

## DATA SHEET

### CYBER SECURITY INCIDENT RESPONSE TEAM

24/7 specialist support for swift security incident remediation

Despite the layers of security you have in place, it's almost inevitable that a cyber attack is going to break through your defences eventually. And when an attack hits, you need a quick and effective response and remediation plan.

If ignored, an attack can lead to a number of negative outcomes – from cyber criminals breaching your networks and stealing data, to holding your entire network hostage in exchange for a ransom payment. And then there are the broader legal issues. If you handle personal customer data, you need

to report any identified data breaches or attacks to the Information Commissioner's Office (ICO) within 72 hours.

Nobody knows the full impact of an attack until it is investigated – even the most innocuous-looking incidents need to be properly scrutinised. The fastest route to remediation and regulatory compliance is to outsource incident investigation to a team of security experts, forensic analysts and legal consultants who will manage the incident from end-to-end.

**If you think you're experiencing a cyber attack, please contact 0844 443 3538 for immediate support.**

### THE NASSTAR WAY

We value your security. Regardless of whether you're a current customer or new to us, if your organisation is concerned that it may be a victim of cyber crime, our CSIRT provides free, confidential advice, with no contractual commitment, 24/7.

On confirmation that a suspected incident is, in fact, a data breach, our team of Tier 3 and 4 Security Analysts and Forensic experts will provide end-to-end incident management and recovery, from analysing the root cause, to dealing with any legal ramifications.

Response time is critical, so the CSIRT work closely with Nasstar's Security Practice to ensure that any recommendations made can be undertaken swiftly, without the need to source a third party.

With a 100% success rate reported in 2019, Nasstar's CSIRT has a proven track record in fully recovering breaches and submitting to the Information Commissioner's Office (ICO) within 72 hours.

### FEEL SECURE WITH NASSTAR



**SC Awards Europe 2020 Winner:**  
'Best Managed Security Service'



**Finalist:**  
'Best Incident Response Solution'



**Finalist:**  
'Best SME Security Solution'



**100% CSIRT Success rate in 2019**

## KEY FEATURES

In the event of a cyber attack, Nasstar's highly trained Cyber Security Incident Response Analysts, led by Nasstar's Head of Security, will carry out the following:

### \\ Analysis and remediation

If an attack is identified, our experienced forensic team will establish the root cause and impact of each incident, using powerful automation technologies, allowing for faster assessment.

### \\ Managing your cyber insurance

If you have cyber insurance in place, we will work with the insurer, providing the information they need to assess your claim and determine their preferred route towards remediation.

### \\ ICO reporting

We'll prepare a clear and concise report of the incident – provided in an ICO-compliant format – to submit within the required 72 hours of the case being spotted.

### \\ Stakeholder management

We are experienced in dealing with the legal ramifications of cyber attacks, and will coordinate all exchanges between law firms, regulators, brokers and technical teams on your behalf.

### \\ Improving your security posture

Once we've eliminated the threat, we will make recommendations as to how your organisation can avoid cyber attacks in the future.

## THINK IT CAN'T HAPPEN TO YOU? THINK AGAIN

**In 2020**, the estimated global average cost of a data breach for SMBs was **£3 million**<sup>1</sup>

**In 2019**, the average time to identify a breach was **206 days**, taking a further **73 days** to contain the incident<sup>1</sup>

**77%** of security and IT professionals do not have a consistent network-wide cyber security incident response plan<sup>1</sup>

**30%** of incidents handled by a CSIRT are targeted attacks towards that organisation<sup>2</sup>

[1] Source: IBM, [2] Source: BAE Systems

As trusted advisors, I know that if an incident were to occur, Nasstar's Cyber Security Incident Response Team would be there 24/7/365 to help resolve the issue. They are more than just an extension of my IT team; they ARE Thrive's security team, and they are backed by processes that deliver an end-to-end approach from alarm response to remediation.

John Stenton, IT Manager at Thrive

## REQUEST A FREE SECURITY CONSULTATION

We've helped thousands of businesses avoid the risk of fines or long-term reputational damage following security breaches. Get in touch to find out how we can help to protect your business [enquiries@nasstar.com](mailto:enquiries@nasstar.com) or call **0844 443 4433**