No drama, no problem*

*Reassuringly dull cyber security

Cybersecurity Incident Response Team (CSIRT) Service

Norm’s Cybersecurity Incident Response Team (CSIRT) Service minimises the impact of any cyber incidents through providing access to our cyber and data protection experts at short notice, when you need it most. Our specialist investigation teams will help you understand how a cyber-attack was perpetrated and support you through remediation.

Norm’s Incident Response Service comprises of three key security modules:

- On-Demand Incident Response Service
- Retainer Incident Response Service
- Incident Response Readiness Service

Our CSIRT service includes access to our highly skilled cyber security and data protection experts who will work alongside your internal staff from initial incident identification, through analysis, containment, malware eradication and restoration of services as well as handling the regulatory and compliance elements of a breach (communication, reporting, etc.).

Norm’s security experts use advanced tools and can 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 investigations.

This service module covers the three elements of Norm’s holistic trinity of cybersecurity - People, Process and Technology.

Its purpose is simple:

- Rapid deployment of Cyber Security Experts in response to a Cyber Security Incident

- Full investigation and response including root cause analysis and incident response plan to ensure the breach is controlled, limiting the damage to your business

- Final Incident report provided detailing findings from the incident and recommendations to prevent similar incidents in the future

Service Offerings

Norm's Cyber Incident Response services are available in three models based on whether an incident has already occurred or whether you are preparing for potential future incidents.

- On-demand Incident Response Service. Suitable for organisations who have identified that a cyber security breach has occurred and/or maybe ongoing. The service offers a rapid deployment of our security experts to investigate the incident looking for aspects including point of entry, scope and breadth of the breach response, as an On-Demand service. We aim to provide immediate advice, suggesting effective next steps to prevent further damage and secure evidence. Being an On-Demand service there are busy times where we may be unable to respond as quickly as our retained service since commercial and legal agreements will need to be executed prior to any engagement and access to your systems can be granted. If guaranteed response times are required, Norm's Retained Service would be most appropriate.
- Retained Cyber Incident Response – Suitable for organisations who wish to ensure that we are available to respond to an incident rapidly; and without delay caused by commercial agreements when an incident occurs. This service includes SLAs on response and a framework contract which will enable you to call off our incident response services as required.
- Incident Response Readiness Service – Suitable for organisations who wish to prepare their business ahead of an incident, we offer services to both assess your current incident response capabilities and help you improve where required. A tailored version of this service is recommended at the beginning of a retained service to enable your first responders and our team to react as quickly and effectively as possible when an incident occurs.

How the CSIRT Service works

Once an incident has been discovered getting our support mobilised is critical. Regardless if you have selected our On-Demand or Retained Incident Response Services our support will comprise the following key activities:

- Confirm what is known about the incident and understand your key personnel, systems and processes
- Capture data, such as logs and disk images, which will contain evidence
- Identify the category/sensitivity of data and whether any Personally Identifiable Information (PII) is included
- Communicate the incident with the relevant Data Protection Authority in line with GDPR requirements where PII information has been breached
- Expose the attack by analysing the data and reveal what damage has been done.
- Remediate the incident by safely repelling the attacker and putting measures in place to confirm remediation and prevent re-infection
- Resume business as usual activities and monitor for new attacks
- Incident report with all details of the findings from the incident and recommendations to prevent similar incidents in the future

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 taken. 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 necessary.

On-Demand CSIRT Service

The on-demand CSIRT service allows a customer to report a potential incident 24 x7 through our incident response hotline. The incident will be recorded and passed onto our response team with a guaranteed first response within one working day. This response will include the details of the commercial agreement that will need to be completed and agreed prior to any engagement commencing.

Retained CSIRT Service

Norm’s retained service is delivered in three tiers, Bronze, Silver and Gold, allowing customers to balance risk and costs effectively whilst ensuring a guaranteed priority service during an incident,
The tiers provide the following core service levels:

	24 x 7 Incident Response Hotline		
	Remote Support	Onsite Support	Inclusive IR hours
Bronze	First responder contact within 4hrs (Mon – Fri 9 - 5)	On-site support next working day	N/A Hours billed at the discounted ‘Bronze Rate’
Silver	First responder contact within 4hrs (Mon – Sun 9 - 5)	On-site support next working day	20 hrs per year Additional hours billed at the discounted ‘Silver Rate’
Gold	First responder contact within 2 hours	Onsite support within 24hrs to pre-agreed sites	40 hrs per year Additional hours billed at the discounted ‘Gold Rate’

All tiers of norm’s retained CSIRT service are backed by 24x7 access to our incident response hotline.

While not compulsory, we strongly recommend that you utilise our Incident Readiness Planning Service at the beginning of a retained service. This will ensure that when an incident does occur, we are able to commence the vital investigation, mitigation and remediation tasks immediately without having to spend time understanding parts of the network or determine where the relevant data may be. We recommended that the incident readiness plan is reviewed and tested annually.

Incident Readiness Service

Protecting your estate from incidents is vital; however, it is not possible to prevent every incident. We regularly help companies respond to major incidents and understand how much a clear and effective response can help mitigate the impacts of an incident.

Our offerings are aimed at ensuring you can react effectively and rapidly when required. The offerings can be tailored to suit your organisation and requirements; however, the typical services include:

- Incident Readiness Assessment - We will work with you to understand your current incident response capabilities, incident readiness and business needs. Typically, this would include, but not limited to, reviewing the following:
    - Incident response plan (including escalation and key people)
    - Data availability and acquisition (logs, disk images etc.)
    - Arrangements with third parties (e.g. infrastructure management)
    - Understanding of network structure
    - Investigation capabilities
    - Remediation and recovery capabilities
    - Data processing activities
    - Identification of Personally Identified Information (PII)

- Incident Readiness Improvement - This service is aimed at improving and developing incident response capabilities within organisations. The scope of readiness improvements will be dependent on the current state of any incident response processes and policies that already may exist in the organisation, however the service typically includes;
    - Building or tailoring processes for incident response, including playbooks, quick reference guides and 'principles' for response to guide staff involved
    - Specifying systems, software, roles and responsibilities
    - Training of staff (can include support in hiring staff also if required)
    - Running incident rehearsals for staff across the organisation and working with teams to implement improvements based on lessons learnt
    - Defining plans for future training, rehearsals and process updates. Improved incident readiness will enable your organisation to rapidly and effectively react to incidents, ultimately lowering the risks of a major impact on the business as a consequence of the incident.

Service Availability

The CSIRT service is managed through norm's UK based Security Operations Centre (SOC), 24hrs a day, every day of the year. The Incident Readiness Service is provided UK business hours, Monday to Friday 9:00 to 17:30hrs, excluding public holidays.

Customer Responsibilities

- For On-Demand CSIRT engagements the customer will be responsible for signing an initial CSIRT order form detailing the daily rate of the service and scope of work and a systems access authorisation form to allow Norm engineers access to the Customer environment prior to initiating the service
- Customer will be responsible for providing the necessary access (physical and logical) to systems, applications, logs, etc. to aid in the investigation work.
- Customer will permit and ensure the installation of norm's Managed EDR agent on all endpoint systems to facilitate forensic data collection and further breach containment if required. This will be subject to additional fees.