KEVIN HAMEL

**FORMER CISO,
BAYSTATE HEALTH**

CURRENTLY IN TRANSITION

Since his last Profile in Confidence feature in 2016, Kevin Hamel has transitioned roles and industries, garnering increased exposure and experience. He has grown significantly as a leader, from both a technical and business alignment standpoint through his CISO positions in both banking and healthcare.

Hamel provided updates on how his career has evolved since we last interviewed him, and discussed the extensive knowledge he gained in regard to the nuances, challenges and complexities of the working in the healthcare industry. He says, "While there's a lot of similarities in the technology that's used in banking and healthcare, there's a lot of differences as well. I think the healthcare technology environment is more complex in many ways, especially when you start to think about medical devices. For larger healthcare organizations, you may be looking at tens of thousands of IoT devices that are hard to manage. Trying to keep all of that data flowing and flowing securely is certainly no easy task."

THE RISING FOCUS ON CLOUD AND REMOTE WORKFORCES

With over 16 years' experience in information security, Hamel understands the constant evolution and growth taking place in the industry. Currently, he says CISOs' goals and challenges have changed dramatically due to the impact of COVID. He explains, "There's been a huge shift to remote work and companies have migrated hundreds or in some cases, thousands of employees to a remote work situation. In many cases, this happened over the span of only a few weeks. I think that's really brought the question of how to manage a remote workforce to the forefront. Not just from a security perspective, but a lot of the obvious things come into play. Things like how to make sure employees are the only ones connecting to an organization's remote connection, or other basic considerations like Multi-Factor Authentication."

Hamel says we must take into account the security implications of a remote workforce, but also consider business-wide concerns such as communicating with employees if there is a system outage. He says in many cases, companies may have an emergency notification system they blast out to let their employees know their system is down. However, many are not prepared for the sudden impact of thousands of employees working remotely and may struggle to adequately maintain the same level of company-wide communication.

With a heavier focus on cloud and remote endpoint technologies, Hamel sees this trend continuing to increase, potentially resulting in additional training budget for information security staff members. He explains, "I'm not sure

> *"For me, I need more digital, I need more cloud, I need more remote technologies. I think that's going to be a big area of focus going forward over the next few years."*

that companies have invested appropriate training dollars in cloud and remote workforce technologies over the past five years. If companies are going to go down this road of having 50% or more of their workforce working remote, technology teams must understand how they're managing remote access to platforms such as Teams, Dropbox and Box."

Hamel says the quote 'the cloud is now my data center, any device is now my endpoint, my network is now the internet' resonates with him because it clearly depicts the new challenges faced by security leaders. He comments, "It has just completely changed the landscape that all companies are operating on. And I think it requires, in some ways, technical skills that I'm not sure every company has. I know I'm looking to invest in staff training around cloud, mobility management and remote connectivity tools so we can support the new workforce."

THE PUSH FOR DIGITAL EXPERIENCES

Hamel believes there is a significant push within organizations for accelerated digital experiences, whether it's internally with employees or externally for consumers and customers. For example, in the healthcare field, digital advancements may include telemedicine or leveraging medical devices outside of the hospital, such as at-home blood testing.

He comments, "So far, a lot of our conversation has revolved around employees, remote workforces and accessing cloud solutions, but it is also important to think about your patients, consumers or customers. You can't ignore the customer or patient side of things. I think this pandemic is going to force a lot of businesses to revisit if they need customers or patients to come directly into their facilities for certain services, or if they should leverage digital channels to consume business services from the comfort of their own home. That's going to put new demands on IT and information security and you're going to see pressure on both sides. Since most employees are now remote, customers and patients need to engage in a digital capacity. For me, I need more digital, I need more cloud, I need more remote technologies. I think that's going to be a big area of focus going forward over the next few years."

IMPLEMENTING ZERO TRUST

Hamel does not believe there is a one size fits all approach for Zero Trust that applies to every organization and industry. Most companies have varying definitions of what Zero Trust means to their program and mission, and their goals ultimately differ.

Hamel explains, "To make a broad statement and say Zero Trust is achievable, is something that's hard to do because every company is probably going to have a different definition of what that means and a different definition of what their Zero Trust end state would look like. Maybe one company decides to do Zero Trust only with certain platforms or another company that is focused on only a certain extent, but across all of their platforms. I don't think there's a one size fits all. Everybody has to chart their own course and figure out what their Zero Trust goals look like."

Zero Trust is a worthwhile and beneficial endeavor according to Hamel. He believes every company should have Zero Trust implemented in some fashion. He says, "Zero Trust at times feels similar to the 'least privileges' concept that was around 10 or 20 years ago, where you give staff or vendors access to only those things that they need to have access to. The buzzword was 'least privilege'. So to me, I don't find the Zero Trust concept too different than giving people access to only what they need access to."

He continues, "Admittedly with Zero Trust, we're talking about different tools to make that happen and more automation, and more on the fly analysis to figure out what resources or IT services a user has access to. But I think that concept is still largely the same where you give someone only what they should have access to at this point in time. I think every company should be moving in that direction and trying to implement some form of Zero Trust, but whatever's right for them as a company and to whatever degree is right for them as a company."