Cybersecurity Insurance Alignment Review (IAR) Checklist

EideBailly
CPAs & BUSINESS ADVISORS

Are you setting out to obtain cyber insurance coverage? Maybe you've been rejected in the past. Either way, Eide Bailly's checklist can help you make sure you're on the right track for approval.

Consider each of the following areas:

□ Is your organization affiliated with any other entities or franchises?

□ Has your organization had a data breach in the last five years?

□ Have any organizations you are affiliated with had a data breach in the last five years?

□ Do you currently or have you in the past had any cyber liability coverage?

□ Does your organization utilize social media? If so, do you regularly review the content and obtain written permission for all images used?

□ Is your network missing any of the following risk management tools?

- Multifactor authentication for remote access and admin/privileged accounts
- Endpoint Detection and Response
- Privileged Access Management
- Cybersecurity Awareness Training and Testing
- Logs and Alerts to Detect Intrusion
- Chip Card Technology for any Payment Devices
- Immutable Backups
- Email Filtering and Web Security
- Hardening Techniques
- End of Life Systems Replaced

□ Does your organization have an incident response plan in place? Has it been tested?

□ Has your organization had any vulnerability assessments (penetration testing, etc.) in the past year?

□ Does your organization have a data retention/deletion policy in place for both print and electronic data?

□ Does your organization have a business continuity plan in place in case of disaster? If so, how often is this tested and how long does full system recovery take?

□ Does your organization encrypt all personally identifiable information? Is personal information encrypted when the information is being transmitted and when information is stored (e.g. mobile devices, laptops, flash drives, etc.)?

□ Does your organization have physical security protocols in place to prevent theft of equipment or printed records?

□ Does your organization partner with vendors? If so, do you have business associate agreements in place? Do those vendors comply with Payment Card Industry Standards?

□ Does any third party store personal information on your behalf?

□ Does your organization conduct background checks on all staff?

□ Is all personally identifiable information restricted access?

□ Do staff members access your network through a VPN? Is that network access tracked and monitored?

□ Do you have a policy in place for how data is managed when a staff member is terminated?

While they may seem like simple yes or no binary answers, there's actually a lot of grey area within them. The way you answer these questions will determine your eligibility for cyber insurance policies. Once you've examined each of these areas, the best course of action is to meet with a cybersecurity professional to discuss your systems and situation before seeking coverage on your own.

What inspires you, inspires us.
eidebailly.com