Example Ltd cydea

CYBER SCORECARD

DATE **January 2023** CONTACT **Michael Mouse** CYBER FTEs **~0.25** CYBER BUDGET **Above typical** PERSONAL DATA **Shared**

ASSESSMENT (Standard profile)

B

Your assessed grade is 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

Example has a mature risk-driven approach to cyber security with good processes for governance and risk management that will allow the organisation to make informed decisions when it comes to managing cyber risk. The appointment of new detection and response providers and capabilities will help to spot suspicious behaviour and help meet increasing customer security requirements.

Increasing the frequency of cyber security related discussions at the board level will help to reduce blind spots and improve decision making. This will also improve visibility of the organisation's information security objectives, helping with strategic decisions around budget and resource allocation. On the operational side there remain some basic controls that are currently not applied, while activities such as penetration testing and incident response exercises will help identify unknown gaps in the organisation's controls.

RECOMMENDATIONS

PRIORITY: Reduce patching time period for the application of critical security patches on endpoints to <14 days (required for Cyber Essentials).

PRIORITY: Establish a regular (annual) programme of external security assurance, such as penetration tests to, identify any unknown gaps in security controls.

Make cyber security a regular board level agenda item with consistent management information being provided to inform decisions, where necessary.

Conduct a board-level exercise to test cyber incident response plans in a 'crisis' scenario.

Review the need for a cyber insurance policy to help with the financial consequences of a cyber incident.

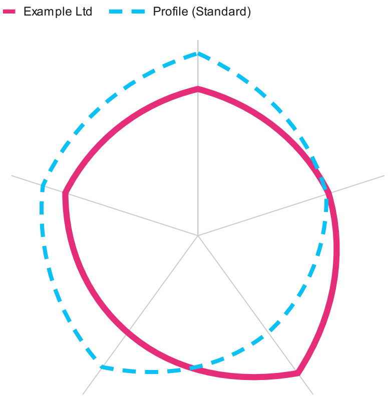
Confirm that weekly backups are tested to ensure data recovery is possible and in a timely manner.

STRENGTHS AND WEAKNESSES

A good understanding of what business changes will require a change in approach to cyber security. Current security spend looks healthy in relation to overall IT budget.

Information security objectives should be tailored to business objectives, such as the migration to the cloud, so that efforts are focused on how best to support the business as it matures and grows. Resource levels are biased towards external support with limited internal resource dedicated to cyber security. As the organisation grows this should be reviewed to ensure the internal resource capabilities are able to deliver the organisation's information security principles.

STRATEGY



OPERATIONAL

The basics are covered with controls such as role-based access controls, multi-factor authentication, and antivirus providing resilience against most common cyber attacks. Mandatory annual cyber awareness training is provided to all staff, and backups are taken weekly.

Patching is currently not in line with Cyber Essentials requirements (<14 days to apply critical security patches). The organisation has not tested its response to a cyber incident in the last 3 years, nor have any penetration tests been conducted in that time. Although backups are taken weekly we were unable to confirm that these are tested to confirm they can be used in the event of data loss. Phishing tests are not conducted on users, and incident detection is done reactively using alerts rather than proactively looking for potential incidents or misconfigurations.

THIRD PARTIES

Critical suppliers and the data shared with them is understood; they are expected to have a cyber security certification. Security contacts are known for some, but not all key suppliers. Having security contacts can help hugely speed up response efforts in the event of an incident.

There is an expectation from customers that the firm will have a formal cyber security certification (currently Cyber Essentials). Personal data is captured and shared with others as part of business activities.

GOVERNANCE

Governance practices are in place, and assurances are provided by Cyber Essentials certification. There is an incident escalation policy in place and the information security policy is regularly reviewed.

Board level discussions happen on an ad-hoc basis, and increasing the frequency on management level reporting of cyber security would help with decision making and allow for faster response to evolutions in threat landscape.

RISK MANAGEMENT

A strong Risk Management process is in place with regular communication of risk profile to both the Board and management group. Critical assets are understood as is maximum allowable downtime, and a data classification system is in place.

There is currently no cyber insurance policy in place to add additional protection against larger risks.

CYBER RISK EXPOSURE

This section explores common cyber risk scenarios and intelligence on the frequency or consequences of these events. It is based on your answers and we have ranked where we think you may have greatest exposure. This may differ from your own cyber risk assessment because you have already implemented mitigations that reduce some scenarios.

Ransomware

The business is a target for cybercriminals due to their sector and IP. Cyber awareness training, along with regular phishing testing and penetration testing, reduces the likelihood of a successful ransomware attack. Severe business disruption, unplanned costs and damage to reputation are the primary consequences of such attacks.

£151,206

the median ransomware payment at the end of 2022. 2/3 organisations do not pay the demands, though other response and recovery costs can be over 15x the ransom demand.

Business Email Compromise

Business Email Compromise is on the rise and as with any organisation that manages multiple invoices from multiple vendors it is important that those with the permission to pay and manage invoices understand how to identify and manage BEC.

£44,619

£44,619, the average loss to Business Email Compromise (aka CEO Fraud), based on data from the FBI and Action Fraud analysed by Cydea.

IP Theft

Having a business geared towards the IP it develops means exposure to IP theft is increased. Regularly reviewing privileged access and updating movers and leavers' access reduces the risk from internal sources, while a good awareness culture and Data Loss Prevention tools also reduce the frequency of attacks from external sources.

2.2x

higher cost associated with data breaches involving theft of intellectual property in 2020. £3.13 million for data breaches, compared to £7 million when IP was stolen.

Hand written by Cydea, and exported 3 May, 2023, with thanks for the input from Rob Watson and Micheal Mouse.