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

About this Guide

This Guide provides details about how to handle cyber security incidents in an appropriate manner. It provides you with practical advice on how to prepare for, respond to and follow up an incident in a fast and effective manner – presented in an easy to use format. It is designed to enable you to determine what a cyber security incident means to your organisation, build a suitable cyber security incident response capability and learn about where and how you can get help.

US President Obama declared that the

"cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cyber security."

This Guide presents a useful overview of the key concepts you will need to understand to handle cyber security incidents in an appropriate manner, which includes: a definition of cyber security incidents; a comparison of different types of cyber security attack; anatomy of a cyber security attack; a summary of the main challenges in responding to cyber security incidents; how you can respond; and the need to employ third party experts to help you to respond in a faster, more effective manner.

The Guide then provides advice and guidance on how to establish an appropriate cyber security incident response *capability,* enabling you to assess your state of readiness to:

1. ***Prepare for a cyber security incident:*** performing a criticality assessment; carrying out threat analysis; addressing issues related to people, process, technology and information; and getting the fundamentals in place
2. ***Respond to a cyber security incident:*** covering identification of a cyber security incident; investigation of the situation (including triage); taking appropriate action (eg containing the incident and eradicating it's source); and recovering from a cyber security incident
3. ***Follow up a cyber security incident:*** considering your need to investigate the incident more thoroughly; report the incident to relevant stakeholders; carry out a post incident review; build on lessons learned; and update key information, controls and processes.

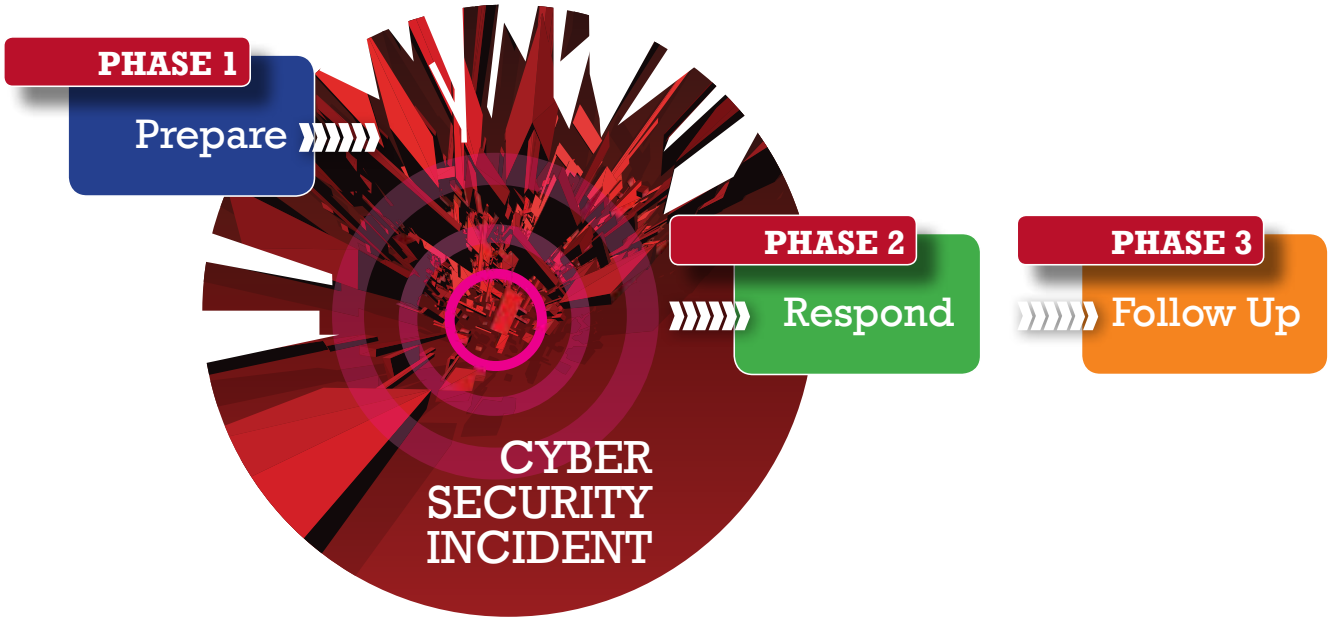

Figure 1: Key elements in a cyber security incident management capability

Finally, the Guide outlines how you can get help in responding to a cyber security incident, exploring the benefits of using cyber security incident response experts from commercial suppliers. It introduces you to a systematic, structured process that you can adopt to help you select an appropriate supplier(s) to meet your requirements.

The four key steps in the process for choosing a suitable supplier of cyber security incident response services ('The Selection Process') are described in detail in the complementary CREST ***Cyber Security Incident Response – Supplier Selection Guide***

Throughout the Guide you will find a set of tips, warnings and quotes provided by a diverse set of contributors, including expert suppliers (such as many CREST members), consumer organisations, government bodies and academia. These bring real-world, practical experience to the Guide, allowing you to get a better feel for the types of action that are most likely to apply to your organisation.

Audience

The CREST Cyber Security Incident Response Guide is aimed at organisations in both the private and public sector. Project research has revealed that the main audience for reading this Guide is the IT or information security manager and cyber security specialists, with others including business continuity experts IT managers and crisis management experts. It may also be of interest to business managers, risk managers, procurement specialists and auditors.

Purpose and scope

The purpose of this Guide is to help you to meet a range of different requirements identified by a wide variety of organisations wanting to know how to best respond to a cyber security incident. The main requirements are laid out in the table below, together with the part(s) of this Guide where more detail can be found.

Requirement	Detail
Identify the main challenges in responding to a cyber security incident, such as a serious, sustained cyber security attack (be it by state-sponsored agents, organised cybercrime syndicates or extremist groups)	Part 3
Learn about the support that is available to help you meet these challenges (both in the public domain and from commercial organisations), including advice and guidance, incident management methodologies and information sharing services	Parts 3 and 7
Build a suitable cyber security incident management capability (possibly in support of a wider cyber security resilience programme)	Part 4
Evaluate the level of maturity in cyber security incident response in your organisation, ie your 'state of readiness'	Part 4
Review the way in which you prepare for, respond to and follow up cyber security incidents, learning from proven cyber security incident response processes	Parts 4-7
Determine how cyber security incidents should be identified and handled in your organisation	Part 5
Select suitable third party experts, be it for some or all of the cyber security response process or just specialised areas like technical or forensic investigations; situational awareness	Part 7

The scope of this Guide could be very large, so it excludes many elements of some important cyber security topics (but certainly not all), including:

- The prevention of cyber security attacks, including detailed cyber security threat analytics
- Cyber security resilience as a whole, including detailed situational awareness
- Deep technical investigation tools and techniques, typically used by commercial cyber security incident response or forensics experts
- Cyber security insurance.

The material in this Guide will provide valuable input to each of these topics, any of which could be the subject of a future research project.

Rationale

Cyber is the latest buzzword that has really taken the media by storm. There are examples everywhere about the possible horrors of cyber security attacks. Many organisations are extremely concerned about potential and actual cyber security attacks, both on their own organisations and in ones similar to them.

Cyber security incidents have become not only more numerous and diverse but also more damaging and disruptive, with new types of cyber security attacks emerging frequently.

> "The UK Government Communications Headquarters (GCHQ) now sees real and credible threats to organisations through cyber security attacks on an unprecedented scale, diversity and complexity. We've seen determined and successful efforts to:
>
> - Steal intellectual property;
> - Take commercially sensitive data, such as key negotiating positions;
> - Gain unauthorised access to government and defence related information;
> - Disrupt government and industry service; and,
> - exploit information security weaknesses through the targeting of partners, subsidiaries and supply chains at home and abroad.
>
> The magnitude and tempo of these attacks, basic or sophisticated, on UK and global networks pose a real threat to the UK's economic security. The mitigation of these risks and management of these threats - in other words, cyber security - is one of the biggest challenges we all face today."
>
> *Source: 10 steps to cyber security – jointly produce by the Communications Electronics Security Group (CESG) and the Centre for the Protection of National Infrastructure (CPNI).*

Organisations are seldom adequately prepared for a serious cyber security incident. They often suffer from a lack of: budget; resources; technology; or recognition of the type and magnitude of the problem. In addition, they do not have the software, testing, process, technology or people to handle sophisticated cyber security threats, such as Advanced Persistent Threats (APTs).

An effective method of responding to cyber security incidents is therefore necessary for rapidly detecting incidents; minimising loss and destruction; mitigating the weaknesses that were exploited; restoring IT services; and reducing the risk from future incidents.

Current cyber security incident response guidelines can be very useful, but do not typically provide:

1. A solid, consistent definition of a cyber security incident - or any real distinction between cyber security incidents and traditional information (or IT) security incidents
2. In-depth guidance about dealing with cyber security incidents, particularly for commercial consumer organisations outside government or Finance sectors
3. Advice on who organisations can ask for help – backed up by selection criteria.

Consequently, many organisations do not have access to appropriate external sources and levels of guidance to help them prepare for most types of cyber security incident, let alone a serious cyber security attack.

The cyber security incident response project

This Guide is based on the findings of a research project - *conducted by Jerakano Limited on behalf of CREST* – which looked at the requirements organisations have to help them prepare for, respond to and follow up cyber security incidents. One of the main reasons for commissioning a research project was that CREST members were concerned about the lack of relevant information many of their customers have access to when responding to cyber security incidents.

This guide builds on a similar report produced by CREST to help you define real business requirements for penetration testing, to conduct tests more effectively and to choose a suitable supplier of penetration testing services. A summary of CREST activities can be found at: http://www.crest-approved.org/.

The research project included:

- Performing desktop research on different sources of information, including GCHQ-related publications, such as the *10 steps to cyber security* from CESG and the *First Responder's Guide – Policy and Principles* from CPNI
- Reviewing a number of other useful guides from international bodies, such as the *Good Practice Guide for Incident Management* from the European Network and Information Security Agency (ENISA); the NIST Computer Security Handling Guide (Special Publication 800-61); and *Responding to targeted cyberattacks* from ISACA (collaborating with E&Y)
- Conducting telephone interviews with key stakeholders, such as CREST members and clients, academia, CESG and ENISA, with site visits to CPNI, GCHQ and the Bank of England
- Creating a detailed project questionnaire based on research (and previous experiences), and analysing the results of responses from participants
- Discussing key issues and requirements with a wide variety of people at CRESTCon, the CREST annual conference
- Running a workshop where experts in cyber security response services from more than 20 organisations validated the findings of this Guide and provided additional specialist material.

The CREST project complements the work done by the UK Government (eg CESG and the CPNI) on cyber security incident response, but provides more detailed guidance for organisations (particularly in the private sector), who might need to respond to a cyber security incident in practice - and procure support from experts in commercial suppliers.

Background

The term cyber (which actually means robotic) can be interpreted in many ways. For example, one dictionary definition defines the term Cyber as 'relating to computers and the Internet', which again can mean different things to different people. Furthermore, project research identified that cyber is often associated with the concept of cyberspace.

> "Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services."
> *Source: UK Cyber Security Strategy, 2011*

Cyberspace is constantly evolving and presenting new opportunities. The desire of businesses to quickly adopt new technologies (using the Internet and adopting cloud services to open new channels) provides enormous opportunity, but also brings unforeseen risks and unintended consequences that can have a negative impact.

> "The interconnectedness of the Internet brings huge benefits to the World but also an unrivalled opportunity for harm"

Many computing devices (eg PCs, laptops, tablets and smart phones) are connected to the Internet on an almost continuous basis. Technical exploits target not only vulnerabilities in infrastructure, but also in many web-based applications. It may be that cyber security is the security of cyberspace and that a cyber security incident is one that impacts on cyberspace or uses cyberspace as part of an attack vector.

The term ***Cyber Security*** is poorly defined – and understood.

It often appears to be replacing the term information (or IT) security, rather than being supplementary to it. For example, the *PwC / BIS cyber security breaches survey* was previously called the *information security breaches survey*, but the questions appear to be virtually the same.

The UK Government tendency to focus on ***Cyber Security and Information Assurance (CSIA)*** seems to work, but is not well understood by commerce – or commonly used outside the UK.

Defining a cyber security incident

There are many types of information (or IT) security incident that could be classified as a cyber security incident, ranging from serious cyber security attacks on critical national infrastructure and major organised cybercrime, through hacktivism and basic malware attacks, to internal misuse of systems and software malfunction.

However, project research has revealed that there is no one common definition of a cyber security incident. There is no authoritative taxonomy to help organisations decide what is (or isn't) a cyber security incident, breach, or attack.

Often cyber security incidents are associated with malicious attacks or Advanced Persistent Threats (APTs), but there appears to be no clear agreement. Many different organisations have different understandings of what the term means, consequently adopting inconsistent or inappropriate cyber security incident response approaches.

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.

The two most common (and somewhat polarised) sets of understanding – as shown in *Figure 2* below - are either that cyber security incidents are no different from traditional information (or IT) security incidents – or that they are solely cyber security *attacks*.

Figure 2: Different types of cyber security incidents

> "We classify all information security incidents as Social; Hacking; Malware; or Misuse; as that is what is commonly understood"

Many respondents to the project questionnaire felt that there is a need to differentiate between a cyber security ***attack***, which requires a more modern approach (both technically and holistically) - and other types of information security incident that can still be addressed by traditional incident handling approaches (often forensics or law enforcement led).

Comparing different types of cyber security incident

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). Therefore, it may be useful to define cyber security incidents based on the type of attacker, their capability and intent.

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.

Some of the most common ways in which different types of cyber security incident can be compared are outlined in the table below – but they can vary considerably for any given incident, with many different groups attacking many different targets.

Topic	Basic cyber security incident	Sophisticated cyber security attack
Type of attacker	• Small-time criminals • Individuals or groups just 'having fun' or ' responding to a challenge' • Localised, community or individual Hacktivists • Insiders	• Serious organised crime • State-sponsored attack • Extremist groups
Target of attack	• General public • Private sector • Non-strategic government departments	• Major corporate organisations • International organisations • Governments • Critical national infrastructure • National security / defence
Purpose of attack	• Financial gain • Limited disruption • Publicity • Vendettas or revenge	• Major financial reward • Widespread disruption • Discover national secrets • Steal intellectual property of national importance • Terrorism • Warfare
Capability of attacker	• Low skill • Limited resource • Publicly available attack tools • Not well organised • Local reach	• Highly skilled professionals • Extremely well resourced • Bespoke tools • Highly organised • International presence
Response requirements	• Restore services • Special monitoring and_organisation • Some industry information sharing	• Tailored guidance for specialist industry and specific capabilities • Implications for government security services • CNI sector-specific industry response

"Sophisticated cyber security attacks often don't have an end"

Some of the differences between traditional information security incidents and cyber security attacks are that the latter often includes:

- Mandatory escalation and reporting
- Use of experts to respond effectively
- Support from the government to respond (in some cases)
- Sharing of attack and response data between investigators.

Most of these do not apply to traditional cyber security incidents, where organisations would typically have to support themselves (possibly with some help from the police). It is not the Government's role to protect every organisation against cyber security attacks. They will provide assistance in responding to major cyber security attacks – or to help protect national defence and critical national infrastructure. They also provide guidance on how to respond to other types of cyber security incident, it is not their role to get actively involved in the actual response.

All types of attack - be they basic or advanced - will utilise similar attack vectors (eg hacking, malware, social engineering) to carry out attacks, but with very different levels of sophistication, scale and resourcing. Furthermore, the nature of attacks is changing from public displays of capability to targeted attacks designed to be covert. Depending on the nature of the cyber security incident, the types of attacker shown to fall into one category (eg insider, hacktivist) may actually fall into the other category.

> "We have to defend against every kind of attack, while the attacker just needs to find one flaw"

Cyber security attacks are closely related to the agent (or actor) responsible for the attack, typically malicious third parties, but can include insiders. There are also a range of more specific (or related) threats, such as those from crafted malware, blended threats and phishing attacks.

Project research revealed that most basic attacks (such as those crafted by small-time criminals, random hackers and most Hactivists) could be dealt with by many suppliers – but that more sophisticated cyber security attacks need to be addressed by properly qualified experts, such as those provided by CREST members.

When it comes to identifying and responding to suspected information, IT or cyber security incidents, most organisations treat them in the same way until some sort of investigation has taken place. Consequently, typical comments made during project research suggested that:

- Cyber should be threaded through all incident response, not identified separately
- A cyber security incident feels more like an attack than a business continuity issue, but at what point does an incident move from any other type of attack to a cyber security attack?

This guide will help organisations respond to all types of cyber security incidents, including traditional information (or IT) security incidents. More focus will, however, be placed on preparing for, responding to and following up ***cyber security attacks***, highlighting key points in this area.

Typical phases in a cyber security attack

Cyber criminals innovate just as business does and the potential rewards for them grow as business use of cyberspace grows. They have access to powerful, evolving capabilities, which they use to identify attack and exploit carefully chosen targets. They also have well-developed marketplaces for buying and selling tools and expertise to execute sophisticated attacks.

When looking at a cyber security attack in more detail there are often a number of phases that attackers will undertake, which can sometimes take place over a long period of time. An example of the basic components of such a phased approach is outlined in *Figure 3* below, together with some of the common countermeasures for each phase.

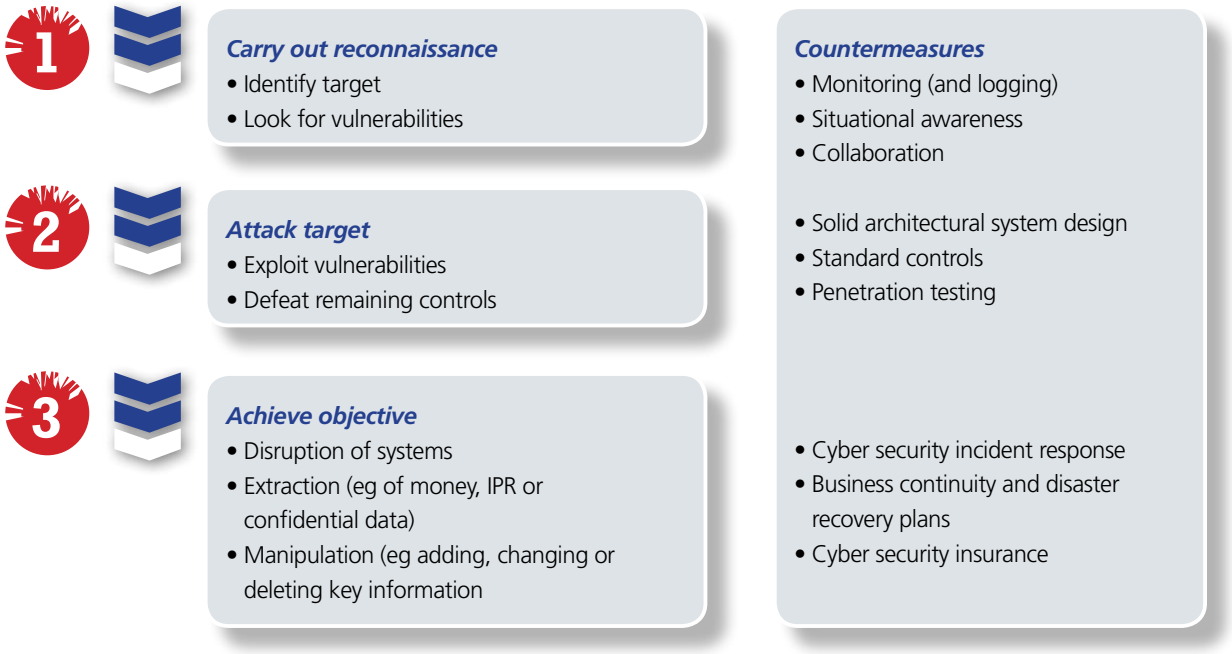

Figure 3: Typical phases in a cyber security attack

When dealing with a sophisticated cyber security attack, it is important to address all stages carried out by an attacker, be they cybercriminals, extremists or state-sponsored agents. However, many organisations do little or nothing before phase two of an attack, often because they do not have the awareness, resources or technical skills to tackle issues during the reconnaissance stage.

> "Confidential information had been siphoned off for the last 5 years, but nobody knew anything about it"

Addressing the first phase is critically important (but outside the scope of this Guide) and involves a number of preventative measures, scenario development and rehearsal; and the need for extensive collaboration.

The APT phenomenon

The term advanced persistent threat (APT) usually refers to a group, such as organised crime syndicates, nation states, state-sponsored groups of individuals or extremist movements, who have both the capability and the intent to persistently and effectively target a specific entity. The term is commonly used to refer to both cyber security threats and incidents, in particular that of Internet-enabled espionage, using a variety of intelligence gathering techniques to access sensitive information.

Advanced Persistent Threat (APT) was not originally intended to be the generic term that it is today. It was developed to refer to specific, known, state-sponsored groups that conducted attacks against specific targets – often aimed at obtaining information to enable either political or commercial advantage.

APT has not tended to refer to organised crime, but these days we are seeing more organised crime attacks that utilise APT style techniques and tools.

The number of APTs is increasing rapidly, many of which are being used for corporate espionage or state-sponsored attack. These attacks follow the broad anatomy of any attack outlined on the previous page, but specifically comprise:

1. Intelligence gathering (eg conduct detailed research into a target)
2. Initial exploitation (eg carry out initial attack and establish foothold)
3. Command and control (eg achieve persistent access that can survive a re-boot of the system and move to new systems)
4. Privilege escalation (eg gain system administrator rights on target systems)
5. Data exfiltration (eg gather and remove (or copy) target data).

This APT life cycle can also be used to describe attacks by other sophisticated attackers, but the essence of an APT attack is its *targeted* nature.

Many evolving APTs are now able to circumvent traditional security controls. For example, some of them now use custom-built malicious code that is:

- Created specifically for a particular target
- Compiled immediately before use
- Tested on the latest antivirus definitions
- Equipped with multiple anti-reverse engineering techniques
- Installed with user privileges
- Added to the host firewall whitelist (eg via an initial malware infection)
- Hosted on a different site for each victim (and a different site for each wave of attacks on a victim).

Many targeted APTs (and some non-targeted ones) initiate communication from within the network, often to circumvent firewalls (which will block suspicious inbound connections but will not routinely block responses to something that started inside). They use standard ports and protocols to hide within obvious/ allowed traffic, thus defeating most Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).

The main challenges in cyber security incident response

In the commercial world (and often in governments), even large organisations can have significant difficulty in responding to cyber security incidents, particularly sophisticated cyber security attacks.

> "We thought we were prepared for a cyber security incident and then got a nasty surprise when one actually occurred."

Findings from the research project indicated that the top ten challenges organisations face in responding to a cyber security incident in a fast, effective and consistent manner are in:

1. Identifying a suspected cyber security incident (eg monitoring evidence of unusual occurrences and assessing one or more trigger points)
2. Establishing the objectives of any investigation and clean-up operation
3. Analysing all available information related to the potential cyber security incident
4. Determining what has actually happened (eg a DDOS, malware attack, system hack, session hijack, data corruption etc)
5. Identifying what systems, networks and information (assets) have been compromised
6. Determining what information has been disclosed to unauthorised parties, stolen, deleted or corrupted
7. Finding out who did it (ie which threat agent or agents); and why (eg financial gain, hacktivism, espionage, revenge, challenge or just for fun)
8. Working out how it happened (eg how did the attacker gain entry to the system)
9. Determining the potential business impact of the cyber security incident
10. Conducting sufficient investigation (eg using deep dive forensic capabilities) to identify (and prosecute, if appropriate) the perpetrator(s).

Top management in organisations often do not believe that they are at risk from a cyber security incident and are unaware of (or unconvinced by) the level of business impact that could result. Even if they provide support during an attack, they can then withdraw this soon afterwards, refusing to acknowledge that they could be badly hit again.

Furthermore, few organisations are well prepared for a cyber security incipient in terms of:

- People (eg an incident response team or individual, technical experts, fast access to decision-makers, representation from key suppliers)
- Process (such as knowing what to do, how to do it and when to do it – eg when detecting, containing, eradicating or recovering from a cyber security incident)
- Technology (eg knowing their network topology, providing the right event logs)
- Information (eg having information close to hand about business operations and priorities; critical assets; and key dependencies, such as on third parties, important locations or where relevant information resides).

For small organisations, one of the biggest problems can be in implementing effective cyber security controls, often due to a lack of awareness, experience, or simply because they are expensive. For larger organisations, many of them will have IT staff who can deal with most cyber security incidents. However, the increasing use of cloud computing – not always supported by appropriate controls or service level agreements (SLAs) – can hamper their cyber security response capability.

Top management in organisations often do not believe that they are at risk from a cyber security incident and are unaware of (or unconvinced by) the level of business impact that could result. Even if they provide support during an attack, they can then withdraw this soon afterwards, refusing to acknowledge that they could be badly hit again.

So how do we respond?

There are many difficulties facing organisations when determining how to prepare for, respond to and follow up a security incident, be it a simple virus or a sophisticated cyber security attack.

There are a number of publicly available offerings to help you respond to cyber security incidents, which include:

- Following the advice and guidance provided on government websites, such as the:
  - CESG *Top ten steps to cyber security*
  - *First Responder's Guide – Policy and Principles* from the centre for the protection of national infrastructure (CPNI)
  - GovCertUK incident response guidelines
- Referring to publicly available traditional or cyber security specific incident response guides, such as:
  - *The Good Practice Guide for Incident Management* from the European Network and Information Security Agency (ENISA)
  - NIST Computer Security Handling Guide (Special Publication 800-61)
  - *Responding to targeted cyberattacks* from ISACA (collaborating with E&Y)
  - Reports produced by a variety of vendors
- Taking part in external events, such as by attending conferences, enrolling in training programmes and subscribing to specialised services
- Collaborating with relevant third parties, such as participating in information exchanges, contributing to scenario-based rehearsals and introducing two-way cyber security alert mechanisms
- Considering the issues and actions highlighted in this Guide.

Project research revealed that organisations find it confusing to know which document or website to go to when seeking guidance on responding to a cyber security incident – and most of information provided does not refer *specifically* to a *cyber* security incident, just incidents in general.

There are many different government bodies involved with cyber security in some way. However, for people who are not deeply entrenched in government-related work this can be confusing, as they typically think about *'The Government'* as being one entity. They do not understand all the different departments, services and objectives – they just want to know where to get information and who to call when they get hit by a cyber security incident.

There is *specialised* support available for government departments. GovCertUK is the Computer Emergency Response Team (CERT) for UK Government. They assist public sector organisations in the response to computer security incidents and provide advice to reduce the threat exposure. They gather data from all available sources to monitor the general threat level. For these reasons the early reporting of incidents and attempted attacks is highly recommended.

However, there is limited publicly available support in the private sector, where it is more common for commercial suppliers of cyber security incident response experts to be employed.

CREST has collaborated with the UK Government to develop *certified* Cyber Incident Response (CIR) services.

The CREST standard for the industry-led segment will act as a foundation to establish a strong UK cyber incident response industry able to tackle the vast majority of cyber attacks. This will enable service providers to establish a track record and, if they so choose, apply for certification under the CESG/CPNI-led scheme for the most sophisticated cyber attacks.

More details can be found in ***Part 7 – Selecting a suitable supplier.***

Limitations with current solutions

Many organisations do not treat cyber security incident response any differently to other forms of information or IT security incident response, which may be reasonable for traditional types of cyber security incidents.

> "Cyber security incident response is just a lot of hype for something we've been dealing with for a while… it's just information security by a different name"

However, project research has highlighted that a traditional information security incident approach, while still useful in many cases, is not always appropriate for dealing with a sophisticated cyber security attack – because these approaches:

- Do not look for flaws across the entire organisation or over time, concentrating on what is perceived as a single event
- Are not agile enough
- Seldom really trace where all the holes are, how attackers got in – or who they are
- Tend to focus on individual machines, such as isolating one particular laptop
- Can actually make things worse in some cases.

A traditional response to an attack on a Domain Controller (DC) could be to take images of certain components – and then recover and re-build the DC from a back-up. This will not help if the attacker already has sysadmin privileges for the DC as they can just start again.

The need for support from third party experts

Organisations of all types are struggling to deal with cyber security incidents effectively, with a growing number of cyber security incidents now taking place on a regular basis – and causing significant business impact.

Many larger organisations can respond to traditional cyber security incidents themselves, sometimes very successfully – but smaller organisations would typically need expert help. However, when it comes to dealing with a sophisticated cyber security attack virtually all organisations should consider employing the services of one or more specialist third party cyber security incident response providers for at least some activities (eg investigating advanced types of cyber security attack or analysing evidence of unusual occurrences).

> "When faced with a sophisticated cyber security attack, CISOs feel like they are looking down the barrel of a gun"

Project research identified many reasons why an organisation may wish to employ external cyber security incident response experts (such as qualified CREST members). For example, upon discovery of a cyber security incident, these specialists can evaluate the situation and undertake the most appropriate actions to enable fast recovery from the incident, and to help prevent reoccurrence.

The top three reasons why organisations hire expert third party suppliers are shown in *Figure 4* below – and explained in more detail in *Part 7 Selecting a suitable supplier.*

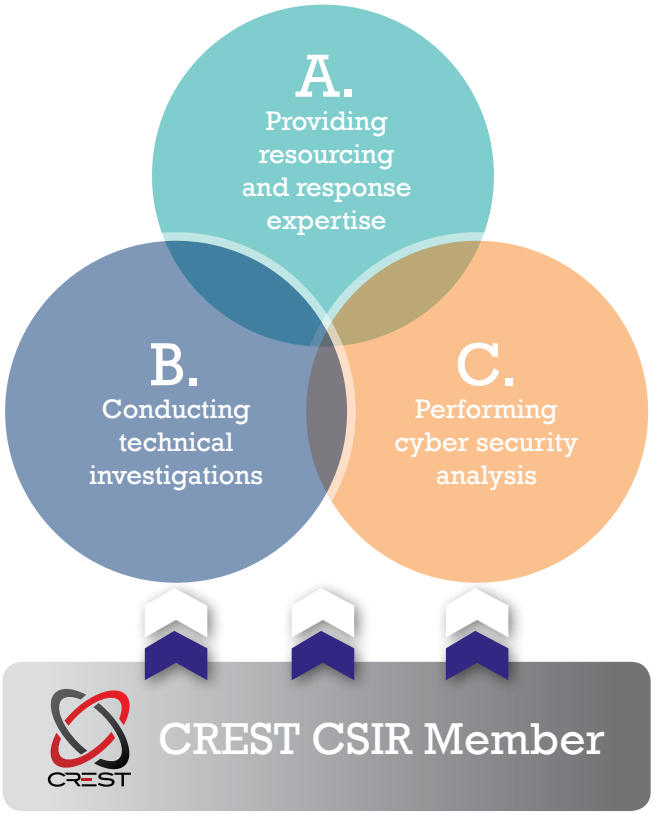

Figure 4: Benefits of using external suppliers

There are many benefits in procuring cyber security incident response services from a trusted, certified external company who employ professional, ethical and highly technically competent individuals. Many CREST member companies are certified cyber security incident response organisations (CREST CSIR members) who fully meet these requirements, having been awarded the gold standard in cyber security incident response, building trusted relationships with their clients.

Building a cyber security incident response capability

Dealing with cyber security incidents – particularly sophisticated cyber security attacks – can be a very difficult task, even for the most advanced organisations. You should therefore develop an appropriate cyber security incident response *capability*, which will enable you to adopt a systematic, structured approach to cyber security incident response, including the selection and management of external suppliers.

To build an effective cyber security incident response capability, it can be useful to examine what you may need to do before, during and after a cyber security attack, as outlined in the 3 phase approach shown in *Figure 5* below.

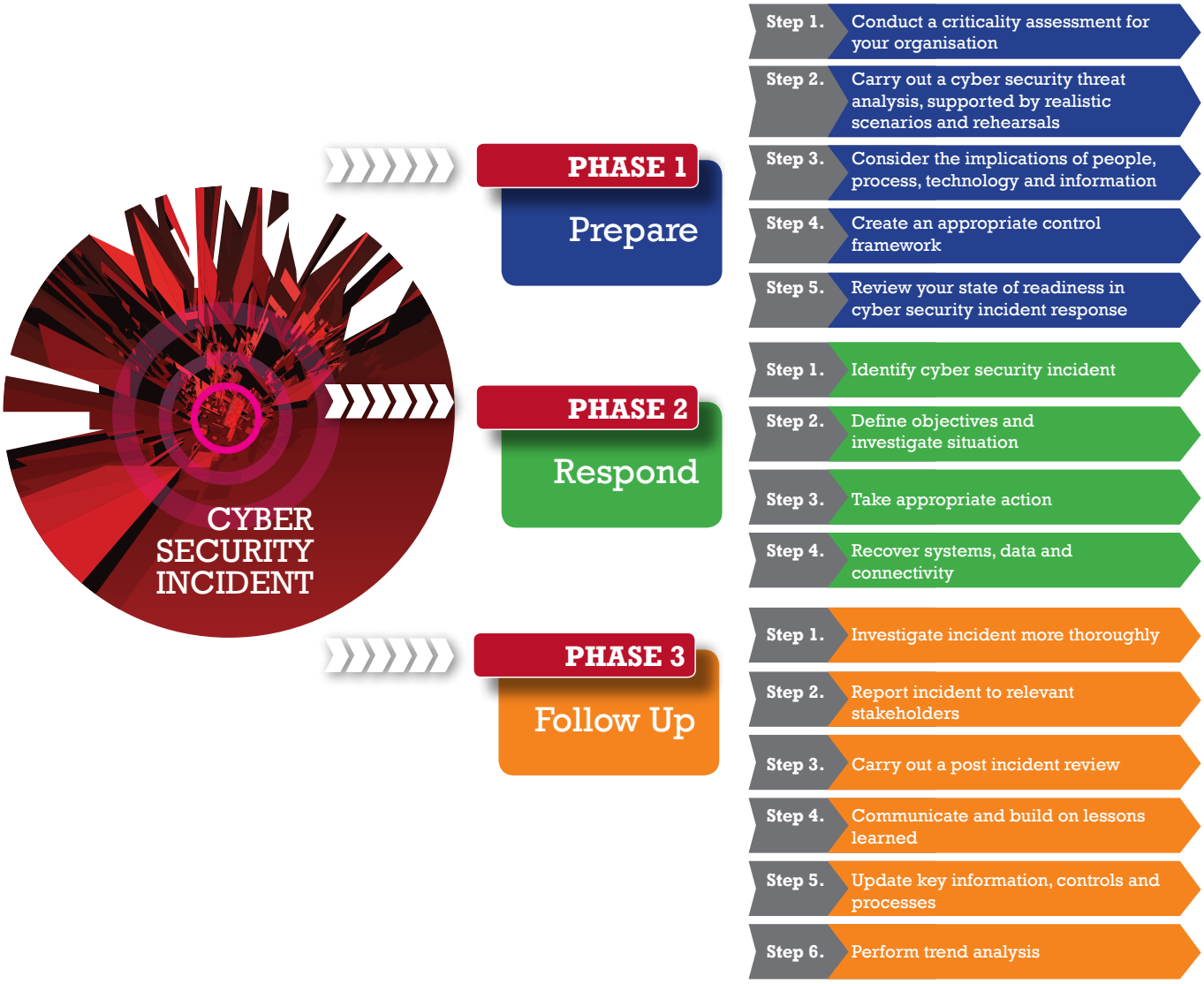

Figure 5: A structured approach to cyber security incident response

The main topics associated with each phase are examined in more details in *Parts 4-6* of this Guide on the following pages.

Most organisations need professional help in responding to a cyber security incident in a fast, effective manner, be it for all of their cyber security response capability - or just specialised areas like technical or forensic investigations; situational awareness; and advanced data analytics.

Overview

When dealing with a cyber security incident, one of the most important actions is to be properly prepared. This will help you to recover your systems more quickly, minimise the impact of the attack, instil confidence in your customers and even save you money in the long term. This first phase is crucial, but can easily be overlooked because of a lack of awareness, support or resources.

To be effectively prepared, you should be able to determine the criticality of your key assets; analyse threats to them; and implement a set of complimentary controls to provide an appropriate level of protection. Considering the implications of people, process, technology and information; you can then update your cyber security response capability and review your state of readiness in cyber security response.

Step 1 Conduct a criticality assessment

Project research revealed that the five main challenges faced by organisations when making the necessary risk assessment and awareness arrangements to help them prepare for a cyber security incident are:

1. Defining their critical information assets
2. Determining which cyber security threats are most likely to affect these critical information assets
3. Applying the relevant management or technical controls to reduce the likelihood and impact of cyber security incidents affecting their critical information assets
4. Raising awareness about the need for an effective cyber security response capability
5. Determining the likely (or actual) level of business impact associated with a possible cyber security incident.

Other concerns included:

- Identifying where their critical information assets are and who is responsible for them
- Setting their expectations, so that they are aware of what can and cannot be done with the time, resources and money available.

Research revealed that many organisations often did not know the criticality of their own assets and failed to carry out business impact assessments, making it difficult to determine how to protect these assets before, during and after a cyber security incident. You should therefore carry out a criticality assessment to identify your critical information assets (eg important business applications, key systems and confidential data), for example in terms of their strategic or monetary value.

The potential harm that could be caused if your organisation was hit by a cyber security incident should then be determined. This is typically achieved by carrying out a business impact assessment – focusing on confidentiality, integrity and availability – determining the level of business impact if:

- Sensitive information was disclosed to unauthorised parties (confidentiality)
- Important information was compromised (eg key data is inaccurate or wrongly processed)
- Critical systems or infrastructure were no longer available.

When determining business impact, it is often useful to consider scenarios and identify any serious implications in the event of a cyber security incident compromising your critical assets, such as:

- Potential and actual financial loss
- Compliance implications (eg fines, business restrictions, or other penalties)
- Damage to reputation
- Loss of management control
- Impaired growth.

Once you have identified your critical assets you should determine where they are located in your organisation (and beyond), and record important details about their level of criticality (eg critical, significant, minor or negligible). Finally, you should assign responsibility for protecting these assets to capable, named individuals.

Step 2 Carry out a cyber security incident threat analysis

The next step in being prepared for a cyber security incident is to understand the level of threat to your organisation from different types of cyber security incidents, which is often achieved by carrying out a cyber security threat analysis. To do this, you should first have produced a definition of what a cyber security incident means to your organisation and created a set of examples of the types of threats associated with these incidents, such as malware, hacking and social engineering.

In order to contextualise the cyber security threat analysis, you will firstly need to gain a solid understanding of the:

- Nature of your business, business strategy, business processes and risk appetite
- Key dependencies your organisation has; for example on people, technology, suppliers, partners and the environment in which you operate
- Assets that are likely to be targeted, such as infrastructure, money, intellectual property or people – and the computer systems that support them
- Potential compromise to the confidentiality of sensitive information; the integrity of important business information and applications; or the availability of critical infrastructure.

Bearing in mind these important business elements, you can then focus the threat analysis on the:

- Technical infrastructure that supports your critical assets
- Cyber security landscape relevant to your organisation
- Different types of cyber security threats that you are concerned about
- Sources of these threats, such as organised crime syndicates, state-sponsored organisations, extremist groups, hacktivists, insiders – or a combination of these
- Possible threat vectors for attacks to exploit (eg Internet downloads, unauthorised USB sticks, misconfigured systems, inappropriate access, or collusion)
- Vulnerabilities to each particular threat (eg control weaknesses or special circumstances).

When looking at vulnerabilities to particular threats, it can be useful to consider the PLEST acronym, which involves considering vulnerabilities associated with the:

- *Political* environment, at both a macro and micro level
- *Legal and regulatory* environment, including compliance (eg reporting) requirements
- *Economic* environment
- *Socio-cultural*, including the important people aspect
- *Technical* environment (eg logging).

Furthermore, cyber security threat analysis should be conducted on a regular basis because the threat landscape shifts and investigation will provide feedback.

Preventive activities based on the results of cyber security risk assessments can lower the number of incidents, but not all cyber security incidents can be prevented.

Cyber security incident scenarios

Delegates at the project workshop believed that realistic scenarios and rehearsals were effective ways of carrying out threat analysis. A good testing method would typically include initiating a fictional (but realistic) attack internally and assessing how well you can respond to it.

You should therefore engage in periodic scenario-based training, working through a series of attack scenarios fine-tuned to the threats and vulnerabilities your organisation faces. These scenarios also help ensure that relevant individuals understand their role and help prepare them to handle incidents.

Effective scenarios should include:

- Determining what the threat is to your organisation
- Assessing your risk profile (to key assets)
- Considering threat intelligence providers (eg the government, collaborative groups, competitors, CERTs and vendors)
- Evaluating situational awareness and applicability to your organisation
- Simulating a real attack as closely as possible
- Ensuring the right person is doing the right thing at the right time.

There are a number of traditional methods of carrying out threat analysis, and some newly emerging ways of conducting more advanced cyber security threat analysis. In particular, threat intelligence can play a key role in improving the effectiveness of cyber security threat analysis.

Some specialised vendors – including a number of CREST members – are investigating cyber security threat intelligence, but more research needs to be done in this area.

Step 3 Consider the implications of people, process, technology and information

Project research has shown the main challenges faced by organisations when making the necessary arrangements to help them prepare for a cyber security incident are to do with People, Process, Technology and Information.

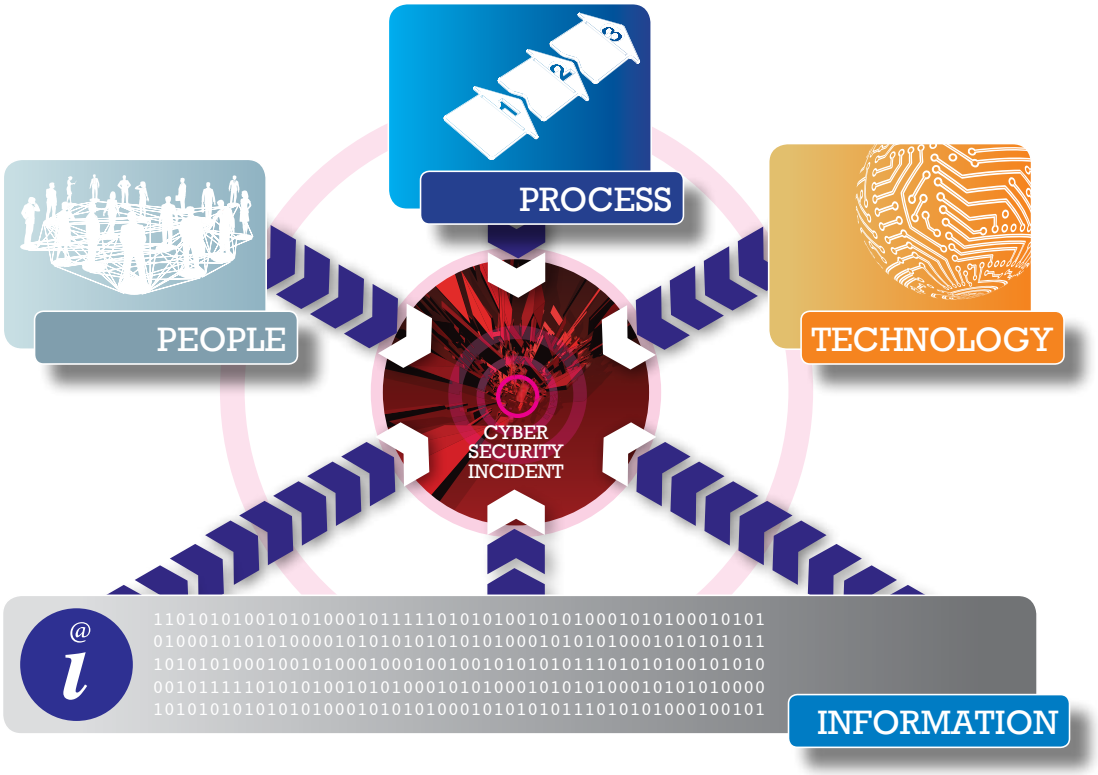

Figure 6: Main considerations for each phase of the cyber security incident response process

Each of these challenges is outlined in the table below and then explored in more detail on the following pages. Whilst they are important to address during the preparation phase, these four components still apply fully when responding to and following up a cyber security incident.

Component	Summary of the main challenges facing CREST customers
People	Organisations often do not have a formal cyber security incident response team or even a named individual who is responsible for dealing with such an incident. More important can be that there is often a lack of technical expertise and nobody available who can take business decisions quickly.
Process	Many organisations do not have adequate processes or methodologies (if they have any at all) to help them deal with cyber security incidents in a fast, effective and consistent manner. They struggle to know what to do, how to do it, who to contact – and can even compromise investigations by their actions.
Technology	Many organisations have not configured their systems or networks to help them identify or respond to cyber security incidents, with inadequate monitoring processes in place. In particular, systems may not have been configured to record appropriate events, identify possible attacks or provide adequate assistance to investigators.
Information	Organisations seldom have information readily available that will help the cyber security incident response team (including third party experts) to respond quickly and effectively, such as details about business management; IT infrastructure; key suppliers; sensitive data; and event logging.

Project research has shown that organisations often do not have a formal cyber security incident response team – or even a point of contact for handling the incident. Nor do they have the budget, resources, technical expertise or support required to respond to cyber security incidents effectively.

Furthermore, cyber security attackers often exploit the people factor (eg by using spear phishing or other social engineering techniques) through the use of common hacking tool kits freely available in the public domain. Consequently, every person in your organisation will need to be aware of the risk from cyber security attacks – and be shown how to help reduce the likelihood and frequency of these attacks.

> "Nearly anyone who can use a web browser can create and control a botnet."

Project research revealed that the main challenges faced by organisations when making the necessary resourcing arrangements to help them prepare for a cyber security incident were:

- Addressing arrangements corporate-wide (including third parties, where needed)
- Providing sufficient funding and resources to deal with cyber security incidents effectively
- Appointing individuals in advance who have sufficient decision-making authority to take action fast in an emergency situation
- Aligning cyber security incident response with business continuity plans and arrangements
- Finding appropriate external sources and levels of guidance to help them prepare for a cyber security incident.

It is therefore important to establish an appropriate cyber security incident response team, with an assigned contact point. This team should be:

- Supported by key stakeholders, such as senior management, the PR department, HR, Legal, IT and business unit management
- Given the authority to confiscate or disconnect equipment and monitor suspicious activity
- Able to undertake external communications and information sharing (eg what can be shared with whom, when, and over what channels)
- Clear about escalation points in the cyber security incident management process
- Understand the requirements for reporting certain types of cyber security incident.

A cyber security incident response toolkit can be provided to help investigators, which may include:

- A suitable method for recording all aspects of the incident, ideally using a template to ensure a consistent, comprehensive approach
- Contact details of all key stakeholders, such as internal and external investigators, technical specialist, suppliers, legal resources, human resources, public relations and business management
- Incident analysis resources: such as port lists; packet sniffers and protocol analysers; documentation for security systems (eg IDS, SIEM, malware protection); network diagrams; and a list of critical assets.
- Forensic imaging tools (eg an imaging laptop; encrypted disks for image storage; mobile phone; digital camera / recorder; portable printer; removable media with trusted versions of programs; and evidence gathering accessories)
- Physical tools (eg screwdrivers, Allen keys, wire cutters, evidence bags, gloves and torch).

Findings from the research project identified that the main functions in organisations that were likely to carry out cyber security incident response would be the:

- IT, cyber or information security department
- IT incident response team
- IT (or other) help desk.

Your incident response team can consist purely of your own staff, be completely outsourced to a third party or – more typically in today's world – involve a combination of both.

However, many organisations have difficulty in determining whether to establish a *specialised* cyber security incident response capability; or *integrate* cyber security incidents into existing incident management processes.

To deal with cyber security incidents effectively, many organisations will need to be able to integrate their response mechanism far more widely across the organisation, not just through the IT department (eg the IT help desk). For example, many third parties (eg suppliers, partners and customers) now have a significant effect on organisations. Furthermore, IT services are often used directly by business units, such as through cloud computing and the use of social networking. Cyber security attacks can use all of these avenues, so an integrated response approach is recommended.

For serious cyber security attacks, both top management and a specialised crisis management team (or equivalent) would also need to be involved, often as part of an escalation process. A wide range of other people may also need to support the investigation, such as:

- Specialist third parties, particularly where organisations have outsourced security services (eg security device management) to Managed Security Services Providers (MSSP) or a Security Operations Centre (SOC)
- Affected business units
- Human Resources (HR), if prosecution is likely or the culprit is suspected to be internal
- Legal counsel and Public Relations (PR).

The people held responsible for dealing with cyber security incidents are typically in IT and information security, but may not have sufficient resources or support, even operating in a blame culture where they fear for their jobs. In some cases, this can be a contributing factor in their reluctance to:

- Escalate the problem to management in a timely manner
- Explain the possible consequences of the cyber security incident – and it's potential impact on the business
- Get outsiders involved – as this might look like failure on their part.

Project research identified that many organisations do not have adequate policies, processes or methodologies (if they have any at all) to help them respond to cyber security incidents effectively. They struggle to know what to do, how to do it, who to contact – and can even compromise investigations by their actions.

To help tackle cyber security incidents in an effective and consistent manner, you should develop an appropriate strategic approach, backed up by a formal cyber security incident response process, which should include:

1. Identifying cyber security incidents
2. Investigating the situation (including triage)
3. Taking appropriate action (eg contain incident and eradicate cause)
4. Recovering systems, data and connectivity.

The process (which is covered in more detail in *Part 5 Responding to a cyber security incident*) should state who should be responsible for each step, how it should be carried out and who to contact for support. Finally, you should ensure that the process has been signed off by appropriate management and test it thoroughly on a regular basis, using a range of different scenarios.

By taking the wrong initial action when a cyber security attack occurs (eg taking systems off the network or cleaning up systems) you could create a detrimental affect like alerting an attacker or destroying vital evidence).

Project research identified that nearly all organisations are likely to use a standard security incident management process, but with cyber security attacks often being dealt with by a major incident response team (or similar). Whatever approach is adopted, a clear methodology and plan should be established to help you respond to cyber security incidents in a fast, effective, consistent manner.

Whilst every situation is unique, there are commonalities that allow for a standardised plan that you can proactively implement and adapt as needed. The plan should be sufficiently comprehensive and agile to cover, and adapt to, many different scenarios, often meaning that it will need to be written at a higher level.

However, the use of standard incident response plans can be a difficult topic for suppliers of cyber security incident response expertise to deal with as the response technique is seldom a linear set of steps and more a set of decisions.

Expert suppliers of cyber security incident response services can help you develop an appropriate process – or implement their own tailored version.

You should appoint a suitable supplier(s) in advance, who is ready to help at short notice, as required (for example by keeping third parties on a retainer for times of need). Should you suffer a cyber security incident, you will then be able to undertake full-fledged breach investigation and eradication quickly and effectively.

Project research revealed that the biggest IT infrastructure challenge faced by organisations when making the arrangements to help them prepare for a cyber security incident is in failing to log the right events or turn on the appropriate logging features.

Many organisations have vastly insufficient logging, archiving, correlation and simulation capabilities. For example, when handling a cyber security incident, historical data can be very important as attacks have often been taking place over an extended period of time – but logs (if they record the right things at all) are often incomplete or do not adequately cover past events.

Effective logging saves you time and money if you experience a cyber security incident. It can also be very helpful as part of a defence (or prosecution) in a court case. You should therefore

- Establish logging standards and procedures
- Configure systems to record the right events
- Monitor these events effectively
- Maintain sufficient historical data (as logs can be overwritten or have insufficient storage space)
- Make appropriate event logs available to investigators in a suitable format.

You should combine key information from as many of the different logs as possible into one central repository, such as a Security Information and Event Management (SIEM) system. For example, evidence of an incident may be captured in several logs that each contains different types of data:

- A firewall log may have the source IP address that was used, whereas an application log may contain a username
- A network IDS sensor may detect that a cyber security attack was launched against a particular host, but it may not know if the attack was successful.

An investigator may need to examine the host's logs to determine that information. Correlating events among multiple indicator sources can be invaluable in validating whether a particular incident occurred.

SIEM solutions are a combination of SIM (security information management) and SEM (security event manager) systems. SIEM technology provides real-time analysis of security alerts generated by network hardware and applications. SIEM solutions come as software, appliances or managed services, and are also used to log security data and generate reports for compliance purposes

"It is not until you are attacked that you realise the value of effective logging"

Project research identified a number of other significant IT infrastructure challenges, which included:

- Having the right tools, systems or knowledge to conduct a suitable investigation
- Understanding the topology of their networks (eg via a suitable network diagram)
- Providing details of technical controls like firewalls, mail filters and intrusion detection systems (IDS) or data loss prevention (DLP) technology
- Deploying other suitable technical controls, as required, such as patching
- Knowing what or where many of their Internet 'touch points' are.

You should try to avoid providing internet access locally, rather than through a central corporate gateway, otherwise you are likely to have no real logging capability and very limited knowledge of your Internet points of presence (sometimes referred to as exfiltration (or infiltration) points).

It is essential to make sure that your organisation has the information readily available that will help the cyber security incident response team (including third party experts) to respond quickly and effectively. Depending on context, the kind of information that expert suppliers typically want to know about falls into four main categories:

1. Business management (eg what the business does, main point(s) of contact, approach to business impact assessment)
2. IT infrastructure (eg network diagrams, system architecture and layout)
3. Data (eg what type of information is processed, where and how)
4. Event logging (eg what types of data and events are logged; on which systems; how and when; as well as how this data is collated and analysed).

The amount of information required by an organisation will differ based on a number of factors, such as its size, market sector, internal capabilities and nature of the particular cyber security incident being investigated.

Organisations can overlook the need to gain fast access to facilities at their outsourced service providers (ie access to premises or equipment). They often have difficulty in getting their third party suppliers (eg cloud service suppliers, infrastructure outsourcers and managed service providers) to provide important information (eg event logs) pertaining to their cyber security incident, sometimes having to wait for several days for something to be actioned.

To operate effectively and efficiently during a cyber security incident investigation, organisations should establish relationships with important third parties in advance of a breach. These third parties may include business relationships, joint ventures, individuals with a link into the network, contractors and anyone else who would be impacted if your organisation had to operate in a degraded capacity.

Once these parties are identified, their contact information should be retained and kept easily accessible by the appropriate individuals, including technical security specialists, business representatives and the Crisis Management Team.

Step 4 Create an appropriate control environment

Advanced cyber security attack or not, many organisations struggle to get the basics right, like establishing a patch management policy – which could stop a large range of malware and make it more difficult for advanced cyber security attackers.

Project research has revealed that there are a number of basic controls that you can implement to help reduce the likelihood of a cyber security incident occurring in the first place, such as access control, firewalls, malware protection and backups. Even if these basic technical controls do not actually prevent cyber security attacks, they can frustrate or slow-down a determined attacker – providing further time for detection before the attack gets to a critical point.
To help you deploy an appropriate control set, CESG have produced two documents based around the *10 Steps to Cyber Security* (an *Executive Guide* and an *Implementation Guide*), produced jointly by GCHQ, BIS and CPNI (see *http://www.gchq.gov.uk/Press/Pages/10-Steps-to-Cyber-Security.aspx*).

The guidance provided is about getting the basics right. Where companies adopt these steps, it has made a tangible difference to their vulnerability to cyber security attack. The document also includes a useful two page section covering incident management.

Many cyber security attacks can now circumvent many traditional security controls, such as malware protection and firewalls, with many cyber security attacks passing through the defences of most signature-based products. Organisations should therefore consider using specialised APT prevention tools available in the market.

There are a number of specialised controls that seemed to be particularly helpful in reducing the likelihood of some types of cyber security attacks, such as:

- Multi factor authentication - something you know (eg a User ID and password) and something you have (eg an access, bank or smart card)
- Digital certificates used to "sign" code from a vendor so that the code can be trusted
- Whitelisting (defining all acceptable ports, addresses or similar – and preventing all other access) or blacklisting (preventing access from specific sites, or addresses)
- Technical monitoring tools, such as intrusion detection or prevention systems (IDS and IPS), data loss preventions (DLP) systems and searchable incident event repository (SIEM).

Even specialised controls are now being defeated. For example, some attackers have been able to break into an application whitelisting vendor and have its code-signing infrastructure sign the malicious code so that they are effectively on the whitelist.

More advanced controls – which are often only adopted by larger or more critical organisations as they are typically expensive, complex and resource intensive - can include:

- Continuous monitoring
- Proactive APT assessments
- Outbound gateway consolidation
- System virtualisation
- Sensitive network or data segregation
- Counterintelligence operations.

Step 5 Review your state of readiness in cyber security incident response

It is important that your organisation maintains an appropriate cyber security incident response capability. This should consist of appropriately skilled people guided by well-designed processes that enable the effective use of relevant technologies. Having the right capability can help 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 ways to help determine your state of readiness 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.

Figure 7 below illustrates a simple model that you can use to determine what your level of maturity is in terms of cyber security incident response, ranging from 1 least effective to 5 most effective.

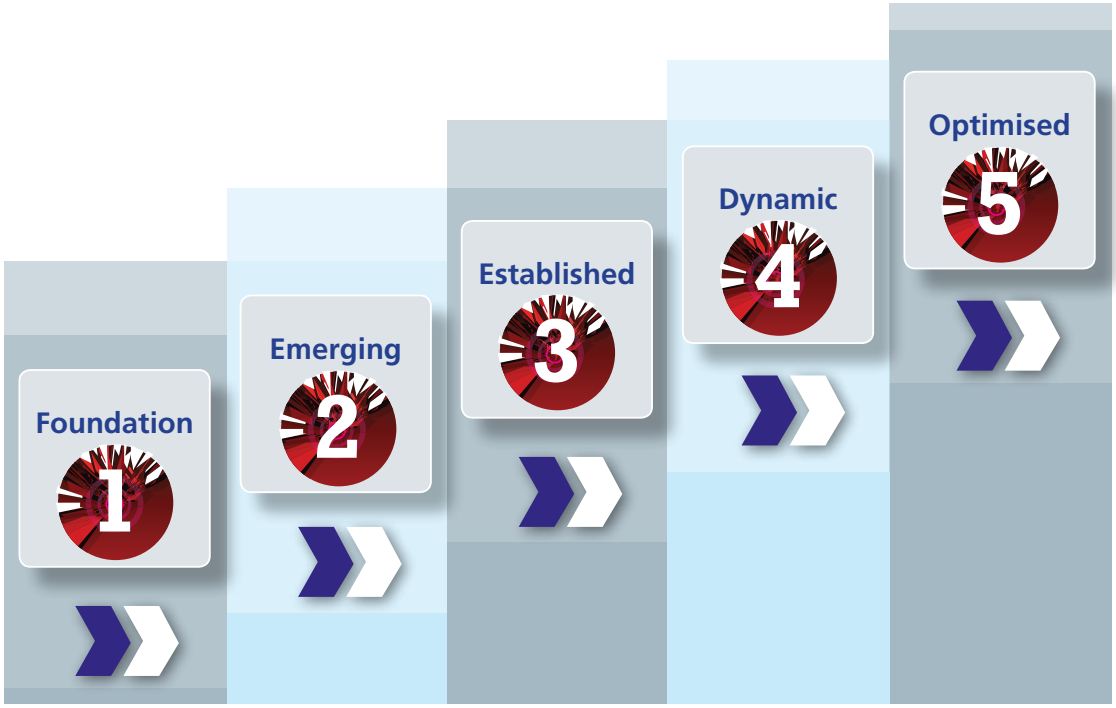

Figure 7: Cyber security incident response maturity model

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, you should review the level of maturity your organisation has in cyber security incident response and compare it to your actual requirements for such a capability. You can compare the maturity of yours with similar organisations to help determine if this level of maturity is appropriate for your organisation.

The maturity of your cyber security incident response capability can play a significant role in determining the level of third-party involvement 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.

Key steps in responding to a cyber security incident

There are a number of common steps that cyber security incident response experts typically follow to help them handle an incident effectively, which should be part of a wider approach, with an emphasis on investigation. Consequently, to provide you with a broader understanding of a typical live situation, the four following steps have been developed.

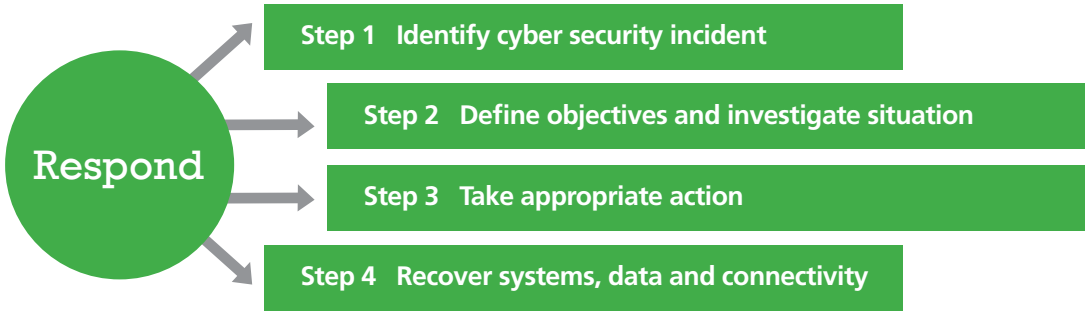

Figure 8: Four key steps in responding to a cyber security incident

Each of these steps is described in turn below and in the rest of this section.

Organisations often treat a cyber security incident as if it is a single one-off event. In reality, for most sophisticated incidents, they have been going on for some time (including reconnaissance) and / or cover more than one part of the organisation.

Step 1 Identify cyber security incident

For many organisations, the most challenging part of the incident response process is accurately detecting and assessing possible cyber security incidents - determining whether an incident has occurred and, if so, the type, extent, and magnitude of the problem.

Project research revealed that the top four challenges faced by organisations when trying to identify a cyber security incident in a fast, effective and consistent manner are:

- Identifying a *suspected* cyber security incident (eg monitoring evidence of unusual occurrences and assessing one or more trigger points)
- Analysing all available information related to the potential cyber security incident
- Determining what has actually happened (eg a DDOS, malware attack, system hack, session hijack or data corruption)
- Confirming that they have actually been subject to a cyber security attack or had a cyber-related breach (the unknown element).

"Not every attack is a cyber security attack – so situational awareness is important"

Detecting potential cyber security incidents

You will need to detect cyber security incidents, analyse them at a high level and confirm what type of incident has actually occurred, if any. Some incidents have overt signs that can be easily detected, whereas others are almost impossible to detect.

Many cyber security incidents are about stealing critical / confidential data – often state-sponsored or organised by cybercrime gangs – that are looking to obtain intellectual property or other sensitive information. As a result, they are mostly non-destructive (although some are very destructive), unobtrusive and difficult to detect (often because attackers have covered their tracks).

Cyber security incidents may also take place over a long timeframe and / or in different parts of the organisation. Advanced targeted attacks can go undetected for many months or years, and even when discovered are often assumed to be nothing more than a common malware infection. Equally, many variants of credential stealing Trojans can remain undetected for many months at a time.

There are many different ways in which a cyber security incident can be identified (with varying levels of detail and accuracy), which include:

- Alerts generated by technical monitoring systems, such as Data Loss Prevention (DLP), intrusion detection systems (IDS), antivirus software, and log analysers
- Suspicious events reported, for example, to the IT help desk by users; to account managers by third parties (often customers); or directly to the security team by industry bodies, your vendor partners or the government
- Anomalies detected by audits, investigations or reviews.

Some specialist organisations, including a number of CREST members, can help you identify potential cyber security incidents, for example by:

- Providing situational awareness (particularly through cyber intelligence)
- Continuously monitoring events that could result in your organisation being affected by a cyber security incident
- Evaluating threat analytics (typically based on the threat model of the behaviour of attacks), helping to determine both symptoms and behaviour
- Performing specialised analysis of host assets, network data and attack files (eg malware)
- Prioritising assets to be investigated
- Addressing unusual or novel problems (eg to do with bespoke file types or encryption).

Cyber security incidents can be detected in any part of the organisation – or through third parties. You should therefore ensure your cyber security incident response process is sufficiently broad and emphasise the importance of incident detection and analysis throughout the organisation.

Users should be informed that they should:

- Report all suspected cyber security breaches to a central point (eg information failures; loss of services; detection of malicious code; denial of service attacks; errors from incomplete or inaccurate business data)
- Note all important details (eg type of breach, messages on screen, details of unusual occurrences)
- Restrain from attempting to take remedial actions themselves.

Monitoring logs and alerts

In an organisation, thousands of possible signs of incidents may occur each day, recorded mainly by logging and computer security software. Signs (also known as triggers or alerts) will be either:

- A precursor, which is a sign that an incident may occur in the future
- An indicator, which is a sign that an incident may have occurred or be occurring now.

Examples of possible cyber security incidents	The sources of these signs include…..
Precursors can include: • Web server log entries that show the usage of a vulnerability scanner • An announcement of a new exploit that targets a vulnerability of the organisation's mail server • A threat from a group stating that the group will attack the organisation. Indicators (there are many) can include: • A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server • Antivirus software alerts when it detects that a host is infected with malware. • A system administrator sees a filename with unusual characters • A host records an auditing configuration change in its log • An application logs multiple failed login attempts from an unfamiliar remote system • An email administrator sees a large number of bounced emails with suspicious content • A network administrator notices an unusual deviation from typical network traffic flows.	• Security software (eg IDS, IPS, DLP, SIEM, antivirus and spam software, file integrity checking software, monitoring services (often provided by a third party) • Logs (eg operating system logs, service and application logs, network device logs and network flows) • Publicly available information (eg information on new exploits, information exchange groups, third party organisations, governments) • People form within your organisation • Third parties (eg customers, suppliers, IT providers, ISPs, partners; government bodies).

Some of the main challenges facing organisations are often to do with monitoring the relevant events on their systems and networks for signs of a cyber security attack. Organisations often collect a lot of data, but do not have the resources, technical skills or awareness to analyse data effectively.

In particular, IDS is not always given sufficient prominence, often seen as a 'fit and forget' solution. Organisations may believe they are monitoring events to detect suspicious attacks, but even though they have an IDS, they fail to:

- Monitor all relevant events
- Carry out monitoring regularly enough - or in an appropriate manner
- Respond to alerts correctly (eg by overlooking indicative alerts or over-reacting to benign alerts)
- Aggregate what may seem like benign alerts into what is a coherent threat message.

"Organisations can put blind trust in the monitoring tools they have purchased, giving them a false sense of security"

Step 2 Define objectives and investigate situation

Understanding the cyber security incident

Once a cyber security incident has been identified, the next stage is to define what the objectives are for the response activities – and to investigate the situation in an appropriate manner. There are many questions that investigators should seek to answer, such as:

- Who has attacked us?
- What is the scope and extent of the attack?
- When did the attack occur?
- What did the attackers take from us?
- Why did they do it?

Project research revealed that the three main challenges organisations face when responding to a cyber security incident in a fast, effective and consistent manner are:

- Determining what information has been disclosed to unauthorised parties, stolen, deleted or corrupted
- Finding out who did it (ie which threat agent or agents) and why (eg financial gain, hacktivism, espionage, revenge, challenge or just for fun)
- Identifying what systems, networks and information (assets) have been compromised.

Other significant response challenges included:

- Working out how it happened (eg how did the attacker gain entry to the system)
- Determining the potential business impact of the cyber security incident
- Performing detailed analysis of the cyber security incident.

When investigating the cyber security incident you should learn as much as you can about the attacker(s) as they will often require differing response approaches and capabilities. You should determine what:

- Methodologies the attackers are using
- Their intention (or motivation), such as financial crime (eg fraud or extortion), theft of intellectual property, personal attack (eg revenge), or disruption to critical services
- Their focus (eg an individual, the whole organisation, your market sector or the government).

Using cyber threat intelligence

During an investigation into a cyber security incident, it can be very useful to have access to *cyber threat intelligence* - research into the attackers to determine their capabilities, motives and likely actions. This can be provided by the government, CERTS, collaborative groups or expert third parties, such as many CREST members.

When a security team conducts and applies cyber threat intelligence, the team will more clearly understand the tactics, techniques and procedures of the attackers and can defeat some attacks by disrupting or degrading their efforts. Threat intelligence can also help you detect an incident during the reconnaissance phase, before you have actually been attacked.

Conducting triage

The early part of an investigation is often referred to as ***Triage***, which consists of:

- ***Classifying*** cyber security incidents (eg critical, significant, normal or negligible impact)
- ***Prioritising*** these incidents (eg high, medium or low)
- ***Assigning*** incidents to appropriate personnel in terms of their legitimacy, correctness, constituency origin, severity or impact.

Cyber security attacks are often more critical than many traditional security incidents, but should still be subject to a consistent classification process. In any situation, the categories defined in the CESG GovCertUK incident response guidelines - explained in the table below - are useful as a point of reference.

Category	Description	Example
Critical	These incidents will usually cause the degradation of vital service(s) for a large number of users, involve a serious breach of network security, affect mission-critical equipment or services or damage public confidence in the organisation.	Targeted cyber security attacks or loss of publicly available online service.
Significant	Less serious events are likely to impact a smaller group of users, disrupt non-essential services and breaches of network security policy.	Website defacement or damaging unauthorised changes to a system.
Minor	Many minor types of incident can be capably handled by internal IT support and security. All events should be reported back to the information security team who will track occurrences of similar events. This will improve understanding of the IT security challenges and may raise awareness of new attacks.	Unsuccessful denial-of-service attack or the majority of network monitoring alerts.
Negligible	It is not necessary to report on incidents with little or no impact or those affecting only a few users, such as isolated spam or anti-virus alerts; minor computer hardware failure; and loss of network connectivity to a peripheral device, such as a printer.	Isolated anti-virus alert or spam email.

Carrying out first response

The first people dealing with the incident are sometimes refrerred to as first responders, ideally as part of a team. These first responders should be able to determine whether any specialist resources – including third parties - will be required.

Many organisations do not have the right tools, systems or knowledge to conduct a suitable investigation. You need to identify quickly when the scope and severity is beyond in-house skills, before decisions are made that may adversely affect an investigation. It is critical for arrangements to have been made in advance so that expert investigators are available at short notice and have enough prior information to be able to hit the ground running.

Whoever actually carries out all or part of the investigation, it is still your responsibility, so you will need to monitor each step carefully – and record what has happened.

As well as expert cyber security incident response experts, other third parties that you may wish to get involved can include technology forensics specialists, technology analysts (for example, database experts), Information analysts (for example, accountants), legal experts and on-site police support.

Some organisations set up a "war room" during serious cyber security attacks. This is the crisis management team's primary meeting and collaboration space, where all relevant parties (incident investigators, IT staff representatives, stakeholders and other leaders) assemble to manage the incident from one central point.

Performing initial analysis

In the early stages of investigating a cyber security incident, the precise nature of the incident may be unknown and initial analysis will be required.

When investigating a cyber security incident, the approach taken can be either:

- Intelligence driven, based on information gathered from: government agencies (eg CPNI), monitoring of internal resources, open source information or data provided internally
- Evidence-driven, based on information gathered from corporate infrastructure or applications (typically event logs).

Investigators will often wish to:

- Examine important alerts or suspicious events in logs or technical security monitoring systems (eg IDS, IPS, DLP or SIEM)
- Correlate them with network data (including data from cloud service providers)
- Compare these against threat intelligence.

All types of event logs should be considered, including:

- Firewall/router logs (including proxy servers)
- Technical security monitoring logs and alerts (eg from intrusion detection (IDS) or data loss prevention (DLP) software
- Traditional Server and workstation logs
- Business application audit logs
- Web server logs
- DNS and DHCP logs covering all devices
- Email history and archives
- Internet usage logs
- Network data
- Building access logs.

Note: *You should retain these logs for as long as possible, as part of an approved log retention policy. During an investigation these logs will provide valuable information and are often requested by third parties.*

When carrying out an investigation, each possible trigger event should be thoroughly investigated, including:

- Date/time
- Internet protocol (IP) address (internal or external)
- Port (source or destination), domain and file (eg exe, .dll)
- System (hardware vendor, operating system, applications, purpose, location).

Step 3 Take appropriate action

Containing the cyber security incident

One of the first key actions to be taken after the initial investigation (and often as part of that investigation) is to contain the damage being done by the cyber security incident, for example by stopping it from spreading to other networks and devices both within your organisation and beyond.

Containment typically comprises a number of concurrent actions aimed at reducing the immediate impact of the cyber security incident, primarily by removing the attacker's access to your systems. The objective of containment is not always to return (directly) to business as usual, but to make best efforts to return to functionality as normal, while continuing to analyse the incident and plan longer term remediation.

There are many ways in which a cyber security incident can be contained, which include:

- Blocking (and logging) of unauthorised access
- Blocking malware sources (eg email addresses and websites)
- Closing particular ports and mail servers
- Changing system administrator passwords where compromise is suspected
- Firewall filtering
- Relocating website home pages
- Isolating systems.

You should consider creating separate containment strategies for different types of major cyber security attack, with criteria documented clearly to facilitate decision-making. These criteria can include evaluating the:

- Potential damage to and theft of resources
- Need for evidence preservation
- Service availability (eg network connectivity, services provided to external parties)
- Time and resources needed to implement the strategy
- Effectiveness of the strategy (eg partial containment, full containment)
- Duration of the solution (eg emergency workaround to be removed in four hours, temporary workaround to be removed in two weeks, permanent solution).

Some specialist organisations, including a number of CREST members, can help you to contain cyber security incidents, for example by:

- Identifying immediate actions to be performed (eg based on high risk assets, time dependant issues, business/commercial decisions)
- Ensuring that actions can be performed safely
- Minimising the risk that an attacker will respond/escalate
- Determining whether findings identified during the investigation are critical
- Reacting to critical findings during the investigation.

Eradicating the cause of the incident

After an incident has been contained, eradication is often required to eliminate key components of the incident (eg removing the attack from the network, deleting malware and disabling breached user accounts), as well as identifying and mitigating vulnerabilities that were exploited.

During the eradication process, there are a number of actions you can take, which include:

- Identifying all affected hosts within (and sometimes beyond) your organisation, so that they can be remediated
- Carrying out malware analysis
- Checking for any response from the attacker to your actions
- Developing a response (preferably in advance) if the attacker uses a different method of attack
- Allowing sufficient time to ensure that the network is secure and that there is no response from the attacker.

Effective eradication plans must be executed with speed and precision because attackers often try to re-establish a base and then entrench themselves again into the network once they sense they have been discovered and eradication is underway.

There are many steps that attackers take to either continue the attack during eradication or avoid identification, which can include:

- Registering new IP addresses for their domain names if they suspect that eradication teams have blocked their IP addresses
- Accessing an undetected web shell they have installed earlier to regain access to the environment after access has been removed
- Installing advanced malware that makes changes to the file system or network to trigger a fail-safe within the malware if detected, which will in turn remove itself together with the evidence of infection.

> **"While investigating a sophisticated cyber security breach may seem like a marathon, effective eradication must be a sprint"**

Gathering and preserving evidence

Research indicated that organisations have significant difficulty in meeting forensic requirements for cyber security incident response, such as in preserving evidence and maintaining a chain of custody.

Evidence will need to be gathered at various points during the investigation, but all evidence will be governed by two main rules, which are:

- Admissibility of evidence – whether or not the evidence can be used in court
- Weight of evidence – the quality and completeness of evidence

When handling computer electronic evidence, you should adhere to the Association of Chief Police Officers (ACPO) Guidelines on Computer Evidence (ACPO).

You will also need to comply with relevant laws, such as the:

- Police and Criminal evidence act 1984 (PACE)
- Data protection Act 1988
- Computer Misuse Act 1990
- Regulation of Investigatory Powers 2000 (RIPA).

It is essential that you maintain a chain of evidence for both paper-based and electronic information. You should keep a detailed written log of every action during the investigation so that:

- Clear and precise evidence can be referred to at a later date
- The sequence of events and actions taken can be repeated by opposition experts, if required.

This action log should include:

- Identifying information (eg the location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses of a computer)
- Name, title, and phone number of each individual who collected or handled the evidence during the investigation
- Time and date (including time zone) of each occurrence of evidence handling
- Locations where the evidence was stored.

When gathering data for a potential prosecution, it is important that you do not:

- Turn off any system under investigation until an expert decision on the risk of doing so has been made.
- Perform analysis on a live system under investigation before a forensically safe image has been taken.

All forensic works should only be performed on copies of the evidential material (eg using imaging technology) and the integrity of all evidential material must be protected. Furthermore, for many cyber security attacks, a more detailed forensic investigation will be required. Organisations should therefore consider employing third party forensic experts.

Step 4 Recover systems, data and connectivity

The final step in responding to a cyber security incident is to restore systems to normal operation, confirm that the systems are functioning normally, and remediate vulnerabilities to prevent similar incidents occurring.

Project research identified that the main challenges organisations face when recovering from a cyber security incident in a fast, effective and consistent manner are:

- Confirming that remediation has been successful
- Reconnecting networks; rebuilding systems; and restoring, recreating or correcting information.

It is therefore important to have an appropriate recovery plan in place, which should include:

- Rebuilding infected systems (often from known 'clean' sources)
- Replacing compromised files with clean versions
- Removing temporary constraints imposed during the containment period
- Resetting passwords on compromised accounts
- Installing patches, changing passwords and tightening network perimeter security, such as firewall rulesets
- Testing systems thoroughly – including security controls
- Confirming the integrity of business systems and controls.

It is important to validate that systems are operating normally again, which can often be achieved by carrying out an independent penetration test of the affected systems, complemented by a security controls assessment.

Advanced cyber security attackers will often try to get back into the network through all of the methods at their disposal. They will also come back knowing that they are being investigated and that their existing tactics, techniques and procedures have been discovered. Therefore, it is important to ensure that all elements of the attack have been eradicated and that the attackers cannot carry out further attacks.

Many CREST members are able to help ensure that a cyber security incident has been eradicated effectively – and help prevent attackers from returning.

To help detect further attacks, cyber security threat intelligence (including network situational awareness) should be gathered and retained and the network monitored for any further attempted attacks. Monitoring may need to take place over an extended time to detect any further attacks (or attempted attacks).

Once systems have been recovered and controls have been tested, stakeholders should then be provided with a brief summary of what took place. The team should report that eradication was completed successfully and note any exceptions and other significant findings. Briefings to stakeholders about the results should be well planned and conducted soon after the event. An initial, high-level communication can be issued within a day or so of the event, followed by a deeper explanation of the activities that took place, as described in *Part 6 - Following up a cyber security incident.*

Overview

PHASE 3
Follow Up

There are many important activities that should be undertaken following a cyber security incident. In practice, some of these (often important) follow-up actions may not be carried out due to insufficient resources, higher priorities, lack of awareness or the pressing need to get the organisation back on track, business as usual.

> "The focus is on protecting the business, rather than following up the cyber security incident"

Research indicated that the biggest challenges organisations face when following up a cyber security incident are:

- Conducting sufficient investigation (eg using deep dive forensic capabilities) to identify (and prosecute, if appropriate) the perpetrator(s)
- Performing problem cause analysis
- Carrying out root cause identification
- Quantifying the business impact of the incident
- Supporting criminal investigations
- Performing trend analysis.

Reporting was also seen as a critical part of following up a cyber security incident, with few organisations admitting having significant challenges in this area.

Project research highlighted a set of key tasks that organisations should consider when following up a cyber security incident, as shown in *Figure 9* below.

Figure 9: Important cyber security incident response follow up actions

Some of these activities may also be performed prior to the ***Follow up*** stage during cyber security incident response.

Step 1 Investigate the incident more thoroughly

There is typically a need for you to investigate a cyber security incident more thoroughly after the event than when responding in the 'heat of the battle'. This will help you to find out what actually happened, improve controls, share data with partners and prevent the incident from reoccurring.

As part of this investigation you should consider:

1. Performing problem cause analysis, using techniques such as:
   - Failure mode and effects analysis (FMEA)
   - Current reality tree (CRT) or fault tree analysis

2. Carrying out root cause identification, using techniques such as:
   - The five-whys approach
   - Why-because analysis (WBA)
   - Cause-and effect (fishbone) diagrams

3. Quantifying the business impact of the incident (eg in terms of financial, reputational, management or compliance impact).

You should carry out sufficient investigation to identify the perpetrators(s) of the cyber security incident, which may involve specialist support, such as from forensic investigators.

> **"Organisations are seldom interested in chasing the perpetrator of a cyber security incident – they just want to recover their systems and get back business as usual as quickly as possible"**

Step 2 Report the incident to relevant stakeholders

Once a cyber security incident has been successfully handled, formal reporting will often be required to both internal and external stakeholders. Key questions to consider include:

- What are our reporting requirements?
- Who do I report to?
- What do I report?
- In what format do I report?
- What is the objective of reporting?

Once you have answered these questions, the actual reporting itself should include:

- A full description of the nature of the incident, it's history, and what actions were taken to recover
- A realistic estimate of the financial cost of the incident, as well as other impacts on the business, such as in terms of damage to reputation, loss of management control or impaired growth
- Recommendations regarding enhanced or additional controls required to prevent, detect, remediate or recover from cyber security incidents more effectively.

Some organisations are mandated to report to particular authorities. For example, Energy companies must report interruption data to the regulator (Ofgem) as part of a reliability incentive scheme.

Government Departments have a responsibility to report computer incidents (including cyber security incidents) under the terms laid out in the Security Policy Framework (SPF), issued by the Cabinet Office. The categorisation is built primarily around whether the Department has been specifically targeted or not. Targeted attacks must be reported to GovCertUK (the Government's Computer Emergency Response Team), whereas other types of attack can be notified to them, but do not generate a "formal report" requirement.

In many cases there can also be benefits in voluntary reporting to other important stakeholders, such as:

- Law enforcement agencies
- Computer Emergency Response Teams (CERTs)
- Regulatory bodies with particular market sectors (eg the FSA or Bank of England in Finance)
- Specialised international bodies, such as NIST or ENISA
- Collaborative partners (see Part 8 The Way Forward for more details)
- Specialised membership organisations.

Project research revealed that:

- There is a lack of reporting from victims, particularly large organisations, where reputation protection and the stigma attached to an attack are important considerations
- Organisations often do not know who to report incidents to or what the benefits are of reporting
- It can sometimes appear that reporting cyber security incidents helps other organisations (or the government), rather than the organisation who actually reports it
- More work needs to be done to improve the reporting of cyber security incidents.

Step 3 Carry out a post incident review

Important information about the cyber security incident should be discussed during a post incident review. Questions to be answered in such a review can include:

1. How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
2. What information was needed sooner?
3. Were any steps or actions taken that might have inhibited the recovery?
4. Could any unforeseen events have been prevented?
5. What would the staff and management do differently the next time a similar cyber security incident occurs?
6. How could information sharing with other organisations have been improved?
7. What corrective actions can prevent similar incidents in the future?
8. What precursors or indicators should be watched for in the future to detect similar incidents?
9. How can results be fed back into our risk assessment methodology?
10. What lessons have we learned?

To support an effective post incident review, all key discussions and decisions conducted during the eradication event should be well documented. A report should be produced from the post incident review and presented to all relevant stakeholders.

Step 4 Communicate and build on lessons learnt

An essential part of following up a cyber security incident is to document, communicate and build on lessons learned. This should be viewed as an on-going process through which you can collaborate and learn from previous mistakes, incidents and experiences.

Communication to all stakeholders should be clear, concise and focused on problem resolution and control improvement. It should clearly identify any gaps that remain and propose efforts to mitigate them.

An action plan should be created that explains how the organisation will leverage lessons learned from the incident to become more resilient in the face of future cyber security attacks. The action plan should include projects or initiatives, technical and nontechnical, that will help reduce an attacker's chance of success and respond to an attacker's activities more rapidly and effectively. Analysis of the cyber security incident should consider whether technical capability gaps contributed to the attacker's success or whether people or process gaps were the main culprit.

Each action should be assigned to a named individual and given a suitable priority and completion date. The status of all action should then be monitored to ensure that they are being completed in a timely and effective manner.

You should use any lessons learnt to share both key issues and good practice across all areas of the business, not just within IT and cyber security teams.

Step 5 Update key information, controls and documents

Following a cyber security incident, it is important to update your cyber security incident response approaches, controls and related documents. However, project research revealed that a number of organisations experienced difficulties in updating their:

- Cyber security incident management methodologies or processes
- Cyber security incident management preparatory activities
- Management controls (eg training and awareness)
- Technical controls (eg patching, configuring system logs, and use of intrusion prevention / detection tools)
- Business continuity or crisis management arrangements
- Internal IT auditing procedures.

When updating controls, research revealed that the attack vectors causing most concern were:

- Poorly designed web applications
- Misconfigured systems
- Internet downloads
- Personal devices (eg tablet or smart phone)
- Authorised third parties (eg customers, suppliers, business partners).

These attack vectors should be examined in your own organisation and relevant controls improved as necessary.

Step 6 Perform trend analysis

You should maintain records about the status of all security incidents (including cyber security incidents), along with other pertinent information. You should review relevant cyber security incident data regularly to help:

- Evaluate patterns and trends of cyber security incidents
- Identify common factors that have influenced cyber security incidents
- Determine the effectiveness of controls (eg which controls are better at preventing, detecting and delaying cyber security incidents or minimising their business impact)
- Understand the costs and impacts associated with cyber security incidents.

Generally there is nothing specifically different about archiving cyber security incidents in comparison to archiving any other data, although:

- You may wish to search your archived data more often.
- Incident-related data is usually sensitive and you should apply appropriate security mechanisms to protect it.

Understand the benefits of using third party experts

There are many reasons why an organisation may wish to employ external cyber security incident response providers, such as to help carry out activities outlined in previous sections. Project research indicated that the top three reasons (by some way) for hiring them are because of the (often significant) advantages of specialised third parties:

- ***Providing resourcing and response expertise*** – giving you access to more experienced, dedicated technical staff who understand how to carry out sophisticated cyber security incident investigations quickly and effectively
- ***Conducting technical investigations*** - for example by providing deep technical knowledge about the cyber security attack; reporting to top management about how they dealt with it; remediating the problem effectively (ensuring that attackers are not alerted thereby allowing them to take further action); and performing expert deep-dive forensics
- ***Performing cyber security analysis***, for example by: monitoring emerging cyber threats (allowing them to be more pre-emptive to cyber security attacks); applying modern analytic capabilities to aggregate relevant data from many different systems; and providing situational awareness, particularly in the area of cyber intelligence (eg to help create a clear picture of their threat adversaries).

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.

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.

Review Cyber Incident Response (CIR) schemes

The National Cyber Security Strategy sets a strategic objective of making the UK more resilient to cyber attacks. Such attacks can vary in terms of persistence, sophistication and impact.

CREST has collaborated with the UK Government to develop a CESG/CPNI Cyber Incident Response (CIR) service, which was launched in August 2013. Drawing on the experiences of a successful CESG/CPNI pilot (funded by the National Cyber Security Programme), a complimentary twin track approach has been developed for the provision of certified Cyber Incident Response services:

- A broad-based scheme focused on maintaining an appropriate standard for cyber incident response, managed by industry professional bodies, delivered by industry and endorsed by CESG and CPNI (initially administered by CREST)
- A smaller, focused Government run Cyber Incident Response (CIR) scheme certified by CESG and CPNI using specialised, highly capable industry partners to help respond to sophisticated targeted cyber attacks against networks of national significance.

This approach will enable all those organisations that may be victims of cyber attack – SMEs, national and multinational industry, the CNI, the wider public sector and central government – to source an appropriate incident response service tailored to their particular needs and allow GCHQ and CPNI to focus on the most challenging attacks. Both schemes will include phased introduction of mandated cyber professional qualifications.

An organisation affected by a cyber security incident should first decide which of the certified incident response schemes best fits their circumstances.

- Those companies participating in the CREST scheme will be listed on the CREST website
- Details of companies certified under the CESG/CPNI CIR scheme will be shown when applications have been assessed.

References: **http://www.cpni.gov.uk/advice/cyber/cir/#sthash.zWZDkOoP.dpuf**
http://www.crest-approved.org/index.html

Select an appropriate supplier who can meet your requirements

If your organisation decides to appoint an external provider of cyber security incident response services, it is important that you choose a supplier who can most effectively meet your requirements – but at a reasonable cost.

Consequently, a systematic, structured process has been developed to help you select a suitable supplier, as shown in *Figure 10* below.

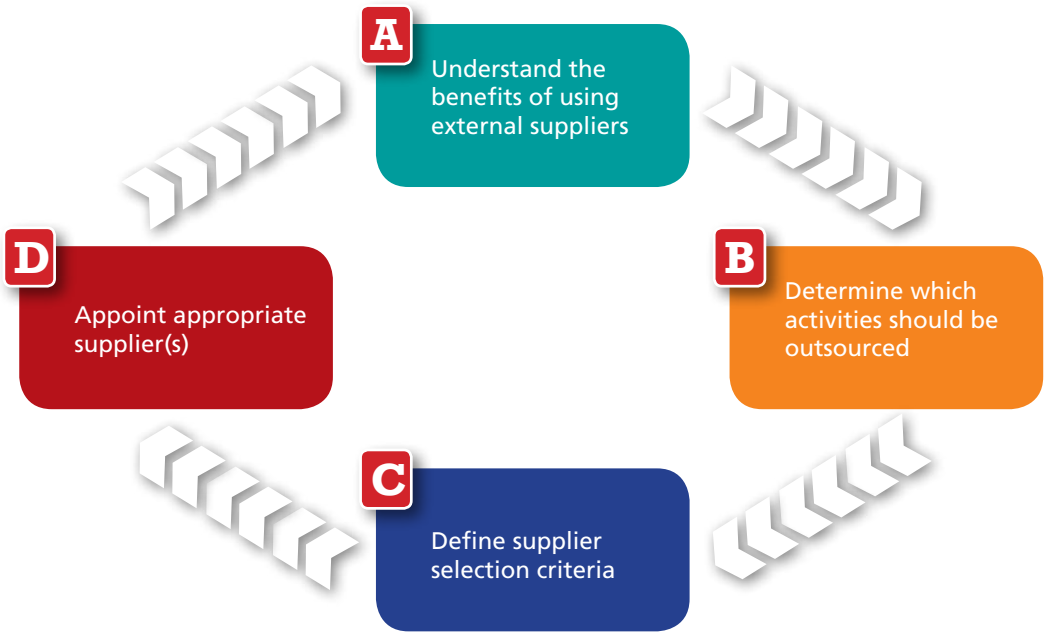

Figure 10: The supplier selection process

Each of these four phases is explained in detail in the companion CREST report ***Cyber Security Incident Response – Supplier Selection Guide.***

The CREST advantage

It has been recognised that organisations suffering cyber security attacks often do not know where to go for help, or what the quality of the service will be from the suppliers who provide expert response services. What organisations really need is the ability to access demonstrably skilled, knowledgeable and competent individuals working for organisations that have been independently assessed against best practice and who have the policies, processes and procedures in place to enact recovery and protect confidential information.

The recent government announcement on the formal launch of two schemes, the CESG/CPNI CIR and CREST CSIR, are designed to help the buying community in this selection process. These schemes provide a recognised set of professional qualifications and set a very high bar for professional services firms working in this area.

The schemes also provide a benchmark for suppliers to meet that reflects defined and agreed best practice, including the need to provide a quality service and understand the requirements to protect client information. Underpinned by meaningful and enforceable codes of conduct these two elements provide a great deal of protection to buyers and will enable you to select 'partners' with a great deal more confidence.

CREST cyber security incident response members are well placed to meet these – and other – requirements. By appointing one of these CREST organisations you can rest assured that you are procuring cyber security incident response services from a trusted, certified external company who employ professional, ethical and highly technically competent individuals.

Research indicated that the areas where organisations believe they will gain most assurance from outsourcing cyber security incident response activities to CREST cyber security incident response members were that these providers will:

- Use staff who act in a professional, ethical manner, according to a code of conduct
- Provide a reliable, effective and proven cyber security incident response service
- Be up-to-date with the latest cyber threats, adversaries, techniques and countermeasures
- Respond to cyber security incidents in a fast, effective manner
- Provide advice on how to reduce the likelihood of a similar incident from taking place
- Create a trusted framework within which the investigation takes place
- Help them achieve compliance with legal, regulatory, corporate or government standards, managing both business constraints and risks
- Protect client information and systems both during and after the event
- Keep the investigation itself confidential (whereas many organisations are happy to for others to know that they have commissioned a cyber security incident response service)
- Adhere to processes and procedures that have been subject to independent vetting.

We need an objective perspective provided by professionally trained and experienced consultants.

Summary of key findings

Project research identified ten key findings about cyber security incident response in general, which could be important to your organisation. You should therefore consider the relevance of these findings, which are outlined below.

1. Cyber security incidents, particularly serious cyber security attacks, such as advanced persistent threats (APTs), are now headline news.
2. There is no common understanding (or taxonomy) of what constitutes a cyber security incident, with no definitive set of threats.
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.
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).
5. Few organisations – of any type - are well prepared for a cyber security incident in terms of people, process and technology and in the information needed to respond effectively.
6. 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.
7. 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.
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, for example in terms of budget, resources, technical skills, support and influence.
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 CREST members), can significantly help organisations to handle cyber security incidents in a more effective and appropriate manner – particularly serious cyber security attacks.

Cyber security resilience

Access points into an enterprise have dramatically expanded. Cloud services, social media, mobile devices and bring your own device (BYOD) policies have moved the corporate perimeter through firewalls, devices and applications down to the most sensitive data that should be protected.

Creative, talented and aggressive attackers continue to drive the threat world into new areas.

The threat landscape will continue to evolve, with new and innovative attack methods being able to adapt to their chosen target environment(s). Furthermore, future attacks will be ever more likely, using automated tools, to compromise hundreds of thousands of computers around the globe.

Even in today's world it will not be possible to prevent all cyber security incidents. As attackers adapt and change, organisations will need to adapt and change as well. You should therefore prepare for an attack executed by an advanced, sophisticated, organised, well-funded and persistent adversary.

To be better prepared, you should consider how you can:

- Protect your most important data in a compromised environment
- Make it more difficult for attackers to be successful
- Detect that an attack is being planned - or is already underway
- Respond to today's sophisticated attacks.

In an ideal world your cyber security incident response capability would be part of a wider *cyber security resilience strategy*, which might include:

- Identifying methods of preventing the cyber security incident occurring in the first place, such as via cyber security situational awareness (eg using cyber security intelligence), data analytics and performance of appropriate rehearsals in realistic scenarios
- Performing cyber security threat identification and horizon tracking
- Integrating cyber security incident response activities into corporate, market sector and government initiatives, including collaboration with a wide range of other organisations
- Carrying out regular rehearsals of the cyber security incident management response process, using realistic scenarios
- Deploying enhanced technical controls to detect and enable effective responses to cyber threats and attack
- Continually evaluating how you can respond to cyber security incidents in a faster, more agile, and more effective nature.

Although this wider topic of cyber security resilience is out of scope for this project, it was highlighted as a particularly important area where further research and focus is required.

The need for collaboration

Project research revealed a need for greater collaboration in cyber security incident response, the main aims of which are to help your organisation, your sector and the government to:

- Proactively respond to cyber security attacks (eg by closing channels or 'attacking the attacker')
- Close down criminal operations
- Prosecute those responsible for the attack
- Reduce the frequency and impact of future security incidents.

The main challenge organisations face in collaborating about cyber security incidents is in:

- Dealing with cloud computing and other outsourced suppliers
- Using cyber security intelligence sharing platforms and collaboration forums effectively
- Adopting a common language for communicating.

The UK is one of many governments around the world which recognise the serious nature of the threat that is emerging from cyber-space. Nations of the world are giving high priority to implementing cyber security strategies that will both improve their resilience to cyber security incidents and (where possible) reduce the impact of cyber security attacks.

Fusion cell and the CISP

The UK has set up a cyber security "fusion cell" for cross-sector threat information sharing. The intention is to put government, industry and information security analysts side-by-side for the first time. Public and private sector analysts will be joined by members of intelligence agencies, law enforcement and government IT as they exchange information and techniques and monitor cyber security attacks in real time.

The fusion cell is a cyber security attack monitoring operations room at an undisclosed location in London as part of a government cyber security initiative. The Cyber Security Information Sharing Partnership (CISP) also includes a secure web portal and programmes aimed at building cross-sector trust to underpin information sharing. The web portal is based on a social networking structure, giving members of the CISP the freedom to choose who they wish to share information with in real time.

Note: *This sort of information sharing is typically only available to very large organisations – and should only be considered as part of your armoury for responding to cyber security incidents.*

Furthermore, a number of international organisations (eg ENISA, NIST, ISF and ISACA) work constantly to promote or use collective defences to analyse the latest developments in cyber threats and cybercrime.

Conclusion

Organisations are seldom adequately prepared for a serious cyber security incident. They often suffer from a lack of budget, resources, technology or recognition of the type and magnitude of the problem. In addition, they do not have the software, testing, process, technology or people to handle sophisticated cyber security threats, such as Advanced Persistent Threats (APTs).

However, you can respond to cyber security incidents in a faster, more effective manner. To achieve this, you will need to:

- Understand a number of key concepts (eg a definition of cyber security incident response; types of cyber security attack; the main challenges and ways in which they can respond)
- Determine your state of readiness for responding to a cyber security incident – and build an appropriate cyber security incident response capability (tailored to suit your organisation)
- Participate in government sponsored and other initiatives related to cyber security incidents or incident response
- Adopt a systematic, structured approach to cyber security incident management, considering the key actions that you might need to take when preparing for, responding to and following up a cyber security incident – addressing requirements for people, process and technology
- Select an appropriate supplier(s) of cyber security incident response expertise who can most effectively meet your requirements – but at the right price - considering an agreed set selection criteria
- Keep an eye on future developments in the evolution and response to cyber security incidents – particularly sophisticated cyber security attacks – and plan an appropriate way forward.

> "The word 'cyber' may be fairly artificial, but it really raised awareness, particularly in the business!"

Assurance In Information Security

Company Membership

Demonstrable level of assurance of processes and procedures of member organisations.

Knowledge Sharing

Production of guidance and standards.

Opportunity to share and enhance knowledge.

Professional Qualifications

Validate the knowledge, skill and competence of information security professionals.

Professional Development

Encourage talent into the market.

Provision of on-going personal development.

CREST Representation	• Demonstrable level of assurance of processes and procedures of member organisations • Validation of the competence of technical security staff • On-going professional development for those entering or progressing in the industry • All CREST examinations reviewed and approved by GCHQ (CESG).
CREST Penetration Testing	• Assignments performed by qualified individuals with up-to-date knowledge, skills and competencies in the latest vulnerabilities and techniques used by real attackers • Confidence that CREST Member companies will protect confidential client information.
CREST Cyber Security Incident Response (CSIR) Scheme	• Company assessments and professional qualifications endorsed by GCHQ and CPNI • Cyber Security Incident Response (CSIR) Scheme, complementing the CESG/CPNI Cyber Incident Response (CIR) Scheme • New Cyber Security Incident Response Manager's certification.
CREST Security Architects	• Professional examinations, which are formally recognised under the CESG Certified Professional Scheme.
CREST Codes of Conduct	• Provide a significant level of protection for organisations procuring technical security testing services • Ensure the quality of the services provided by, and the integrity of, both the companies and individuals involved; and enforce adherence to audited policies processes and procedures.
CREST Research	• Procurement guides compiled to assist the buying community and suppliers alike in procuring the right technical security testing services • Work closely with e-Skills, academia and training organisations.
CREST Overseas	• Member companies in a growing number of countries, such as a formally established Chapter in Australia, which has full support of the Australian Government.

Abbey House | 18-24 Stoke Road | Slough | Berkshire | SL2 5AG

T: 0845 686 5542
E: admin@crest-approved.org
W: crest-approved.org