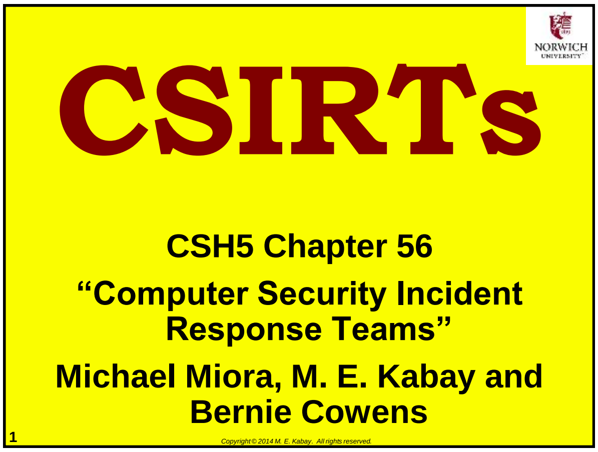


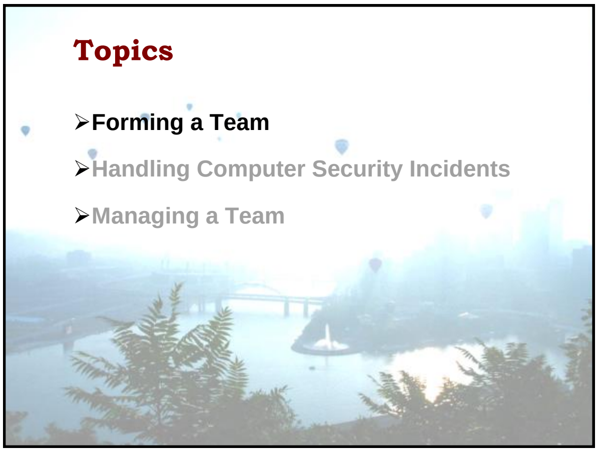
CSIRTs

CSH5 Chapter 56

"Computer Security Incident Response Teams"

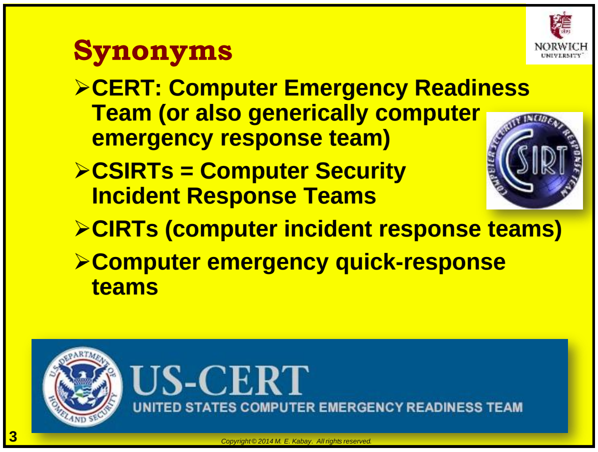
Michael Miora, M. E. Kabay and Bernie Cowens

1



Topics

- ➢Forming a Team
- ➢Handling Computer Security Incidents
- ➢Managing a Team

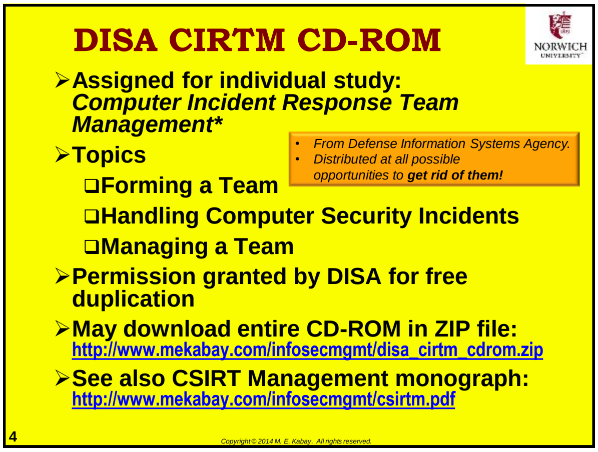


Synonyms

- ➢CERT: Computer Emergency Readiness Team (or also generically computer emergency response team)
- ➢CSIRTs = Computer Security Incident Response Teams
- ➢CIRTs (computer incident response teams)
- ➢Computer emergency quick-response teams

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

3

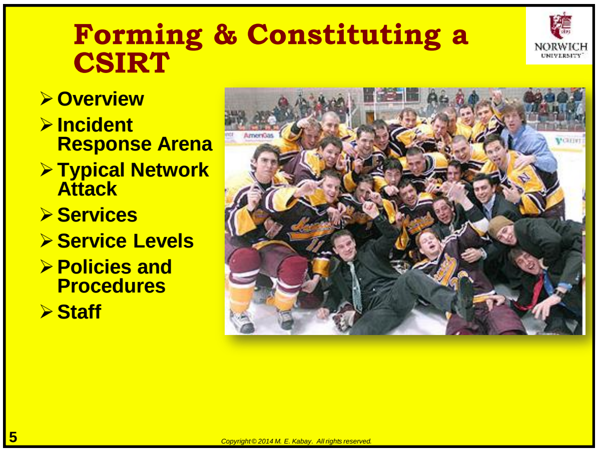


DISA CIRTM CD-ROM

- ➢Assigned for individual study: *Computer Incident Response Team Management**
- ➢Topics
  - ❑Forming a Team
  - ❑Handling Computer Security Incidents
  - ❑Managing a Team
- ➢Permission granted by DISA for free duplication
- ➢May download entire CD-ROM in ZIP file: http://www.mekabay.com/infosecmgmt/disa_cirtm_cdrom.zip
- ➢See also CSIRT Management monograph: http://www.mekabay.com/infosecmgmt/csirtm.pdf

- *From Defense Information Systems Agency.*
- *Distributed at all possible opportunities to **get rid of them!***

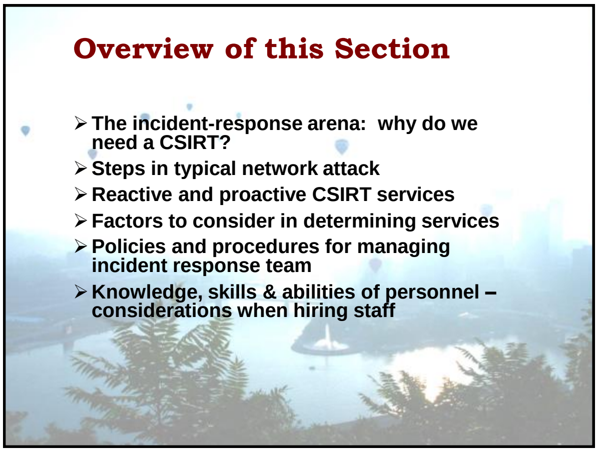
4



Forming & Constituting a CSIRT

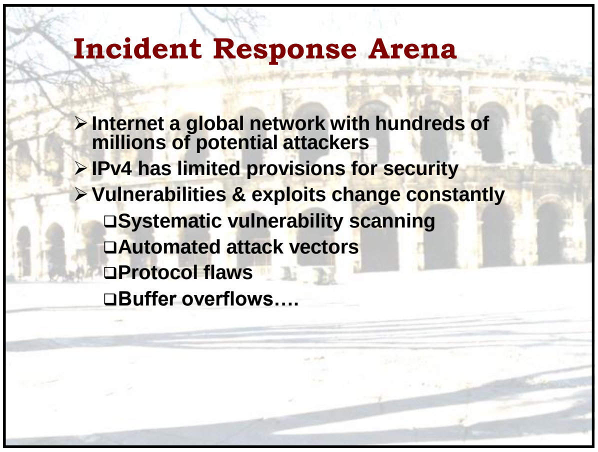
- ➢Overview
- ➢Incident Response Arena
- ➢Typical Network Attack
- ➢Services
- ➢Service Levels
- ➢Policies and Procedures
- ➢Staff

5



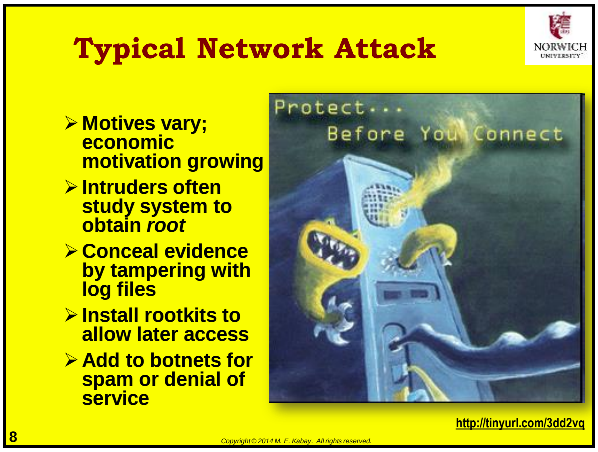
Overview of this Section

- ➢The incident-response arena: why do we need a CSIRT?
- ➢Steps in typical network attack
- ➢Reactive and proactive CSIRT services
- ➢Factors to consider in determining services
- ➢Policies and procedures for managing incident response team
- ➢Knowledge, skills & abilities of personnel – considerations when hiring staff



Incident Response Arena

- ➢ Internet a global network with hundreds of millions of potential attackers
- ➢ IPv4 has limited provisions for security
- ➢ Vulnerabilities & exploits change constantly
  - ❑ Systematic vulnerability scanning
  - ❑ Automated attack vectors
  - ❑ Protocol flaws
  - ❑ Buffer overflows….



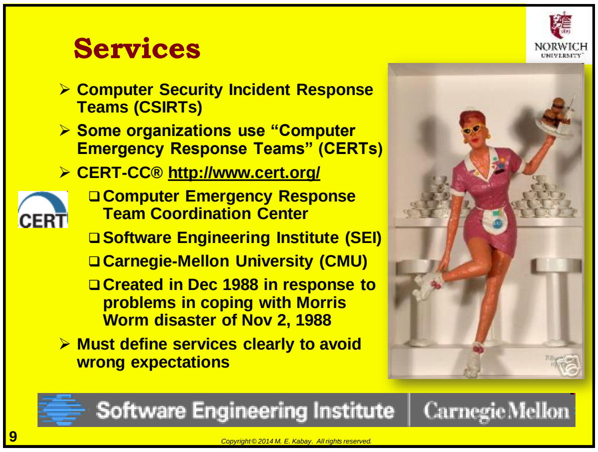
Typical Network Attack

- ➢ Motives vary; economic motivation growing
- ➢ Intruders often study system to obtain *root*
- ➢ Conceal evidence by tampering with log files
- ➢ Install rootkits to allow later access
- ➢ Add to botnets for spam or denial of service

Protect...
Before You Connect

http://tinyurl.com/3dd2vq

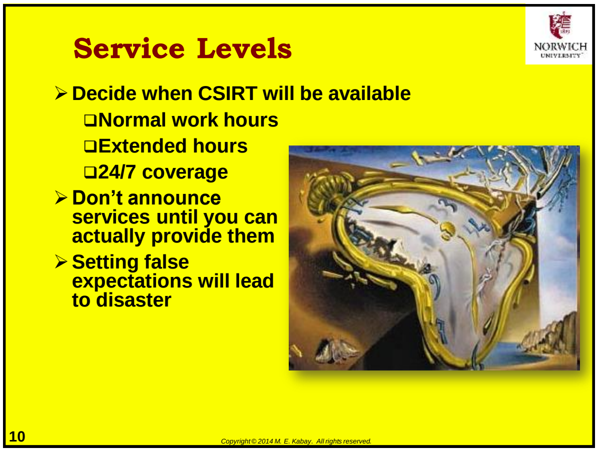
8



Services

- ➢ Computer Security Incident Response Teams (CSIRTs)
- ➢ Some organizations use "Computer Emergency Response Teams" (CERTs)
- ➢ CERT-CC® http://www.cert.org/
  - ❑ Computer Emergency Response Team Coordination Center
  - ❑ Software Engineering Institute (SEI)
  - ❑ Carnegie-Mellon University (CMU)
  - ❑ Created in Dec 1988 in response to problems in coping with Morris Worm disaster of Nov 2, 1988
- ➢ Must define services clearly to avoid wrong expectations

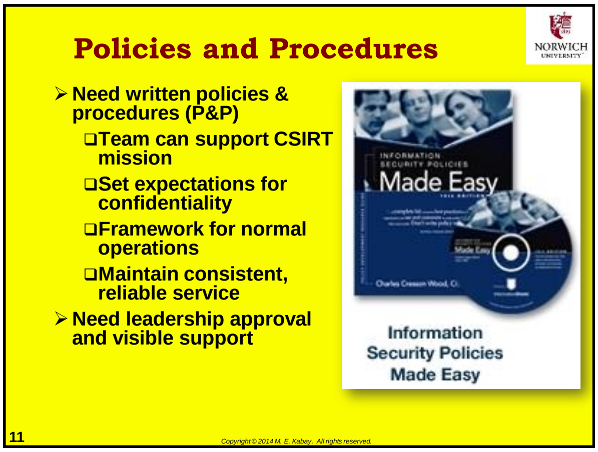
9



Service Levels

- ➢ Decide when CSIRT will be available
  - ❑ Normal work hours
  - ❑ Extended hours
  - ❑ 24/7 coverage
- ➢ Don't announce services until you can actually provide them
- ➢ Setting false expectations will lead to disaster

10



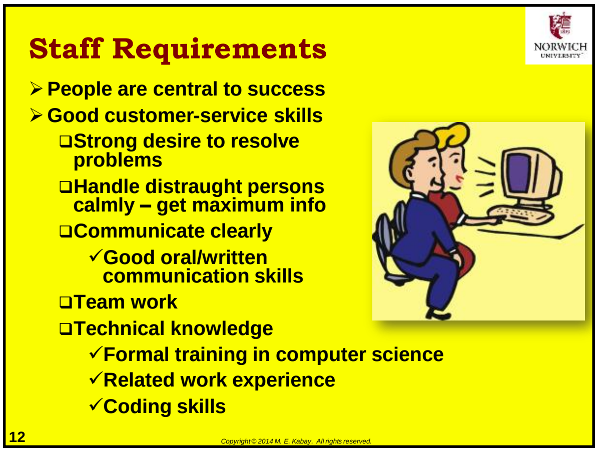
Policies and Procedures

- ➢ Need written policies & procedures (P&P)
  - ❑ Team can support CSIRT mission
  - ❑ Set expectations for confidentiality
  - ❑ Framework for normal operations
  - ❑ Maintain consistent, reliable service
- ➢ Need leadership approval and visible support

Information Security Policies Made Easy
Charles Cresson Wood, CISSP

Information Security Policies Made Easy

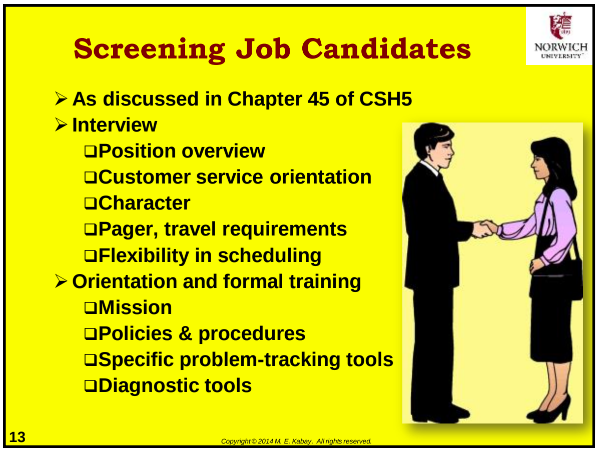
11



Staff Requirements

- ➢ People are central to success
- ➢ Good customer-service skills
  - ❑ Strong desire to resolve problems
  - ❑ Handle distraught persons calmly – get maximum info
  - ❑ Communicate clearly
    - ✓ Good oral/written communication skills
  - ❑ Team work
  - ❑ Technical knowledge
    - ✓ Formal training in computer science
    - ✓ Related work experience
    - ✓ Coding skills

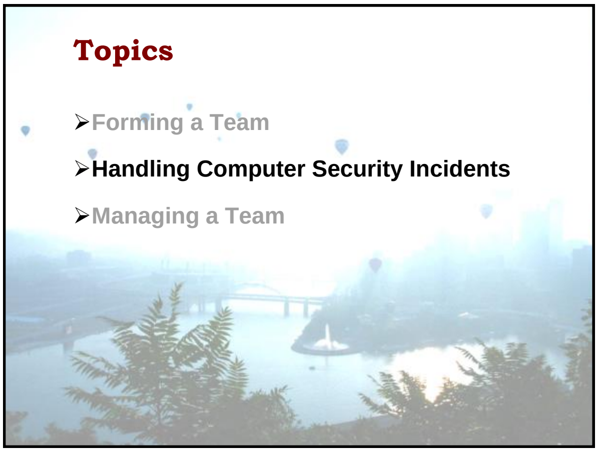
12



Screening Job Candidates

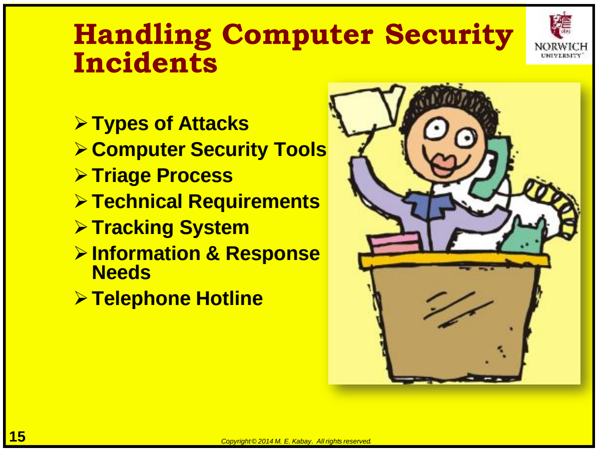
- As discussed in Chapter 45 of CSH5
- Interview
  - ❑Position overview
  - ❑Customer service orientation
  - ❑Character
  - ❑Pager, travel requirements
  - ❑Flexibility in scheduling
- Orientation and formal training
  - ❑Mission
  - ❑Policies & procedures
  - ❑Specific problem-tracking tools
  - ❑Diagnostic tools

13



Topics

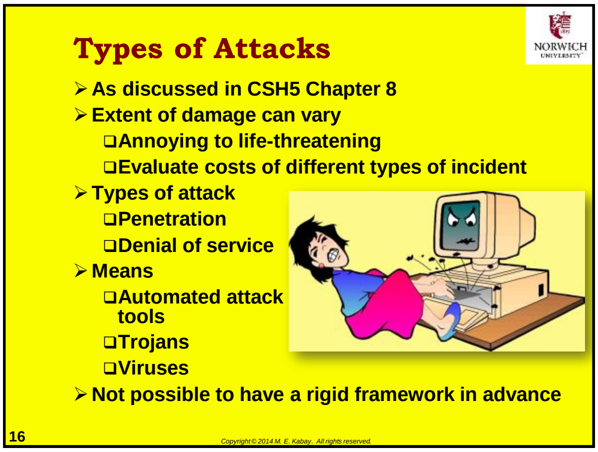
- Forming a Team
- Handling Computer Security Incidents
- Managing a Team



Handling Computer Security Incidents

- Types of Attacks
- Computer Security Tools
- Triage Process
- Technical Requirements
- Tracking System
- Information & Response Needs
- Telephone Hotline

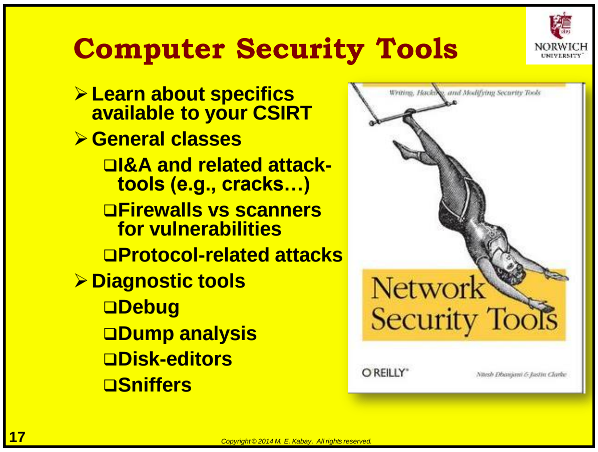
15



Types of Attacks

- As discussed in CSH5 Chapter 8
- Extent of damage can vary
  - ❑Annoying to life-threatening
  - ❑Evaluate costs of different types of incident
- Types of attack
  - ❑Penetration
  - ❑Denial of service
- Means
  - ❑Automated attack tools
  - ❑Trojans
  - ❑Viruses
- Not possible to have a rigid framework in advance

16

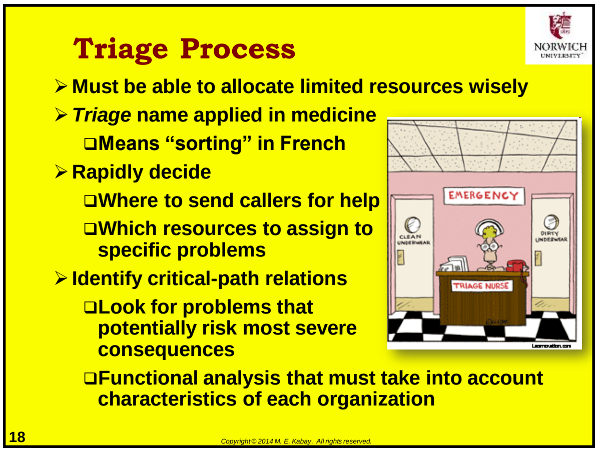


Computer Security Tools

- Learn about specifics available to your CSIRT
- General classes
  - ❑I&A and related attack-tools (e.g., cracks…)
  - ❑Firewalls vs scanners for vulnerabilities
  - ❑Protocol-related attacks
- Diagnostic tools
  - ❑Debug
  - ❑Dump analysis
  - ❑Disk-editors
  - ❑Sniffers

Writing, Hacking, and Modifying Security Tools
Network Security Tools
O'REILLY
Nitesh Dhanjani & Justin Clarke

17



Triage Process

- Must be able to allocate limited resources wisely
- *Triage* name applied in medicine
  - ❑Means “sorting” in French
- Rapidly decide
  - ❑Where to send callers for help
  - ❑Which resources to assign to specific problems
- Identify critical-path relations
  - ❑Look for problems that potentially risk most severe consequences
  - ❑Functional analysis that must take into account characteristics of each organization

18

Prioritizing Incidents

- Sensitivity and/or criticality of the data affected
- Amount of data affected
- Which host machines are involved
- Where and under what conditions the incident occurred
- Effects of the incident on mission accomplishment
- Whether the incident is likely to result in media coverage
- Number of stakeholders affected
- Possible relationships to other incidents currently being investigated
- The nature of the attack
- Economic impact and time lost
- Number of times the problem has recurred
- Who reports the incident

Technical Requirements

- Assign least-skilled staff to triage stage – enough skill to
  - ❑Identify nature of problem
  - ❑Collect basic information
  - ❑Decide quickly to whom to send caller
  - ❑Let more experienced staff avoid clerical functions
- Information requests: low to medium skill levels
- Incident response: medium skill levels
- Vulnerability handling: high skill levels

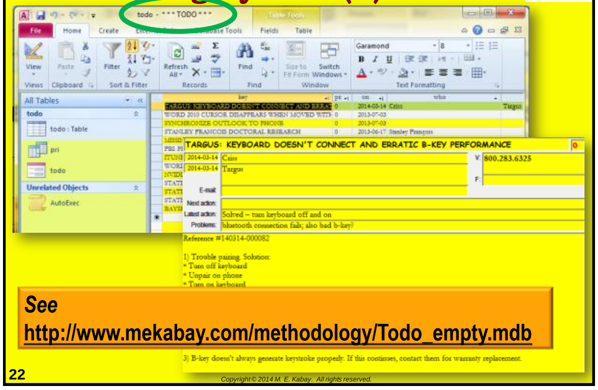
http://www.summum.us/images/jpg/pyramid3.jpg

Tracking System (1)

- Critically important to track information
- Use formal tracking system (many products available) to ensure
  - ❑Easy notes
  - ❑Availability to entire group
  - ❑Keyword and full-text retrieval
  - ❑Status settings
- May play crucial role in solving problems
- For course notes on a course taught in the 1980s and 1990s about managing technical-support issues, see http://www.mekabay.com/courses/academic/jac/TSP/index.htm

http://tinyurl.com/3xsued
Used with permission of the photographer, Mike Robinson. See catalog at http://tinyurl.com/3dm33c

Tracking System (2)



key	pri	on	who
TARGUS: KEYBOARD DOESN'T CONNECT AND ERRAT	0	2014-03-14 Criss	Targus
WORD 2010 CURSOR DISAPPEARS WHEN MOVED WITH	0	2013-07-03	
SYNCHRONIZE OUTLOOK TO PHONE	0	2013-07-03	
STANLEY FRANCOIS DOCTORAL RESEARCH	0	2013-06-17 Stanley François	

TARGUS: KEYBOARD DOESN'T CONNECT AND ERRATIC B-KEY PERFORMANCE 0

2014-03-14 Criss V: 800.283.6325

2014-03-14 Targus F:

E-mail:

Next action:

Latest action: Solved – turn keyboard off and on

Problems: bluetooth connection fails; also bad b-key?

Reference #140314-000082

1) Trouble pairing. Solution:
* Turn off keyboard
* Unpair on phone
* Turn on keyboard

3) B-key doesn't always generate keystroke properly. If this continues, contact them for warranty replacement.

See http://www.mekabay.com/methodology/Todo_empty.mdb

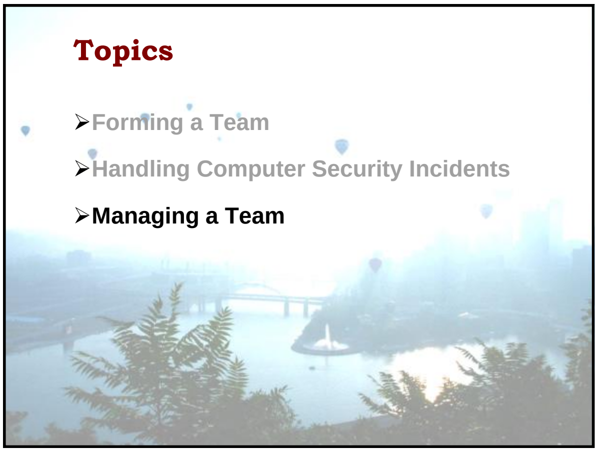
? ? ? ? ? ?

Information & Response Needs for Every Incident Report

- Who is the reporting organization?
- What other organizations are involved or need to know about the incident?
- What is the date and time of the incident?
- What type of incident is it?
- What is the name or ID of the information system or systems affected?
- What is the mission impact of the incident?
- What are the technical details or the who, what, when, where, why, and how of the incident?
- What actions have been taken?
- Has there been any coordination with other commands on the incident?
- Are there any other clues or is any information missing?

Telephone Hotline

- Must handle phone calls at all times of day/night
  - ❑Call-forwarding to agent on duty
  - ❑Pagers
  - ❑Message service
  - ❑SMS to cell phones
  - ❑Answering machine / voicemail(☹)
- Define rules for taking details and then *transferring calls to right person*
  - ❑MOST IMPORTANT: *Never drop the caller!* Always monitor the transfer and ensure there is a live person (not voicemail) on the other end of the line to take control of the situation
  - ❑Always provide direct-line phone # & case # for use in case of interruption
- Define procedures to handle cranks/pranks



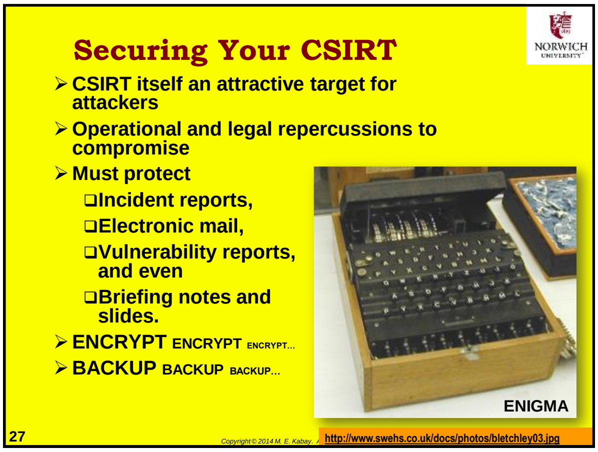
Topics

- ➢Forming a Team
- ➢Handling Computer Security Incidents
- ➢**Managing a Team**

Managing a Team

- ➢ Securing Your CSIRT
- ➢ Using a Code of Conduct
- ➢ Prioritizing Incidents
- ➢ Balancing Workload

26



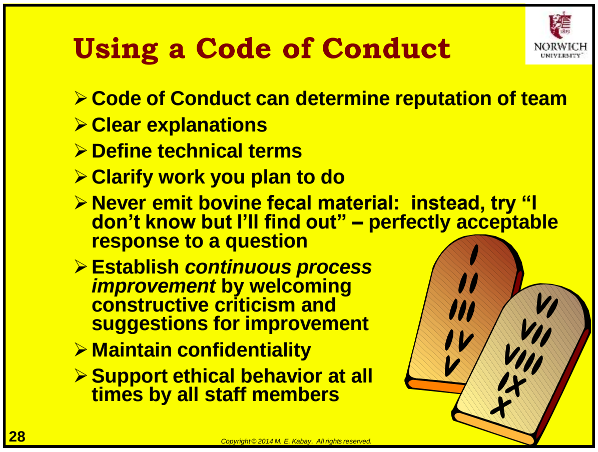
Securing Your CSIRT

- ➢ CSIRT itself an attractive target for attackers
- ➢ Operational and legal repercussions to compromise
- ➢ Must protect
  - ❑Incident reports,
  - ❑Electronic mail,
  - ❑Vulnerability reports, and even
  - ❑Briefing notes and slides.
- ➢ ENCRYPT ENCRYPT ENCRYPT…
- ➢ BACKUP BACKUP BACKUP…

ENIGMA

27

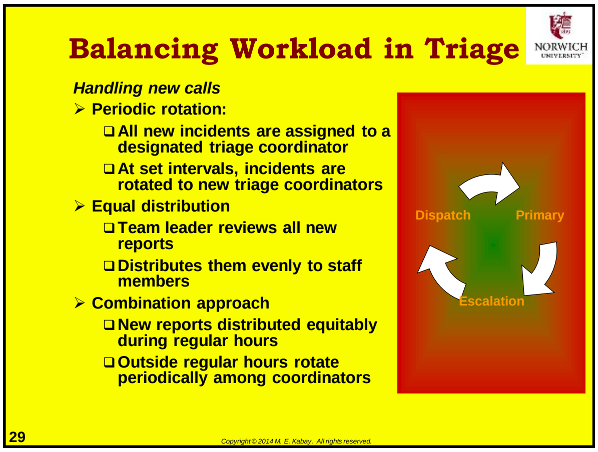
http://www.swehs.co.uk/docs/photos/bletchley03.jpg



Using a Code of Conduct

- ➢ Code of Conduct can determine reputation of team
- ➢ Clear explanations
- ➢ Define technical terms
- ➢ Clarify work you plan to do
- ➢ Never emit bovine fecal material: instead, try "I don't know but I'll find out" – perfectly acceptable response to a question
- ➢ Establish *continuous process improvement* by welcoming constructive criticism and suggestions for improvement
- ➢ Maintain confidentiality
- ➢ Support ethical behavior at all times by all staff members

28

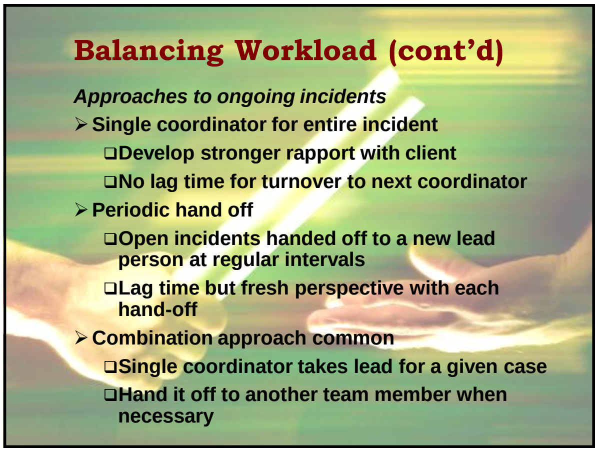


Balancing Workload in Triage

Handling new calls

- ➢ Periodic rotation:
  - ❑All new incidents are assigned to a designated triage coordinator
  - ❑At set intervals, incidents are rotated to new triage coordinators
- ➢ Equal distribution
  - ❑Team leader reviews all new reports
  - ❑Distributes them evenly to staff members
- ➢ Combination approach
  - ❑New reports distributed equitably during regular hours
  - ❑Outside regular hours rotate periodically among coordinators

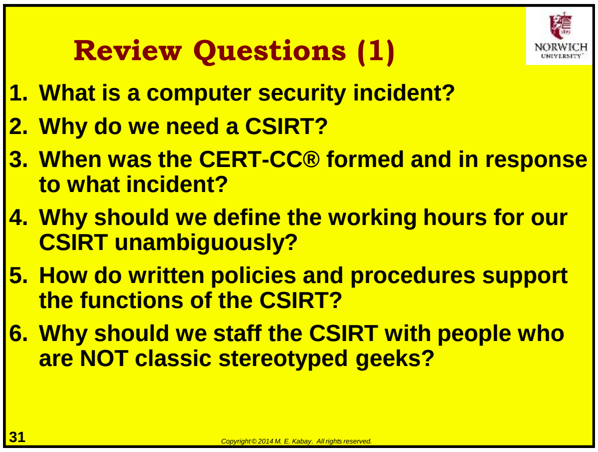
29



Balancing Workload (cont'd)

Approaches to ongoing incidents

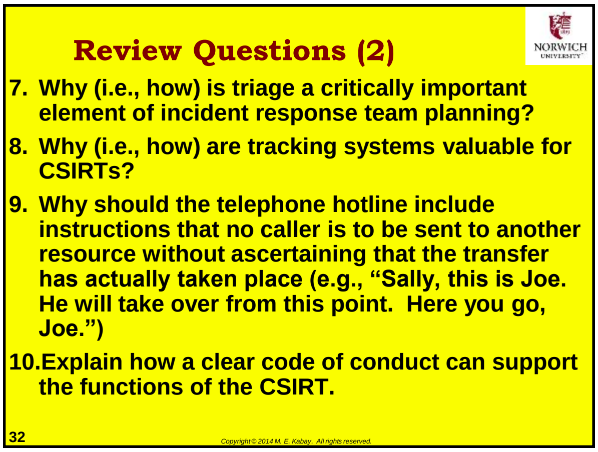
- ➢Single coordinator for entire incident
  - ❑Develop stronger rapport with client
  - ❑No lag time for turnover to next coordinator
- ➢Periodic hand off
  - ❑Open incidents handed off to a new lead person at regular intervals
  - ❑Lag time but fresh perspective with each hand-off
- ➢Combination approach common
  - ❑Single coordinator takes lead for a given case
  - ❑Hand it off to another team member when necessary



Review Questions (1)

1. What is a computer security incident?
2. Why do we need a CSIRT?
3. When was the CERT-CC® formed and in response to what incident?
4. Why should we define the working hours for our CSIRT unambiguously?
5. How do written policies and procedures support the functions of the CSIRT?
6. Why should we staff the CSIRT with people who are NOT classic stereotyped geeks?

31



Review Questions (2)

7. Why (i.e., how) is triage a critically important element of incident response team planning?
8. Why (i.e., how) are tracking systems valuable for CSIRTs?
9. Why should the telephone hotline include instructions that no caller is to be sent to another resource without ascertaining that the transfer has actually taken place (e.g., “Sally, this is Joe. He will take over from this point. Here you go, Joe.”)
10. Explain how a clear code of conduct can support the functions of the CSIRT.

32

DISCUSSION

33