Cybersecurity Is a Business Issue and Why That Matters to Business Leaders

Traditionally, businesses approached cybersecurity as a technology concern, driven by IT. However, as technology becomes more integral to business strategy, and as cyber-attacks grow in sophistication, cybersecurity requires a more comprehensive approach. Consequently, successful organizations recognize that cybersecurity is a business issue.

Find the Sweet Spot Balancing Cybersecurity with Business Needs

Business executives shoulder responsibility for a broad spectrum of business needs that sometimes conflict. For instance, they must balance productivity and revenue goals with regulatory compliance and the need to protect digital assets. The trend toward remote work, quickened by the pandemic, adds additional complexity.

Technology plays an essential role in all those business goals. But implementing the best solutions requires business leaders and tech personnel to work closely together. For instance, not all data requires the same approach to security. Personal health information (PHI) requires much tighter security controls than marketing data, for example.

Business leaders with an overall view of the organization and business processes are better positioned to establish security priorities. They can also more easily identify what data carries greater potential for harm if breached and where that data resides.

Regulatory Compliance Goes Beyond Tools

One cybersecurity concern that frequently straddles the line between business and technology involves regulatory compliance. Securing sensitive data in accordance with regulations certainly requires technology solutions. But it also requires understanding of business processes and a whole picture view.

For example, any organization that takes credit cards must demonstrate PCI compliance. The IT guy who simply fixes computer issues likely does not stay on top of regulations. However, PCI compliance requires organizations to show evidence of strict processes and controls around handling of credit card data.

Business leaders that do not stay on top of privacy regulations set themselves up for trouble. If a third-party audit uncovers compliance issues, auditors will hold business leaders accountable, not the IT consultants.

Managing Supply Chain Proves Essential

As hackers ramp up their attacks, they frequently gain entrance through the supply chain. Every department, from the factory floor to the sales team, manages supplier relationships. Those relationships need to factor into risk management strategies. For instance, the organization must thoroughly vet both the vendors and the tools they supply.

Additionally, supply chain relationships affect regulatory compliance and logistics. Business leaders find themselves in a better position than an isolated IT department to develop a complete picture of vendors and the risks they introduce.

Technology Does Not Replace the Need for Good Communication

When organizations design cybersecurity from a primarily technology-driven approach, they miss critical human elements. Sometimes, for instance, well-meaning security teams implement solutions that make it difficult for people to access the information they need to do their jobs. When that happens, employees find ways to bypass security measures, introducing risk.

With good communication, however, business leaders can create a security mindset throughout the organization, from the top down. This requires coordination between business and technical elements. It also requires building trust through two-way communication. Leadership must educate employees about risks and security policies and also understand employee needs.

Cybersecurity Is a Business Issue that Requires Investment

To safely navigate an increasingly dangerous cyber landscape, businesses need to begin treating cybersecurity as an investment rather than a cost. Effective security programs can prove expensive. However, with effective planning, implementing the right tools and processes in the right ways delivers a critical return on investment.

In the first place, a solid cybersecurity strategy will prove more cost effective than ransomware recovery. Additionally, keeping systems up-to-date and secure can introduce efficiencies and increase client trust and loyalty.

The business cybersecurity professionals at eMazzanti understand the difficult balancing act required to support business goals while protecting digital assets. They will help your organization drive productivity and revenue growth while meeting security and compliance goals.