BARNES & THORNBURG LLP

Cybercrime & Your Company – Failing To Prepare = Preparing To Fail, Part 2

May 27, 2014 | | Privacy,The GEE Blog

George E. Horn, Jr.
Partner

Continuation of last week's Cybercrime & Your Company - Failing to Prepare = Preparing to Fail, Part 1.

V. If Your Company Becomes the Next Victim

If your company becomes the next target/victim of cybercriminals, personal information of your employees and customers can be compromised. Sensitive and proprietary data can be stolen and sold to the highest bidder, usually one of your competitors. Financial resources can disappear and the reputation of your business can be ruined.

VI. Key Steps to Protect Your Computer System from the Cybercriminal

How can you protect your computer system from a cybercriminal, a digital terrorist, waiting to wreak havoc upon your company? Here are some key tips:

- Ensure your employees set strong passwords, change them periodically and do not share them with anyone
- Establish safe browsing and email habits for your employees and make following these habits mandatory, not a choice
- Be wary of email from unknown senders
- Never open or download an attachment unless you are sure you know what it is and that it is safe
- Be especially wary of unexpected emails from postal or packaging companies
- Establish a strong cybersecurity compliance plan, implement it and update it regularly
- Conduct and document annual refresher training for your employees addressing cybersecurity issues
- Adopt security policies that must be implemented and followed by companies that are allowed to have contact with your computer network

RELATED PRACTICE AREAS

Financial and Regulatory Litigation
Government Litigation
Securities and Capital Markets
White Collar and Investigations

RELATED TOPICS

Cybercrime
Tips

- Ensure that your network security is multi-layered so numerous obstacles will be in the way of any would-be-intruder
- Ensure that every possible entry point in your network is secured
- Identify “weak links” in your network and shore them up tight
- Keep firewalls turned “ON.” They are a key tool in helping protect your network from cybercriminals
- Install and update regularly your anti-virus software
- Install and update regularly anti-spyware software
- Keep your Operating System up to date - these updates are generally put out to stay in tune with new technology and to fill in security gaps that may exist on your system
- Require that users turn their computers “OFF” when finished using them. This effectively cuts a cybercriminal’s connection to your network
- Back up, back up, back up. Your backups should be a snapshot of everything on your system rather than a simple synchronization. A recent backup can help a business recover from Cryptolocker.

Developing a strong cyber compliance plan cannot guarantee 100 percent security for your network, but it can go a long way toward keeping your company, its employees and customers safe from cybercriminals.