SECURING DATA
THE NEW OIL OF THE DIGITAL ECONOMY
The Highest Level of Security on the Go

MILITARY GRADE SECURITY * AFFORDABLE * EASY TO DEPLOY / MANAGE * MADE IN THE U.S.

SPYRUS Solutions provides the strongest protection of data in motion, at rest and in use. For 20+ years, SPYRUS encryption, Multi-factor Authentication, and digital signature and content products have enabled customers to meet stringent Public and Private regulatory data protection requirements with the highest level of confidence. FIPS 140-2 Level 3 validated, anti-tamper USB and microSD tokens offer protection for any after market computing / IoT device; our Rosetta security chip provides OEM partners with equivalent onboard security; and our DevicePatrol™ platform enforces enterprise policies to all Rosetta protected user or unattended devices.

www.spyrus.com
**EDITOR’S NOTE**

Security is paramount for customer data

As the U.S. elections draw near, I am reminded of the Facebook-Cambridge Analytica data breach reported in early 2018. Without consent, personal data of millions of Facebook users was allegedly harvested and sold to Cambridge Analytica for political advertising. The massive data scandal eroded Facebook’s reputation, and users closed their accounts and abandoned the social media giant with disdain. Remember the #DeleteFacebook online movement? That one incident changed the world and became a talking point in data privacy discussions.

If this incident were to be repeated today, the organizations involved could be heavily penalized with stiff fines imposed by GDPR, CCPA, and other regulatory norms.

But our story is not about fines and loss of reputation.

Organizations are responsible for protecting customer data, personally identifiable information, confidential data, intellectual property, and transactional data. Data sovereignty and data residency are on the compliance checklist.

Governments, CISOs, and CDOs (Chief Data Officers) need to have a holistic approach and ensure Data Security, Data Governance, and Data Integrity through stringent compliance and policies. They must ensure that data access is strictly on a need-to-have basis. These are the tenets for customer trust, loyalty, and the reputation of an organization.

With enterprise infrastructure increasingly moving to the cloud, an organization’s data is in transit through public networks. It goes to the cloud for processing and is momentarily held in storage buckets or data lakes; it could go to a partner’s network or database. It is likely to transgress borders at lightning speed and go to servers in other regions and availability zones (a matter of great concern for government and regulators). It then comes back to storage/a database and finally ends up in archival or offline backups. So, it is necessary to secure data wherever it exists – throughout the data life cycle.

It is common for enterprises to host their infrastructure in hybrid, multi-cloud environments. In this scenario, it is vital to implement a singular data protection strategy across an enterprise, on-premise, and hybrid and multi-cloud environments.

This issue of CISO MAG includes our third Market Trends report for the year on Data Security. The aggregated findings in the report are confirmed by 231 survey respondents and validated by industry experts.

Our latest report observes that 80.95% of respondents want to protect Contact/Identity information, and 77.92% are particular about Financial/Banking data. Secondary importance is given to Medical Records/EHR, location data, and Biometric data.

This issue of CISO MAG includes our third Market Trends report for the year on Data Security. The aggregated findings in the report are confirmed by 231 survey respondents and validated by industry experts.

Please read the full report on page 54 for other revealing data points and insights.

Our next Market Trends report will be released in December, focusing on Endpoint Security.

We hope you enjoy reading all the other articles in this issue as well.

Please write to us at editorial@cisomag.com.

Jay Bavisi
Editor-in-Chief
CISOs and CIOs are not aware that chatbots need protection: Chaitanya Hiremath, CEO, SCANTA INC.

Data Security Requires a Holistic View

Data Security - The New Oil of the Digital Economy

Managing IoT Data Security Risks - The Need to Secure Data in Modern Computing
If you aren’t Phishing your staff, somebody else might be!

Web search results hijacked by cybercriminals to distribute malware

Using public Wi-Fi especially insecure networks that do not require a password

Unsolicited attachments (high-risk file types such as .exe, .scr & .zip)

Text messages that create a sense of urgency, panic, greed, curiosity or fear

Emails pretending to come from trustworthy sources such as banks or credit card companies

Spear phishing emails with the usage of corporate logos and other identifiers

Click for your free demo!
Join us, where the African Infosec Community will meet. And witness gripping discussions, engrossing keynote sessions and engaging innovation addresses.

17th September, 2020
Nigeria (9:55 AM) - South Africa (10:55 AM)
Kenya (11:55 AM) - Egypt (10:55 AM)

REGISTER NOW

300+ Infosec Leaders
100+ Top Companies

Individuals Corporates Startups Government Products Academia
KEY QUESTIONS FOR IMPLEMENTING STRONG SECURITY AND COMPLIANCE PROGRAMS

Jason Taule
Vice President of Standards & CISO
HITRUST
To arrive at the right answers, one first needs to ask the right questions! CISOs who discover that their actions do not generate the desired results to strengthen security and compliance postures may not be asking the right questions. Effectively managing data, information risk, and compliance is complex and ever-changing. There are many components and considerations in developing and implementing a robust program that encompasses and integrates all the elements needed to manage risk and achieve one’s compliance objectives effectively. A critical component is making sure to ask the right questions of the right people.

The right questions include those that CISOs should ask themselves as well as the management team, the operations team, and other key stakeholders, including the Board of Directors. CISOs who come up with the questions on their own will likely tailor the questions to their situation and environment — often driven by functional and operational priorities that may not directly line up with the top-line business objectives. More specifically, an ad-hoc approach usually overlooks some of the core questions that matter in establishing a strong security and compliance posture.

**Answer the Right Questions to Drive Business Results**

By collaborating with people from across the organization and asking questions focused on risks and controls tied directly back to the business, CISOs can drive decisions that truly get at what the organization needs to achieve the security and compliance postures the business is seeking. This, in turn, leads to an action plan to produce the desired business results.

The ad-hoc approach perpetuates managing the security and compliance program in a reactive fashion — where the focus is only on the immediate situation at hand. How should CISOs avoid situations where they have to ask themselves, “Where did I fail the business?” They can do this by taking a results-driven, proactive approach adopted by others in their industry. They can work with internal stakeholders to adopt a set of questions that demonstrate how to get to the “why” behind their security and compliance programs.