# Response Strategies

Module 15

# Introduction

- Protections will fail
- We know this and are looking for signs
- What are we going to do when mechanisms fail or controls are defeated?
  - In other words, what are we going to do when we experience an incident?
- We respond
  - But, how?
- ~~That is the topic of this module~~

Copyright 2013 Iowa State University

# Response Strategy

- Incidents can occur at anytime
- Incidents can be minor (e.g. account lockout)
- Incidents can be major (e.g. compromise of sensitive database)
- Having a strategy will facilitate:
  - Managing impact and risk
  - Managing expectations
  - Managing costs

Copyright 2013 Iowa State University

# Response Strategy

- An overall strategy should be developed to set priorities and lines of communication
- Different incident types may require different focused strategies
- Not all incidents can be anticipated, but you should anticipate developing a response plan quickly

Copyright 2013 Iowa State University

# Conceptual Strategies

- Resilience
- Block/Deny
- Evaluate, Contain, Eradicate, Recover
- Offensive Response (aka Hack Back)
  - Orlando Doctrine

Copyright 2013 Iowa State University

# Resilience

- Two definitions
  - 1. An ability to spring back into shape
  - 2. An ability to recover quickly from adverse events
    - New American Oxford Dictionary 3rd Edition, Oxford University Press
- Automated recovery can help with springing back into “shape”
- Prompt intervention can result in resilience

Copyright 2013 Iowa State University

# Resilience

- Redundancy can help with automated recovery
  - Hardware solutions
    - Multiple power supplies
    - Error Correcting Code (ECC) memory
    - RAID (Redundant Array of Inexpensive Disks)
    - Multiple network cards
    - Multiple network paths
    - Server clustering
    - Dynamic capacity provisioning
    - Distributed services architecture
    - Multiple points of Internet presence or data centers

Copyright 2013 Iowa State University

# Resilience

- Controls architecture
  - Defense in Depth
  - Effective prevention
    - E.g. Antivirus detects and cleans malware
    - E.g. Patches that remediate relevant vulnerabilities
  - Automated-controls policy adjustment
    - Tricky, are policy adjustments appropriate?
- Second definition - quick recovery
  - Implies impact of incident not prevented
  - However, impact was minimized by swift response and fault tolerance

Copyright 2013 Iowa State University

# Resilience

- Risk management strongly influences resilience
  - Spending and labor investments will be prioritized based on risk
- Often resilience is introduced by increasing complexity
  - Complexity results in more opportunities for operational and security failure if the “solution” is not designed, implemented and managed properly

Copyright 2013 Iowa State University

# Block/Deny

- Strategy: Limit further exposure
  - By denying selected sessions/sources further access
    - Changing network access control policy
    - Changing identity and access management policy
  - Taking service offline
    - Removing host from network
    - Stopping specific services
    - Rebuilding host without regard to establishing an alternate platform to host the services being disabled.

Copyright 2013 Iowa State University

# Evaluate, Contain, Eradicate, Recover

- Preventative and automated resilience have failed or are not relevant
- Strict blocking is not acceptable
- We need a more comprehensive strategy
  - Evaluate, Contain, Eradicate, Recover is a framework
  - After identifying the incident's nature (Evaluate) a more specialized approach to executing Contain, Eradicate and Recover can be taken

Copyright 2013 Iowa State University

# Evaluate, Contain, Eradicate, Recover

- Evaluate
  - Determine the scope
    - Symptoms or indicators help
    - Understanding the technical environment helps with knowing:
      - How are things related.
      - What relevant trust relationships exist.
      - What do things have in common.
  - Investigate the likely root cause
    - Symptoms or indicators help with developing hypothesis

Copyright 2013 Iowa State University

# Evaluate, Contain, Eradicate, Recover

- Evaluate
  - Root cause can be thought as a combination of:
    - Vector of attack
    - Exploited vulnerabilities
    - Method of attack
    - Source of attack
      - Accurate attribution is not so important within response
        - » Data leading to attribution may need to be collected during response to avoid data loss and corruption
      - However, differentiating the source as an insider or outsider is important
        - » An insider is better able to compensate and continue to press the attack or back off and return.

Copyright 2013 Iowa State University

# Evaluate, Contain, Eradicate, Recover

- Contain
  - Limit the attack from spreading
  - Stop the attack from continuing
    - Some attacks are discovered after the attack has gone dormant or the attack has shifted into a stealthy phase.
  - Patch unaffected systems before the attack reaches them
    - An attack conducted “live” may adapt to the change to the remaining attack surfaces

Copyright 2013 Iowa State University

# Evaluate, Contain, Eradicate, Recover

- Eradicate
  - Remove malware and footholds (e.g. backdoors, rootkits)
  - Correct or patch relevant vulnerabilities on affected systems
- Recover
  - Restore affected systems to their normal operating state

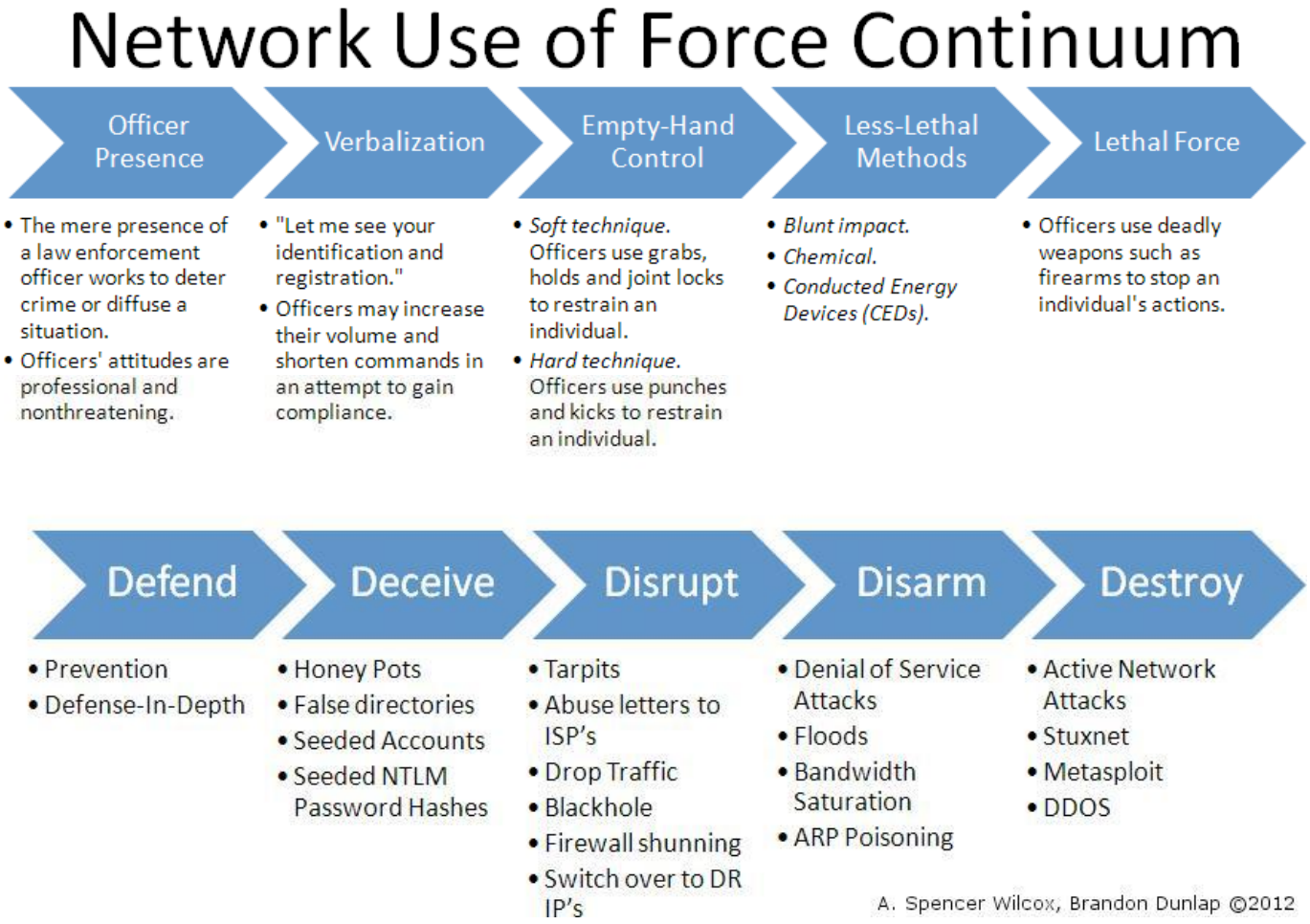
Copyright 2013 Iowa State University

# Evaluate, Contain, Eradicate, Recover

- Unlisted but necessary steps
  - Communicate
    - Stakeholders need to know what is going on at all stages of the response
  - Reflect
    - Review the incident and response after the dust settles
      - Significant incidents should be documented in order to preserve institutional knowledge and promote sharing with parties outside of the response.
    - Learn from mistakes
  - Improve
    - Take corrective actions

Copyright 2013 Iowa State University

# Offensive Response




Copyright 2013 Iowa State University

# Impact Management

- Risk management
  - Oriented towards the future
    - Time horizon ranges from months to years from today
  - Meant to manage costs resulting from potential adverse events
- Impact management
  - Oriented towards now and coming days
  - Meant to manage costs resulting from an actual adverse event
    - Costs need not be strictly quantified in currency (e.g. US $)

Copyright 2013 Iowa State University

# Impact Management

- Impacts can be:
  - Productivity
  - Revenue
  - Reputation
  - Compliance or Regulatory violations
  - Security
  - Safety
  - Response labor and materials costs

Copyright 2013 Iowa State University

# Impact Management

- Technical responders need to be aware that minimizing an incident's impact:
  - May not be strictly technical
  - May prolong the incident's duration
  - May require allowing employees and customers to work on systems you are attempting to service
    - If a service must go offline, the outage is kept to absolute bare minimum
      - » Ideally, another service instance can service requests while the original is offline

Copyright 2013 Iowa State University

# Impact Management

- CDC
  - The exercise does not directly consider many real-world impacts
  - However, the scoring breakdown expresses cost by the way that points are allocated.
  - For the exercise, minimizing points loss is impact management

Copyright 2013 Iowa State University

# Response Planning

- Strategic
  - Develop high-level plans for types of incidents
  - These plans incorporate the organization's priorities and policies
    - CDC: Rules and points allocation will influence priorities
  - If helpful, these plans provide an action framework
    - This framework can have gaps that get filled in when incident particulars are known
  - Actual incident response incident may not be strictly faithful to planning, but previous planning will likely help, because:
    - Priorities have been articulated
    - Vocabulary has been established
    - Environmental details and interrelationships have been considered
    - Tools and methods have been acquired and practiced

Copyright 2013 Iowa State University

# Response Planning

- Tactical
  - An accurate identification of the incident will help with picking from your strategic plans
  - Let the incident's nature drive planning using your strategic plans as guidance
  - Be flexible, the incident may not be what you initially thought it was or it may adapt to you
    - This is especially true if your attacker is live
    - Multiple attackers may be working independently or cooperatively using complementary tools

Copyright 2013 Iowa State University

# Response Planning

- Tactical
  - Plan to communicate and do it
    - Avoid duplication of work
    - Avoid interfering with each other's efforts
    - Seek help from your teammates
    - Stick to the plan or coordinate closely with your team to change it
      - Plan can be goal oriented instead of action oriented if that helps
    - Consider letting a teammate "run point"
      - Focus required to achieve one objective hinders big picture thinking
    - CDC points are assigned for communication beyond the team

Copyright 2013 Iowa State University

# Response Planning

- Tactical
  - Take a moment and write the plan down somewhere the team can see it
    - Diagramming can help express the order of actions and their dependencies
    - Write down action assignments
      - This helps each team member know what their task is as well as how it relates to the others
      - Knowing what the next action before finishing the current action helps keep focus and energy towards the issue at hand
        - » It also may help with fitting in a bio or brain break

Copyright 2013 Iowa State University