Not All Facebook Friends Are Friendly

Cyber security is a much less visible threat, but a very real one. Digital extortion, data breaches and cyber-attacks are now routine occurrences, and with **nearly one million new malware threats released every day**[i], these incidents will likely continue to become more frequent and severe.

Most companies are aware of the risks associated with cyber security, but they may not have considered the risks of staff members on social media. Social media platforms may seem safe at first glance, but entire databases can be hacked with very little information that can be obtained online. Clicking links, liking articles and sharing news are standard social media behaviors, but these actions could lead to the accidental installation of malicious malware. With just a single click, a company's security can become severely compromised.

Beyond potential data breaches, social media also leaves the door open to defamation, privacy issues, liability, copyright infringement and other legal concerns. Staff members may post personal opinions online, but if they are tied to an organization, these posts could damage the reputation of the company, be used in litigation or acquire unwanted attention that could entice a cyber security threat.

Developing a written social media policy is a great way to help limit these risks. To create an effective policy and help guard against cyber crime: define the goal of the policy, explain its importance to those who will be impacted by it, select responsible and educated people to oversee it, develop a plan to implement it and evaluate potential consequences. **A well-developed social media policy may discuss:**

- The creation of an official company social page that will have limited authorized users
- The development of content for the page that will aim to serve the company's mission statement
- How information will be approved and posted for various departments
- Staff guidelines involving requirements for posting about official business or sharing identifying/confidential information
- Computer/device rules (limiting downloading/installing, preventing use of untrusted Wi-Fi connections, etc.)

Providing advanced cyber security training from an IT consultant or expert may prove to be incredibly valuable for the entire company to inform those who are unaware of basic cyber security tactics. **Cyber security training may include:**

- Understanding cyber security (terminology, risks, types of attacks)
- Describing the specific risks that social media poses on security
- Explaining the benefits of making personal social media accounts private
- Understanding the ramifications of sharing racially-focused, political or controversial content
- Implementing a "Bring Your Own Device" policy to limit access and exposures

Companies should also connect with their insurance agents to discuss what types of cyber coverage are available to help protect them in the event of a security breach or issue. Not only can this provide peace of mind, but it can also help protect the company against significant financial loss.

---

[i]Harrison, V., & Pagliery, J. (2015, April 14). Nearly 1 million new malware threats released every day, CNNTech. Retrieved April 21, 2017, from http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/

Glatfelter Public Practice℠
A Division of Glatfelter Insurance Group