INSIGHTS FROM THE BDO REAL ESTATE AND CONSTRUCTION PRACTICE

Real Estate and Construction Industries' Growing Cybersecurity Threat

In the last few years, real estate and construction leaders have made great strides to implement new technologies into their regular practices. While these advances have uncovered additional efficiencies, their adoption has created a critical vulnerability: data security.

Cyberattacks are on the rise, with a **22% increase** in major attacks year over year, according to the Verizon Mobile Security Index 2022. Given the wealth of personal information they hold, real estate and construction companies are particularly attractive targets for these attacks and should take steps to safeguard their data. Whether training its workforce to follow data management and **cybersecurity best practices**, improving security software or establishing data backup plans, each measure assists in building a more secure digital environment for a company's data and may help safeguard their reputation and the safety of their customers, employees and residents.

CYBERCRIMINALS THREATEN AN INDUSTRY'S SAFETY AND SUCCESS

Construction companies have been particularly susceptible to cyberattacks, in large part because cybercriminals are aware the industry is under-protected. This is supported by a **2022 study by KnowBe4** which used simulated phishing techniques to demonstrate that wide-net cyberattacks like email phishing scams have been particularly effective in targeting the construction industry. As a whole, construction views cybersecurity as a lesser business priority: Just 64% say it's a high priority versus 77% of businesses overall, according to the KnowBe4 study.

The **real estate and construction industries** are not unlike others in that the COVID-19 pandemic forced them to replace in-person tasks with their virtual equivalents. Unlike other industries, however, construction has had more ground to cover to catch up - it is widely understood to be a laggard in terms of **digital transformation**. The adoption of new technologies has helped companies achieve higher productivity by automating time-consuming administrative processes, simplifying communications and streamlining data management. To remain competitive, real estate and construction companies will need to continue to utilize these technological advances.

However, these new advances often come with more interconnectivity. Unfortunately, the more connected devices and software a company relies on, the more access points hackers can use to infiltrate that company's cybersecurity system. Many industry leaders are concerned that mounting attacks are not being met with adequate security measures. According to a study by Venafi, **82% of CIOs** believe that their software chains are vulnerable to cyberattacks.

Webinar: Cybersecurity Guide for the Board

DON'T DISMISS DUE DILIGENCE FOR YOUR THIRD PARTIES

In addition to potential vulnerabilities arising from software interconnectivity, external vendors or third parties may add new cyber risks. Whether hiring a contractor, a new vendor or working with a new client, companies should thoroughly assess each third party's own cybersecurity measures, as they could by extension be inadvertently exposed to vulnerabilities. Some considerations include:

REQUESTING AN INTERNAL REPORT

Determine whether a third party has undertaken its own cyber security measures by requesting it produce an internal report. For example, the third party can undergo audits regarding the secure management of data by producing an SOC2 report, which assesses five "trust service principles": security, availability, processing integrity, confidentiality and privacy.

ASSESSING CYBERSECURITY MEASURES

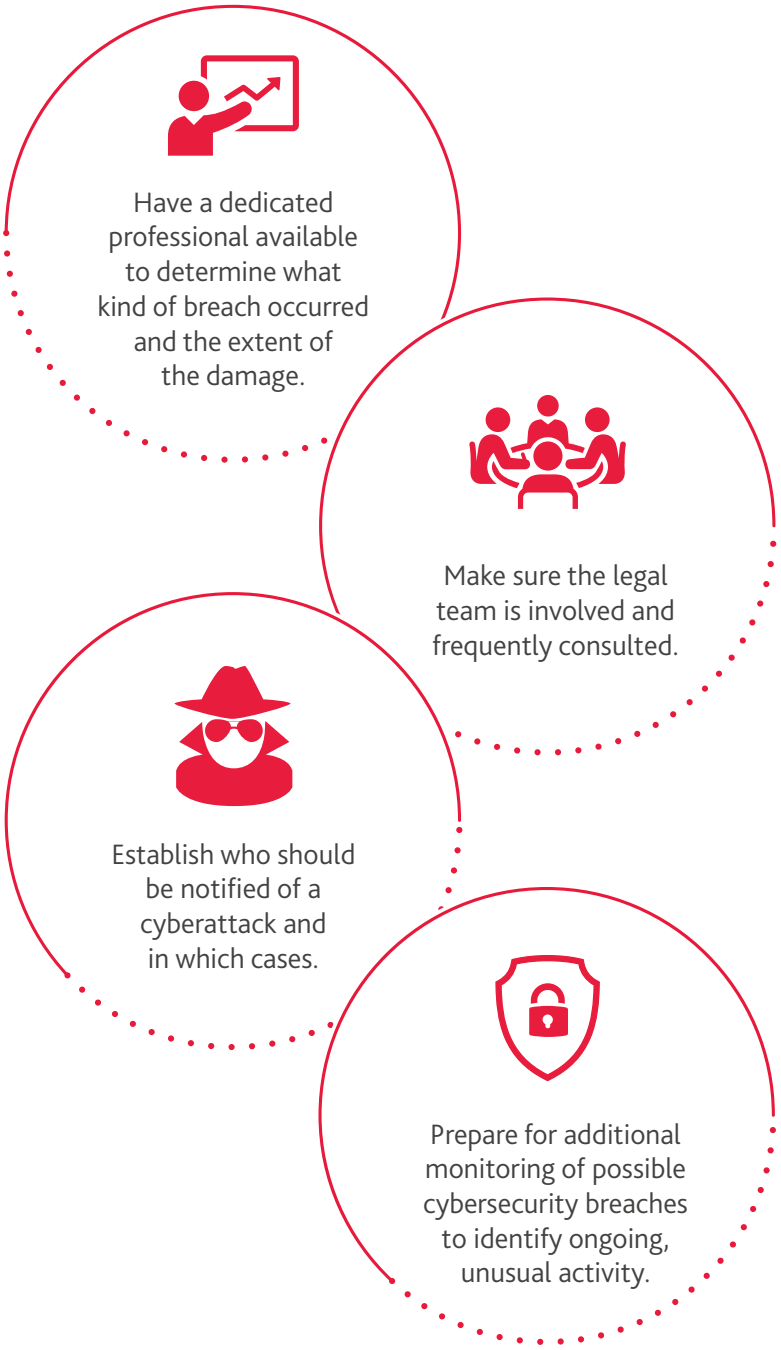
Determine whether a third party independently tests its operations, holds insurance against cyberattacks and follows best security practices, such as multifactor verification and unique login identification.

When working with a **third-party cybersecurity provider**, having established roles and responsibilities is paramount. If an organization is a victim of cybercrime, for instance, determining whether data backup will be performed in-house or outsourced to a security provider can speed up the recovery process.

PROTECTING YOUR ORGANIZATION AGAINST "CYBER THREATS"

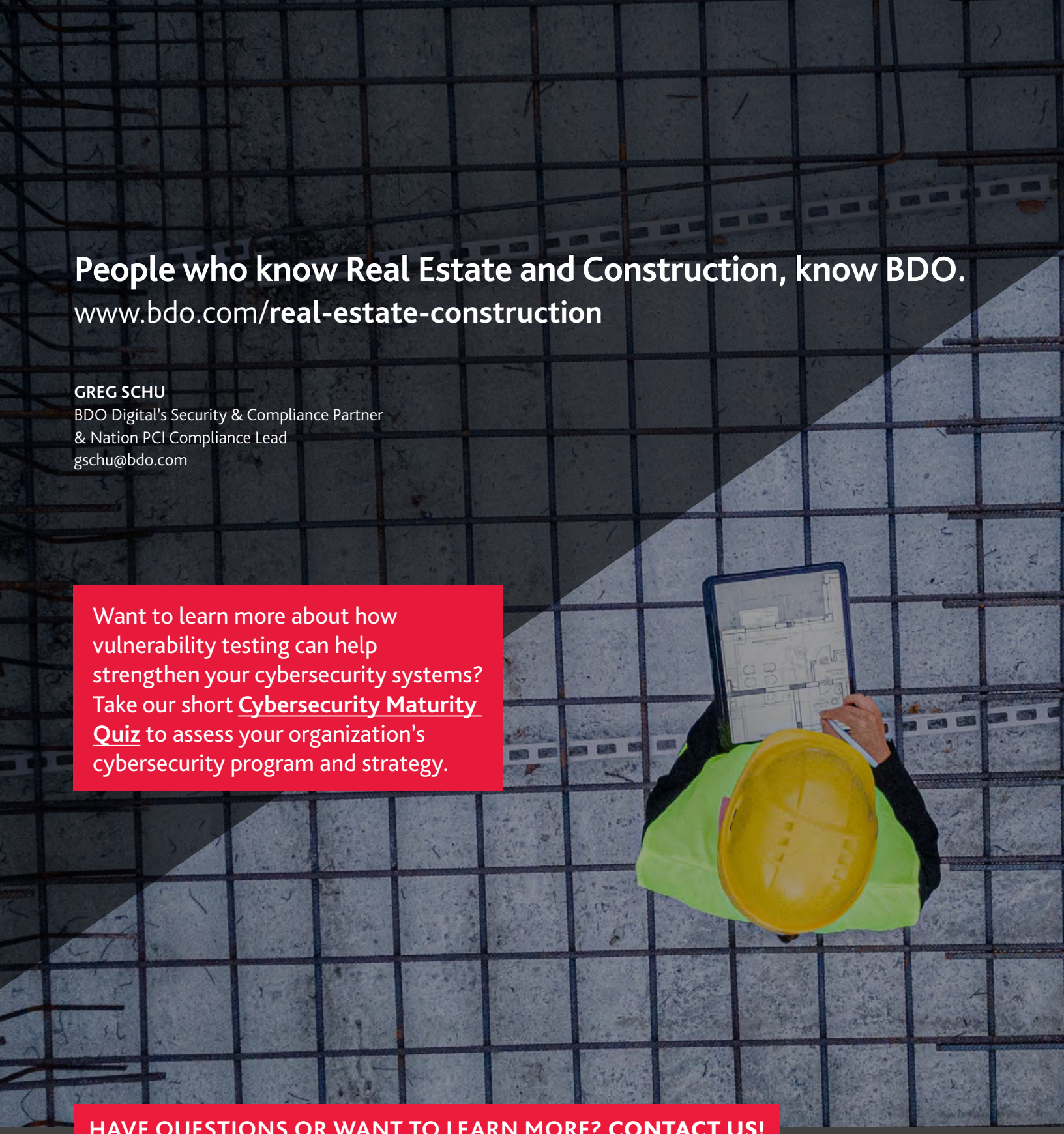
Many cybercriminals develop attacks by testing for weaknesses in software programs designed to protect against cyberattacks. The more outdated cybersecurity software is, the more time cybercriminals have had to find vulnerabilities. Having a dedicated IT team to help regularly monitor and **update cybersecurity software systems** can help organizations stay ahead of cybercriminals. If an in-house IT team is not feasible, having a dedicated vendor can also help facilitate and maintain a company's cybersecurity program.

Simple measures — including two- or multi-factor authentication, unique login identifications or virtual private networks (VPNs) — can protect companies substantially against cybercriminals. Once such practices have been established, it is important to prepare an incident response and backup plan. By having professionals simulate attacks to test for vulnerabilities, penetration and vulnerability testing can help strengthen these plans. When developing a backup plan, it is important to:



Having cyber insurance as part of the overall incident response and backup plan is a consideration, as well. While insurance does not cover all possible costs, it can help an organization bridge the gap should a cyber event occur.

A **robust cybersecurity program** is essential for real estate and construction companies' long-term viability. As technology evolves, companies should be prepared to handle increasingly sophisticated cyberattacks by keeping high security standards for themselves and others. Training employees in cybersecurity practices, investing in reliable software and building and testing backup plans can help maintain an organization's data, reputation and safety.



People who know Real Estate and Construction, know BDO.

www.bdo.com/**real-estate-construction**

GREG SCHU
BDO Digital's Security & Compliance Partner
& Nation PCI Compliance Lead
gschu@bdo.com

Want to learn more about how vulnerability testing can help strengthen your cybersecurity systems? Take our short **Cybersecurity Maturity Quiz** to assess your organization's cybersecurity program and strategy.

HAVE QUESTIONS OR WANT TO LEARN MORE? CONTACT US!