TAG CYBER

# WHAT KEEPS A CISO UP AT NIGHT (IN 2022)

EDWARD AMOROSO, TAG CYBER

VERIDIUM
TRUSTED DIGITAL IDENTITY

# WHAT KEEPS A CISO UP AT NIGHT (IN 2022)

EDWARD AMOROSO, TAG CYBER

Apart from the day-to-day management issues related to budget, staffing, and the like, three major technical issues – identity, inventory, and complexity – keep many modern enterprise Chief Information Security Officers (CISOs) awake at night.

## INTRODUCTION

I was delighted when my my friends at **Veridium**, a leading cybersecurity firm focused on developing cutting edge identity verification and authentication technologies, asked if I'd comment briefly to identify and explore these issues. This question of what keeps a CISO up at night is, without a doubt, the number one question we hear during media inquiries at **TAG Cyber**. But I've noticed that our answers tend to shift rather rapidly. A few years ago, it was worms, then it was botnets, and then it was ransomware. And it goes on and on.

One thing to mention as a preface is that I'll stay away from the day-to-day management challenges facing the modern CISO. Tasked as the interface between security staff curating cyber controls and senior management governing cyber risk, the CISO has had to learn a plethora of executive skills related to communication, interaction, negotiation, sales, budgeting, and people. These challenges keep CISOs up for sure – but I'll stick to technical issues here.

Based on TAG Cyber's ongoing work with enterprises across several sectors, following are three major issues that we've noticed are top of mind, for CISOs. Yes – we could probably have listed another twenty relevant issues, but for this note, I chose three primary concerns that have been consistently on our customers' minds – and also on their task request lists as they engage with our TAG Cyber Research as a Service (RaaS). I hope the list provides you with some insight into the psyche of the modern CISO.

## SECURITY CHALLENGE 1: IDENTITY

A major root cause of nearly every major cyber breach that we've observed over the past few years has been an insufficient set of controls related to identity. The difficulty of identifying, authenticating, and continuously validating users – regardless of the business context – has been consistently under-estimated by security teams. This explains why this issue of identity has been such a nagging issue for CISOs.

A typical example of this identity challenge involves customer authentication. The traditional method of issuing user IDs and passwords has been shown to create environments rich in account takeover and fraud. Instead, CISOs who support on-line customer engagement have had to create programs that analyze user behaviors, develop advanced verification methods, and do so consistent with regulatory and compliance objectives.

Another aspect of the identity challenge is the internal friction that slows business processes and adds complexity to routine employee tasks and responsibilities. One such example is the continuing reliance in the banking sector for branch floor personnel to carry physical identity tokens. Replacement of lost tokens and trips home to retrieve forgotten ones are routine. Other sectors present similar problems around physical identity schemes.

This transition has not been easy – and the wise CISO partners with a good commercial vendor (or set of vendors) to ensure constancy with the best available technologies and methods for handling identity verification and authentication, among many other aspects of the identity equation. (My friends at Veridium are in this business and would be a wise choice for setting up a discussion to learn their authentication solution.)

## SECURITY CHALLENGE 2: INVENTORY

A second major issue for CISOs that not only keeps them up at night, but also causes considerable tossing and turning for IT operations executives involves inventory. This includes both an inventory of assets such as devices and endpoints, as well as data. While it would seem so obvious that inventory must be properly managed as a foundation for all security controls, it tends to be neglected by most enterprise teams.

The most common issue that emerges with respect to inventory involves something we refer to at TAG Cyber as sprawl. An organization might have started one or more decades ago with a reasonably manageable inventory. But growth of data creation, minimal data removal, corporate actions (such as mergers), third-party data creation, explosion of app usage, and expansion to cloud and SaaS have all contributed to inventory sprawl.

The only reasonable solution for CISOs and their IT partners is to initiate a comprehensive program to tackle their inventory (which also includes the identities mentioned above). Such a program should use the best available technology that can locate, classify, and secure all assets and resources. Without such action, it seems inconceivable that a security architecture can be viewed as standing on solid foundations.

## SECURITY CHALLENGE 3: COMPLEXITY

A third and perhaps the most important challenge that keeps CISOs up at night these years involves complexity. This refers to the difficulty any person or group has in understanding the IT infrastructure, security systems, and business processes of an organization. Every CISO knows that complexity in these areas always implies insecurity – and, in recent years, complexities have abounded.

A reasonable test for the level of complexity in an organization involves the simple question of whether a security team has schematics for the network infrastructure, deployed systems and applications, and all stored data (obviously related to the inventory problem managed above). If a CISO does not have diagrams of how the enterprise network has been arranged, then things are simply too complicated.

Good technology from commercial vendors can be used to scan and graph the network (often to the dismay of teams reviewing the output). Managers can also demand that engineers and operators focus on simplifying infrastructure in day-to-day decision-making. Here is a hint: If you are adding complexity to your security architecture, you might be doing things wrong. Removing complexity is always the best security action – and will help with CISO sleep.

## ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.