Key benefits of Centrally Co-ordinating Security Operations

When a single, centralised authority is responsible for the detection, investigation and response to security events, organisations can realise the following business and security benefits.

Business Benefits

Regulatory Compliance
A centralised operation can provide enterprise-wide evidence of compliance with security policy, regulatory/legal requirements, and service level agreements.

Operational Costs
The long-term operational costs of hosting and managing a disparate number of security teams and personnel can be reduced, and the use of operational toolsets can be standardised.

Holistic Risk Management
Centralised operations can process threat intelligence and analyse log data (and supporting information) to identify and counter potential threats to an organisation.

Administration Overheads
By correlating the output from all monitored networks and devices across the enterprise into a centralised location, costs can be reduced.

Security Controls
Most security devices are capable of producing a range of data that is often under-utilised. Dedicated operational staff have the expertise to fully exploit the output from all security devices to achieve the maximum business and security benefit.

Online Services
The ability to make decisions in near real-time is central to delivering a secure online service. Centralised operations can monitor transaction data, analyse it to identify high risk transactions, and help determine the most appropriate service responses.

Cyber Attack Recovery
Your organisation is highly likely to suffer a cyber attack at some point. Centralising decision making, incident response and recovery operations, and working in conjunction with other departments, will all help to reduce the time to recover from a cyber attack.

Security Benefits

Vulnerability Management
A centralised operation can support the compliance monitoring of patching and malware protection, and therefore deliver definitive communication on vulnerabilities and alerts.

Informed Risk Management
Organisations can make more informed risk management decisions when information on vulnerabilities and attack statistics is provided by a centralised operation.

Raised Awareness
A centralised operation can help to raise awareness of cyber security across the organisation, business partners, and third-party suppliers, reducing the likelihood of cyber incidents occurring.

Cyber Incident Management
A centralised operation enables an intelligence-led and consistent approach to cyber incident management across the organisation.

Security Processes
When a centralised team is responsible for delivering the security operation (rather than individual teams spread across the organisation), then security processes are more likely to be repeatable and consistent.

Security Optimisation
Security controls can become less effective over time. A centralised operation allows controls across the organisation to be routinely measured and assessed for weaknesses.

Attack Detection
A dedicated monitoring capability spanning the entire organisation greatly increases the likelihood of detecting attacks and malicious behaviour.

Smarter Defences
Many incidents are preceded by abnormal activity. A centralised operation can assist prompt detection and reaction, and could counter the threat before it becomes an incident. Prevention is more cost effective than dealing with a full incident.

Situation Awareness
More informed threat intelligence and situation awareness can help shape defences and support broader operational assurance activities.

CESG