ENTERPRISE RISK AND CYBERSECURITY THREATS - WHAT EXECUTIVES NEED TO KNOW

BY JASON BROWN
CISO, Merit Network

The technological, infrastructure, policy and security landscapes are changing more quickly than firms can keep pace. As the Information Technology field continues to mature, the roles of Chief Security Officers (CSOs) are giving way to the rise of Chief Risk Officers (CROs). Though organizations appoint these positions to oversee and mitigate business threats, ultimate responsibility for organizational risk is the responsibility of executive leaders.

It is critical to an organization's security to define operational roles and policies before the occurrence of an incident. Additionally, corporate IT and leadership must develop a common vernacular to communicate organizational risk and related business impacts when developing security controls and infrastructure policy.

The executive leadership team is responsible for setting the security and IT strategy for an organization. They must interpret risk analysis from their security cabinet in a way that minimizes exposure while achieving organizational goals. The creation and implementation of security frameworks and enterprise policies and procedures are also the duty of executive leadership. Facilitating a culture of end user training, appointing appropriate talent and understanding the implications of a breach, in areas such as revenue, reputation and PII, are additional executive obligations.

> **"It is critical to an organization's security to define operational roles and policies before the occurrence of an incident."**

Chief Security and Chief Risk Officers are liable for the education of leadership and the Board of Directors regarding risks associated with new systems and the re-architecting of existing systems. These roles play an integral part in the development of policies, procedures and the creation of an incident response plan. In addition, CSOs and CROs must dedicate their departments to enabling the vision and strategy of the business in a way which drives risk to an acceptable and efficient level.

Whether your organization needs professional services support with defining and implementing policy and framework, or educating the executive staff and board - Merit is here for you. Merit offers customized workshops to provide your organization with an in-depth analysis of the current threat landscape and an incident response plan, which will ensure that your organization is prepared to address cybersecurity incidents and threats.

Visit Merit.edu/Cybertraining to learn more