How to build a compliant, secure business

ARTICLE 09.18.18 DEAN DORTON

What does a compliant, secure business look like? The reality is that a compliant, secure business is going to look different based on industry, size of business, type of regulatory environment the organization operates in, and the organization's risk appetite.

Each organization has the ability to lay the groundwork for future compliance and security. Simple steps facilitate the building of the desired culture. These include:

- Development of a defined organizational chart.
- Written policies and procedures for key processes and controls to facilitate consistency and continuity.
- Routinely educating staff and leadership on the current regulatory environment for your industry.
- Identifying the key risks to the organization's continuity and business model.
- Defining the organization's risk appetite by specifying what level of risk is acceptable and what level of risk is too high.
- Defining the information technology environment in which the organization will operate.
- Identifying disrupters which may materially impact the operational effectiveness of the organization.

Each of the above elements become part of the whole picture of the organization, and are the foundation upon which a compliant organization should be built.

One area which many organizations fail to consider when establishing the above building blocks are the cyber risks to the organization. As technology becomes more prevalent across all industries, and networked devices become the norm, there is an increased risk of cyber incidents.

As noted in the 2018 IBM/Ponemon Cost of Data Breach report, the average cost of a data breach in the U.S. is $7.91 million, but can vary widely depending on the industry in which you operate. As an example, the cost of a single breached healthcare record is at its highest point ever – $408 per record. The cost includes items such as legal fees, incident response, notification costs, loss of reputation, loss of business, remediation costs, etc.

The reputational harm; harm to your clients or customers and other distractions caused by a cybersecurity incident, can devastate the operations of any organization. Cybersecurity is about maintaining the confidentiality of sensitive information, whether that be healthcare data, manufacturing trade secrets, student, or donor data. Cybersecurity is not just about confidentiality, it is also about maintaining the integrity of your information and maintaining system operations.

Looking to learn more?

Join us for our annual Board Oversight and Risk Management seminar on Wednesday, October 3, 2018 at the Olmsted in Louisville, Kentucky. During the seminar, you will gain a firm grasp of common financial and operational risks that companies and nonprofit organizations are confronted with daily. You'll learn what you need to do, beyond insuring against the risks, to properly identify and navigate the most serious risks threatening you and your

organization. This seminar is ideal for executive nonprofit and private company board members, corporate executives, senior compliance and risk officers, and in-house counsel.

Register Today

For more information on how to build a compliant business, while integrating cyber security and fraud considerations, contact Shawn Stevison or Gui Cozzi at 502-589-6050.

As originally featured in Louisville's Business First