NATILIK

Cyber security posture for your **insurance requirements**

Your eight point guide to ensuring a security posture to support your insurance requirements

1. Endpoint detection & response (RDP)

Implemented on all servers, where possible.

2. Multi-factor authentication (MFA)

Required for remote access as well as connections to Office365

3. Privileged access management (PAM) tool

To monitor accounts with access to key assets.

4. Asset management

Inventory of all assets in your environment, including details of all potential security gaps.

5. Security operations centre (SOC)

Monitoring of the network.

6. Local administration rights

Local administrators should have separate accounts for their daily usage and for tasks requiring admin access.

7. Backup procedures

Offline backup or alternative backup solution making it possible to delete existing backups.

8. Employee training

A form of training and/or awareness campaign run for all IT users, at least on an annual basis.

Contact us today to see how we could help you with any or all of these requirements.

hello@natilik.com
www.natilik.com

London
+44 203 597 8000

New York
+1 646 766 8600

Sydney
+61 2 8294 5500