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

Dugas, Thomas & McDorman, Doug

"Rating Criticality of Technology Assets"

Risksense.com

RiskSense Inc.

21 January 2019

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

Accessed: 15 August 2019

Synopsis: A key task of any cyber-risk assessment is determining which technology assets are most important to the business. The most critical assets are ones that the business depends on most to continue its normal operations, or assets that would cause an existential threat to the business if compromised. For instance, if an airline company's ticketing system goes down, it has to cancel flights even if there's no physical reason why the airplanes can't fly. That makes the ticketing system a highly critical asset to the airline company.

RISKSENSE

CONTACT US

Rating Criticality of Technology Assets

by Thomas Dugas | Jan 21, 2019

Rating Criticality of Technology Assets

Article written by: Thomas Dugas (CISO, Duquesne University) and Doug McDorman (Principal Security Architect, T-Mobile)

A key task of any cyber-risk assessment is determining which technology assets are most important to the business. The most critical assets are ones that the business depends on most to continue its normal operations, or assets that would cause an existential threat to the business if compromised. For instance, if an airline company's ticketing system goes down, it has to cancel flights even if there's no physical reason why the airplanes can't fly. That makes the ticketing system a highly critical asset to the airline company.

In a complex technology environment where there's lots of integration and interdependence between technology assets, rating asset criticality is essential for properly managing and prioritizing vulnerabilities. As Doug McDorman, principal security architect at T-Mobile, says, "Cybersecurity engineers and architects are limited resources. Prioritizing where to apply those resources more heavily requires a risk- centric approach."

Several interrelated factors go into rating the criticality of technology assets as part of a broader risk-scoring and cybersecurity strategy. For example, the criticality of a piece of infrastructure, such as a server, may depend on how important it is to a key business operation, but also how critical the data is that it hosts. These considerations become central to decisions about how to allocate security resources. Thomas Dugas, chief information security officer (CISO) and director of information security at Pittsburgh's Duquesne University, explains, "Duquesne University is currently building a vulnerability management program (VMP) that identifies and rates assets based on the level of data they host. Duquesne University has three levels of data: 1. restricted data which is compliance regulated and PII and poses great risk to reputation or finances if exposed; 2. private data which is limited to internal use only and poses moderate risk to reputation and finances if exposed; and 3. public data that is widely available

and has no risk to reputation or finances if exposed. Identifying which assets host our most sensitive data is critical for how we protect the confidentiality, integrity, and availability of those assets."

This is a great example that illustrates using the criticality of data assets that touch the IT infrastructure as an indicator of where to focus infrastructure- hardening efforts (see the article "Rating Criticality of Data Assets"). "By looking at what assets are critical infrastructure for your business, classifying your data, and applying a risk-based scoring methodology, you can identify the assets requiring prioritization," says McDorman. "The end result may take a variety of forms, including a more in-depth threat model, requirements for multifactorial authentication, encryption, privileged access management, or more extensive auditing, logging, and monitoring."

One challenge in rating the criticality of technology assets is deciding what kind of scale you should use. The scale needs to be useful and meaningful to decision-makers who are part of the resource-allocation decision process but may not be security experts. This would include senior management and financial management. Dugas explains his approach. "We have leveraged a variety of resources to help assess the criticality of technology assets. We are working on our compliance to NIST 800-171 and are leveraging aspects of the NIST Cybersecurity Framework which recommends ways to identify and classify assets. We also look at the Common Vulnerability Scoring System (CVVS) to assess a vulnerability rating against our risk. We often have mitigating controls which may help with reducing the risk and thus changing our internal priority."

In addition to deciding on a useful rating system, one must also do the hard work of finding all your technology assets. This in itself can be a challenge, especially in the kinds of distributed

IT infrastructures and infrastructure-as-a-service environments that are becoming so common today. It may require special expertise and tools, yet it is an essential part of the process that must be thorough and ongoing to avoid gaps in a mitigation strategy.

Rating criticality of technology assets is important work, and as Dugas's comments indicate, it is part of a broader risk-assessment process. This broader cybersecurity risk assessment is a foundation for more than just making decisions about prioritizing security efforts. It also becomes a fundamental consideration for any business decision in which factoring in risk plays an important role.

Key Point:

1. In a complex technology environment where there's lots of integration and interdependence between technology assets, rating asset criticality is essential for properly managing and prioritizing vulnerabilities.
2. In addition to deciding on a rating system, you must find all your technology assets. This can be a challenge, especially in the kinds of distributed IT infrastructures and infrastructure-as-a- service environments that are becoming so common today.

Most Recent Blogs

The Art and Science of Predicting Weaponization >

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