Empowering Your GRC Program with Actionable Cyber Intelligence

Posted on April 9, 2024

Governance, risk, and compliance (GRC) is a threefold strategy for managing an organization's overall structure, potential risks, and regulatory adherence. Today's increasing regulatory complexity, data privacy concerns, and evolving cybersecurity risks are driving the market, which is projected to reach US$104.5 billion by 2030.

GRC has come a long way since organizations saw its significance in the early 2000s. From using Excel spreadsheets and performing each GRC component separately, today's professionals can now employ platforms to automate almost any relevant business process.

However, not all GRC solutions are created equal. Those that stand out help organizations address the growing challenge of obtaining consistent, high-quality information to inform their GRC efforts.

How Does GRC Implementation Work?

73% of cyber executives and business leaders view data privacy and cybersecurity regulations as effective tools for minimizing cyber risks. Therein lies the value of GRC that goes beyond regulatory compliance and combines governance, risk management, and regulatory compliance in a single comprehensive and integrated approach.

Implementing GRC effectively and efficiently requires organizations to leverage solutions with advanced technological capabilities to enable tasks like internal auditing, risk assessment, and compliance monitoring.

These solutions become more powerful when augmented with complete, accurate, and up-to-date

cyber intelligence, including DNS, IP, and domain data. The quality of the data fed into a GRC platform is crucial to generating reliable insights to improve governance, intensify risk mitigation, and support regulatory compliance.

Improving Governance through Digital Infrastructure-Wide Audits

Internal audits are critical aspects of an organization's policymaking process. They enable organizations to identify policy gaps and weaknesses and improve corporate policies. However, traditional audits may be limited when it comes to comprehensively and ongoingly assessing an organization's digital infrastructure.

Utilizing reliable and accurate DNS, IP, and domain intelligence in internal audits allows organizations to gain visibility into Internet-facing properties that are often sprawled and consequently overlooked. The auditing insights gained from these cyber intelligence sources can support evidence-based policymaking.

Take, for instance, a digital infrastructure-wide audit of all domains and subdomains containing a company's trademark or brand names. WHOIS database queries can reveal hundreds (in many cases, even thousands) of domains registered and used by external parties. While some of these web properties may be innocently parked, GRC professionals can uncover malicious campaigns, such as:

- **Phishing attacks:** Threat actors may register domains with slight variations of a company's domain name to trick users into visiting phishing websites.
- **Unauthorized brand use:** Third parties can use domains containing a company's trademark without permission in counterfeiting and impersonation campaigns, potentially diluting its brand's value.
- **Brand abuse:** Malicious actors can use cybersquatting domains to launch smear campaigns or spread misinformation about an organization.

Based on these findings, an organization may develop or improve security policies and procedures to address typosquatting.

Intensifying Risk Management Efforts with Multibranched Intelligence Sources

Digital risks can come from various directions (e.g., internal vulnerabilities, third-party vendors, supply chain channels, and even customers). GRC professionals need Internet-wide access to multibranched intelligence to keep up with existing and emerging risks, including those related to geolocation, supply chain, and domain-based attacks.

Geopolitical Risks

Most business and cyber leaders believe that geopolitical instability worldwide can possibly lead to a disastrous cyber event in the next few years, prompting them to respond to geopolitical risks through efforts, including:

- Strengthening policies and practices for third parties with direct access to organizational data
- Strengthening controls for third parties that process data
- Reevaluating the countries where their organization does business
- Verifying if suppliers are based in sanctioned or restricted areas

IP-related intelligence containing geolocation, Autonomous System (AS), and ISP data can help inform these geopolitical risk management strategies.

Third-Party Risks

Threat actors have been targeting supply chains more frequently, aiming to victimize as many organizations as possible with one attack. The most recent example is the Okta data breach that gave hackers access to the data of 99.6% of the company's customer support system users.

To minimize the risk of similar incidents, IP netblocks and WHOIS databases can help identify and investigate domains and IP ranges that organizations and individuals use to interact with corporate networks. Moreover, ownership and administrative details gleaned from these databases can inform vendor vetting activities, aiding organizations in performing due diligence.

Domain-Based Cyber Attack Risks

Domain spoofing or typosquatting, domain hijacking, distributed denial-of-service (DDoS) attacks, and malware distribution are classic examples of cyber attacks that utilize domain names.

Leveraging DNS and domain intelligence can help organizations minimize their exposure to these threats by:

- Identifying newly registered domains (NRDs) with characteristics often associated with malicious activity
- Monitoring domain registrations for variations of an organization's legitimate domain names
- Analyzing DNS records to identify the infrastructure behind a malicious domain
- Investigating traffic patterns and identifying suspicious activity that may indicate a DDoS attack in progress

Support Regulatory Compliance

Organizations may need to demonstrate compliance with not just one but various regulatory frameworks. However, among the common mandates across most regulations and frameworks is to show proactive cybersecurity efforts and have procedures in place to detect security incidents promptly and respond effectively. Below are some examples.

- **ISO 27001:2022:** This is the international standard for information security management systems (ISMSs) requiring organizations in many sectors to identify and assess information security risks and implement controls to mitigate them. One of the standard's recommendations is to use threat intelligence (Annex A control 5.7) to examine an

organization's threat environment and identify emerging threats, vulnerabilities, and potential attack vectors. Threat intelligence data feeds containing up-to-date lists of indicators of compromise (IoCs) can aid in complying with this mandate.

- **NIST CSF 2.0:** The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) has been widely adopted by various organizations across several industries. The new version now has six core functions—Govern, Identify, Protect, Detect, Respond, and Recover. The Identify, Protect, and Detect core functions require organizations to integrate cyber threat intelligence and other contextual information (e.g., domain, IP, and DNS data) in detecting and analyzing adverse events. For further insights into NIST CSF 2.0 and the role of cyber intelligence in achieving compliance, check out our in-depth article on this topic.

- **Payment Card Industry Data Security Standard (PCI-DSS):** PCI-DSS outlines a set of controls that merchants must implement to safeguard cardholder data. The standard requires organizations to have a complete inventory of all their IT assets and monitor changes in their DNS configurations. Furthermore, analyzing DNS records helps identify external domains and IP addresses that interact with the cardholder data environment, helping merchants detect unauthorized data transfers or potential data exfiltration attempts.

Conclusion

GRC professionals often struggle with fragmented data residing in different systems, limiting their visibility and making it difficult to implement programs. While they can easily leverage the technological capabilities of various GRC platforms available in the market, the challenge lies in tapping high-quality and unified data.

WhoisXML API cyber intelligence sources can help address this challenge by providing extensive and adjacent DNS, IP, and domain data. By integrating these intelligence sources into existing GRC platforms, professionals can obtain a unified view of digital risks, enhance threat detection capabilities, improve regulatory compliance, and streamline incident response.

Learn more about how WhoisXML API's comprehensive cyber intelligence sources can enable and empower GRC platforms. Contact us now.