Cybersecurity: Playing Defense

Highmark's CISO talks tools and protections to keep data safe

By Katie Dvorak

Cybersecurity at Highmark is all about playing defense. And although good defense doesn't typically win the game, bad defense can certainly put you in the losers' column, Chief Information Security Officer Omar Khawaja tells *FierceHealthPayer*.

"The rest of the company—be it the product team, the marketing team, the sales team—everyone else is playing offense," working to grow Highmark's brand, make things better for customers and lower costs, he says.

But the job of a CISO is the converse: Khawaja has to look at keeping customers and the company from getting hurt. That's his version of playing defense.

The Pittsburgh-based payer knows the importance of layering security tools to keep data safe and the need to be risk-driven in its efforts, Khawaja says. Highmark has to look at the risks they face as a company and what makes the most sense for a successful business—not implementing security controls just because someone told them to.

Those controls are wide-ranging—from user access and encryption to data de-identification and information policies.

Khawaja spoke with *FierceHealthPayer* about how his organization is using those controls, and others, to keep consumer information safe and about what it takes to be on the winning side of security.

FierceHealthPayer: What security tools does Highmark employ?

Khawaja: We divide up the security program into nine areas, and we use a variety of tools across each.

1. Metrics and aligning to the business: Making sure we have the budget and wherewithal to be successful.
2. Risk management: How we figure out what we're going to do, what controls to implement and what tools we're going to buy.
3. Compliance management: This ties in with risk management, and complying with outside regulations.
4. Vulnerability management: Identifying weaknesses in our environment across anything or anyone that stores,

processes or transmits confidential information.

5. Data protection: The tools focused on directly protecting the data itself, not the applications or infrastructure. That's really where the future or information security is, it's all about data protection. The other tools won't be nearly as important if we fast forward to five years from now.

6. Identity and access management: When you have thousands of applications and tens of thousands of users, how do we make sure the right user has access to the right application at the right level?

7. Direct management: Sensors on our desktops, on our databases, on our internal network, on our perimeter, on our servers and even outside our environment work to figure out what's going on. They allow us to make smart decisions in terms of where we need to add additional layers of protection or change configurations.

8. Investigative response forensics: If we do have an incident, this helps us understand what to do and how to respond.

9. Culture: This is the foundation of it all and one of the most important security areas. It's all about creating an appropriate level of consciousness among our user base when it comes to the protection of our customers' information.

FHP: What's your process for vulnerability management?

Khawaja: Under vulnerability management, a large part of what we do is identify vulnerabilities and, subsequently, prioritize what we identify. We do about ten different kinds of vulnerability assessments. We do internal network vulnerability assessments, external vulnerability assessments, external penetration tests, internal penetration tests, Web application dynamic scanning and Wi-Fi assessments. We also do a variety of different assessments to identify weaknesses in our systems, including sending phishing emails to our own users.

FHP: What tools do you use for data protection?

Khawaja: Encryption is certainly one, and we're very deliberate about our use of encryption. Encryption on any device that's portable is of the utmost importance, so a tablet, a phone, a laptop—those have to be 100 percent encrypted. There's very little tolerance for unencrypted devices.

However, when it comes to encryption at rest for devices that aren't easily moveable, there is very limited utility in that encryption. So we'll apply it where it makes sense, and we won't go too far in other cases.

For example, even if the data had been encrypted in every single data breach over the last two years, the data breach would have happened in the exact same way. Encryption would have not been a very useful control at all. Encryption is the equivalent of a lock, and a lock is only as secure as the key.

Another control is data de-identification. In testing environments and other environments we don't need all of the data—we're data masking. In some cases we don't

need all digits of a consumer's Social Security number, just the last four. In some cases, we may not even need the Social Security number. We can use a different number or ID that has less value. Data protection controls, especially the ones around data de-identification or data deletion, are the absolute most effective controls you can have from a security standpoint.

We also apply layers upon layers of controls so you may get past one control and not the other. There are controls a hacker can't get around, such as deleting the data. So we've got a massive effort to work closely with our business and our customers to say 'is there data that we can simply delete?' The question we ask at Highmark is, 'do we even need the data to begin with?'

FHP: How do you address user access to data?

Khawaja: That is definitely something we spend quite some time looking at. It's hard sometimes to tell the good users apart from the bad users and the good users behaving properly from the good users behaving improperly. We have a significant effort in place to identify the users that absolutely need access to the data versus the ones that just have it because it's nice to have. We recommend removing access to certain apps and data for a good portion of users. Those are some pretty significant risk reductions.

FHP: How do you keep information secure when it moves between different locations such as servers, the cloud and mobile devices?

Khawaja: This goes back to data governance, which is basically the librarian. The librarian knows the location of every piece of information in the building. The data governance function knows where every piece of data is within the enterprise. Knowing where the information is and where it goes is absolutely critical. So it all starts with policies: How data can be stored, shared, transmitted and deleted. That gets clarified in contracts and business associate agreements.

With the cloud and mobile, especially, we're trying to be more forward looking by revamping our policies to reflect that it's not about where the data is. It's about the data itself. If you have a breach, it doesn't matter if it was in a mobile device or the cloud: You're responsible. So we're saying our controls should not be dictated by the environment in which the data is in, but dictated by the data.

If we deem a certain set of data to be critical, we're going to say for this criticality of data we need to have these 12 controls implemented. Now when we engage with outside providers, we're happy to ship them data, but we need controls and they need to meet them. In addition, our standard is to be HITRUST certified, so we need to make sure third-parties live up to the same standard.

FHP: What are the biggest challenges when it comes to data protection?

Khawaja: The biggest challenge and biggest opportunity is the people. We need a strong culture. To that end, about six months ago I hired someone who has no IT experience, no healthcare experience—he is a change management and behavioral specialist. We can deploy all

the right technology in the world, but it's all for naught if we don't have a strong security culture. Data is the fuel of our economy and the fuel of the business we're in. It's much like oil; it's an asset you need, but if misused, mishandled, misstored or mistransported, it can very quickly become a liability. So employees need to see it that way and think about that when hitting send on an email or sending data.

FHP: What advice would you give to other payers when it comes to cybersecurity?

Khawaja: Security is not something that a security department can singlehandedly achieve. Security professionals have to build partnerships across the organization—with the business, with IT, with audit, with compliance, with privacy—and when you build those partnerships everyone understands why you're doing things, why it's important and why it could hurt the organization if not done well.

Editor's note: This interview has been edited for clarity and length. ■