RISK ASSESSMENT'S IMPORTANCE IN CYBER SECURITY

Risk identification and assessment has been part of business strategy, operational decisions, and other parts of the business for many years.

In looking at the business, risk identification examines and identifies areas of weakness or where the business may be susceptible to competition, natural or man-made disasters and other factors that may impact or jeopardize the continuance of the business.

But risk identification and assessment has not always been part of cyber security planning and budgeting. Yes, the common and well-known cyber threats were considered, and cybersecurity tools were installed. However, if tools protected against all cyber threats, or even the majority, we wouldn't read about new breaches all the time.

In looking at business threats, the identification of competitors is not sufficient. It is necessary to consider their strengths and weaknesses, market presence, how easy or difficult it may be to get people to switch products, opportunities in existing and new markets and other factors. For natural or manmade disasters, consider the area of the country, frequency of the event, and the impact on buildings including flooding and power outages among other factors.

Cyber risk identification and assessment has to go much deeper than just knowing there are viruses and other "bad things." The common attack methods and success rate is a start. But for each cyber threat category consider what it will do to the business if successful. Will it take down one desktop, all the desktops, the servers, or more? Will it be ransomware and lock up all your data making it unavailable? What will it cost to remediate the successful attack? Remember to include the cost of reduced or no business being transacted.

How quickly will your customers begin seeking alternatives? What if you can't order new product, or ship product, or bill for accounts receivable? How long can your business be down before it is no longer viable to continue?

Evaluation of these risks need to be factored into your disaster recovery and business continuity plans.

That should then feed into cybersecurity and IT budgeting and staffing. Without knowing the possible risks and their impact on the business, how can you know if you are allocating budget and staff correctly?

Do not go just by the latest breach to hit the news. Include it in the evaluation but be sure and look broadly. Consider the impact on the business.

Severity of event, probability of event, and impact on the business are the three main factors to consider in planning for cyber security risks.

Want to learn more about cyber security and education, contact AIM Cyber at info@AIMglb.com or call (888) 773-1920.