ServiceScaler

INTRODUCTION

LawCover Cyber Risk Assessment

Since January 1st 2018, LawCover has been providing cyber risk insurance for their insured Law Practices at no additional cost to their client's premiums. The policy provides crisis assistance and protection arising from cyber-attacks for losses up to $50,000.

Since the policy inception, law practices have notified LawCover of a range of cyber incidents. They are being targeted by cyber criminals, and incidents have mostly fallen into one of two categories being Ransomware Attacks, and Email-Enabled Impersonation Fraud.

To assist firms to protect themselves further, LawCover have been providing educational materials and guides on understanding the risk factors, including their online Cyber-Risk Assessment

RESULTS

How do you interpret the results?

The cyber-risk assessment is an online form which firm leaders can complete to be provided with a cyber awareness indication result. The result is a graphical representation, not an actual risk assessment result.

The results and tips aren’t specific, but provide a list of items requiring consideration and action if they are not already implemented in the firm. It also doesn’t offer specific recommendations, nor best practices for implementation of more holistic cyber-security solutions, leaving many firms in a position where they need to rely on a third party to analyse, interpret, and make specific solution recommendations to firms.

TAKING ACTION

How do you take action on your result?

To take action on the results and tips, ServiceScaler has put together the below guide with details and recommendations on how to implement or take constructive action on each of the tips as mentioned within the cyber-risk assessment results

These have been broken down into individual categories and components for consideration:

1. Software and Virus Protection
2. Payment Processes
3. Education
4. Control Mechanisms
5. Incident Planning

The requirements and recommendations for each have been placed into the tables below

SOFTWARE

Software and Virus Protection

Requirement	Recommendation*
Antivirus	Webroot SecureAnywhere
Network Protection	Sophos XG Firewall**
Wireless Protection	Sophos Wireless**
Web Protection	Sophos Secure Web Gateway**
Email Protection	Sophos Email**
Endpoint Device Protection	Sophos Mobile

*Or equivalent

**Can be bundled as a Universal Threat Management Appliance such as Sophos SG UTM

SOFTWARE

Software and Virus Protection cont’d

Requirement	Recommendation*
Multi-Factor Authentication	Duo MFA (Cisco)
Security Patch Solution	ServiceScaler Device Agent
Backup Software	Arcserve Backup
Disaster Recovery Software	Arcserve UDP
Backup Hardware (Onsite)	NAS/SAN/Storage Server
Backup Hardware (Offsite)	Portable Hard Drive

*Or equivalent

**Can be bundled as a Universal Threat Management Appliance such as Sophos SG UTM

PAYMENTS

Payment Processes

Requirement	Recommendation*
Confirm Payment Instructions	Two-step, dual mechanism payment details confirmation (Eg, Letter + Phone, Email + Meeting)
Confirm Payment Details Change	Three-step, tri-mechanism confirmation (Eg, Letter + Phone + Email) with acknowledgement

EDUCATION

Staff education

Requirement	Recommendation*
Policies	Develop and implement SOP’s for firm technology users to mitigate cyber-risks
Awareness	Reminder Emails, Discussion Item at Team Meetings
Education	Regular workshops with staff which demonstrate cyber crime attack vectors, what to look out for, and how to handle a potential event.

CONTROL

Cyber security control measures

Requirement	Recommendation*
Passwords	Set regular password reset policies for all users
Vendor Access	Provide supervised, and temporary access to digital systems only
Data Security	Disable or limit the ability for staff to transport any firm data via non-encrypted mediums (Ie, USB, mobile devices, personal emails or storage software)

PLANNING

Planning incident response and action

Requirement	Recommendation*
Disaster Recovery Plan	Develop a disaster recovery plan
Business Continuity Plan	Develop a business continuity plan
Risk Assessment	Regularly complete and update your internal cyber risk assessment which should include both risk areas, and consequences in case of incident

SUMMARY

What Now?

Given the ever-increasing risk of cyber vulnerability, firms must ensure that they are aware of the risks, and have a considered strategy to mitigate the identified risks.

At ServiceScaler, we assist legal firms to not only identify the risks, but provide practical and functional solutions to address these risks.

To find out how ServiceScaler can assist you to reduce your firms cyber-risk, please contact us to speak with one of our legal IT specialists today.

(02) 8188 4740

info@servicescaler.com

www.servicescaler.com

ServiceScaler

For more information, click
Contact Us below

Contact Us