ADVANCED BUSINESS SOLUTIONS
Strategic IT Partner

Insurance Requirement Checklist

In a review of 6+ Cybersecurity Insurance questionnaires we found that there were some technological solutions that are essential to modern cybersecurity systems. This list will summaries these solutions and provide some context on why they are important in the modern cyber landscape.

- [ ] **Multi-Factor Authentication (MFA)**
  MFA has quickly grown to be one of the most impactful things a company can do to secure their environments. By adding this to your user's authentication process you immediately address common security flaws like traditional password cracking and poor IT hygiene. MFA keychains and Single Sign On are both solutions that make this effort more manageable for many companies.

- [ ] **Next-Gen AV and EDR**
  These two generally go together but the main reason they are important is because they look for and trigger on behavior rather than the old AV's dictionary scans. Most attacks are now conducted via fileless malware which lives off your IT land and harnesses poor practices to spread. Additionally, EDR will be gathering logs about the activity on the network which will be utilized by the Insurance Company's forensic IT team to determine the area of entry and scope of compromise in a cybersecurity incident.

- [ ] **Email Threat Protection and Best Practice Security Protocols**
  Spam filtering has evolved into Email Threat Protection over the past few years by adding more AI and decision making to the filtering process. Additionally, security protocols like SPF and DKIM records all layer additional protection against spoofing and phishing.

- [ ] **End User Training**
  Security awareness training and simulated phishing are commonly required to maintain an effective security posture. These services are often gamified to engage with the employees, but are one of the best ways to protect from technical and general criminal behavior.

- [ ] **SIEM and Vulnerability Management**
  Many underwriters like to know that companies are taking their internal systems seriously by proactively patching and correcting systems that are out of compliance. A Security Information and Event Management system and a Vulnerability Management System are key to knowing what needs attention and how to be accountable for the changes that are needed.

- [ ] **Annual Threat Assessment**
  Many companies are commissioning Cybersecurity Threat Assessments to find out what their security posture is and what they should be prioritizing. These assessments will review best practices, usually a vulnerability scan, dark web reconnaissance, and a risk workshop for the line of business systems that the company depends on. These assessments can be labor-intensive, but they shine a light on the elements that are generally exploited by bad actors.