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

Author: Franklin Jr, Curtis

Title: "7 Steps to Start Your Risk Assessment"

Website: DarkReading.com

Organization: Dark Reading

Date: 04 October 2018

URL: https://www.darkreading.com/network-and-perimeter-security/7-steps-to-start-your-risk-assessment/d/d-id/1332975?image_number=3

Accessed: 15 October 2019

Synopsis: Risk assessment can be complex, but it's vital for making good decisions about IT security. Here are steps to start you down the path toward a meaningful risk assessment process. "Managing risk is one of the most, if not the most important, functions in an organization," says Tony Martin-Vegue, enterprise security management strategist for LendingClub, a peer-to-peer lending company based in San Francisco. "It's really important to have a structured, formalized process for measuring risk, managing risk, and the entire remediation process."

If a formal process is the best way to assess and manage risk, then what sort of process should an organization use? "The most commonly used risk model is the mental model of the person waving their wet finger in the air," says Jack Jones, executive vice president of research and development at RiskLens and chairman of the FAIR Institute. "And mental models are notoriously flawed," he says. The reliance on flawed mental models is one of the many reasons Jones says that the IT industry is horrible at properly assessing risk.

How does an organization go about finding a better model and using it to figure out what their risk is? There are a number of options, from NIST SP 800-30 to aspreadsheet-based model that can be found from a wide variety of sources with a quick Google search to FAIR — Factor Analysis of Information Risk.

Large organizations will have teams dedicated to assessing and re-assessing risk on a regular basis. Small organizations may lack the team, but they will not lack the need to understand what risks IT faces and how those risks are reflected in the rest of the business units.

"I don't feel any organization can even begin to think about what it wants to do from an information security perspective without making some proper attempt at being able to understand the risks that matter most to their organization," says Zulfikar Ramzan, CTO of RSA. "I don't want this to be confused with 'expensive' or 'complex' or, you know, beyond the scope of what I think even a small- to medium-sized organization can do," he explains. "What I really mean here is try to be a bit principled trying to look at it and get a more quantitative assessment."

Getting started on this quantitative path can be confusing, so Dark Reading researched the major frameworks and spoke with Jones, Martin-Vegue, and Ramzan to get their ideas on best initial steps. We found seven steps that apply to a variety of frameworks — and that are applicable no matter where the process takes your organization.

DARKReading

10/4/2018
04:30 PM

Curtis Franklin Jr.
Slideshows

7 Steps to Start Your Risk Assessment

Risk assessment can be complex, but it's vital for making good decisions about IT security. Here are steps to start you down the path toward a meaningful risk assessment process.

"Managing risk is one of the most, if not *the* most important, functions in an organization," says Tony Martin-Vegue, enterprise security management strategist for LendingClub, a peer-to-peer lending company based in San Francisco. "It's really important to have a structured, formalized process for measuring risk, managing risk, and the entire remediation process."

If a formal process is the best way to assess and manage risk, then what sort of process should an organization use? "The most commonly used risk model is the mental model of the person waving their wet finger in the air," says Jack Jones, executive vice president of research and development at RiskLens and chairman of the FAIR Institute. "And mental models are notoriously flawed," he says. The reliance on flawed mental models is one of the many reasons Jones says that the IT industry is horrible at properly assessing risk.

How does an organization go about finding a better model and using it to figure out what their risk is? There are a number of options, from NIST SP 800-30 to aspreadsheet-based model that can be found from a wide variety of sources with a quick Google search to FAIR — Factor Analysis of Information Risk.

Large organizations will have teams dedicated to assessing and re-assessing risk on a regular basis. Small organizations may lack the team, but they will not lack the need to understand what risks IT faces and how those risks are reflected in the rest of the business units.

"I don't feel any organization can even begin to think about what it wants to do from an information security perspective without making some proper attempt at being able to understand the risks that matter most to their organization," says Zulfikar Ramzan, CTO of RSA. "I don't want this to be confused with 'expensive' or 'complex' or, you know, beyond the scope of what I think even a small- to medium-sized organization can do," he explains. "What I really mean here is try to be a bit principled trying to look at it and get a more quantitative assessment."

Getting started on this quantitative path can be confusing, so Dark Reading researched the major frameworks and spoke with Jones, Martin-Vegue, and Ramzan to get their ideas on best initial steps. We found seven steps that apply to a variety of frameworks — and that are applicable no matter where the process takes your organization.

(Image: Alexas_Fotos)

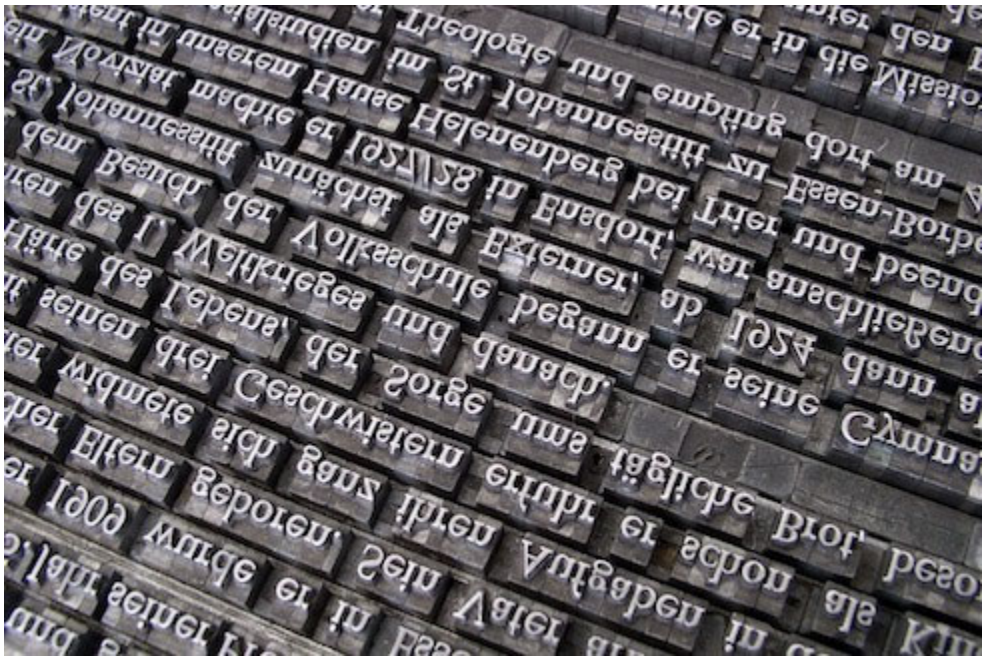
Curtis Franklin Jr. is Senior Editor at Dark Reading. In this role he focuses on product and technology coverage for the publication. In addition he works on audio and video programming for Dark Reading and contributes to activities at Interop ITX, Black Hat, INsecurity, and ... View Full Bio

7 Steps to Start Your Risk Assessment

Curtis Franklin Jr.Slideshows

Risk assessment can be complex, but it's vital for making good decisions about IT security. Here are steps to start you down the path toward a meaningful risk assessment process.

2 of 8



Start With a Common Language

"I think [risk assessment] does start with at least beginning with a consistent definition of what risk means," says Ramzan. Agreeing on language is important because there are so many terms that will be used by everyone involved in the process and so many decisions that need to be made on the outcome of the process.

Among the most important terms to be agreed on are assets, value, losses, threats, and measurements. And the reason that there should be formal, stated agreement on the language is that many of the terms have meanings that can vary from discipline to discipline, or even person to person based on their background and experience.

Once there's agreement on the terms to be used and their meanings, it's time to start assigning values to those terms.

(Image: wilhei, VIA Pixabay)

2 of 8

Comments

Rate It

100%

0%

gwskelton,
User Rank: Apprentice
1/3/2019 | 11:37:49 AM
Value of Article and Risk Assessment
Your article was a concise overview of the process of risk assessment. Many organizations have a difficult time in starting a risk assessment program, following through on all of the necessary steps - identification of assest, threats, controls, and determining what particular controls are worth the expense. Furthermore, risk assessment is a life-long process that must continue in an ongoing basis, not just once a year or whenever compliance is required.

Thanks again for your overview.

Gordon Skelton, CISSP, CEH, Security+

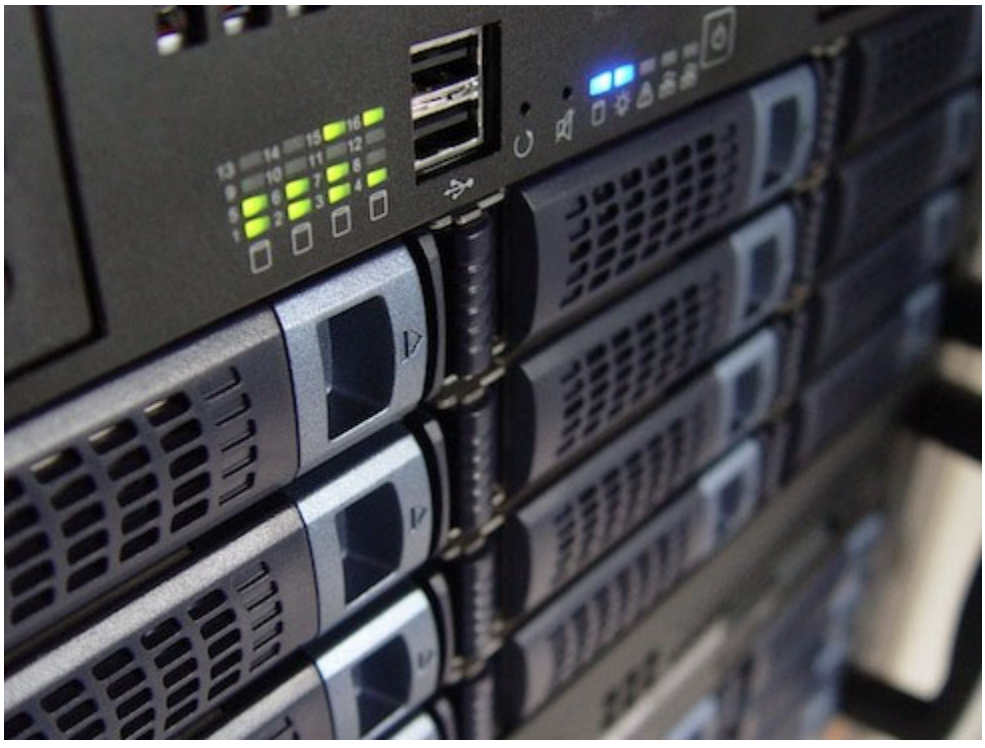
Security and Analytics, LLC

7 Steps to Start Your Risk Assessment

Curtis Franklin Jr.Slideshows

Risk assessment can be complex, but it's vital for making good decisions about IT security. Here are steps to start you down the path toward a meaningful risk assessment process.

3 of 8



Define Assets

An asset is anything that brings potential value — or represents potential risk — to the organization. The critical point to be made in figuring out whether something is an asset, is that the value or risk doesn't have to be represented solely in dollar amounts.

Assets can be materials and equipment, or they can be customer data, intellectual property, or the organization's reputation. While the categories into which assets can fit is large, it's important to know that, from a risk analysis perspective, not

everything is an asset.

Why would it matter if there are extra "assets" on the list? Jones describes a problem he frequently sees. "You have a severe signal-to-noise ratio problem," he says. "The risk registers are filled with things that are part of risk landscape but aren't themselves risks." Deciding whether something belongs on this list is going to depend on whether value and risk of loss can be defined — and those come next.

(Image: heladodementa, via Pixabay)

3 of 8

Comments

Rate It

100%

0%

gwskelton,
User Rank: Apprentice
1/3/2019 | 11:37:49 AM
Value of Article and Risk Assessment
Your article was a concise overview of the process of risk assessment. Many organizations have a difficult time in starting a risk assessment program, following through on all of the necessary steps - identification of assest, threats, controls, and determining what particular controls are worth the expense. Furthermore, risk assessment is a life-long process that must continue in an ongoing basis, not just once a year or whenever compliance is required.

Thanks again for your overview.

Gordon Skelton, CISSP, CEH, Security+

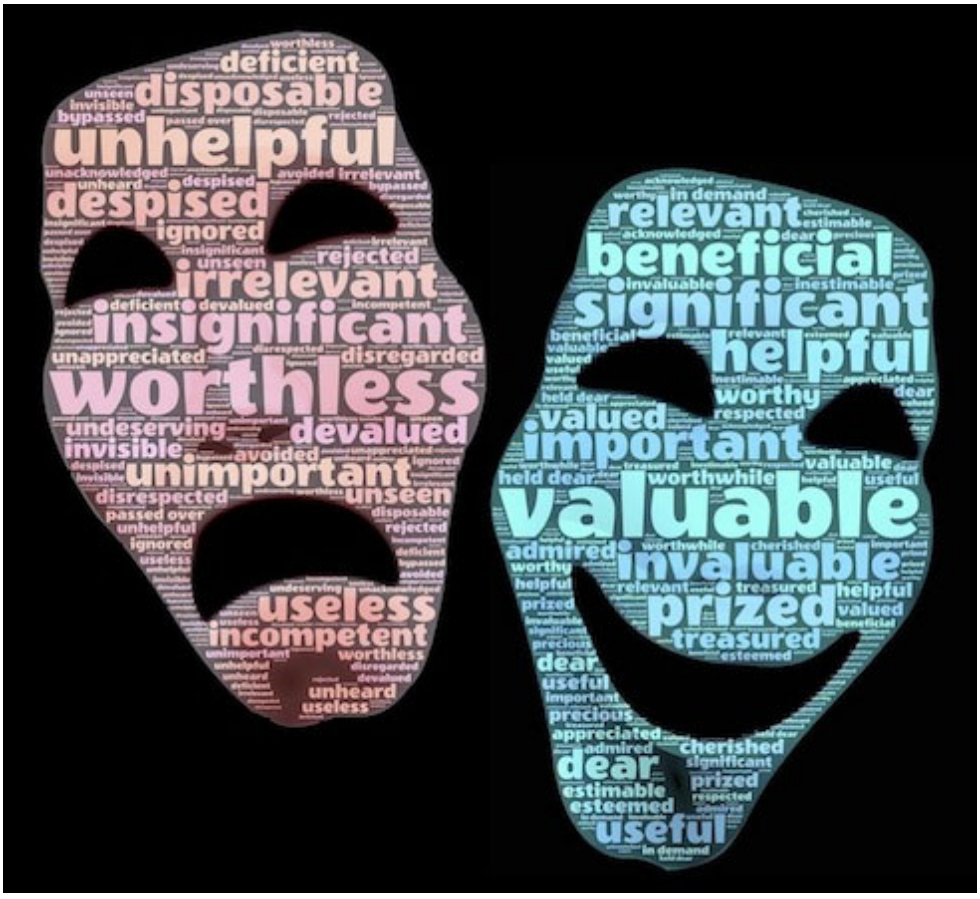
Security and Analytics, LLC

7 Steps to Start Your Risk Assessment

Curtis Franklin Jr.Slideshows

Risk assessment can be complex, but it's vital for making good decisions about IT security. Here are steps to start you down the path toward a meaningful risk assessment process.

4 of 8



Define Value

In the FAIR model there are three kinds of value (and their mirror image, loss). The first of these is **criticality** — the impact the asset has on the organization's productivity. Is something a component in manufacturing? Is it part of the billing process? Is it key to selling the organization's products or services? If so, then its

criticality value will be high.

The next value is **competitive advantage**. Does the asset allow the organization to do something its competitors can't do, or do something in a way that's superior to the way the competition does it? Then it has value from a competitive advantage standpoint.

The final value/risk is **sensitivity**, basically a measure of how much the asset's loss will cost the organization. The model breaks this value into four separate risks:

- *Embarrassment* -– Would having this information become public show that the organization had engaged in unethical or unsavory activities?
- *Competitive advantage* –- How significant an impact does this have on the overall competitive advantage of the organization?
- *Legal/regulatory* -– Is this asset regulated by national or industry agencies? Would disclosure or loss of this asset prove a violation of regulations or law?
- *General* -– And this is the catch-all for assets that don't neatly fit into one of the other categories, but are still important to the organization, and a risk if they're lost, exposed, or compromised.

(Image: johnhain, via Pixabay)

4 of 8

Comments

Rate It

100%

0%

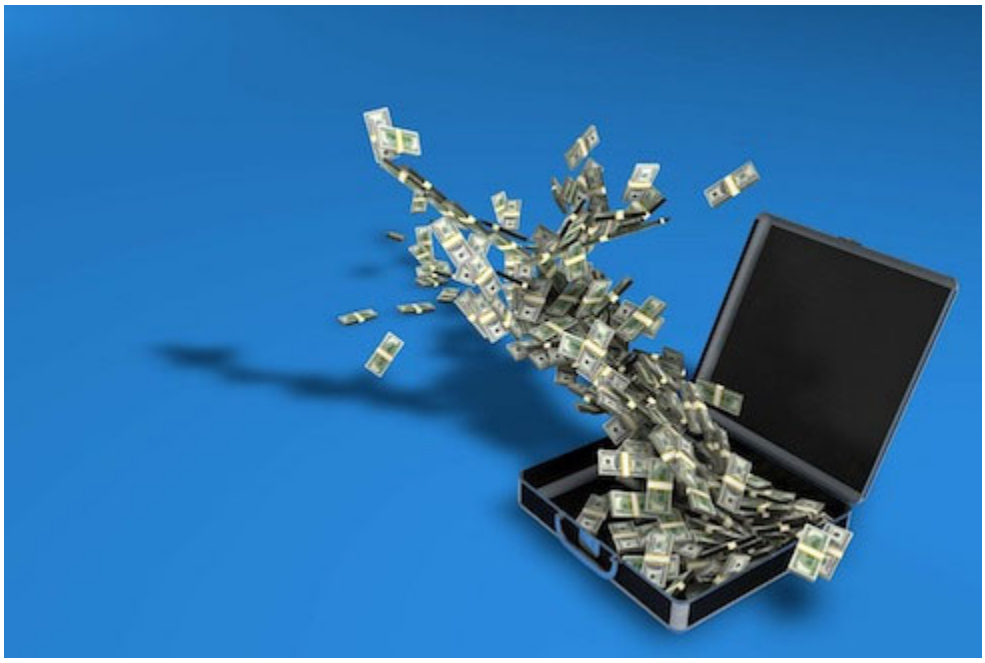
gwskelton,
User Rank: Apprentice
1/3/2019 | 11:37:49 AM
Value of Article and Risk Assessment
Your article was a concise overview of the process of risk assessment. Many organizations have a difficult time in starting a risk assessment program, following

7 Steps to Start Your Risk Assessment

Curtis Franklin Jr.Slideshows

Risk assessment can be complex, but it's vital for making good decisions about IT security. Here are steps to start you down the path toward a meaningful risk assessment process.

5 of 8



Define Losses

Just as there are multiple ways of determining value, there are many ways of looking at the loss of an asset. The FAIR method describes six categories of loss in their model:

- **Productivity** –- A loss doesn't have to bring the effective production of goods or services to a halt; all it has to do is reduce the effectiveness. If that happens, a loss has occurred.
- **Response** -– Most organizations won't ignore a loss that occurs regarding one of their assets; they will respond. The cost of that response, whether large or small, is a loss that must be considered.

- **Replacement** -– Speaking of responses, if an asset is lost or damaged it will be replaced. The cost of that replacement is a loss to the organization.
- **Fines and judgments** -– If the loss exposes the organization to legal or regulatory action, the cost of responding in court and of any fines or judgments is part of the overall loss.
- **Competitive advantage** -- When a loss alters the competitive landscape or forces the organization to miss sales opportunities because of the incident or response, then it's a loss to competitive advantage.
- **Reputation** -– And if the incident makes potential customers, clients, or partners think less of the organization and its business suffers for that, then it's a material loss to reputation that must be taken into account.

(Image: PublicDomainPictures, via Pixabay)

5 of 8

Comments

Rate It

100%

0%

gwskelton,
User Rank: Apprentice
1/3/2019 | 11:37:49 AM
Value of Article and Risk Assessment
Your article was a concise overview of the process of risk assessment. Many organizations have a difficult time in starting a risk assessment program, following through on all of the necessary steps - identification of assest, threats, controls, and determining what particular controls are worth the expense. Furthermore, risk assessment is a life-long process that must continue in an ongoing basis, not just once a year or whenever compliance is required.

Thanks again for your overview.

7 Steps to Start Your Risk Assessment

Curtis Franklin Jr.Slideshows

Risk assessment can be complex, but it's vital for making good decisions about IT security. Here are steps to start you down the path toward a meaningful risk assessment process.

6 of 8

Define Threats

Threats can come in many forms and guises, from outside the organization and inside, from malicious acts to accidents, and from human action to *force majeure*.

Regardless of the threat's source, it will have an impact in one of five ways on an asset:

- **Access** -– The threat can read or gain access to the data without proper authorization.
- **Deny access** -– The threat agent can prevent legitimate users from accessing the asset.

- **Disclose** -– The threat can let other people or organizations access the asset.
- **Misuse** -– The threat can use the asset in ways that were never intended or authorized.
- **Modify** -– The threat can change the asset, whether data or configuration.

(Image: stevepb, via Pixabay)

6 of 8

Comments

Rate It

100%

0%

gwskelton,
User Rank: Apprentice
1/3/2019 | 11:37:49 AM
Value of Article and Risk Assessment
Your article was a concise overview of the process of risk assessment. Many organizations have a difficult time in starting a risk assessment program, following through on all of the necessary steps - identification of assest, threats, controls, and determining what particular controls are worth the expense. Furthermore, risk assessment is a life-long process that must continue in an ongoing basis, not just once a year or whenever compliance is required.

Thanks again for your overview.

Gordon Skelton, CISSP, CEH, Security+

Security and Analytics, LLC

7 Steps to Start Your Risk Assessment

Curtis Franklin Jr.Slideshows

Define Measurements

How will you define the impact of a loss? It's easy to say that dollars are all that matter, but individual stake-holders may define the impact differently. "If you think about the concept of a risk owner, that is somebody who owns the risk, somebody who essentially has their neck on the line," says Martin-Vegue. "If something goes south, this is the person that's accountable."

Measurement is important because so many of the decisions to be made around risk assessment involve multiple business units and management teams. Martin-Vegue explains, "Let's say you can implement this new product that has a ton of vulnerabilities but it also gets me all of this new revenue - it increases my business. So what should I do?" he asks, continuing, "Should I put the new product in and take the risk with cyber vulnerabilities, or should I not put the product in and take the risk of not getting new customers?

Martin-Vegue points out that these are the sorts of decisions that involve multiple stakeholders from multiple business units. Without common definitions of terms, threats, and measurements, making those decisions in a rational way is all but impossible.

(Image: arielrobin, via Pixabay)

7 Steps to Start Your Risk Assessment

Curtis Franklin Jr.Slideshows

Define the Audience

Why, precisely, is the organization going through the process of risk assessment? Knowing the reasons for the exercise, and therefore the audience for the final assessment, will help guide the language decisions in the report that results. "Risk assessments and risk management always always needs to support a management decision," says Martin-Vegue, adding, "Before you embark on any risk analysis you really need to ask yourself, 'what decisions am I supporting?'"

In almost all organizations, those decisions will come down to answering questions about how to spend resources. "When you look at risk and it being multifaceted as it is, it's very easy to overspend in certain areas and underspend and others," says Ramzan. "We have to make sure we think about risk with a holistic and balanced view that enables us to spend money in the correct ways."

Spending in correct ways is ultimately a decision for the executive committee, and a rigorous risk assessment leading to a report written in business language will support that decision. Jones says, "How I think about it is this: our problem space is complex and dynamic with a lot at stake, and we have limited resources. Every dollar that goes to us is a dollar that doesn't go to growing the business or other operation imperatives, so it's critically important that we prioritize."

(Image: qimono, via Pixabay)