Asian Legal Business: Philippine Data Privacy Forum

Breach Management: How to effectively prepare and respond to a data breach, from legal and technical perspectives

ANGEL "LITO" S. AVERIA, JR.

President

Philippine Computer Emergency Response Team

ASIAN LEGAL BUSINESS

the answer company™ THOMSON REUTERS®

phcert Philippine Computer Emergency Response Team

Manila Hall, Thomson Reuters Manila Office, 20 Building Upper McKinley Hill, Taguig City | August 10, 2017

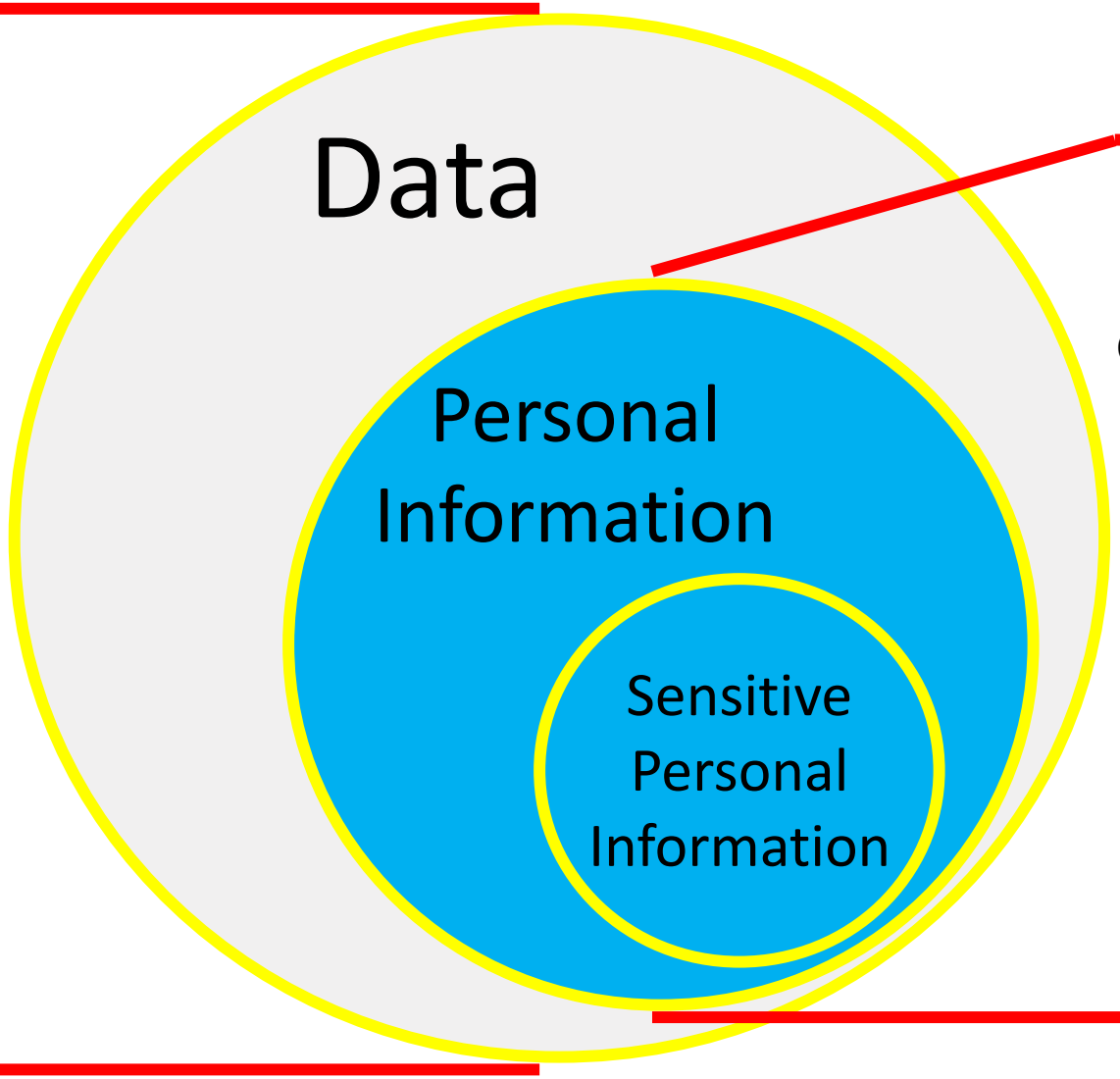
NPC's Data Privacy Compliance Roadmap

Data, Personal Information and Sensitive Personal Information

Information security concerns:

Confidentiality, Integrity, and Availability of data assets (includes data, software, and hardware)

Protection of Information Infrastructure and Data Assets by ensuring that policy & procedural, physical, organizational, and technical control measures are in place



Personal data protection concerns:

Confidentiality, Integrity, and Availability of personal information

Protection of Personal Information by ensuring that policy, physical, organizational, and technical measures are in place.

Accountability of personal data holders

Personal Information must be secured

The Data Privacy Act requires that the personal information and sensitive personal information be secured against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing. *(See Data Privacy Act Section 20)*

Image Source: https://www.grantmcgregor.co.uk/wp/wp-content/uploads/2016/01/DataProtection_ArticleImage.jpg

What is a security breach?

Security breach: The accidental or unlawful destruction, alteration and disclosure, as well as any other unlawful processing. *(See Data Privacy Act Section 20(a))*

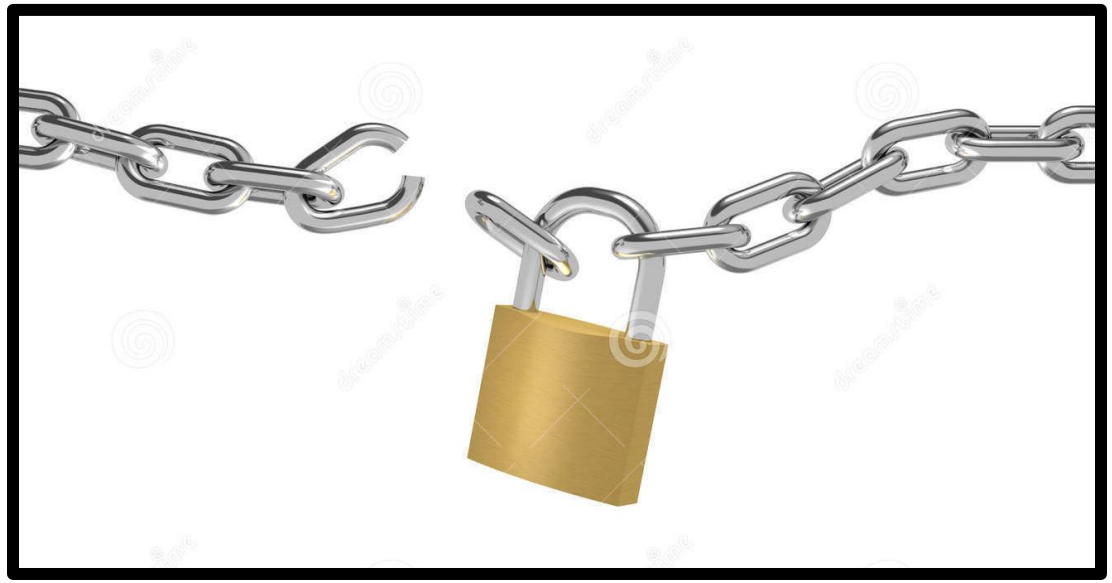


Image Source: https://thumbs.dreamstime.com/z/broken-chain-7130190.jpg

Security breach: paper-based documents or electronic documents

Image Sources: http://www.documentsystems.com/sites/default/files/imce/ts/block-document-solutions.jpg
http://life-registry.net/wp-content/uploads/2015/12/digital_documents__670-article.jpg

What will you do when it happens?

Image Source: http://cdn1.itpro.co.uk/sites/itpro/files/styles/article_main_wide_image/public/2/92//data_breach.jpg?itok=ZbPHSQN3

Notification is mandatory

The personal information controller shall **promptly** notify the Commission and affected data subjects x x x *(See: Data Privacy Act Sec. 20(f))*

"Promptly" = Within 72 hours

See: https://privacy.gov.ph/exercising-breach-reporting-procedures/

Image Source: https://openclipart.org/image/2400px/svg_to_png/3130/eastshores-Warning-Notification.png

Information required in the notification

The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach x x x

(See Data Privacy Act Sec. 20(f))

Image Source: https://www.google.com.ph/search?q=document+image&rlz=1C1CHZL_enPH738PH738&tbm=isch&tbo=u&source=univ&sa=X&ved=0ahUKEwjHgc_5vrXVAhUGKpQKHd9VADEQ7AkIRg&biw=1163&bih=559#imgrc=hMKzF8tkQMy9fM:

Breach response is not simply about complying with the law's notification requirements

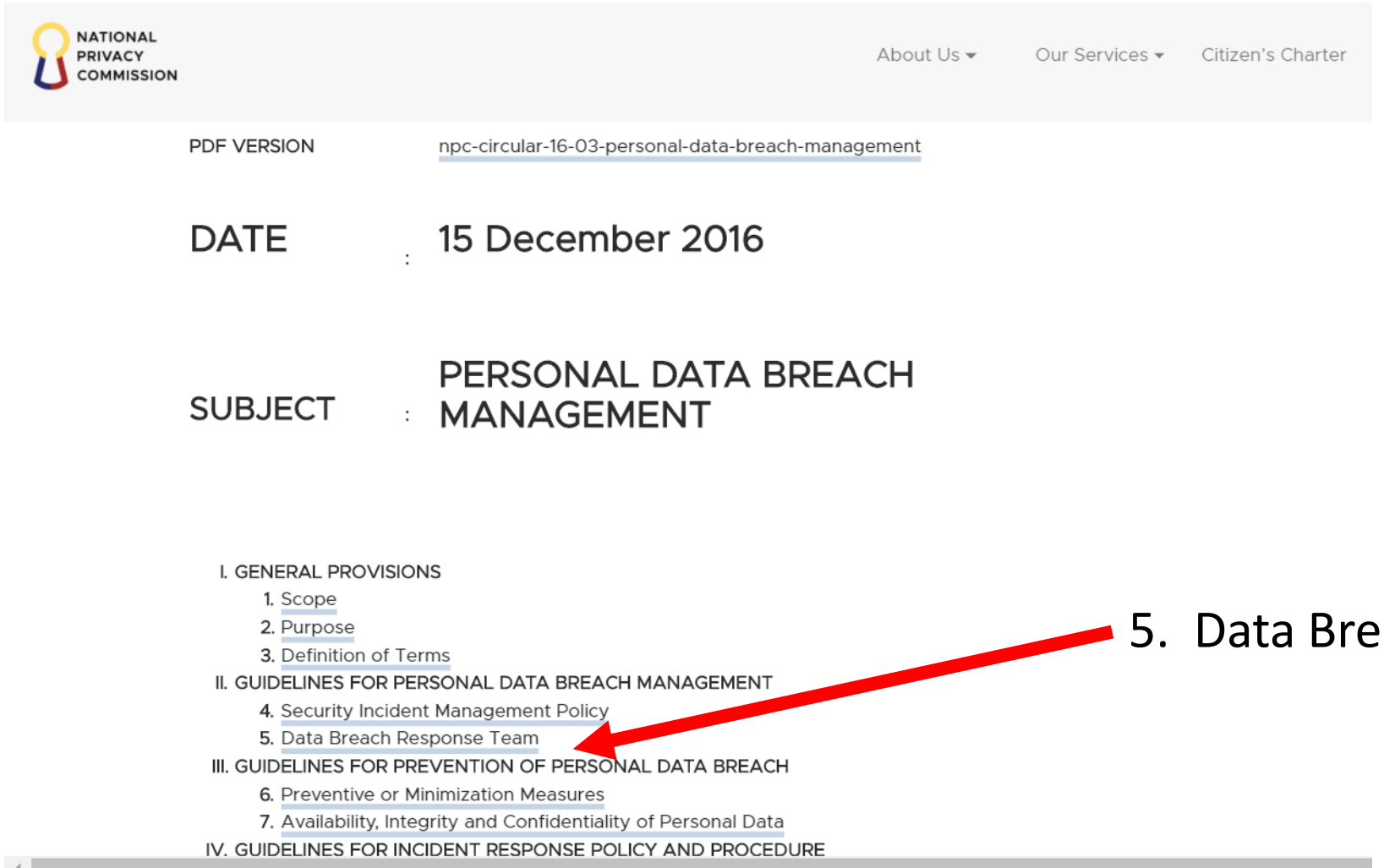
Breach response is about being prepared

Best practice: Have a team and a plan in place

Image Sources: https://www.google.com.ph/search?q=team+image&rlz=1C1CHZL_enPH738PH738&tbm=isch&tbo=u&source=univ&sa=X&ved=0ahUKEwjQ9oS6xLXVAhULj5QKHapnCV0Q7AkIQA&biw=1163&bih=559#imgdii=CGg2wFYbIohLOM:&imgrc=nfCz597LMr7DYM
http://www.istockphoto.com/photo/jigsaw-puzzle-on-blue-gm493959601-40910604

NPC Circular No. 16-03 Personal Data Breach Management

https://privacy.gov.ph/memorandum-circulars/npc-circular-16-03-personal-data-breach-management/



5. Data Breach Response Team

Why breach response?

Need to be prepared to mitigate or minimize impact of a data breach and quickly recover and restore business as usual mode

Data breach can lead to:

- Financial losses
- Cost of remediation
- Damage to reputation
- Personal losses - shareholders
- Legal costs, fines, and penalties

Image Source: http://www.arborinvestmentplanner.com/wp-content/uploads/2013/06/ProbableMaximumLoss.jpg

Why plan for a data breach response?

There is very little time to decide on anything

Coordinate and orchestrate response activities

Know what to do in the event of a data breach

Manage messaging >> management, customers, employees, legal (internal and external), regulatory agency, law enforcement, media

Image Source: http://www.socialmediaexaminer.com/wp-content/uploads/2013/06/hc-plan-istock-16596422.jpg

A team of teams

- ✓ IT and Security Team
- ✓ Public Relations and Notification Handling Team
- ✓ Help Desk and Customer Care Team
- ✓ Legal (int. and/or ext.)
- ✓ Vendors: Security, etc.

- ✓ Breach Response Planning Team
- ✓ Breach Response Training Team

Image Source: https://lindajohnsonleadership.files.wordpress.com/2015/05/team-building.jpg

IT and Security Team

Primary objectives:

Determine the nature, scope, and magnitude of the security breach.

Determine the corrective measures to be applied.

Restore the system to BAU mode.

Image Source: https://media.licdn.com/mpr/mpr/AAEAAQAAAAAAAAdCAAAAJDRhOGM0Y2VmLTI1ZGEtNDE0Ni1hYmU2LTliZmU3ODg1ZWVkMg.jpg

Public Relations and Notification Handling Team

Primary Objectives:

Serve as communications nerve center:

- Send notifications to National Privacy Commission and Affected Data Subjects.

Compose messages:

- Nature of the security breach
- Scope and magnitude of the security breach
- Remediation actions being undertaken
- Assurance to stakeholders

Prepare call scripts for Help Desk and Customer Care Team

Be the face of the company in front of stakeholders, including media.

Image Source: http://i.istockimg.com/file_thumbview_approve/10414009/3/stock-illustration-10414009-blue-bird-with-announcement-message.jpg

Help Desk and Customer Care Team

Primary objectives:

Receive and record calls of stakeholders, including customers.

Be the voice of the company.

Provide necessary assistance.

Deliver message of assurance.

Image Source: http://www.coredoc.net/wp-content/uploads/2016/08/help-desk.jpg

Legal Team

Primary Objectives:

Provide assistance to the other teams, especially where messaging is concerned.

Review all communications prior to release.

Take the lead role in reporting to law enforcement authorities, if necessary.

Image Source: https://s-media-cache-ak0.pinimg.com/originals/d4/9d/a0/d49da0be410de24fc67b8345c6630f01.jpg

Vendors Team

Primary Objectives:

Provide assistance in identifying latest vulnerabilities in the system that may have been missed or recently discovered (zero-day vulnerabilities).

Provide advise on what remedial actions may be taken.

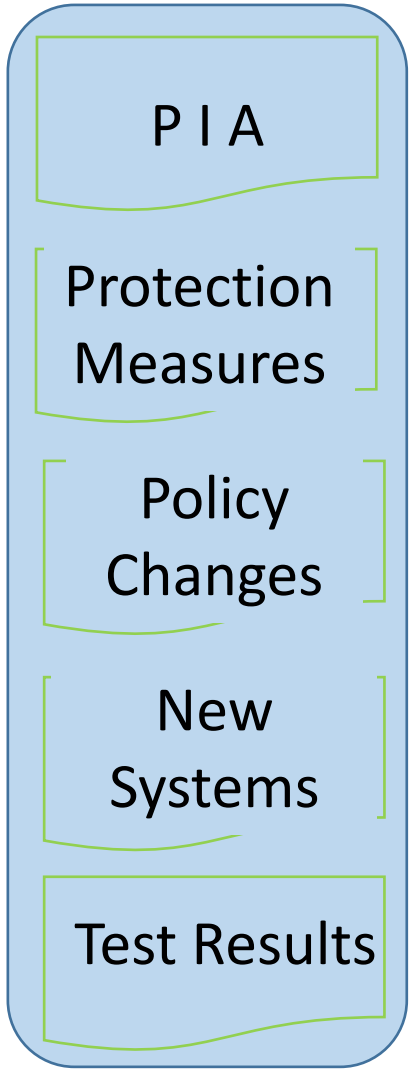
Image Source: http://workingatheight.us/cms/wp-content/uploads/2017/03/Vendor-Management.jpg

Breach Response Planning Team

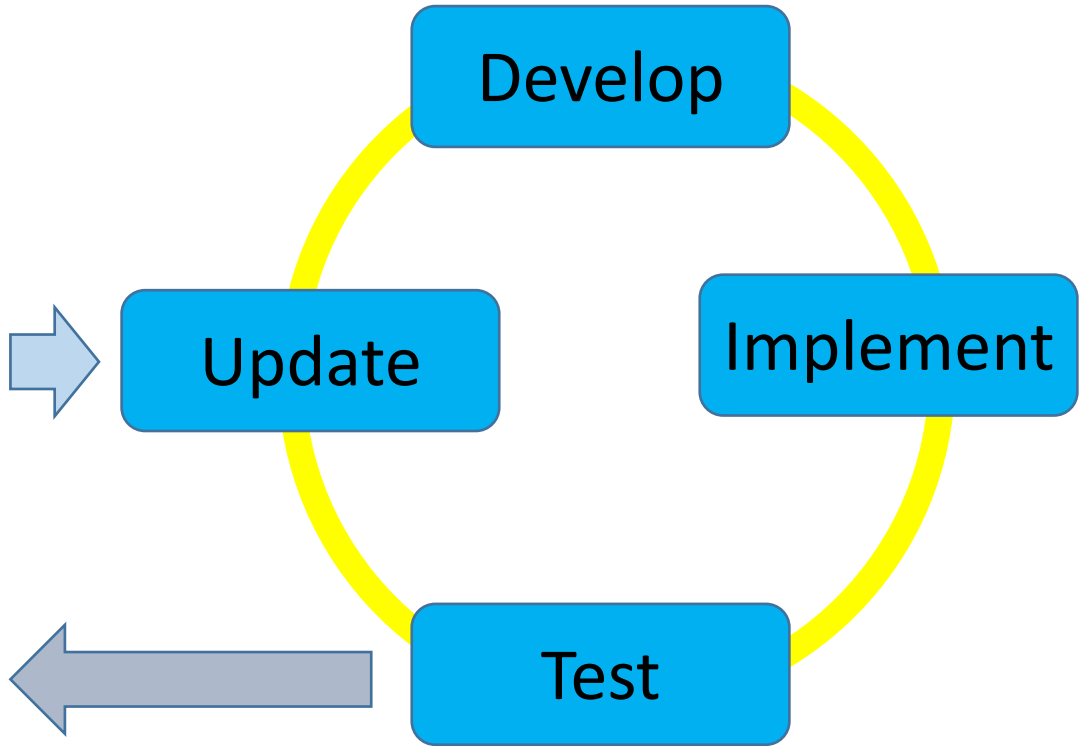
Primary Objectives:

Develop the Breach Response Plan

Maintain and update the Breach Response Plan



The Breach Response Plan is a living document. It must be exercised and updated as necessary.



Reference: Deming Cycle > Plan-Do-Check-Act

Breach Response Training Team

Primary Objectives:

Develop awareness program and conduct awareness sessions.

Develop capacity building programs and conduct education and skills development sessions.

Conduct drills and exercises

Image Source: https://3.imimg.com/data3/PR/TW/MY-13796177/placement-service-250x250.jpg

The Breach Response Team Lead

Primary Objectives:

Serve as link to senior management.

Ensure proper communication, coordination, and cooperation between and among the teams.

Take the lead in developing and maintaining the Breach Response Plan.

Conduct post breach debriefing.

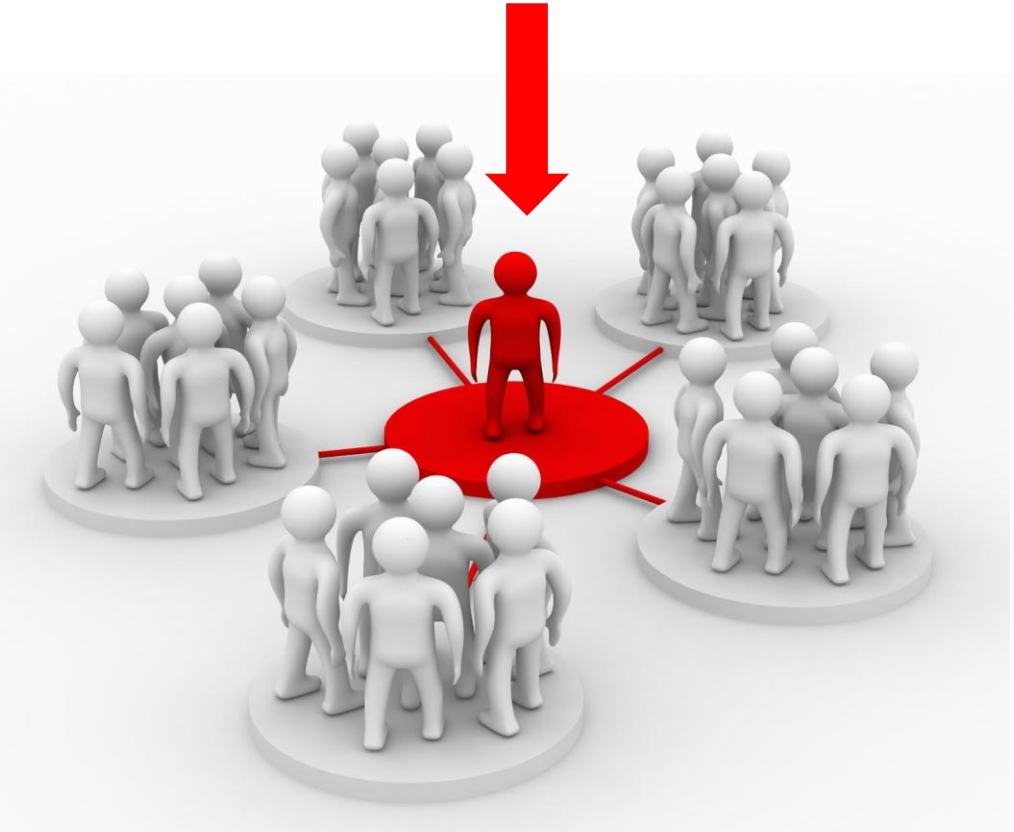


Image Source: https://lindajohnsonleadership.files.wordpress.com/2015/05/team-building.jpg

Angel “lito” S. Averia, Jr.

President, Philippine Computer Emergency Response Team (PhCERT)

ICT Consultant

Business Continuity Planner

Lecturer and Workshop Facilitator: Cybercrime, Data Protection, Disaster Recovery and Business Continuity

Tel. No. +63 905 424 2026

Email: lito.averia@gmail.com