IP Wales

Protecting your ideas

IP Community Guide to SMEs Outsourcing Cybersecurity Incident Response & Data Recovery Activities

Building a cybersecurity incident response capability

The National Cybersecurity Centre (NCSC) has made it clear that, whatever their level of cyber protection client, all firms can now expect to experience a cybersecurity incident at some stage and, ”*investment in establishing effective incident management policies and processes will help to improve resilience, support continuity, improve customer and stakeholder confidence and potentially reduce any impact*.” - According to a UK government report published in 2016, many smaller businesses experience breaches of once a month or more.

There are different types of cybersecurity incidents ranging from traditional IT security incidents initiated by small-time criminals, groups or individuals ‘having fun’, Hacktivists and insiders to more advanced persistent threats (APTs) emanating from serious organised crime, state-sponsored attackers and extremist groups - noting more serious cybersecurity attacks often “don’t have an end”.

Planning a cybersecurity incident response capability requires good preparation and a comprehensive review of the state of readiness for the client business. Under the CREST[1] Cybersecurity Incident Response Guide[2] firms are advised to first assess their maturity in respect of preparedness, responsiveness and follow-up capabilities. Undertaking this assessment enables client firms to identify gaps in their capabilities and specify required improvements e.g.

- Preparedness - has the organisation carried out a criticality review (looked at its data estate and identified/prioritised trade secret data), conducted realistic cybersecurity threat analysis, considered the implications for people/processes/technologies/information, created an appropriate control framework, reviewed their overall state of readiness;

- Responsiveness - has the organisation the ability to identify cybersecurity incidents, conduct investigations, take appropriate and proportionate actions, recover systems/data/connectivity;

- Follow-up - can the organisation undertake ‘deep-dive’ investigations of a cybersecurity incident, report to relevant stakeholders effectively, conduct post

[1] CREST is the not-for-profit accreditation and certification body representing the technical information security industry offering internationally recognised accreditation for organisations and individuals providing penetration testing, cyber incident response and threat intelligence services.

[2] *“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 cybersecurity incidents. The research project complements the work done by the UK Government on cybersecurity incident response...”*

incident reviews, build on lessons learned, update key information/controls/processes, conduct future trend analysis.

Contracting the services of third party experts can significantly help client firms to handle cybersecurity incidents in a more effective and appropriate way, especially APTs. Depending upon the nature of the cybersecurity incident external suppliers can offer support with intrusion analysis, log analysis, forensic imaging, malware analysis, reverse engineering and mitigation advice. Such support can be offered at arms-length (via telephone/email) or on-site and offered on a 24hrs basis.

Client firms may look to outsource the entirety of their cybersecurity incident response management, given that for smaller firms this will provide resources and response expertise, the ability to conduct comprehensive technical investigations and perform in-depth cybersecurity analysis. However, the responsibility for resolving a cybersecurity incident cannot be outsourced and corporate risk management dictates there are benefits for the client firm in retaining basic incident response skills in-house. The maturity of the client firm may well therefore result in some of the expertise being taken in-house to save costs.

Determine the activities to be outsourced

CREST project research reveals that the three main challenges organisations face when responding to a cybersecurity 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, how they did it and why they did it
- Identifying what systems, networks, data has been compromised.

In terms of response, each incident will necessitate a proportionate response – overreacting can be detrimental.

Previously designated personnel should:

- Verify the breach and work to contain and then eradicate it.
- Confirm the extent of the breach and the data/services which have been affected.
- Identify the risks arising to the business and others from the breach
- Conduct a detailed post-mortem review including lessons learned exercise.

CREST project research reveals the main aspects of a cybersecurity incident investigation to be **handled internally** include:

- Reviewing the data estate and identifying/prioritising trade secret data
- Identifying the level of business impact associated with a cybersecurity 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 an external supplier's work
    - Maintenance of incident reports
    - Preservation of evidence

- Clear-up and return to business as usual (details of which are better understood by the business itself), including lessons learnt and on-going continuous improvement. The risk of litigation to the client business arising from the cybersecurity breach will also need to be assessed.

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 dependent on specific knowledge of the business:

- Prioritising cybersecurity incidents (e.g. high, medium or low priority)

- Classifying these incidents (e.g. critical, significant, negligible)

- Appropriate assignment of responsibility for particular activities either to in-house specialists or nominated external suppliers.

The U.S. Department of Commerce notes that for many organisations the most challenging part of the incident response process is accurately detecting and assessing possible incidents (determining whether an incident has occurred or still is occurring and, if so, the type, extent, and magnitude of the problem). Signs of an incident fall into two categories: precursors and indicators – a *precursor* is a sign that an incident may occur in the near future, whereas an *indicator* is a sign that an incident has or still is occurring. Once an incident has been detected all the facts regarding the incident need to be recorded – not only to help resolve the incident but also to assist in any potential future legal proceedings[3]. Prioritising the incident is a critical decision point in the process with the relevant factors being functional and/or information impact on the business and recoverability i.e. an incident with high impact but low effort to recover from is an ideal candidate for immediate action.

Client firms need also to consider retaining many of the supporting elements of cybersecurity incident response, such as:

- Meeting data protection and other legal requirements (e.g. where the data is held in a different country or legal jurisdiction)

- Accounting (dependent upon company type and size)

- Public relations (who to notify and when, any legal obligations to consider etc.). In addition to keeping other members of the business apprised (ensuring media dialogue is co-ordinated through one person/team operating under legal advice), relevant parties who may need to be informed include the Police/Action Fraud; Banks/Credit Card Companies; Regulators (note the 72hr reporting deadline under GDPR 2018)/Insurers (SRA in the case of Solicitors) and potentially 'Data Subjects".

[3] U.S. National Institute of Standards and Technology (INST) Special Publication 800-86 provides detailed information on *Forensic Techniques into Incident Response*

The main aspects of a cybersecurity incident investigation revealed to be often **handled externally** include:

- Carrying out the detailed technical investigation itself, helping the client firm to detect, contain and eradicate the cybersecurity incident

- Access to advanced technical tools and facilities (e.g. a tailor-made testing laboratory)

- Carry out an appropriate recovery plan confirming that the remediation has been successful and reconnecting networks, rebuilding systems using ‘clean sources’, restoring/recreating or correcting data and testing systems

- Methods of reducing the likelihood of the attacker regaining access to systems.

Client firms should also consider outsourcing specialist monitoring services, such as:

- Real-time monitoring of intrusion detection sensors, firewalls and other security devices

- Threat intelligence.

When outsourcing Client firms will need to consider whether they should provide external suppliers with legal authority to make operational decisions (e.g. disconnecting a web server) and/or allowing them access to particularly sensitive information (e.g. trade secret data) – requiring a Non-Disclosure Agreement (NDA) to be signed by the External Supplier.

Once a client firm has determined which cybersecurity incident response activities need to be outsourced it should then produce a documented set of outsourcing requirements in respect of assignments, presentations, identifications, containment, eradication, storage/retention/destruction, reporting.

These requirements will set the specification for the range of services an external supplier is required to delivery, although the business will also need to consider:

- The scope – and costs - of the services to be provided

- How the external supplier will meet these requirements

- From which location(s) services will be provided

- What response times are acceptable

- Roles and responsibilities.

Supplier selection criteria

The CREST research project identifies six main criteria for selecting an external supplier, noting, “there can be a big difference between a cheap cybersecurity incident response service and one that provides real value for money.”

1. ***Solid Reputation***

   Suggested questions the client firm may wish to pose to a prospective external supplier include:

   Are you able to demonstrate how you have successfully responded to cybersecurity incidents in other similar environments – and any lessons learnt?

   Can you provide independent feedback on the quality of work performed and conduct of your staff involved?

2. ***High Quality Value for Money Services***

   Suggested questions the client firm may wish to pose to a prospective external supplier include:

   Can you show [in a language I can easily understand] that you provide high quality services, (including the methodologies, tools, techniques and sources of information you will use) to conduct a fast and effective cybersecurity incident response investigation?

   Can you demonstrate your organisations’ cybersecurity incident response capabilities (e.g. by making a presentation; showing examples of similar (sanitised) investigations you have undertaken) and providing a sample summary /wash up report)?

   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?

3. ***R&D Capabilities***

   A suggested question the client firm may wish to pose to a prospective external supplier includes:

   Do you perform sufficient research and development to be able to prepare for, respond to and follow up the latest sophisticated cybersecurity attacks?

4. ***Highly Competent Experts***

   Suggested questions the client firm may wish to pose to a prospective external supplier include:

   Can you specify: named individuals who will be responsible for managing and conducting the investigation; their experience of the environment within the scope of the investigation; their qualifications; and the exact role each individual will perform?

   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?

5. ***Security Risk Management***

   Suggested questions your client firm may wish to pose to a prospective external supplier include:

   Are you able to demonstrate how you can ensure that all relevant evidence is properly gathered and preserved when conducting an investigation?

   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?

   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?

6. ***Complaint Process***

   A suggested question your client firm may wish to pose to a prospective external supplier includes:

   Can you outline the problem reporting and escalation processes that you adopt should there be a problem with the cybersecurity incident response service?

If seeking a reference for the external supplier, client firms should be advised to ensure that the referee has used the supplier they are recommending for a similar service to the one required.

Procurement

The aim is to contract an external supplier who can help the client firm meet specific and clearly identified requirements – at the right price – not just one who can offer a range of impressive products and services which may not be relevant for the client business.

Ultimately both parties, the client firm and the external supplier, need to have a common understanding of what can and cannot be done with the time, resources and money available.

Likely costs should be agreed in advanced, in terms of typical day rates and the expected level of support required to deal with a range of incidents. This will enable the client business to assign a realistic contingency budget in advance, thereby reducing the potential financial impact when a cybersecurity incident occurs.

Meeting the costs of cybersecurity incident response and data recovery

The aforementioned pages are illustrative of the time resource required to prepare and deliver Cybersecurity Incident Response and Data Recovery, and given 'time is money' many SME client firms may find the outsourcing costs to be unduly prohibitive (quotations in excess of £50k are not uncommon).

One potential solution is Cyber and Data Insurance, with the Institute of Directors (IoD) currently using the HISCOX product for its membership. The advantage of this type of insurance (which can also cover losses to the client firm by supplier breaches) is it not only covers the costs of outside computer forensic analysis to confirm the breach and any legal costs incurred in managing the breach but it can also cover damages caused to the client firm and/or claims made against it resultant from the breach (subject to the limit of indemnity). This type of insurance product can also cover costs associated with data recovery and even the ransom payment demanded under a ransomware attack, in addition to any regulatory awards made against the client firm for breaches of personal data or sensitive commercial information, where legally insurable (subject to the limit of indemnity).

The disadvantage of this insurance product is it does not meet the claims, losses or breaches of intellectual property rights (other than compensation and defence costs where a hacker has altered emails, website etc.), noting that by definition a trade secret ceases to have any further commercial value once it has been disclosed to competitors. Cover for the financial loss of any trade secret which was the target of the cyberattack will require the client firm to consider a more general Intellectual Property Insurance product. Insurance products will often require the client firm to inform or allow the insurance company to inform appropriate law enforcement authorities about the Cybersecurity Incident.

An alternative solution might be for the client firm to extend its cybersecurity protection beyond Cyber Essentials Plus in the expectation of a future breach. We have already referenced in our previous ***SME Guide to IP Cybersecurity***, the use of deception technologies, under which shadow networks can be created to divert and mislead the malicious intruder (e.g. see www.countercraft.eu). Whilst the cost of deception technologies might also be unduly prohibitive for some SME client firms at present, other more affordable 'active' cyber defence methodologies may also be available (e.g. obfuscation or data fragmentation see www.prizsm.co.uk).

Further reading

This Guide is intended for educational use only and uses selected text and adaptations from:

HISCOX Cyber and Data Insurance Policy Summary (2018)

CREST *Cybersecurity Incident Response Supplier Selection Guide* (2013)

CREST *Cybersecurity Incident Response Guide* (2013)

U.S. Department of Commerce National Institute of Standards and Technology Special Publication 800-61 *Computer Security Incident Handling Guide* (2012)