National Association of Home Builders

Cybersecurity – What You Need to Know[1]

What is cybersecurity? Cybersecurity is the protection of computer systems, mobile devices such as phones and laptops, computer networks, and other systems holding data from unwarranted, illegal or malicious access.

You may think that as a small business, no cybercriminal would ever attack you. You might ask why anyone would choose to target your company. But cybersecurity should be of concern to every business, regardless of size. Indeed, the smaller your business, the more vulnerable you may be.

Ask yourself these questions:

- Do you store important business information on a computer or other device connected to the internet?
- Do you ever share important information by email?
- Do you use your computer to pay invoices?

If the answer is "yes" to any of these questions, then you really should read on, because you probably need to take steps to protect important, electronic information.

Cyberattacks continue to grow in number and sophistication. Therefore, it is imperative to consider the potential risks to your business. The risks include:

- Ransomware attacks, which are common in the homebuilding industry. This occurs when cybercriminals hold access to data and computer networks hostage in demand for payment of money.
- Cyber criminals may also attempt to hack into your networks or computer systems, potentially exposing you to loss of your operating funds, interruption of your business, and work delays. This in turn may create liability to third parties such as customers.
- Hackers might also steal your customer data or your proprietary information such as building designs or bid data.
- With the advent of computerized work technology, hackers may even interfere with a project and cause bodily injury and property damage through the use of remote access systems.

Therefore, if you have not already, you should take proper measures to prevent any cyberattacks and mitigate any potential risks.

In order to do so, consider the information in your business that needs to be protected. It may include:

- Intellectual property (such as blueprints, schematics, patents) and licenses

[1] Developed with assistance from Philip R. Stein, Esq., Bilzin Sumberg, 1450 Brickell Avenue, 23rd Floor, Miami, Florida 33131. Mr. Stein may be contacted at pstein@bilzin.com.

- Material pricing
- Bid data
- Bank records and other financial information
- Employee information (including private health information)
- Customer data

Once you have identified these assets, you should identify the technology that stores or processes this information. This technology may include emails, cloud storage, websites, computer network systems, laptops, cell phones.

Once you have identified technology, ask yourself this question: Do you have a system in place to manage access to your business information and assets? This system should include:

- Securing the information transmitted/received and stored as follows:
  - Protect your network by establishing firewalls
  - Update virus protections software/security programs
  - Consider using web and email filters to block users from inadvertently visiting malicious websites or receiving email from malicious actors
  - Secure wireless access points to ensure that only authorized systems connect to the network and that communications between devices are encrypted and not able to be seen by others
  - Encrypt sensitive data
  - Patch operating systems and applications
  - Use multi factor authentication, whenever available
  - Backup critical data and applications regularly

- Making sure each employee has unique passwords and/or accounts to ensure accountability for their actions

- Limiting the number of users and/or limiting access to information to only users who require the information for business purposes

- Training employees on a regular basis about best practices. Employees should understand cybersecurity expectations for protecting your business and be presented with the company policies on cybersecurity for them to sign-off on. Training should be updated on a regular basis. This training may include:
  - How to recognize and avoid data breaches/attacks
  - What to do if an attack or breach is suspected
  - What not to do if an attack or breach is suspected
  - Passwords – are you changing passwords often and not reusing them?

- Using an outside IT firm to do a security audit, test security, and create security plan

- Creating response and recovery plans. What will you do in those cases to ensure that the business keeps operating in the event of a data breach or cyber-attack?

In addition to putting a system in place to secure private and/or sensitive data, business owners should consider cyber insurance in order to minimize and transfer the risk of any potential losses. There are several types of coverage:

- Data breach expenses
- Cyber Ransomware
- Business interruption
- Fraudulent wire transfer
- Tech Errors & Omissions

Another way to minimize and transfer the risk of loss is by reviewing your contracts with non-employees such contractors, subcontractors, architects, vendors, etc. and determine whether it is necessary to include provisions in those contracts that will safeguard your private information. Such provisions may include:

- Approval of any cloud-based project management planforms and file sharing platforms, including how information is stored and disposed of
- Creation of a uniform and secure method of data transmission and file sharing
- Prohibition against the use of unsecured file-sharing platforms
- Mandatory and routine data security training for any one on their projects with access to project data
- Insurance requirement for all losses and damages arising from data security incidents of any kind, from breaches to accidental losses.

In conclusion, every small business wants to minimize the risks that might harm their ability to continue operating, cost them money or damage their company's name and reputation. Therefore, it is important to understand cybersecurity and take to mitigate risks and provide a way to recover from any cyber threats.