Identity Takes Center Stage in the Digital Transformation

By Stephanie Hadley
Marketing Content Manager

Mobility, cloud computing and the Internet of Things (IoT) are game-changing technologies that are enabling massive innovation in business. With all the innovation, efficiency and advancement they bring, they also expose new security risks.

- **Threat vectors are multiplying**
- **Access control is overwhelming burdened security staff**
- **Data and information are being accessed from outside of the secure enterprise network**

Despite the risks and exposures, saying no to these innovations is simply not an option for most CISOs; the business benefits are too clear. According to our own data from K logix interviews of CISOs, 79 percent of organizations have already, or will soon, invest in digital transformation.

As a result, security teams must embrace this evolution and enable their enterprises to reap the business benefits of these innovations in a secure and transparent manner.

A key piece to securing the digital transformation is identity. As identities proliferate within cloud computing, securing those identities and limiting access to only appropriate users is a high priority.

AVOID AN IDENTITY CRISIS

Identity protection, long bundled with access management as an administrative function, is now a critical component of comprehensive security strategies. We asked CISOs and other C-level executives how identity protection programs are evolving this year.

"As we see more of a digital transformation continue within organizations, the proliferation of digital identities along with internet enabled devices will become more of a reality, and also a challenge to properly secure. Intelligent and effective identity protection strategies are crucial to cover the breadth of a user's total digital footprint." - Rick Grimaldi, Chief Strategy Officer, K logix

Identity protection strategies must enable an organization to understand and secure a user's complete digital footprint while being transparent to the business user and operations.

Many organizations are aspiring to least privileged access models, both to meet compliance requirements and to ensure better protection of critical assets. Tony Meholic, CISO at The Bancorp Bank says, "User access is a huge priority for us. Now we know everyone's system access automatically and systems that interact with PCI data are flagged. The participation from management is much better, largely because the systems is web-based and simple to use. Our user access levels decreased 8 percent in June. Now we are trending towards least privileged access."

> "Intelligent and effective identity protection strategies are crucial to cover the breadth of a user's total digital footprint."
>
> - Rick Grimaldi, CSO, K logix

80% of all security breaches involve privileged access

Identity is the Weakest Link

Forrester Research estimates that 80 percent of all security breaches involve privileged access. In the age of cloud computing, user access is the weakest link in the network, and ripe for exploitation. As a result, identity protection is increasingly a first line of defense.

In PWC's 2017 "State of Information Security", Richard Kneeley says, "Identity has been at the heart of almost every breach in the past two years. Many of these breaches have involved someone gaining access by using compromised identity, then changing their identity once inside the network to ratchet up access to data and systems by taking over a privileged account and in the process gaining unlimited access to the network, to systems and to data."

HOW ARE YOU ADDRESSING IDENTITY IN THE ENTERPRISE?

As a broad technology category, Identity and Access Management has a long history in security and IT departments. As a result, many organizations are running multiple IAM solutions, and controlling user access in a variety of ways across systems and departments. This patchwork strategy creates confusion, limits efficiency and is difficult for strapped security teams to manage.

As CISOs look to next generation IAM tools that enable behavioral analysis and intelligent identity protection, many need help understanding the capabilities of their existing investments and mapping a go-forward strategy.

K logix's Identity and Access Management project advisory service helps clients understand the following:

• Identity management solutions for on-premise and cloud environments;

• Ways to address elevated privileges with security and monitoring;

• How to empower individuals with access to the right resources at the right times and for the right reasons;

• When to enforce second factor or adaptive user authentication to critical or sensitive infrastructure, apps, accounts, and data;

• Available solutions to analyze normal and anomalous user behaviors that may be indicators of an attack or insider threat activity.

K logix's project advisory service helps security organizations strategically address their specific identity protection challenges with organization-specific decisions about appropriate technology and policies.