Postlethwaite & Netterville

Cyber Awareness is Not Enough

by Geoffrey Smarada

Awareness is not enough.

Over the last month, P&N has provided a variety of insights related to cyber security, including BYOD, Phishing and Employee Education, and the Dark Web. These resources are designed to be informational—providing you with a broader base of knowledge with which to consider the landscape of cyber security. Cyber education and awareness is a great start, but is not enough to keep your organization secure. Ask yourself these six questions related to cyber risk, compliance, and strategy. The answers could help your organization develop a cyber security action plan.

Risk

1. What are your greatest risks and vulnerabilities? Have you had an IT risk assessment in the last 24 months?
2. When is the last time you conducted penetration testing?

Compliance

1. What is your approach to managing IT security compliance?
2. Which regulations apply to your organization? Are you subject to PCI, HIPAA, HITECH, FISMA, GDPR, SOX, or other complex regulations?
3. Is your organization in a highly regulated industry such as healthcare, financial services, government, education, or others? What tools are you using to manage compliance requirements and track regulatory changes? Are these tools inclusive, efficient, and effective?

Strategy

1. Do you have the internal resources you need? Many IT departments have strong internal teams to manage desktop and business-specific responsibilities, but who may not have expertise in cyber security. Can your IT team:

- *Train your employees initially, repeatedly, and effectively?*
- *Implement/update your written IT policy?*
- *Manage/monitor your IT policy?*
- *Identify breaches?*
- *Respond to incidents?*
- *Recover your data?*

Cyber security is one of the greatest threats to any organization. It is not an annual check-up; it requires constant evaluation, monitoring, and education. If you need assistance better understanding or addressing cyber risks, compliance requirements, or strategic resources, contact our Technology Services Group.