GJØVIK UNIVERSITY COLLEGE

Security Planning and Incident Management

Marie Moe, NSM/HiG

Gjøvik 31.03.14

AGENDA

Criteria for Project Evaluation

Incident Response

- *Reaction*
- *Recovery*
- *Maintenance*
- *Co-operation between CSIRTs and law enforcement authorities*

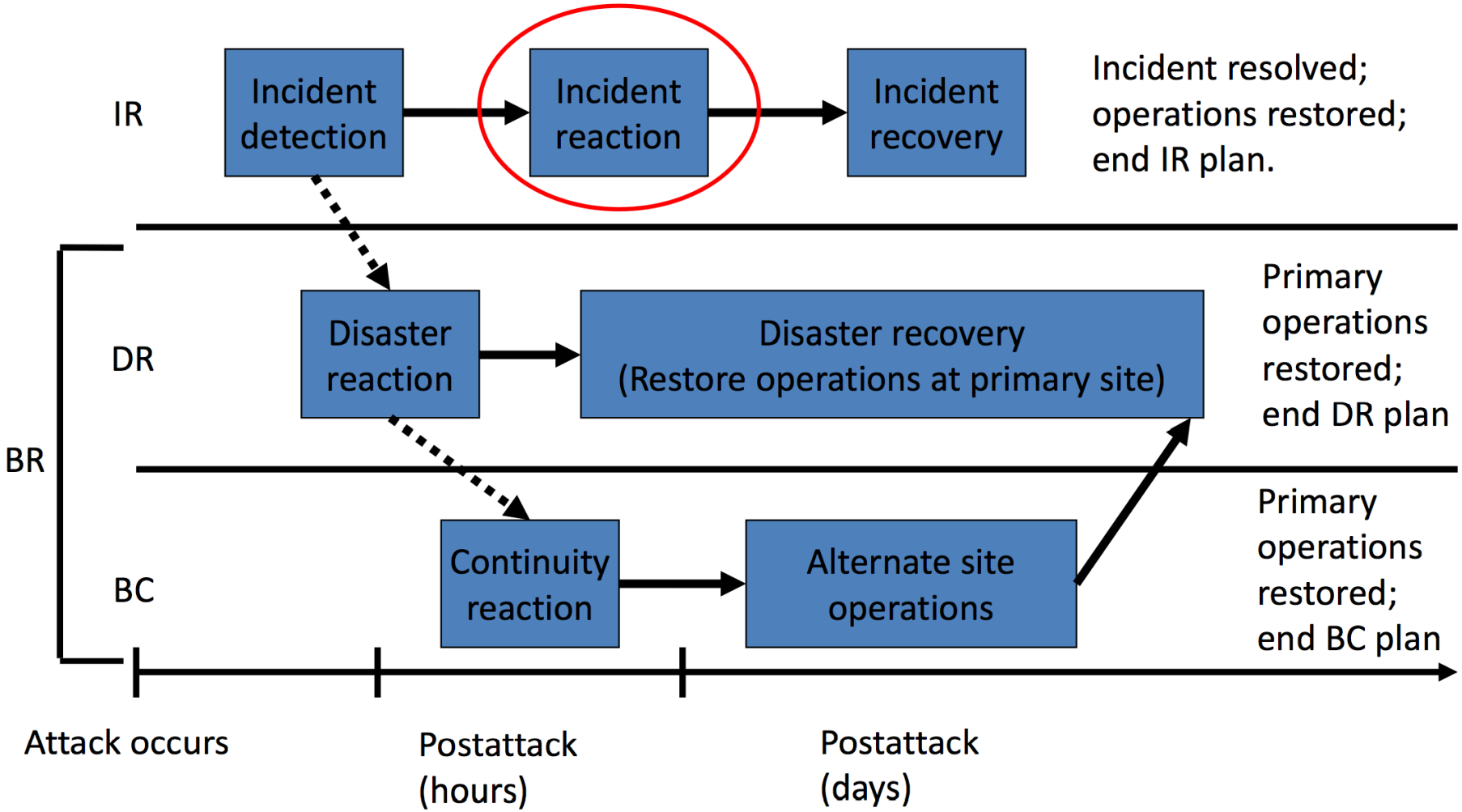
PROJECT WORK

- The deadline for a complete draft of your project work is approaching
  - Please submit your drafts via Fronter, not by e-mail
- For the final report you also have to write an evaluation of your own report, this is not mandatory for the drafts but you may do this for practice
  - Your self-evaluation **will count** towards your grade
- You will also be asked to evaluate the draft of another group
  - This will **not** count towards your grade
- *The project work will account for 50% of the grade for this course*
- We will now agree on the criteria for the project evaluation

CRITERIA FOR PROJECT EVALUATION

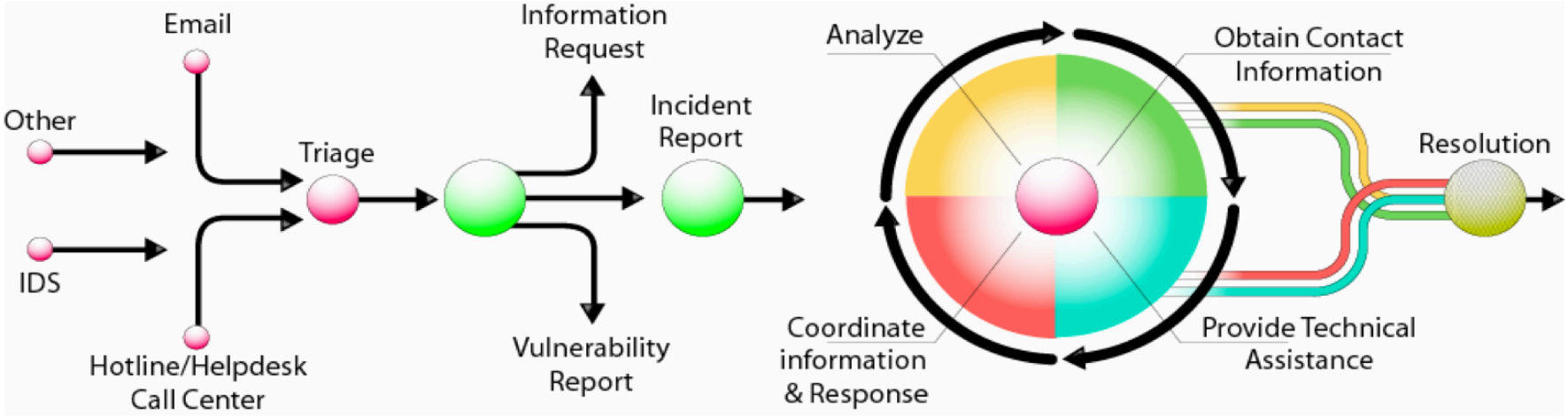
symbol	description	General, qualitative description of valuation criteria
A	Excellent	An excellent performance, clearly outstanding. The candidate demonstrates excellent judgement and a high degree of independent thinking.
B	Very good	A very good performance. The candidate demonstrates sound judgement and a very good degree of independent thinking.
C	Good	A good performance in most areas. The candidate demonstrates a reasonable degree of judgement and independent thinking in the most important areas.
D	Satisfactory	A satisfactory performance, but with significant shortcomings. The candidate demonstrates a limited degree of judgement and independent thinking.
E	Sufficient	A performance that meets the minimum criteria, but no more. The candidate demonstrates a very limited degree of judgement and independent thinking.
F	Fail	A performance that does not meet the minimum academic criteria. The candidate demonstrates an absence of both judgement and independent thinking.

Universitets- og høgskolerådet, 6. august 2004)



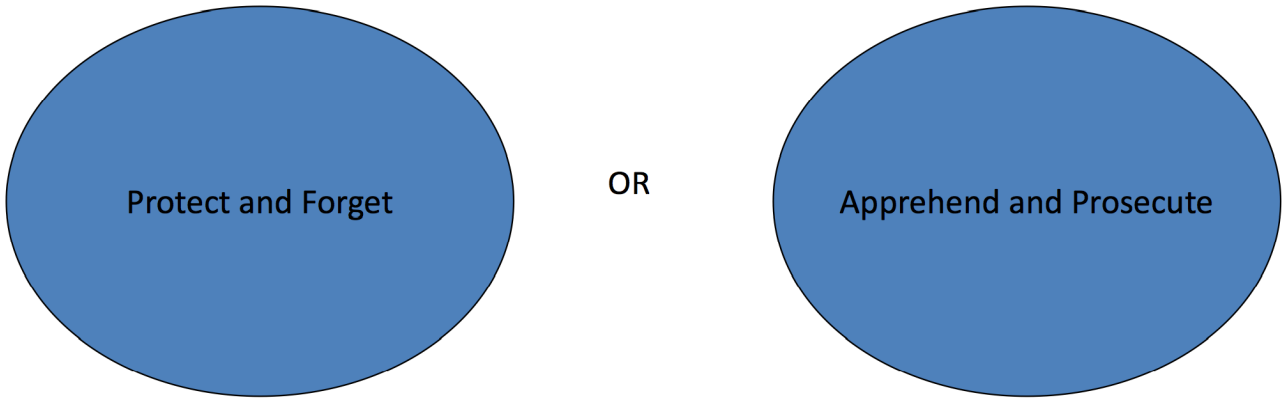
Whitman and Mattord 2007, p. 27

INCIDENT HANDLING LIFE CYCLE (CERT/CC)



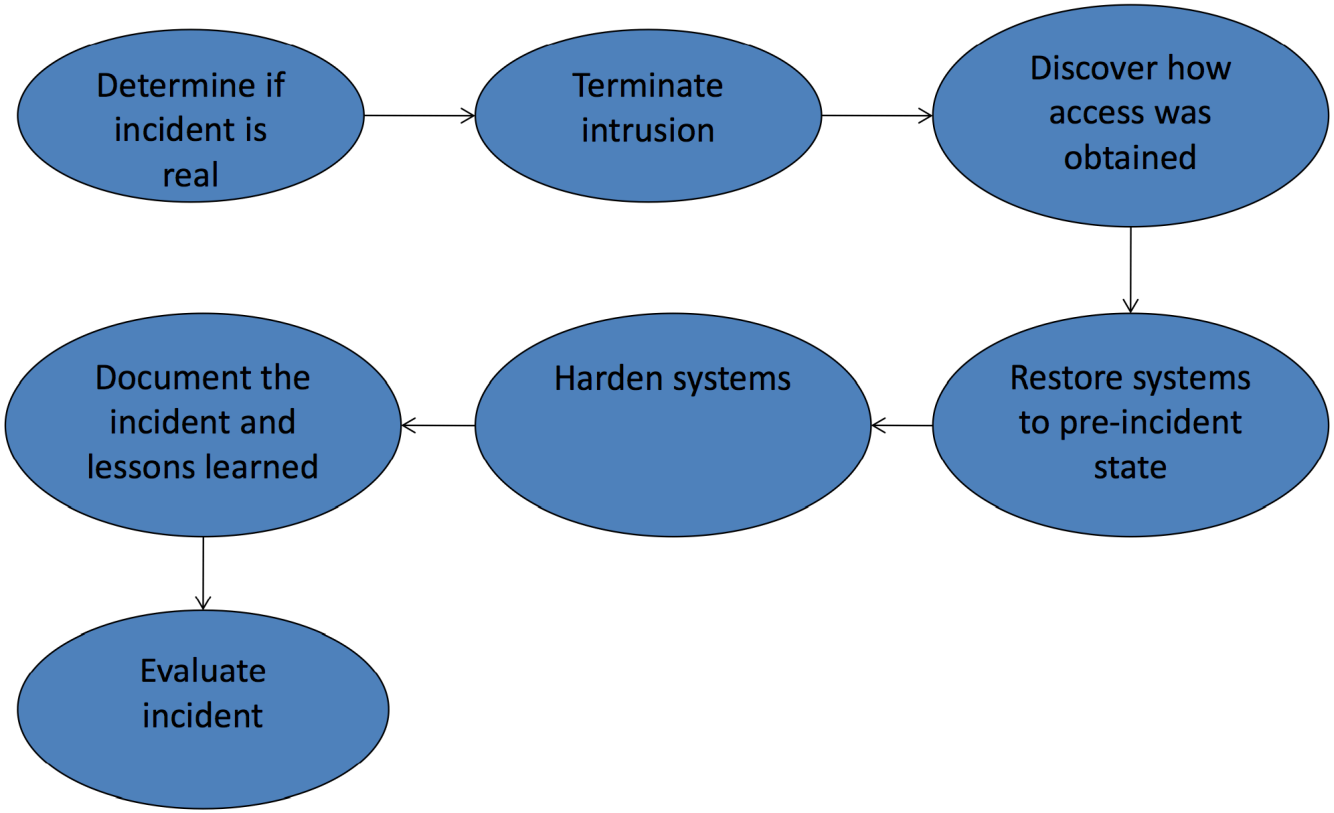
Handbook for Computer Incident Response Teams (CSIRTS)

SELECTING AN INCIDENT RESPONSE STRATEGY



D. Adler, K. Grossman. Establishing a Computer Incident Response Plan. See also Whitman and Mattord 2007, p. 185

PROTECT AND FORGET



D. Adler, K. Grossman. Establishing a Computer Incident Response Plan. See also Whitman and Mattord 2007, p. 185

PROTECT AND FORGET

1.Determine if the event is a real incident.

2.If so, terminate the intrusion.

3.Discover how access was obtained and which systems were compromised.

4.Restore compromised systems to pre-incident configuration.

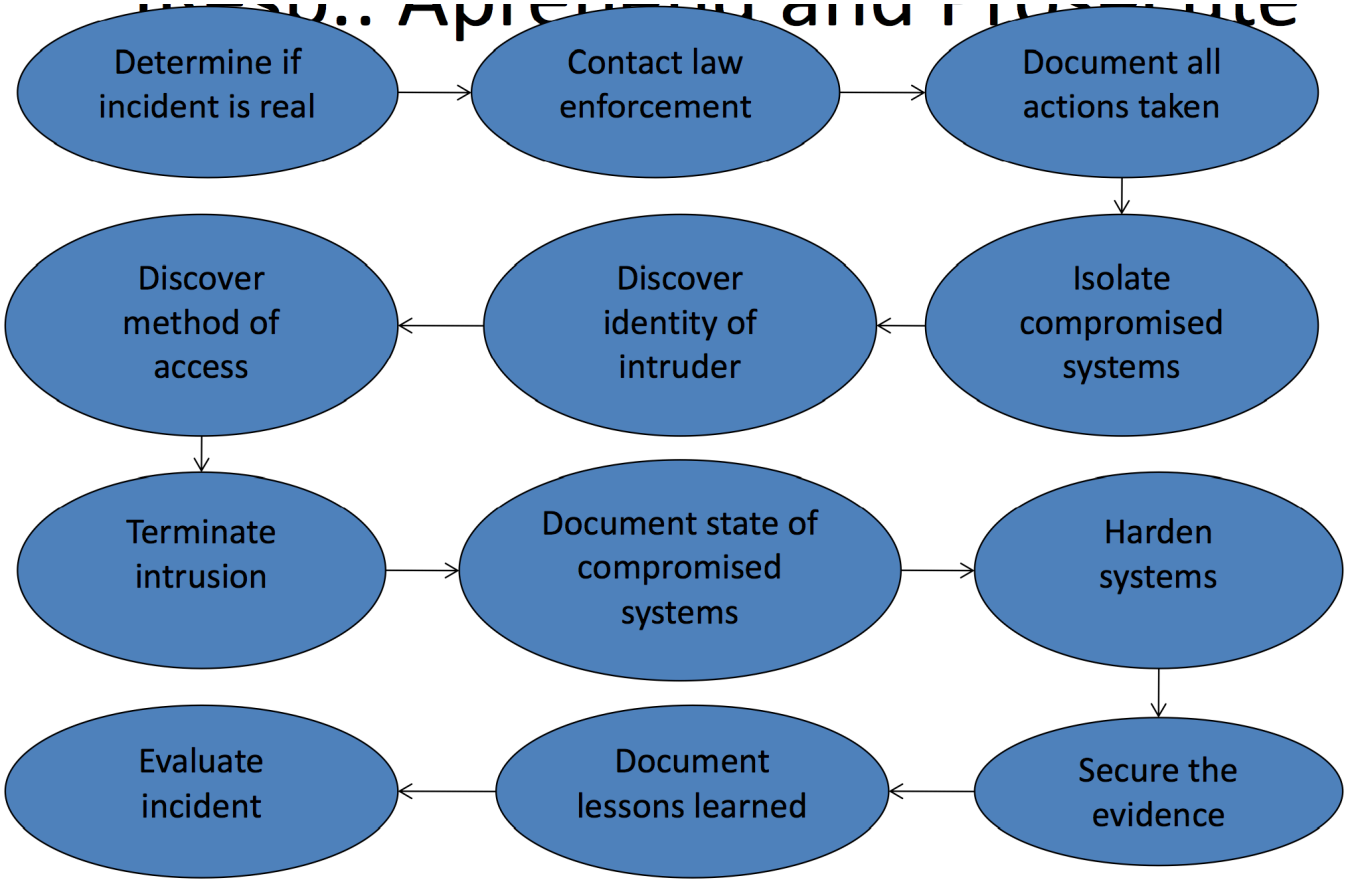
5.Secure the method of unauthorized access on all systems.

6.Document steps taken to deal with the incident.

7.Develop lessons learned.

8.Upper management performs a brief evaluation of the incident aftermath.

APPREHEND AND PROSECUTE



D. Adler, K. Grossman. Establishing a Computer Incident Response Plan. See also Whitman and Mattord 2007, p. 185

APPREHEND AND PROSECUTE

1.Determine if the event is a real incident.

2.If it is and the circumstances warrant it, contact law enforcement.

3.Document each action taken, including the date and time, as well as who was present.

4.Isolate the compromised systems from the network.

5.If the organisation has the capability, it should entice the intruder into a safe system that seemingly contain valuable data (decoy tactic).

6.Discover the identity of the intruder while documenting his or her activity.

7.Discover how the intruder gained access to the compromised systems, and secure the access points.

APPREHEND AND PROSECUTE

8.Terminate the intrusion when sufficient evidence has been collected.

9.Document the current state of compromised systems.

10.Restore the compromised systems to their pre-incident configuration.

11.Secure the method of unauthorized access by the intruder on all compromised systems.

12.Document in detail the time in man-hours, as well as the cost of handling the incident.

13.Secure all logs, audits, notes, documentation, and any other evidence gathered during the incident and appropriately identify it to secure the ”chain of custody” for future prosecution.

14.Develop lessons learned.

15.Upper management performs a brief evaluation in the incident’s aftermath.

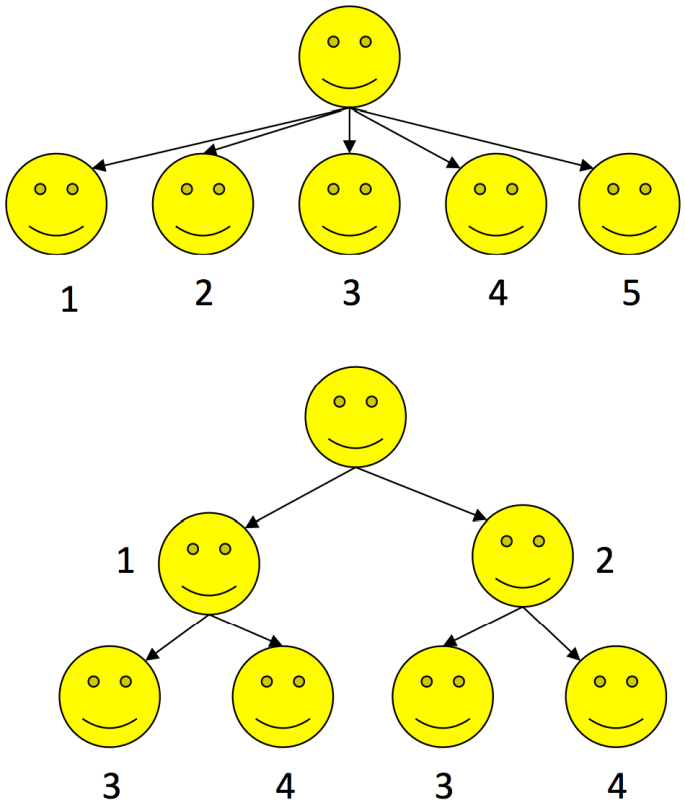
NOTIFICATION

Develop and maintain an **alert roster**

– Document containing contact information on all those who need to be contacted during an incident.

– **Sequential** roster: One person calls everyone on the list.

– **Hierarchical**: First person calls certain other people, who then call those below them.



Whitman and Mattord 2007, p. 188-189

NOTIFICATION

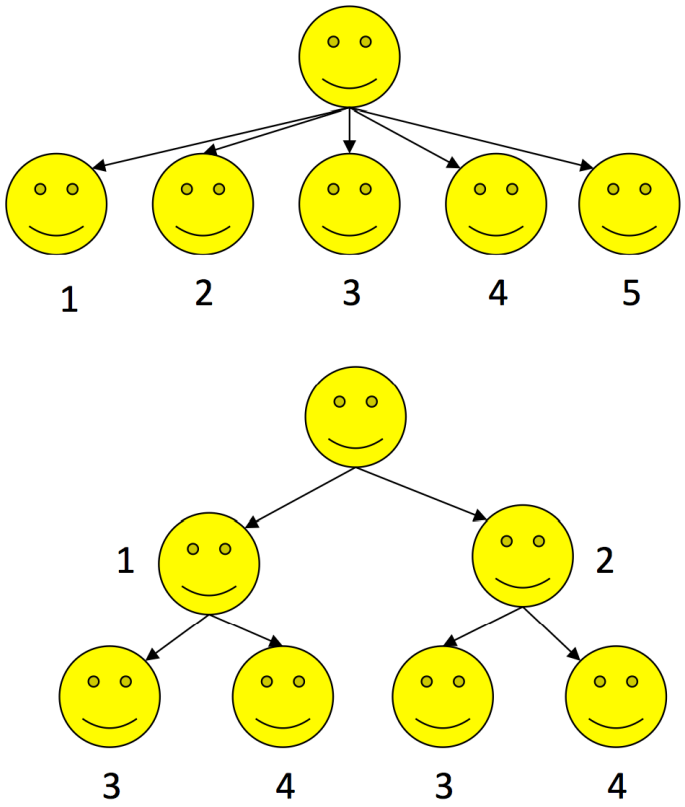
The **alert message**

- Is a scripted description of the incident.
- Contains just enough information so that each responder knows what portion of the IR plan to implement, without impeding the notification process.

Not everyone should be on the alert roster!

- Includes key personnel such as general management.
- Other organisations may also have to be notified.

The alert roster should be updated, tested and maintained!



Whitman and Mattord 2007, p. 188-189

DOCUMENTING AN INCIDENT

- Who? What? When? Where? Why?
- Serves as a case study after the incident
  - Essential for quality improvement
- Protection against lawsuits
  - (Hopefully) proves that everything possible was done to contain the incident and due care was followed

INCIDENT CONTAINMENT STRATEGIES

- Vary depending on incident.
- Affected areas must first be identified.
- Simple analysis determines actions to be taken. Speed is essential. Detailed analysis performed later in the forensic process.
- Strategies focus on two tasks:
  - **Stopping the incident.**
  - **Recovering control of the affected systems.**
- May involve:
  - *Disconnecting communication circuits.*
  - *Disabling compromised user accounts.*
  - *Reconfiguring a firewall to block the problem traffic.*
  - *Temporarily disabling the process or service.*
  - *Taking down the conduit application or server.*
  - *Stopping all computers and network services.*

INTERVIEWING THOSE INVOLVED

Involves three groups of stakeholders:
– End users
– Help desk personnel
– System administrators

Each group can provide a different perspective with respect to clues to:
– its origin
– cause
– impact

May be dangerous in the case of an insider!

INCIDENT ESCALATION

- If incident increases in severity you may have to hit the big red PANIC button.
- Disaster recovery plan may have to be invoked, or
- Incident transferred to outside authority such as law enforcement.
- The BIA is the basis for making this decision.
- The criteria for making the decision must be included in the IR plan.

HANDLING OF DENIAL OF SERVICE INCIDENTS

Before the DoS incident:

- *Coordinating with service provider*
- Collaborating and coordinating with professional response agencies
- Implementation of prevention technologies
- *Monitoring resources*
- Coordinating the monitoring and analysis capabilities
- *Setting up logging* and documentation
- Configuring network devices to prevent DoS incidents

HANDLING OF DENIAL OF SERVICE INCIDENTS

During the DoS incident:

- *Detecting* the DoS incident – should be straightforward
- *Containment* strategies:
  - Shut off network connection – might cause more damage
  - Block traffic on source addresses – might be difficult
  - *Try to fix the source problem*
  - Change the filtering strategy
  - Filter based on the characteristics of the attack
  - *Engage your upstream partners*
  - Eliminate or relocate the target system

HANDLING OF MALWARE INCIDENTS

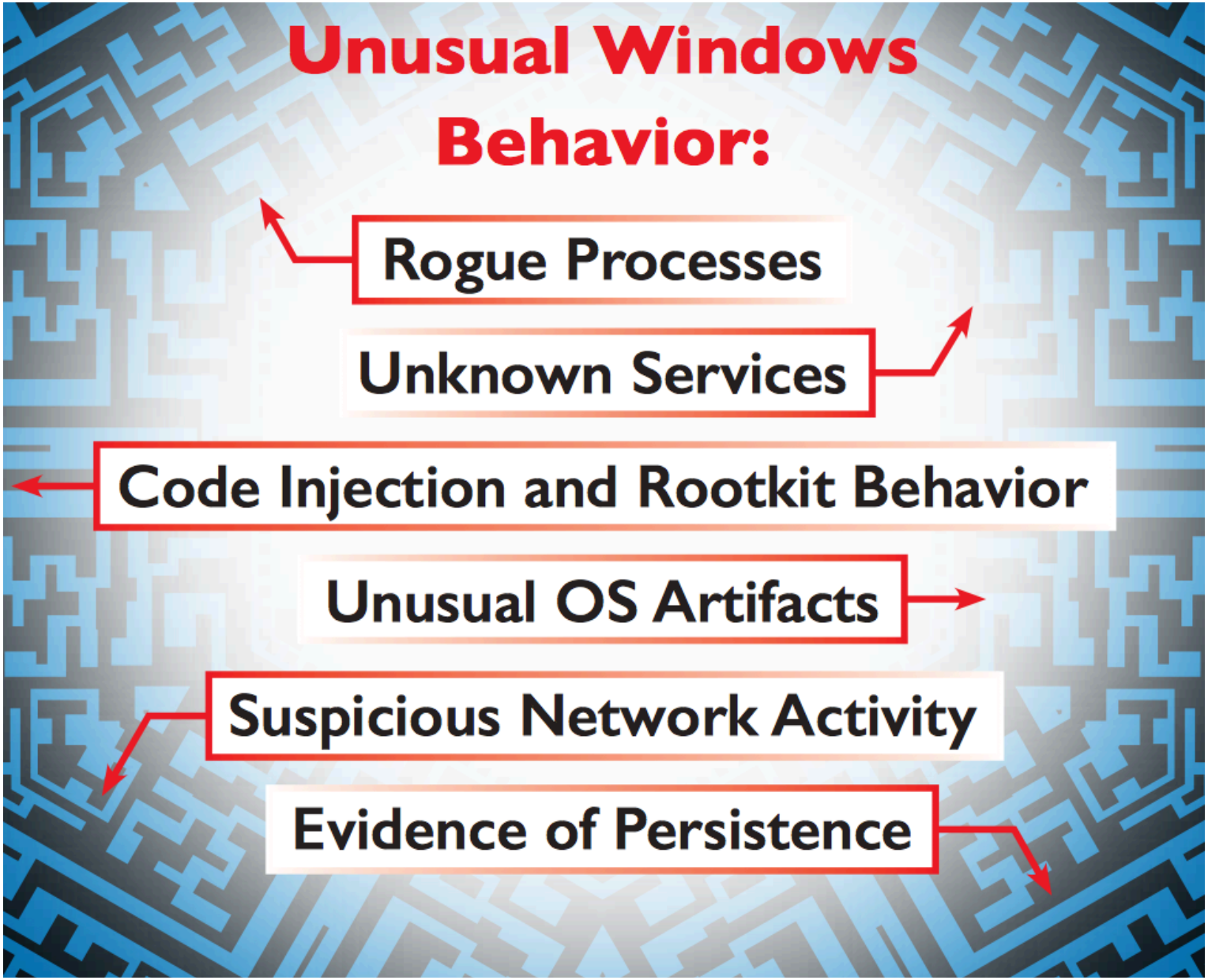
Before the malware incident:

- *Awareness programs* informing users
- Keeping up on IR agency postings and bulletins
- Implementing appropriate IDPS
- Effective inventory and data organization
- Implementing and testing data backup and recovery programs
- *Use antivirus software*
- *Block suspicious files* by configuring servers and networking devices to prevent distribution of certain file extensions
- *Filter unwanted e-mail traffic* and prohibit open relays
- Minimize file transfer capabilities
- Eliminate or prohibit file sharing and print sharing

HANDLING OF MALWARE INCIDENTS

During the malware incident:

- Beware of indicators of malicious code
- Once an infection has been detected, *look for further infections*
- Consider notification of appropriate entities, if the malware found is not commonly known
  - Can be checked by submitting hash value of sample to services like Virus Total
- *Filtering e-mail* based on subject, attachment type using malware signatures
- Blocking known attackers
- Interrupting some services
- Severing networks from the Internet or each other
- Engaging the users
- Disrupting service

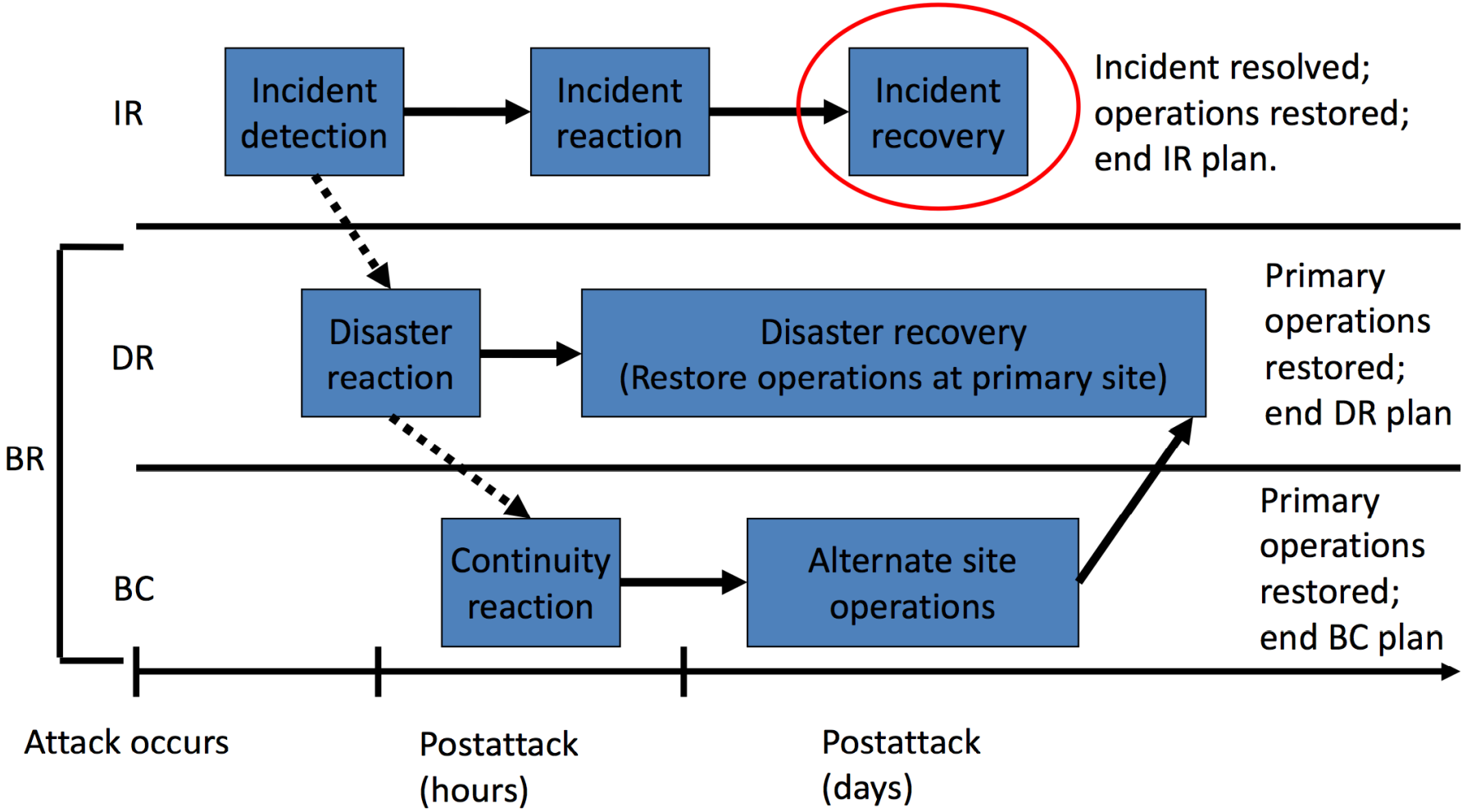


http://digital-forensics.sans.org/media/poster_2014_find_evil.pdf

When searching for malicious processes, look for any of these anomalous characteristics:

- **Started with the wrong parent process**
- **Image executable is located in the wrong path**
- **Misspelled processes**
- **Processes that are running under the wrong account (incorrect SID)**
- **Processes with unusual start times (i.e., starts minutes or hours after boot when it should be within seconds of boot)**
- **Unusual command-line arguments**
- **Packed executables**

http://digital-forensics.sans.org/media/poster_2014_find_evil.pdf



Whitman and Mattord 2007, p. 27

IDENTIFY AND RESOLVE VULNERABILITIES

- May not be simple to identify or resolve vulnerabilities.
- Computer forensics may be necessary to determine how an incident occurred.
- Afterwards, address any safeguards that failed to stop or limit the incident.
- If safeguard is missing, assess why and consider putting one in place.
- Document missing or ineffective safeguards.
- Evaluate monitoring capabilities. Improve detection or reporting methods.

COMPUTER FORENSICS

- Is a massive field which is beyond this course to cover.
- Involves
  - collecting evidentiary material, and
  - analyzing evidentiary material.
- Maintain chain of custody of evidence.
- Make sure evidence is not altered. A simple file access may alter evidence and make it inaccessible or dubious in court.
  - All writeable media should be imaged so that analysis can be performed on the copy without danger of altering the original.
  - Documentation of analysis must be rigorous.
- Acquire appropriate training in computer forensics!

RESTORE DATA

- Understand the backup strategy used in the organisation.
- Restore the data contained in the backups
- Use appropriate recovery processes from incremental backups or database journals.
- Data recovery MUST be TESTED!

RESTORE SERVICES AND PROCESSES

Compromised services must be:

- Examined
- Verified
- Restored

Continuously monitor the systems

- An incident can easily happen again
- Copycat attacks

AFTER ACTION REVIEW

- Detailed examination of events that occurred from first detection to final recovery.
- Document lessons learned and Generate IR plan improvements.
- Historical record of events
  - May be required for legal proceedings.
  - In any case, it is useful to establish a timeline of events.
- Case Training Tool
- Closure
  - People require closure, especially to traumatic events.

RESTORE CONFIDENCE ACROSS THE ORGANISATION

- Ensure everyone that the incident was handled and the damage was controlled.
- If the incident was minor, say so.
- If it was major, reassure users that they can expect operations to be back to normal ASAP.
- Objective is to prevent panic.
- Also raise awareness about security issues. Remember, the user can be your best friend!

MAINTENANCE

On-going maintenance of the IR plan is not trivial!

The IR plan should include procedures to:

- Complete effective after-action review meetings
- Plan review and maintenance
- Train staff involved in incident response
- Maintain readiness

REPORTING TO UPPER MANAGEMENT: LOSS ANALYSIS

How much was lost, and how much will it cost us to recover?

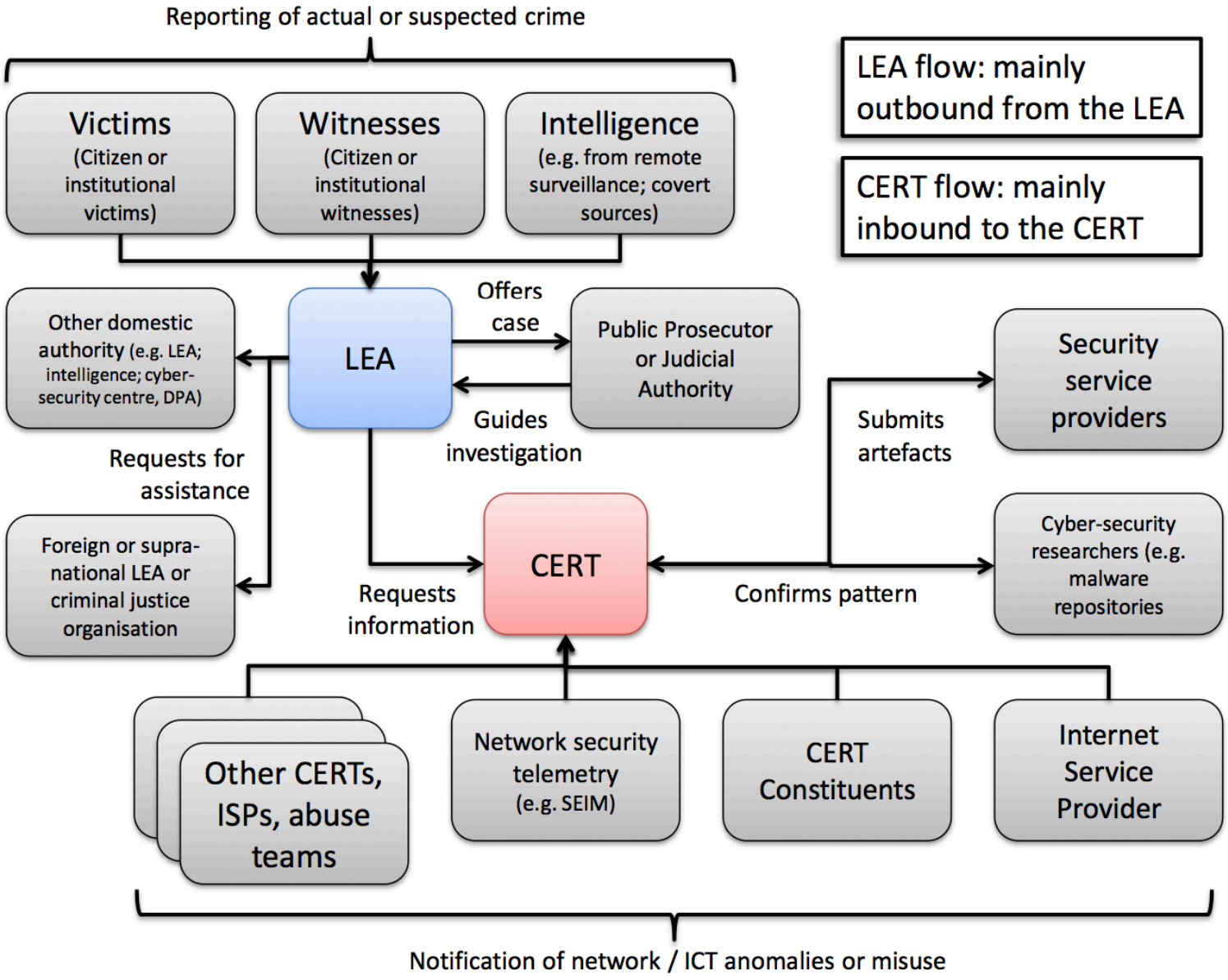
- Number of person-hours diverted from normal operations to react to the incident
- Number of person-hours to recover data
- Opportunity costs associated with the number of person-hours that could have been devoted on more productive tasks
- Cost associated with reproducing lost data
- Legal costs associated with prosecuting offenders
- Cost associated with loss of market advantage or share due to disclosure of proprietary information
- Cost associated with acquisition of additional security mechanisms ahead of budget cycle

LAW ENFORCEMENT INVOLVEMENT

	Computer Emergency Response Teams (CERTs)	Law Enforcement Authorities (LEAs)
Focus on different definitions of cybercrimes/attack	Unintentional incidents; attacks against the confidentiality, availability and integrity of ICT	Where there is evidence or suspicion of a crime (including fraud or crimes where the confidentiality, availability and integrity of ICT systems has not been affected)
Character of each community	Informal, problem solving based	Procedural, rules based
Objectives of each community	Remediation	Prosecution
Direction of request	Inward (CERTs more likely to have to respond to requests)	Outward (LEAs more likely to transmit requests)

CERT AND LEA COOPERATION STRATEGIC CHALLENGES

- Different definitions of cybercrimes/attacks
- Different meaning of information sharing
- Different character of community
- Different objectives of each community
  - CERTs focus on remediation
  - LEAs focus on evidence acquisition and integrity
- Different types of information
- Different directions of requests


Reporting of actual or suspected crime
LEA flow: mainly outbound from the LEA
CERT flow: mainly inbound to the CERT
Victims (Citizen or institutional victims)
Witnesses (Citizen or institutional witnesses)
Intelligence (e.g. from remote surveillance; covert sources)
Other domestic authority (e.g. LEA; intelligence; cyber-security centre, DPA)
LEA
Offers case
Guides investigation
Public Prosecutor or Judicial Authority
Requests for assistance
Foreign or supra-national LEA or criminal justice organisation
Requests information
CERT
Submits artefacts
Security service providers
Confirms pattern
Cyber-security researchers (e.g. malware repositories
Other CERTs, ISPs, abuse teams
Network security telemetry (e.g. SEIM)
CERT Constituents
Internet Service Provider
Notification of network / ICT anomalies or misuse

LEGAL AND REGULATORY FACTORS

- Legal pitfalls of data sharing:
  - Data protection laws
  - How can a CERT verify the legitimacy of data sharing requests?
  - Noncompliance with legal rules theoretically creates the risk of future legal proceedings being disrupted.
  - Information sharing *across international borders* can be problematic due to insufficient familiarity of international legal frameworks

NEXT LECTURE

The topic of the next lecture on the 7th of April will be:

Disaster Recovery: Preparation, Implementation, Operation and Maintenance

Recommended reading to prepare for the next lecture:

- Chapter 9 & 10 in Whitman, Mattord and Green

Note that the lecture will be held in K109 at 10:15-12:00

Please submit your anonymous evaluation of this course by answering the questionnaire on Fronter before next lecture.