VISIT OUR
FRAUD HUB

Protect your fortress:
Keeping bad actors at bay

Businesses must make industry-specific considerations to prevent cyberattacks and fraud. We look at healthcare and commercial real estate companies to see this in action.

continued on next page >

VISIT OUR FRAUD HUB

> *"It's life or death. Nursing homes, for example, wouldn't be able to know what medication to give their residents."*
>
> Kerry Jessani, National Head of Healthcare, Higher Education & Nonprofit Industries, Commercial Banking

The cybersecurity stakes have never been higher: According to our 2021 Business Leaders Outlook Pulse Survey from June, one-third of company executives said they had been directly impacted by some type of cyberattack or fraud attempt during the pandemic.

For many, the fortress is under constant attack. Ransomware, business email compromise (BEC) and other fraud threats continue to proliferate and evolve. To protect their organizations, business leaders must take action and build a comprehensive defense.

While investment, training and controls are broad cyber preparedness priorities, each business has unique considerations depending on its industry. The cyber threats are often the same, but the playing field has changed.

Cyber preparedness can be life or death in healthcare

For companies in healthcare, Kerry Jessani, National Head of Healthcare, Higher Education & Nonprofit Industries, JPMorgan Chase Commercial Banking, says fortress defenses hinge on two critical points: protecting data and identifying indirect vulnerabilities.

Healthcare providers are more awash in data than ever before, thanks to the adoption of electronic health records and other technologies. However, this makes hospitals and other organizations a top target for cybercriminals.

One challenge is that this data is frequently in transit, moving in and out of organizations to other places like insurance companies and doctor's offices. Each access point is an opportunity for sensitive patient data to be intercepted or abused.

"Data is sacred," Jessani says. "But what hospitals need to understand is they must create a framework for understanding who has your data. The fewer touchpoints, the better."

The constant exchange of data with outside parties further elevates the risks of BEC or ransomware. Without rigorous controls, there may be an increased chance that a healthcare provider's data could be held hostage, breached or otherwise manipulated for criminal gain. One slip and the worst could come to pass.

"It's life or death," Jessani says. "Nursing homes, for example, wouldn't be able to know what medication to give their residents."

Given the stakes, it's critical to have an effective data security program in place that utilizes a stacked approach to protection, including:

1. **Shutting down systems when not needed.** Why continue to run a patient database over the weekend when the office is closed and no one is using it?
2. **Activating unused security controls.** Work your way through all your systems and activate security features such as multifactor authentication, encryption tools and firewalls. Don't forget your router: Many elevated security settings are not activated by default.
3. **Segmenting your network.** Creating and utilizing separate networks for patients and the practice can help you keep random, unauthorized users away from your company network traffic.

continued on next page >

VISIT OUR FRAUD HUB

Vulnerabilities

Organizations can prevent intrusions or attacks before they happen by proactively identifying vulnerabilities. At healthcare organizations, the weak point may not exist internally and could be several steps down the supply chain.

"For hospital systems, the refrain you should consistently hear is 'You're only as strong as your supplier's weakest supplier,'" Jessani says. "For instance, the situation during the pandemic was, 'Yes you might use this supplier to provide masks, and they're just an intermediary supplier,' but they have 15 suppliers. So, you need to go through all of those to find the weak points."

The degrees of separation along a supply chain might not be front of mind for a healthcare business, but the consequences could cost them. That's why these organizations need a culture of vigilance.

"It has to be in the DNA in everything," Jessani says. "Get all the senior people in the room together from various departments. This impacts everyone; but often not everyone understands the importance of developing a preparedness culture until it's too late."

You can help to foster such a proactive culture by establishing a vulnerability management cadence. This includes:

1. Scanning and identifying vulnerabilities
2. Prioritizing vulnerabilities
3. Remediating
4. Rescanning to ensure you have closed the gap

When conducting an internal scan of your network(s), look specifically for unknown users and devices. To strengthen your vulnerability program, review current threat intelligence data and read about current vulnerabilities, how they are being exploited and what remediation options are available.

Wire volume multiplies the risks for commercial real estate

Protecting a commercial real estate fortress entails more than just maintaining physical properties. Winston Fant, Managing Director and Head of Commercial Real Estate Treasury Services, JPMorgan Chase, says it requires strict attention to detail given the vast volume of wire transfers these companies initiate.

Running fast and going hard

Commercial real estate businesses conduct massive amounts of wire transfers each day. With payments moving in and out, the rush of wire activity can create openings for fraud.

"Even for big companies, treasury staff is not usually large," Fant says. "They're running fast and going hard."

Without serious controls in place and in use, companies may risk multimillion dollar fraud losses. "It's not a matter of if, but when," he says.

Businesses should place a major focus on process hygiene and training employees to be vigilant in their diligence. For instance, a known email account can still be taken over by a fraudster, and it won't show a telltale spelling error in the

> *"There's no one single defense that can prevent everything."*
>
> Winston Fant, Managing Director and Head of Commercial Real Estate Treasury Services, Commercial Banking

continued on next page >

domain name. Following procedures like calling a trusted number can prevent a loss.

Even though added controls may slow down business, it's a necessary side effect.

"Businesses need to feel comfortable with having layered checks on dollars flowing out," Fant says. "There's no one single defense that can prevent everything."

Employee training is a best practice to help ensure that controls are followed. In the 2021 Business Leaders Outlook Pulse Survey, 79% of business executives said **employee education was the most helpful** measure undertaken by companies that experienced a cyberattack or fraud.

While training treasury staff is crucial for commercial real estate organizations, Fant doesn't think companies should stop there.

"It's advantageous for companies to train a broad swath of employees, not just those in treasury," he says. "Fraud happens because people make mistakes, and real estate is a people business, whether they're moving money, transacting or doing deals. The more people that are trained, the better."

Lastly, commercial real estate companies must look externally as vendors can be targets, too. Businesses should consider talking with suppliers about their security policies and how they are protecting their own organizations. Many companies require vendors to undergo an oversight process and submit documented security protocols.

Don't delay: Protect your fortress

Your cyber preparedness can never be considered complete if you don't account for industry-specific factors. Just as healthcare providers must focus on patient data and commercial real estate businesses must focus on wires, your business has its own set of special considerations that should govern how you address cyber and fraud risks.

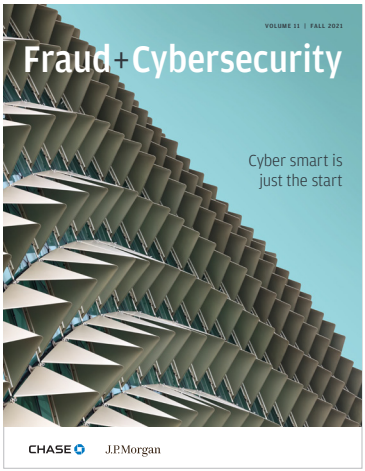
Regardless of your industry, however, you should have a sense of urgency about your cybersecurity posture. A great place to start is by doing one thing each day to protect your company, such as:

- Reading an intelligence article (you can find some on the JPMorgan Chase Commercial Banking **Insights** page)
- Reminding colleagues about trending scams and attacks
- Asking your information technology or security team to review settings on patched systems (sometimes the updates make changes without proper notifications)

Key takeaways

- Evaluate your business to determine which industry-specific factors present an increased risk for fraud or cybercrime.
- Create a framework that minimizes touchpoints to sensitive data.
- Enforce process hygiene with payments, even at the expense of speed.
- Build security into your corporate culture.

The previous article is an excerpt from Fraud + Cybersecurity Magazine: Fall 2021.



DOWNLOAD