EXAMPLE Ltd

cydea

CYBER SCORECARD

DATE **November 2020** CONTACT **Michael Mouse** CYBER FTEs **~3** CYBER BUDGET **Below typical** DATA SHARING **UK EU**

ASSESSMENT (Standard profile)

B

This grade suggests the business is demonstrating commitment to the governance and management of cyber risk and ~3/4 of expectations are being met. There are still opportunities to reduce exposure to cyber risk. Recommendations should be reviewed and action plan agreed to continue protecting business operations and investment.

EXECUTIVE SUMMARY

Overall Example has a mature approach to cyber security which would be expected of a company that handles sensitive data as a core part of their business. Cyber security appears to be appropriately resourced, with appropriate headcount and a cost-effective outsourced partner contributing to a 'below typical' spend. Most of the expected operational controls are in place with basic monitoring capabilities in place. The lack of cyber security awareness training raises concerns about social engineering attacks on staff members which could cause unnecessary downtime and financial loss.

RECOMMENDATIONS

PRIORITY: Enable Multi-Factor Authentication (MFA) on all remote access and cloud systems.

PRIORITY: Conduct cyber security awareness training for staff and something specific for board members and finance teams who can be particularly targeted.

PRIORITY: Test backups to ensure they are effective and replacement systems can be rebuilt from them.

Consider additional third party assurance programme for critical suppliers.

Formalise risk acceptance processes to ensure ownership and accountability within 'the business' rather than IT.

STRENGTHS AND WEAKNESSES

Primary changes to cyber driven by change to remote work. This shift, in particular if it involves adopting cloud services, should be accompanied by multi-factor authentication. There are no reported end-of-life technology risk to manage. Security spend is well below expectations, and may need to increase to ensure capabilities are extended to cover the new customer portal (presumed to hold PII).

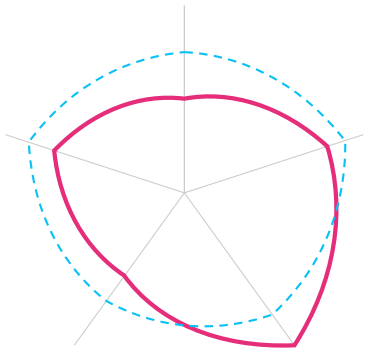
Key:
Your results
Profile expectations

STRATEGY

OPERATIONAL

General cyber hygiene in place, in line with ambition to achieve Cyber Essentials. Basic detection capability in place through self-managed detection suite. High levels of phishing testing with some external audits and assessments against cyber frameworks.

No regular cyber security awareness training in place any staff. Backups are taken regularly but have not been tested for three years. Multi-Factor Authentication only used on VPN.



GOVERNANCE

Regular discussion of cyber security at board level along with monthly reporting. There is evidence that a good set of policies are in place, with updates made recently, for information security and cyber response.

The firm is working towards Cyber Essentials certification which will provide assurance to stakeholders and customers that the basics are in place to prevent common internet threats from phishing and malware.

THIRD PARTIES

A very tech focused view of critical suppliers but not surprising given nature of business. Third parties are currently expected to demonstrate a formal cyber certification.

This is suitable for most suppliers, however bespoke requirements may be required for technical partners delivering the new customer portal.

RISK MANAGEMENT

Good understanding of the 'crown jewels' that need protecting and where they reside. There is regular reporting to the board and a dedicated cyber insurance policy in place.

Policy on risk ownership needs to be agreed and, ideally, should be owned by 'the business' (not technology/security teams).

CYBER RISK EXPOSURE

This section explores common cyber risk scenarios and, based on your answers, we have ranked where we think you may have greatest or least exposure. This may differ from your own cyber risk assessment because you have already implemented mitigations that reduce some scenarios.

Business Email Compromise

Cyber criminals send emails to a finance department employee that look like they are from your CFO, making an urgent request to transfer a large amount of money to an external bank account.

Theft of money is the primary consequence of this scenario if cybercriminals are able to spoof invoices or impersonate senior staff. Cyber awareness training, particularly for executives and key finance personnel, will help staff spot such attacks.

Ransomware

Cyber criminals exploit a known vulnerability in your remote working technology to gain access to your systems and install ransomware that finds your customer database and encrypts it, demanding a significant ransom to make the data available again.

Significant business disruption and unplanned costs are expected with a ransomware incident which would cause significant problems with expectations around zero downtime of key systems. Regular backups reduces impact of such attacks but need to be rested regularly to prove effectiveness.

Personal Data Breach

Cyber criminals find a flaw in one of your online services that enables them to access and download large amounts of sensitive personal information of your customers which they then attempt to sell on, leading to the data breach being made public.

Large amounts of sensitive data increase exposure to regulatory penalties resulting from a data breach. Outsourced security detection and response capability reduce the frequency of successful malicious access. Regular penetration tests also aid in identification and resolution of weaknesses in the perimeter.

Supply Chain Attack

An outsourced IT provider is hacked and the attackers then have access to your data and/or systems as result.

There is a strong reliance on key technical suppliers to store client data securely and consequences of this may manifest as unplanned costs, damaged reputation and, in extreme case, loss of supplier (and associated migration costs).

Malware Outbreak

An employee accidentally clicks on a link in a spam email that downloads and installs malware on their PC that then tries to infect your entire internal network.

Cyber Essentials certification ensures the basics are in place to prevent common, Internet-based threats such as malware. Good endpoint protection in place. Lack of user awareness training puts staff at greater risk of social engineering attacks.

Critical Vulnerability

A customer finds a flaw in one of your public services whilst using it and publicly discloses it on Twitter, meaning you have to patch it before malicious attackers exploit it to steal data.

Regular penetration testing provides assurances around external vulnerabilities and patching is regular with critical patches applied promptly to minimise exposure.

IP Theft

Cyber criminals guess the password of one of your board members and use it to gain access to your computer systems and install their own software that exfiltrates your intellectual property.

Business model is not geared around R&D / intellectual property and value held here is minimal.