Want Cyber Safety? Focus On Your Data

Katie Kuehner-Hebert

From incident response plans to employee training to staying on top regulatory demands, cybersecurity has become a complicated—and critical—area, notes Dannie Combs, CISO at Donnelley Financial Solutions. Here's what to know.

Cyber threats are only getting worse – how can IT professionals best protect their organizations?

Dannie Combs shares how. Combs is senior vice president and CISO of Donnelley Financial Solutions, a global risk and compliance solutions company based in Chicago.

What are the best risk management strategies organizations can implement to mitigate data cybersecurity threats?

Organizations need to have a strong risk management posture with robust strategies in place. With risks to data ever evolving, mitigating data cybersecurity threats requires a comprehensive and proactive approach that includes risk assessments and incident response plans, implementing multi-layered security measures such as deploying firewalls, intrusion detection systems, encryption protocols, regular software updates and patches—as well as employee training and staying informed and ahead of the latest threats. Understanding your global regulatory and legal obligations is another critical element of risk management.

How can organizations get better visibility into their data?

When you have sharper insights into your data management practices, including visibility into where your data resides, your organization is better positioned to mitigate data security risks.

Considering the unprecedented amounts of dispersed data that IT teams are required to manage, data visibility can be complicated. Data may live on-premises and off-premises, throughout the IT infrastructure, devices like smartphones and laptops, file servers, applications, third-party suppliers and the cloud. To improve data visibility, organizations can implement various strategies:

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

MORE INSIGHTS

Want Cyber Safety? Focus On Your Data

How Office

decisions.

- **Establish robust data governance practices.** Create 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.

Why is managing identities such an important part of an organization's cybersecurity strategy?

Identities are the gateway to an organization's systems and sensitive data—and the compromises to digital identity are growing exponentially. In fact, 74 percent of all breaches are caused by the human element through error, privilege misuse, social engineering or use of stolen credentials, according to the 2023 Verizon Data Breach Investigation Report.

That's why managing identities and identity access management are essential to an organization's cybersecurity strategy. Proper identity management enables organizations to enforce granular access controls and permissions to ensure that only authorized individuals gain access to their networks and resources. By enforcing a model of least privilege, we can be more confident that access to datasets is appropriately limited to what we need, not necessarily what we want.

To help strengthen an identity management posture, I recommend that enterprises focus on identity governance administration and privileged access management technologies as well as evaluate their current IAM framework.

Fortunately, there has also been a remarkable uptick in the emphasis on IAM for user accounts, privilege levels of applications, administrative roles and even customer accounts. By establishing robust identity and access management systems, organizations can identify suspicious activities, such as unauthorized access attempts or unusual patterns of data access, enabling swift response and mitigation.

What are the latest data regulations that companies need to be aware of?

Staying on top of and complying with the latest data regulations to ensure the protection of data is imperative in today's business landscape. You likely already know about these important data regulations:

- General Data Protection Regulation
- California Consumer Privacy Act
- Health Insurance Portability and Accountability Act
- Payment Card Industry Data Security Standard
- New York State Department of Financial Services Cybersecurity Regulation
- Children's Online Privacy Protection Act
- European Union Network and Information Security Directive
- Personal Information Protection and Electronic Documents Act
- Brazilian General Data Protection Law

New regulations and laws within the United States and worldwide continue to evolve, with several new bills working their way through Capitol Hill. For example, the RESTRICT Act, if passed, will restrict data movement significantly.

Known as Restricting the Emergence of Security Threats that Risk Information and Communications Technology Act, the bill is intended to address technology-based threats, giving the U.S. Department of Commerce power to regulate technology produced by countries that have adversarial relationships with the U.S.

The Securities and Exchange Commission proposed new rules related to cybersecurity risk governance and mandatory cybersecurity incident reporting. The proposed rules require companies to establish policies and procedures for identifying, assessing, and managing cybersecurity risks and incidents, as well as to provide disclosures to investors regarding such risks and incidents.

Katie Kuehner-Hebert

Katie Kuehner-Hebert has more than two decades of experience writing about corporate, financial and industry-specific issues. She is based in Running Springs, Calif.

Surveillance Can Backfire

5 Tactics To Protect Your Business Against Cyberattacks This Holiday Season

When It Comes To AI, Sometimes You Have To Do It Yourself

It Isn't All About Tech

How One Company Is Using AI

interviews.

First | Last

Email

SUBSCRIBE

StrategicCIO360
a Chief Executive Group community

StrategicCIO360.com is powered by **Chief Executive Group**, publishers of *Chief Executive* and *Corporate Board Member* since 1977. CEG exists to improve the performance of business leaders, build communities and strengthen society. Visit chiefexecutivegroup.com to learn more.

GET IN TOUCH

203.930.2700
contact@chiefexecutive.net

FOLLOW US