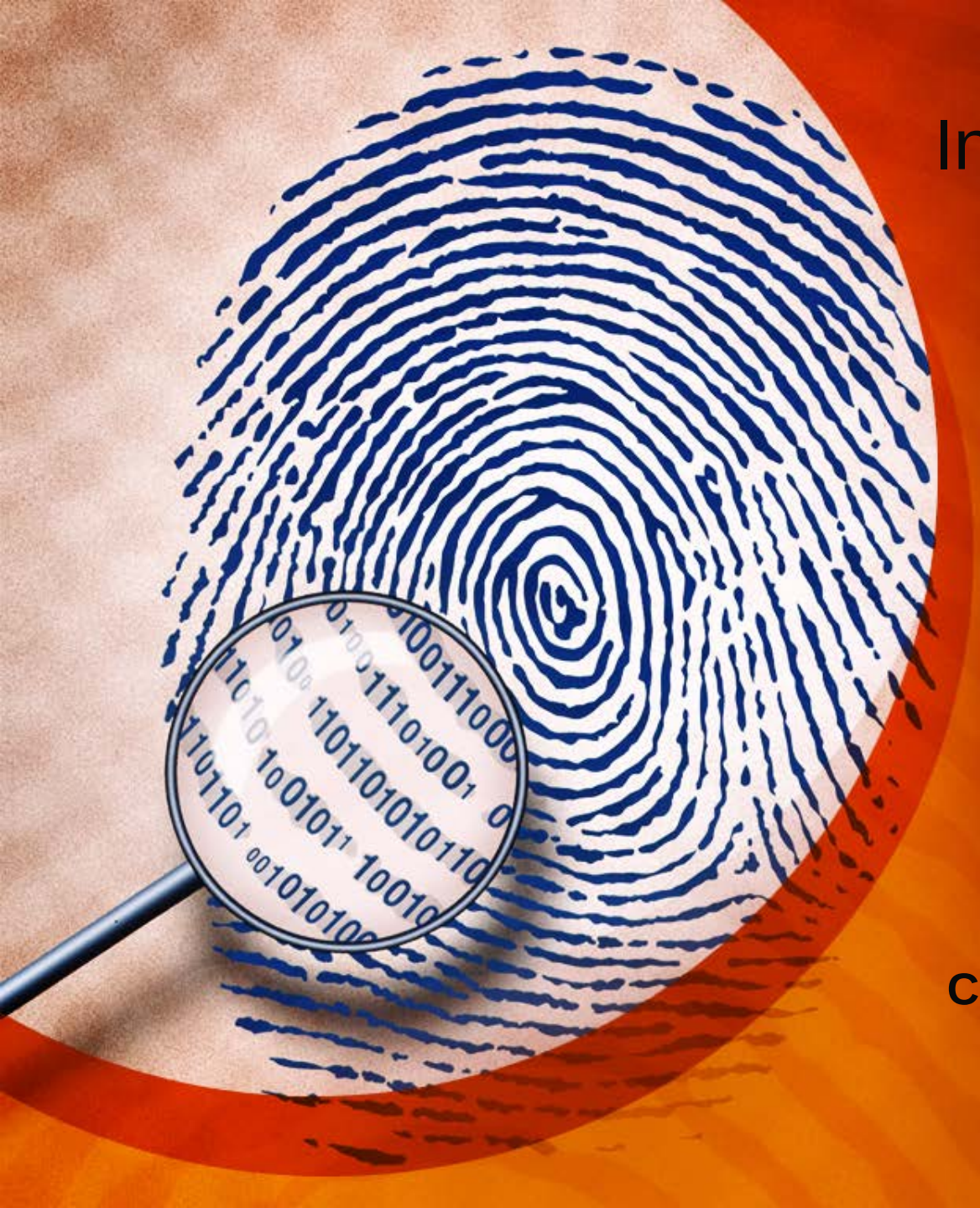


Incident Response and Risk Management

CISC 6920

James Doyle

Class Four- October 23, 2016

Todays

- IRCF: CH 1, 2 & 3
- Discuss Metrics Assignment, Staffing Paper
- Discuss Tools
- Cost of a Breach
- What is a plan?
- Discuss the Standards and Frameworks
- A little bit on ISO 27001
- Begin Review of CIRP- Methodology
- 11thHR: CHs 3,7 &9

Plans

- Please make sure your group has emailed it to me.
- Don’t start review just yet.

Digital Forensic/Incident Response

Digital Forensics is a discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law. In short, it is the process of using the scientific method to collect, analyze, and present evidence to the courts

Digital Forensics Process

Acquisition	The process of collecting/documenting digital media exhibits, then the creation of a bit copy. Image and Authenticate
Analysis	The actual process of investigation, which can take many forms
Reporting	Production of an evidence package along with a report describing the analysis and findings in layman's terms

Incident Response is an organized process to address and manage the impact of an incident. To combat incidents at scale, a wide variety of techniques can be used. Experience in fields such as security architecture, IT operations, and development can be beneficial to the team.

Incident Response Process

Detect	Review events, identify incidents, and escalate
Analyze	Information gathering and determination of the incident's priority Investigate the incident
Respond	Risk mitigating actions taken to prevent further impact to the organization
Recover	Near-term incident remediation, remediation strategy and roadmap development
Resume	Resume, to the extent possible, normal business operations and provide long term risk mitigation, long-term remediation, and document lessons learned

IRCF- Chapter One

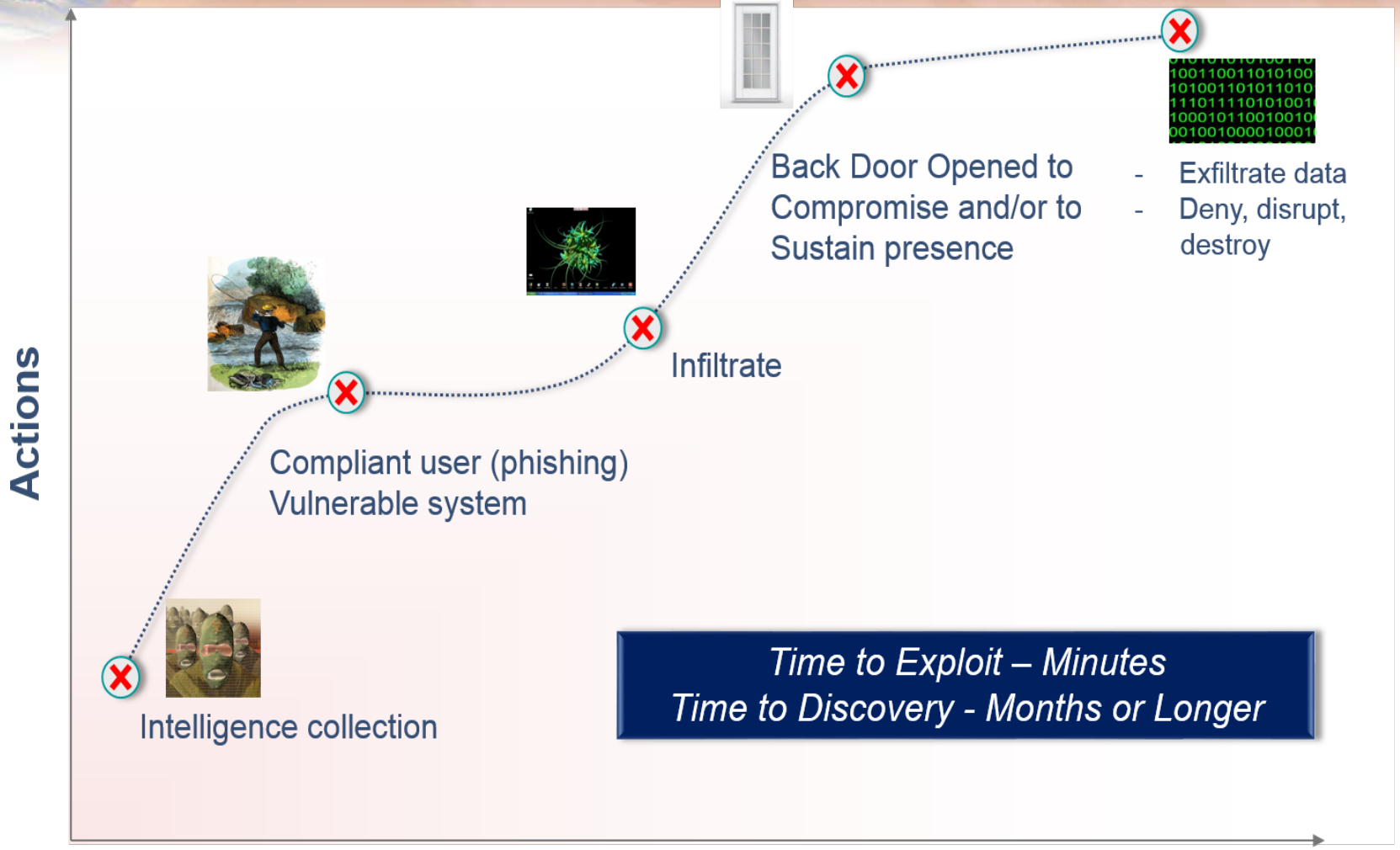
What is incident Response- pg 5

- Confirm whether or not an incident has occurred
- Provide rapid detection and containment
- Determine and document the scope of the incident
- Prevent a disjointed, non-cohesive response
- Determine and Promote facts and actual information
- Minimize disruption to business and network operations
- Minimize the damage to the compromised organization
- Restore normal operations
- Manage the public perception of the incident
- Allow for criminal or civil actions against perpetrators
- Educate senior management
- Enhance the security posture of a compromised entity against future incidents

Attack Lifecycle

- Initial Compromise
- Establish Foothold
- Escalate Privileges
- Internal Recon-
  - **Move laterally**
  - **Maintain presence**
- Complete Mission

Anatomy of a Cyber Attack



Concept of Attack Life Cycle

Note- Different from NIST IR Life Cycle

Book Has Seven, but we expand:

1. Selection of target through different motives:
   - Hacktivists
   - Criminal Group
   - Opportunist

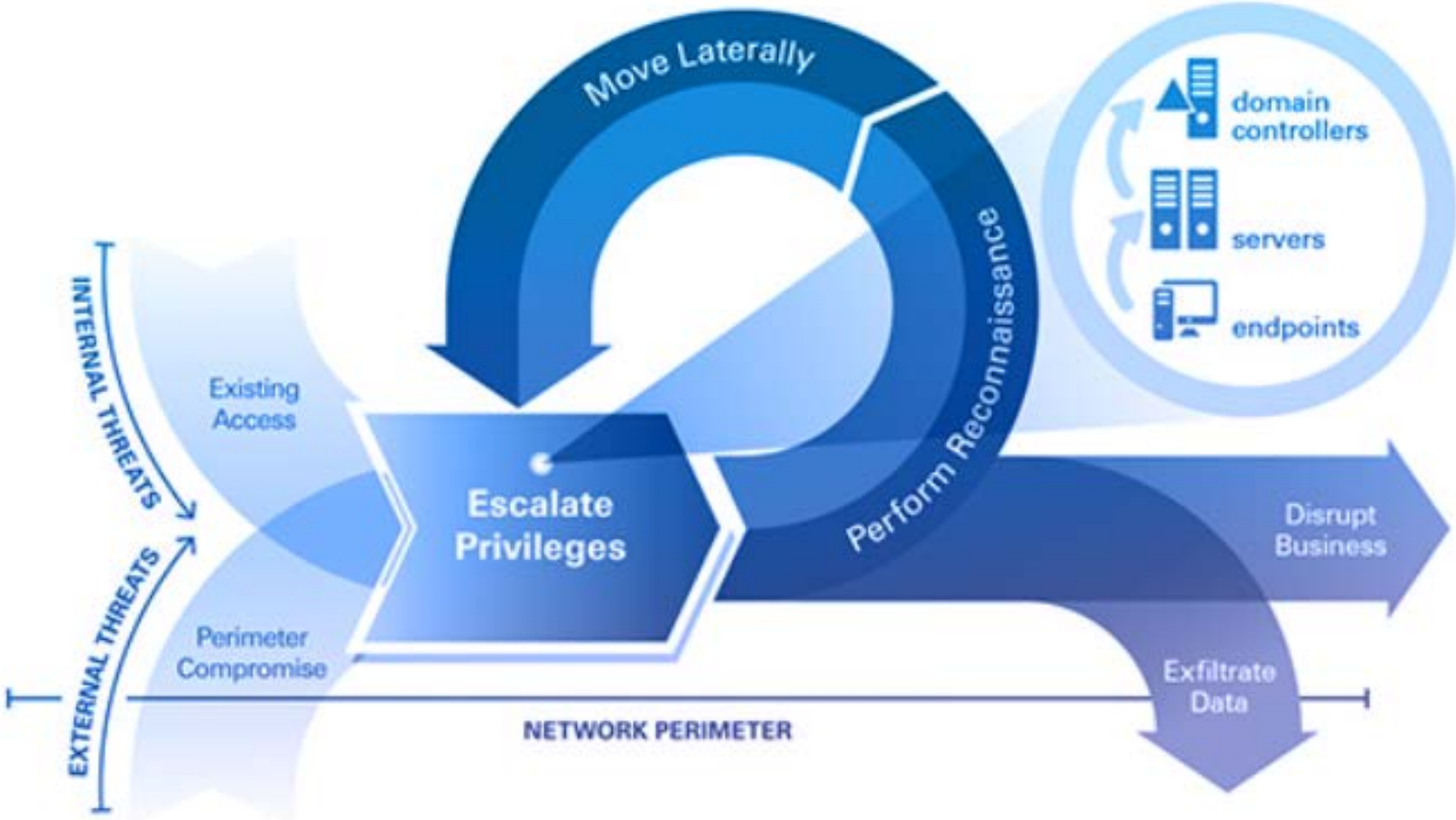
2. Reconnaissance:
   - Media Sources, Job Postings, Social Media
   - Scanning
   - Probing
3. Initial Compromise (methodology):
   - Spear phishing with custom malware
   - Third party Application exploitation
   - Web Vulnerability Exploitation

Concept of Attack Life Cycle

Continued

4. Establish Foothold
   - Custom Malware
   - Command & Control
5. Escalate Privileges
   - Password Cracking
   - VPN subversion
   - Back doors
   - Sleeper malware
6. Internal Recon
   - Critical system identification
   - System, Active Directory and user communications
     - (email, VOIP, IM, Cell Phones, Meetings)
7. Move laterally (netuse commands, reverse shell)
8. Maintain presence
9. Complete Mission
   4. Staging servers
   5. Data Consolidation
   6. Data Theft
   7. Disrupt Business

Cyber Ark


Move Laterally
Perform Reconnaissance
domain controllers
servers
endpoints
INTERNAL THREATS
EXTERNAL THREATS
Existing Access
Escalate Privileges
Disrupt Business
Perimeter Compromise
Exfiltrate Data
NETWORK PERIMETER

IRCF- Chapter Two

- Risk Management
- What is an event
- What is an incident
- What is an adverse event
- What is a cyber incident

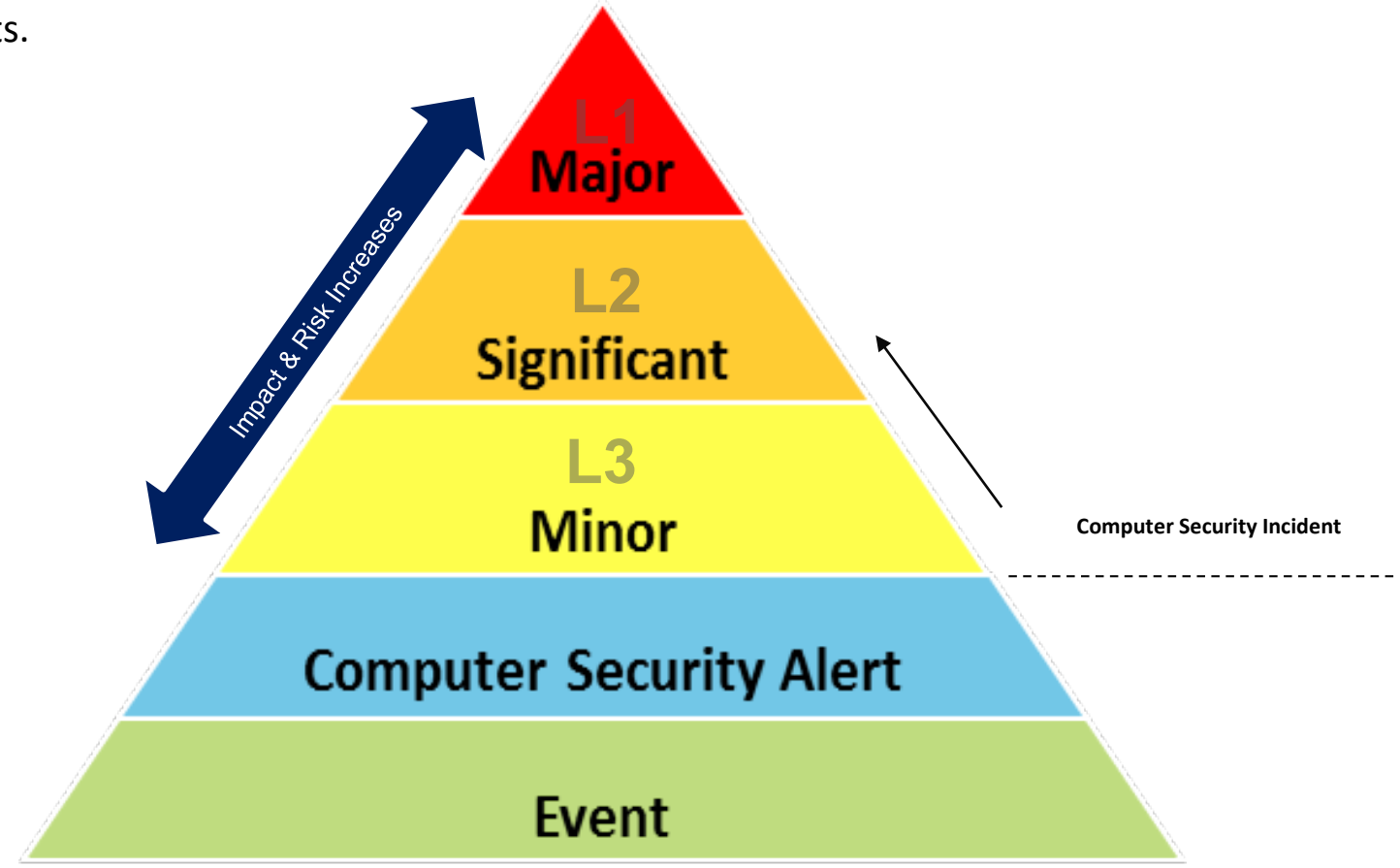
Definitions- Repeated

- The following definitions in this section are aligned with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 and 800-53 standards.

- **Event**
- An event is defined as an observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt.
- **Cyber Security Alert**
- A cyber security alert is an event that is, or has the potential to be, a cyber security incident. Cyber security alerts should be investigated to confirm whether they are a cyber security incident (true positive). Once confirmed, the incident severity, along with other criteria, should be defined in order to enact the proper cyber security handling protocol.
- **Cyber Security Incident**
- A cyber security incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits. A cyber security incident is an incident in which there has been, or there is the imminent potential for, a violation of security policies, acceptable use policies, or standard security practices.

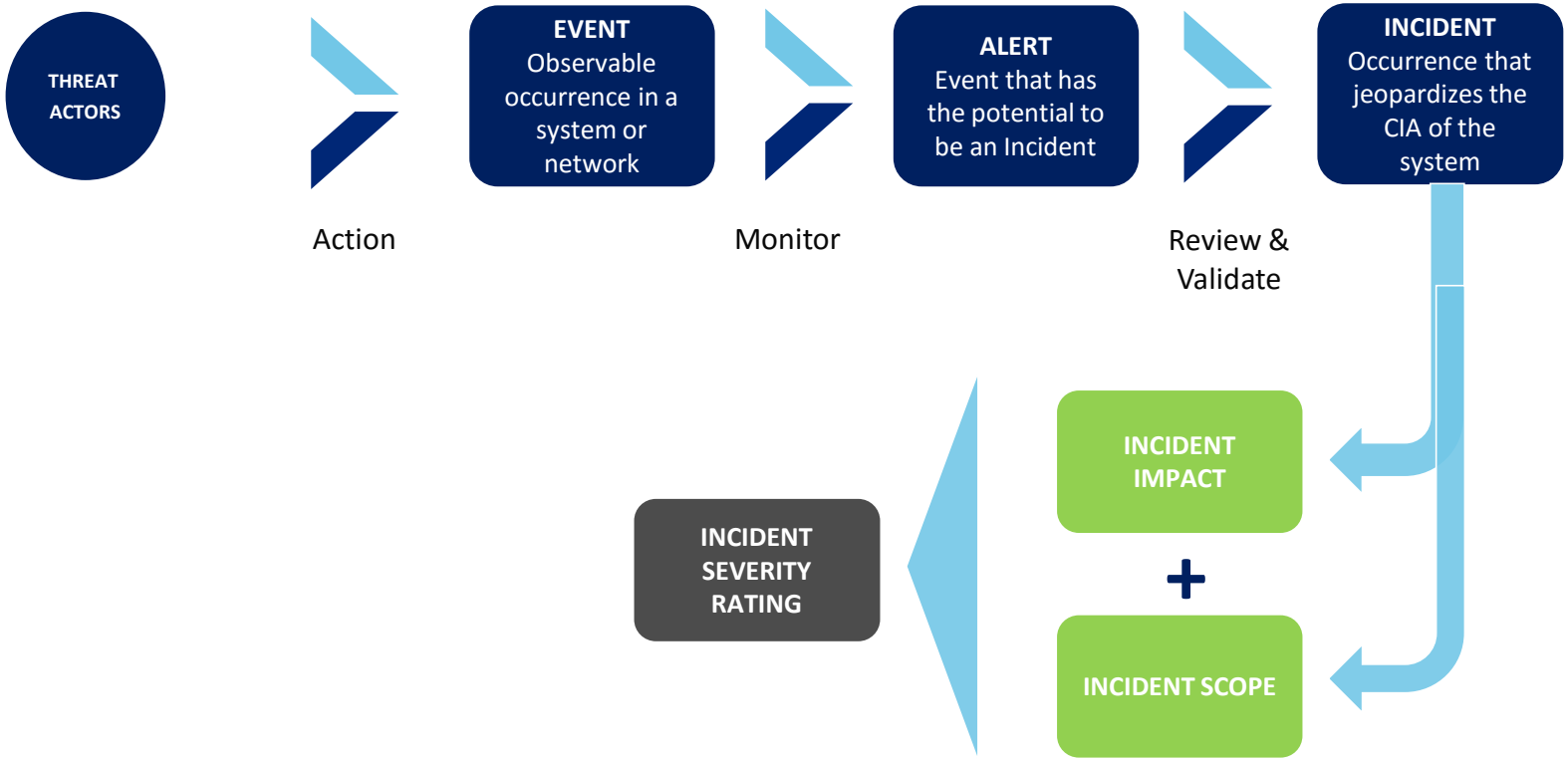
CSIRT Framework:

The CSIRT Plan outlines a holistic framework to provide clear guidance on roles and responsibilities along with specific criteria for prioritization, escalation, and communication of computer security incidents.



CSIRT Framework: Introduction

Computer security incident severity levels are used to classify computer security incidents based upon a number of factors (impact, threat type, incident type, and scope). The computer security incident severity level determines the magnitude of the response effort required by the appropriate teams. Response efforts are based on potential impacts and may change throughout the course of the investigation.



RM- What

- Value
- Location
- Cost to create
- Cost to replace

Threat Categories

- Threat categories are a combination of the threat actors' relationship with the organization and their focus relative to the organization. This provides added context to the cyber security incident that aids in the prioritization and the appropriate allocation of response resources.
- Therefore, threats are therefore be categorized as having one of the following location/employment based associations:
- **Internal/Insider**: An employee or contractor operating from within the organization. This threat has pre-existing trust, access, and (to some extent) inside knowledge of the organization.
- **External/Outsider**: A non-employee operating from outside of the organization. This threat typically has limited knowledge, trust, or access to the network. This type of threat is at a disadvantage compared to an insider.
- In addition, threats can be categorized as having one of the following types of focus against the organization:
- **Intentional** or **direct**: The threat is specifically focusing or intending to benefit from harming the organization. There is something the organization has that they are after.
- **Unintentional**, **accidental**, or **indirect**: The threat actor is not specifically focusing the organization, may not have intended to harm the organization, or is not concerned with the organization they are harming.

RM- Who wants it

External Indirect

External Direct

Internal Indirect

Internal Direct

Computer Security Threat Categories

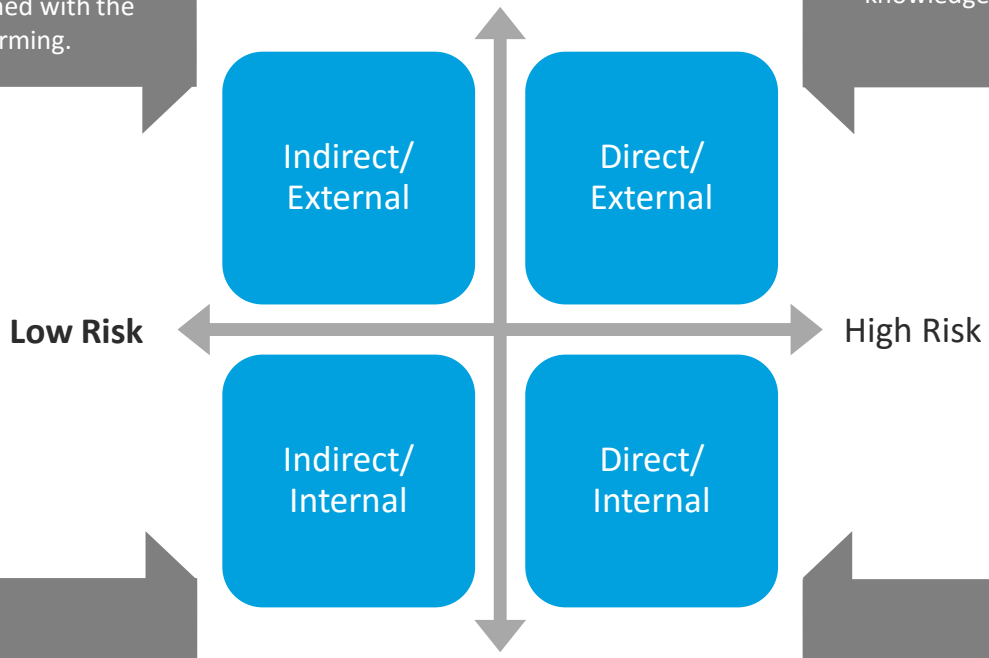
Threat categories are a combination of the threat actors' relationship with the organization and their focus relative to the organization. This information provides added context in prioritizing and appropriately allocating response resources.

Unintentional/Accidental/Indirect

The threat actor is not specifically focusing on the organization, may not have intended to harm the organization, or is not concerned with the organization they are harming.

External/Outsider

A non-employee operating from outside of the organization. This threat typically has limited knowledge, trust, or access to the network.



Threat Matrix

Internal/Insider

An employee or contractor operating from within the organization. This threat has pre-existing trust, access, and (to some extent) inside knowledge of the organization.

Targeted/Direct

The threat is specifically focusing or intending to benefit from harming the organization. There is something the organization has that they are after.

Computer Security Alerts Types

There are a number of different classifications for computer security alerts. These alert types are outlined below:

Computer Security Alert Types	Description
 **Suspicious File**	A file on an information system or other device that is potentially malicious or anomalous in nature.
 **Suspicious Network Activity**	Network traffic that is anomalous in nature and/or associated with malicious signatures.
Suspicious Behavior	Observed activities indicating potential malicious and/or criminal intent.
 **Suspicious Email/Attachment**	An email containing a file that is potentially malicious or anomalous in nature.
 **Data-Loss Prevention Alert**	A DLP alert that is triggered from a specific rule.

Computer Security Incident Types

There are a number of different classifications for computer security incidents. These incident types are outlined below:

Computer Security Incident Types	Description
 **Unauthorized Access**	An individual gains logical or physical access without permission to a network, system, application, data, or other resource.
 **Denial of Service (DOS)**	An attack that effectively prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DOS.
 **Malicious Code**	Installation of software or firmware (e.g., virus, worm, Trojan horse, or other code-based entity) intended to perform an unauthorized process that adversely impacts information system confidentiality, integrity, or availability.
Improper Usage	A person violates acceptable computing use policies.
 **Scan/ Probe/ Attempted Access**	This category includes any activity that seeks to access or identify a computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.
 **Other/Investigation**	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

Impact Classification

Incident scope is a variable that impacts incident severity, but may not be tied together in some cases. It is a combination of the number of assets, users, and records affected.

Rating	Description
1 (LARGE)	Enterprise wide or affecting a large number of customers or affecting a large number of records.
2 (MEDIUM)	Department wide or affecting medium number of customers or affecting medium number of records.
3 (SMALL)	Affecting low number of customers or affecting low number of records.

Computer security incidents are prioritized based on a series of factors, rather than a first-come, first-serve basis. The categories of impact are based on the following criteria:

Rating	Asset	Recoverability	Information	Brand/Reputation
1 (MAJOR)	Organization can no longer provide critical services to any (or a significant portion of) users.	Recovery from incident is impossible, unpredictable, and/or will require extreme measures.	Sensitive personally identifiable information (PII), protected health information (PHI), proprietary information, or classified data of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated.	Confirmed or high possibility reputational impact or disclosure.
2 (SIGNIFICANT)	Minimal effect; the organization can still provide critical services to all users but has lost efficiency.	Recovery from incident may require effort and resources beyond normal operations.	Sensitive or proprietary information was changed or deleted.	Minimal possibility of reputational impact or disclosure.
3 (MINOR)	No effect to the organization's ability to provide all services to all users.	Recovery from incident requires effort, but within normal operations.	No (or publicly available) information was exfiltrated, changed, deleted, or otherwise compromised.	No reputational impact or disclosure.

Computer Security Incident Severity

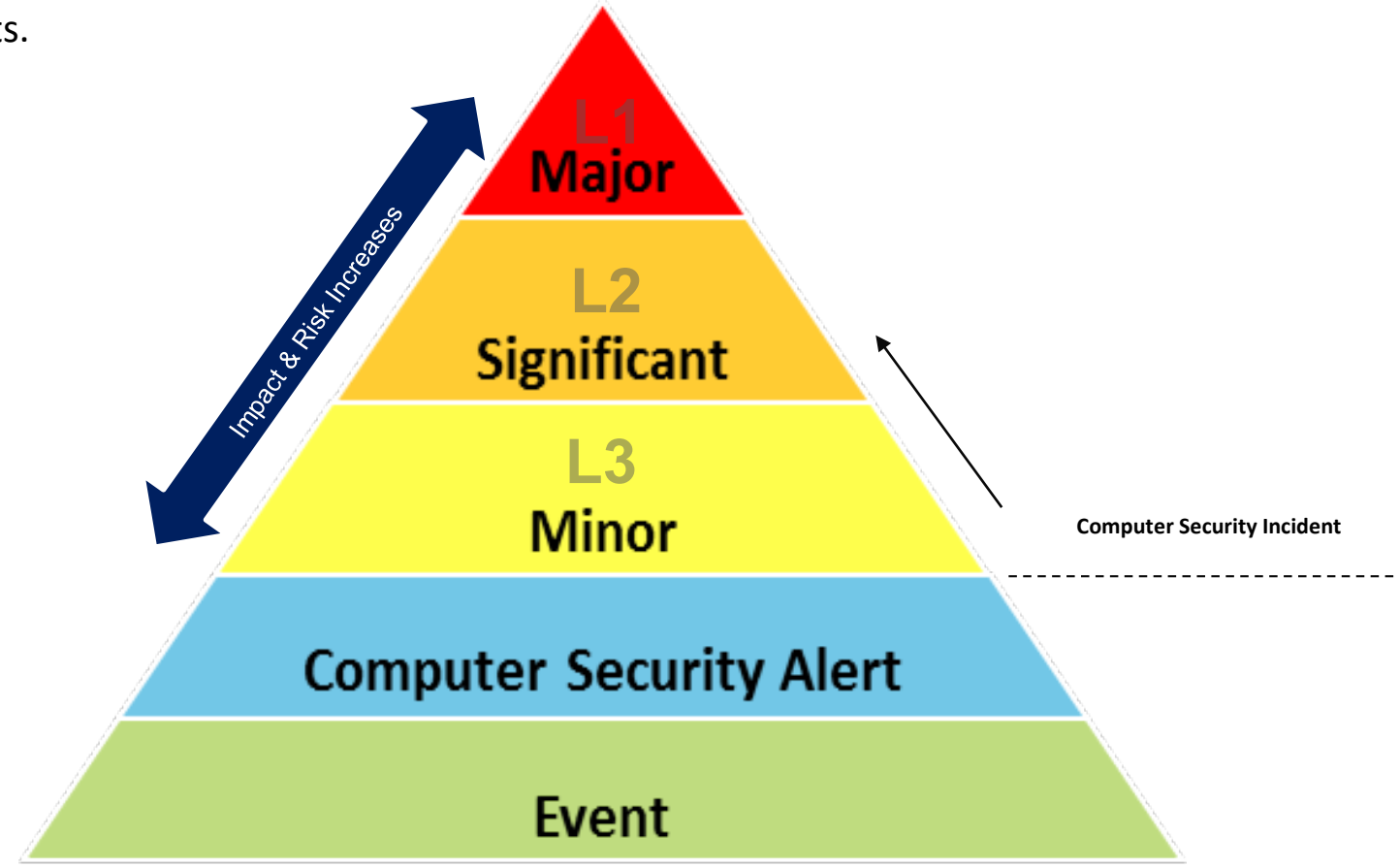
To determine the overall severity of a computer security incident, ***scope*** and ***weighted criteria ratings*** are combined and a suggested ***severity rating*** is calculated using the matrix which has been developed to assist in assigning both a severity rating as well as possible courses of action.

SEVERITY RATING MATRIX		*SCOPE*		
		1 (Large)	2 (Medium)	3 (Small)
IMPACT CRITERIA	*1 (MAJOR)*	L1	L1	L2
	2 (SIGNIFICANT)	L1	L2	L3
	3 (MINOR)	L2	L3	L3

Major Computer Security Incident -L1	An incident impacting or having a **high likelihood of impacting** a **significant volume** of sensitive information (e.g. PII, PHI, and PCI), users, critical assets, and/or electronic services. It has the potential to disrupt critical services across the enterprise. Recovery might be **impossible** and requires coordinated response from a number of various functional teams across the enterprise.
Significant Computer Security Incident- L2	An incident impacting or having the potential of **impacting sensitive information** (e.g. PII, PHI, and PCI), users, assets, and/or electronic services. It has the potential to disrupt services across departments or business units within the enterprise. Recovery time is **moderately unpredictable** and requires coordinated response from various functional teams across the enterprise.
Minor Computer Security Incident- L3	An incident having **minimal or no impact** to sensitive information (e.g. PII, PHI, and PCI), users, assets, and/or electronic services. It has the potential to cause a loss in efficiency and/or worsen over time. Recovery time is **predictable** and requires response efforts from the incident response team along with relevant subject matter experts.

CSIRT Framework:

The CSIRT Plan outlines a holistic framework to provide clear guidance on roles and responsibilities along with specific criteria for prioritization, escalation, and communication of computer security incidents.



Severity by Numbers

- This is just a placeholder

Likelihood Factors	
Host Events	Select
Num of Businesses Impacted	Select
Network Events	Select
Human Events	Select

Host Events	Weight
Select	0
>1 million events	2
10000 events	5
< 9000 events	6

Businesses Impacted	Weight
Select	0
Single Bus > 10	3
Multiple Bus > 10	6

Network Events	Weight
Select	0
>1 million events	27
10000 events	23
< 9000 events	19

Human Events	Weight
Select	0
>40 per day	16
<40 per day	14
< 10 events	12

Impact Factors	
PII Records Affected	Select
Data Classification	Sensitive

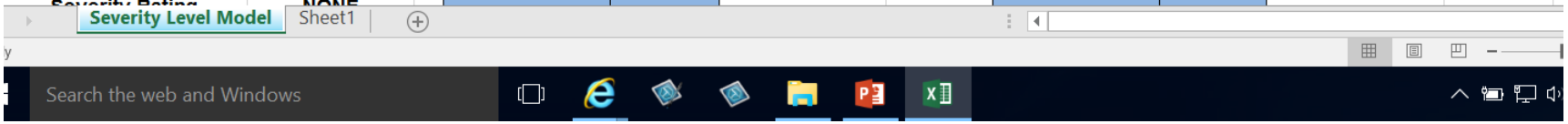
PII Records	Weight
Select	0
> 50	100
1 to 49	50
Other	10
Not Applicable	50

Data Classification	Weight
Select	0
Sensitive	100
Confidential	50
Public	10
Not Applicable	50

Sum of Impact Values	0.00
Sum of Impact Factors	2.00
Threat Level Score	0
Severity Rating	NONE

Likelihood Factors			
External Chatter	0	Intel Collection	0
Num of Biz Impacted	0		
Intel Requests	0	SUM	0
SUM	0		

Impact Factors	
Under Investigation	0
Incident Severity Count	100



IRCF- Chapter Two

- Risk Management
- What is an event
- What is an incident
- What is an adverse event
- What is a cyber incident

RISK- From OWASP

- RISK= Likelihood X Impact
- Threat agent involved
- The attack that will be used
- The vulnerability involved
- The impact of a successful exploit on the business.

Likelihood: Threat Actor

- Skill level
  - Security penetration skills (9)
  - Network and programming skills (6)
  - Advanced computer user (5)
  - Some technical skills (3)
  - No technical skills (1)
- Motive: find and exploit this vulnerability?
  - Low or no reward (1)
  - Possible reward (4)
  - High reward (9)
- Opportunity: What resources and opportunities are required
  - Full access or expensive resources required (0)
  - Special access or resources required (4)
  - Some access or resources required (7)
  - No access or resources required (9)
- Size : How large is this group of threat agents?
  - Developers (2)
  - System administrators (2)
  - Intranet users (4)
  - Partners (5)
  - Authenticated users (6)
  - Anonymous Internet users (9)

Likelihood: Vulnerability

Ease of discovery

How easy is it for this group of threat agents to discover this vulnerability?

Practically impossible (1),
difficult (3),
easy (7),
automated tools available (9)

Ease of exploit

How easy is it for this group of threat agents to actually exploit this vulnerability?

Theoretical (1),
difficult (3),
easy (5),
automated tools available (9)

Awareness

How well known is this vulnerability to this group of threat agents?

Unknown (1),
hidden (4),
obvious (6),
public knowledge (9)

Intrusion detection

How likely is an exploit to be detected?

Active detection in application (1),
logged and reviewed (3),
logged without review (8),
not logged (9)

Impact: Technical

Loss of confidentiality: How much data could be disclosed and how sensitive is it?

Minimal non-sensitive data disclosed (2), minimal critical data disclosed (6), extensive non-sensitive data disclosed (6), extensive critical data disclosed (7), all data disclosed (9)

Loss of integrity

How much data could be corrupted and how damaged is it?

Minimal slightly corrupt data (1), minimal seriously corrupt data (3), extensive slightly corrupt data (5), extensive seriously corrupt data (7), all data totally corrupt (9)

Loss of availability

How much service could be lost and how vital is it?

Minimal secondary services interrupted (1), minimal primary services interrupted (5),
extensive secondary services interrupted (5),
extensive primary services interrupted (7),
all services completely lost (9)

Loss of accountability

Are the threat agents' actions traceable to an individual?

Fully traceable (1),
possibly traceable (7),
completely anonymous (9)

Impact : Business

Financial damage: How much financial damage will result from an exploit?
- Less than the cost to fix the vulnerability (1),
- minor effect on annual profit (3),
- significant effect on annual profit (7),
- bankruptcy (9)

Reputation damage : Would an exploit result in reputation damage that would harm the business?
- Minimal damage (1),
- Loss of major accounts (4),
- loss of goodwill (5),
- brand damage (9)

Non-compliance :How much exposure does non-compliance introduce?
- Minor violation (2),
- clear violation (5),
- high profile violation (7)

Privacy violation : How much personally identifiable information could be disclosed?
- One individual (3),
- hundreds of people (5),
- thousands of people (7),
- millions of people (9)

Recovery- Price Effort

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology#Step_1:_Identifying_a_Risk

Severity

Threat agent factors			
Skill level	Motive	Opportunity	Size
5	2	7	1

Vulnerability factors			
Ease of discovery	Ease of exploit	Awareness	Intrusion detection
3	6	9	2

Overall likelihood=4.375 (MEDIUM)

Technical Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability
9	7	5	8
Overall technical impact=7.25 (HIGH)			

Business Impact			
Financial damage	Reputation damage	Non-compliance	Privacy violation
1	2	1	5
Overall business impact=2.25 (LOW)			

Overall Risk Severity

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

- In the example above, the likelihood is medium and the technical impact is high, so from a purely technical perspective it appears that the overall severity is high. However, note that the business impact is actually low, so the overall severity is best described as low as well. This is why understanding the business context of the vulnerabilities you are evaluating is so critical to making good risk decisions.

Other Examples

Likelihood Factors	
Host Events	Select
Num of Businesses Impacted	Select
Network Events	Select
Human Events	Select

Host Events	Weight
Select	0
>1 million events	2
10000 events	5
< 9000 events	6

Businesses Impacted	Weight
Select	0
Single Bus > 10	3
Multiple Bus > 10	6

Network Events	Weight
Select	0
>1 million events	27
10000 events	23
< 9000 events	19

Human Events	Weight
Select	0
>40 per day	16
<40 per day	14
< 10 events	12

Impact Factors	
PII Records Affected	Select
Data Classification	Sensitive

PII Records	Weight
Select	0
> 50	100
1 to 49	50
Other	10
Not Applicable	50

Data Classification	Weight
Select	0
Sensitive	100
Confidential	50
Public	10
Not Applicable	50

Sum of Impact Values	0.00
Sum of Impact Factors	2.00
Threat Level Score	0
Severity Rating	NONE

Likelihood Factors			
External Chatter	0	Intel Collection	0
Num of Biz Impacted	0		
Intel Requests	0	SUM	0
SUM	0		

Impact Factors	
Under Investigation	0
Incident Severity Count	100
LOG	2.00

Threat Level	%	Low Value	High Value
1 - Red	90%	252	
2 - Orange	70%	196	251
3 - Yellow	50%	140	195
4 - Green	30%	84	139
5 - Blue	15%	1	83

Assessment factors

- Scope is a variable that impacts incident severity, but may not be tied together in some cases. Incident scope is a combination of the number of assets, users, and records affected. Large medium small
- Impact-Asset, Recoverability, Information, Brand Reputation- Minor, Significant, Major

SEVERITY RATING MATRIX		SCOPE		
		1 (Large)	2 (Medium)	3 (Small)
IMPACT CRITERIA	1 (MAJOR)	1	1	2
	2 (SIGNIFICANT)	1	2	3
	3 (MINOR)	2	3	3

						SCOPE				
						1	2	3	4	5
						Enterprise Large Number Customers affected	Major Facility Significant Number of Customers affected	Satellite Facility Department Small Number Customers affected	Small Facility Multiple Users Minimal Number of Customers affected	Single User No Customer Impact
DESCRIPTION			ASSETT	RECOVERABILITY	IMPACT		SEVERITY			
CRITICAL	CRITERIA	1	High Level Application affected Significant customer data lost/stolen	Recovery from incident is not possible or will require extreme measures to complete	Safety of customers or employees threatened Significant revenue impact World Wide Implications	1	1	1	2	3	3
MAJOR		2	Core IT Intrastructure affected Affected assett contains sensitive data	Recovery from incident requires considerable effort beyond normal operations	Potential impact to network operations Potential regulatory compliance impact	2	1	2	2	3	3
MODERATE		3	Mid Level Application affected Server or non-core infrastructure affected	Recovery from incident requires beyond normal operations	Potential brand or reputation impact	3	2	2	3	3	4
MINOR		4	Low Level Application affected Workstations affected	Recovery from incident requires significant effort but within normal operations	Non-significant functional impact	4	2	3	3	4	4
NOT SIGNIFICANT		5	No Application affected Workstations affected	Recovery from incident requires minimal effort within normal operations	Neglible functional impact	5	3	3	4	4	5

Assessing Risks

Two basic types:

1. **Quantitative:** Relating to, concerning, or based on the **amount or number** of something.
   - Requires good data regarding actual cost of the loss or impact of a threat and how frequently the threat will occur.
   - Expresses "probability" as a percentage or ratio, i.e.,

     $$\frac{\text{the number of outcomes in an exhaustive set of equally likely outcomes that produce a given event}}{\text{divided by the total number of possible outcomes}}$$

   - **Basic concept:** ***the more ways a particular event can occur in given circumstances, the greater the probability that it will occur.***
   - Effectively assessing quantitative probability requires knowing and recognizing as many circumstances that could produce the loss as possible.

2. **Qualitative:** Relating to that which is **characteristic of something** and which makes it what it is.
   - The most widely used approach to risk analysis. Actual probability data is not required and only estimated potential loss or impact is used.

Risk Analysis: ASIS

Quantitative Approach

- Fundamental elements: (1) the event's probability and (2) the computed likely loss.
- These two elements produce a single figure: the Annual Loss Expectancy (ALE).

  ALE = threat probability X the value of the potential loss
- Ranking events in order of ALE quantifies the "risk" and facilitates decisions based upon this value.
- Caveats: Availability, unreliability, and inaccuracy of the data regarding replacement costs and threat probability affect ALE validity.
- Probability is rarely precise and can promote complacency. Controls and countermeasures often tackle various potential events and the events themselves are frequently interrelated.
- Notwithstanding the drawbacks, a number of organizations have successfully adopted quantitative risk analysis.

Qualitative Approach

Qualitative Approach

- Assigns a relative value to assets based on replacement cost, criticality, or impact of recovery. Example: FEMA uses a combination of a seven-level word-based scale and a ten-point numeric scale (1 = very low, 10 = very high).
- Assigns relative value to threats, based on their probability. Example: FEMA uses a value of one to ten based on the likelihood (1 = very low, 10 = very high).
- Computes risk to any asset for a particular threat by the following equation:

Risk = Impact X Likelihood

ALE

Annual Loss Expectancy Equation

$$ALE = \frac{10^{(f+i-3)}}{3}$$

i = the *"cost valuation"* (impact) of the event in successive values such as *i = 1 ($10); i = 2 ($100); i = 3 ($1000), etc.*

f = the *"estimated frequency"* of the event in successive values such as *f = 1 (once in 300 years); f = 2 (once in 30 years); f = 3 (once in 3 years), etc.*

The Risk Equation

The Risk Equation

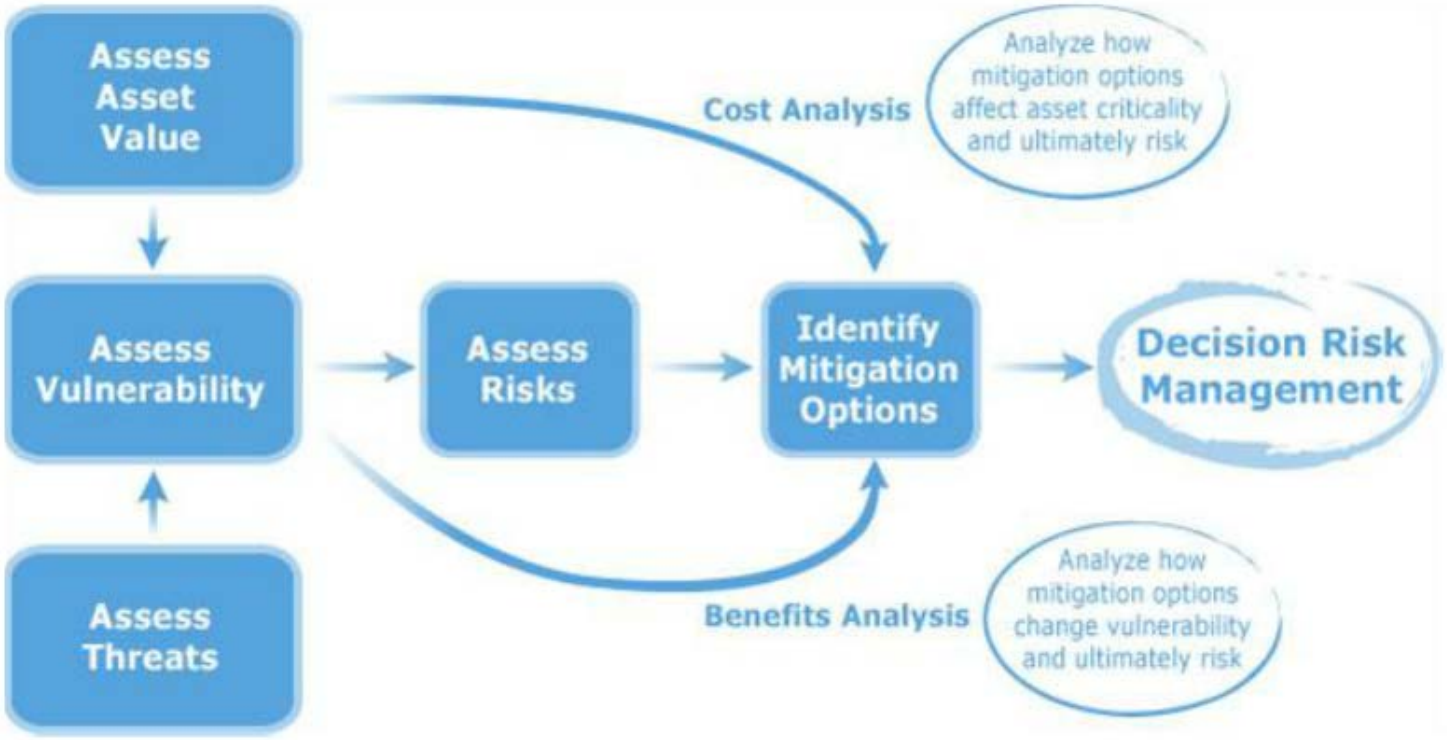
$$R = P_A * [1-(P_i)]*C$$

- R = Risk to the facility of an adversary gaining access to assets (ranges from 0 to 1.0)
- P_A = Probability of an adversary attack during a period of time
- P_i = Probability of attack interruption (e.g., interruption by security force response)
- C = Consequence value

Note: If P_i is the probability of interruption, then $[1-P_i]$ must be the probability of the adversary being successful.

* The Design and Evaluation of Physical Security Systems, Garcia, Mary Lynn, Butterworth-Heinemann, 2001

Risk Analysis Overview



Valuing Assetts

Valuing Assets

- To help assign a value and to rank critical assets by priority, consider the following factors:
  - Injuries or deaths related to facility or infrastructure damage
  - Replacement costs of assets
  - Loss of revenue due to lost functions
  - Existence of backups and systems redundancy
  - Availability of replacements
  - Critical support agreements and lifelines in place
  - Critical or sensitive information value
  - Impact on reputation and loss of revenue

- Costs of assets can be direct or indirect.

Valuing Assetts

Valuing Assets (Continued)

Direct costs in determining value:

- Financial losses (e.g., the value of goods lost or stolen)
- Increased insurance premiums
- Deductible expenses on insurance coverage
- Lost business (e.g., stolen goods cannot be sold to consumers)
- Labor expenses (e.g., increase in security coverage post-event)
- Management time (e.g., dealing with the media)
- Punitive damages awards not covered by ordinary insurance

Indirect costs:

- Negative media coverage
- Long-term negative consumer perception (e.g., that a certain business location is unsafe)
- Additional public relations expenses to overcome poor image problems
- Lack of insurance coverage due to being considered higher risk
- Higher wages to attract future employees (to overcome negative perceptions)
- Shareholder derivative suits for mismanagement
- Poor employee morale, leading to work stoppages, higher turnover, etc.

Risk Mitigation

Risk Mitigation

- **Definition:** A systematic methodology used by senior management to reduce overall operational risk.
- **Techniques:**
  - **Risk Assumption -** Accept the potential risk and continue security operations "as is." Alternatively, implement some controls to lower risk to an acceptable level. (No Cost)
  - **Risk Avoidance -** Avoid risk by eliminating its cause and/or consequence (e.g., move assets to another location.) (Some Cost)
  - **Risk Limitation -** Limit risk by implementing controls that minimize the adverse impact (e.g., preventive, detective, and response controls). (Some Cost)
  - **Risk Transference -** Transfer risk by using other options to compensate for the loss, such as purchasing insurance. (Some Cost)
  - **Site Hardening -** Harden the site against as many threats as possible. (Greatest Cost).

Risk Assessment- ISC^2

- Qualitative
- Level of Risk= LHD X IMP
- Residual Risk- after countermeasures to
  - **Minimize**
  - **Transfer**
  - **Avoid**
  - **Accept**
  - **The left over.**

Risk Assessment- ISC²

- Quantitative
- SLE – Single Loss Expectancy
  - SLE= Difference between original value and remaining value after a single exploit
  - SLE= Asset Value($) X Exposure Factor
  - ARO= Annualized Rate of Occurrence
    - How many times a year
  - ALE= SLE X ARO
  - No countermeasure should be greater than the cost of the risk it mitigates, transfers or avoids

Example

- Company reviews logs, one breach in the last 30 days. Dollar Impact is $10K.
  - Security team's recommendation for countermeasure costs $30K.
  - Annual Loss= $120,000
  - Good Investment?

Risk Assignment/Acceptance

- Risk Avoidance-
  - discontinue activity because you don't want to accept it's risk
- Risk Transfer-
  - pass the risk to another entity like an insurance company. There is a cost, and not all risk can be transferred.
- Risk Mitigation
  - Elimination of or significant decrease in level of risk
- Risk Acceptance
  - Will engage or continue activity and pay the cost

Other Frameworks: ERM

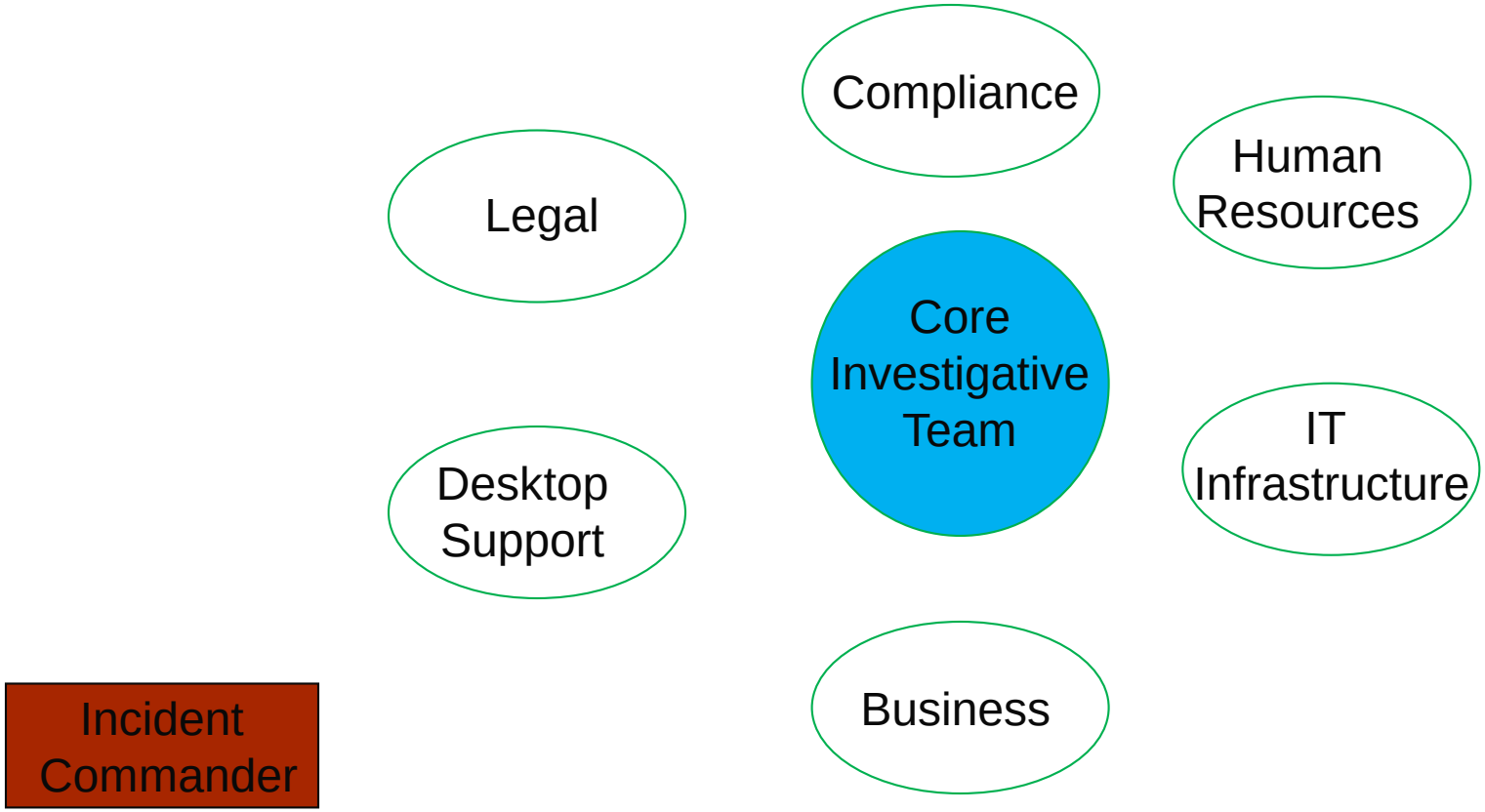
- COSO:2013
- ISO 27005: 2008
- AS/NZS and 31000: 2009
- ISO Guide 73: 2009
- NIST Special Publications 800-37 & 800-39
- ISACA:2009 RISK IT Framework

IRCF- What are goals of IR

- Investigate & Remediate
  - **Stop the bleeding**
  - **Catch the bad guy?**
- Determine Initial attack vector
- Determine malware and tools used
- What systems affected, and how
- Damage assessment
- Is incident ongoing
- Establish time frame
- Remediate: from investigation develop and implement a remediation plan

IR- Who is Involved

- Not just IT incident: business impact



IR Team- Talent

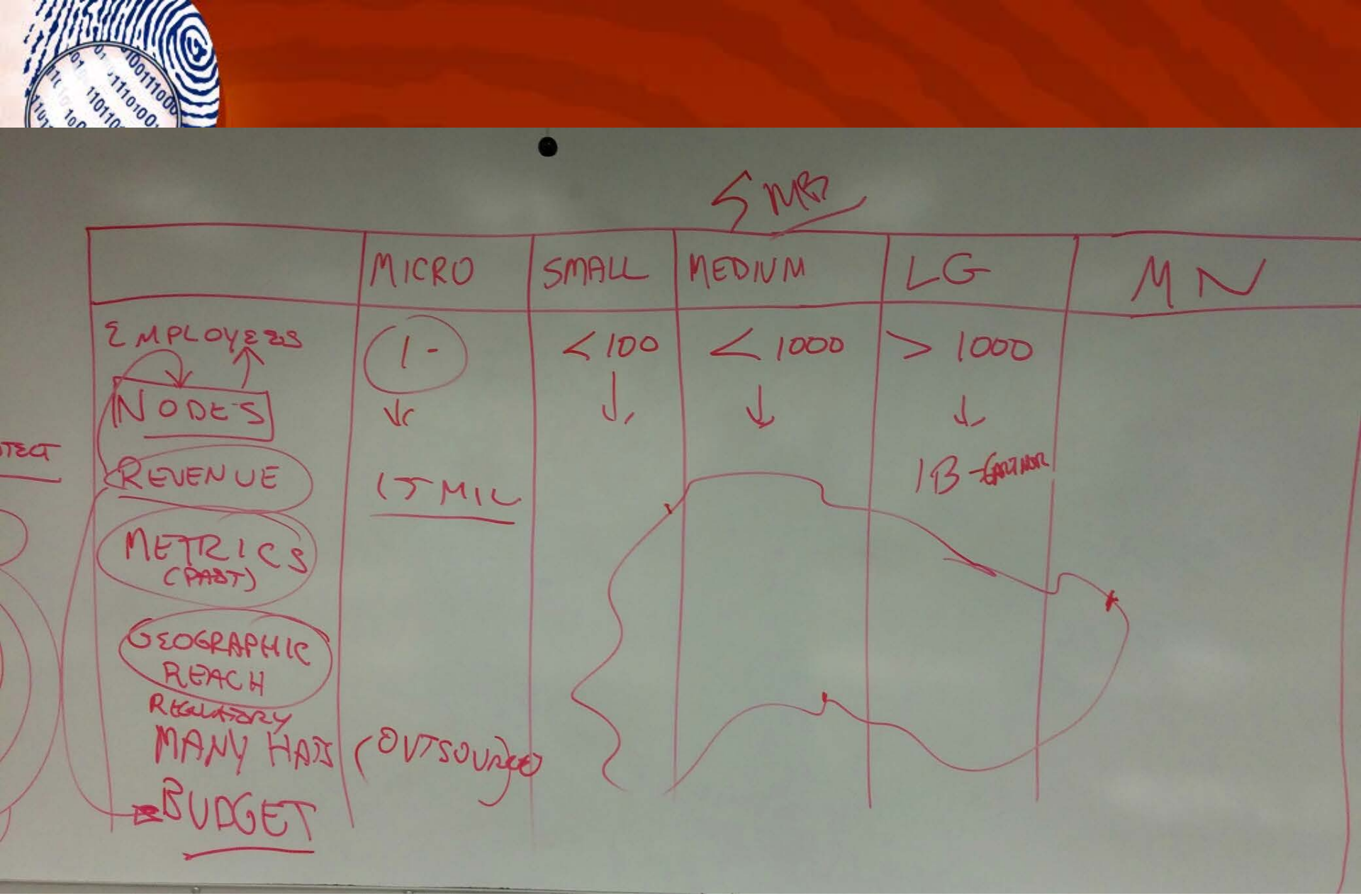
- In house vs. outsourcing:
  - **Cost of maintaining an IR Team**
  - **Culture of outsourcing**
  - **Mandated by regualtors**
  - **Experienced Investigators**
  - **Lack of in house specialization, double hatting not an option.**

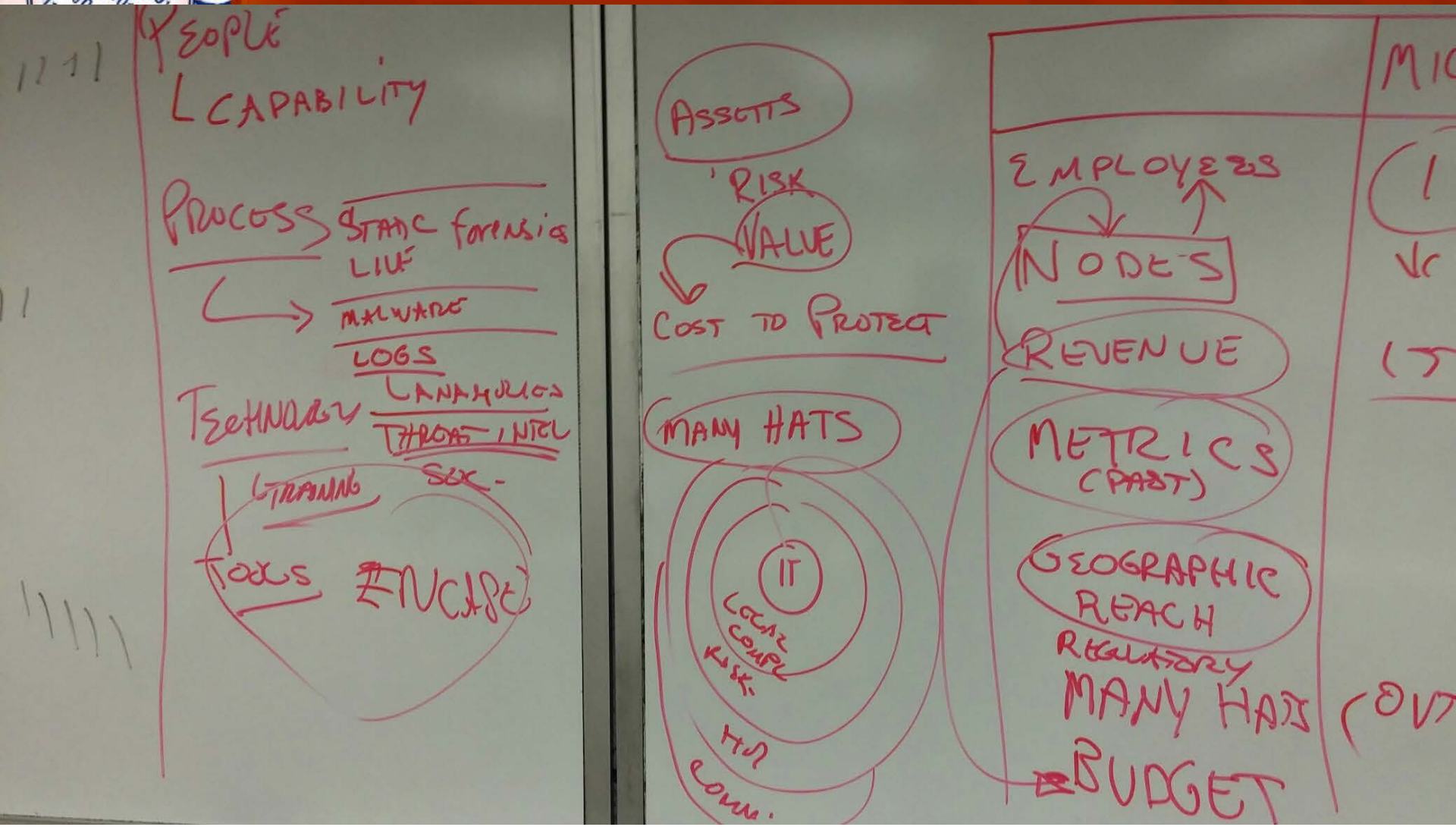
IR Talent- Skills required

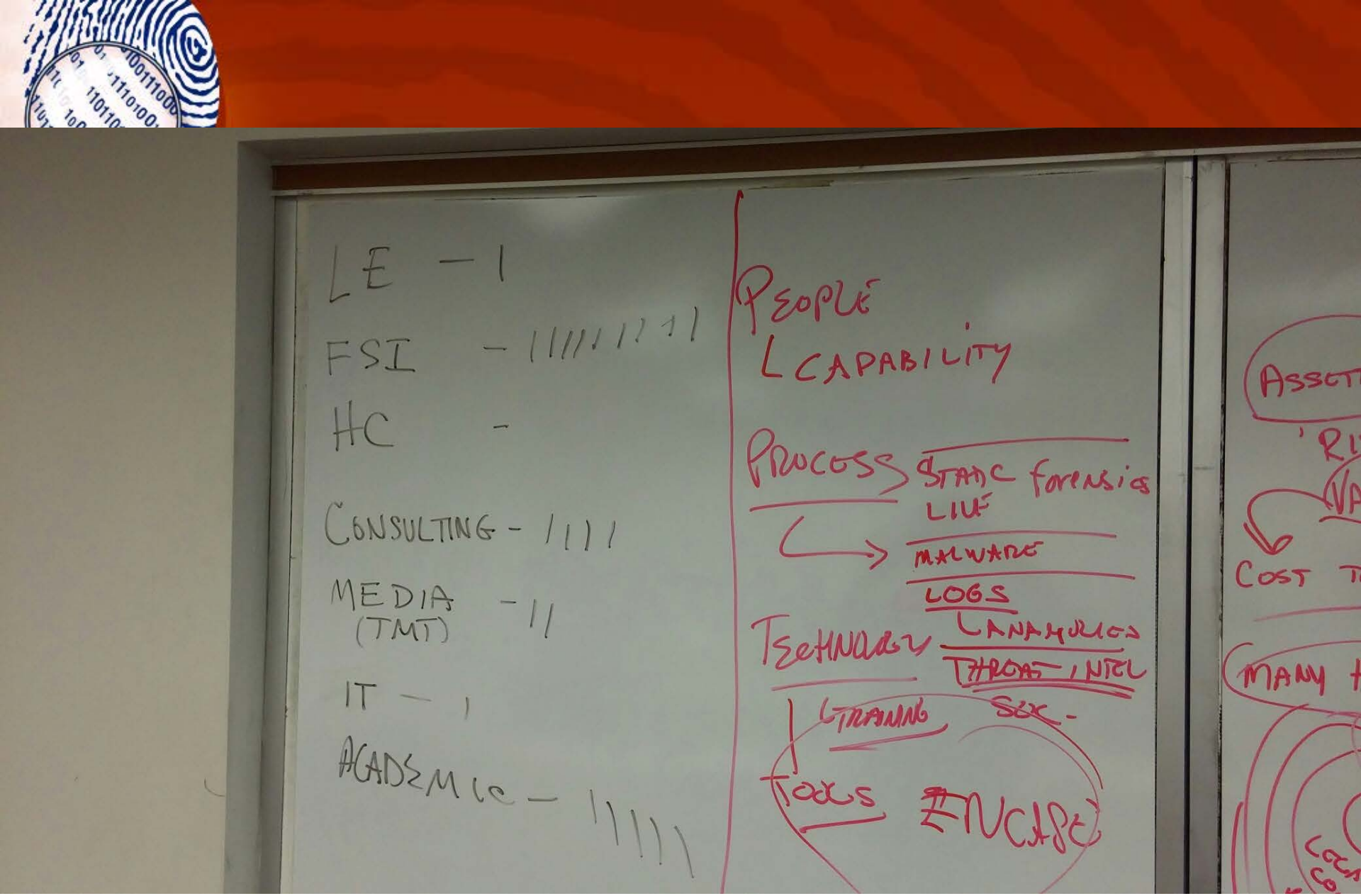
- Fundamentals:
  - **Observation**
  - **Communication**
  - **Classification**
  - **Measurement**
  - **Inference**
  - **Prediction**

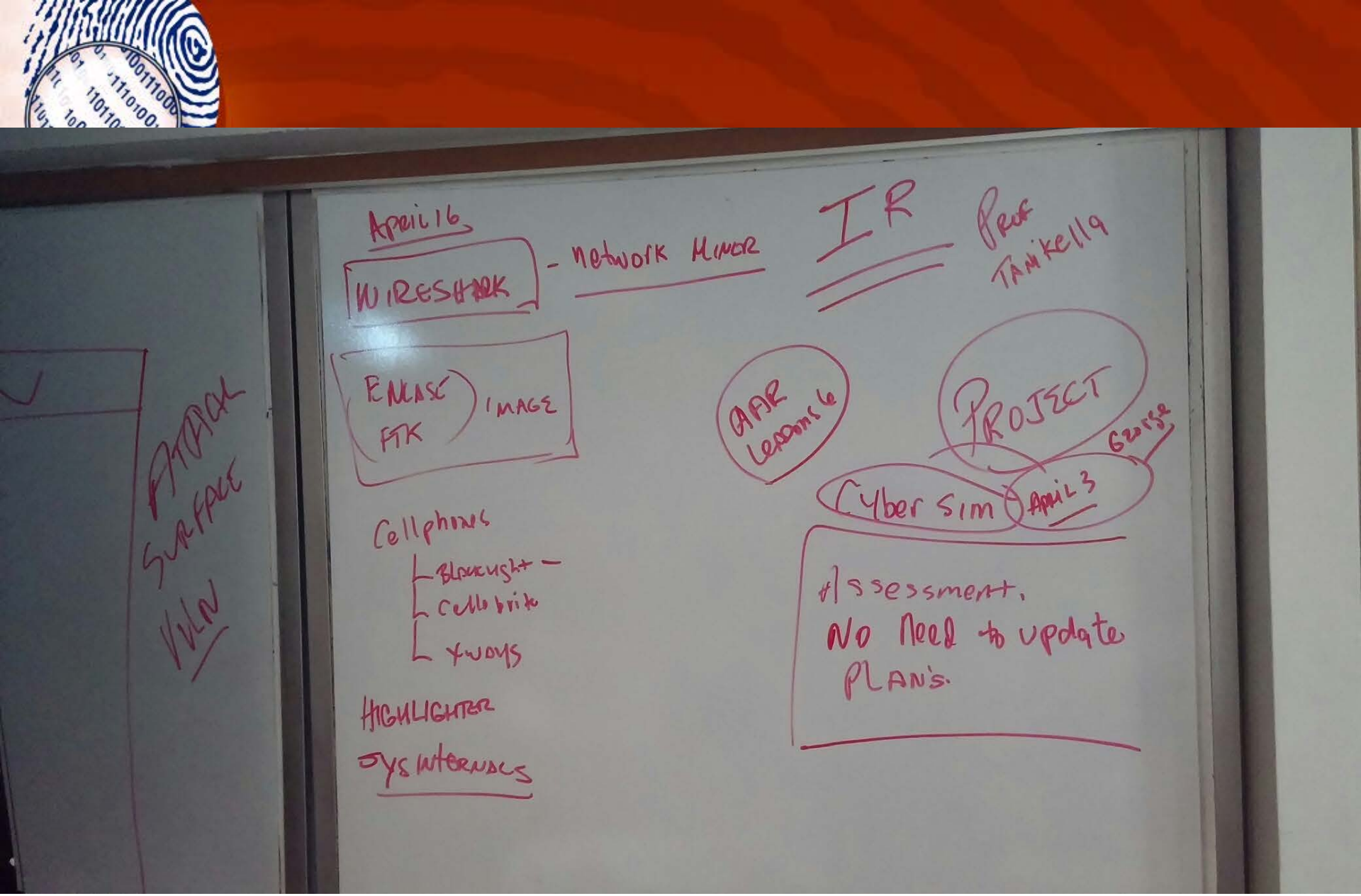
Capabilities and Qualities

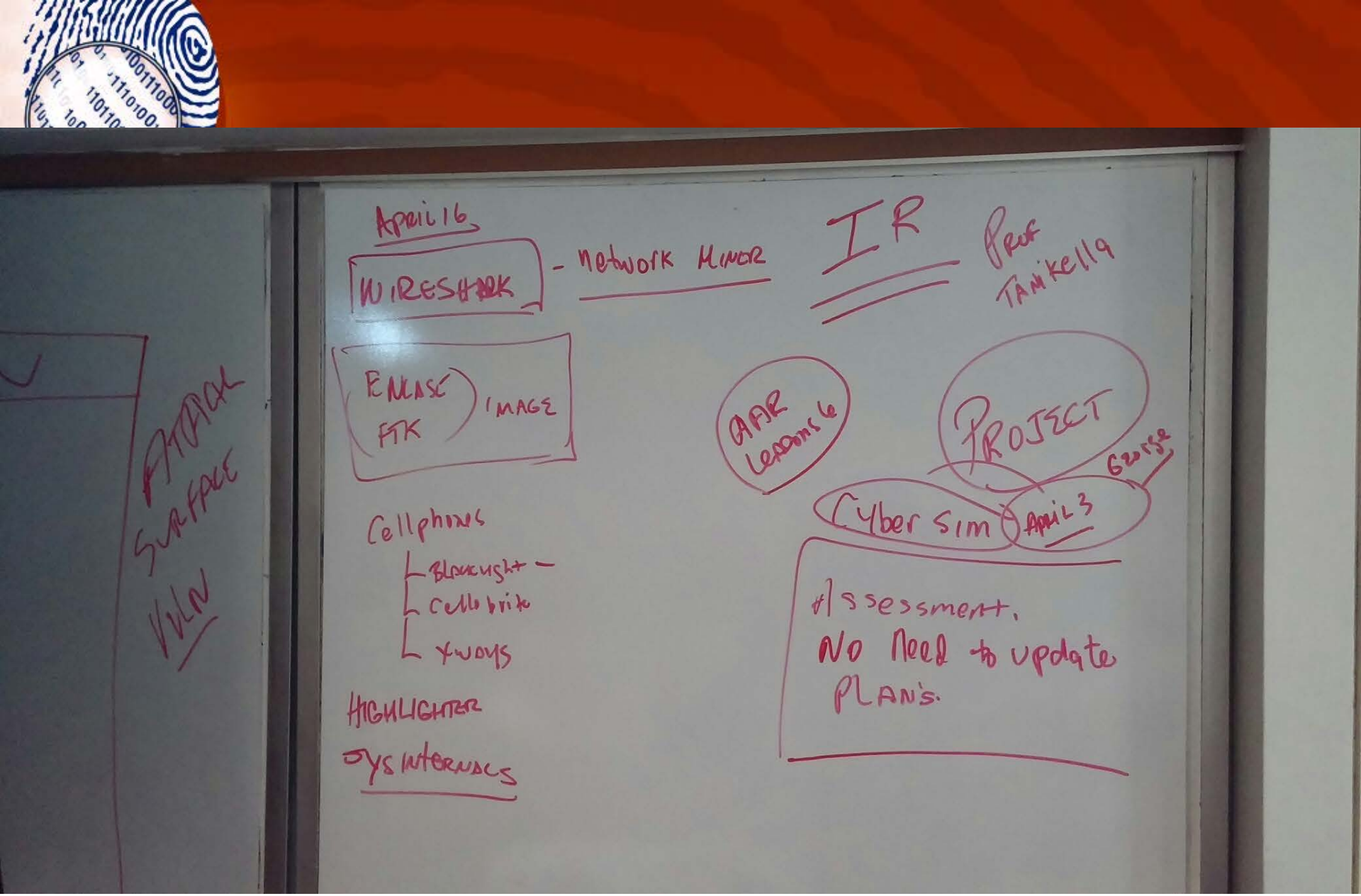
- High Technology Investigation acumen
- Computer forensics
- Network Traffic analysis
- Knowledge of industry applications
- Knowledge of enterprise IT
- Malicious code analysis


SMB
MICRO
SMALL
MEDIUM
LG
MN
EMPLOYEES
NODES
REVENUE
METRICS (PAST)
GEOGRAPHIC REACH
REGULATORY
MANY HATS
BUDGET
1-
< 100
< 1000
> 1000
1B
(OUTSOURCED


PEOPLE
CAPABILITY
PROCESS
STATIC forensics
LIVE
MALWARE
LOGS
LANGUAGES
TECHNOLOGY
THREAT INTEL
SOC
TRAINING
TOOLS
ENCASE
ASSETS
RISK
VALUE
COST TO PROTECT
MANY HATS
IT
LOCAL COMPL
RISK
HR
COMM.
EMPLOYEES
NODES
REVENUE
METRICS
(PAST)
GEOGRAPHIC
REACH
REGULATORY
MANY HATS
BUDGET


LE - 1
FSI - 11111111
HC -
CONSULTING - 1111
MEDIA (TMT) - 11
IT - 1
ACADEMIC - 1111
PEOPLE
CAPABILITY
PROCESS
STATIC forensics
LIVE
MALWARE
LOGS
TECHNOLOGY
LANGUAGES
THREAT INTEL
TRAINING
SDK
TOOLS
ENCASE


April 16
WIRESHARK - Network Miner
IR
Prof TANKELL9
ENCASE
FTK
IMAGE
AAR Lessons
PROJECT
Cyber Sim
April 3
George
Cellphones
Blacklight
Cellebrite
Xways
HIGHLIGHTER
Sys Internals
#1 assessment.
No Need to update
PLANS.
ATTACK
SURFACE
VULN


April 16
WIRESHARK
- network Minor
IR
Prof TANIKELLA
ENCASE
FTK
IMAGE
AAR Lessons
PROJECT
Cyber Sim
April 3
Cellphones
Blacklight
cellebrite
xways
HIGHLIGHTER
SYS INTERNALS
#1 assessment.
No Need to update PLAN's.
FTP
SURFACE
VULN

Process

- Analyze Data
  - **Malware analysis**
  - **Live response analysis (lead generation)**
  - **Forensic exam**
    - Registry
    - File inventory
    - Netflow

Remediation

Track Significant Information:

- List of Evidence Collected – Inventory and Chain of Custody
- List of affected systems- how identified
  - **Affected by exploit, or accessed suspiciously**
- List of files of interest
  - **Malware**
- List of accessed or stolen data
- List of significant attacker activity (timeline)
- IOCs (network and host)
- List of copmpromised accounts
- Task List- to dos

Report

- Templates for consistency

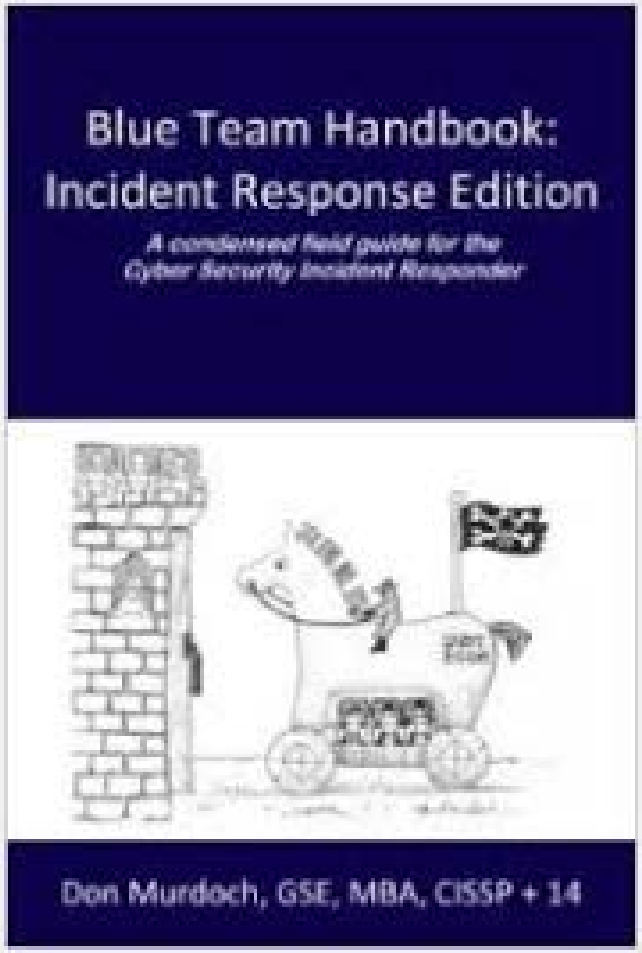
Case Studies

- Case Study 1- Groups 1 & 2
- Case Study 2- Groups 3 & 4
- Review and Create Timelines
- Be ready to present in 30 Minutes
- Locard principle
- Case Study 1- answer
- Case Study 2- answer

Reading

Incident Handler's Handbook

Blue Team Handbook



Chapter 3- Pre-Incident Preparation

- Preparing an organization
  - **Identifying risk, policies, outsourced IT, global infrastructure concerns, user education**
- Preparing the IR Team
  - **Communication procedures, resources: hardware, software, training and documentation**
- Preparing the infrastructure
  - **Asset management, instrumentation, documentation, investigative tools, segmentation and network services**

Identifying Risk

- Crown jewels- assets- are the quantified
- Reputation
- Confidential business information
- PII PHI PFI
- PCI
- Critical assets produce the gretest liability or potential loss - liability occurs through exposure
- Three biggest buzzword: dta breach, ransomware, insider threat

Policies that will impact Preparedness and Risk

- Acceptable Use Policy
- Security Policy
- Remote Access Policy
- Internet Usage Policy
- IR Response
- Communication
- BCP
- CR
- CM

Continuing On

- Outsourced IT
  - **Contracts, SLA, management**
- Global Infrastructure
  - Privacy and Labor Regulations
  - Team Coordination (follow the sun)
  - Data Accessibility
  - Company Structure

Basic Items in Plan

- Purpose/Scope/Overview – section that provides the purpose and overview of the document
- Roles and responsibilities matrix – section that defines what the roles and responsibilities are of stakeholders, aligned to the response process phases
- Incident severity matrix – section that defines the severity of an incident with associated examples
- Response workflow – section that graphically depicts the phases of the incident response lifecycle, with associated steps detailed out in text form
- Escalation procedures – section that details triggers, when and how incidents are escalated to the next severity level, and relevant stakeholder organization decision points
- Communications matrix – section that details when and how updates are communicated to stakeholders
- Lesson Learned- section that deals with after action review and identification of process or policy that needs enhancements, scheduled testing of plan and updating
- After Action- Evaluation, Enhancement and Testing
- Templates – an appendix with templates such as chain of custody form, sample breach notification letter, incident form

Table of Contents

Table of Contents

Table of Contents

Cyber Incident Response Plan Analysis

Analysis was conducted of the Information Technology Incident Response Plan (ITIRP, the plan) and the relevant Work Instructions and Operating Procedures by reviewing its components according to four categories: Functionality, Precision, Breadth and Association to identify and document gaps in the existing incident response plan. The questions below were used as a guide in the analysis, and in those cases where it was deemed an observation should be recorded to highlight a deficiency a recommendation accompanies it. If the organization has the capability or process identified in the question, there is no need for a recommendation.

- ***Functionality:***
  - Is the Plan operational?
  - Can it direct a response from intake to closure?
  - Does it contain the processes and procedures to respond, investigate, contain, eradicate and remediate according to leading practices?
  - Does it define communication protocols for internal and external information flow?
  - Are the definition for defining types of incidents, their severity and impact to the business and the escalation touch points present?
  - Does it contain a procedure for evidence collection, processing and handling?
  - Is there a mechanism to disseminate lessons learned from incidents or internal testing/exercises?
  - Is there a procedure to periodically test the effectiveness of the Plan and supporting processes?
  - Does the plan include a log retention policy?

- ***Precision:***
  - Is the policy of the company with regards to the criticality of a cyber incident response defined in the Plan?
  - Is the importance of Purpose & Scope conveyed?
  - Does the Plan indicate who the designated responders are within the organization?
  - Does the Plan indicate the Executive sponsor and the owner of the Plan?
  - Are workflows illustrated and documented?
  - Are escalation points defined with full call tree information?
  - Does the Plan follow accepted structure as defined by NIST, SANS or other published leading practices?
  - Are the roles and responsibilities for incident response defined?
  - Does the Plan define intake sources and the resulting triage and escalation?
  - Does the plan include the ways in which incident database has to be maintained and shared?
  - Does the plan include SLAs (when a team doesn't respond within specified time frame) ?

Cyber Incident Response Plan

Breadth

- Does the Plan reference Governance & Regulatory Standards the company should consider?
- Do the phases of Incident Response(IR) contain specific guidance on activities of the IR team?
- Are descriptions of tools, training, certifications required and skill levels of practitioners described?
- Does the document contain data classification frameworks for the company?
- Does the document identify incident types and severity and have run books for each scenario?
- Does the Plan have workflows for incident reporting and response?
- Are there workflows to define intake and the triage escalation for the incidents?
- Are there procedures to return the business to pre-incident status, and notification process?
- Is there a procedure to analyze and confirm eradication?
- Is there a periodic review implemented, possibly after industry trend report have been released?
- Are points of contact for inter-department collaboration listed?
- Does the plan establish mechanisms to prevent incidents by securing networks, systems and applications?
- Does the plan establish baseline level of logging and auditing on all systems and higher baseline on all critical systems ?

- ***Association***
  - Is the Plan integrated across businesses; are there other response plans escalated from and initiated by the Plan?
  - Does the company maintain relationships with external organizations: Law enforcement, ISACs, industry peers to conduct information sharing?
  - Is the decision-maker to refer cyber incidents to law enforcement identified?
  - Are there other response plans in which cyber should be linked, such as Business Continuity, Disaster Planning or Crisis Management?
  - Do specific entities have access to the incident reporting system?
  - Are past indicators or compromise retained for lessons learned and disseminated within the organization for risk, compliance and legal impact?
  - Does the Plan contain communications protocols, and are the collaboration points identified?
  - Does the Plan identify forms regarding evidence handling and the location of the forms?
  - Does the Plan include links to referenced documents?
  - Is the terminology consistent amongst the response plans?
  - Is cyber awareness and incident response training conducted in the enterprise and is it mentioned in the Plan?
  - Is the plan has been accepted and approved by the sponsors and executives?

FINRA Guidance

Next Assignment

- Due 11/12- Rethinking This. A lot of discussion lately on KRI, KPI, how to measure and what to measure.
- Group Project?
- PPT to be submitted.
- All must contribute

http://www.cio.com/article/2940481/security0/how-cisos-can-create-security-kpis-and-kris.html

https://www.fireeye.co

https://assets.kpmg.com/content/dam/kpmg/pdf/2015/04/Cyber-Security-Dashboard1.pdfm/blog/executive-perspective/2015/03/measuring_success.html

A wider look:
Potential costs of cyberattacks

Above the surface:

- Customer breach notification
- Post-breach customer protection
- Regulatory compliance costs
- Public relations costs
- Attorney fees and litigation
- Cybersecurity improvements
- Cost of lost customers

Below the surface:

- Impact to current contracts
- Devaluation of trade name
- Loss of intellectual property (IP)
- Impact of operational disruption and/or destruction
- Insurance premium increases
- Increased cost to raise debt

Data Source: *1 2013 Cybercrime Report, Symantec

Additional Informational Material

Several leading practices, standards and guidelines exist in the industry. Below are a number of additional information sources for consideration:

- NIST: Computer Security Incident Handling Guide
  - http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

NIST: Guide to Integrating Forensic Techniques into Incident Response

- http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

SANS: Incident Handler's Handbook

- http://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Microsoft: Responding to IT Security Incidents

- http://technet.microsoft.com/en-us/library/cc700825.aspx#XSLTsection125121120120

ITC: Cyber Security Incident Response Plan

- https://www.efis.psc.mo.gov/mpsc/commoncomponents/viewdocument.asp?DocId=935724411

Carnegie Mellon University: Action List for Developing a CSIRT

- http://www.cert.org/incident-management/csirt-development/action-list.cfm?
- Chris to give ENISA

Frameworks

- Cyber Security
- FSSCC FFIEC

Metrics & Tools

- “Reporting on Risks to the Board”- Kenna
- Current Version

ISO 27001

BalaBit-ISO-27001-lets-make-the-impossible-possible.pdf

Dejan: Compliance, Marketing Edge, Lowering expenses, putting business in order

133 Controls
requirements of ISO, PCI DSS, SOX, HIPAA,
Basel II, GPG, FISMA
PDCA stands for “Plan,
Do, Check and Act”
RACI

- Mitigating, accepting, avoiding, or sharing the risk is also an option in the course of risk management.

Resources

- https://www.linkedin.com/learning/troubleshooting-your-network-with-wireshark
-
- https://www.linkedin.com/learning/foundations-of-cybersecurity/welcome