Guide to **Incident Response**

evalian

This extensive guide will give you a detailed overview of security incident response. You can use the table of contents in the right-hand sidebar to navigate to different sections.

Introduction

Penetration testing is a common way for companies to gain assurance and information about the security of their IT infrastructure. But for many, it's seen as a dark art, carried out by hoody-wearing geeks with confusing terminology and (excuse the pun) impenetrable reports that can be hard to interpret, let alone act on.

Irrespective of the nature of your organisation, its size, and the variety of systems used, it is highly likely you will suffer a security incident at some point. Hopefully, these will be minor incidents that cause limited damage but there is always the risk of a major incident that has a much more significant impact on your organisation.

For example, a simple phishing email that leads to a single mailbox being compromised might have minimal impact if detected and mitigated quickly. On the other hand, a phishing email that starts a ransomware attack affecting all systems could result in a need for the business to move to pen and paper processing.

When a high-impact security incident arises, you will want to leave as little to chance as possible. This is where security incident response comes in – the most successful 'response' is built on planning, preparation, agreeing on strategies to follow, rehearsing and improving.

In a smaller organisation, a single Incident Response Plan may be sufficient, but in a larger organisation a high impact incident will likely trigger several plans including the Incident

Response Plan (for IT or security operations personnel), the Business Continuity Plan (to be followed by the wider business to keep the wheel turning) and potentially a Crisis Management Plan (to manage wider communications and reputational damage).

This guide is focused on the Incident Response Plan which is followed by your computer security incident responders who have the unenviable task of detecting incidents affecting systems, containing them and recovering from them. This team has historically been referred to as a Computer Emergency Response Team ("CERT") or Computer Security Incident Response Team ("CSIRT").

Sources of Best Practice

There are two authoritative sources of best practice for security incident response we recommend to clients: NIST Special Publication 800-61 and ISO 27035 (currently in two parts).

NIST SP 800-61 is the Computer Security Incident Handling Guide, a set of recommendations published by the US National Institute of Standards and Technology (NIST). NIST is (among other things) responsible for developing information security standards and guidelines for implementation by US Federal organisations. For this reason, NIST publications set out the very best practice guidance and form a useful benchmark for all organisations.

ISO 27035 forms part of the ISO 27000 series of standards and guidance issued by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Unlike ISO 27001, ISO 27035 is not a standard – it is a guidance document and sets out techniques organisations can follow when seeking to implement incident response best practice.

There is considerable overlap between NIST SP 800-61 and ISO 27035, but with some differences in terminology. Both follow the same broad incident response lifecycle, as shown in the images below:

Both sets of guidance place emphasis on planning, preparation, detection and analysis before response. This is what sets a good incident response apart from making decisions on the fly. There will always be a need to respond according to the specifics of the incident, but there is much you can plan and prepare for to make incident response more successful.

Another source of authoritative guidance is, of course, the UK National Cyber Security Centre. The NCSC aims to make their guidance easy to understand and consume. Their focus is on the fundamentals or minimum incident response plans and considerations you have addressed rather than very best practice, which include:

NCSC Incident Response	Have Key Contacts	Escalation Criteria	Basic Flowchart	At Least One Conference Number	Basic Guidance on Legal or Regulatory Requirements

If you haven't taken any steps towards Security Incident Response Planning so far, the NCSC's guidance is a good starting point to understand what your baseline should be. If you plan to implement a comprehensive incident detection, analysis and response capability then NIST SP 800-61 or ISO 27035 are your reference points. Just bear in mind that both are best practices and may need to be 'right sized' for your own organisation.

Our cyber security incident response service

Security Events, Incidents and Severity

Within IT governance and security, it is important to agree on the meanings of specific terms and incident response is no exception. At the very least you should define 'security event' and 'security incident'. ITIL, NIST SP 800-61 and ISO 27035 define them differently so it's easy to think people within the same business could take a different view. Whatever approach you take, be consistent.

We tend to lean towards the ISO 27035 definitions: in our view, a security event is an occurrence that indicates a possible breach of cybersecurity or failure of controls; and a 'security incident' as an event (or series of related events) which has or is likely to result in a breach of policies and/or compromise of systems and assets.

To help contextualise this, think about security monitoring. If your organisation has a SOC or has security analysts, they will monitor security events all the time. Some of this may be automated (e.g. using a SIEM) whereas other monitoring may be more manual. If any of these events indicate a breach of a security policy affecting system (or data) integrity or

availability or unauthorised access, then the security event should be treated as a security incident.

Once a security incident has been identified, it is important to classify the incident based on its potential impact on the business. For this reason, an agreed classification scheme is essential to ensure incident response activities are proportionate to the potential impact on the business.

For example, a low-impact security incident may best be dealt with through your standard IT incident management process. A high-impact security incident, by contrast, will necessitate escalation within the business and require management by a dedicated Incident Response Team ("IRT") in accordance with the Incident Response Plan.

Incident Response Preparation & Planning

Incident response starts with preparation and planning. If you read our recent Guide to Penetration Testing, you'll remember that Penetration testing is a common way for companies to gain assurance and information about the security of their IT infrastructure. In a larger organisation a policy or a 'charter may also be advisable, in which senior management set out their commitment and expectations, along with key roles, responsibilities and related requirements.

Have a Plan & Supporting Documentation

Whatever the size of your organisation, an Incident Response Plan ("Plan") for your CERT to refer to during a high impact incident is a minimum requirement. The Plan should set out roles and responsibilities, details about IRT membership and authority level requirements for invoking the plan and mobilising the IRT.

The Plan should be supported by documents setting out strategies for responding to specific threats and containing and recovering from them generally and on specific systems (starting with the most business-critical systems). These strategy documents are sometimes called procedures but are most commonly referred to as 'playbooks' or 'runbooks' and should include guidance on technical processes to follow, tools to be used, techniques for different systems and might include, for example, checklists and decision trees.

Having a plan and supporting documents doesn't mean you should overladen your organisation with paperwork and indigestible documentation. Sometimes a simple checklist for quick reference will do the job – you don't need to recreate War and Peace.

Have a Team Warmed Up & Ready to Go

It is important to know who needs to form part of your IRT, for them to know their roles and responsibilities and to have their contact details to hand. Ensure the IRT team members know who they are and who their alternate will be if they are away from work for any reason.

Train your IRT members on the contents of the Plan and the supporting documentation, especially where they apply to their specific responsibilities. The makeup of your team will depend on the systems you use, the size of your team and the skills available.

In large organisations you may have dedicated CERT staff, but in most other organisations you'll likely have a virtual IRT made up of people with other day jobs. Your IRT may even include external specialists, such as personnel from your outsourced SOC or MSSP and specialists from retained forensic or incident response consultancies.

Identify Relationships & Authorities

Although your IRT is primarily focused on systems, input will be required from other functions in the business. This will almost certainly include Legal and Data Protection / DPO (where applicable) and will likely include HR, Facilities and other functions. The IRT will also need to understand what authority they have and where authority for some decisions requires approval from or decision making at a high level.

For example, does your IRT have the authority to disclose the incident to the NCSC or does that require approval from legal? Can the IRT engage an incident response specialist or is that provided by your insurance company, meaning they have to be notified? Can the IRT take down any system, including revenue-generating or business-critical systems, to prevent an incident from spreading, or is senior management approval required?

External relationships will also be very important. Spend time compiling the list of third parties you may need to communicate with. This could include the NCSC, industry bodies (especially in the public sector), regulators, IT and security suppliers, incident response specialists, your insurers, technology vendors and cloud service providers.

Include contact details for external parties in the plan or a supporting document. As covered above, make sure you understand the authority levels for disclosing details about the incident. In larger organisations there may be a wider communication plan, but in smaller organisations you may need approval from senior management.

Agree Primary & Backup Communication Methods

It's extremely important to ensure you have backup communication methods if your primary communication tools have been affected by the incident. These days there are so many different communications tools so this should not be a challenge, but make sure everyone understands what is to be used and everyone has details to access the backup tools – including everyone's mobile numbers!

Secure communication is critically important as you don't want attackers accessing any communications, so consider the encryption settings and secure communication channels available for internal and external communications when establishing your communication methods.

Have Incident Analysis Resources Available

During the initial stages of a major incident, analysis is critically important. The last thing you want to be doing is cobbling together old equipment and downloading new tools from the internet. As such, think about the minimum hardware and software tools you could require during an incident, ensure they are available and that incident responders know how to use them.

This might include, for example, having a clean laptop for forensic work, packet capture software your team is experienced in using, and digital forensic tools your team knows how to use. Clearly, there are commercial tools available but there are some good open-source tools available too if budget is an issue – but you want your incident responders to be practiced in using them and to have access to information including port lists, network diagrams, asset lists and maybe even hashes for critical files to compare against.

You should also prepare the tools needed during containment and recovery, which might include, for example, copies of operating systems used, access to backups for critical systems even alternative anti-malware tools to help with eradication.

Train, Practise & Prepare for an Incident

Prepare your IRT for the incident by running awareness training, page turn walkthroughs of the Plan and carrying out tabletop incident exercises. More detailed incident simulations are also an option but can be quite disruptive in their own right. A well-prepared and facilitated tabletop exercise can be impactful and help IRT members to understand what their roles will be in the event of a real incident.

The NCSC has created various incident response exercise resources in their Exercise in a Box tool. The exercises are quite generic but are a good start and you can tailor them. You can also work with third parties who can create bespoke incident response exercises for you based on agreed scenarios and objectives.

Incident Response Detection & Analysis

Clearly, the starting point in responding to any major security incident is detecting it in the first place. Ideally, you will have tools available to help automate this process, including anti-malware, IDS/IPS, SIEM or even an in-house or managed SOC service.

At the same time, technology can present a lot of false positives and where your security monitoring is limited to specific systems, you may actually be reliant on reporting of notifications by end-users (or even affected third parties).

1. You should therefore spend time thinking about the sources from which you might receive indicators of an incident. Start with your users and make sure they know what they should report and to whom they should be reporting it. This is a critical step in your security awareness programme.
2. To help ensure you are prepared to analyse the incident, ensure your team has carried out baseline profiling of networks and key systems so they know what 'normal' behaviours look like, to compare with current system behaviours and network traffic.

3. Ensure logs for your systems are centralised and available to the IRT for review and, ideally, establish a process for event correlation using suitable tooling. During the analysis phase, you'll likely have too much data to sift through so prioritise hard – filter out categories of data less significant to reaching the answer you need.

4. Be realistic about your analysis capabilities. If you don't have the skills of the resource in-house to analyse your system and identify the root cause, ensure you have a supplier who can assist with this. As covered above, have a relationship with them already and know the services available to you and the likely costs. Retainer services are available but 'pay as you go' options are starting to become available. Your insurers may cover incident analysis and response services but may also have their preferred suppliers.

5. Ensure the IRT keeps a comprehensive record about the status of the incident, actions taken, decisions made and details of evidence collected – especially the chain of custody for evidence (which will be important in any criminal investigation). You can prepare forms for record-keeping or you can use tooling. Either way, the records are important during the incident and also after it. You can identify vulnerabilities to be addressed and improvements to be made from the records you keep.

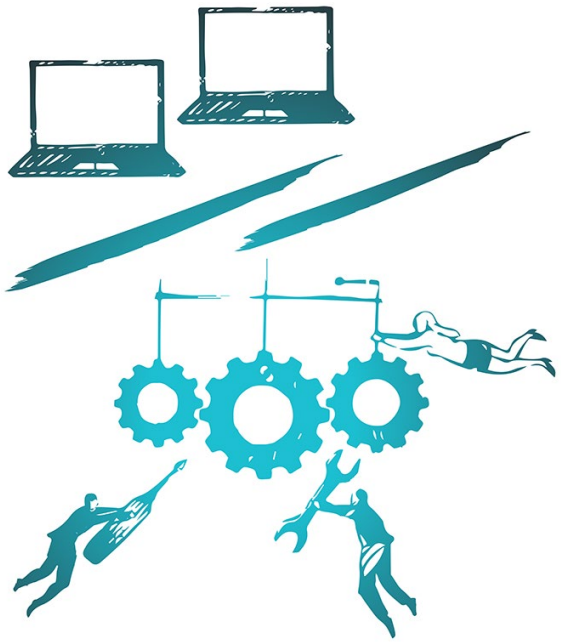
6. During incident analysis, you will also need to classify the incident based on impact on the business. As covered above, have an easy-to-understand classification matrix with clear escalation/notification requirements for each level of severity. Keep the

classification under review – what might seem low impact initially might quickly need to be classified as high impact as more information becomes available. Likewise, the initial impact might not be as bad as first thought, meaning the classification can be downgraded.

Our cyber security training services

Containment, Eradication & Recovery

When responding to an incident, there is pressure to focus on getting systems back up – especially business-critical systems. For critical national infrastructure, the security focus is typically on availability for industrial control systems. To avoid penalties and potential regulatory action there will 8be demands to get systems rebuilt and operational again, but this can exacerbate the problem.



The first step is to contain the breach – disconnect affected systems from the network, segregate sections of the network, disable compromised user accounts and advise users not to connect or use specific systems. If you move too quickly to try and recover systems then the problem may spread or systems may simply become infected again, which will slow you down and use up valuable resources.

When the incident is under control you have reached the point at which you can reconnect or recover systems. Ensure you know the critical systems within the business and the impact an incident will have if they are compromised or become unaffected. Prioritise those systems aggressively during containment, eradication and recovery.

Your containment, eradication and recovery strategies should be set out in the procedures or 'playbooks' referred to earlier. At a high level, have these in place for common threats, such as ransomware, malware and suspicious network activity. At the next level down, you may want to create specific playbooks of procedures for business-critical systems including those which process your most sensitive data.

Your recovery activity could include, for example, restoring from backups, rebuilding systems from the ground up, patching, changing authentication details, tightening controls and running enhanced monitoring on compromised systems in the immediate aftermath. Much of this can be pre-planned, especially for priority, specialist, or legacy systems where knowledge may be limited.

Remember to keep recording all details about the incident, including decisions made by the IRT and to gather evidence and store evidence in line with a set procedure and in a manner that protects the chain of custody.

Post-Incident Activity

The good news is you will have contained and recovered from the incident by this point. On the flip side, this may have taken days, weeks, or even months in some cases.

Your lessons learnt review is not simply a tick box exercise – it is a genuine opportunity to identify steps to be taken to prevent similar incidents and respond more effectively to incidents in the future. Your review should reflect the scale of the incident – a light touch review for smaller incidents and a larger scale review for more serious incidents.

Schedule the review as soon as possible after the incident so it is fresh in the IRT's mind and refer back to the records and notes kept during the incident. Key questions to ask include

What exactly happened and when?

Were the Plan and supporting documents followed?

Were they adequate?

What information was needed sooner?

What would we do differently next time?

What additional tools or resources would have helped?

What corrective actions should be taken to improve our incident response capabilities?

How Important is Security Incident Response, Really?

If the above sounds complex and expensive, then you may be wondering is it worth the effort? The short answer is yes, but don't just take our word for it.

In March 2019, Norwegian aluminium company Norsk Hydro was hit by Ransomware which reportedly cost the firm £45m. All of Norsk's systems and sites were impacted, meaning all computers and systems become unavailable. It took Norsk more than a month to return to full operation, with staff required to use pen and paper and retired staff invited to help advise on historical manual processes to keep the business running.

More recently the UK infrastructure business Amey suffered an attack in December 2020. Amey was hit by Mount Locker ransomware in what they called a "complex" cyber-attack which presented Amey with a double whammy problem. Not only did the attackers encrypt their systems, they had also exfiltrated a large quantity of data to leak on the internet in advance.

This technique is increasingly being used by ransomware attackers in case their victims have good data backups they can use to recover encrypted data without paying the ransom. In total, 143GB of data were stolen, from which 65GB was published online to apply pressure to Amey to pay the ransom demand.

In response Amey was forced to hire specialist incident response services, to shut down their network and systems and to move to manual operations for a significant period. The initial intrusion was reported to have happened in mid-December, with data published on Boxing Day 2020. Recovery work was still ongoing in late January.

Clearly, no one wants to be hit by such a high-impact incident, but if you are, your organisation will be in a much better place for having followed the steps set out in the guide. It also helps to pr

Contact us

Telephone

03330 500 111

Email

hello@evalian.co.uk

Head Office

West Lodge, Leylands Business Park, Colden Common, Hampshire, SO21 1TH

London Office

10 Fitzroy Square, London W1T 5HP

Manchester Office

Jactin House, 24 Hood Street, Ancoats, Manchester, M4 6WX

Dublin Office

69 Main Street, Blackrock, Dublin, Ireland, A94 N6D0

Visit

www.evalian.co.uk