Cyber Security Incident Response
High-level Maturity Assessment Tool

Introduction

Overview

Many organisations are extremely concerned about potential and actual cyber security attacks, both on their own organisations and in ones similar to them. Dealing with cyber security incidents – particularly sophisticated cyber security attacks – can be a very difficult task, even for the most advanced organisations. Each organisation should therefore develop an appropriate cyber security incident response capability, which will enable them to adopt a systematic, structured approach to cyber security incident response.

Your cyber security incident response capability should consist of appropriately skilled people guided by well-designed, repeatable processes and effective use of relevant technologies that will enable you to conduct a thorough investigation and successfully eradicate adversaries who are deeply embedded in your environment.

However, many organisations do not know their state of readiness to be able to respond to a cyber security incident in a fast, effective manner. One of the best ways to help determine this is to measure the level of maturity of your cyber security incident response capability in terms of:

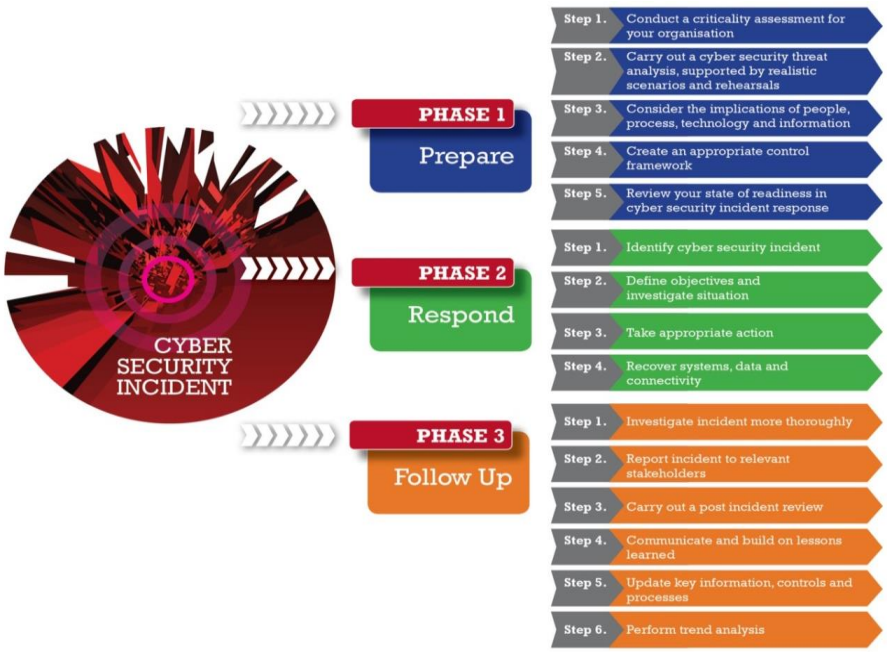
- People, process, technology and information
- Preparedness, response and follow up activities

This assessment tool provides a mechanism for carrying out an assessment of the level of maturity an organisation has for their cyber security incident response capability at a high level. It can be used to assess your state of readiness in being able to respond to a cyber security incident in a fast, effective and secure manner.

Note: There is also a *Detailed Maturity Assessment Tool* available, which allows an assessment to be made to determine the level of maturity of your cyber security incident response capability in depth.

Cyber Security Incident response process

This tool provides a high-level assessment against a maturity model that is based on the 15 steps within the 3 phase Cyber Security Incident response process presented in the CREST Cyber Security Incident Response Guide, as shown in the diagram below.



Instructions on how the tool works and how it can be used can be found on the *Guidelines* worksheet.

Acknowledgements

CREST would like to extend its special thanks to those CREST member organisations and third parties who took part in interviews, participated in the workshop and completed questionnaires.

Warning

This Guide has been produced with care and to the best of our ability. However, CREST accepts no responsibility for any problems or incidents arising from its use.

Credits

This tool has been developed for CREST by JERAKANO

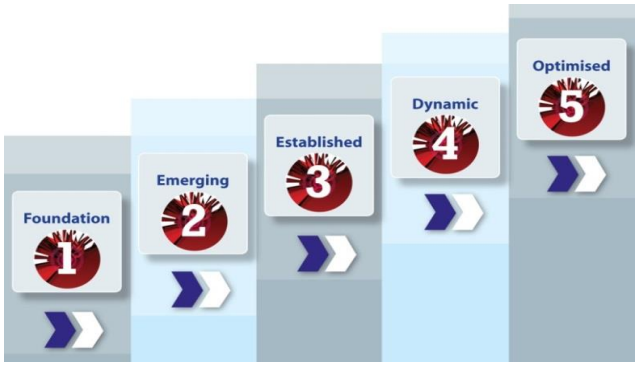
Cyber Security Incident Response
High-level Maturity Assessment Tool

Guidelines

Maturity model

To deal with a cyber security incident quickly and effectively you will need to build an appropriate cyber security incident response capability, the maturity of which can be assessed against an appropriate maturity model by using this assessment tool.

The maturity model used in this tool is based on a traditional, proven model shown below. This model can be used to determine the level of maturity of an organisation cyber security incident response capability, ranging from 1 (least effective) to 5 (most effective).



Different types of organisation will require different levels of maturity in cyber security incident response. For example, a small company operating in the retail business will not have the same requirement – or ability – to respond to cyber security incidents in the same way as a major corporate organisation in the finance sector – or a government department.

Consequently, the level of maturity your organisation has in cyber security incident response should be reviewed in context and compared to your actual requirements for such a capability. The maturity of your organisation can then be compared with other similar organisation to help determine if the level of maturity is appropriate.

Note: The maturity of the cyber security incident response capability can play a significant role in determining the level of third-party involvement required during a breach investigation and eradication event. Organisations with mature cyber security incident response capabilities may conduct most of their operations in-house, while those who are less mature may depend entirely on third parties.

How to use the tool

This tool allows an assessment to be made to determine the level of maturity of an organisations' cyber security incident response capability at a high level. It is based on a simple selection of the level of maturity for each of the 15 steps.

A weighting factor can be set to give the results for particular steps more importance than others. The selected levels of maturity are then displayed graphically for each of the three phases and overall. Calculations are based on a carefully designed algorithm that takes account of both the level of maturity selected for each step and the step's given weighting.

Step 1 - Complete the details for the environment being assessed in the *Profile and Scope* worksheet using the text boxes and drop-down lists provided. The name entered for *Name of Area of Assessment* will automatically appear on the *Results* worksheet.

Step 2 - On the *Configuration* worksheet use the checkboxes next to each step to deselect any steps not appropriate to the assessment. Then use the first column of drop-down lists to select the target level of maturity required for each step. Any steps you feel warrant greater importance can be given a higher weighting using the second column of drop-down lists. Evidence required to support responses can be entered in the *Evidence* column.

Note: The weighting values set on the *Configuration* worksheet can be overriden on the *Assessment* worksheet. If you are configuring the tool for a respondent and do not want these weightings to be changed, use the *Lock weighting* and/or *Hide weighting* buttons as appropriate, and then hide the *Configuration* worksheet by right-clicking on the relevant tab at the bottom of this spreadsheet and choosing *Hide* .

Step 3 - Carry out the assessment by selecting the appropriate level of maturity within the assessed environment for each step using the drop-down lists on the *Assessment* worksheet. Any additional comments can be entered in the *Comments* column.

Step 4 - Review a summary of the results using the *Results* worksheet to gain a high level picture of the overall level of maturity for the environment assessed.

Note: You may wish to consider conducting a more in-depth assessment of one or more elements of your cyber security incident response capability by using the *Detailed Maturity Assessment Tool.*

Cyber Security Incident Response
High-level Maturity Assessment Tool

Scope of assessment

*All fields marked * MUST be completed*

Name of area of assessment *	Production control
Business unit (or equivalent) *	UK branches
Organisation *	Acme Mfg Ltd
Sector *	Investment banking
Scope of assessment *	Business unit
Key components	

Respondent details *All fields marked * MUST be completed*

Date of assessment *	2014-02-02
Name of respondent *	John Smith
Role or position *	CISO
Department *	InfoSec
Organisation *	Acme Mfg Ltd
Type of assessment *	(●) Internal ( ) External
Qualifications of assessor - CREST *	Certified
Qualifications of assessor - other *	CISSP

Configuration

	Not selected	Target maturity level	Weighting	Evidence required
Phase 1 - Prepare				
Step 1 - Conduct a criticality assessment for your organisation	☐	Level 3 - Business Enabling	x 1	
Step 2 - Carry out a cyber security threat analysis, supported by realistic scenarios and rehearsals	☐	Level 3 - Business Enabling	x 2	
Step 3 - Consider the implications of people, process and technology	☐	Level 4 - Quantitatively Managed	x 1	
Step 4 - Create an appropriate control environment	☑	Not yet answered	x 3	
Step 5 - Review your state of readiness in cyber security response	☐	Level 3 - Business Enabling	x 1	
Phase 2 - Respond				
Step 1 - Identify cyber security incident	☐	Level 2 - Established	x 1	
Step 2 - Define objectives and investigate situation	☐	Level 2 - Established	x 1	
Step 3 - Take appropriate action	☐	Level 3 - Business Enabling	x 3	
Step 4 - Recover systems, data and connectivity	☐	Level 4 - Quantitatively Managed	x 1	

Phase 3 - Follow Up			
Step 1 - Investigate incident more thoroughly	☐	Level 2 - Established	x 1
Step 2 - Report incident to relevant stakeholders	☐	Level 2 - Established	x 1
Step 3 - Carry out a post incident investigation review	☐	Level 2 - Established	x 1
Step 4 - Communicate and build on lessons learned	☐	Level 1 - Initial	x 3
Step 5 - Update key information, controls and processes	☐	Level 4 - Quantitatively Managed	x 3
Step 6 - Perform trend analysis	☐	Level 5 - Optimised	x 3

High-level assessment

Statement	Level of maturity	Weighting	Evidence	Comments
Phase 1 - Prepare				
Step 1 - Conduct a criticality assessment for your organisation	Level 1 - Initial	x 1		
Step 2 - Carry out a cyber security threat analysis, supported by realistic scenarios and rehearsals	Level 2 - Established	x 2		
Step 3 - Consider the implications of people, process and technology	Level 1 - Initial	x 1		
Step 4 - Create an appropriate control environment	Question not selected	x 3		
Step 5 - Review your state of readiness in cyber security response	Level 3 - Business Enabling	x 1		
Phase 2 - Respond				
Step 1 - Identify cyber security incident	Level 2 - Established	x 1		
Step 2 - Define objectives and investigate situation	Level 3 - Business Enabling	x 1		
Step 3 - Take appropriate action	Level 1 - Initial	x 3		
Step 4 - Recover systems, data and connectivity	Level 1 - Initial	x 1		
Phase 3 - Follow Up				
Step 1 - Investigate incident more thoroughly	Level 2 - Established	x 1		
Step 2 - Report incident to relevant stakeholders	Level 2 - Established	x 1		
Step 3 - Carry out a post incident investigation review	Level 3 - Business Enabling	x 1		
Step 4 - Communicate and build on lessons learned	Level 4 - Quantitatively Managed	x 3		
Step 5 - Update key information, controls and processes	Level 3 - Business Enabling	x 3		
Step 6 - Perform trend analysis	Level 4 - Quantitatively Managed	x 3		

Aggregated maturity level results for Production control

Cyber Security Incident Response	Maturity level (1 to 5)	Target maturity (1 to 5)
CSIR - Overall	1.2	1.6
Phase 1 - Prepare	0.8	1.3
Step 1 - Criticality assessment	1	3
Step 2 - Threat analysis	2	3
Step 3 - People, Process, Technology and Information	1	4
Step 4 - Control environment		
Step 5 - Maturity assessment	3	3
Phase 2 - Respond	0.8	1.4
Step 1 - Identification	2	2
Step 2 - Investigation	3	2
Step 3 - Action	1	3
Step 4 - Recovery	1	4
Phase 3 - Follow up	2.2	2.0
Step 1 - Incident investigation	2	2
Step 2 - Reporting	2	2
Step 3 - Post incident review	3	2
Step 4 - Lessons learned	4	1
Step 5 - Updating	3	4
Step 6 - Trend analysis	4	5