Inside the Interview
Excerpts that inspired episodes of CISO Stories from the acclaimed book, CISO Compass.

CISO Compass
Navigating Cybersecurity Leadership Challenges with Insights from Pioneers

Todd Fitzgerald
Foreword by Dr. Larry Ponemon

"Comprehensive Roadmap with Over 75 Top Chief Information Security Officers and Cybersecurity Leaders."
on security after the fact is both expensive in the real dollar impact, and politically expensive through the perception that the CISO was not engaged with the business to help. By designing sufficient controls from the start, the CISO may be able to improve the user experience through suggesting items such as biometric authentication (i.e., smartphone integration with Touch ID, operating system integration with facial recognition, or usage of mobile devices as proximity badges).

Engaging with the applications management team is a must to ensure that security is baked into the systems through a Secure Systems Development Life Cycle (s-SDLC) process supporting newer methods of development, such as Agile Development where Scrum masters serve as shepherds to ensure development is cohesive. Agile-developed applications are developed in Sprints—small pieces of the project are developed in iterations, and later iterations continue to “bite off” a little more of the project until completed. Or using a Dev-Ops approach whereby the communication between the traditional development and operations teams is increased, thought to be a by-product of Agile Development. Use of these concepts, combined with the leveraging of cloud technology, has increased the automation developer’s use within their jobs. Understanding these approaches will help the CISO understand how to be engaged in the development of new products and services within the IT organization.

GLENN KAPETANSKY: INTEGRATING SECURITY WITH SDLC/AGILE DEVELOPMENT

*Chief Security Officer, Trexin Group*

For a long time, I resisted working directly in the information security field. While at Bell Labs, we did not have a distinct security function—UNIX, the Internet, and Web were developed as open ecosystems with some trust assumed. But we did believe passionately in privacy, and that culture shaped my thinking.

I remained happy in IT operations for years. Later, on Mergers and Acquisition teams at banks and health-care insurers, I was able to shorten my due diligence time dramatically, often to 2–3 days. My trick was to focus on the Systems Development Life Cycle (SDLC) at the target company, very specifically on the protection of data as it moved from development, to test, into production. I invariably found this to be the weakest security in the company. This also shaped my thinking.

So, when challenged at ThoughtWorks to develop a framework for Secure Agile Development, my experience led me to split my advice into two parts: one for producing secure code, and the other for the preproduction environments that support the SDLC. I will spare you the details but share with you my conclusions:
Third-Party Outsourcing

As companies shift more processing overseas for the IT processing, many times the security administration/operations are also moved. This requires increased coordination with the offshore providers and an understanding of the functions remaining onshore and how they integrate with the offshore functions. For example, the testing of business continuity functions requires local business involvement, while the daily maintenance of the backups may be remotely covered offshore or be managed through a combination of internal and external data centers. Individuals may be dealing with service desks located in foreign countries and security administration functions supported by a combination of portals and staff. The countries supporting outsourcing may also be a patchwork of skills in multiple countries, leveraging the unique skills and cost advantages a country may offer. For example, technical resources may be more plentiful and cost-effective in India on a per-hour basis, and other countries such as the Philippines with an abundance of lower-cost, college-educated fluent English-speaking technical resources provide a large pool of resources to staff the call centers, where a projected revenue of $40 billion in call-center handling is expected by 2022 in the Philippines alone.

External/Internal Audits

Publicly traded companies are subject to SOX assessments made by external audit firms to ensure financial statements accurately represent the company’s operations and correct results. The audits provide insight as to whether the operations are adequately supported by the security controls, attesting to the adequacy of design.