Writing a Cyber Security Incident Response Plan

WHAT IS A CYBER SECURITY INCIDENT RESPONSE PLAN?

If your organisation suffers a cyber attack - and the chances are that at some point it *will*, the faster you respond, the more you limit the risk of damage to your business. Having a Cyber Security Incident Response Plan to follow will ensure you know what to do, who to involve – and reduce the panic!

You may actually be required to have such a plan by your insurers, and certainly it is a requirement from the Information Commissioners Office as part of the GDPR.

A Cyber Security Incident Response Plan should be a simple document, which all your staff have access to, for them to follow if they believe they are being attacked or have identified a breach.

GETTING STARTED

- To get started you need to decide what you consider to be a cyber security incident and document this on your plan. Remember this does not have to necessarily be an external attack and could, for example, be an internal breach. Examples are:

  - Loss of confidentiality of information
  - Denial of service
  - Unauthorized access to systems
  - Misuse of systems or information
  - Theft and damage to systems
  - Virus (attacks)
  - Phishing emails and targeted emailing
  - Inadvertently giving out passwords or media
  - Exposure of uncollected print-outs

- In case you are unsure whether it is a security event/incident or not, we advise you to note it down anyway so that you have it recorded.

INITIAL ACTIONS

- Should the worst happen, there are some initial actions that you may need your staff to carry out to contain the incident – particularly if it is a malware or ransomware attack. Some suggestions are:

    - Remove any network cables from the affected computer and switch off wireless
    - Unplug any peripherals (such as external disk drives or printers)
    - Leave the computer switched on and connected to power
    - Report the incident (see next section)
    - Wait for instructions

REPORTING

- Now you need to decide what information you should be collecting. Typically, you should collect the following but your requirements will depend on your business needs:

    - Date of the incident
    - Name of the person who is reporting the incident
    - Location of the incident
    - Type of incident & description
    - Others involved/ affected?
    - Next steps (if applicable)

- Your next task is to decide how to record this information and who to distribute it to. A form is usually best – this could be an online form but remember that all staff should also have access to a paper-based copy in case their computer is disabled. Here is an example of a collection form.

WRITING YOUR PROCESS

- Now you need to write your process document, which describes what you do when someone reports an incident and who deals with it. Your process should describe the different stages of your response, who deals with them and what they should be doing. Stages will include:

    - Co-ordinating the people involved in the response and how they will communicate
    - Assessing the scale of the incident and agreeing next actions
    - Communicating and providing updates to everyone on your contact list as well as to internal staff
    - Documenting your findings and responding to questions
    - Ensuring everything is covered from initial reporting of the incident to closing it down

THE CONTACT MATRIX

- It's critically important you record all the parties you may need to communicate with in event of a security incident. This could be:

    - Internal staff such as Directors and the Data Protection Officer
    - Any suppliers involved in managing your information systems such as IT outsourcing companies
    - The Information Commissioners Office
    - Your clients – remember it is much better for them to hear their data is compromised from you (and that you are managing it) rather than a third party, or even worse a cyber criminal
    - Others include Police, Insurers, Investors, Information Commissioners office, marketing & legal
    - You should list the appropriate contacts for each type of incident and list contact details

For each contact / company you contact you should document:

- Why you are contacting them (eg. the purpose and what you expect them to do)
- How to contact them (eg. phone / email / web portal)
- Their contact details (eg. phone number / email address etc.)
- The information you need to provide them
- When you need to contact them (eg. how soon after the incident)
- The response you should expect (eg. how you receive it, when you receive it)

Company / Contact	Scenario to contact them	How to contact them	Information to provide them	When to contact them	Response to expect
Pro Drive	Any incident involving the IT systems. Pro Drive will manage the technical elements of the incident to isolate the threat and recover the systems	Call them on 0330 124 3598 during 08.30-17.30 Monday to Friday	Name of the person who is reporting the incident Date of the incident Location of the incident Type of Incident Description of Incident Others involved/ affected?	You should contact them as soon as possible after the incident occurs	A maximum 15-minute response. Pro Drive will communicate in their response what their next steps will be
Information Commissioners Office	Any breach where you believe personal data to be involved. If unsure about whether to report, use the ICO assessment here	To report a breach please follow the instructions and use the form on the ICO website here	Name of the person who is reporting the incident Date of the incident Location of the incident Type of Incident Description of Incident Others involved/ affected?	Within 72 hours of the breach occurring	It can take several days to receive a response from the ICO. This will usually happen by email

TESTING THE PLAN

- You must test your plan at least once a year, based on an example security incident and following through all your contact procedures. You do not necessarily need to contact the companies/contacts in your response plan but you should validate that your processes are correct.

FURTHER INFORMATION

- A very detailed guide to writing a Cyber Incident Response Plan can be found on the National Cyber Security Centre website here.

- For assistance in ensuring all your information security policies conform to best practice, consider certifying your business to the IASME Governance Standard – further details here.

Account Team – 0330 124 3599
Helpdesk Team – 0330 124 3598
Email: helpdesk@prodriveit.co.uk