The Internet Wasn't Designed To Be Secure

Karen Higgins-Carter, Gilbane's chief information officer and a former banking industry executive, says contractors need to band together against cyber threats.

Cybersecurity incidents are on the rise, and contractors need to be prepared. Karen Higgins-Carter, the chief information and digital officer for Providence, Rhode Island-based Gilbane Building Co., brings a wealth of experience from previous roles protecting the banking and financial services industries from cyber criminals. She warns that the internet wasn't originally built to be secure, and that the onus is on contractors to make sure they're up to snuff on today's security demands. Here, Higgins-Carter spoke with Construction Dive about where the biggest threats come from, how Gilbane keeps its employees up to date and what the industry can do to protect itself.

What's the state of cybersecurity in the construction industry?
KAREN HIGGINS-CARTER: I'll start with my view on cybersecurity in general. I think it's important to understand two things. First, the internet was not designed to be secure. It was designed to be open. Second, we are going to continue to see a volume of attacks coming from countries that are effectively safe harbor for this type of activity. Because of that environment, we're seeing the regulatory response. SEC disclosure requirements being first and foremost, that were implemented in December. What I find is the need to adjust and connect with our people based upon their current level of awareness. There's a predictable cycle of bringing our people from a position of not really being aware of the threats to feeling invested in protecting the company and being on board with that mission.

How do you get everyone to an optimal level of comfort with cybersecurity when their experiences differ?
One of the things that we have implemented in building, in terms of our innovation practices, is responsible innovation. That it's important to take risks in order to grow. There is no risk-free path to achieving your strategic objectives. Where that's important in innovation is understanding, how does this innovation support our strategic goals? What are the inherent cybersecurity risks that we need to identify? And, as part of experimentation, and scaling and innovation, we need to ensure that we are mitigating those risks at the same time. There's a level of awareness that happens through the process of innovating.

What are the biggest risks to builders right now on the cybersecurity front?
As for the two biggest attack vectors, the first is phishing. That's why awareness is so critical, because people are the first line of defense against phishing attacks. The second attack surface involves application programming interfaces. Our connectivity to third parties and third-party software providers is the next most prominent threat. Where that plays into our industry, and where there's really an opportunity for leadership, is in working with our software vendors. With the recent investment in construction technology, and lots of startups, security's not necessarily first on their roadmap in terms of demonstrating early returns for their investors. Recognizing that we can have a collective voice as an industry and help those software vendors reach a higher level of capability, particularly in securing APIs. Vendors can sometimes make it sound very easy, and it's really something that we, as end users, need to manage.

What does Gilbane do to keep itself secure?
In terms of starting from a strategy perspective, our board is engaged in cybersecurity. We have drafted what we call a cybersecurity risk appetite statement. That's a practice that I brought over from banking, which is identifying how a cybersecurity attack creates losses for Gilbane and impacts our customers. So we identify those top risks, and then based on that view, how it would impact us. We have a cybersecurity program where we prioritize our cybersecurity investments in processes and in

controls to mitigate those risks. We prioritize safeguarding our clients' confidential information. We safeguard our employees data because that is personally identifiable information. There's other internal information about some of our investments in our development company. I would say the other aspect of what we protect is a disruption in a business process. If our jobsite can't perform, because either Gilbane or one of our trade contractors has a ransomware attack and can't access their systems, we also look at how a critical business process would be impacted, and then, how you manage through that impact.

What can construction learn from the banking and financial fields on cybersecurity?
First, I think we can really collaborate on threat intelligence. And I don't mean general best practice sharing. I mean very specific threat intelligence, such that we can collaborate and work together on preventing that same threat from impacting another business. I think the second thing that we can do is collectively and proactively define our security expectations, particularly for software vendors.
By Matthew Thibault

For questions or a cybersecurity assessment, reach out to Computer Dimensions today @ 520-743-7554.