Cyber Security Incident Response Guide

Version 1

Published by:
CREST
Tel: 0845 686-5542
Email: **admin@crest-approved.org**
Web: **http://www.crest-approved.org/**

Principal Author
Jason Creasey,
Managing Director, Jerakano Limited

Principal reviewer
Ian Glover, President,
CREST

DTP notes

For ease of reference, the following DTP devices have been used throughout the Guide.

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.

A Good Tip

A Timely Warning

An insightful Project Finding

Quotes are presented in a box like this.

Key findings

The top ten findings from research conducted about responding to cyber security incidents, undertaken with a range of different organisations (and the companies assisting them in the process), are highlighted below.

1 Cyber security incidents, particularly serious cyber security attacks, such as advanced persistent threats (APTs), are now headline news. They bring serious damage to organisations of all types – and to government and international bodies. Ways to respond to these attacks in a fast, effective and comprehensive manner are actively being developed at the very highest level in corporate organisations, government bodies and international communities such as the World Economic Forum, where cyber security attacks are seen as a major threat.

2 There is no common understanding of what a cyber security incident is, with a wide variety of interpretations. With no agreed definition– and many organisations adopting different views in practice – it is very difficult for organisations to plan effectively and understand the type of cyber security incident response capability they require or the level of support they need.

3 The original government definition of cyber security incidents as being state-sponsored attacks on critical national infrastructure or defence capabilities is still valid. However, industry – fuelled by the media – has adopted the term wholesale and the term cyber security incident is often used to describe traditional information (or IT) security incidents. This perception is important, but has not been fully explored – and the term cyber is both engaging and here to stay.

4 The main difference between different types of cyber security incident appears to lie in the *source* of the incident (eg a minor criminal compared to a major organised crime syndicate), rather than the *type* of incident (eg hacking, malware or social engineering). At one end of the spectrum come basic cyber security incidents, such as minor crime, localised disruption and theft. At the other end we can see major organised crime, widespread disruption, critical damage to national infrastructure and even warfare. Furthermore, the nature of attacks is changing from public displays of capability to targeted attacks designed to be covert.

5 Organisations vary considerably in terms of the level of maturity in their cyber security incident response capability, but also in the way in which they need to respond. Whilst good practice exists – and is being improved – the lack of both a common understanding and a detailed set of response guidance is limiting organisational capabilities and approaches, as well as restricting important knowledge sharing activities.

6 Few organisations really understand their 'state of readiness' to respond to a cyber security incident, particularly a serious cyber security attack, and are typically not well prepared in terms of:

- *People* (eg assigning an incident response team or individual; providing sufficient technical skills; enabling decisions to be taken quickly; and gaining access to critical third parties)
- *Process* (knowing what to do, how to do it and when to do it), eg identify cyber security incident; investigate situation; take appropriate action (eg contain incident and eradicate cause); and recover critical systems, data and connectivity
- *Technology* (knowing their data and network topology; determining where their Internet touch points are; and creating / storing appropriate event logs)
- *Information* (eg recording sufficient details about when, where and how the incident occurred; defining their business priorities; and understanding interdependencies between business processes, supporting systems and external suppliers, such as providers of cloud solutions or managed security services).

7 In practice it is often very difficult for organisations to identify the type of cyber security incident they are facing until they have carried out an investigation, particularly as very different types of cyber security incident can show similar initial symptoms. Even when organisations have comprehensive detection software and logging it can be difficult to determine the nature of an attack in a timely manner.

8 Despite the current level of threat from cyber security incidents, those responsible for preparing for, responding to and following up cyber security incidents in many organisations still face significant challenges in:

- Persuading senior management to appreciate the extent of the problem – restricting budget and resources
- Knowing who to contact to provide expert help (and why)
- Involving experts at a sufficiently early stage in proceedings
- Providing them with sufficient information to be able to investigate effectively.

9 Most organisations need professional help in responding to a cyber security incident in a fast, effective manner. However, it is very difficult for them to identify trusted organisations that have access to competent, qualified experts who can respond appropriately whilst protecting sensitive corporate and attack information.

10 Employing the services of properly qualified third party experts (such as those CREST members who provide cyber incident response), can significantly help organisations to handle cyber security incidents in a more effective and appropriate manner – particularly serious cyber security attacks. Research revealed that the main benefits of using this type of external supplier are in:

- *Providing resourcing and response expertise*, by gaining access to more experienced, dedicated technical staff who understand how to carry out sophisticated cyber security incident investigations quickly and effectively
- *Conducting technical investigations*, by providing deep technical knowledge about the cyber security incident, including: the different types of attacker (and how they operate); advanced persistent threats; methods of compromising systems; and sophisticated analysis of malware
- *Performing cyber security analysis*, for example by monitoring emerging cyber threats; applying modern analytic capabilities to aggregate relevant data from many different systems; and providing situational awareness, particularly in the area of cyber intelligence.

Contents