GROUP 2: PLANNING FOR SECURITY (Chapter 5)

Presentation - September 28, 2024
Script Deadline -

Concept Options

- S.O.C.O.
  - Stands for:
    - Security Organization in Computers Operatives
    - Security Of Computer Operatives
    - Security Optimization for Computer Operations
    - Specialists Of Cybersecurity Operations
  - Concept: Scenarios showing lack of computer security + discussion on how to plan for security
    - Recorded videos showing a case to investigate
      - Suggestion as intro: I love you virus (walang policy sa ph abt cybersecurity) — show its effects
      - Main case: iaact natin
    - Live (with some recorded portion) discussing the slides
    - Mini activity for the class (example: quick questions & text the answer or interviews)

(1) Main video editor / visuals - **nigel** (assist in ppt: gwy)
(1) Scriptwriter - **gwy**
(1) Anchor/Host - **Kyle**
(2) Specialist - **Edjin**, **Mark (kung okeee lng po hehe)**
(2) Actors (who will assist in script writing) - **Jc, Charles**

Flow [from show: video]

- Intro
  - Background about cybersecurity in ph
  - Host will enter/speak
- Main Act (Part 1)
  - Case story preview (recorded)
  - Interview with guest (pwedeng live?)
  - Anchor discussing the issue/case and conducting some investigation??
- Commercial/Game
- Discussion
  - Specialist and anchor will discuss steps to solve the case (connect sa slides discussion!)
- Main Act (Part 2)

    - Interview again with guest and/or other persons involved in issue
    - Fast forward to solution to case (applying lessons) (recorded)
- Ending
    - Anchor will summarize the case and insights gained
    - Announcement of game winner ???
    - Ending animation

Script

[Overview]:

In the virtual world of Roblax, Chat to Impress is the latest social media game sensation. CTI allows players to create virtual avatars and engage in over-the-top conversations. Players can chat, compete in dress up challenges, and even throw digital parties. The app's charm has made it a hit among Roblax enthusiasts. However, recently, the CTI office has encountered a cyberattack. The cyberattack has exposed the private conversations of those who play CTI, and has also leaked their emails, hence revealing their personalities. One of the victims is a famous TV personality.

The famous actor went to SOCO (Specialists Of Cybersecurity Operations) to complain about what happened to the game. The SOCO team communicated with the owners and developers of CTI, to uncover details about the breach. They also reached out with the police to find the suspect. While the host and the police team investigates, the host calls an expert to teach the owner of CTI, about Security Planning to avoid any of the attacks happening.

[Characters]

- Gus Abelgas (Host) - Kyle
- Cyber Security Specialists - Edjin, Mark
- Owner/Founder of CTI - Charles
- Celebrity - Victim of the Information Leak - Jc

[Scene 1]

Recorded

[**Show**: Clips about I love you virus]

Narrator (Voiceover):

In May of 2000, the world was introduced to a new kind of cyber threat. It began with a seemingly innocent email attachment, but what followed was anything but ordinary.

A young hacker from the Philippines, Onel de Guzman, created an email worm that would forever alter the landscape of cybersecurity. Known as the 'ILOVEYOU' virus, this malicious code spread like wildfire, infecting around 45 million Windows computers worldwide.

ILOVEYOU wasn't just another computer virus; it was a wake-up call. The worm's reach extended to about 10% of the world's internet-connected computers, creating chaos and disruption on a scale previously unimaginable. The Department of Defense, among many others, was caught completely off guard.

The consequences were severe. Billions of dollars were spent on mitigation, repairs, and lost productivity. The worm's brief yet devastating reign underscored a harsh reality: the world was unprepared for the new age of malware and hacking.

The fear and urgency sparked by this incident ignited a global movement towards enhanced cybersecurity.

That's why — we are now here to investigate cyberattacks and plan for security. We are SOCO (Specialists of Cybersecurity Operations)

fade

[Show: Animation Video of SOCO]

[Show: Animation: "Episode 1: Chat to Impress – HackED?"

[Scene 2]

Recorded ▾

[Show: Scenes of Random People praying dress to impress and some clips from game**]**

Host (Voiceover): Sa virtual na mundo ng Roblax, ang Chat to Impress ay ang pinakabagong social media game sensation. Ang CTI ay nagbibigay daan sa mga manlalaro na lumikha ng kanilang sariling mga virtual avatar, at makipag-chat sa kanilang mga kaibigan habang sumasali sa mga dress-up challenge, at themed parties.

- Youtube scenes

[Show: Clip na kunwari hinahack - kahit kunwari may tinatype lang sa keyboard din magaappear na may access na sa game or something**]**

Host (voiceover): Ngunit kamakailan lamang, ang CTI office ay nakaranas ng isang cyberattack. Ang pag-atake na ito ay nagbunyag ng mga pribadong usapan ng mga manlalaro ng CTI at na-leak din ang kanilang mga email, na nagbigay-daan upang malaman ang kanilang mga personalidad.

-

fade

[Show: Clip nung actor na nakatalikod or shadow lang or yung iba sa mata or bibig lang example: https://youtu.be/IJCPqCnTwTY?si=4QGBiwszpm0sTLWW **]**

Host (voiceover) Isa sa mga biktima ay ang sikat na TV personality na si Jc Aguilar. Siya ay pumunta sa SOCO (Specialists of Cybersecurity Operations) upang magreklamo tungkol sa nangyari sa laro.

Jc (video): Around this time last week, nagising na lang ako na trending na ang pangalan ko. Akala ko dahil lang sa sikat na movie ko or commercial or something pero pinaguusapan lang pala yung mga chat ko sa Chat to Impress.

Sobrang disappointed ako kasi grabe yung tiwala ko sa game. Akala ko pa naman eto na yung hinahanap kong platform para maging chill lang ako for once in my life and mag-enjoy nang walang iniisip na audience.

[Show: Clips na kunwari na-leak yung messages and maraming tweets about kay actor

// fake tweets generator??? HAHAH **Caption:** Pagsasadula **]**

Jc (video): Sana mabigyan ng justice 'to kasi privacy ko at ng ibang users ang pinag-uusapan eh. We have the rights to be protected and stay anonymous kung gugustuhin namin. Tingin ko problema na to ng Chat to Impress group — except syempre sa hackers, kailangan maging responsable ang Chat to Impress kasi hindi secured yung larong ginawa nila.

fade

[Show: Clip ulit nung owner na nakatalikod or shadow lang or yung iba sa mata or bibig lang example: https://youtu.be/IJCPqCnTwTY?si=4QGBiwszpm0sTLWW **]**

Host (voiceover) : Bilang head ng Chat to Impress, ano po ang masasabi ninyo?

Charles (video): Humihingi ako ng tawad kay Sir Jc and sa ibang naging biktima. Inaamin kong pagkakamali rin namin ang nangyari. Naging priority namin ang pagpapaganda ng laro at kinulang kami sa security planning…

[Scene 3]

Live ▾

Host: Nakita na nga natin kung ano ang nangyari kay Mr. Jc Aguilar. Bago pa lumapit ang aktor sa SOCO team, ang kaso ng CTI ay nailapit na rin sa legal investigation team. Ayon sa aking sources, patuloy ang kanilang pag-alam kung sino nga ba ang nagpasimula ng cyberattack at nag-leak ng mga personal na impormasyon.

Pero ang isa pang malaking tanong ay kung paano makaka-recover ang Chat to Impress sa nangyaring cyberattack. For sure, malaki ang epekto nito sa kanila at sa kanilang operation processes.

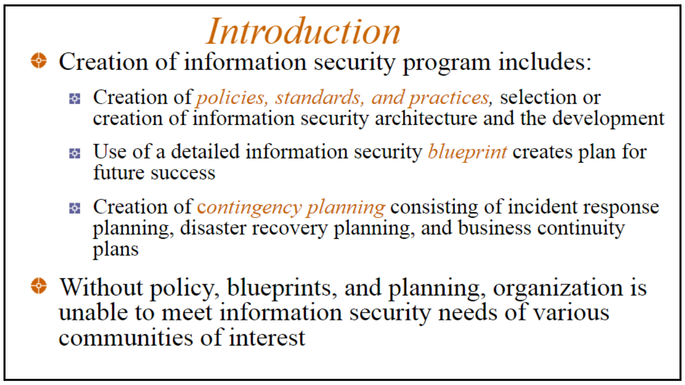
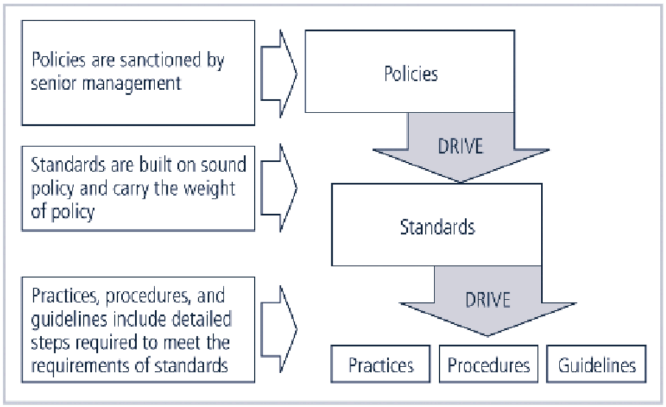
Kaya naman, tawagin natin ngayon ang aking partner, ang eksperto sa Computer Security, si Edjin Payumo!

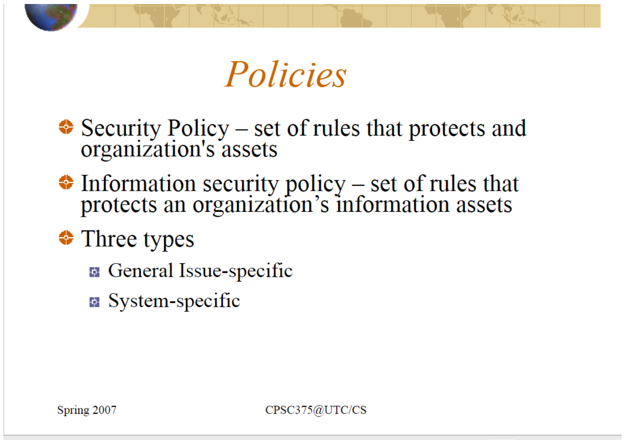
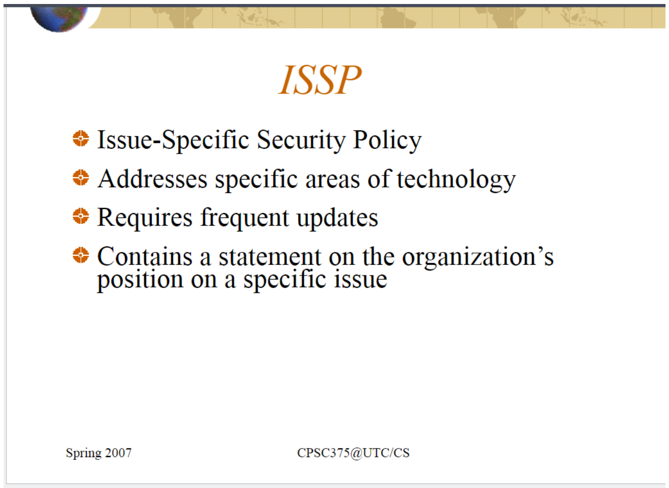
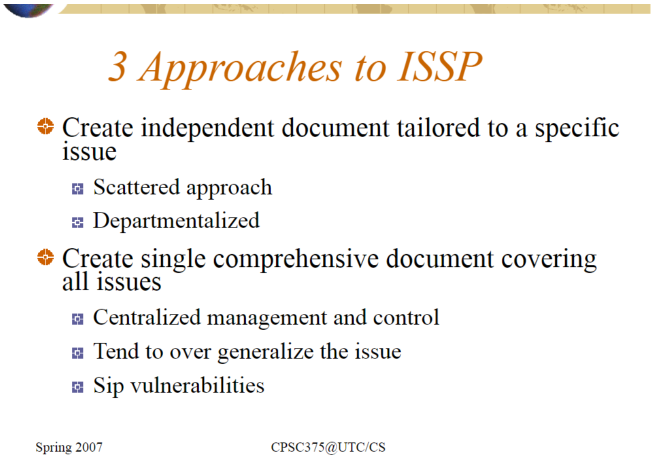
Edjin: Magandang hapon sa inyong lahat!

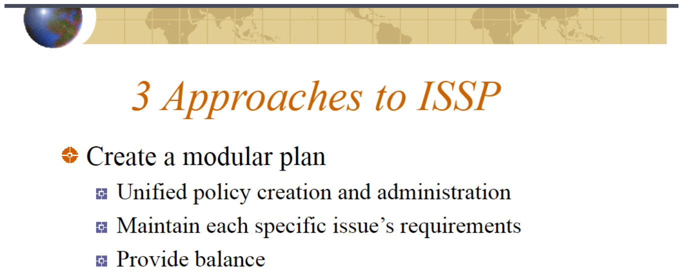
Host: Magandang hapon, partner! Kanina lang ay napanood natin ang pahayag ni Actor 1 at ang nangyaring cyberattack sa Chat to Impress. Sa iyong palagay, ano kaya ang dapat gawin ng mga creator ng CTI upang malampasan ang pagsubok na ito.

Edjin: Isang malaking problema nga ang nangyaring iyon, partner. At sa tingin ko, bago ang lahat, dapat munang matutunan ng creator ng CTI kung paano magkaroon ng Information Security Program.

shows PPT slides

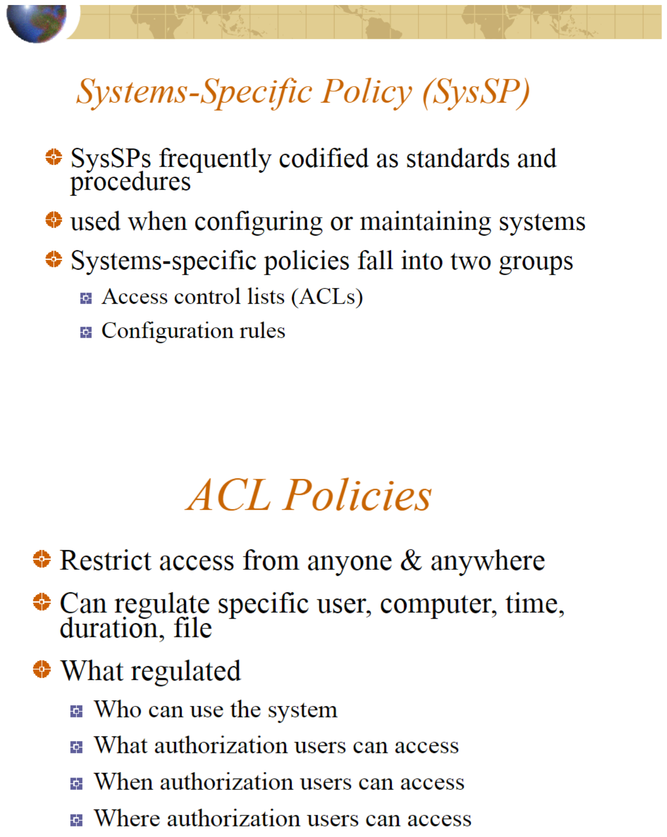
 *Introduction* - Creation of information security program includes: - Creation of *policies, standards, and practices*, selection or creation of information security architecture and the development - Use of a detailed information security *blueprint* creates plan for future success - Creation of *contingency planning* consisting of incident response planning, disaster recovery planning, and business continuity plans - Without policy, blueprints, and planning, organization is unable to meet information security needs of various communities of interest	**Edjin**: Upang makagawa ng Information Security Program, kailangan nila gumawa ng policies, standards, and practices. Syempre, dapat meron ding detailed information security blueprint at contingency planning consisting of incident response planning, disaster recovery planning, at business continuity plans. Kung wala ang mga ito, hindi magiging maayos ang information security.
 Policies are sanctioned by senior management Standards are built on sound policy and carry the weight of policy Practices, procedures, and guidelines include detailed steps required to meet the requirements of standards Policies DRIVE Standards DRIVE Practices Procedures Guidelines	**Host**: Tama yan. And take note, mga manonood — ang mga polisiya o policies ay pinagtibay ng senior management; ang standards ay nakabase sa polisiya at may parehong bigat ng polisiya; habang ang mga practices, procedures, at guidelines naman ay naglalaman ng mga detalyadong hakbang para matugunan ang mga kinakailangang requirements ng standards. Sa maikling salita, kung titingnan natin ang larawan: Policies drive Standards, and Standards drive Practices,

	Procedures, and Guidelines.
 **Policies** - Security Policy – set of rules that protects and organization's assets - Information security policy – set of rules that protects an organization's information assets - Three types - General Issue-specific - System-specific Spring 2007 CPSC375@UTC/CS	**Edjin**: Meron tayong iba't ibang policy. Una, merong Security Policy, o yung set of rules na pumoprotekta sa assets ng isang organization, at Information Security Policy na naka-focus naman sa information assets ng organization. At di lang diyan natatapos, meron ding General Issue-specific at System-specific policies.
 **ISSP** - Issue-Specific Security Policy - Addresses specific areas of technology - Requires frequent updates - Contains a statement on the organization's position on a specific issue Spring 2007 CPSC375@UTC/CS  **3 Approaches to ISSP** - Create independent document tailored to a specific issue - Scattered approach - Departmentalized - Create single comprehensive document covering all issues - Centralized management and control - Tend to over generalize the issue - Sip vulnerabilities Spring 2007 CPSC375@UTC/CS	**Edjin**: Sa kaso ng CTI, tingin ko dapat nilang malaman ang ISSP o Issue-Specifc Securty Policy. May tatlong approaches to ISSP, una ay ang paggawa ng independent document tailored to a specific issue; pangalawa, single comprehensive document na tumatalakay sa lahat ng issue; at huli, isang modular plan na naglalaman ng unified policy creation and administration.



3 Approaches to ISSP

- Create a modular plan
  - Unified policy creation and administration
  - Maintain each specific issue’s requirements
  - Provide balance



Systems-Specific Policy (SysSP)

- SysSPs frequently codified as standards and procedures
- used when configuring or maintaining systems
- Systems-specific policies fall into two groups
  - Access control lists (ACLs)
  - Configuration rules

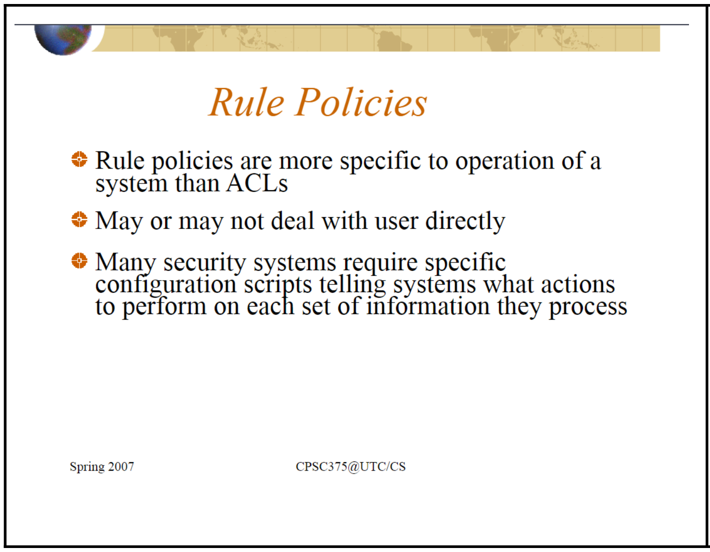
ACL Policies

- Restrict access from anyone & anywhere
- Can regulate specific user, computer, time, duration, file
- What regulated
  - Who can use the system
  - What authorization users can access
  - When authorization users can access
  - Where authorization users can access

Host: Kung ang kanilang problema naman ay systems-specific, dapat din silang gumawa ng Systems-Specifc Policy o SysSP; kung saan maaari silang gumawa ng Access control lists (ACLs) at Configuration Rules.

ACL Policies can regulate specifc user, computer, time, duration, file. Dito, malalaman kung sino, ano, kailan, at saan ang maaaccess ng authorization users.

Habang ang Rule Policies naman ay policies na mas specific sa operasyon ng isang system kumpara sa ACLs. Maraming security systems ang nangangailangan nitong specific na configuration scripts.



Rule Policies

- Rule policies are more specific to operation of a system than ACLs
- May or may not deal with user directly
- Many security systems require specific configuration scripts telling systems what actions to perform on each set of information they process

Spring 2007 CPSC375@UTC/CS

....

[Scene 4]

Live
Host: Napakahusay ng pagpapaliwanag mo, partner! Sana ay maraming natutunan ang mga nakikinig sa atin ngayon, lalo na ang mga businesses at companies na hindi pa alam kung paano simulan ang Planning for Security. Huwag kayong mag-alala, mga manonood dahil marami pa kayong matutunan, sa pagbabalik ng SOCO (Specialists of Cybersecurity Operatives)!

Recorded
[Show: Question and answer slide] **Narrator (Voiceover)**: Kapamilya, eto na ang pagkakataon mo upang manalo ng Brand New Gaming Laptop at 100,000 worth of Robux! Sagutin mo lang ang SOCO questions of the day

at ipadala ang iyong sagot sa 2366!

1. It is the basis for design, selection, and implementation of all security policies, education and training programs, and technological controls
   a. Information Policy Blueprint
   b. Security Blueprint
   c. Information Policy Framework
   d. Security Framework
2. The following are approaches to ISSP except ______?
   a. Create a modular plan
   b. Creare single comprehensive document covering all issues
   c. Create access control lists
   d. Create independent document tailored to a specific issue
3. What is SETA
   a. Security Education, Training and Awareness
   b. Security Education, Teaching and Awareness
   c. Security Education, Training and Application
   d. Security Evaluation, Training and Awareness

// scan google form tapos paunahan na lang kung sino yung makakasagot nung tatlo. One google form for each ques para iba iba yung mananalo

Live ▾

Host: Mga kapamilya, welcome back! Ngayon ay tawagin na natin ang mga nanalo sa SOCO questions of the day!

call winners

flash correct answers

Host: Makikita niyo sa ating screen ang tamang sagot sa mga SOCO questions. Maraming salamat sa inyo at congratulations. Narito ang inyong premyo!

picture taking

Host: Mukhang natuto na ang ating manonood sa Security Planning Discussion namin ni Edjin! Natuto naman kaya ang Chat to Impress Group, lalo na si Mr. Charles De Lara? Tawagin natin siya ngayon!

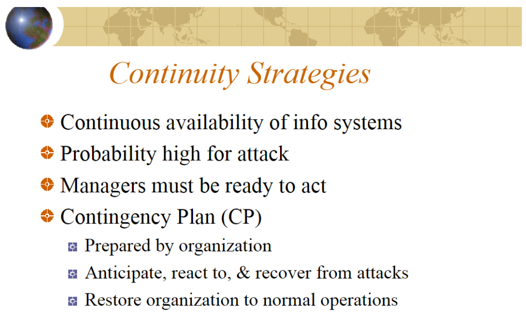
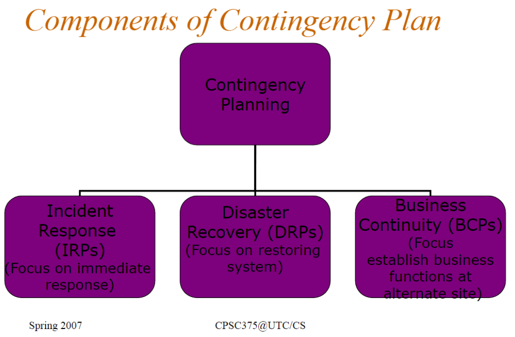
[Scene 5]

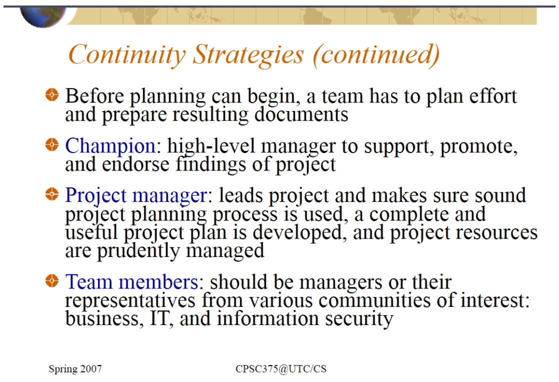
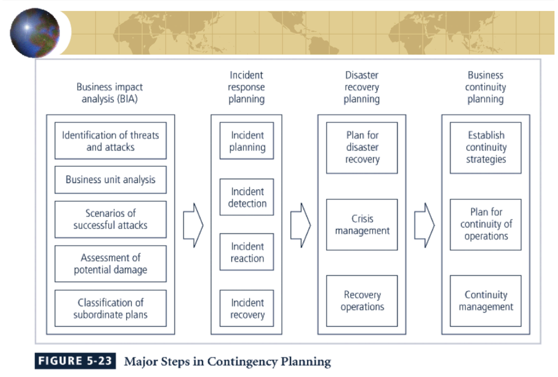
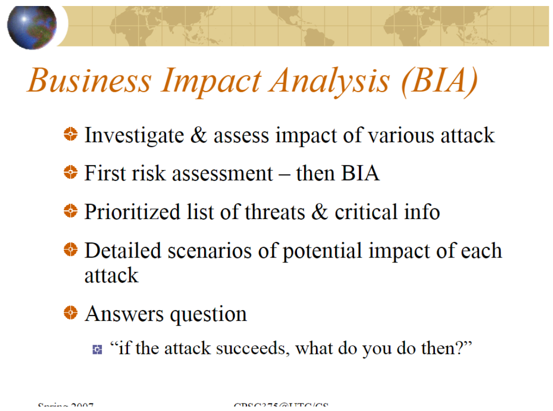
Live ▾

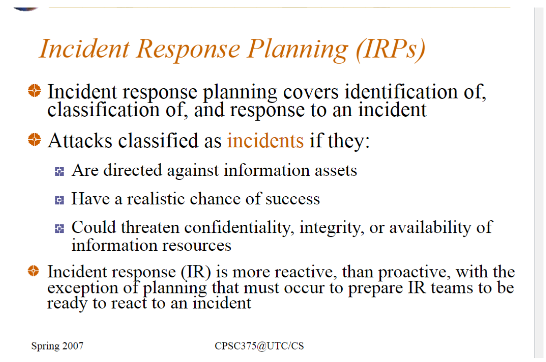
Charles: Magandang hapon po!

Host:Magandang hapon, Mr. de Lara! Balita ko ay dumalo na daw kayo sa isang Security Planning Seminar. Ngayon naman ay makakausap ninyo ang isa pang eksperto sa Computer Security na kasama rin natin ngayon, si _________.

Mr. de Lara, maaari niyo bang ibahagi dito sa SOCO kung ano ang mga alam niyong continuity strategies?

 *Continuity Strategies* - Continuous availability of info systems - Probability high for attack - Managers must be ready to act - Contingency Plan (CP) - Prepared by organization - Anticipate, react to, & recover from attacks - Restore organization to normal operations	**Charles:** Natutunan ko po ang isa sa mga continuity strategies, ang pagkakaroon ng Contingency Plan, kung saan ang organization po namin ay dapat magplano kung paano i-anticipate yung mga attacks, paano mag-react sa mga ito, at kung paano na rin makarecover at makabalik sa aming normal operations.
 *Components of Contingency Plan* Contingency Planning Incident Response (IRPs) (Focus on immediate response) Disaster Recovery (DRPs) (Focus on restoring system) Business Continuity (BCPs) (Focus establish business functions at alternate site) Spring 2007 CPSC375@UTC/CS	**Expert 2**: Tama po ‘yan. Dagdag ko lang po, under ng Contingency Planning ay merong Incident Response (IRPs), Disaster Recovery (DRPs), at Business Continuity (BCPs). Familiar na po ba kayo rito, sir?

 *Continuity Strategies (continued)* - Before planning can begin, a team has to plan effort and prepare resulting documents - Champion: high-level manager to support, promote, and endorse findings of project - Project manager: leads project and makes sure sound project planning process is used, a complete and useful project plan is developed, and project resources are prudently managed - Team members: should be managers or their representatives from various communities of interest: business, IT, and information security Spring 2007 CPSC375@UTC/CS	**Charles:** Opo, kasalukuyan ko na rin po itong pinag-aaralan. Naghahanda na rin po kami ng mga resulting documents. **Expert 2:** Mabuti naman po, at dapat mayroon din kayong mga assigned persons, lalo na po yung tinatawag na champion, isang high-level manager na sumusuporta, nagpo-promote, at nag-eendorso ng mga findings ng project; project manager na tumitiyak na maayos na na-manage ang mga project resources; at mga team members na galing sa business, IT, at information security.
 Business impact analysis (BIA): Identification of threats and attacks; Business unit analysis; Scenarios of successful attacks; Assessment of potential damage; Classification of subordinate plans Incident response planning: Incident planning; Incident detection; Incident reaction; Incident recovery Disaster recovery planning: Plan for disaster recovery; Crisis management; Recovery operations Business continuity planning: Establish continuity strategies; Plan for continuity of operations; Continuity management **FIGURE 5-23** Major Steps in Contingency Planning  *Business Impact Analysis (BIA)* - Investigate & assess impact of various attack - First risk assessment – then BIA - Prioritized list of threats & critical info - Detailed scenarios of potential impact of each attack - Answers question - "if the attack succeeds, what do you do then?" Spring 2007 CPSC375@UTC/CS	**Expert 2**: At dahil nabanggit niyo na rin po kanina, siguro naman po ay ginagawa niyo na itong mga major steps in contingency planning. Simula na sa Business Impact Analysis (BIA), naassess niyo na ba ang impact ng nangyaring attack? Nasagot niyo na ba ang tanong na "If the attack succeeds, what do you do then?" **Charles:** Opo. After po ng risk assessment ay tinitingnan na po namin ang impact nito sa aming business. Inaasikaso na po ng team ko kung paano namin haharapin ang naging impact ng attack.

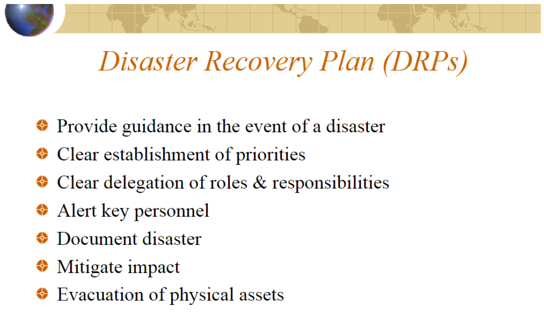


Incident Response Planning (IRPs)

- Incident response planning covers identification of, classification of, and response to an incident
- Attacks classified as incidents if they:
  - Are directed against information assets
  - Have a realistic chance of success
  - Could threaten confidentiality, integrity, or availability of information resources
- Incident response (IR) is more reactive, than proactive, with the exception of planning that must occur to prepare IR teams to be ready to react to an incident

Spring 2007 CPSC375@UTC/CS

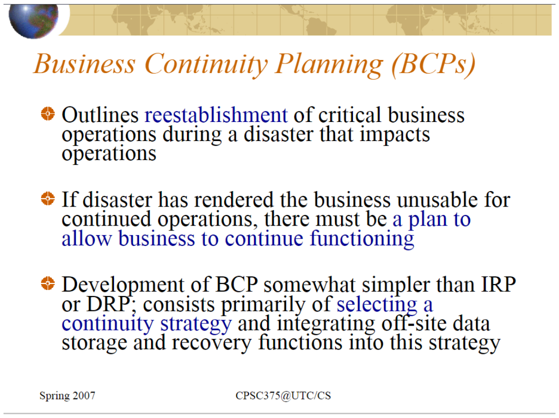
Expert 2: Tama po yan! Pagkatapos ng BIA, siguro ay dapat niyo na rin gawin ang Incident Response Planning. Iyo po ay reactive planning kung saan ang mga IR teams ay hinahanda ninyo kung paano magreact sa incident. Kasama na sa bahaging ito ang Incident Planning, Incident Detection, Incident Reaction, and Incident Recovery. Take note lang na ang nangyari sa inyo ay matuturing na isang incident dahil ito ay directed against information assets and it threatens the confidentiality, integrity, and availability of information resources.



Disaster Recovery Plan (DRPs)

- Provide guidance in the event of a disaster
- Clear establishment of priorities
- Clear delegation of roles & responsibilities
- Alert key personnel
- Document disaster
- Mitigate impact
- Evacuation of physical assets

Expert 2: Dagdag kaalaman lang din, in case po na may mangyari namang disaster. Dapat din po kayo magkaron ng Disaster Recovery Plan kung saan may clear delegation ng roles and responsibilities, plan to mitigate impact, evacuation of physical assets, at iba pa.



Business Continuity Planning (BCPs)

- Outlines reestablishment of critical business operations during a disaster that impacts operations
- If disaster has rendered the business unusable for continued operations, there must be a plan to allow business to continue functioning
- Development of BCP somewhat simpler than IRP or DRP; consists primarily of selecting a continuity strategy and integrating off-site data storage and recovery functions into this strategy

Spring 2007 CPSC375@UTC/CS

Charles: Noted po, sir. Sisiguraduhin ko po na magagawa ko po ang mga ‘yan lalo na po ang Business Continuity Planning kung saan naka-outline po ang reestablishment of critical business operations and plan para po magpatuloy ang functioning ng aming operations.

Host: Mabuti at marami na kayong natutunan, sir. Sure akong malalampasan niyo rin ang nangyaring attack at maiiwasan niyo na sa susunod dahil alam niyo na ang mga steps ng Security Planning! Salamat po sa inyong pagpunta.

At syempre, maraming salamat din sa ating Cybersecurity specialists, Mr. Edjin Payumo and Mr. _________ sa makabuluhang impormasyon na hatid mo ngayong araw.

Mga kapamilya at manonood ng SOCO, narito po ang recap ng mga impormasyong natutunan natin ngayong episode:

[Scene 6]

Recorded ▾

Narrator (Voiceover):

Para sa maintenance at pagpapatupad ng information security policy, standards, practices, procedures, at guidelines, mahalaga ang matibay na plano. Ang tinatawag nating **Information Security Blueprint** ay isang dokumento na nagsisilbing gabay sa disenyo, pagpili, at implementasyon ng lahat ng security policies, education at training programs, at pati na rin ang mga technological controls.

Mahalaga rin ang **Information Security education, training, and awareness (SETA)**. Isa itong control measure na nakakatulong para mabawasan ang mga aksidenteng security breaches at palakasin ang depensa ng organisasyon laban sa iba't ibang uri ng mga atake.

At syempre, kasama rin sa mga mahahalagang aspeto ng security ay ang **Contingency Planning (CP)**, na binubuo ng tatlong bahagi: ang **Incident Response Planning (IRP)**, **Disaster Recovery Planning (DRP)**, at **Business Continuity Planning (BCP)**. Ang mga ito ay mahalaga upang mapanatili ang operasyon at seguridad ng isang organisasyon kahit sa oras ng mga di-inaasahang pangyayari.

Kung kayo ay interesado pa sa topic na ito, i-scan niyo lamang ang QR code upang basahin ang buong talakayin!

Live ▾

Host: Muli, maraming salamat sa inyong pagsubaybay sa SOCO. Kami, ang Specialists of Cybersecurity Operatives, na laging nasa inyong serbisyo.

Sa mga sitwasyon kung saan may banta sa inyong cybersecurity, huwag mag-atubiling makipag-ugnayan sa amin. Nandito kami para magbigay ng gabay, solusyon, at kaalaman upang maprotektahan ang inyong mga digital na ari-arian.

Tandaan, ang proteksyon ng impormasyon ay hindi lamang responsibilidad ng isang tao—ito ay isang sama-samang pagsusumikap ng bawat miyembro ng isang organisasyon. Kaya naman, huwag kalimutang sundin ang ating mga itinakdang polisiya, standard, at guidelines upang maiwasan ang anumang insidente ng cyber attack.

Sa ngalan ng buong SOCO team, muli po kaming nagpapasalamat at nagpapaalala—Stay safe, stay secure, at maging laging handa sa anumang hamon sa mundo ng cybersecurity!

Hanggang sa susunod na episode, ako si Gus Abelgas, at ito ang SOCO!