Infosys
Navigate your next

VIEWPOINT

CYBERSECURITY AND THE NEW ERA OF ECOSYSTEMS

Digital transformation demands more than updated technology and business efficiency. Chief information security officers are under increasing pressure to secure their companies platforms, evaluate ecosystems, and find new ways to communicate risk to the rest of the C-suite.

Infosys | Knowledge Institute

Cybersecurity is best when it goes unnoticed outside an organization. It is the failures that move sentiment and stock prices. These dynamics put increasing pressure on chief information security officers (CISOs). A recent Infosys study shows that 96% of enterprises consider cybersecurity to be a top priority in their digital transformation efforts.

Basic cybersecurity hygiene is no longer enough. Successful companies must build a security culture and keep pace with the changing technology landscape, from expanded attack surfaces that accompany remote working to supply chain vulnerabilities. In response to these evolving and escalating risks, Infosys created a CISO Advisory Council to help peers share knowledge and evaluate how to combat threats.

The objective of this thought leadership forum is to evaluate cybersecurity strategies and frameworks, develop niche solutions, and build a culture of secure by design. The knowledge gained will allow CISOs to innovate more effectively and make their companies more secure and prosperous. These quarterly meetings, featuring CISOs from top multinational corporations, are conducted in private to enable free-flowing discussions. Here are some insights generated at the second Advisory Council meeting, which focused on platforms and ecosystems.

Cybersecurity's path toward zero trust

A CISO described his journey through the world of cybersecurity, from the early days of bespoke, pure-play solutions to concerns now about protecting data in the cloud or improving dashboards. In those formative days, he said that cybersecurity required many employees with highly technical skills and that reporting was "poor at best." Now, his current company is far along on its path to zero trust security (an Infosys priority) with the help of platforms and strategic partners. In his earlier experiences, company leaders were concerned about being trapped in an ecosystem relationship. While those concerns still have merit, he said the scale and synergies that these partnerships provide often outweigh potential risks.

Balancing cybersecurity platforms, ecosystems, and partnerships

Increasingly, CISOs must navigate the growth of platforms. Although the council was mostly positive about this trend, some had concerns, criticisms, and questions. For many CISOs, benefits and drawbacks can be industry specific as they take into account risk tolerances and priorities regarding portability. For some, budget has been a driving factor in the adoption of platforms and the creation of more strategic partnerships. "I have to make sure that the cost is low, and we simply can't meet our objectives without strong partnerships," said one CISO.

Another concern is what happens when the platform does not keep pace with the tools a company needs. Another CISO said, "We don't need perfect, but we do need good enough."

> It is crucial to be able to measure everything and get a unified view of the efficacy of a company's controls

Many companies avoid ecosystems because executives do not believe one single platform can address all the needs. They prefer to have the best of offerings that partners can provide, even if it means working with multiple companies. A council member mentioned that if a company relies entirely on a single partner, it will only be as smart as that partner.

Metrics are critical to determine the direction the organization takes with respect to cybersecurity. The ability to measure everything and get a unified view of the efficacy of a company's controls is crucial, noted a CISO.

Tech giants' expansion into cybersecurity

Cybersecurity's progress over the past decade has moved steadily toward more control and better reporting. Also, in that time, pure-play security companies disappeared as they were snapped up by tech industry giants, such as Cisco and Microsoft. A CISO council member said that the consolidation has offered customers opportunities to "consume more readily in an integrated way."

Another peer said the cybersecurity industry is either at an inflection point or almost there. With consolidation, platforms are constantly adding new capabilities. In the next couple of years, he said, CISOs and their companies will be in a better position to commit to an ecosystem without worrying that the decision could lead to security gaps.

But right now, he explained, there is still a lot of "churn" in the markets in certain areas. More consolidation is needed to solidify the existing platforms.

Growing leadership interest in cybersecurity

Security cannot be an afterthought. The consensus view among CISOs was that security needs a seat at the table from the beginning, particularly since cybersecurity has drawn greater interest from boards.

Increasingly, CISOs are explaining their cybersecurity strategies and operations in greater detail to business leaders and the board.

Infosys has prioritized this element of cybersecurity — coordinating multiple feeds to provide a single pane of glass showing the security posture, incidents, and other critical data to leadership. That offers "visibility into the state of affairs and visibility into the vulnerabilities," an Infosys executive explained. "You have to basically show them [leadership] where you are, instead of getting into the weeds of data."

> Regular independent third-party assessments help identify vulnerabilities and instill greater trust in cybersecurity operations

With greater prominence also comes heightened scrutiny from the board. Regular independent third-party assessments can help identify vulnerabilities and instill greater trust in the cybersecurity operations.

A CISO, whose company has been transformed by mergers and acquisitions, said one of his greatest challenges has been complexity. The company has more than 100 different ERP versions. However, the CISO's office has been in the driver's seat to some degree. He is levying "sin taxes" for units using outdated ERPs. Although the old versions save money in one area, they are costly in others due to the added risk. It is the only workable solution when you have a problem like this, he explained.

That evolutionary journey applies to the CISOs as well. Even as outside cybersecurity threats increase, CISOs will need to navigate changes and turmoil internally — whether it's greater scrutiny from leadership or trade-offs inherent in many new technologies.

Traditional security measures that were effective in earlier eras are no longer reliable. Meanwhile, the perimeter that organizations need to defend has grown exponentially; an entire ecosystem and global supply chain must now be safeguarded. The pace of change and the pressure to secure the systems will only grow as digital transformation accelerates and evolves. All the while, the boards and the rest of the C-suite will look to the CISOs for guidance and security.

Author

Jeff Mosier

Infosys Knowledge Institute

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.
To view our research, visit Infosys Knowledge Institute at infosys.com/IKI

For more information, contact askus@infosys.com

Infosys®
Navigate your next