Officers

Faced with escalating cyber threats and increasingly complex regulatory mandates, chief information security officers (CISOs) are experiencing growing pressure to protect critical information and infrastructure assets, while also embracing strategic ...

Aug. 26, 2015

Faced with escalating cyber threats and increasingly complex regulatory mandates,

CISO can no longer rely on his or her technical expertise alone. They must understand how strategic initiatives create risks and develop security programs that balance the need to drive business performance with the growing realities and complexities of protecting customers, intellectual property, and brand."

This can be especially challenging for CISOs who are new to their roles and those who are hired from outside and don't have deep knowledge of the organization. "One of the early expectations of a new CISO is that somehow you are going to step back and see the forest through the trees and be able to tell what you are going to do to make this security program take off. That is where the results of the Transition Lab came into play," added Powers.

"Going through the CISO Transition Lab enabled me to understand these dimensions and make choices about how I can better build my team as well as discern my role that enables me to give more value to my organization," said Tim Callahan, chief information security officer for insurance company, AFLAC, the largest provider of supplemental insurance in the US. "Given all the pressures of the job, without that, you're always putting out fires instead of having meaningful impact on the risk posture of the enterprise."

Findings from Deloitte's CISO Transition Lab reveal that the highest priority for 77 percent of Lab participants is to promote better integration of business and information security strategies, followed by improvement of data governance and protection. Improvements in the areas of security program governance and talent management are also named as key priorities.

Deloitte reports common challenges shared by new CISOs:

- Lack of resources and effective team structure

- Ineffective communications/reporting among stakeholders and throughout the

Four faces of the chief information security officer

- **Strategist**
  Drive business and cyber risk strategy alignment, innovate and instigate transformational change to manage risk through valued investments
- **Advisor**
  Integrate with the business to educate, advise, and influence activities with cyber risk implications
- **Guardian**
  Protect business assets by understanding the threat landscape and managing the effectiveness of the cyber risk program
- **Technologist**
  Assess and implement security technologies and standards to build organizational capabilities

Lab findings also indicate that, on average, CISOs today spend 77 percent of their time as "technologists" and "guardians" on technical aspects of their positions, and that they would like to reduce this investment to 35 percent. This demonstrates a recognizable shift in their desire to place greater emphasis on the "strategist" and "advisor" functions.

Deloitte's CISO Transition Lab is an immersive one-day workshop that allows a newly appointed or incumbent CISO to step out of their daily work to take a fresh look at their function. After conducting more than 25 labs in its first year, Deloitte's CISO Transition Lab continues to generate data and insights and highlights patterns in CISO priorities.

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us