Cyber Security Incident Response Team (CSIRT) Service

What is it?

The **norm.** Cyber Security Incident Response Team (CSIRT) Service minimises the impact of cyber security and personal data breaches by providing instant access to fully trained cyber and data protection experts when you need it most. Our specialist investigation teams will help you understand how a cyber-attack was perpetrated, and support you through remediation.

Our experts will work alongside your internal staff from initial incident identification, through analysis, containment, malware eradication and the restoration of services. We also handle the regulatory and compliance elements of a breach, such as communication and reporting.

Our cyber security experts use advanced tools to quickly investigate and assist in remediating a security incident, allowing you to resume business as usual in the shortest possible time, whilst gathering important data that can assist in an investigation.

The purpose of the **norm.** Cyber Security Incident Response Team service is simple:

* To provide rapid access to the appropriate experts in response to a cyber security incident
* To control and limit the damage caused by a breach by conducting a full investigation and response including root cause analysis and incident response plan
* To prevent future incidents by reporting on findings from the incident and providing practical recommendations

What's included?

* Rapid deployment of **norm.** cyber security experts in response to cyber security incidents
* Full investigation and response including root cause analysis and an incident response plan to ensure the breach is controlled, limiting the damage to your business
* Deployment of **norm.** cyber security experts to identify weaknesses in your corporate environment
* An optional Incident Readiness Service to support organisations that wish to prepare their organisation ahead of an incident
* A final incident report including detailed findings from the assessment and recommendations to prevent similar incidents in the future

Want more detail?

For the full Service Description of our Cyber Security Incident Response (CSIRT) Service <<ClickHere>>.
To register your interest and get one of the team to call you <<ClickHere>>
or just give us a call on **+44 (0)20 385 55242.**

***Reassuringly dull cyber security**

norm.

In a nutshell…

The **norm.** Cyber Security Incident Response Team (CSIRT) Service is available on either a retained or on-demand basis. Regardless of which you choose, the aim of the service is to help organisations to recover from the implications of a personal data or security breach as soon as possible. Our team of experts will also work with the affected organisation to ensure that the likelihood of a future breach is minimised.

Why now?

Technology is consistently evolving, and alongside that, cybercriminals are continuously developing new attack techniques in order to breach defences. New vulnerabilities are constantly being discovered in a wide range of technologies including laptops, desktops, servers, IoT devices and web applications.

For most companies it isn't a case of IF a breach occurs, but rather WHEN a breach occurs. Incident management includes detecting and responding to computer security incidents as well as protecting critical data, assets, and systems to prevent incidents from reoccurring.

How does it work?

Once an incident has been discovered mobilising a response is critical. Regardless of whether you have selected the **norm.** On-Demand or Retained Incident Response Service our support will comprise of the following key activities:

* **Identify the category/sensitivity of data** and whether any Personally Identifiable Information (PII) is included
* **Expose the attack** by analysing the data and revealing what damage has been done
* **Remediate the incident** by safely repelling the attacker and putting measures in place to confirm remediation and prevent reinfection

Throughout the incident we will provide you with regular updates on key findings; ensuring that you are aware of the progress and any urgent actions that need to be undertaken. We will provide a full report at the end of the investigation detailing the work done, findings and recommendations for further work and estate hardening as required.

FAQs…

I have Cyber Insurance – doesn't that cover this sort of work?

Cyber Insurance will cover you for some of the tangible costs associated with a breach, but it probably won't cover all of them. By acting quickly and limiting the scale of the breach it is possible to reduce the full impact. In addition, some insurance companies will expect you to demonstrate a level of preparedness before accepting a claim.

I don't think my business would be a target for cyber criminals, we don't store credit card numbers or lots of customer data?

Regardless of the industry you operate in or the types of data you hold, all businesses are the potential target of a cyber-attack. The perpetrators of attacks such as ransomware are indiscriminate in their victimology. In some cases you may not even be the direct target of an attack, but your systems could be used as a stepping stone to attack one of your suppliers or customers.

Once we've been breached surely the damage has been done?

The earlier you identify and act against a breach, the less damage it will cause. A prompt response is essential to stopping a breach from turning into a crisis.

Can't I just a call you if I have a problem?

We do offer an on-demand option for CSIRT, but there will be some delay in addressing the incident as we set up and initiate the service. Any delay can allow the attack to penetrate further into your organisation, increasing the impact and possibility of a hefty fine.

Isn't this something my IT team should handle?

Cyber-attack forensics requires a highly skilled team to analyse logs and data, understand the affected areas of your network and repair the damage. Our CSIRT experts are very well trained in finding the root of the attack and getting organisations back up and running as soon as possible. In addition, breaches are not merely a technical issue. Data protection is equally as important, and effective management of the impact and communication with the relevant parties is essential.