Cross Industry CISO

Expert Exchange

Q2 Executive Summary
April 11, 2023

kyndryl™

Overview

In this Expert Exchange session, several CISOs convened to discuss the definition, implementation, challenges, and impact of zero trust framework. The agenda was created based on mutual interest, determined through advance interviews with participants.

Hosts

Michael Restivo
US Sales Vice President,
Security and Resiliency,
Kyndryl

Jimmy Nilsson
Vice President,
Domain Lead for Zero Trust,
Kyndryl

Key Topics

Defining zero trust

- Zero trust continues to grow in popularity as the preferred approach to security, with 60% of all organizations expected to embrace zero trust as a starting point for security by 2025. Many people think of zero trust as a tool or technology, rather than as a people, process, and strategy framework.

- Managing access is a key component of zero trust. But rather than looking at a particular pillar of zero trust as being the most important, we should always put the asset we are trying to protect in the center i.e., an asset centric zero trust approach. And all pillars and security capabilities in your environment should be leveraged in an optimal way to secure all traffic flows to, from, and within the asset we are trying to protect.

> *"When we talk about zero trust, it's often referenced to as some access management-type of solution via a VPN, micro segmentation solution, or an SDP-type of solution. But, if it's done correctly, it should help you not just with preventing, but also detecting, responding, and recovering."*
>
> *— Jimmy Nilsson, Kyndryl*

3 steps to implement a zero trust policy

Learn more →

Engaging leadership

- Zero trust and cyber security can still be confusing topics to discuss with senior leaders since many top executives often do not realize what security leaders do. There is a misconception among some senior leaders that zero trust is a shiny new product that will solve all security issues. The reality is that zero trust is a framework, a methodology that needs to be implemented correctly.
- Culture plays a significant role in how CISOs communicate zero trust to senior leaders. In some cases, plain English is needed to explain the framework in non-technical terms. In other cases, especially at highly data-driven organizations, quantitative support for zero trust is required. CISOs must know their audience and communicate in a way that resonates with the culture of their organizations. Using data to quantify how zero trust supports a reduction in risk is helpful when garnering leadership buy-in.
- The risk appetite of management is also an important consideration, so all scenarios must be presented. For this reason, some leaders favor quantitative analytics in security conversations with leadership because it's not about one person's opinion. Since the focus will always be on risk mitigation, quantitative results enable the CISO to tell that story through data.

> *"For us as leaders in our organizations around this space, we've got to be clear about what resonates with our leadership. For me, if I don't come in with data, I don't get consideration at all. And I certainly won't get the kind of investment that they're making in me now."*
>
> *— Member, Cross Industry CISO Expert Exchange*

Changing threat landscape

Learn more →

Challenges of zero trust

- Organizations face a number of challenges when implementing zero trust. Talent is a major consideration because expanding zero trust will require organizations to have adequate staff to support it. Zero trust has not been commoditized to the point that everyone understands it, meaning it will place increased demands on those that do understand.

- CISOs recognize a need for governance around zero trust. While cybersecurity frameworks like NIST with its long list of controls cover everything, it is almost impossible to apply those controls all the time. Therefore, security leaders must determine governance frameworks that allow access when needed and make identity the "new perimeter." To this end, some security leaders are emphasizing rule-based access and relying on the principle of least privilege.

- Gauging success with zero trust has proven challenging for organizations since industry benchmarks around zero trust simply don't exist. In the absence of industry benchmarks, some CISOs are relying on quantitative data to measure the impacts of zero trust.

The irony of zero trust

Learn more →

The Expert Exchange is hosted by Kyndryl, Inc. Please contact Michael Restivo or Jimmy Nilsson with any questions about Kyndryl or this Expert Exchange.

This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice. Not all offerings are available in every country in which Kyndryl operates. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.

05-17-2023