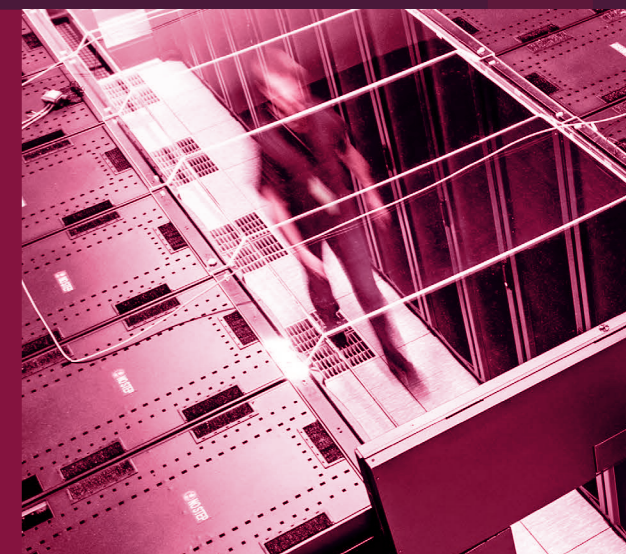







# 5

## Recommendations for a Secure Environment for Innovation



1	2	3	4	5
 <b>Communicate early and often</b> <hr/> <p>Engage executives and key stakeholders</p> <hr/> <p>Understand the plans for innovation</p> <hr/> <p>Empower the security team to start the conversation</p>	 <b>Rationalize and simplify the security stack</b> <hr/> <p>Reduce complexity</p> <hr/> <p>Eliminate redundancy</p> <hr/> <p>Create a single pane of glass</p> <hr/> <p>Develop a strong procurement evaluation process</p>	 <b>Establish cybersecurity guardrails</b> <hr/> <p>Define policies</p> <hr/> <p>Implement access controls</p> <hr/> <p>Integrate across logical and physical systems</p>	 <b>Stay flexible, get creative</b> <hr/> <p>Be open to new security methods</p> <hr/> <p>Focus on security methods that accommodate innovation</p> <hr/> <p>Keep in mind that innovation can take place in the security office</p>	 <b>Foster a strong security culture</b> <hr/> <p>Facilitate broad involvement</p> <hr/> <p>Promote transparency</p> <hr/> <p>Drive collaboration</p>

# Create a Secure Environment for Innovation.

**To maximize innovation in our technology and data-driven world, cybersecurity must be built to support innovation. But how does an organization create an environment that empowers growth, creativity and innovation without compromising security?**

To investigate a real-world example of such an environment, Sameer Shah from Dell Cybersecurity Marketing met with Dr. Tony Bryson, the Chief Information Security Officer (CISO) for the Town of Gilbert, AZ, to discuss the innovative City of the Future initiative and the role security played in driving it.

Read on for a summary of Dr. Bryson's recommendations, and to watch the entire conversation visit [dell.com/cybersecuritymonth](https://dell.com/cybersecuritymonth).

## Communicate early and often

Dr. Bryson stressed the need to engage executives and other key stakeholders early in the innovation process. "Make sure you know where they want to go, and how they're likely to leverage technology and innovation to benefit the business and the customer," he said.

A natural extension of communicating early is to have the cybersecurity conversation at the start of the innovation cycle, and as a key partner, the cybersecurity team can be the catalyst for these discussions.

The Town of Gilbert's use of AI offers a prime example. The Security Office began these conversations two years ago and took a leadership role in asking critical questions: how to trust AI generated data, how to store it, and how to ensure that residents properly understood the use of AI. This led to the creation of a cross-functional committee, which then led to the hiring of the town of Gilbert's full-time Chief Artificial Intelligence Officer, also a first for the Western US.

"None of this would have happened if we were drawing out a security fence that prevented that particular innovation from happening," Dr. Bryson says. "So when it comes to trying to innovate and trying to do things the right way, conversation is where it starts."

## Rationalize and simplify the security stack

One of Dr. Bryson's first tasks was to inventory the security stack to understand the use for each product and service. That effort uncovered significant redundancy. Reducing and rationalizing would save money, but more importantly, it would give the small security team a single pane of glass and a single source of truth by which to administer the cybersecurity capabilities and address issues.

Dr. Bryson echoed the old adage that complexity is the enemy of cybersecurity when he said, "I don't want to see people having to bounce from system to system trying to figure out what's going on."

## Establish the right cybersecurity guardrails

The innovators in the organization need to understand and abide by the security guide rails that keep systems and data secure. Those rules can be policies, access controls, or other tenets that help the innovators understand the playing field. This playing field represents the secure environment for innovation, created through an effective partnership between security and the innovators.

## Stay flexible, get creative

Dr. Bryson noted that while it's important to have and enforce cybersecurity standards, innovation will require fluidity and creativity at times. He pointed out, "Innovation does not just happen in the business unit. Innovation many times happens within information technology and even in the Information Security Office. You may have to find new and creative ways of securing your systems and data as your business innovates around you. So just be prepared for that."

“  
Make sure you know where [stakeholders] want to go, and how they're likely to leverage technology and innovation to benefit the business and the customer.”

**Dr. Tony Bryson**, the Chief Information Security Officer (CISO) for the Town of Gilbert

## The City of the Future

The Town of Gilbert's City of the Future initiative was designed to build a sustainable, resilient infrastructure that uses data to enrich the lives of its citizens. Technology is heavily involved in providing services from residents paying their bills, to traffic operations, to water availability and quality. It also involves collecting data to predict future service usage and needs. The initiative does not have a finite ending point, rather it's an iterative process that drives continuing progress.

As its first CISO, Dr. Bryson's mandate was to take a more strategic approach to cybersecurity. Providing modern, technology-enabled city services would require strong data protection, classification and control functions designed to support the town's ambitious goals.

As that process has continued and succeeded, Dr. Bryson identified a few key recommendations that facilitated success and created the right environment on which to grow and innovate securely.

## Foster a strong cybersecurity culture

Dr. Bryson stressed the importance of developing a strong security culture. "Culture is pretty much everything...when it comes to cybersecurity. If you don't have a culture where people are cybersecurity aware, recognize the threat surface."

The foundation of a robust cybersecurity culture is built upon many of the elements already discussed: open and transparent dialog, broad involvement, clearly articulated standards, and a spirit of collaboration between the security team and its customers, both internal and external.

As growth accelerates, cybersecurity must evolve from a reactive stance focused on defense to a proactive approach that prioritizes facilitating positive outcomes.

Organizations should adopt a modern security mindset that not only protects but also empowers innovation.

This can be achieved through communication and collaboration that integrates security measures into the development process. The goal is an environment where creativity thrives without compromising security.

Learn how to address some of today's top cybersecurity challenges at [dell.com/cybersecuritymonth](https://dell.com/cybersecuritymonth)