From Crisis to Recovery:

Solace Cyber's Expert Guide to Navigating a Cyberattack

In the hours and days following a cyberattack, businesses must act swiftly to mitigate damage, recover operations, and prevent future incidents. Here, Solace Cyber offer our key considerations for optimal recovery:

1. Assess and Contain the Breach

To effectively respond to a security incident, it is crucial to determine the scope and impact by identifying the affected systems, data, and users. Once the scope is clear, isolate the affected systems by disconnecting compromised devices from the network to prevent further spread of the issue. Simultaneously, preserve evidence by securing logs, files, and other relevant data to facilitate thorough forensic analysis and support potential remediation or legal actions.

2. Activate the Incident Response Plan

In the event of a security incident, it is essential to follow the predefined steps outlined in your organisation's Incident Response Plan to ensure a structured and effective response. If you haven't created a plan yet, Solace Cyber can assist in its development. Additionally, promptly engaging an Incident Response Team to leverage their expertise in managing and mitigating the incident is vital. Solace Cyber scope of support extends the full breadth of the UK, with teams available for deployment the same day a breach call is received.

3. Communicate Internally and Externally

During a cyber security incident, it is critical to notify key stakeholders, including employees, management, and IT teams, to ensure coordinated efforts and awareness. Legal counsel and compliance officers should also be informed to address legal and regulatory obligations effectively. Additionally, communication with affected customers or partners must be conducted as required by applicable laws and regulations, ensuring transparency and compliance while maintaining trust.

4. Engage Experts

When addressing a security incident, consulting cybersecurity experts such as Solace Cyber is the best step forward as we can provide specialised knowledge and resources to manage and resolve the issue effectively. If the incident involves criminal activity or poses significant risks, involving law enforcement or cybercrime agencies such as the NCSC and Action Fraud may also be necessary to facilitate investigation and potential legal action.

5. Fulfil Legal and Regulatory Obligations

To fulfil legal and regulatory obligations following a security incident, organisations must report the breach to relevant authorities or regulatory bodies, such as under GDPR requirements, ensuring compliance with applicable laws. If required, affected individuals whose data was compromised must also be notified to uphold transparency and meet legal standards.

6. Evaluate and Mitigate Financial and Operational Impact

Most ransomware breaches cost approximately £500K, while smaller email data breaches typically cost around £50K. Evaluating and mitigating the financial and operational impact involves assessing the financial losses incurred and addressing potential liabilities. Interim solutions should be implemented to maintain critical business functions while long-term recovery efforts are underway.

7. Secure the Environment

Your digital environment is a crime scene. It is crucial to leave the environment untouched to allow for a forensic investigation. It is recommended that you engage Digital Forensic specialists like Solace Cyber to secure the environment by addressing vulnerabilities exploited during the attack. This may include patching software and updating security configurations. Credentials may need to be reset, and enhanced monitoring tools deployed to detect any further malicious activity and bolster defences.

8. Restore Operations

The Solace Cyber Incident Response team deploy forensic tools to collect and analyse relevant digital evidence, employing forensic data storage to guarantee the proper preservation of gathered evidence. Additionally, comprehensive digital forensics are conducted by capturing detailed records of system activity through log capture. Restored systems will be thoroughly tested and validated to confirm their integrity before resuming normal operations.

9. Review and Learn

A comprehensive review and learning process should follow, involving a post-incident analysis to determine what occurred and why. Lessons learned should guide updates to your organisation's incident response plan to improve future preparedness.

10. Implement Preventative Measures

Preventative measures should include enhancing cybersecurity defences with tools such as firewalls and endpoint protection. Educating employees about phishing, social engineering, and other threats is crucial, along with conducting regular audits and penetration testing to proactively identify and address vulnerabilities. Solace Cyber is well-equipped to deliver these services and offers tailored solution bundles to meet your specific needs.

11. Maintain Transparent Communication

Transparent communication throughout the recovery process is vital. Organisations should provide ongoing updates to stakeholders, customers, and partners regarding recovery progress, ensuring honesty and proactivity to preserve trust.

Each of these steps should be handled with urgency and precision to minimise damage and restore normalcy as quickly as possible. Solace Cyber can provide a holistic approach to incident response – ensuring full support from initial breach right through to system recovery.

If you want to look at preventative actions or need assistant to handle an existing breach, then get in touch today.

Contact us today:

Email: **cyber.sales@solaceglobal.com** | **Tel: +44 (0) 1202 308 810**

www.solaceglobal.com/cyber

Assured Service Provider
in association with
National Cyber Security Centre
Cyber Incident Response
(Level 2)

Solace Cyber

LEADERS IN INCIDENT RESPONSE

in