DARKReading

1/25/2019
10:30 AM

Todd Fitzgerald
Commentary
Connect Directly

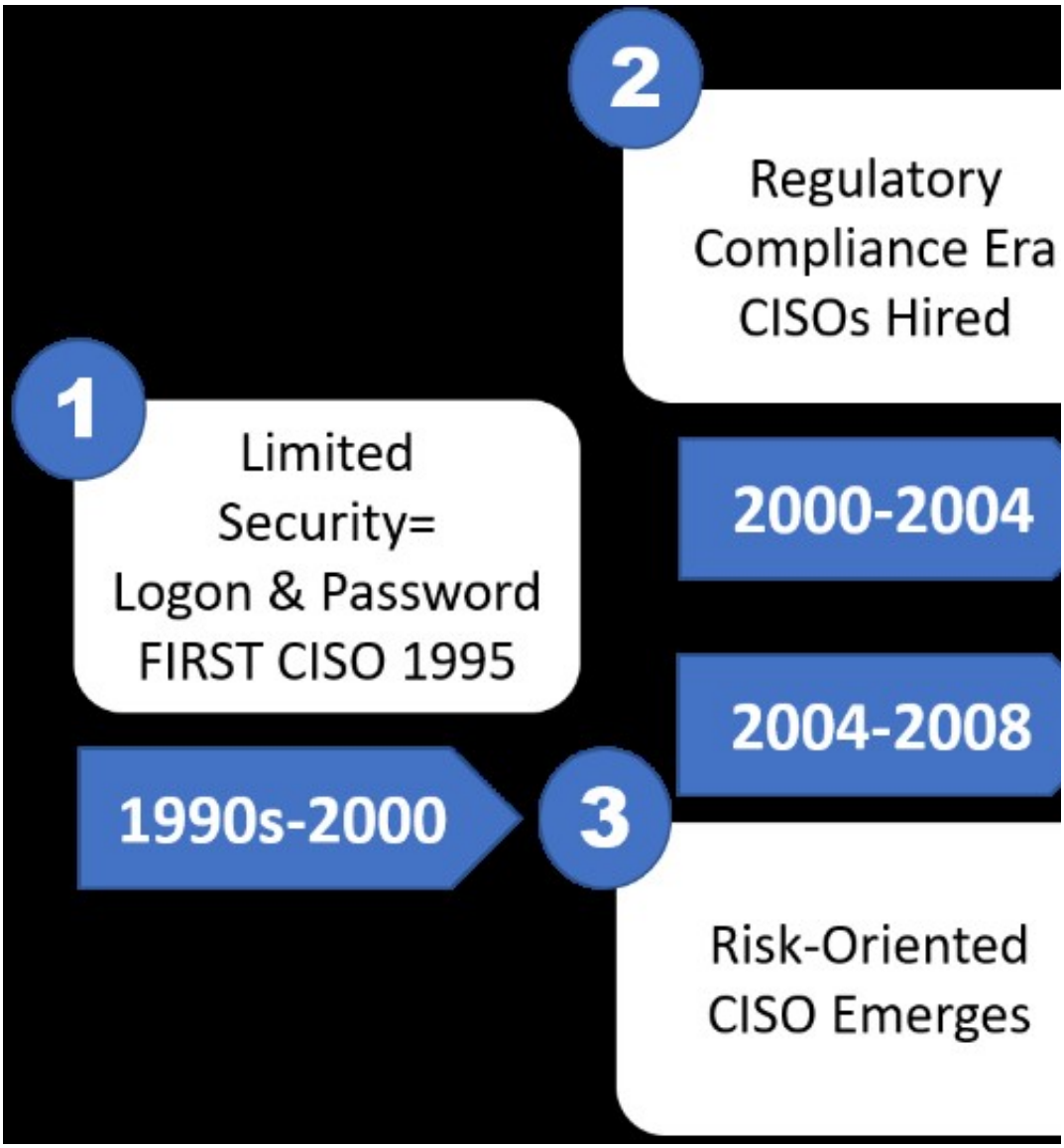
The 5 Stages of CISO Success, Past & Future

In cybersecurity, as in history, security leaders who forget the lessons of the past will be doomed to repeat them.

The chief information security officer (CISO) role may seem relatively new to those who work in organizations hiring their first or second CISO. However, it has been almost 25 years since Steve Katz was hired as the first CISO at Citibank. While few organizations would argue today that an organization does not need someone accountable for the cybersecurity program, the role is quite varied across organizations.

The position may exist at an executive level (i.e., executive or senior vice president role), a middle management role (director/manager) or may be an individual role combined with other system administration activities in a small organization. Whatever the level, to quote Harry Truman, what CISOs should know to be successful today is that the only thing new in the world is the history you *don't* know."

I believe the past teaches us that there are five distinct stages of CISO evolution that lead to a cybersecurity success story. Each stage had a different focus based upon the events at the time, as shown in the following diagram.



Graphic Source: Todd Fitzgerald

CISO Phase 1: The Limited Security Phase (Pre-2000)
Organizations secured their assets during this phase, but without the level of management and board of director awareness we have today. The function was typically buried in the data center and the main function was to provide logon access and authorization to files. As such, the function was primarily a technically oriented function.

2019 CISO Advisory: Technical skills are still necessary, but not sufficient for CISO success. Emphasis should be on breadth of technical knowledge across the entire infrastructure versus depth in a specific technology.

CISO Phase 2: Regulatory Compliance (2000–2004)
This phase saw the passage of a plethora of new laws addressing privacy and security in the healthcare, government, and financial sectors. It was during this period that the requirement for an "information security officer," commonly referred to today as the CISO, came into being for many organizations. Connectivity to the Internet and mainstream awareness of data breaches were

occurring. Company resources were mobilized to "check the box" for security compliance, typically adhering to a set of controls defined by ISO27001/2 or COBIT.

2019 CISO Advisory: The laws are ever-changing, and the CISO needs to be aware of laws affecting the organization, as well as the differences between the controls necessary to be compliant with each law. Successful CISOs will consolidate these requirements and tie implementation projects to satisfy multiple laws to reduce organizational change management disruption.

CISO Phase 3: Risk-Oriented CISO (2004–2008)
The "check-the-box" compliance phase did not live up to expectations because organizations could not afford to secure all the information equally. The movement to a risk-based approach facilitated allocation of funds to more critical assets and a better use of people, process, and technology. This also provided an inroad to corporate risk management and enabled a conversation of information security risk along with other organizational risks.

2019 CISO Advisory: CISOs must always look at controls in terms of probability and impact, recognizing the organization can choose to accept, mitigate, transfer, or avoid the risk. These risk strategies must be clearly defined and explicitly approved by management.

CISO Phase 4: Socially Mobile Cloud-Enabled Threat Aware CISO (2008–2016)
Just when the CISO was getting a handle on risk, new technologies were implemented, such as the introduction of social media on a mass scale, a smartphone in every pocket, consumerization of technology, and migration to the cloud. All of this happened in less than a decade, and the CISO had to adjust. The CISO could not say, "No, this technology is too risky."

2019 CISO Advisory: The technical environment today will substantially change within the next five to 10 years. Artificial intelligence, the Internet of Things, managed security service provider outsourcing, machine learning, quantum computing, blockchain, mobile applications, managing third-party vendor relationships, and different methods of managing these components will emerge, and the CISO will need to stay ahead of the curve to adapt. Always.

CISO Phase 5: Privacy and the Data-Aware CISO (2016–2020s)
Several major incidents involving the use of personal information for social media purposes beyond the expectations of individuals has given rise to an increased focus on privacy. The General Data Protection Regulation (GDPR), effective May 2018, also increased the visibility of data protection through the introduction of substantial fines as much as 4% of annual turnover (revenue). Organizations, until now, typically have been deficient in the management and retention of unstructured data as well as business ownership and access to the structured information within the organization.

2019 CISO Advisory: The CISO must have knowledge of the critical information assets, or crown jewels: where they are kept, for what purpose, and for how long. The CISO should become as knowledgeable in privacy laws and concepts as much as being knowledgeable of security practices. The CISO must know where the data is, how it flows through the organization, and how it is being secured. In the event of a breach, this information becomes crucial for the incident response teams.

We still have a long way to go to educate members of the workforce with their own roles with respect

to cybersecurity. As indicated in recent culture of cybersecurity research from ISACA and CMMI Institute, only 34% of employees, outside of the security team, adequately understand their role in the organization's desired cybersecurity culture.

Bottom line, in 2019 the CISO who understands the breadth of technology used and desired by the organization, complies with the regulations via control frameworks, assesses information asset risk, expands security beyond the organization (such as cloud, mobile, social media, threat intelligence networking), and knows how the privacy regulations affect the organization (where the data is, how it is being used, and how it is being protected) will be the CISOs in demand by their organization and others.

Author's note: *This evolution to CISO and the implications, along with an insightful interview with the first CISO, Steve Katz, are detailed in the author's newly released 2019 book, CISO COMPASS: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers.*

Related Content:

- Real-World Threats That Trump Spectre & Meltdown
- Think Twice Before Paying a Ransom
- Enterprise Malware Detections Up 79% as Attackers Refocus

Todd Fitzgerald has built and led information Fortune 500/large company security programs for 20 years. He was named 2016–17 Chicago CISO of the Year, ranked Top 50 Information Security Executive, authored four books — CISO Compass: Navigating ... View Full Bio