Elmore

ASCERIS

Controls to Prevent Cyber Insurance Claims

Elmore has partnered with Asceris, a cyber security consultancy, to highlight the two main causes of cyber insurance claims:

Business Email Compromise (BEC)
Enables attackers to steal funds via social engineering.

Ransomware Attacks
Encrypting business data until a ransom is paid to unlock it.

There are two ACTIONS every business MUST TAKE:

1. Deploy multi-factor authentication (MFA) wherever possible (across all software applications and services) to prevent threat actors from gaining unauthorised access with only a username and password. Use hardware tokens for privileged accounts to mitigate risks associated with phishing kits bypassing MFA.
2. Develop a patch management programme with your IT provider to make sure that your systems are constantly updated and decommission systems promptly when they are removed from active use.

Tips to mitigate a BEC attack:

Please forward the following recommendations to your IT team or IT provider and request they confirm each of the recommendations is implemented.

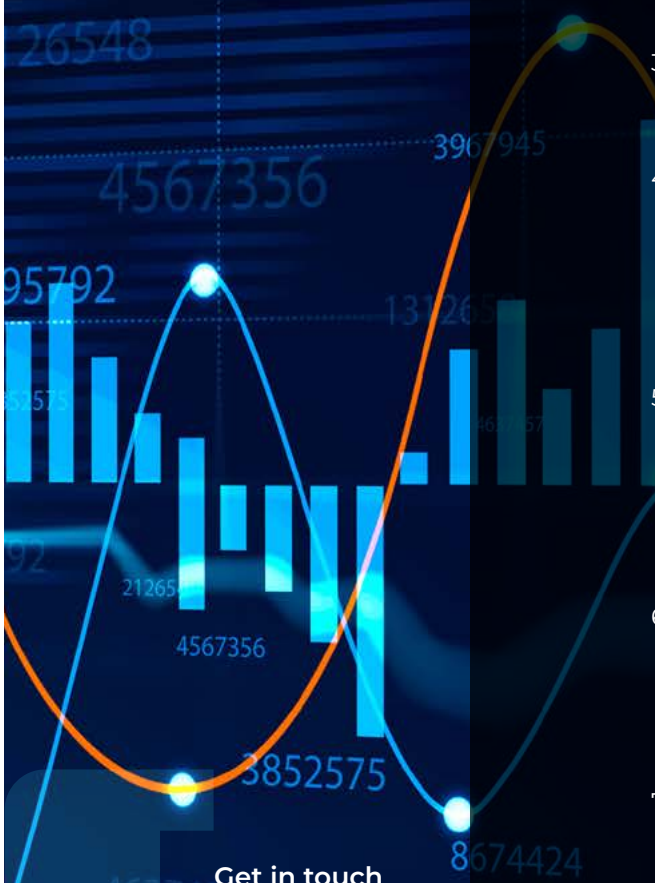
1. Limit access to only approved or enrolled devices (especially for high-risk accounts). Consider the use of physical hardware authentication such as a FIDO2 security key.
2. Use number matching and additional context in Microsoft 365 for multi-factor authentication notifications. The additional context features display the name of the application signing in and the user's location.
3. Prevent users from linking unverified web applications with their email accounts (in Microsoft 365, block third-party consent grants).
4. Prevent email spoofing by implementing the most widely used email authentication methods (SPF, DKIM and DMARC) to limit threat actors' ability to forge phishing and fraudulent emails.
5. Capture and retain logging information to help detect and respond to attacker behaviour.
6. Use custom company branding on sign-in pages so that your users are more likely to differentiate between a normal and a fake login experience.
7. Reduce the sign-in frequency setting to limit the amount of time that a threat actor would have access to a compromised account in the event of an incident.
8. Block direct sign-ins to shared mailboxes which, by default, are permitted.
9. Reduce the risk of MFA fatigue attacks by enabling the fraud alert feature of Azure Active Directory to allow users to report fraudulent MFA push notifications and block the account.
10. Implement cyber and phishing awareness training to help staff to recognise and combat cyber threats, particularly phishing attacks (where fraudsters often masquerade as trusted parties). Social engineering using spoofed domains of trusted contacts provides the threat actor with a human entry vector into the environment by manipulating an employee.

To apply for a Cyber Security Review.

CLICK HERE ▶

To apply for a Cyber Insurance Risk Review

CLICK HERE ▶



Get in touch to learn more about reviewing existing cyber security and insurance arrangements.

Tips to mitigate a ransomware attack:

1. Always ensure that data and systems are backed up offline and regularly tested. Attackers will often attack backups that have been left connected to the company network or systems.
2. Disable Remote Desktop Protocol (RDP). Disable this service if it is not being used. If it is required, consider changing the default port to one other than 3389, and if possible restrict the external IP addresses that can access it. Additionally, consider limiting the users that can log in using RDP and set an account lockout policy.
3. Encrypt your data at rest. This protects your data stored in databases and offline backups from any exfiltration attempts by the threat actor.
4. Detecting incidents early can help prevent the ransomware from being launched. Deploy an endpoint detection and response (EDR) platform to continuously monitor for suspicious activity. Use proactive security measures that create alerts in the event of a breach.
5. Remove admin privileges for standard user tasks. Remove and restrict administrative rights whenever possible, implementing the principle of least privilege. Users should have the minimum necessary rights for any operation type during the shortest duration necessary.
6. Minimise your attack surface and limit opportunities for lateral movement by segmenting the network or implementing a zero-trust architecture. Disable commonly exploited file-sharing protocols such as SMBv1.
7. Set your firewall to block by default. The firewall should be configured to block all ports and/or services by default and allow only those authorised and verified to be legitimate.
8. Conduct regular penetration testing to find vulnerabilities before attackers.
9. Conduct regular cyber awareness training and tabletop exercises to mitigate the human factor.

ELMORE

Elmore is a specialist risk and insurance intermediary offering advisory, broking, and claims management services to businesses from start-up to enterprise.

We provide professional advice and support at every stage of an insurance transaction. We simplify buying processes and make insuring new risks accessible to businesses of all sizes.

Telephone: +44 (0)207 118 1839
Website: elmorebrokers.com
Email: info@elmorebrokers.com

Simon Gilbert - Managing Director
simon.gilbert@elmorebrokers.com

ASCERIS

Asceris was created to be the friendly face that organisations go to for help when they need to deal with cyber incidents and other crisis events.

We use our position at the intersection of cyber insurance and cyber security to collect and share insights, enabling our global customers and insurance and legal partners to reduce the financial and business impact of cyber incidents.

Telephone: +44 (0) 207 873 2278
Website: asceris.com
Email: enquiries@asceris.com

Anthony Hess - CEO
ahess@asceris.com