CYBERSECURITY

CEO and CISO: a critical partnership for data management

Navigating a complex and rapidly evolving business landscape — especially in times of economic uncertainty — requires today's senior business leaders to be agile, forward-thinking and adaptive.

July 21, 2023

View Image Gallery

Navigating a complex and rapidly evolving business landscape — especially in times of economic uncertainty — requires today's senior business leaders to be agile, forward-thinking and adaptive.

They must devote time and energy to an array of interconnected imperatives: innovation and digital transformation, talent acquisition and retention, regulatory and legal compliance and governance, and the customer experience.

Senior executives must also devote more attention than ever before to cybersecurity. The exponential growth of data and increase in cyberthreats — from ransomware attacks to large-scale data breaches — threaten business imperatives. In such a fraught environment, the chief executive officer (CEO) needs a partner in guiding and defending the company's assets. The chief information security officer (CISO) is poised for the role.

LATEST IN CYBERSECURITY

Cybersecurity

What we can learn about data privacy from big tech's...

Arlo Gilbert July 20, 2023

Healthcare

Feds warn healthcare industry about security ris...

July 20, 2023

The CEO and CISO, working together, can master the two essential components of an effective cybersecurity strategy: data management and risk mitigation.

- **Data management** requires implementing robust policies and procedures that govern data collection, use, storage, and sharing. Effective data management ensures that data is accurate, consistent and secure while complying with relevant regulations and legal obligations. According to the 2023 Data Breach Investigations Report from Verizon, "83% of breaches are initiated by external attackers looking for quick financial gain." Adds *VentureBeat*, "Smash-and-grab attacks on customer and financial data are commonplace, with ransomware the weapon of choice.
- **Risk mitigation** is dependent on data visibility. When you have sharper insights into where your data resides, your organization is better positioned to mitigate data security risks. Better insights into your organization's data security landscape will help you better navigate the cybersecurity landscape, bolster your data security and risk mitigation measures, prioritize cybersecurity investments, and comply with regulatory requirements — all critical for doing business today.

Data visibility helps improve data resiliency and the ability to recover and continue operations in the face of disasters or cyberattacks that could result in data loss. An organization's data resiliency is built on a solid data governance foundation. Clear guidelines for data management will help identify and mitigate potential risks and vulnerabilities.

Your CISO: Valuable Insights

So what does this C-Suite collaboration look like?

A crucial task CISOs must face is understanding where mission critical data resides. IT teams manage enormous amounts of organizational data from untold disparate sources.

On- and off-premises servers, third-party suppliers, applications, employee computers and storage clouds, to name a few, all contain organizational data that needs to be monitored, tracked and kept out of the wrong hands. The CISO should help the CEO understand where all this data resides and how the IT team protects it.

The second task is understanding how much data the organization is housing. In addition to the data being actively used, an organization's dark data — such as old emails, HR records of former employees and presentations — must also be governed. This data often remains hidden or forgotten within organizations. Dark data is often attractive targets for hackers. If dark data is exposed during a ransomware attack or a leak, it could have severe financial and reputational consequences for organizations.

CISOs can help implement and oversee strategies that improve data visibility practices. These include:

- **Inventory data through data mapping.** Create an inventory of all data that your organization collects, processes, and stores. This includes data stored on-premises, in the cloud, or by third-party vendors and suppliers. Once the data is mapped, organizations can

MOST READ

School security professionals assess the Parklan...

Schools must be extra vigilant against mass...

Healthcare in the crossfire of mental health crisis,...

identify any gaps in their data protection and compliance strategies and take steps to address them.

- **Use data discovery and data visualization tools.** These tools scan an organization's network and systems to identify data sources and provide detailed information on the data's location, type, and sensitivity. This information can be used to better understand the organization's data landscape, improve data security, and ensure compliance with relevant data regulations.
- **Leverage advanced data analytics solutions.** These tools enable real-time analysis of large data volumes, providing valuable insights and uncovering hidden patterns and trends. By visualizing complex data sets, organizations gain a deeper understanding and make informed decisions.
- **Establish robust data governance practices.** Clear policies and procedures for data management, including classification, ownership, and stewardship, ensure data accuracy, security, and compliance with regulations.
- **Centralize data.** By consolidating data from different sources into a unified repository, organizations eliminate data silos and achieve a holistic view of their information. This centralized approach enhances accessibility, data quality, and consistency.
- **Secure data.** Once data is located, various strategies must be implemented to secure it. These include maintaining a patching discipline, robust identity and access management, multi-factor authentication, mature vulnerability management, anti-malware software, endpoint protection, modern data loss prevention techniques, rigorous security monitoring, and comprehensive employee cybersecurity training.

Rising to the challenge

In addition, as global data regulations continue to evolve, understanding your legal obligations is critical. Companies like DFIN help organizations stay current with the latest rules, proactively address potential risks and vulnerabilities, and enhance their customers security posture and resilience.

Why must the CEO be actively involved with these complex security issues?

Times are changing. Cybercriminals are far more sophisticated than they were just a few years ago. The threat they pose to business operations is far more grave. Increasingly, boards of directors, customers, and other stakeholders want to be reassured that the company's cyber strategy is robust enough to weather powerful attacks. Consequently, the CISO's role has taken on a new importance.

Working together, the CEO and CISO can meet the evolving data threat landscape. They can elevate the company's defenses to where they need to be in a fast-moving and dangerous world.

Craig Clay is president of global capital markets for Donnelley Financial Solutions, a leading global risk and compliance solutions company. Clay joined DFIN in 2016 to lead the company's business strategy and support customer and market growth worldwide. Under *his leadership, Clay was instrumental in transforming what was once a financial division of RR Donnelley into the leading regulatory and financial technology organization it is today. Before joining DFIN in 1995, Clay was executive vice president of capital markets and global sourcing, RR Donnelley. He also served as leading financial analyst for American Eurocopter Corp.*

CONTINUE READING

Schools must be extra vigilant against mass shootings in April

School security professionals assess the Parkland trial and verdict

SPONSORED RECOMMENDATIONS

CEO and CISO: a critical partnership for data...

Navigating a complex and rapidly evolving business landscape — especially in times of economic uncertainty — requires today’s senior business leaders to be agile, forward-thinking...

What we can learn about data privacy from big tech’s...

If it’s bad form to break into someone’s home and steal their valuables, organizations shouldn’t use private data without consent

The enhanced role of security guards in cannabis operations

Owner/operators must be realistic in their expectations and create strong oversight for personnel

Feds warn healthcare industry about security risk...

The FTC and HHS' Office for Civil Rights say websites and mobile apps may be impermissibly disclosing consumers’ sensitive personal health data to third parties.

Load More Content

SIW SECURITY INFOWATCH.COM