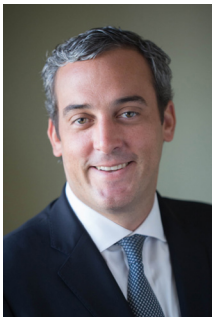
NAWRB WOMEN IN THE HOUSING & REAL ESTATE ECOSYSTEM

# Cybersecurity Q&A with Crowell & Moring's Paul Rosen



Paul Rosen, White collar, investigations and cybersecurity lawyer—former federal prosecutor & homeland/national security executive

For many of us, hacking and cybersecurity concerns are the last thing we want to worry about as we advance our real estate business and work with clients. But, as cybersecurity and government investigations lawyer Paul Rosen shares with us, now is the time to start thinking through your company's protocols and preparedness. He would know. While chief of staff at the U.S. Department of Homeland Security, Paul helped navigate the government's response to major hacking and security attacks, including attacks on critical infrastructure and personnel data.

## Q. Paul, who should worry about cybersecurity?

**A.** Cybersecurity is now an issue that impacts every U.S. business. The headlines in the news often focus on hacks at major companies, but small and mid-sized businesses are targeted every day. The real estate industry is regularly subject to system breaches, fraud scams, phishing attempts, and a host of other attacks. Historically, these problems were simply delegated to an IT consultant. But today, every business owner and executive should understand their cybersecurity infrastructure and be able to explain it to their clients and employees. For industries like real estate, which handle sensitive personal information and banking accounts for clients, the stakes are particularly high.

## Q. What should executives do now?

**A.** Begin by building the right team and understanding the key issues that must drive a cybersecurity plan. The goal of your plan should be not only to prevent a breach, but to have a clear and well-practiced incident response plan for when one occurs. A primary goal will be to protect your company's sensitive and proprietary data, including any client information. If and when a breach occurs, know what you're going to do, who you're going to call, and how to quickly and effectively address the breach.

## Q. How do you build a team?

**A.** Your team should be a cross-disciplinary group that includes not only tech experts, but representatives from legal, customer relations, business units, public relations, and other areas. The key is to bridge the knowledge gap between the technical experts and the senior decision makers. This team should assess sensitive data, the technology in place to protect that data and prevent attacks, training opportunities for employees, and how you will respond if a hack occurs.

Ultimately, you must identify the accountable executive who will stay on top of the plan—from ensuring technology updates are made to facilitating regular check-ups. The buck always stops at the top, but a CEO or general counsel can't be expected to have the necessary depth and bandwidth in cybersecurity to own the issue. But someone has to, and that someone has to be a senior, proactive, problem-solving executive.

## Q. What should senior executives who are not well-versed in technology understand?

**A.** You must understand your network and data. Ask yourself: What data is sensitive or vulnerable to

theft, either from a cyber breach or from an insider? What systems need to be protected, and how? What marketing data and trade secrets need to be protected? Your lead cybersecurity executive should also ensure that all patches and updates on software and threat prevention software are updated in a timely way.

Sometimes protecting your own data and systems isn't enough. Often times, businesses rely on third-party vendors to transfer or store sensitive data. This means that the cybersecurity teams need to be involved in selecting contractors and vendors, including appropriate legal provisions in those contracts to protect your business. Any company considering an acquisition needs to ensure cyber due diligence is conducted.

## Q. What does it mean to practice an incident response plan?

**A.** If your company is a victim of a cybersecurity attack, it could mean a tremendous disturbance to your operations, and it will unfold at lightning speed. Take, for example, the recent Ransomware attacks that occurred over the summer. In many of those attacks, executives came into work to find their computers—and all of their files—completely inaccessible and held for ransom. Companies had to face serious questions about whether they would pay the ransom and whether it was legal to pay. In less problematic scenarios, companies face hours or days of downtime, which can jeopardize deals and raise client concerns.

When you practice a plan, you identify a scenario that your company could face. The cybersecurity team, and often executives, in your organization schedules a time to work through how they would respond and develop solutions for the problem scenario. Knowing who needs to be in the room, who to call, and what actions to take (or not take) with limited information are all critical learning experiences when it comes to the real thing. It will also help you think through business issues beyond the technology, such as client communication and press response. Practice is a key component to an effective incident response plan.

## Q. How do you know if you're ready?

**A.** Today, cybersecurity is an issue that every business must manage, and even the most sophisticated technology companies must stay vigilant. The important thing to do now is to treat the issue as a business priority and to develop a plan for prevention, maintenance, and incident response that you can improve over time.  It is also important to understand what your legal obligations are in the event there is a breach, which is often rooted in the nature of the sensitive information that is entrusted to you.

At the end of the day, cyber risks are here to stay and the more businesses can do to prevent and manage that risk, the better off they will be as the challenges around cybersecurity continue to evolve.

---


Women's Economic Growth
Vol. 7/Issue 1
May 2018