HEIGHTENED CYBER SECURITY RISK:

What This Means for the CRE Industry

Cybersecurity is a broad term that encompasses many different elements.

For years, retail, healthcare and financial services cyber-attacks have received a great deal of attention. But the same issues exist for all businesses. And now the commercial real estate industry is starting to feel the same pressure on their organizations. This is driven by the recent boom in CRE technology, IoT (the Internet of Things), the emergence of smart buildings, and the amount of data that all these different systems are collecting and exchanging in today's real estate organizations. Even though the CRE industry is well-aware of cybersecurity risk, many are still unclear on what components drive cyber risk and how to protect organizations from the threats associated with it.

This guide provides an overview of some common cybersecurity risks that the CRE industry faces today, and how organizations can address and protect themselves from these concerns. As a leading technology provider, it is Building Engines' intent to supply CRE professionals with helpful information on cybersecurity to help make the industry a safer place for everyone.

THREE DRIVERS CAUSING HEIGHTENED CRE CYBERSECURITY RISK

#1: INTERNAL CYBERSECURITY RISK

One of the biggest drivers of cyber risk is a company's own employees. This makes sense since companies have multiple employees, each with access to different technologies that expose organizations to risk. The more employees, the greater the risk. Even though this is the simplest problem to understand, it's arguably the most difficult to solve because solving it requires continuous education and managing human behavior.

Mike Mullin, CEO at IBS described this challenge as the "last inch" problem - the last inch being the distance between the finger and the mouse before someone clicks on a potentially dangerous link. Such links can install Malware that operates in the background recording keystrokes and capturing information and potentially sensitive data from businesses. This is also the way that Ransomware is installed. Ransomware operates by locking down access to critical data or parts of systems until a ransom, usually in the form of an untraceable bitcoin payment, is made to the cyber-criminal.

In fact, the infamous WannaCry ransomware attack snuck in via email infecting over 230,000 computers with an estimated loss of $4 billion. Ransomware is said to be one of the most profitable criminal business models in malicious computer software. According to KnowBe4, there were over 40,000 attacks per day with ransomware hiding in over 40% of all email spam last year.

Tip: Protect Against Malicious Email

With employees receiving hundreds of emails that contain dangerous links, it's difficult to control what gets clicked on. The best way to combat this problem is education. CRE organizations should be educating employees through new employee onboarding programs and continuous education on this topic. These programs should enforce lessons such as:

- The four most common actions that cyber criminals want you to take are:
    1. Replying or unsubscribing to an email
    2. Clicking a hyperlink in the message
    3. Opening an attachment from the email
    4. Forwarding the email to others

- What traits of an email address to look for when determining if it's malicious. KnowBe4, the world's largest security awareness training platform, suggests looking at red flags such as:
    - **The "from" email address:** If the email is from a stranger, that's a red flag, or if the email address looks like it is from someone you do know but the email content is out of character. Tip: hover over the email address to check if it is a legitimate address.
    - **Email date:** Receiving an email that you would usually get during business hours late in the evening or on a weekend.
    - **The "to" email address:** Check the list of other recipients. If you don't know the other people on the email or the email was sent to a group of people from your organization that all start with the same letter for their last name, this is suspicious.
    - **Subject line:** Look to see if the subject line is irrelevant or doesn't match the content. Also, if the subject line is covers something you never asked for or something you know nothing about, this is a sign that it's malicious.
    - **Body of the email:** If the sender is asking you to click on a link or open an attachment, you should be on alert.
    - **Links in the email:** Beware of any links within emails.
    - **Attachments:** any attachment is a red flag. Typically, the only file format that is okay to open is a .txt file.

Tip: look closely at any links within suspicious emails. Hover over links to see if the address is legitimate. Sometimes cybercriminals use fake links that look similar to legitimate links to trick you.

- Use internal "Phish Tests," including:
  - **Monthly Phishing Campaigns** to test employees and help keep them alert and trained on how to identify phishing attempts, what to do if they find a phishing scam, and techniques for protecting the business against such attacks.
  - **Phishing Tools** that monitor and provide reports on how susceptible companies are to attacks.
  - **Regular Phishing Trainings** that teach employees basic network security such as password strength training.

#2: CONNECTED SYSTEMS LIKE IOT AND SMART BUILDING TECHNOLOGIES

The poster child for a cyber-attack of this type is the infamous Target breach in 2013 that occurred via an outsourced HVAC contractor. The problem was attributed to a lack of data network segmentation. The contractor installed an infected monitoring system on the same network that Target used for their point of sales system, where all the credit cards were stored. This unfettered access to 70 million records cost Target $18.5 million in restitution and millions more in market and reputation value.

With the advent of IoT and networked sensors on major systems in CRE, the opportunity for similar breaches and access to sensitive building, organization and tenant information is at risk. When these IoT devices are set up improperly they provide an easy entry point for hackers to access other networks within your organization.

According to a report by BOMA International, the smart building market is growing annually at 31.5% and will be valued at $58 billion in 2023. The more that smart building and IoT technologies are woven into commercial real estate, the more susceptible the industry is for cyber-attacks, even including cyber terrorism.

Many building owners and managers are still unaware of how great the threat and cyber risk that IoT and smart building technologies are creating, and the ones that do understand the threat don't know what to do about it. As these technologies become more complex it will get even more difficult to manage these cyber risks.

Tips: Protecting Against Common IoT and Smart Building Cyber Risks

HERE ARE A FEW TIPS THAT WILL HELP KEEP YOU PROTECTED:

- Improve and continuously update network security
- Put protocols in place for monitoring and protecting computers and networks
- Require stronger credentials to log into software and other technology solutions
- Disable unused features in tools to reduce cyber risk gaps
- Regularly backup systems
- Lastly, perform-cross functional training for all teams within the organization

It's not only one person, or team's, responsibility to protect organizations against cybersecurity; the whole company needs to work together as one team. CRE organizations need to become more educated and proactive when it comes to cybersecurity. Acting as one unified team, rather than soiled departments, to create a company culture that is aware of cyber risk is the right start for CRE companies to protect themselves from threats.

#3: SAAS APPLICATIONS

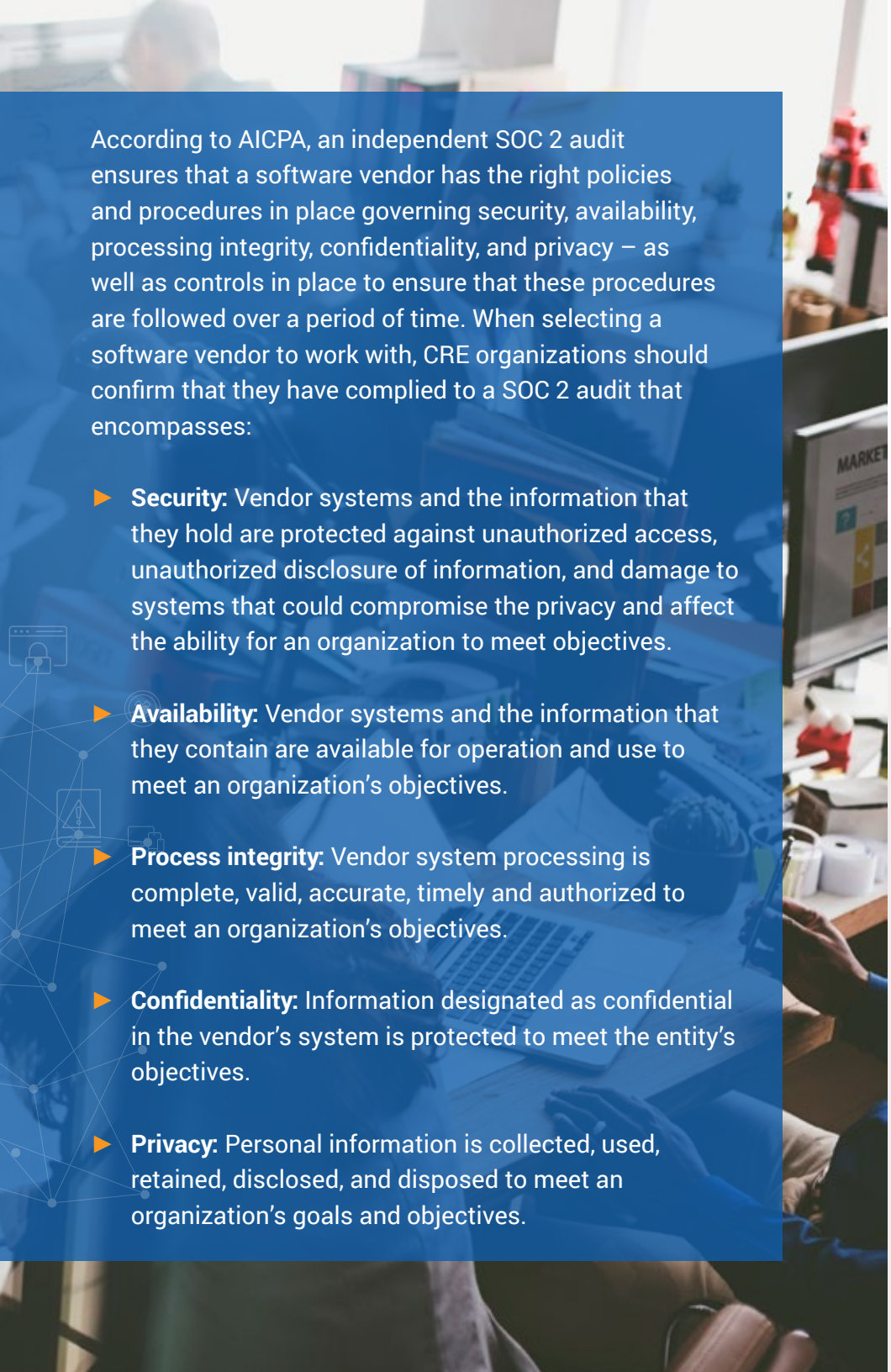
Cloud-based software applications have many of the same cyber risks as software installed and managed on-premise. But the big difference is that where you can control what happens within your firewall, in general you cannot directly control what a SaaS vendor does since they are an independent organization. But you can ensure that the SaaS vendor does meet your security requirements. That's where SOC 2 comes in.

Tip: Protect Your Company by Using SOC 2-Compliant Vendors

The AICPA overseen SOC 2 audit is a common compliance requirement attesting that a service provider's (such as a SaaS software provider) information security practices, procedures, and operations meet SOC 2 standards. It's specifically designed to ensure the vendor is following strict security procedures so that their customers' data is secure.

Ensuring that your software vendors are SOC 2 compliant is critically important for publicly-traded REITs, medical office facilities associated with healthcare networks, and financial services organizations that need to comply with industry-specific regulations. But it is also extremely valuable for any company that needs to ensure the integrity and security of its data.

One of the challenges that the CRE industry faces is that many times vendors and products are not assessed regularly on their cybersecurity and data protection practices and policies. Another issue we see is that owners and managers don't fully examine contracts with their vendors to see who has access to the data created and stored by the software. This is important for any CRE organization that uses software to interact with their tenants. When you use operations software or any type of tenant engagement software, you are exposing not only your company to cybersecurity risk but also your tenant's information. CRE organizations should ensure that all software vendors they rely on to store important customer data are SOC 2 compliant.



According to AICPA, an independent SOC 2 audit ensures that a software vendor has the right policies and procedures in place governing security, availability, processing integrity, confidentiality, and privacy – as well as controls in place to ensure that these procedures are followed over a period of time. When selecting a software vendor to work with, CRE organizations should confirm that they have complied to a SOC 2 audit that encompasses:

- **Security:** Vendor systems and the information that they hold are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the privacy and affect the ability for an organization to meet objectives.
- **Availability:** Vendor systems and the information that they contain are available for operation and use to meet an organization's objectives.
- **Process integrity:** Vendor system processing is complete, valid, accurate, timely and authorized to meet an organization's objectives.
- **Confidentiality:** Information designated as confidential in the vendor's system is protected to meet the entity's objectives.
- **Privacy:** Personal information is collected, used, retained, disclosed, and disposed to meet an organization's goals and objectives.

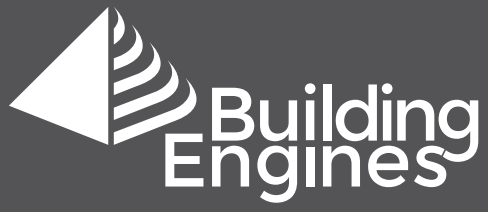
If you aren't checking to make sure your vendors are SOC 2 complaint you are opening your organization up to cyber risk and others, and potentially exposing yourself to threats against the data that vendors are collecting and storing.

With the CRE tech sector expanding each year, the threat of cybersecurity will only become greater. In the past it seemed that cybersecurity only presented a risk against industries such health care or finance but with the emergence of new technologies, the CRE industry is facing these same threats now. Arm your organization against cyber risk with the tips in this guide.

ABOUT BUILDING ENGINES:

Building Engines is a leading cloud-based provider of property management software for operations teams at commercial office, medical, retail, and industrial real estate properties. Building Engines has been SOC 2 compliant since 2015 and works with hosting providers that are SOC 2 compliant as well.

For more information visit: www.buildingengines.com



BUILDINGENGINES.COM
866.301.5300
INFO@BUILDINGENGINES.COM