Six Actions to Improve Your Organisation's Cyber Resilience Following the Optus Breach

TLP: WHITE

Australia's cyber threat landscape has never been more contested or unstable. In response to client concerns following the Optus breach, CyberCX has prepared this baseline checklist of six actions that every organisation should take to address the key issues arising from that incident as we understand them.

1. Stress Test Your Incident Response Plans

Collate and review your Cyber Security Incident Response Plan, your Incident Response Playbooks and your other crisis management documents.

Your organisation should consider stress testing your existing planning documents with a Cyber Incident Response Exercise involving all parties in your cyber ecosystem, incorporating learnings from real-world incidents, and preparing both your technical and executive leaders for the practical considerations at the centre of a cyber incident.

2. Embed Internal and External Threat Monitoring

The most effective cyber security environments perform continuous monitoring to detect and respond to cyber threats.

Internal monitoring should include logs from critical systems and applications (especially those holding the most sensitive data), activity on servers and user computers, and network ingress points such as VPNs and internet-facing applications. External monitoring should include dark web monitoring for references to the organisation on underground channels and regular collection.

All detections should be responded to quickly and thoroughly by properly trained specialists.

3. Conduct a Personal Information Audit

Review what personal information your organisation is storing, where it is saved, how long it is retained, how it is accessed, and by whom.

What Personal Information is Stored

Ensure that your organisation is aware of exactly what personal information is being stored in your systems.

Location, Location, Location

Personal information is frequently held across multiple systems with varying levels of security.

Most organisations would be surprised at the amount of information stored in development and testing environments, and in email systems and share drives - the "low hanging fruit" locations from which attackers most frequently steal confidential data.

How Long Personal Information is Retained

A foundation of best-practice privacy, and an Australian legal requirement, is that personal information must be permanently deidentified or destroyed when it is no longer needed for business or compliance purposes.

Your organisation should review what data is currently retained and consider limiting what is stored to meet your business and legal obligations.

Understand Access

Ensure that your organisation has clear protocols for who (or which programs) may access what personal information, and under what circumstances. You should be able to understand how you monitor this, and how unauthorised access would be detected.

4. Understand Your Exposure to the Internet

Manage your attack surface by understanding which of your organisation's applications and systems are exposed to the internet.

As you develop or integrate new systems, ensure that they adhere to secure coding guidelines, with a documented security profile. Once deployed, your organisation should regularly validate the security of these interfaces with both automated tools and penetration testing.

5. Review Your Cyber Security Risk Profile

Your organisation should work across your executive and technical leaders to specifically identify your cyber risks and address each specifically to ensure that they have been mitigated – and where this is not possible, that residual risk positions are accepted by the organisation.

6. Elevate your Cyber Hygiene Training and Education

Training and testing staff to ensure that cyber security remains an organisation-wide priority is critical to ensuring that gaps in your cyber defence are avoided, and to increase the likelihood that attacks are detected and disrupted.

This could take the form of phishing simulations, escape rooms, online training modules or face to face training.

Organisations must be vigilant in the wake of the Optus breach.

Those who action these six steps in the coming weeks and months will be working from a stronger, more secure foundation as the cyber threat environment continues to evolve.

If you would like to know how CyberCX can help, please contact your CyberCX Account Manager, or contact us **here.**