MESSAGE FORM

(INSTRUCTION: FILL-UP BOXES INSIDE DOUBLE LINES ONLY)

FOR COMCEN/SIG USE

PRECEDENCE ACTION/PRECEDENCE INFO
"PRIORITY"

FM: CG, PA

TO: All Unit Commanders
Attn: G6/Signal Officer/IS Officer

INTERNAL: All G-Staff, Personal, Special & Tech Staff, C, AOC/SAGS/XA

INFO: CSAFP
Attn: J6

GROUP:
04 January 2016

SECURITY CLASSIFICATION:
CONFIDENTIAL

ORIGINATOR:
6/CMB 0401-01-2016

1. References:

   a. Command Guidance
   b. VAPT and PANET Monitoring Result

2. As per above references, forwarded is the Cybersecurity Bulletin number 041 with topic regarding **The Seven Basic Principles of IT Security.**

3. ITR, all concerned G6/Signal Officers/Information System Officer/NCOs are reminded to include this information as part of TI & E on all of its subordinate units as part of enhancing the Cybersecurity Awareness of the Philippine Army.

4. For information and widest dissemination.

DRAFTER'S NAME AND TITLE	**PHONE NR:**
MAJ JOEY T FONTIVEROS (INF) PA Chief, CMB, OG6, PA	6630
RELEASER'S NAME AND TITLE COL VENER ODILON D MARIANO GSC (SC) PA AC OF S FOR CEIS, G6, PA	

HEADQUARTERS
PHILIPPINE ARMY
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS, G6
Fort Andres Bonifacio, Metro Manila

6/CMB

04 January 2016

CYBER SECURITY BULLETIN

Cyber Security Bulletin: #41

THE SEVEN BASIC PRINCIPLES OF IT SECURITY

Security is a constant worry when it comes to information technology. Data theft, hacking, malware and a host of other threats are enough to keep any IT professional up at night. In this article, we'll look at the basic principles and best practices that IT professionals use to keep their systems safe.

The Goal of Information Security

Information security follows three overarching principles:

- Confidentiality: This means that information is only being seen or used by people who are authorized to access it.
- Integrity: This means that any changes to the information by an unauthorized user are impossible (or at least detected), and changes by authorized users are tracked.
- Availability: This means that the information is accessible when authorized users need it.

So, armed with these higher-level principles, IT security specialists have come up with best practices to help organizations ensure that their information stays safe.

IT Security Best Practices

There are many best practices in IT security that are specific to certain industries or businesses, but some apply broadly.

1. **Balance**

   Computers in an office could be completely protected if all the modems were torn out and everyone was kicked out of the room - but then they wouldn't be of use to anyone. This is why one of the biggest challenges in IT security is finding a balance between resource availability and the confidentiality and integrity of the resources.

   Rather than trying to protect against all kinds of threats, most IT departments focus on insulating the most vital systems first and then finding acceptable ways to protect the rest without making them useless. Some of the lower-priority systems may be candidates for automated analysis, so that the most important systems remain the focus.

2. **Split up the Users and Resources**

   For an information security system to work, it must know who is allowed to see and do particular things. Someone in accounting, for example, doesn't need to see all the names in a client database, but he might need to see the figures coming out of sales. This means that a system administrator needs to assign access by a person's job type, and may need to further refine those limits according to organizational separations. This will ensure that the chief financial officer will ideally be able to access more data and resources than a junior accountant.

   That said, rank doesn't mean full access. A company's CEO may need to see more

data than other individuals, but he doesn't automatically need full access to the system. This brings us to the next point.

3. **Assign Minimum Privileges**

   An individual should be assigned the minimum privileges needed to carry out his or her responsibilities. If a person's responsibilities change, so will the privileges. Assigning minimum privileges reduces the chances that a personnel from design will walk out the door with all the marketing data.

4. **Use Independent Defenses**

   This is a military principle as much as an IT security one. Using one really good defense, such as authentication protocols, is only good until someone breaches it. When several independent defenses are employed, an attacker must use several different strategies to get through them. Introducing this type of complexity doesn't provide 100 percent protection against attacks, but it does reduce the chances of a successful attack.

5. **Plan for Failure**

   Planning for failure will help minimize its actual consequences should it occur. Having backup systems in place beforehand allows the IT department to constantly monitor security measures and react quickly to a breach. If the breach is not serious, the business or organization can keep operating on backup while the problem is addressed. IT security is as much about limiting the damage from breaches as it is about preventing them.

6. **Record, Record, Record**

   Ideally, a security system will never be breached, but when a security breach does take place, the event should be recorded. In fact, IT staff often record as much as they can, even when a breach isn't happening. Sometimes the causes of breaches aren't apparent after the fact, so it's important to have data to track backwards. Data from breaches will eventually help to improve the system and prevent future attacks.

7. **Run Frequent Tests**

   Hackers are constantly improving their craft, which means information security must evolve to keep up. IT professionals run tests, conduct risk assessments, reread the disaster recovery plan, check the business continuity plan in case of attack, and then do it all over again.

The Takeaway

IT security is a challenging job that requires attention to detail at the same time as it demands a higher-level awareness. However, like many tasks that seem complex at first glance, IT security can be broken down in to basic steps that can simplify the process. That's not to say it makes things easy, but it does keep IT professionals on their toes.

DO YOU WANT TO KNOW MORE? TALK TO US.

POC: MAJ JOEY T FONTIVEROS (INF) PA – Chief, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0917-628-1057.

.Reference:

This was cross-posted from https://www.techopedia.com.