INCIDENT READINESS.

EFFECTIVE MANAGEMENT OF CYBER INCIDENTS.

A PLANNED RESPONSE

It is a consequence of our interconnected world that nearly every organisation today faces a real possibility of cyber attack. In fact the UK Government now recognises cyber attacks as a Tier One threat[1] to our national security.

Many cyber attacks can be defeated by rigorous and well-maintained defences. However some attacks, particularly those launched by a determined attacker, will eventually evade such safeguards and inflict their impact on the targeted organisation.

Managing a response to an cyber incident is a complex task that involves the coordination of many decisions, resources, tasks and information. Events and threats must be understood. Decisions must be taken. Technical measures must be deployed. Further damage must be avoided. Stakeholders must be updated. Evidence must be preserved. All under intense time pressure and scrutiny.

A further complication of targeted cyber attacks is that there is an intelligent adversary focused on your estate; any actions you take may alert them and cause them to change tactics and potentially worsen the attack if you are not prepared and able to react.

Without a well planned and rehearsed response, such incidents can quickly develop into unmanageable, unpredictable and even chaotic situations.

React quickly, coherently and effectively to major cyber attacks.

CYBER INCIDENT READINESS

For more than a decade BAE Systems experts have been at the frontline of cyber security - helping our customers prepare for, contain and recover from even the most sophisticated cyber attacks.

Our expertise in combating state-sponsored, criminal and other highly motivated attackers is recognised by our status as a founding member of the CESG Cyber Incident Response Scheme.

We understand that when a cyber incident occurs, however serious, time is of the essence. The remedial actions taken in the first few hours will critically influence the eventual outcome. The right decisions are needed, at the right times.

Our Cyber Incident Readiness services give our customers the ability to respond rapidly and effectively to cyber attacks. We provide two types of service:

- Readiness Assessment: to measure the effectiveness of existing response plans, tools and resources
- Readiness Improvement: to design, build and deploy comprehensive and enduring incident management capabilities.

[1]https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace

Applied Intelligence

BAE SYSTEMS
INSPIRED WORK

ASSESSMENT SERVICES

Features

- Expert assessment of every aspect of your incident management capability – people, process and technology
- Recommendations including quick wins and other prioritised improvement opportunities
- Development of an improvement plan tailored to the specific needs of your organisation and any capability gaps found by our assessment

Benefits

- You will have a clear understanding of your organisation's current ability to manage major cyber incidents
- You will have clearly documented risks and plan for improvements to supplement a business case

IMPROVEMENT SERVICES

Features

- Development and deployment of response processes tailored to your organisation
- Specification of any new systems, roles and responsibilities needed to enable your response
- Comprehensive training and incident rehearsals for your staff, using realistic and relevant scenarios

Benefits

- Your technical teams and business decision-makers will have the training and confidence to respond effectively to cyber incidents
- Your risk of implementing a counterproductive response will be significantly lowered
- Your customers, shareholders and partners can be given confidence in your ability to protect vital information and systems

READINESS CRITERIA

Authority
- Clear roles and responsibilities
- Defined escalation routes
- Empowered to make business-impacting decisions

Resource
- Access to skills and expertise
- 24/7 availability if needed
- Third party specialists on call for complex cases and surge

Practice
- Regular training & rehearsals
- Test backup, failover and recovery procedures
- Ensure familiarity with process

Process
- Clearly defined, accessible & communicated
- Guidelines and check lists
- Integrated with rest of business

Legal
- Have extra processes for when court action may result
- Law enforcement contacts and know when they can help

Reporting
- Understand commercial or legal disclosure requirements
- Approach to handling press
- Backup if systems are down

Evidence
- Relevant logs collected and retained on key security devices
- Record of where evidence is, who can access & how to capture

Investigation
- Ability to triage, find unknown unknowns & root cause
- Network and disk forensics
- Malware analysis & attribution

Remediation
- Ability to apply remediation actions synchronously across estate
- Monitoring to confirm success
- Continual improvement

Threat Aware
- Receive and use threat intel to understand attackers
- Know how to adapt the response to the typical threat behaviours

Impact Aware
- Understand safety and business implications of attacks
- Adapt remediation actions to minimise additional impacts

Context Aware
- Maintain awareness of sensitive business activities (product launches or financial results)
- Proactively increase readiness

Global Headquarters UK
BAE Systems Applied Intelligence
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom

Australia: +61 (0) 1300 027 001
Dubai: +971 4369 4369
Malaysia: +60 3219 130 84
UK: +44 (0) 1483 816000
USA: +1 (617) 737 4170
E: learn@baesystems.com
W: www.baesystems.com/ai

www.linkedin.com/company/baesystemsai

www.twitter.com/baesystems_ai

Victim of a cyber attack? Contact our emergency response team on:

US: 1 (800) 417-2155
UK: 0808 168 6647
Australia: 1800 825 411
International: +44 1483 817491
E: cyberresponse@baesystems.com

CREST
CESG Certified Service
Cyber Incident Response
CPNI Centre for the Protection of National Infrastructure