National Association of Home Builders

NAHB OVERVIEW AND CHECKLIST TO ASSESS CYBER RISKS[1]

I. Most Common Cyber Risks in the Home Building Industry

a. Ransomware attacks
   1. Third most common industry to experience ransomware attacks in 2021

b. Fraudulent wire transfers

c. Business interruption and liability for delay

d. Breach of Intellectual Property (IP)

e. Breach of Bid data

f. Breach of confidential information

g. Liability to third parties as a result of breach

h. Unauthorized access and interference with project

i. Bodily injury and property damage through failure of remote access systems

II. Data Targeted by Hackers

a. Intellectual property (e.g., blueprints, schematics, patents) and licenses

b. Material pricing

c. Company financials

d. Bank records and other financial reports

e. Employee information

III. Sources of Cyber Threats

a. Human error
   1. Large number of individuals involved in a project can lead to errors

b. Employees
   1. Remote work
   2. Former employees
   3. Lost or unsecured devices

c. Phishing emails

d. Cyber attacks

e. Infected downloads, attachments, USBs

f. Weak passwords

g. Connecting to Wi-Fi

h. Cloud storage: Are you using cloud-based software such as Procore or Prolog to store and transmit information?
   1. Is that information encrypted?
   2. Do you know the security protocols for the vendor?
   3. Do you know the vendor's policies for notifying you if there is a problem with your data?
   4. Do you back-up the data on the Cloud to a local network to mitigate risk of loss from ransomware, etc.?

[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.

IV. Data Inventory Checklist: what is vulnerable, and what are you doing to secure what you actually have?

a. Types of confidential/sensitive data stored (i.e., payroll, architectural designs, schematics)
   1. Do you have employee health information that might require extra levels of protection?
   2. Are you isolating the confidential/sensitive/personal data you have, and limiting the number of people who have access to it?

b. Types of data collected/transmitted

c. How do you receive the data (i.e., Building Information Modeling, Integrated Project Delivery and file sharing)?
   1. What file sharing are you using?
   2. What are the vendor's protections?
   3. Are you under a contract with the vendor and do you understand its terms?

d. Who has access to the data?

e. Where is the data stored?
   1. Are you storing on site in a trailer or strictly on the Cloud?

f. Determine whether there is a need to continue collecting or storing information

V. Securing the Information Transmitted/Received and Stored

a. Physical security of data

b. Electronic security (including email and Cloud security)
   1. Establish Firewalls
   2. Update virus protections software/security programs
   3. Encryption sensitive data
   4. Continued patching and updates to software
   5. Multi factor authentication
   6. Backup critical data and applications

c. Consider hiring outside IT firm to do a security audit, test security, create security plan

d. Restrict access to data to only necessary individuals

VI. Policy and Protocols

a. Do you have written policies?
   1. Are you actually following your written policies?
   2. Why is it important to actually follow policies?
   3. If you do have policies, do they make sense for the size of your business?

b. Separate policies for employees, customers, and third parties (including contractors, professional designers, vendors, etc.)
   1. What are the basic policies everyone should have?
   2. Acceptable use, mobile use, personal use of devices, etc.

c. In-house document retention and disposal of data policy
   1. Is there a different policy for personally identifiable information (PII) and/or confidential information, as opposed to other types of information and documents?

d. Breach response plan
   1. Create response team both internal and external
   2. Address business continuity/contingency plans
   3. Consult with insurers to discuss coverage availability
   4. Consult pertinent contractual obligations
   5. See sample from Sedona Conference – we can create a different plan for a smaller organization using this as a template

e. In-house breach notification plan
   1. Breach notification laws

VII. Employee Training

a. How to recognize and avoid data breaches/attacks
b. What to do if attack or breach is suspected
c. What not to do
d. Passwords – are you changing passwords often?
e. Are you offering training?
   1. What are the training options available?
   2. How often must you reinforce training?
   3. Are you running background checks on employees before you permit them to be exposed to sensitive information?

VIII. Cyber Insurance

a. Types of coverage
   1. Data breach expenses
   2. Cyber Ransomware
   3. Business interruption
   4. Fraudulent wire transfer
   5. Tech Errors & Omissions
   6. Understanding policy coverage and policy exclusions

IX. Contractual Provisions with Non-employees

a. This applies to contractors, subcontractors, architects, vendors, etc.
b. Approval of any cloud-based project management planforms and file sharing platforms, including how info is stored and disposed of.
c. Uniform and secure method of data transmission and file sharing
d. Prohibition against the use of unsecured file-sharing platforms
e. Mandatory and routine data security training for any one on their projects with access to project data
f. Require insurance for all losses and damages arising from data security incidents of any kind, from breaches to accidental losses.