ACEC
American Council of Engineering Companies of Massachusetts

Risk Tip 16 – Cyber Risk Management

Provided as a courtesy by the ACEC/MA Risk Management Forum

March 2017

Today's businesses have grown increasingly dependent on networks and digital information, and while technological advancements have helped increase productivity, they've also increased exposure to computer attacks, viruses and the loss of sensitive customer data. Almost two –thirds of U.S. firms report that they have been the victim of cybersecurity incidents or information breaches. Certainly, engineering firms are not immune to the risks faced in other industries.

Engineering firms have reaped the benefits of improving cyber technology. Most firms now utilize digital design software to provide their clients with greater speed, accuracy and creativity during the design phase. Additionally, communication has become universally internet based, as firms communicate with their co-workers, collaborators, and clients almost exclusively through email. There is no doubt that evolving technology has streamlined many facets of the modern engineer's work, but with these benefits come increasing risks.

There are myriad risks posed to an engineering firm in regards to cyber technology. Depending on the structure of your operation and your services offered, you may be more prone to certain attacks against which you may not be fully protected. Some of these risks include:

Extortion- A hacker can completely shut down your business operations for days at a time, promising to restore your network access in exchange for payment.

Social Engineering- A technologically savvy third party can create an email posing as an executive of your company to seek a transfer of funds or access to your network. These requests can be virtually identical to those from legitimate company accounts, so a confirmation procedure must be put into place.

Network and Data Security- Your firm may be liable to third parties if your network is compromised, and personal information is leaked. You may also be held accountable for transmission of viruses, or even blocked access for authorized users.

Electronic Media- Claims can arise from domain infringement, personal injury, copyright violation and libel due to information published on a company website, via email or social media.

As cyber-attack methods have evolved, so too have company safeguards and prevention procedures. It is crucial that your firm has a cyber security policy in place, as it can be a costly and frustrating endeavor to repair the damage after a loss. Company procedures are critical for firms of all sizes, as more than 70% of total cyber-crime in the past five years has targeted small businesses with personal customer information.[1] An uncovered loss can have a devastating effect on both a firm's reputation and finances, as 60% of small and medium size businesses that experience a data breach go out of business after six months.[1] So, what steps should you take to protect your company from a cyber loss?

- Classify data according to usage and sensitivity. Limit access to personally identifiable information on a need-to know basis.

- Limit those with the authority to edit the company website and post on social media.
- Set up a defined chain of command for requested transfers of funds.
- Educate your entire staff to recognize and avoid "phishing" emails.
- Ensure that all company computers have up to date anti-virus software.
- Enact a strict password protection policy, and ensure combinations are updated regularly.
- Have a protocol to restrict access in the event that an employee leaves or is terminated.
- Use battery backup and surge protectors to protect against electrical issues.
- Regularly backup data to an off-site location, if possible.
- Maintain an emergency response plan, including specific employee actions in the event of lost or stolen data.
- Consider hiring an outside IT consultant to evaluate your specific risks and responses.

While these safeguards will certainly reduce your likelihood of suffering a cyber loss, you should also consider a contingency plan. Cyber Risk insurance policies cover damages to both third parties (your clients and colleagues) as well as losses suffered by your firm. There is still some variance in cyber policies, but most policies will include these stock coverages:

- Network and Data Security: Network security liability refers to liabilities that result from the breach of an electronic network. A network breach occurs when someone a) gains access without authorization b) transmits a virus to the network c) prevents an authorized third party from accessing the network. Information can be deleted or altered to incur a claim; dissemination is not the only pathway to liability.
- Electronic Media Liability: This agreement affords coverage when the insured incurs liability in conjunction with material published on its website or social media profiles.
- Extortion Demand: Reimbursement for reasonable expenses incurred by the insured entity to respond to a network extortion or demand.
- Business Interruption and Extra Expense: Covers funds lost as a result of a cyber breach that limits your firm's ability to conduct business.
- Loss or Damage to the Insured's Network: Covers restoration costs of files, data, and systems to pre-breach levels after a cyber loss event.
- Basic E-Theft: Provides first party defense coverage for money, securities, or goods that are stolen through a network breach or hacking event. (Note that Social Engineering risk is usually covered as an endorsement to a crime policy.)

No firm can be truly insulated from technological attacks, but through a combination of preparedness and risk management, you can greatly reduce your firm's likelihood of becoming a cyber victim.

This ACEC/MA Risk Tip is intended to provide current and accurate information to assist the reader in becoming more familiar with the subject matter. It is informational only and not intended to substitute for technical, legal, or risk management professional advice. The reader is encouraged to consult with an attorney or appropriate professional consultant to explore this information further.

For more information on the ACEC/MA Risk Management Forum or on other ACEC/MA activities, call 617-227-5551 or go to: www.acecma.org.

1. Creating a Cyber Security Culture in Your Business. (2016, January 19). Retrieved March 13, 2017, from https://www.paychex.com/article/human-resources/creating-cyber-security-culture
Note: Statistics from National Cyber Security Alliance.