SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Security Program Strategy & Operations > Emerging Issues >

Why Security Needs to Understand Digital Transformation: A Primer

By Don von Hollen, Business Innovation and Support Team Lead- City of Calgary Corporate Security; and Kathleen Kotwica, EVP and Chief Knowledge Strategist, Security Executive Council and Principal Analyst, Security Leadership Research Institute

Of the many lessons COVID-19 has taught businesses, one that will resonate well into the future is that internal and external customers expect their transactional experiences to be easy, fast, reliable, and often interactive (e.g., online). More and more, this is accomplished by converting physical processes or reinventing processes through technology.

Of course, this isn't news to everyone. Many companies have been pursuing "digital transformation" for years. (Netflix shifting its business model from DVD to streaming rental services is one common example cited, and you can see six others here.) But in many other companies, the concept hasn't yet gained traction.

So, what is digital transformation? And why do security leaders need to know about it?

What Is Digital Transformation?

Digital transformation is an end state that is generally preceded by two other steps. In defining digital transformation, it's helpful to look at the three together.

1. Digitization: the transitioning of technology from analog to digital such as text, images, voices, or sound. For security, examples include moving from CCTV to IP cameras and moving from local proprietary access to IoT access systems.
2. Digitalization: the process of making changes to processes using digital technology to enable or enhance business operations. For security, examples include the integration of HR systems with access control systems to automate the creation of credentials and leveraging open-source intelligence feeds to distribute information to frontline security staff. A security service example is the CAP Index[1], which compiles crime data to measure the likelihood that crime and loss will occur at a given address (e.g., corporate headquarters) and presents it visually.
3. Digital transformation: the strategy across the enterprise to adopt digital technologies with the intent to reimagine and transform business competencies and models.

As you can see, digital transformation is less to do with the technology itself than the culture shift that drives the technology's use.

Executive leadership will often pursue digital transformation with one or more of these outcomes in mind:

- New revenue channels
- Increased competitiveness
- Increased efficiency; reduction in operational costs
- Streamlined decision making
- Improved customer (internal or external) experience/satisfaction

Common technologies used to reach these ends may include:

- Artificial intelligence
- Big data/analytics
- Blockchain
- Cloud/managed services
- IoT

What digital transformation looks like differs from organization to organization. However, in one example presented in the MIT Sloan Management Review report "Strategy, Not Technology, Drives Digital Transformation," an online travel company used wearable sensors on employees to identify patterns of collaboration by analyzing how and where employees talked

[1] CAP stands for Crimes Against Persons, Crimes Against Property. See www.capindex.com

to one another. The results showed that when more employees ate lunch together, they shared more insights, which led to higher productivity. A simple change based on this analysis – increasing the size of the tables where the workforce ate lunch – had a direct and measurable impact on employees' ability to produce.

What Is the Impact on Security?

At first brush, it may not look like this concept has a lot to do with the security function. Chances are that digital transformation isn't on the radar of most security leaders.

The critical thing to understand, though, is that it is on the radar of executive leadership.

According to the Wall Street Journal, "Existing operations and legacy technology infrastructure pose a risk to companies that can't transform quickly enough to compete against companies that were 'born digital,'" and executives' concern about this competitive disadvantage has surged in the last two years.

The SEC believes that the security industry will find opportunities for digital transformation specifically in the areas of risk assessment/management and the integrated optimization between IT and corporate security. But before they pursue these possibilities, security leaders need to be asking where their organizations stand on the path to transformation and where their executive leaders want the company to go. Is the company even on this path? Only with this understanding can the security function position itself appropriately and successfully within the corporate strategy.

Are You a Candidate for Digital Transformation?

Once you know where your company wants to go, it's also essential to think about how prepared your function is for digital transformation.

How do you assess if there's a business value in moving toward transformation at this time? At what level are your services now? Remember that in security's case, the customers whose experience you may be looking to improve are likely internal customers. Could you benefit from digitization but not yet digitalization? Would it make sense to pursue the goal of increasing efficiency through digital technology, but not yet innovation?

Remember, there are no blanket solutions. The right equation for you will depend on your current circumstances, conditions, culture, and resources (what we at the SEC call your C4R).

Visit the Security Executive Council web site to view more resources in the Security Program Strategy & Operations: Emerging Issues series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com/

