GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Vishnevetsky, Genady ; Missimore, Cory & Schaufenbuel, Bradley

"Rating Criticality of Data Assets"

Risksense.com

RiskSense Inc.

23 January 2019

The URL: https://risksense.com/rating-criticality-of-data-assets/

Accessed: 15 August 2019

Synopsis: There are no standard methods for calculating the value of a business's data, and insurance companies generally do buy cover for lost data. Yet many businesses consider data to be their most valuable asset. Critical business data can include soft assets such as intellectual property, proprietary software and processes, financial data, customer data, supplier data, market data, historical business data, media, research, and other kinds of information. Cory Missimore, assistant manager information security at Bloomberg BNA, points out the changing role of data in business operations. "Business intelligence, which was traditionally forward-facing analysis on competitors' or potential clients' strategies and technologies, has now turned internal to the organization itself. Knowing what data is being held within an organization, how it is being used, and why it is being used has enabled C-suite personnel to understand their internal processes, their risk posture, and how current and potential new endeavors can expose or support the organization. In other words, executives can now make more informed decisions for their organization, balancing the need to protect their business while simultaneously running and expanding it."

Rating Criticality of Data Assets

by Genady Vishnevetsky | Jan 23, 2019

Rating Criticality of Data Assets

Article written by: Genady Vishnevetsky (Chief Information Security Officer, Stewart Title), Cory Missimore (Assistant Manager, Information Security, Bloomberg BNA), and Bradley Schaufenbuel (CISO, Paylocity)

There are no standard methods for calculating the value of a business's data, and insurance companies generally do buy cover for lost data. Yet many businesses consider data to be their most valuable asset. Critical business data can include soft assets such as intellectual property, proprietary software and processes, financial data, customer data, supplier data, market data, historical business data, media, research, and other kinds of information. Cory Missimore, assistant manager information security at Bloomberg BNA, points out the changing role of data in business operations. "Business intelligence, which was traditionally forward-facing analysis on competitors' or potential clients' strategies and technologies, has now turned internal to the organization itself. Knowing what data is being held within an organization, how it is being used, and why it is being used has enabled C-suite personnel to understand their internal processes, their risk posture, and how current and potential new endeavors can expose or support the organization. In other words, executives can now make more informed decisions for their organization, balancing the need to protect their business while simultaneously running and expanding it."

Any company with a vulnerability- management program needs to include an evaluation of the criticality of data assets as part of an overall cyber-risk assessment. That's because protecting data that is most critical to ongoing business operations needs to have highest priority. Rating data assets criticality is essential for properly managing and prioritizing risk mitigation. As Genady Vishnevetsky, chief information security officer (CISO) at Stewart Title, notes, "There always will be more threats and vulnerabilities than we have the capability to address. When you know what your crown jewel is and where it is located, you can focus on making the biggest impact on protecting your business. Start with assigning criticality to your data."

Bradley Schaufenbuel, VP-CISO of Paylocity, suggests that data criticality is the key criterion for prioritizing security efforts. “Data criticality should be the primary input into a business’s operational decisions about cyber-risk mitigation,” he says. “The level of effort made and resources expended to manage cyber risk should be directly proportional to the criticality of the underlying data being protected.”

But how do you decide which data is your most critical and therefore requires your strongest protection? Missimore says if you are already using a security framework, that may a good place to start. “There are many methods, frameworks, and tools, available for users to understand the assets, both physical and logistical, within an organization. There are also tools that can help identify assets within an organization. Coupled with frameworks such as the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO), these can provide context for interpreting the results we need to help apply appropriate risk ratings and corrective-action plans,” he says.

Vishnevetsky points out that rating the criticality of data assets differs from one business to another, and it ties closely to how your business operates. “There is no silver bullet as data criticality is different from business to business. It will be a manual process. Determine how your company makes money and what are the regulatory requirements applicable to your business. Then use data-discovery tools, both network and agent-based, to determine where the critical data your business needs to survive is located.”

Schaufenbuel suggests developing a rating system that scores data criticality based on how it is accessed, used, and regulated. “I would contend that a data-criticality rating should be set based on the confidentiality, integrity, and availability

requirements for the data as well as its volume. The more extensive the confidentiality, integrity, and availability requirements for data are, and the more of it there is, the greater its criticality rating should be."

In keeping with other recommendations about scoring cyber risk, a good data-criticality score should take into consideration the impact to the business if that data were lost. Additionally, for criticality scores to be most useful to decision-makers, the scores should be kept simple and meaningful.

Key Points

1. The level of effort made and resources expended to manage cyber risk should be directly proportional to the criticality of the underlying data being protected.
2. A data criticality score should take into consideration the impact to the business if that data were lost. Additionally, in order for criticality scores to be most useful to decision makers, the scores should be kept simple and meaningful.

CONTACT US

Most Recent Blogs

The Art and Science of Predicting Weaponization >

Finding and Patching the Microsoft 'BlueKeep' Vulnerability (CVE-2019-0708) >

Adobe Spotlight Research Report – 2018 Vulnerability Weaponization Top Concern >