Risk assessment
A vital step in cybersecurity development

Adapted from:
http://searchcompliance.techtarget.com/tip/Risk-assessment-a-vital-step-in-cybersecurity-program-development
Written By: Jeffrey Jenkins

Why risk assessment is a good starting place

To protect digital information, companies must first determine where their biggest risks lie. In this tip, learn why risk assessment analysis is an important first step when crafting a cybersecurity program.

Most organizations understand the need for a cybersecurity program to protect data -- whether it's people's PII, entire IT systems or sensitive financial information. Determining exactly how to provide that security, though, is where risk assessments become critical to the success of a cybersecurity program.

Trying to apply all security principles and controls to every system, piece of data and process is nearly impossible, much less sustainable. It also typically undermines the credibility of the cybersecurity program as a whole. Imagine, for example, taking all the security controls from some of the more stringent standards or regulations, like PCI DSS or FISMA, and applying them to every server, device, file and user that touches your network. Not only would it not make sense to spend money protecting non-sensitive information or systems, but security functions like monitoring and responding to hacking attempts or vulnerabilities would be ineffective, given that cybersecurity and IT staff would likely respond to numerous non-critical security incidents.

The "value" of risk assessments to a cybersecurity program is that they help identify the risk associated with using a particular information system or type of data. Understanding risk helps an organization prioritize what it should be most concerned with protecting, provides guidance as to how to best protect those systems or data, and helps determine what should (or possibly shouldn't) be invested to protect those assets. In more specific terms, the value of risk assessments can range from financial savings (by concentrating security spending on the company's most sensitive systems and data) to loss mitigation (by keeping personnel and monitoring systems primarily focused on and responding to threats against critical assets).

Where to target your cybersecurity risk assessment

Risk assessments can vary significantly from organization to organization, but most capture at least the following pieces of information:

The sensitivity and/or criticality of the system or data. For example: What would the impact be to the organization if the system or data were not available?

The threats that put the system or data at risk. For example, if an Internet-facing server is exposed to malware or hacking attempts, what critical data being is at risk?

The value of the system or data to the organization. For example, what would be the monetary or reputational loss if the system or data were compromised?

These three pieces of information determine how to focus cybersecurity efforts, attention and resources -- and ultimately, the tone and strategy of the program itself.

I did some consulting work a few years ago for a healthcare organization looking to revise its cybersecurity strategy. The first activity I undertook was to perform risk assessments on all of the company's major IT platforms. Considering the company's business model centered on providing healthcare services to individuals, the organization had focused most of its security attention and spending on its patient records systems.

A risk assessment showed most of the patient records systems were adequately secured and had been for a long time. As a result, nearly 90% of the security budget was being spent (or overspent) to improve patient records controls that were already sufficient. Only 10% of the budget was dedicated to other platforms, and this left a recently deployed online billing system insufficiently secured. The billing system was considered critical due to the payment and consumer information it contained and its potential impact on revenue projections. After the risk assessments, there was a realignment of the organization's security budget to better address payment system and Internet security. There were also revisions to the company's incident response and disaster recovery (DR) plans to help avoid outages -- and subsequent revenue losses -- involving the online payment system.

The cybersecurity benefits of risk assessment analysis

The case mentioned above is a fairly classic case of security and IT teams "not seeing the forest for the trees" and overspending and over-focusing on certain areas. The risk assessment analysis can help enlighten a cybersecurity program, if not the entire company, as to where the company's assets really are and whether the appropriate security focus and attention are being given to those assets.

In addition to capturing information like sensitivity, threat and value of a system or data store, the analysis of risk assessment information can provide much greater insight and benefit -- depending on how detailed the assessment gets. Risk assessments often involve a fairly nominal amount of effort, including:

- Interviewing personnel knowledgeable about the system or data
- Reviewing security controls already in place for the system or data and determining what the surrounding IT environment looks like
- Determining cost vs. revenue information
- Determining data asset management details, such as business owner vs. technical owner
- Analyzing these types of data points through a risk assessment will help security and IT teams build DR plans, validate or update asset and configuration management information, and calculate return on investment.

Another benefit of a cybersecurity team performing risk assessments is that it teaches them to think in terms of both business and risk. Cybersecurity staff are often too focused on verbatim enforcement of security across all systems and data, rather than thinking in terms of risks vs. reward. A cybersecurity team experienced in performing risk assessment analysis is typically better prepared to work with business functions that regularly deal with risk, such as product management, finance and legal. While this might seem like a secondary or more trivial benefit, it can be instrumental when defining strategy or obtaining funding for appropriate security technologies or resources.

Risk assessments are a critical component of cybersecurity programs in that they provide important information needed to guide strategy, prioritization, procedures and even funding of security controls. Similar to how architectural plans are instrumental to erecting buildings, risk assessments are just as important in providing a blueprint for how an organization should best apply and enforce security measures to safeguard a company's interests. In addition to mitigating risks, you will also likely find that effective assessment will better position your cybersecurity team and program with business leaders.

About the author:
Jeff Jenkins is a regulatory compliance, information security and risk management expert and currently the director of cybersecurity at Travelport LTD. Prior to his role with Travelport, Jeff served in security executive/leadership roles for a number of private and public sector organizations including Cbeyond, Equifax, The First American Corporation, S1, Georgia's Dept. of Human Resources, and Cobb County Public Schools. Jeff currently holds CISSP, CISA, CISM and CGEIT certifications.