Freedom of Speech / Digital Right

Blocking the Internet from negative and illegal content that is a solution in between, as it gradually creates some difficulties in the the future. Because the definition of negative and illegal content is still very fluid, everyone may have different definition. The definition of the commons may be different from the government or party members.

In the recent years, there has been disputes on the Indonesian Internet especially on freedom of speech and digital rights issues. For a clear criminal activity such as pornography this is not too much of a problem, as it is very clear - which one is right, and the other one that is wrong.

For things that are not clear, especially those that are more focused on ethics, usually the government  may have difficulties to determine the right and the wrong ones. These unclear conditions may create potential conflicts in the field of Freedom of Speech and Digital Right.

Some examples that may lead to a conflict in the field of Freedom of Speech / Digital Right, such as,

- LGBT - it can not be explicitly categorized as pornographic activities.
- Spreading the religion - often becoming disguised with terrorist activities.
- Political Issues - Attacking / Dropping Among the Politics. On many occasions, it appears in the form of hate speeches / hoaxes.
- Fraud / hoax - often we will have trouble determining a post wether it is right or hoaxed.

To resolve this issue, a deeper discussion with the various stakeholders is needed. This discussion is likely to be very difficult, because each of the camps will most likely hold on to his opinion.

## Tips for Corporate / Private Sector Employees

For IT managers, or IT personals, here are some empowerment tips that may be used for corporate / private sector employees, among others,

- Regularly discuss with employees about cyber security.
- Remember that top management and IT staff are also employees.
- As we strive to secure corporate infrastructure, the system is only good limited by its weakest links.
- Organize forums / focus periodic discussions to explore different types of cyber attacks.
- Remind employees not to underestimate social engineering.
- Do not underestimate or bully any red flag reports that come in, including from low-level employees.
- In the event of an incident, help the employee as closely as possible.
- Training to be able to distinguish the existence of cyber attack.
- Periodically test employees' knowledge of cyber attack / cyber security.
- Invite, listen and respond to feedback.

# CHAPTER 3 Cyber Security for the Operator

This section is the most strategic part of the whole book. This section will discuss about cyber security for network providers / operators / administrators. This section is important, as the network operators / administrators are the one who implement are look after various matters on network / cyber security.

The level of difficulty may vary greatly, because the network scope to be handled. In general, we can divide the level of difficulty as follows,

- Operator Telekomunikasi / Internet Service Provider (ISP).
- Operator Corporate / Enterprise
- Operator / Administrator of School / Community Access Point such as Free WiFi.

Of course, the most difficult is the telecommunications operator and ISP. While, the school operator / Free WiFi is relatively simpler.

The level of difficulty in Indonesia is somewhat higher due to the limited background knowledge of the operators as most of the required knowledge is never obtained in schools. The condition of most administrators in Indonesia,

- Not many administrators knows how to work with UNIX / Linux servers.
- Not many are familiar with Command Line Interface (CLI).
- Not many really understand how computer networks work, such as, understand routing, understand ports, understand reading the results of packet sniffing.
- Usually differences in background knowledge among training participants will vary widely, this will also cause difficulties in equating the material that needs to be taught.
- Usually the trainees will prefer to receive the recipe skill, steps cheat to be run, to do something without understanding the theory behind the steps. The result is usually a bit difficult to develop / adapt if there is a cyber security problem or a new cyber attack technique.
- Usually participants will have difficulty reading error messages that written in English, and tend to ask the simple solution to it, without any effort to read the error message.

## Modul and Ecosystem Preparation

The important part is in the modules and supporting ecosystem preparation, some of them need to be prepared in detail. Some of them are,

- Digital library setup, various teaching materials. Material that is important to be prepared especially attack techniques, network security, information security management and IT forensic. Materials in softcopy / e-books are preferred to make it easier for participants to access the teaching materials.
- Setting up the server / system e-Learning. The server may make many things easier. Some of the things to be prepared are,
    - Server e-Learning, we normally like to use Moodle.
    - Learning Materials / Modules, the easiest is to upload slides or links to the wiki.
    - Questions Bank, this is probably the most important as the number of questions should be around 10-20 times the number of issued questions in the test so that such tests may

be performed many times at random. Creating questions bank is the most time consuming task.

- IntraNet and PenTest ecosystem preparation. Ideal-nya every participant received,
  - A minimal of one laptop / per participant, with multi operating system, including Kali Linux, Windows, and Ubuntu.
  - A minimal of one Virtual Machine for attack targer practice.
  - A minimal of one Virtual Machine for defence practice.
  - A minimal access to WiFi, a LAN is prefereable for higher performance network.
  - Access to the Internet should be provided through the Ecosystem.

## Participant Conditioning – Pre-Training.

Our experience in Indonesia so far, would be better if

- Participant does like cyber security topics.
- Participant already has field experience.
- Participant likes to read, to try, to experiment on cyber security techniques. It would be better if he likes to read materials in English.
- Educational background and diploma is actually not too important.

Often, participants especially from government agencies attends based on rank / position / task, and not based on their interest. Providing training for those who are not very interested in the field of cyber security is not an easy task.

There are several things that need to be done to conditioning participants before the training is done. Some of them are,

- Work on pre-qualification quiz and assess each participant ability. From pre-qualified quizzes, we may design more appropriate training modules, such as how much basic material needs to be given before we get into real cyber security materials.
- If the training time is long enough, for example 6-12 months, participants should be invited to prepare the needed ecosystem for training processes. It includes setting up servers, laptops, and networks.

Usually the preparation work for these participants becomes much easier, shorter, if the participants have received some good lectures in the field of networking, operating system and hopefully some cyber security. Unfortunately, in Indonesia, no campus is good enough to provide the foundation of cyber security skills for its students. In Indonesia, most of the lecturers are from the academic world and more science-focused, scientists not practitioners in the industry. It is understandable as the industry especially manufacturing industries in Indonesia is not / less developed. As a result, in Indonesia, good participants must find their own foundations needed in the field, from where they work, or from the Internet. This process is more difficult, longer, compared to structured education processes.

## Participant Conditioning – During Training

During the training process, there are several things that need to be done to condition the participants. The cultural behaviour of many of the Indonesian would create a big challenge, such as,

- Participants prefer skill / practical knowledge, but lack of theoretical knowledge.
- Participants prefer to hear explanations from tutors / lecturers, in comparison with searching for their own materials.
- Participants have difficulty reading English materials. Thus, a big challenge for tutors to prepare the materials in Indonesian.

At the time of training there are some interesting techniques that may be interesting be examined. Especially for Indonesian, some of the teaching techniques are,

- Most participants will only learn by forced :) ... Unfortunately, commands, such as, saying "You must learn!" will likely fail.
- Participant will feel the force if there is some sort of peer-pressure in front of other participants. For example by, telling who among them receive the highest mark or managed to achieve something better than others. In a relatively new cyber security world, sometimes we will see a lot of surprises, for example, to see a participant with academic degree in economics, she got the highest score in one of the cyber security exam.
- After each modul, a module exam should be performed. The exam may be performed multiple times through the e-learning server. Thus, at the end of the day, we as a teacher may accountable and control the participant's competency per modul. Some of the benefits of multiple online exams are,
    - Create a peer-pressure and competition among participants. As the progress mark of the exam is periodically published as done by, OWP, one of the author.
    - We can easily force the participants to read the teaching materials, either through exam questions or the exam process. As a result, participants are forced to understand the theory behind the skills they are learning.
    - We can reduce the number of participants who fail, because they can improve their mark. In addition, the lecturer may gradually improve the competency level of the participants through multiple online exams process.

Quiz / exams become very important to us in Indonesia as the exams will be a driving key in forcing the learning processes. There are some experiences gain in the online exam processes, such as,

- Question bank should be carefully produced. Make sure that all material in the module is asked through various random questions. It takes a long time to map between the module and the question bank.
- In Indonesia, most participants will study at the time of the exam, or exam time. In order for participants to learn continuously - then the most powerful technique is to force the examinees to do the online exams many times. Since the exam may be done online, there is no time restriction. There is no need for a special room, no need to be guarded. To ensure, to increase difficult in cheating, the simplest way is to make the exam time very narrow, for example 40 minutes to 100 random questions.
- Continuous exams also reduce the likelihood of participants willing to take exams for other participants. In our experience, all participants who want do the exam will pass it after many exams.
- Every module should have quiz with the total question bank of about 10-20 times the number of issued question. Quiz in each module is needed to make sure, the participant mastered each module.
- Our experience shows that  it takes an average of 10 times of exam to get a score above 80%.
- Another technique that we can use to sharpen the participants' mindsets is by asking them to produce book / report. In the process of writting a book, the participants inevitably have to read the material and try it before they can write the book. Experience shows that only 0.1-0.5% of participants able to write a book, most will likely choose the exam option although it must be done many times to be able to pass.

The next issue is the teaching materials, some of the concerns are

- The dilemma of material balancing. What percentage of skills? What percentage of theory? In general, it may not be 100% skill or 100% theory, as this will weaken the participants later on in the field. Usually, the teacher will try to balance the skill and theory within the training time frame. But this will also vary depending on the participants' background knowledge.
- In explaining cyber security / network security, it will be very difficult if participants do not understand how an attacker works. Consequently, trainers have to teach techniques to perform various attacks. Surely the attack is done in an enclosed ecosystem with vulnerable targets.
- The first attack technique taught is a technique of tapping / sniffing on the network. Here we may show the consequence of unencrypted communication.
- Dilemma in teaching attack techniques. The teaching materials is very dangerous, especially if the participant has unstable integrity. Should we teach the attack technique? Sniffing technique? Trojan making techniques? Technique to inject trojan? SQL inject technique? Brute force technique?
- The dilemma of balancing attack vs. defence techniques. In a limited time, we should be able to teach attack and defense techniques, as well asl forensic. It is an art to be able to balance all of them especially in 1-2 days of training.
- The backgroup knowledge dilemma. Most participants usually have very limited background knowledge. It would be difficult to explain the attack & defense technique without adequate background knowledge. Often at the time of teaching, we must review the knowledge foundation that should have been aquired by the participants.
- Staging, topical, or jumping dilemma. In delivering the material, we will often encounter the dilemma of whether we should deliver the materials gradually, or by topics, or jump forward. Usually staging / stages will make the participant to be bored. Giving topics that are too fast forward will cause the participants failing behind. While giving topic-based material will usually also cause the participants to be unable to follow if a topic depends on another topic. In the end, we must improvise forward, backward, jump to the required topic at a time.
- One of the primary keys in the defense system is knowing the attack technique, and is able to create defense rules to counter such attacks. For that we will usually need to do the "See it and Responds to it" technique, like,
  - Attack, sniff it, Intrusion Detection System, rule creation.
  - Attack, sniff it, Firewall, rule creation.
  - Attack, sniff it, Web Application Firewall, rule creation.

## Participant Conditioning – After Training

No less important is the bond with the participants after going through the training process. This tie should be kept up as this will be needed durting mitigation processes if there is defense / cyber security issues. The process for strengthening this bond may be done using,

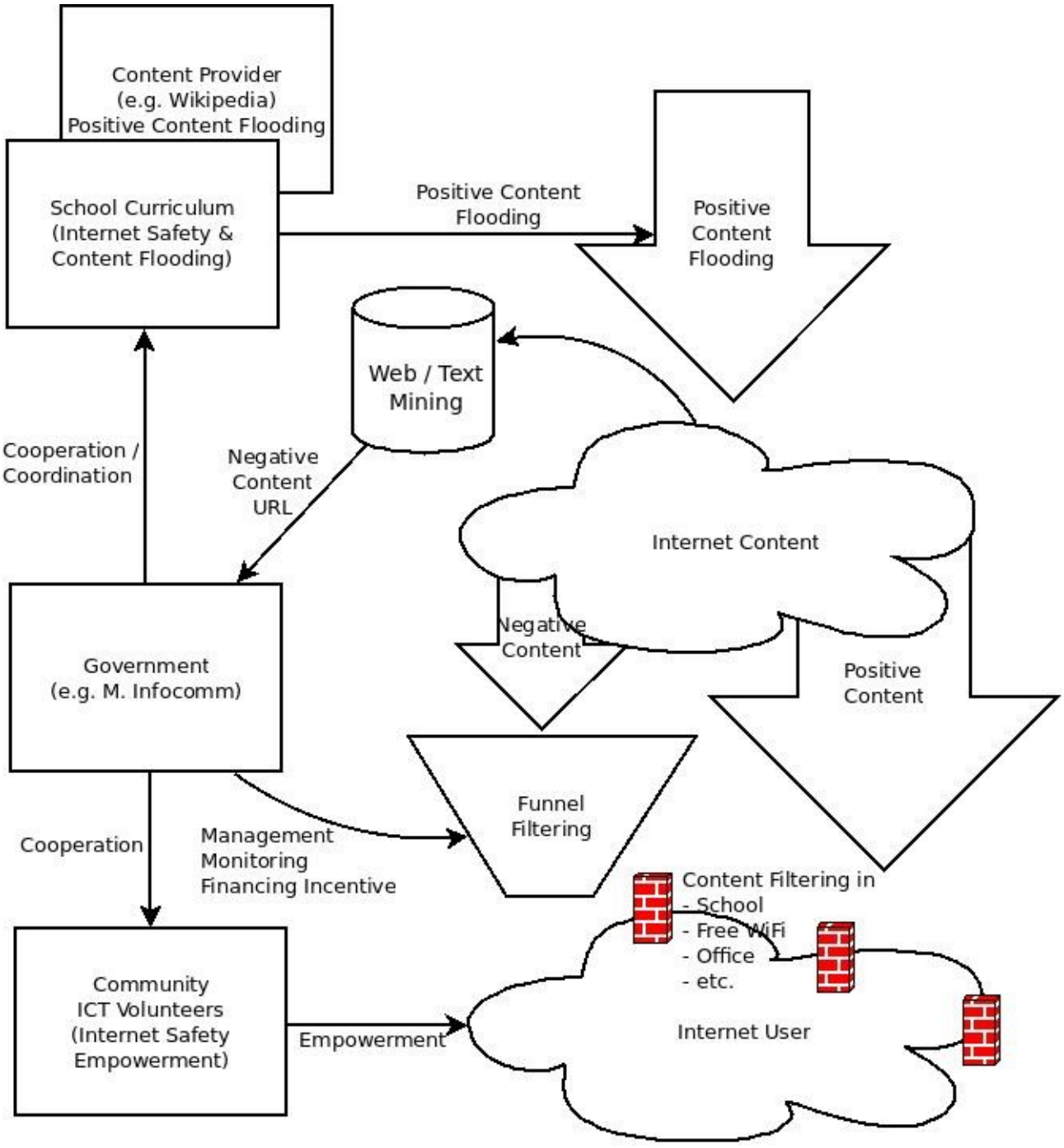
- Group Chats, such as Whatsapp, Telegram. Fortunately, in Indonesia, security professionals are crowded in secure group chat made in Indonesia, namely, PesanKita Indonesia which can be freely downloaded from the Android Play Store.
- Periodically hold physical meetings. Physical meetings are usually more difficult to organzied. Several attempts to hold such a physical meeting were conducted by the Indonesian Ministry of Defence (KEMHAN) as well as Cyber and Crypto State Agency (BSSN).
- Various events / seminars. In various computer events / seminars, especially those related to cyber security, cyber security professionals often meet. It will also create personal closeness among professionals.

# CHAPTER 4 Cyber Security for Government / Regulator

In the field of cyber security, the government / regulator plays several roles at once and each of the roles will usually be undertaken by certain agencies / agencies within the government. In Indonesia, some of these roles are,

- Capture cyber criminal - this role is done by the Police, especially Cybercrime Unit. In this task ability to deterse and forensic is crucial.
- Protect the citizens from illegal information / content - this role is done by the Ministry of Information and Communication. This has been partly discussed in the cyber security for users / end users section. Part of the regulator side of cyber security will be discussed in this section.
- Protect institutions / agencies / corporates from cyber attacks - this role is performed by network administrators of each institution / corporate. Institutions such as ID-SIRTII (now apparently under BSSN) should be able to play an active role in empowering this process. This is partly discussed in the cyber security section for network administrators.
- Maintaining the sovereignty of the Indonesian republic in the cyber world - this role should be actively coordinated / carried out by BSSN. Part of this role will be discussed more deeply in this section.

## Strategies to Safe Indonesian Internet Users




The government strategy, especially for end user's cyber defense / cyber security is shown in the picture. In general, there are some focus activities, that is,

- Filtering illegal content.
- Content filtering at schools / institutions / public facilities.
- Positive content flooding.

To achieve the objectives, several tasks may be performed, such as,

- Perform management, monitoring, as well as financial incentive options for the filtering systems operation in the operator's network.
- Work with community organizations, including ICT Volunteers (RTIK), to empower communities in self-defence while online on the Internet and to develop / use local filtering techniques for schools, and more.
- Cooperate with the Ministry of Education (DIKNAS) to enable schools to empower 46.5+ million Indonesian students to self-protect, as well as to flood positive content to the Internet. Positive content flooding on the Internet can be done by posting as part of school lessons, for example, writing about local customs, local cuisine, local ethnic tours by students as part of their language classes.
- Cooperate with Ministry of Research and Higher Education to develop technology related to negative content filtering, as well as positive content flooding.
- Work with Content Provider to flood the Internet with positive content, for example with Wikipedia and others.
- DNS filtering should remain operational as it is technically the most efficient. Fixing the workflow / business process so that filtering processes may be done faster.

Some notes:

- Funding - The filtering process will require substantial funds, if precision content (URL-based) filtering planned to be employed rather than DNS / IP address based.
- Content filtering for web or sites based on SSL (HTTPS) has a significant problem to filter its content, as HTTPS requires valid and legit SSL certificates to prevent security warning on the end user browser..
- Massive filtering capabilities - performed at all levels, from international gateways up to the end users.
- Edukasi masyarakat untuk bisa menjaga / memproteksi diri pada saat menggunakan Internet, terutama edukasi di kalangan muda.

Responsibilities

- The mandate to perform content filtering is provided by the Information and Electronic Transcation Act to the Ministry of Information and Communication.
- Implementation can be done by the Licensed Telecommunicatikon Network Operators.
- Filtered Site / URL / content management may be deliberated by the screening panel of the agency / unit under Ministery of Information and Communication and executed by filtering system administrator at the Ministery office.
- Conducting reliable security on systems built so that the system qualifies as a public service system.
- Content filtering system management must be operated by different levels of access (operator) so that it can be used for other agencies / ministries.

# Awareness Tactics for Government / Private Sector Officials

Basically the government is responsible for making regulations and policies for cyber defense / cyber security. Policy / rules will usually be made by the high officials or their advisors. Therefore, the focus of awarness efforts are needed around these top officials.

One of the main problem is the background knowledge of these officials. The majority is not from computer science background, let alone specialization in cyber defense. As a result, it is not suprising to see decisions, policies / policies made far away from the core issues.

The same is true for the private sector. Often the company officials are strong in corporate management, but not in the IT field, especially cyber security / cyber defense. As a result, not much different, frequently the decision, policy / policy in the field of cyber security is made far from the core problems.

Therefore, opening insights for officials / government officials / regulators needs to be prioritized prior to maneuver at a more tactical / operational level at the inter-institutional level.

The insights opener for government officials / officials is somewhat difficult to do by giving advice / lecture as they are normally quite senior and usually more "wise" than the average staffs. Our experience, the most effective opening techniques, are,

- For events that involve many people, a live demo is more preferrable and explicitly shows how to obtain confidential data / information, such as,
  - Surfing on the Internet / social media - Performing target profiling. Sometimes people careless and post confidential things in the public media / social media.
  - Surfing the Google Maps - show the country's strategic facilities, such as military bases, a wide-ranging military training ground on the Internet.
  - Tap Wifi in the event location and show tap results directly in front of the audience.
  - Perform active attacks / hacking to participant's owned sites.

- Having discussion with officials at a relaxed time / not in front of their subordinates.
- Sit together with the officials to develop a suitable strategic plan for the institutions / corporate.

## Strategy for Information Security Management System (ISMS)

Some strategies that can be used to build Information Security Management System, among others, are,

- Discuss various scenario
- People vs Process vs Tool
- Discussion on Staging for Top Management

## Strategy for International Cooperation / Coordination

As we know, cyber crime does not see country's boundaries. Thus, we need to do some international coordination efforts to facilitate cyber defense, such as,

- Officials from high-ranking state institutions in Indonesia, such as BSSN, KEMHAN, should communicate frequently and meet with formal and non-formal International friends especially from neighboring countries.
- Information sharing and interagency coordination.
- Build bridges to the private sector.
- Building alliances, coalitions, and partnerships abroad.

# CHAPTER 5 Stories from the Ground

To provide an overview of the human side of the interaction process in the field. In this section, challenges faced in the process of empowering cyber defense will be shown. In layman language, this is probably the art in people empowerment in cyber security / cyber defense.

## End User Mindset

- Most of the problems that occur due to the simple and naive end user's mindset that is normally overconfident with the Internet.
- One of the example, since the Internet looks very sophisticated, it often assumes that the person on the other end is probably more educated, trustable. It create a condition that fraud / social engineering may easly be performed to a novice user on the Internet Indonesia. Losses of up to hundreds of millions and even billions of Rupiah had happen to the Indonesian due to social engineering on the Internet.
- End Users often feel that with Internet they can be anonymous, they can not be known. As a result, many end users post improper status on someone / policy / institution. This resulted in them are being trapped in defamation charges.

## Officers Mindset

- In recent times while running workshops, Information is something abstract, hard to imagine. The fact that information can be stolen, can be manipulated, can be utilized is very difficult to imagine.
- This happened while providing training to the Indonesian defense members, after from providing network attack demo the whole day from morning untill the afternoon, showing clearly how to steal someone's password while doing telnet remote login. The tapping process is done using a sniffer, because telnet is a communication that is not in the encryption then obviously the password will be seen easily. In the afternoon, one asks permission to ask, and the question is very simple "Where is the cyber attack?" .... Honestly, at that time, one of the author, OWP, was speechless in answering such simple question.

## Bureaucrats / Leaders Mindset

- Many people especially the layman who thinks cyber security / cyber defense is not much different from hitting gun's trigger in the military. We simply point the weapon to the target, hit the trigger, bang ... and the target will be destroyed. In fact, it's not that simple. It takes a complex technique and a long time to perform an attack to produce tangible results.

# Writer (Aphabetical)

## Abraham Ferdinand

## Andy Minar Widjaja

## Aris Budiman Hartono

## Dicky Prasetia

## Gildas Deograt

Gildas Deograt is a Certified Information Systems Security Professional (ISC)² and Certified Information Systems Auditor ISACA. In 1999-2002, was the Head of Information Systems and Telecommunication Security, Total E&P Indonesie. In 2002-2005, Information Systems Security Officer as well as Member of Committee Technology Group, SCADA Security of Total. In January 2010-December 2011, Expert Team Member Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII). In 2006-2011, Information Security Trainer at SecurityFirst, XecureIT Division of Education and Community Development. In June 2009-December 2009, Member of Government Regulation of Indonesia Cyber Law Development Committee, Kementrian Komunikasi dan Informatika. In January 2016 until now, Deputy Director Coordination and Mitigation Group, National Desk of Cyberspace, Coordinating Ministers for Politics, Justice & Security Republic of Indonesia. In 2008, Founder and Coordinator, Information Security Professional Network (ISPN). In August 2005, Owner, XecureIT is one of major Information Security Consultant Company in Indonesia.

## Kalpin E. Silean

## Onno W. Purbo

Onno W. Purbo holds a Ph.D in Electrical Engineering from University of Waterloo, Canada, is a copy left, educator and ICT evangelist. He has published 40+ books, including free ICT ebook for high school in 2008. The latest books in 2016 entitled, "Perjuangan Menyebarkan Internet" (Struggle in Deploying Internet) and "Buku Pegangan Internet untuk Desa" (Internet Handbook for Villages) in Indonesian. He led the first Internet connection at ITB and use it to build the first education network. He liberates WiFi frequency, and introduces neighborhood network, wajanbolic antenna and OpenBTS cellular network. He led the first community telephony network over

Internet, VoIP Merdeka, later known as VoIP rakyat and uses +62520 and +62521 area code. He currently actives in introducing e-learning, run the largest free e-learning servers with 19,000+ participants.