



daisy.

INCIDENT RESPONSE

CYBER BREACH
PREPARATION &
RESPONSE



CYBER BREACH PREPARATION AND RESPONSE

We have all seen how a cyber security breach can cripple IT systems, and destroy organisational and individual management reputations. When you suffer an incident, an immediate, calm, incident response and expert management guidance is essential. When an incident hits, time is of the essence to limit the damage.

The challenge for many organisations is that they don't have any direct experience of dealing with a serious cyber security breach. Even cyber security professionals may not have encountered a significant incident with public impact in their current or previous roles. In our experience, when called out to an incident, we often encounter confusion and, in some cases, blind panic.

All too often, management are led by preconceptions based on media hype and Hollywood portrayals of hacker activities. This situation is made worse when internal technical staff are in disagreement and giving contradictory advice.

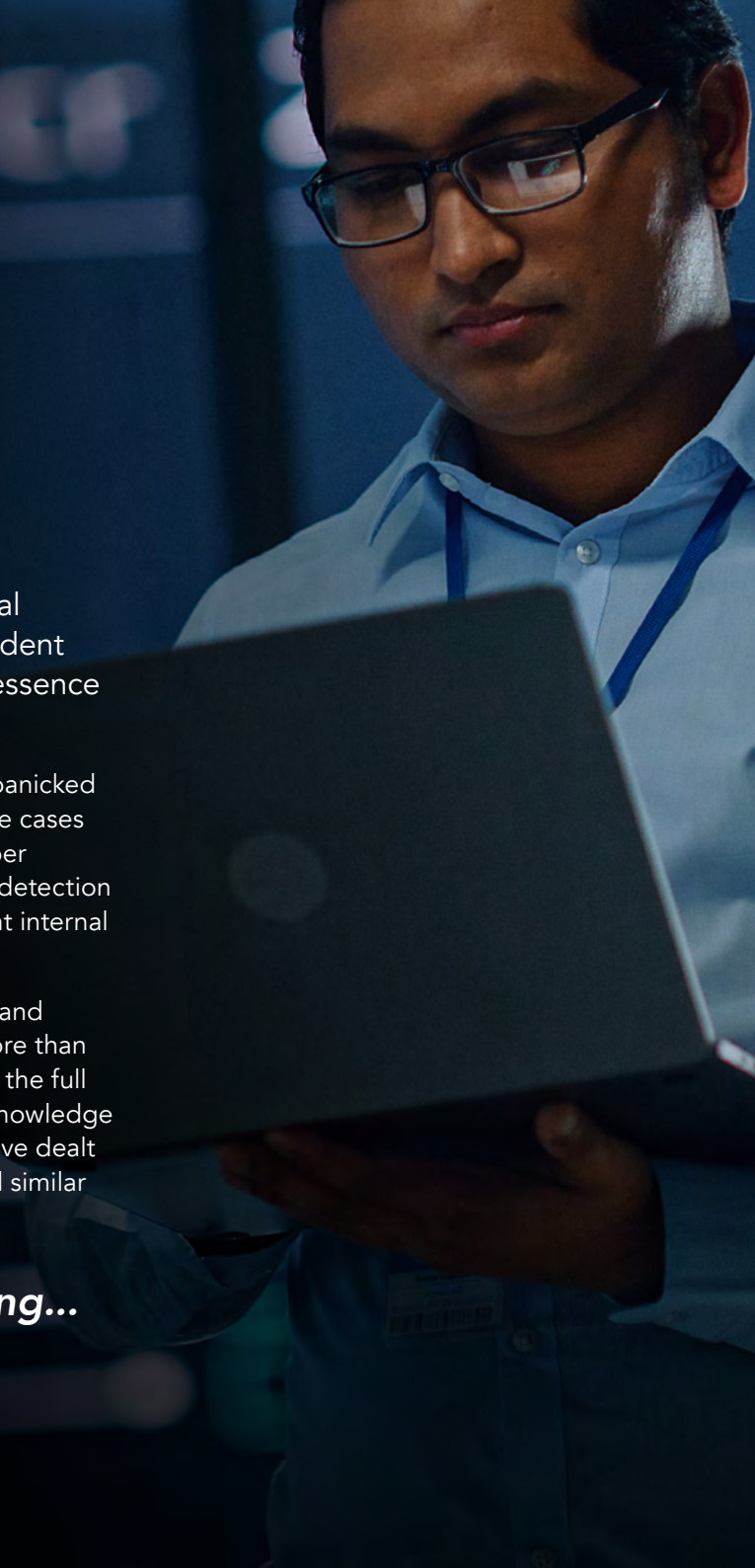
Increasingly, we find that organisations can be panicked into thinking they have a serious breach, in some cases even reporting the event externally before proper confirmation. This is often because the internal detection technologies are lacking, and there is insufficient internal expertise to understand the situation fully.

As you will understand, each incident is unique and requires a different response. However, with more than 20 years of experience, Daisy* has encountered the full range of attack scenarios, and has up-to-date knowledge of the latest attack trends. In many cases, we have dealt with recent incidents where attackers have used similar techniques.

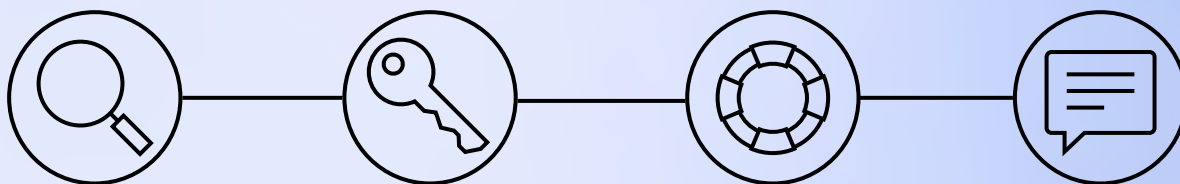
***"Thank you for the fantastic response to our emergency this morning...
to have an engineer on-site within two hours is astonishing!"***

Business Support Manager, Legal Practice

*Daisy acquired Security Specialist Company ECSC in June 2023



You can think of an incident response as containing distinct phases of operation:



Investigation

We need to understand what evidence you have that has led you to conclude, or suspect, that you have an incident.

In many cases, we are often able to identify incidents as false alarms – these situations are becoming more common, as people jump to conclusions, blaming external attacks for IT system failures.

Conversely, we can help identify and confirm attacks where you may have no reliable intrusion detection capabilities.

Containment

Once an attack is understood, it is vital that the attack route, and related vulnerabilities, are removed and systems secured.

Breach investigations usually find a wide range of security weaknesses, and immediate action is needed to secure these. In some cases, evidence is uncovered of multiple historic breaches that have remained undetected.

Recovery

Restoring IT systems and related business functions is clearly a top priority in limiting the financial impact of a breach.

Decisions need to be taken regarding when to shut systems down, and, more importantly, when it is safe to turn them back on. The right incident support can help facilitate these important decisions.

Communication

Calm, timely communications (internally and, where required, externally) is a critical senior management function. Our role is to guide you, help develop content, and rehearse for potentially challenging media attention.



UNDERSTANDING YOUR RISKS

Cyber security risk is now becoming a real concern for senior executives. Many have lived through a major incident (or near miss) and therefore understand the potential organisational impact. Those without direct experience of a breach are still aware of the media attention on cyber security and the focus on organisations following an incident.

You will regularly see in the press that details are revealed of serious breaches of security, and the significant consequences for organisations and the executives forced to answer for their organisations' technical failings. Of course, these are only the tip of the iceberg, with most breaches kept quiet, and many more remaining undetected.

It is worth considering what your most serious cyber security breach would involve:

- What systems might be compromised?
- What data could be lost?
- How would the media report such an event?

A myth of cyber security breaches is that organisations are targeted because of what they do, the information they hold, and their public profile. The reality is much simpler – people get hacked because they are vulnerable. Simply ask your security team how many potential scans and attacks your firewall blocks in a single day – attackers look everywhere for weaknesses. Only once on the inside do they see what prize is available for their efforts.

That is not to say that the nature of your operations does not influence the risks you face. However, in today's connected world, most organisations have similar cyber security challenges and related risks.



DAISY'S ROLE IN YOUR INCIDENT


The role of external experts in a breach response can be wide-ranging. However, we see our role as assessing the nature of your problem, understanding your response capability, and providing timely expertise to fill the gaps and resolve the incident.

The following are examples of the types of management activities that Daisy can perform, where required:

- Direct internal and external response team actions
- Provide regular update briefings to senior executives
- Liaise with external agencies, such as the Information Commissioners Office (ICO) and law enforcement
- Design external customer communications
- Co-ordinate with your internal or external legal advisers
- Interview staff
- Instigate actions with third-party service providers and system vendors

Technical actions depend upon the nature of the incident. However, some common activities include:

- Network traffic capture and analysis
- Review of system logs
- Forensic imaging of systems
- Suspicious file investigation
- Network vulnerability scanning
- User communication review
- User behaviour review
- Account activity checks

A photograph of two men in a server room. The man in the foreground is wearing a dark turtleneck and glasses, looking towards the right. The man behind him is also wearing glasses and a light blue shirt, looking in the same direction. The background shows server racks with blue lighting.

"A highly professional service at a time when we required it most. They quickly understood our needs and integrated with our own people in a seamless way which was incredibly effective."

Group FD, High Street Retailer

SERVICE OPTIONS

If you have been, or suspect you have been, a victim of a security breach, Daisy's 24/7 Incident Response service can provide instant on-site support. Whether you are new to Daisy, an existing customer, or have a guaranteed response retainer in place, you can call us now and speak to one of our experienced security engineers.

In order to ensure a quality response in all cases, we have to prioritise which incidents we agree to resolve. Daisy deals with all incident responses according to the following priorities:

1. Customers with Incident Response Retainers and contractually guaranteed response
2. Existing PROTECT managed services customers
3. Other Daisy customers
4. Non Daisy customers

It can make sense to set up a Daisy Incident Response Retainer (IRR). All customers holding an IRR will receive a 20% discount on any future incident response rates.

We offer Incident Response Retainers on four levels

BRONZE

Giving you guaranteed access to the Daisy incident response team (IRT). Four hour response target. 50% reduction in minimum spend.

SILVER


Giving you guaranteed access to the Daisy incident response team (IRT). One hour response SLA. No minimum initial incident payment.

GOLD

Silver, plus an initial engagement with the IRT to create an incident response plan and for the IRT to hold critical information to facilitate a rapid and effective response. Plus Incident response playbooks.

PLATINUM

Gold, plus we also provide regular systems backup, with recovery data copied and stored remotely. We then provide an annual technical and management tabletop exercise, confirming the integrity of the recovery data and test the system recovery processes.



It can make sense to set up a Daisy Incident Response Retainer (IRR). All clients holding an IRR will receive a 20% discount on any future incident response rates.

SERVICE SPECIFICATION

BRONZE

- Guaranteed unlimited 24/7/365 incident responses from the Daisy Security Operations Centre (SOC)
- 20% discount on Daisy incident response rates

SILVER

- Guaranteed unlimited 24/7/365 incident responses from the Daisy Security Operations Centre (SOC)
- 20% discount on Daisy incident response rates
- Rates held for duration of contract initial term

GOLD

As silver, plus important response preparation to ensure a smooth transition response from the Daisy SOC, including:

Set-up (Year 1)

- Initial threat assessment
- Protection capability summary
- Information repository creation
- Response plan production

Annual (Year 2+)

- Capability summary update
- Information repository update

PLATINUM

As gold, plus to protect you against ransomware encrypting your backups, we provide the following:

- Regular systems backup, plus recovery data copied and stored remotely
- Annual ransomware exercise to confirm integrity and recovery data and test system recovery processes

This ensures that you are never forced to pay ransoms due to disrupted, disabled, or encrypted backups.

"Above all, Daisy's calm and assured approach bred a level of confidence within our team that undoubtedly helped us achieve a successful outcome."

FD, Online Retailer





NEXT STEPS

If you want to find out how Daisy can help you to improve your cyber security, contact us on:

 **0344 863 3000**

**Or if you're an existing customer,
get in touch with your account
manager directly.**