CREST

# Cyber Security Incident Response Supplier Selection Guide

Version 1

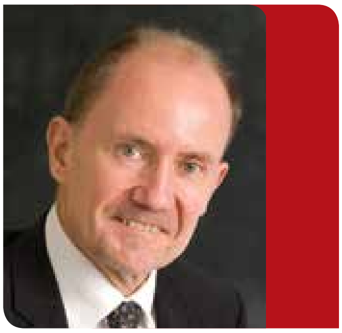
***Published by:***

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,<br>
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.

## Contents

### Part 1 – Introduction and overview

### Part 2 – Key concepts

### Part 3 – Understand the benefits of outsourcing

### Part 4 – Determine which activities should be outsourced

### Part 5 – Create an appropriate set of supplier selection criteria

### Part 6 – Appoint a suitable supplier

## About this Guide

This *Cyber Security Incident Response – Supplier Selection Guide* (the Guide) provides practical advice on the procurement of cyber security incident response services. It outlines the key concepts you will need to define a cyber security incident and build an appropriate cyber security incident response capability. It then presents detailed guidance on how to apply a systematic, structured process to help you select a reputable commercial supplier who can most effectively meet your requirements at a reasonable price.

✓ A separate CREST publication, the *Cyber Security Incident Response Guide*, provides detailed advice and guidance on how you can prepare for, respond to, and follow up a cyber security incident in a fast and effective manner.

This Guide explores the main reasons why you may wish to outsource some or all of your cyber security incident response capability, which will typically be because of the (often significant) advantages of specialised commercial suppliers:

- ***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 your adversaries).

The Guide explores the benefits of using appropriately qualified third party experts, such as those:

- Holding CREST Intrusion Analysis or Cyber Incident Response qualifications; and
- Working for trusted independently assessed companies, such as CREST Cyber Security Incident Response (CSIR) or CESG/CPNI Cyber Incident Response (CIR) scheme members.

Employing the services of these experts can significantly help you to handle cyber security incidents in a more effective and appropriate manner – particularly serious cyber security attacks.

! The outsourcing of your cyber security incident response activities does not diminish the need for internal staff with management responsibilities to ensure compliance requirements are met and confidential information is protected.

## *Audience*

This Guide is aimed at organisations in both the private and public sector. Project research has revealed that the main audience for 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*

The purpose of this Guide is to help you to:

- ***Understand the benefits of using external suppliers,*** which includes: providing resourcing and response expertise; conducting technical investigations; and performing advanced cyber security analysis
- ***Determine which activities should be outsourced,*** be it all of your cyber security response capability or just specialised areas like technical or forensic investigations; situational awareness; and advanced data analytics
- ***Define criteria upon which to base selection of a suitable supplier,*** including: solid reputation, history and ethics; high quality, value-for-money services; research and development capability; highly competent, technical response experts; security and risk management; and strong professional accreditation
- ***Appoint suitable third party experts,*** providing guidance on: identifying potential suppliers; reviewing the CREST CSIR or CESG/CPNI CIR scheme requirements for membership; selecting a supplier who can meet your requirements; and managing your expectations.

## *Rationale*

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

However, 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).

Current cyber security incident response guidelines can be very useful, but do not typically provide in-depth guidance about dealing with cyber security incidents or advice on who organisation can ask for help – backed up by suitable 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.

### *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. The research 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 that might need to respond to an incident in practice and procure support from experts in commercial suppliers (such as CREST CSIR and CESG/CPNI CIR scheme members).

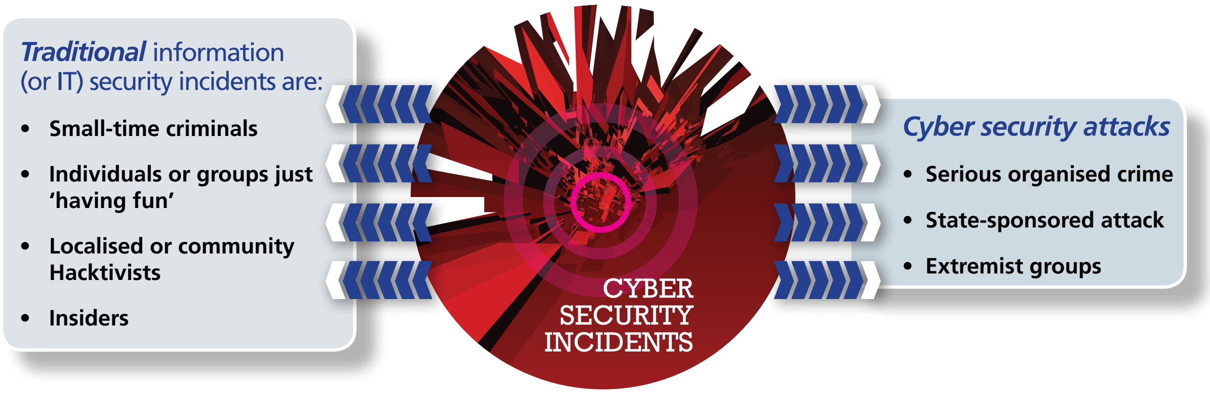
✓ More details about the CREST CSIR and CESG/CPNI CIR schemes can be found in ***Part 6 – Appoint a suitable supplier*** and at *crest-approved.org.*

## 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.

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 two most common (and somewhat polarised) sets of understanding – as shown in *Figure 1* 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***.



***Traditional*** information (or IT) security incidents are:

- **Small-time criminals**
- **Individuals or groups just 'having fun'**
- **Localised or community Hacktivists**
- **Insiders**

***Cyber security attacks***

- **Serious organised crime**
- **State-sponsored attack**
- **Extremist groups**

***Figure 1: Different types of cyber security incidents***

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.

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

## Responding to a cyber security incident

Dealing with cyber a security incident – particularly a sophisticated cyber security attack – can be a very difficult task, even for the most advanced organisations.

Furthermore, project research revealed that 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 (eg 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).

To deal with a cyber security incident quickly and effectively you will need to build an appropriate cyber security incident response ***capability***, which should include:

- Being suitably prepared for a cyber security incident, considering the implication for People, Process, Technology and Information
- A consistent, repeatable cyber security incident response process or ***methodology*** for handling cyber security incidents (or suspected incidents) as they occur, so that the appropriate actions are taken
- Mechanisms to ensure that cyber security incidents are properly followed up once they have been responded to effectively.

Creating an effective cyber security incident response capability involves several (sometimes major) decisions and actions, and your first considerations should be to:

- Create an organisation-specific definition of the term *"cyber security incident"* so that the scope of the term is clear
- Appoint a cyber security incident response team (internal and / or external) and determine what services they should provide
- Create appropriate cyber security incident response plans, policies, and procedures.

> ✓ 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).

## *The need for support from third party experts*

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 intrusion analysis, malware reverse engineering or forensic investigations; situational awareness; and advanced data analytics.

However, it is very difficult for them to identify trusted organisations that have access to competent, qualified experts, working for trusted organisations that can respond appropriately whilst protecting sensitive corporate and attack information.

> Chloe Smith, Minister for Cyber Security stated in August 2013:
> "We know that UK organisations are confronted with cyber threats that are growing in number and sophistication. The best defence for organisations is to have processes and measures in place to prevent attacks getting through, but we also have to recognise that there will be times when attacks do penetrate our systems and organisations want to know who they can reliably turn to for help.
>
> I am delighted to announce a unique Government-Industry partnership to tackle the effects of cyber incidents. This scheme and others like it, together with the '10 Steps to Cyber Security' guidance for business launched last year, are an important part of our effort to provide assistance to industry and government in order to protect UK interests in cyberspace."

CREST is the industry body that represents the technical security industry in this joint venture and has a proven track record of expertise in this field. Their scheme can cover the diverse needs of the UK economy from small to multinational businesses and local authorities to central government.

By relying on CREST to certify cyber incident response services suitable for the widest range of customers, GCHQ and CPNI can focus their expertise where it is really needed – the most sophisticated attacks.

✓ More details about these cyber security incident response schemes can be found later in this Guide in ***Step D*** of the ***Supplier Selection Process***.

Employing the services of properly qualified third party experts can significantly help organisations to handle cyber security incidents in a more effective and appropriate manner – particularly serious cyber security attacks.

Depending on the nature of the incident, a cyber security incident response organisation may offer a variety of services including incident management, intrusion analysis, log analysis, forensic imaging, malware analysis, reverse engineering, mitigation advice and general good practice guidance.

A range of response options is often available, ranging from telephone or email triage through to on-site assistance as required. Where such services are not available within the organisation, a reputable supplier of cyber security incident response expertise will know where and how to procure appropriate services from third parties.

## *Choosing a supplier*

There are several different approaches you can adopt when acquiring the services of an expert cyber security incident response expert, which include:

1. Employing one or more experts directly as part of your own team
2. Buying a complete monitoring and response service (possibly as part of an outsourcing decision)
3. Agreeing a particular response service in advance
4. Calling someone when you suffer an incident.

> "In some cases (particularly for less mature organisations) it can be better to just trust the supplier (ideally pre-agreed) to carry out the entire cyber security incident response, although ultimate responsibility always lies within the organisation"

If you decide to appoint a third party supplier to meet all or part of your requirements, it is important that you choose one who can most effectively meet your requirements – but at a reasonable cost. This raises many questions that you will need to answer, such as:

- What type of service do I need?
- How much service do I buy?
- When do I buy it?
- Who do I buy it from?
- What do I need to look for from a potential supplier?

To help you select a suitable supplier a systematic, structured process has been developed, as shown in *Figure 2* below.

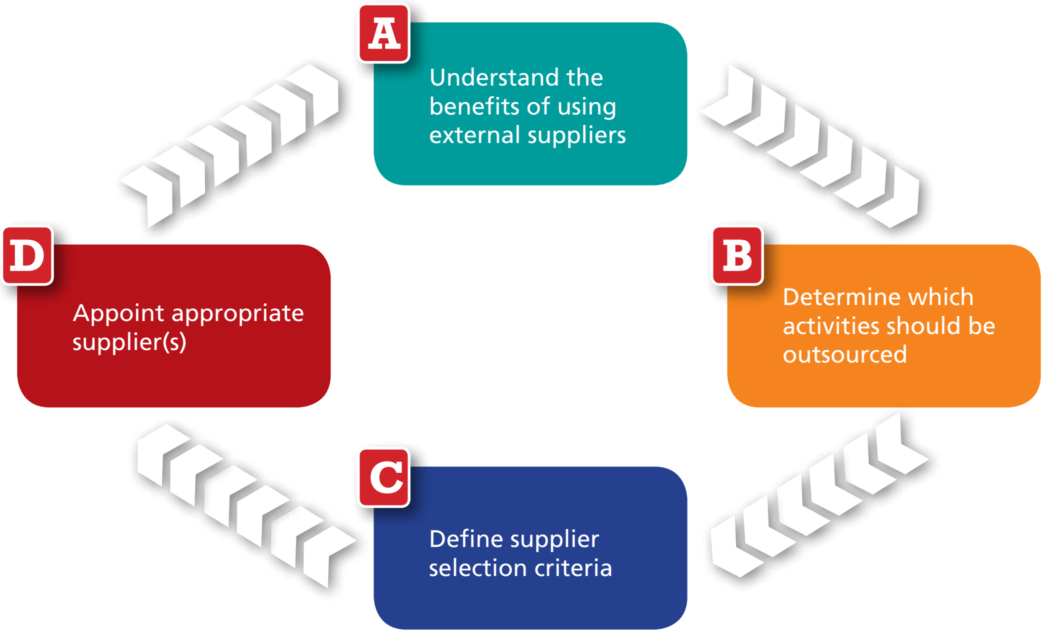

A
Understand the benefits of using external suppliers
B
Determine which activities should be outsourced
C
Define supplier selection criteria
D
Appoint appropriate supplier(s)

*Figure 2: The supplier selection process*

Each of the four steps in the process is described in detail in *Parts 3-6* of this Guide.

A

Understand the benefits of using external suppliers

## Summary of benefits

There are many benefits in outsourcing some or all of your cyber security incident response capability to external cyber security incident response experts.

Project research highlighted that the top three reasons (by some way) why organisations hire expert third party suppliers are shown in *Figure 3* below – and explained in more detail in the remainder of this section.

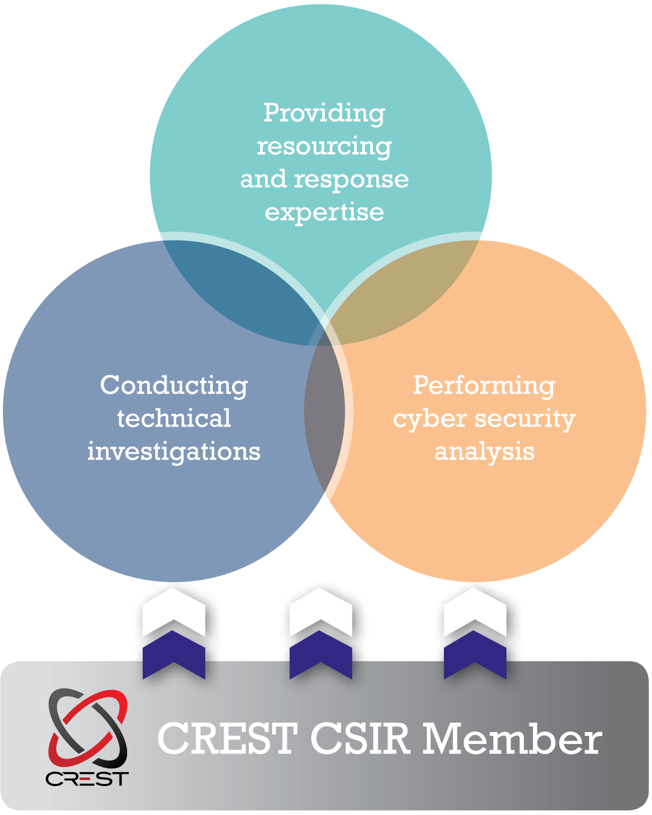

Providing resourcing and response expertise
Conducting technical investigations
Performing cyber security analysis
CREST
CREST CSIR Member

*Figure 3: Benefits of using external suppliers*

Organisations should use qualified experts in cyber security incident response, who are supported by trusted professional organisations, such as CREST CSIR and CESG/CPNI CIR scheme members.

You should procure cyber security incident response services from a trusted, certified external company who employ professional, ethical and highly technically competent individuals.  CREST cyber security incident response member companies are independently assessed and can provide you with a certified, trusted relationship, backed by an effective industry body.

## *Providing resourcing and response expertise*

Project research indicated that the two main benefits organisations believe they will gain from outsourcing ***resourcing and response*** activities to external cyber security incident response providers are in:

- Gaining access to more experienced, dedicated technical staff who understand how to carry out cyber sophisticated security incident investigations quickly and effectively
- Providing competent cyber security response capabilities to deal with unexpected (in their eyes) cyber security incidents.

Many organisations also strongly believed that resourcing and response benefits included external providers:

- Increasing the speed (often significantly) of dealing with a cyber security incident
- Undertaking short term engagements, eliminating the need to hire their own specialised (and often expensive) staff
- Applying the latest best practice in cyber security incident investigation and response
- Reducing the overall cost of cyber security incident response
- Adhering to a structured cyber security incident response process (or methodology) developed by experts.

✓ Another benefit can be the suppliers' experience in liaising with appropriate external bodies, such as CERTs; the government (eg CESG or CPNI); law enforcement; or regulatory bodies, such as the ICO (Information Commissioner's Office).

By appointing suitably qualified individuals working for trusted organisations (such as CREST CSIR and CESG/CPNI CIR scheme members), you will benefit from employing seasoned professionals with relevant in-depth experience of:

- Investigating sophisticated cyber security incidents
- Providing the appropriate tools and techniques to support the investigation
- Identifying what the perpetrator took – and how they got in
- Monitoring developments in cyber security attacks to know what to expect and how the attacker is likely to behave
- Remediating the problem effectively - ensuring that attackers are not alerted (thereby giving them a chance to act before sufficient blocking and other actions have taken place)
- Confirming that the remediation has been successful.

## *Conducting technical investigations*

Project research indicated that the main benefits organisations believe they will gain from outsourcing ***technical or specialist investigation*** activities to external cyber security incident response providers are in:

- Providing deep technical knowledge about the cyber security attack, including:
  - The different types of attacker (and how they operate)
  - Advanced persistent threats (APTs)
  - Methods of compromising systems
  - Sophisticated analysis of malware
- Obtaining their own data about a cyber security incident via independent means (eg via the use of packet tracing, taking a copy of the mail store and aggregated log analysis)
- Remediating the problem - effectively ensuring that attackers are not alerted (thereby giving them a chance to act before sufficient blocking and other actions have taken place)
- Performing expert deep-dive forensics
- Providing a report to their top management about the cyber security incident itself – and how they dealt with it – but also highlighting the potential business impact of such an attack.

Suppliers may need to perform correlation across multiple data sources, handle incidents at different locations – and be available at short notice. If the outsourcer is offsite, consider where the outsourcer is located, how quickly they can have an incident response team at any facility, and how much this will cost.

✓ There are a number of CREST cyber security incident response members that can provide qualified professional in a range of detailed technical investigation topics, such as ***registered intrusion analysts*** or ***certified experts*** in:

- Host-based malware analysis
- Network-based malware analysis
- Malware reverse engineering.

The CREST website (see *crest-approved.org* for more details) allows you to identify which organisations have the specific capabilities that you require.

## *Performing cyber security analysis*

Project research indicated that the three biggest benefits organisations believe they will gain from outsourcing ***cyber security analysis*** activities to external cyber security incident response providers are in:

- Monitoring emerging cyber threats (eg those associated with the move to IPV6 and with ubiquitous mobile devices) allowing them to be more pre-emptive to cyber security attacks, helping to reduce their likelihood and impact
- Applying modern analytic capabilities to aggregate relevant data from many different systems
- Providing situational awareness, particularly in the area of cyber intelligence (eg to help create a clear picture of their threat adversaries).

### *Advanced data analytics*

It can be a significant challenge for your organisation to analyse all the different data that relates (or may relate) to a cyber security incident, such as having to sift through many different firewall logs, liaise with cloud service providers and deal with Web 2.0 and 3.0 web traffic used in social networking. Some suppliers can provide cyber security analytical services, which may include:

- Situational awareness.
- Artificial intelligence, including clustering and 'lassooing'of data
- Coverage of both structured and unstructured data (ie 'big data')
- Monitoring of data in a way that enables visualisation.

✓ Some suppliers have tools that combine 'Big Data' analytics with event analysis and investigation capabilities.

## 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 organisations 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 significant 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 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.

## *Professional accreditation*

In some cases, professional services companies are accredited to incident response schemes, but do not use qualified individuals to conduct cyber security incident response services, so the required quality of cyber security incident response may not be achieved. In other cases, an individual may be qualified, but does not work for an accredited organisation, meaning that there are fewer assurances about the protection of confidential information or the overall quality of the service provided and any complaint may be difficult to resolve.

The optimum combination is shown in the green box in *Figure 4* below. This is the only combination that provides you with a tangible level of protection should things go wrong – and also reduces the likelihood of a problem occurring in the first place.

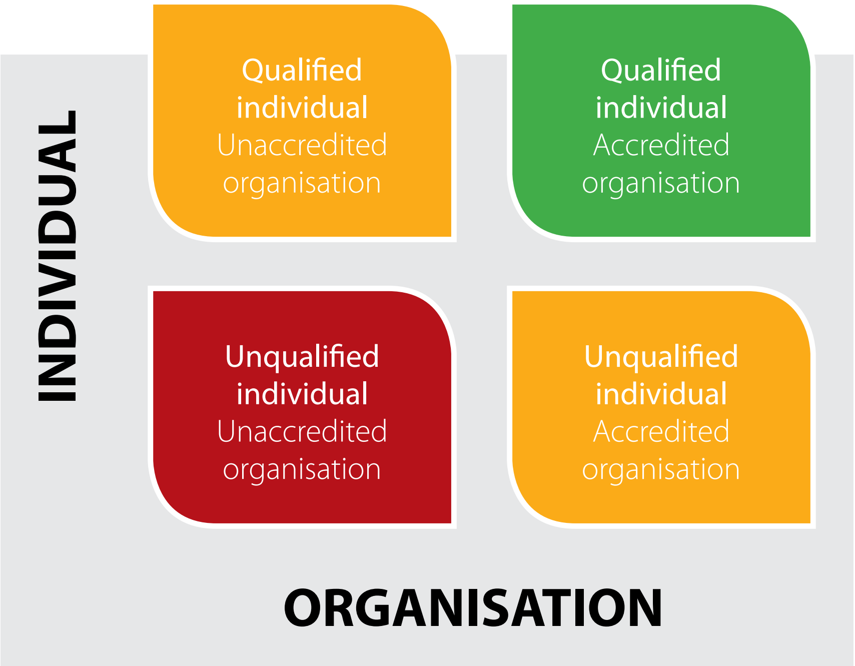

INDIVIDUAL
Qualified individual Unaccredited organisation
Qualified individual Accredited organisation
Unqualified individual Unaccredited organisation
Unqualified individual Accredited organisation
ORGANISATION

*Figure 4: Combinations of accreditation for organisations and the individuals they employ*

✓ Although value can be obtained by appointing either qualified individuals or accredited organisations, it is the combination of these that will provide you with the greatest assurance that the most effective tests will be conducted – and in the most professional manner.

Furthermore, by procuring cyber security incident response service services from qualified individuals who work for trusted organisations (as CESG/CPNI CIR and CREST CSIR schemes require), you can rest assured that an expert and independent body – with real authority – is on hand to investigate any complaint thoroughly and ensure that a satisfactory conclusion is reached.

"CREST provides demonstrable assurance of the processes and procedures of member organisations and validates the competence of information security investigators"

By using a supplier who is a CREST cyber security incident response member, you will also gain reassurance that:

- You are dealing with a ***trusted*** organisation in what is a very new area
- They have signed up to an independent code of conduct
- A proven cyber security incident response methodology will be adopted
- Their processes and procedures will have been subject to independent vetting
- Your systems and data will be handled carefully, in a professional manner
- The investigation itself we be kept confidential
- Advice will be given on how to reduce the likelihood of a similar incident from taking place.

## *Independent complaints process*

Appointing suppliers that are members of a professional cyber security incident response body can provide you with a reliable and proven complaint process (including constructive advice), as shown in *Figure 5* below.

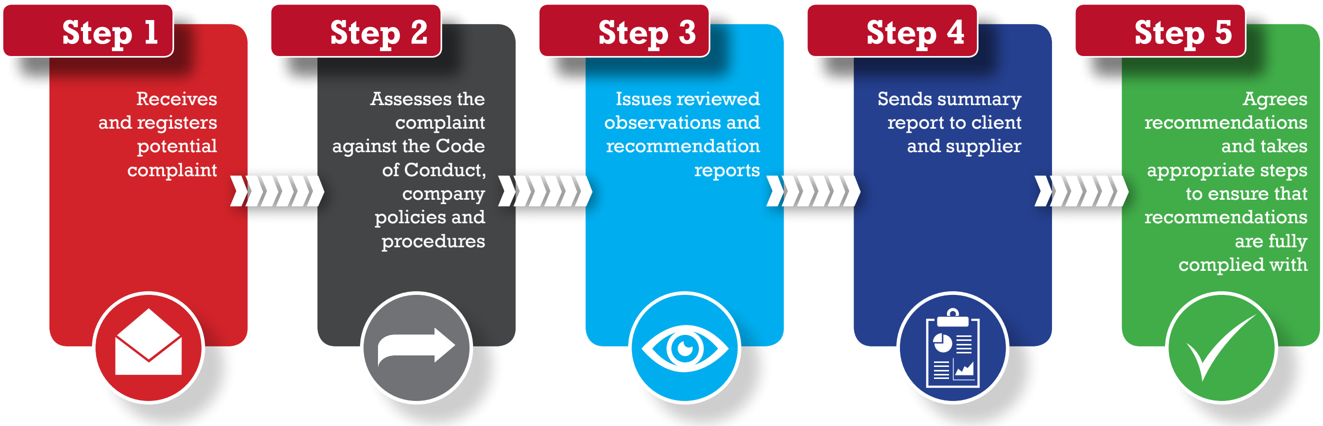

Step 1
Receives and registers potential complaint
Step 2
Assesses the complaint against the Code of Conduct, company policies and procedures
Step 3
Issues reviewed observations and recommendation reports
Step 4
Sends summary report to client and supplier
Step 5
Agrees recommendations and takes appropriate steps to ensure that recommendations are fully complied with

*Figure 5: Typical complaint handling process for a professional body*

If there are any problems with the quality of work done or the approach taken by the incident response team (including investigators, analysts and recovery experts) you can rest assured that an expert and independent body is on hand to investigate any complaint thoroughly and ensure that a satisfactory conclusion is reached.

A CREST CSIR member can expect to receive severe penalties if they do not:

- Adhere to the CREST Code of Conduct
- Act in a professional, ethical manner
- Ensure all their recovery team and ancillary staff comply with their submitted and reviewed policies, processes and procedures to protect client information.

They can have their membership of the scheme removed if they do not meet required standards or have proven in an investigation to have been significantly negligent or unethical. In the worst case, this could result in a significant reduction in business, as clients would not be prepared to procure their services.

**B** Determine which activities should be outsourced

## Define your objectives for cyber security incident response

The main objective of cyber security incident response is to respond to an incident effectively - and to restore your systems, networks and connectivity as soon as possible, enabling your organisation to get back to 'business as usual' as soon as possible. It is also important that exploited vulnerabilities are addressed to reduce the risk of subsequent attack.

Project research revealed that the main ***outcomes*** of cyber security incident response that organisations were looking for from their cyber security incident response capability were to:

- Protect the reputation of their organisation
- Protect confidential information
- Restore business services as soon as possible
- Limit the amount of financial loss
- Provide assurance to third parties that everything is under control
- Limit liabilities if things go wrong - or if there is a court case (ie take 'reasonable' precautions)
- Comply with legal and regulatory requirements (eg PCI / DSS, ISO 27001 or the ICO)
- Identify weaknesses in their cyber security controls
- Reduce the frequency and impact of future security incidents.

You will need to determine the main objectives for cyber security incident response in your organisation and ensure that these are well understood by key stakeholders. These objectives will help drive the outsourcing approach you decide to take.

## Review your cyber security incident response capability

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.

You should review your cyber security incident response capability to help determine requirements you have for outsourcing some or all of any associated services.

When reviewing your cyber security incident response capability, you should consider what you may need to do before, during and after a cyber security attack, as shown in *Figure 6* below.

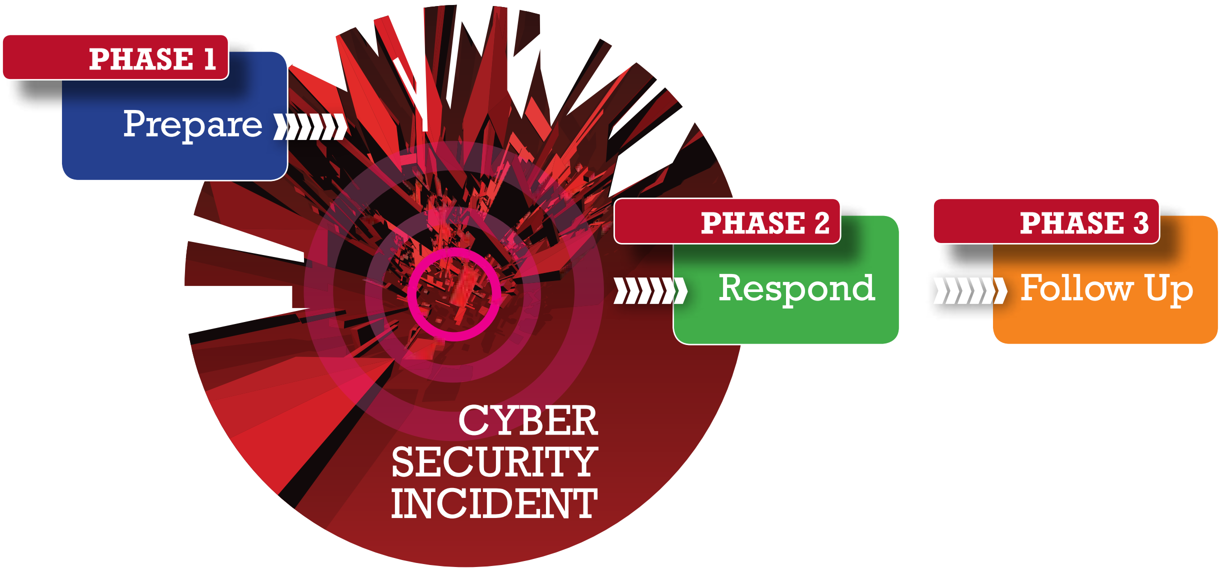


*Figure 6: A structured approach to cyber security incident response*

You should then examine the main steps associated with each phase in more detail. These are outlined in the table below, and described in detail in the ***CREST Cyber Security Incident Response Guide***.

| Phase | Main steps |
|---|---|
| Preparing for a cyber security incident | 1. Conduct a criticality assessment for your organisation<br>2. Carry out a cyber security threat analysis, supported by realistic scenarios and rehearsals<br>3. Consider the implications of people, process, technology and information<br>4. Create an appropriate control framework<br>5. Review your state of readiness in cyber security incident response. |
| Responding to a cyber security incident | 1. Identify cyber security incident<br>2. Define objectives and investigate situation<br>3. Take appropriate action<br>4. Recover systems, data and connectivity. |
| Following up a cyber security incident | 1. Investigate incident more thoroughly<br>2. Report incident to relevant stakeholders<br>3. Carry out a post incident review<br>4. Communicate and build on lessons learned<br>5. Update key information, controls and processes<br>6. Perform trend analysis. |

Furthermore, many organisations do not know their *state of readiness* to be able to respond to a cyber security incident in a fast, effective manner. To help determine your state of readiness, you should measure the maturity of your cyber security incident response capability, compare it with similar organisations (if possible) and put it in the context of your own requirements.

✓ Different types of organisation will require different levels of maturity in cyber security incident response. For example, a small company in the retail sector 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.

## Consider your need for outsourcing

Once you have reviewed (and refined) your cyber security incident response capability, you should now determine the cyber security incident response services you require and which of them you will consider outsourcing to expert suppliers.

When considering your outsourcing options, some of the initial questions to consider can include:

- Why do you need (or want) to outsource certain cyber security incident response services?
- What result do you expect those services to deliver?
- How quickly will you need suppliers to be able to respond?
- How much will it cost?

> "Organisations often know they can't build everything in-house, so we help them figure out what should be managed internally and what should be outsourced (eg first-response capability in-house, enterprise breach containment strategy development outsourced)."

Project research has revealed that there are very different levels of maturity in organisations when it comes to cyber security incident response, each of which may require a different level of support, be it internally or externally (or both). The type of services which external cyber security experts might provide to their clients is outlined in *Figure 7* below.

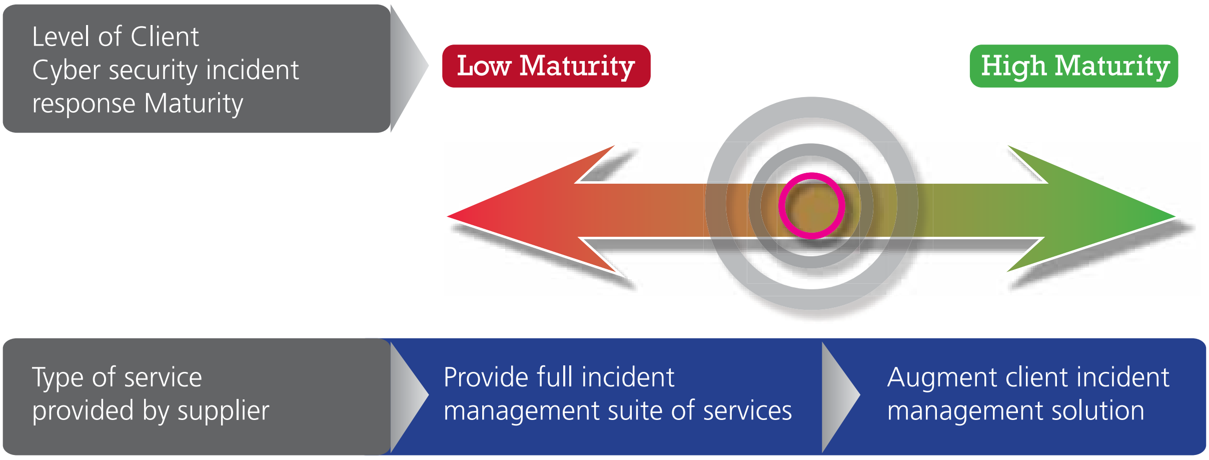


*Figure 7: Differing levels of maturity for cyber security incident response*

You will need to determine what is appropriate for your organisation, identifying which cyber security incident response services should be retained in-house (and maybe enhanced) and which should be outsourced to specialist third parties.

> "We know what we must retain in-house and where we definitely need help – it's all the middle ground that gives us a headache"

## Determine what should be retained in-house

You should determine which cyber security incident response activities need to (or must) be retained in-house. Reasons for this can include:

- The level of maturity of your cyber security incident response capability
- Availability of technical or other specialist expertise, such as intrusion analysis, malware reverse engineering or forensic investigation
- Desire to retain control of critical systems, processes or areas of the business
- Compliance with legal or regulatory obligations
- Requirements to protect the confidentiality of particular systems or information
- Direction set by corporate policy, politics or sensitivities.

Responsibility can never be outsourced: It is your organisation that is responsible for resolving an incident. Therefore, you should not outsource those parts of the cyber security incident handling process that give away complete control.

Project research revealed that the main parts of an investigation you should consider handling internally are:

- Defining what your assets are; how critical they are; where they are; and who is responsible for them
- Identifying the level of business impact associated with a cyber security incident
- Determining the scope of the investigation (but often with expert advice and guidance)
- Appointing  someone to act as a central point of contact
- Retaining control over the incident handling process, which may include:
  - Supervision of investigations and oversight of supplier's work
  - Maintenance of incident reports
  - Preservation of evidence
- Clear-up and return to business as usual (details will be better understood), including lessons learnt and on-going continuous improvement.

Many organisations also carry out the role of *'First responder'* themselves, dealing with all the initial activities prior to the more detailed investigation. This typically includes activities that are dependent on specific knowledge of your environment, such as ***Triage***, which covers:

- Prioritising cyber security incidents (eg high, medium or low priority)
- Classifying these incidents (eg critical, significant, minor or negligible)
- Appropriate assignment of responsibility for particular activities either to in-house specialists or nominated third party specialists.

You should also consider retaining many of the supporting elements of cyber security incident response, such as:

- Meeting data protection and other legal requirements (eg where the data is held, such as in a different country or jurisdiction)
- Accounting (dependent upon company type and size)
- Public relations (who to notify and when, any legal obligations to consider etc.).

Some organisations perform basic incident response work in-house and call on external experts to assist with handling sophisticated cyber security incidents.

## *Identify what you should consider outsourcing*

There are many tasks that you can consider outsourcing to third party experts, ranging from the provision of specialist support to performance of the entire investigation.

Project research revealed that the parts of the investigation that you should most consider outsourcing include:

- Carrying out the detailed technical investigation itself, helping you to detect, contain and eradicate the incident – and recover your services effectively
- Application of the latest best practice in cyber security incident response
- Analysis of: malware or other advanced persistent threat vectors; methods of compromising systems; and some types of deep-dive forensics
- Access to advanced technical tools and facilities (eg a tailor-made testing laboratory)
- Cyber security incident response service, for example to help validate that remediation was successful
- Methods of reducing the likelihood of the attacker regaining access to your systems.

You should also consider outsourcing specialist monitoring services, such as:

- Cyber situational awareness (environment analysis)
- Data analytics (including for 'big data', both structured and unstructured)
- Real-time monitoring of intrusion detection sensors, firewalls and other security devices
- Threat intelligence.

! You should think hard about giving an outsourcer authority to make operational decisions for the environment (eg disconnecting a web server) or providing them with access to particularly sensitive information. For example, your supplier may determine what user ID was used in an incident (eg ID 123456) but need not know what person is associated with the user ID.

A number of important preparatory or supplementary services can also be outsourced, such as

- Independent review of the 'state of readiness' of your cyber security incident response capability
- Training and awareness for you and your team
- Provision of expert advice and guidance
- Specialist support, such as handling trans-border evidence and dealing with cloud service providers.

Cyber security incident response is, by its very nature, a two-way street.  Due to the current global economic climate there is a great deal of cost-cutting taking place and consequently less surplus expertise in-house to deal with an attack.

However, the maturity of your organisation may result in some expertise being taken in-house to save costs. Furthermore, if you completely outsource your incident response capability you may still need to maintain basic incident response skills in-house, in case the outsourcer is unavailable.

> "Defining the scope of our requirements was key to our success"

## *Document your outsourcing requirements*

Once you have determined which cyber security incident response activities need to be retained in-house and which might be outsourced you should then produce a documented set of outsourcing requirements.

Your main requirement is likely to be for a supplier to be able to help you prepare for, respond to and follow up a cyber security incident quickly and effectively. They should be able to identify potential and actual cyber security incidents, contain them, eradicate the source and recover from them – using appropriate tools for the target environments.

The primary content of this requirements specification is the range of services that you would like the supplier(s) to provide.

However, you will also need to consider:

- The scope – and costs - of the services to be provided
- How the supplier will meet these requirements
- From which location services will be provided
- What response times are acceptable
- Roles and responsibilities.

The requirements specification should be reviewed and agreed by a range of appropriate stakeholders - and formally signed off by senior management. It can then be used to help produce a more formal RFP (Request for Proposal), or ITT (Invitation to Tender), to be sent to a short list of prospective suppliers – possibly through your procurement department.

However, your outsourcing requirements are unlikely to be complete at this stage as they are typically refined during your evaluation of potential suppliers of cyber security incident response services.

✓ Having documented your outsourcing requirements, you should be in a better position to be able to:

- Appoint suitable third party experts ahead of time
- Set your expectations, so that you are aware of what can and cannot be done with the time, resources and money available.

C

Define supplier selection criteria

## Determine what you require from a supplier

Once you have documented your outsourcing requirements you can now define a set of supplier selection criteria to help you appoint a suitable supplier who can meet – or exceed – your requirements.

✓ The supplier selection criteria will primarily be based on your outsourcing requirements. However, project research revealed that it is not just what you want a supplier to be able to do that is important, as most organisations also need a *reputable* commercial supplier who they can *trust*.

Your supplier of cyber security incident response expertise will need to understand your outsourcing requirements and have a clearly defined scope of the services being discovered, for example in terms of skills, approach and output. They should be able to develop a suitable approach to tackle your specific cyber security incident, backed up  by a consistent and repeatable response process, and help you initiate an effective remediation and improvement programme.

A reputable supplier will provide experts in cyber security incident response who:

- Are trained, proficient and professionally qualified in their specialist area
- Maintain an up-to-date, relevant understanding of your business and technical environment (which may be sector specific)
- Hold the necessary qualifications / permissions (eg security clearances) to work within relevant environments, both at your premises and at those of your suppliers or partners
- Have experience in responding to the type of cyber security incident you are most concerned about
- Conduct the investigation and response in a fast, effective and professional manner
- Bring in additional cyber specialisms, if required
- Collaborate with relevant third parties, such as law enforcement, CERTs and the Government.

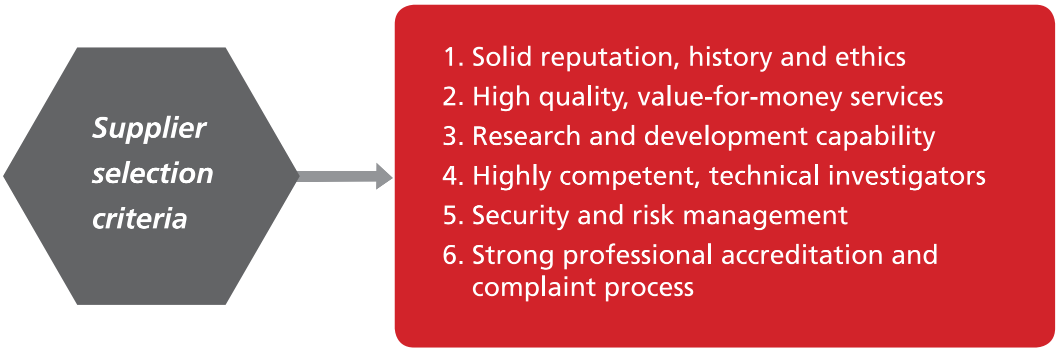
Suppliers should also be able to:

- Produce a contract, which includes the cyber security incident response activities they will perform; when; where; how; and by whom
- Comply with all legal / regulatory requirements
- Protect the security of your critical assets when conducting an investigation
- Manage the risks to your organisation when responding to a cyber security incident
- Have appropriate accreditations aligned to industry standards
- Provide appropriate cyber insurance and liability insurance.

## *Define supplier selection criteria*

There can be a big difference between a cheap cyber security incident response service and one that provides real value for money. For example, many low cost services may not provide certified, professional staff that can respond quickly and effectively to a range of sophisticated cyber security attacks or act in an ethical manner according to a defined code of conduct. Furthermore, there is typically little recourse in the event of a dispute (eg no independent adjudication and sometimes not even any indemnity insurance).

To ensure that your chosen supplier will meet your requirements it can be helpful to define a set of supplier criteria, which you can use to help evaluate the suitability of potential suppliers. The six main criteria identified during the research project are shown in *Figure 8* below.



*Supplier selection criteria*

1. Solid reputation, history and ethics
2. High quality, value-for-money services
3. Research and development capability
4. Highly competent, technical investigators
5. Security and risk management
6. Strong professional accreditation and complaint process

*Figure 8: Key selection criteria for choosing a suitable supplier*

Each of these criteria is outlined on the following pages together with examples of the types of questions you may wish to consider as part of the selection process.

✓ You should consider who is driving the relationship with the supplier within your organisation. It is seldom a good idea to just leave it to a corporate procurement person, as this is unlikely to deliver maximum value. From interviews with service providers, when clients have used a security or compliance person to drive the relationship, this has typically produced better results.

> "A good supplier helps to assure the process for an effective cyber security investigation without creating misunderstandings, misconceptions, or false expectations"

*Supplier selection criteria*

## 1. Solid reputation, history and ethics

| Typical questions to ask a potential supplier | Comments |
|---|---|
| a. Do you adhere to a formal code of conduct overseen by an independent industry body?<br>b. Can you provide evidence of a solid reputation, history and ethics (eg a full trading history; a reliable financial record; good feedback from both clients and suppliers; and a strong history of performance)?<br>c. Do you take part in specialised industry events or conferences (such as CRESTCON, 44con, the ISF Congress or the Cyber Security Summit)?<br>d. Are you able to demonstrate how you have successfully responded to cyber security incidents you have found in other similar environments – and any lessons learnt?<br>e. Can you provide independent feedback on the quality of work performed and conduct of staff involved? | A reputable supplier will have achieved suitable professional accreditation (such as the CREST CSIR or CESG/CPNI CIR schemes) and be a member of current, relevant professional and industry bodies.<br>Two of the most important criteria for a buyer of cyber security incident response services to consider are the reputation (and history) of the supplier and the ethical conduct they both adopt and enforce.<br>They will also have processes in place for agreeing scope and obtaining permissions for the type of work to be conducted; where it will take place; and what information and systems will be accessed. |

*Supplier selection criteria*

## 2. High quality, value-for-money cyber security incident response services

| Typical questions to ask a potential supplier | Comments |
|---|---|
| a. Can you show that you provide high quality services, (including the methodologies, tools, techniques and sources of information you will use) to conduct a fast and effective cyber security incident response investigation?<br>b. Can you describe your proven methods of providing cyber security response expertise; conducting technical investigations; and performing cyber security analysis?<br>c. How do you apply a rigorous cyber security incident response process, tailored for particular environments, to ensure that a wide range of cyber attacks can be successfully detected and contained; sources of the attack eradicated; and systems / networks recovered?<br>d. Can you demonstrate your organisations' cyber security incident response capabilities (eg by making a presentation; showing examples of similar (sanitised) investigations you have undertaken) and providing a sample summary / wash up report)?<br>e. Do you have independently reviewed quality and security assurance processes that apply to each investigation being undertaken, to help make sure client requirements are met in a secure, reliable manner? | Some suppliers will hit you with a volley of 'vendor hype' that can be difficult to penetrate. If a vendor cannot use language understood by the business during a tender process, it is likely to be much worse at a time of crisis.<br>A good supplier will help you to prepare for, respond to and follow up the cyber security incidents you are most concerned about. Therefore, their ability to demonstrate competence in the whole lifecycle is essential pre planning, through recovery, to clean-up.<br>Suppliers should be able to produce insightful, practical and easy to read reports, engaging with senior management in business terms, resolving issues with IT service providers, and addressing global risk management issues.<br>A quality supplier will not only deliver a highly effective cyber security incident response process, but can differentiate themselves by the quality of the customer services they offer, effectively providing a professional service wrapper around the service. They would also be able and willing to have their services independently reviewed. |

*Supplier selection criteria*

## 3. Research and development capability

| Typical questions to ask a potential supplier | Comments |
|---|---|
| a. Do you have an active, continuous and relevant research and development capability?<br>b. Have you produced research papers, published vulnerabilities or won awards in the industry?<br>c. Do you perform sufficient research and development to be able to prepare for, respond to and follow up the latest sophisticated cyber security attacks from differing types of attacker (eg state-sponsored, organised crime syndicates, extremist groups or insiders)?<br>d. How do you create specially tailored scenarios to test the effectiveness of your technical capabilities (eg for network and host intrusion analysis or malware reverse engineering)? | One of the biggest selling points for some suppliers is the quality and depth of their technical research and development (R&D) capability. It is important that a supplier has a research capability to keep up-to-date with both common and new attack profiles.<br>Some suppliers will constantly develop specific methodologies to address different types of attacks – and attackers. The manner in which they publicise these will provide an indication of their approach to responsible reporting.<br>A good technically competent supplier is likely to maintain up-to-date specialist monitoring services, including:<br>• Cyber situational awareness (environment analysis)<br>• Data analytics (including for “big data”, both structured and unstructured)<br>• Real-time monitoring of intrusion detection sensors, firewalls and other security devices<br>• Threat intelligence.<br>Your organisation needs to assess it’s own cyber security incident response capability and compare it with suppliers. |

Supplier selection criteria

## 4. Highly competent, technical cyber security incident response experts

| Typical questions to ask a potential supplier | Comments |
|---|---|
| a. How will you:<br>• Define the scope of the investigation?<br>• Manage the cyber security incident response process?<br>b. What qualifications do your cyber security incident response experts hold in the various areas in which investigations may be required (such as incident response, intrusion analysis or forensics)?<br>c. How do your investigators identify the 'root cause' of cyber security incidents; strategically analyse findings in business terms; prevent attackers from regaining access to target systems; help develop security improvement strategies; and recommend countermeasures to both remediate cyber security incidents and prevent them recurring?<br>d. Can you specify: named individuals who will be responsible for managing and conducting the investigation; their experience of the environment within the scope; their qualifications; and the exact role each individual will perform?<br>e. If you intend to work in collaboration with other parties, how do you validate their experience and ensure that they adhere to professional policies, process and procedures? | It may be difficult to find a single supplier who can meet all your requirements, so they may need to outsource or partner for some areas of service. You will need to have confidence that they will look after your data; adhere to company policies, procedures and processes; and be backed by codes of conduct.<br>The manager of the service you will procure is essential to the overall recovery. The cyber security incident response manager can be key to an effective investigation and would often be directly employed by the service provider.<br>The cyber security incident response experts used by your supplier should have deep, technical capabilities in the specific areas that are relevant to your target environment. It is also important that they analyse root causes of incidents to prevent weaknesses being re-exploited.<br>***"Put the right people from the right organisation on the right job at the right time"***<br>There can be significant temptation to jump straight into investigation and recovery. But a good quality supplier will ensure that the objectives and scope of the investigation, recovery and clean-up phases are defined during an accelerated project management process.<br>It is essential that suitably skilled, knowledgeable and competent people are employed in the recovery team. Quality organisations invest in the development and recognition of their staff and put them forward for industry recognised qualifications, such as those provided by CREST. Any company procuring services in this area should understand what these qualifications mean.<br>See www.crest-approved.org for more details. |

*Supplier selection criteria*

## 5. Security and risk management

| Typical questions to ask a potential supplier | Comments |
|---|---|
| a. Do you apply independently validated security and risk management controls over the cyber security incident response process, all relevant people involved, key aspects of target systems and any client data affected?<br>b. Are you able to demonstrate how you can ensure that all relevant evidence is properly gathered and preserved when conducting an investigation?<br>c. Can you provide written assurances that the security and risks associated with our critical systems and confidential information (together with any other business risks) will be adequately addressed – and compliance requirements met?<br>d. How do you ensure that results of investigations are generated, reported, stored, communicated or destroyed in a manner that meets incident management compliance requirements, but does not put the organisation at risk? | It is important that the supplier themself operates in a secure manner – and has a positive approach to both security and risk. Your supplier should be able to provide assurances – preferably in writing – that the security and risks associated with your critical systems and confidential information (together with any other business risks) are being adequately addressed in line with recognised security-related standards, such as ISO 27001.<br>During any cyber security incident response investigation it is likely that the response team will encounter sensitive or business critical data. You will need to be comfortable that you can trust both the supplier, and every individual who is part of the investigation team, not to disclose this information. Sensitive data is likely to be obtained and analysed during the investigation, so the supplier must be able to demonstrate how they will protect this material during and after incident response activities. |

*Supplier selection criteria*

## 6. Strong professional accreditation and complaint process

| Typical questions to ask a potential supplier | Comments |
|---|---|
| a. Does your organisation hold strong professional accreditation, and is it a member of the CESG/ CPNI CIR or CREST CSIR schemes?<br>b. Does your organisation provide a wealth of experience drawn from client work across a range of companies and sectors, allowing lessons learnt from one to be transferred to others?<br>c. Can you outline the problem reporting and escalation processes that you adopt should there be a problem with the cyber security incident response service?<br>d. Is your organisation supported by a constructive, expert complaint process, with sufficient independence and authority to resolve issues? | Suppliers of cyber security incident response services who have been professionally accredited will provide you with confidence that major cyber security attacks have been identified and properly resolved.<br>The CESG/CPNI CIR and CREST CSIR schemes require organisations to demonstrate that they have appropriate processes, procedures, governance, qualifications, skills and experience to provide effective incident response for a significant proportion of cyber security incidents. Should anything go wrong during the relationship with the supplier(s) you must be able to make a complaint and know that this will be acted upon. The CREST codes of conduct are linked to the member companies' complaint process. These codes of conduct are meaningful, enforceable and have real 'teeth' in ensuring that any recommendations are implemented. |

The company assessment process for approval to join the CREST CSIR scheme has already obtained answers to and received accreditation for all the criteria described in this section. This means that CREST CSIR scheme members should be able to answer these questions easily and would already have been independently assessed against them.

D

Appoint appropriate supplier(s)

## Identify potential suppliers

Once you have created an appropriate set of supplier selection criteria the next stage is to identify a short list of possible suppliers and evaluate how well they can meet your criteria. These suppliers should fully understand your approach to cyber security incident response including preparation, response and follow up – and be able to tailor services accordingly.

However, it can often be difficult to produce a short list of potential suppliers, not least because there are so many to choose from. For example, cyber security incident response suppliers can include:

- Organisations specialising in traditional incident response (often small boutique firms)
- Information security consultancies and integrators, with cyber security incident response teams
- Specialised systems integrators and outsourcing service providers with cyber security incident response teams
- Regulated professional services firms, including the 'Big 4' accountancy and audit firms, with cyber security incident response teams.

A number of suppliers provide a wide range of other related services. They can effectively provide a one-stop shop for their clients by helping them to monitor threats and systems; implement suitable controls; investigate and safely remediate cyber security attacks and incidents; and reduce the risk of similar incidents happening again in the future.

✓ Some speciality organisations focus on targeted cyber security attacks on an organisation's systems or networks. These are often nation-sponsored attacks that are looking to obtain confidential information or intellectual property. Smaller, specialised organisations can often handle simple incidents like a virus attack, but would not have the breadth and depth of experience required to effectively handle sophisticated cyber security attacks in the way that specialists can.

> "What we are looking for from a supplier is certainty, prioritisation, trust and security"

## Get a recommendation or reference

If you have colleagues or industry peers you can trust, seek out their advice and ask them to recommend a suitable supplier. You should talk to the referee directly and ask them questions like:

- Do you still use this supplier?
- How long have you been using them?
- Would you consider changing?
- What are their strengths?
- What are their weaknesses?

✓ Make sure the referee has actually used the supplier they are recommending, and acquired a service similar to the one you require – for the same type of target environment.

## Review Cyber Security Incident Response schemes

Two schemes that provide access to industry expertise to respond effectively to the consequences of cyber security attacks were formally launched in August 2013 by CESG, the Information Security arm of GCHQ and the Centre for the Protection of National Infrastructure (CPNI), in collaboration with CREST, the professional body representing the technical security industry.

The Cyber Incident Response schemes follow on from the successful pilot conducted by CESG and CPNI, funded by the National Cyber Security Programme. The new CESG scheme will provide a list of government assured, certified providers of response and clean up services in the event of a cyber security attack.

The pilot concluded that the objectives of the National Cyber Security Strategy in providing greater resilience to CNI companies as well as wider public and private sector organisations can be best met by adopting a complementary twin track approach for certified Cyber Incident Response services:

- A broadly based scheme led by CREST and endorsed by GCHQ and CPNI, which focuses on appropriate standards for incident response aligned to demand from all sectors of industry, the wider public sector and academia.
- A small and focused Government run Cyber Incident Response scheme certified by GCHQ and CPNI responding to sophisticated, targeted 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 include phased introduction of mandated professional qualifications for *Cyber Security Incident Response Managers*.

### Industry-led certification

CREST has worked with industry and government to define standards that companies providing Cyber Security Incident Response (CSIR) services should have in place to protect client information. CREST will assess the service providers against these standards and ensure compliance through codes of conduct. Combined with professional qualifications for individuals, this will provide the buying community with confidence in the integrity and competence of the companies they are employing. These standards and requirements have been reviewed and endorsed by CESG and CPNI.

✓ A summary of the requirements for company membership to the CREST scheme are outlined in ***Appendix A*** with full details being available from CREST on request.

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.

✓ The role of an effective Cyber Security Incident Manager is often crucial as they can:

- Quickly and accurately identify the type of cyber security incident you are experiencing
- Determine what actions need to be taken
- Establish the structure and skills required from the incident response team
- Identify where to go to obtain the appropriate specialist support
- Oversee all aspects of the entire cyber security incident response investigation
- Act as an interface to senior management.

## *Evaluate services provided by potential suppliers*

It is often important to validate the credentials of the suppliers you wish to consider. You should review the services they provide and make sure they can deliver what you specifically require from an expert supplier, as well as any generic supplier selection criteria.

Many cyber security incident response services on the market can be very expensive to implement, maintain and manage and don't scale down to smaller consumer environments.

As part of the evaluation process, you should consider asking your potential suppliers to:

- Make a presentation of their capabilities
- Show examples of similar (sanitised) cyber security incident response investigations they have undertaken
- Demonstrate an effective methodology.

The individual performing the investigation and remediation of a cyber security incident must not carry out actions beyond the agreed scope: to do so would be unethical – and, in some cases, illegal.

Consequently, a great deal of trust will be placed in the individual investigator that you employ. To reduce this risk, you can:

- Check the professional certifications of a sample of the incident response team (eg investigators, analysts and recovery experts) – and their depth of experience
- Examine background checks suppliers perform on their employees - and validate a sample -for example to identify criminals, ex-hackers or other potentially unsuitable individuals
- Review the track record of the investigation team to see who they have worked with and in what capacity
- Exercise your right to reject particular individuals.

CVs of individual investigators, analysts and recovery experts, as well as confirmation of their qualifications, can be sent to you upon request – another way of highlighting their competence. However, this can be a double-edged sword as the supplier may have to provide alternative experts if named individuals are otherwise engaged.

## *Obtain formal written confirmation of supplier capability*

You may wish to produce a specific set of questions that a short list of suppliers will need to respond to in writing, possibly as part of a scope statement – and make sure they either meet or exceed requirements. If you require a more comprehensive service, you should consider including these questions in a formal *Request for Proposal* (RFP) or *Invitation to Tender* (ITT).

## *Review CREST cyber security incident response service provider requirements*

You should check to see that a supplier provides the necessary range of services needed to carry out the specific cyber security incident response service you require, either directly or through formally defined partnerships or collaboration.  CREST has produced a set of requirements that you can review to help you achieve this.

You should find out if the supplier has a documented policy, procedure, process or contract in place (or a combination of these, as required) addressing important areas of your outsourcing requirements specification, such as:

- ***Assignment –*** (eg signing NDAs prior to commencing work; gaining permission to access information or assets; ensuring awareness of any legal/regulatory compliance; establishing the skill, knowledge and competence requirements of the incident response team; and considering the potential objectives of the assignment)
- ***Presentation –*** (eg assigning communication and data delivery; gathering and storing information about the nature and extent of the incident, ownership of assets, sources of log data, software topology and evidential sources; agreeing the objectives, initial scope and limitations of the assignment; and stating details in the contract about software and processes to be used)
- ***Identification –*** (eg determining their capability to execute the assignment successfully;  performing analysis of host assets, network data and key files (eg malware); approaching unusual/novel problems; gaining authorisation from third parties; prioritising assets to be investigated; and a description of their tool selection method)
- ***Containment –*** (eg determining immediate actions; ensuring that they are safe to enact; minimising the risk that attacker will respond/escalate; determining whether a finding is critical; and reacting to critical findings during the investigation)
- ***Eradication –*** (eg determining remediation actions to remove the attack from the network; checking for any response from the attacker; identifying a response if the attacker uses different attack methods; ensuring that the network is secure; and other methods of validating success)
- ***Asset/Information/Document Storage, Retention and Destruction –*** (eg defining the documents/assets/information to be collected; stating how they will be recorded, protected, returned and/or destroyed; protecting personal information identified during the assignment; performing actions required to prevent a breach of relevant laws; detailing how information will be removed, archived and protected)
- ***Reporting –*** (eg presenting key sections in their client report; facilitating a formal post incident management meeting with key personnel; reporting key findings; communicating lessons learnt; and achieving suitable sign-off from your organisation)

## *Consider Scenario-based assessment*

If you represent a particularly large organisation – or have significant cyber security incident response requirements – you could ask potential suppliers to take part in a ‘dry run’ test, conducted with several other suppliers, based around fictitious, but real-world, scenarios. This might involve asking a range of different vendors to:

- Respond to a mock-up of a cyber security incident on a test system that has been attacked in a variety of ways
- Demonstrate how they would detect cyber security incidents, contain them, eradicate the source and recover systems effectively
- Show how they would help prevent an attacker from re-gaining unauthorised access
- Write up their findings in a suitable manner, so that you can understand the nature and content of their approach.

## *Appoint and monitor selected supplier*

After carefully considering all the relevant supplier selection criteria – and evaluating potential suppliers - you will then need to formally appoint one or more suppliers. The key consideration should still be to appoint a supplier who can help you meet your specific requirements – at the right price - not just one who can offer a variety of often impressive products and services, some of which may not necessarily be relevant.

✓ Large organisations may also choose to invite competitive tenders from a number of different cyber security incident response providers to be on a 'call-off' contract framework. They then call off work against it, perhaps re-tendering the providers on the framework for larger cyber security incident response services.

There may be other considerations when selecting a supplier. For example, your organisation may have a well-established (or preferential) relationship with a particular supplier or a need to appoint (or reject) an organisation for commercial or political reasons.

Furthermore, your requirements can be influenced by:

- The size (and bargaining power) of your organisation and the market sectors in which it operates
- Political, legal/regulatory, economic, social and technological (PLEST) issues.

### *Manage your expectations*

You should be aware of what to expect from your supplier, which will differ dependent upon the type of cyber security incidents covered and the level of service required. You should agree likely costs, in terms of typical day rates and level of support required to deal with a range of incidents (noting that this varies to a large degree following detailed scoping of each individual cyber security incident response service). This will help organisations assign a contingency or budget item in advance – reducing the potential financial impact should an incident occur.

> "We have to help set the expectations for many of our clients, so that they are aware of what can and cannot be done with the time, resources and money available"

✓ By appointing an appropriately qualified CREST member, you can be assured that services will be provided in a professional, competent manner – even at the last minute – ensuring that key systems and data are suitably protected.

Furthermore, you will also have access to an independent complaints process if you are not happy with services provided.

## *Ensure contractual requirements are met*

Prior to work starting, arrangements with your chosen supplier should be clearly defined in a detailed contract that has been signed off by authorised individuals in both parties.

Contract management, both operational and financial, can be critical in dealing with any supplier irrespective of what stage you make the appointment. For cyber security incident response services, the importance of the operational side of controlling your supplier is not always given sufficient priority. Whilst the costs may be managed by the finance department, you are also responsible for ensuring they deliver what you have agreed.

When assessing any possible contractual implications, you should consider:

- Both the content of the contract itself and any underlying service level agreements (SLA).
- How to handle any breach of the contract
- What action you will need to take if the outsourcer is not available or does not meet requirements.

If you do not have an agreement in place prior to a cyber security incident occurring, you may need to sign an interim agreement, which is not likely to:

- Deliver the same value-for-money than a pre-arranged contract
- Guarantee that an appropriate, qualified expert is available to carry out the investigation
- Give you assurance that the incident will be resolved effectively
- Ensure that compliance requirements are met, confidential data is adequately protected, and critical systems are restored quickly and effectively.

Furthermore, you will need to ensure that a more appropriate contract is signed either during the investigation (if possible), or as soon as possible after the event.

> "We are so pleased we had a signed contract with our supplier BEFORE we were hit by a cyber security incident."

When handling a cyber security incident, it is essential that the supplier you appoint has a suitable framework of people, processes, technology and information to meet your requirements.

CREST have developed the following set of questions (based around 7 key elements of a *Cyber Security Incident Response Framework*) that you should consider asking your suppliers to respond to when determining their suitability.

## Assignment

Does the supplier have a documented policy or procedure in place for:

1. Signing NDAs prior to commencing work?
2. Gaining permission to access information or assets as required for the performance of the service – and for validating the authority of the permissions given?
3. Ensuring that the client is aware of any legal/regulatory compliance related to the assignment?
4. Establishing and documenting the skill, knowledge and competence requirements of the incident response team for the assignment, including their qualifications (eg. CREST qualification, forensics/evidence, etc.)?
5. Considering the potential objectives of the assignment (eg to stop infection, take legal action, monitor to identify source of attack to ensure the correct team construct and processes are applied. (It is recognised that this may change during the life of the assignment and should be managed under change control)?

## Presentation

Does the supplier have a documented policy or procedure in place for:

1. Agreeing a method of assignment communication and data delivery with the client?
2. Gathering and storing information on first contact with the client covering:
   - The known nature of the incident?
   - The known extent of the incident?
   - Ownership of known affected assets?
   - Sources and coverage of known log data?
   - Topology of software applications and connected third parties?
   - Available evidential sources (network traffic captures, logs)?
   - An understanding of the client's existing capability?
   - Agreeing the objectives, initial scope and limit of the assignment with the client?
   - Communicating the details and objective of the assignment to the incident team?
   - Agreeing the objectives, initial scope and limit of the assignment with the client?
3. Agreeing and documenting changes in the scope of the assignment to the client and incident team?

Does the supplier have a clear statement in the client contract:

1. Detailing the incident response software to be used?
2. Verifying that the software has been validated as being free from malicious software?
3. Defining processes to prevent the targets being further infected with malicious software originating from the original attack?

## *Identification*

Does the supplier have a:

1. Policy or procedure for determining their capability to execute the assignment successfully and therefore to bid or not bid for the assignment?
2. Process for analysis of:
   - Host Assets?
   - Network Data?
   - Key files (eg. malware)?
3. Suitable approach to unusual/novel problems, (eg. bespoke file types, encryption)?
4. Process for gaining authorisation from third parties as part of the investigation?
5. Policy or procedure for:
   - Guiding clients through the provision of required information at the commencement of the assignment?
   - Prioritising assets to be investigated?
6. Description of their tool selection method (eg. hard/mechanical, soft/intellectual)?

## *Containment*

Does the supplier have a process:

1. For determining immediate actions (eg. high risk assets, time dependant issues, business/commercial issues), ensuring that they are safe to enact, have minimum risk that attacker will respond/escalate and communicating this to the client?
2. During investigations for determining whether a finding is critical?
3. For reacting to critical findings during the investigation?

## *Eradication*

Does the supplier have:

1. A process for determining remediation actions to remove the attack from the network?
2. A method to:
   - Check for any response from the attacker?
   - Identify a response if the attacker uses a different method such that signatures will not be effective?
   - Allow sufficient time to ensure that the network is secure and that there is no response?
3. Other methods of validating the success of eradication?

## Asset Management

Does the supplier have:

1. A definition of the documents/assets/information to be collected from the client and a clear statement of how this will be recorded, protected, returned and/or destroyed?
2. A clear statement in the client contract:
   - On the implications of the protection personal information identified during the assignment (for example Data Protection Act 1988 and the Human Rights Act Article 8 "The right to respect for private and family life" and actions required to prevent a breach of either of the Acts)?
   - On the implications of the Computer Misuse Act 1990 (and equivalents) and actions required to prevent a breach of the Act?
   - Detailing how information will be removed and archived from both the reporting environments and the attacked platforms?
   - Detailing the protection applied to the archived information?

## Reporting

1. Do they request a formal post incident management meeting with the client?
2. What do they propose as:
   - The structure of the post incident management client meeting?
   - Reporting topics to be covered in the post incident management client meeting?
3. How do they:
   - Communicate lessons learnt to your (cyber security) incident team?
   - Ensure all relevant media is returned to the client?
   - Destroy all information pertaining to the incident held by the supplier?
   - Achieve a suitable sign-off from your organisation?

## Notes

# 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<br>• Validation of the competence of technical security staff<br>• On-going professional development for those entering or progressing in the industry<br>• 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<br>• 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<br>• Cyber Security Incident Response (CSIR) Scheme, complementing the CESG/CPNI Cyber Incident Response (CIR) Scheme<br>• 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<br>• 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<br>• 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