Checklist – Data Security and Responding to Ransomware Threats[1]

1. Data Security Overview Facts
    - Data is collected because it's important and potentially valuable
    - It's collected electronically to make it more valuable (more easily accessible, more usable, and more easily transferred to others)
    - Volume of data collected and stored is increasing exponentially
    - Types and uses of electronic data for builders include stored project specifications, financial data, predictive analytics/productivity assessments, employee/staff/crew information
    - The value of the data builders collect and store makes them attractive targets for hackers and cybercriminals.

2. Key Data Security Considerations for Builders
    - Access to company data—who needs access, who has access, and what level or extent of access do you want people to have?
    - Admin rights on company computer systems – who has rights? How easy is it to change those rights? How good are the system administrators at ensuring the safety and security of company data and electronic records?
    - Mobility – need a plan and a policy (preferably a written policy for how you, your staff and your crews are going to use mobile devices for company work and on company time.
    - Training – are you training your team to meet your expectations regarding keeping data secure and safe?
    - It's strongly recommended that builders implement dual-factor (or "two-factor") authentication. This means that if you're logging in via a desktop or laptop you will receive a prompt on your mobile device to verify that you are an authorized user of the company's computer network.

3. Identifying Threats and Malicious Attacks
    - Spear phishing – victim receives an attachment or link that they click on
    - Drive-by – attacker exploits a vulnerability in the web browser or a related application
    - Exploitation – attacker gains access to a remote system and installs spyware or ransomware that replicates itself on the victim's system
    - Valid accounts – insider jobs in which someone with authorized access makes improper personal/criminal use of company data

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

4. Ransomware Attacks and Best Practices for Responding
    - Ransomware is a sub-category of malware. It is designed to encrypt (lock) files on a device or computer system, making those files unusable for the people who need them
    - Ransomware criminals often threaten to sell or leak data/files or authentication information if the victims don't pay a ransom
    - Important to have an incident response plan in case you are ever victimized in this way
    - Have a "playbook." Who on your team is responsible for what if an attack of this type occurs?
    - Speak with IT professionals about how to identify ransomware on your systems before files start getting encrypted
    - Also learn about containment – how to limit the damage when an attack is in progress
    - To pay or not to pay? Most authorities, including the FBI, recommend NOT paying the ransom that is being demanded. Among other problems with paying, you don't even know that you will get the files back as promised, and your payment might encourage hackers to attack you again in the future
    - There are often alternative means of getting data back (without paying the ransom). Some groups, including the "No More Ransom" project have "decryption keys" that they may be able to share. In addition, many governments and law enforcement agencies can provide guidance on responses and recovery of data
    - Post-attack, are you able to scope the incident thoroughly to understand what happened, what systems were affected, and prevent this from happening again?
    - Recovery – are you able to take the necessary steps after an attack to get things back to normal as quickly as possible?