LETTER FROM KEVIN WEST

CEO

MY PASSWORD IS 1MPO$$!BLE

I dislike passwords immensely. Sounds crazy coming from a CEO of a security company? Maybe not. I think nearly everyone knows the anxiety and frustration when making their third and sometimes final attempt to get into an application before they get locked out. Trying to maintain so many different passwords for business and personal applications is mind bending. At work, my employees hear me exploding and they know it is for one of two reasons; I forgot a password or I'm being asked to change an existing password. Our internal IT team dare not give me their canned answer around the need and value of passwords. My rants always include how I truly understand why information security programs get a bad rap as productivity inhibitors.

Passwords are a burden and they make me less effective. Multiple passwords create inefficiencies, limit effectiveness and are a drag on productivity. If password management is a nightmare for someone like me with years of security experience and a real understanding of the value of identity protection, we have to know this is a major problem for enterprise users.

No matter how strong the security awareness training program, when identity and access control impede productivity, CISOs lose the support of their organization. And, when CISOs are seen as an impediment rather than an enabler, it puts the entire security program at risk.

STRATEGIC IDENTITY PROTECTION

The good news is that as an industry we are re-imagining identity protection. Until recently, identity was not a strategic element of any security program. Combined with access controls and user provisioning, identity management was viewed as a tactical element that lacked a coherent and thoughtful strategy. That is just one of the reasons why we have so many passwords.

Identity is not just a security concern, and not just a password problem. In fact, as we explain in our article on the significant market growth for IAM, identity is fundamental to nearly every part of the organization. Chief Marketing Officers have made customer identity central to their marketing campaigns, creating unique user profiles and targeting customers based on their digital footprint. Human resource and IT departments assign identities and user privileges each time an employee or contractor joins or leaves the organization. Risk and privacy officers view identity proliferation as a challenge they must manage to achieve compliance and protect personally identifiable information.

Every executive at the table has a stake in identity, but the onus is on the CISO to lead. As Fairfax County CISO Michael Dent says in his profile, "our leadership is clear that identity is a security issue." As explained in "Identity Takes Center Stage," also in this issue, next generation identity protection strategies will incorporate intelligent identity monitoring, understand a user's entire digital footprint, and leverage behavioral analysis to predict threats. Strategic CISOs will embrace these new tool sets as part of their overall IAM program.

AN OPPORTUNITY TO MAKE AN IMPACT

Regular readers of our magazine will recall that CISOs we interview report three top priorities.

1. Align with business goals

2. Enable competitive advantage

3. Make an overall positive impact on their business

Creating a strong identity protection program affords CISOs the opportunity to align with the business goals of other executives, and enable agility, which is a competitive advantage, at the same time.

There is another piece of the puzzle that makes this the perfect time for CISOs to re-engineer their identity protection programs. Nearly four out of five CISOs list digital transformation as their major challenge. Floyd Fernandes, the CISO at CBSi, discusses this challenge in his profile in this issue of the magazine.

Digital transformation, in and of itself, represents significant change for users. They must learn a new way of working with data and applications. CISOs who engage early on in digital transformation discussions may influence how identity is addressed and secured in the cloud. This allows CISOs to introduce a comprehensive identity strategy as part of the change that digital transformation requires, making it a lot more palpable to business users, and therefore a lot easier to roll out.

Whether they are tackling identity protection challenges in the era of digital transformation, or other program elements, I continue to be impressed with the quality and vision of the CISOs that we profile in Feats of Strength. In this issue, in addition to Fernandes and Dent, we also profile Holly Ridgeway, EVP and CSO at Citizens Financial Group, Geoff Belknap, CISO of Slack, Josh Koplik, CISO of IAC, Nick Nedostup, CISO of Johnson Controls, and Tony Meholic, CISO of The Bancorp Bank. Each of these executives share their insights on tackling specific challenges with thoughtful and strategic security programs.

As I consider our path forward to solve the identity protection challenge, three things are clear to me. First, digital transformation represents a great opportunity to usher in a new identity strategy. Second, CISOs will gain even more organizational leadership credibility when they deliver seamless and transparent data and application access that empowers user productivity. Third, I cannot possibly remember one more password.

Please enjoy reading this issue and learning more about this pivotal topic. As always, we love to hear your feedback.

KEVIN WEST is the founder and CEO of K logix, a leading information security company based in Brookline, MA. K logix helps create confident information security programs that align with business objectives.