

Incident Severity Assessment Checklist

SECTION 1 - Intruder Characteristics/Behavior

a. Assess the threat based on evidence related to motive or intent of the intruder.

Indicators that imply a high threat associated with the intent of the intruder would be:

- Targeting specific systems.
- Actions to steal configuration files.

Choose one: Low Medium High

b. Assess apparent skill level of the intruder.

Behaviors indicating low skill level:

- Uses "everyday" known techniques and commands.

Behaviors indicating high skill level:

- Exhibits swift and sure execution of manual commands.

Choose one: Low Medium High

c. Assess paranoia level of the intruder.

Indicators that imply paranoia level of the intruder would be:

- Constantly checking who is online.

Choose one: Low Medium High

d. Assess degree to which intruder attempts to hide or cover evidence of his or her presence.

Behaviors indicating a high level of attempt to hide/cover evidence of his/her presence:

- No evidence of posting or bragging on WWW related to the intrusion.

Choose one: Low Medium High

e. Assess risk level based on how long the intruder has gone undetected.

Scale:

Low: 0-48 hours

Medium: 2-7 days

High: 8+ days

Choose one: Low Medium High

f. Assess risk level based on client's lack of knowledge concerning the intrusion.

Characteristics indicating a high risk associated with client's knowledge level concerning the intrusion:

- No data is available or found for initial intrusion event.

Choose one: Low Medium High

g. Assess degree of evidence/indications intrusion is perpetrated by more than one individual.

Evidence that indicates a high probability that intrusion was committed by more than one individual are:

- Intrusions occur from 4 dial-ups from the same source.

Choose one: Low Medium High

h. Assess threat based on the number of machines involved or cracked.

Scale:

Low: 1-4 systems

Medium: 5-10 systems

High: 11+ systems

Choose one: Low Medium High

i. Compile the overall Intruder Threat Assessment for SECTION 1:

Count the number of **High** ratings and multiply by 2 = ____

Count the number of **Medium** ratings = ____

SUM = ____

Using the scale below, determine the overall Intruder Threat Assessment Rating: ____

Low: 1-4

Medium: 5-10

High: 11+

SECTION 2 - Environmental Factors

a. Assess risk caused by affected network architecture.

Consider the following:

- Complexity of interconnections or routing.

Choose one: **Low Medium High**

b. Assess risk-based system and network admin skill level at local affected site(s).

Choose one: **Low Medium High**

c. Risk caused by inability to protect/counter or patch vulnerability used to gain access.

Choose one: **Low Medium High**

d. Risk caused by system backup capabilities.

Characteristics of a low risk associated with backup capabilities are:

- Backup system not vulnerable and provides same performance as primary

Characteristics of a medium risk associated with backup capabilities are:

- Backup system contains same vulnerability as compromised system.

Choose one: **Low Medium High**

e. Risk caused by operational considerations.

Characteristics of a medium risk associated with operational considerations are:

- Operational data is at risk.
- Operations degraded with loss or removal of compromised system

Choose one: **Low Medium High**

f. Compile the overall Environmental Risk Assessment for SECTION 2:

Count the number of **High** ratings and multiply by 2 = ____

Count the number of **Medium** ratings = ____

SUM = ____

Using the scale below, determine the overall Environmental Risk Assessment Rating: ____

Low: 0-2

Medium: 3-7

High: 8+

SECTION 3 – Characteristics/Capabilities

a. Assess risk caused by number of incidents currently open.

Low: 1-2

Medium: 3-5

High: 6+

Choose one: **Low Medium High**

b. Assess risk caused by current IRT personnel availability.

Characteristics of a medium risk associated with IRT personnel availability are:

- 1-2 IRT personnel available

Choose one: **Low Medium High**

c. Assess risk caused by current incident response team skill level availability.

Low: Experienced personnel

Medium: Semi-skilled to skilled personnel

High: Inexperience to semi-skilled personnel

Choose one: **Low Medium High**

e. Compile the overall Characteristics/Capabilities Risk Assessment for SECTION 3:

Count the number of **High** ratings and multiply by 2 = ____

Count the number of **Medium** ratings = ____

SUM = ____

Using the scale below, determine the overall e-fense Characteristics/Capabilities Risk Assessment Rating: ____

Low: 0-1

Medium: 2-4

High: 5+

Determine Recommended Course of Action:

Based upon the Incident Severity Assessment Checklist results, determine the Recommended Course of Action by using the chart, below.

		Environmental Risk		
		Low Risk	Medium Risk	High Risk
Threat	High Threat	Pursue - Good probability of successful pursuit - Skilled intruder - Unknown tools - Good network conditions - Ideal for a fishbowl	Pursue with caution - Fair probability of successful pursuit - Skilled intruder - Unknown tools - Fair network conditions - Fishbowl possible	Secure and Recover - Poor probability of successful pursuit - Skilled intruder - Unknown tools - Poor network conditions - Fishbowl difficult
	Medium Threat	Pursue - Good probability of successful pursuit - Semi-skilled intruder - Known tools - Good network conditions - Ideal for a fishbowl	Pursue with caution - Fair probability of successful pursuit - Semi-skilled intruder - Known tools - Fair network conditions - Fishbowl possible	Secure and Recover - Poor probability of successful pursuit - Semi-skilled intruder - Known tools - Poor network conditions - Fishbowl difficult
	Low Threat	Pursue - Good probability of successful pursuit - Intruder is unskilled - Well-known tools - Good network conditions - Ideal for a fishbowl	Pursue with caution - Fair probability of successful pursuit - Intruder is unskilled - Well-known tools - Fair network conditions - Fishbowl possible	Pursue with caution - Poor probability of successful pursuit - Intruder is unskilled - Well-known tools - Poor network conditions - Fishbowl difficult

Your Capabilities		
Low Risk	Medium Risk	High Risk
GREEN - Continue actions - Capabilities are robust	YELLOW - Re-evaluate actions - Capabilities are fair	RED - Cancel pursue actions - Develop alternate actions - Capabilities are poor

Recommended Course of Action:

Based upon all the criteria, what is the course of action you will choose:

- Pursue/Fishbowl/Monitor
- Secure and Recover

Pro's and Con's to courses of Action:

	<u>Pursue/Fishbowl/Monitor</u>	<u>Secure/Recover</u>
Pro's	<ul style="list-style-type: none"> - Helps client "identify hostile source" - Can help you identify the scope of the incident (i.e. what systems the hacker has compromised not only on their network, but others as well) - Helps in identifying the technique used to gain access (if not known) 	<ul style="list-style-type: none"> - Minimizes downtime...gets their system and data back on-line ASAP for operational reasons.
Con's	<ul style="list-style-type: none"> - Allows their system to continue to be hacked for a short period - The system could be crashed by the hacker (rm -rf'd) <ul style="list-style-type: none"> -- Could lose all data & operating system configuration data - Cannot use the system for operational purposes during the monitor <ul style="list-style-type: none"> -- Consider the data "lost" -- Loss of the use of a hardware asset 	<ul style="list-style-type: none"> - Only solves short-term problem. The hacker will be back later, if not on their system, then elsewhere.
Security Provided by "fishbowl"	<ul style="list-style-type: none"> - Protects the rest of their network from the hacker <ul style="list-style-type: none"> -- Compromised system continues to be hacked -- Compromised system can't be used to hack other systems on base - Transparent to the hacker. 	<ul style="list-style-type: none"> - N/A