Threats and Risk Calculation

Table of Contents

Threats

Any person or tool that can take advantage of a vulnerability to compromise the CIA of an asset (i.e., exploitation of vulnerabilities).

Common threat tools/techniques

- Malicious Code
  - Worms, Viruses, Trojans, DoS
- Social Engineering
- Packet Sniffing and Network Scanning

**017 Threats; that's a person or a tool that can take advantage.

Some threats are automated. Some threats, somebody releases something into the world and lets it go and says: Go scan for this particular thing and report back in.

The individual isn't coming to your computer and saying: Hey let me take a look at this, take a look at this. They've released that threat. They were the person that started it, the threat agent; but the threat is that botnet crawls all those websites on the outside. Or that thing that

searches Google for this particular string that's on your website.

Some of the most common threats are malicious code.

Social engineering; remember that's done by a person. Malicious code is written by a person. Social engineering is done by a person.

Packet sniffing and network scanning. Those are threat to our organization.

When we do network scanning, that's a reconnaissance threat. They can learn more about our organization than they should know. They're eroding the confidentiality of our organization.

So threat is a person or tool.

Threat Vectors

Path by which an attacker can gain access to a target in order to cause harm (i.e., attack vector)

- Web – Fake sites, session hijacking
- Email – Links, attachments
- Mobile Devices – Tablets, phones
- Social Engineering
- Malware

**018 Threat vectors is the path that they take to get there: web mail, email, mobile devices.

Threat Vector Types

Human

- Malicious
  - External
    - competitors
    - organized crime
    - foreign governments
  - Internal
    - disgruntled employees
- Ignorant

System

- Automated privilege elevations

Threat probability or likelihood - calculation of the potential for a threat to cause damage to an asset.

**019 Now when we look at the threat vector types-- sometimes this is called threat agents; it depends on who you talk to; some books you read it one way, some books you read it another-- we usually talk about how to break this down based on human or system. And when we talk about humans, we talk about accidental versus intentional. So if you don't even know that that's the wrong thing to do, you will do it.

Now when we look at the threat vector types, we talk about the probability or likelihood, we've got to calculate based on the- I would say the adversarial-ness-- I don't even

know if that's a word-- but the evilness or the- a little bit more on the intent side of things.

If we have somebody who is truly, truly evil, and they have an axe to grind against us, they have a grudge against us, we got a serious problem.

If we have somebody out there that wants to make money off of our poor security practices, eventually they'll take a nap; because only so much money will incent them; and at a certain point in time it's not enough money for them to go after us.

And the opposite could be true. They could say: Okay look, if I send out this email to ten million people, only one percent of those people has to come back to me-- 10,000 people; I think that's the right calculation. Ten-thousand people have to come back to me and say: Yes I'm interested.

So they'll play it as a numbers game. Do they know you? No they don't. You're just one in a sea of numbers. And then they'll take advantage of that.

Vulnerabilities

Weaknesses in an asset

- Software Weaknesses
  - Weak default settings
    - Default accounts/passwords, access controls, unnecessary software
  - Bugs
  - Buffer overflows, poor error handling
- Architecture Weaknesses
  - Single points of failure
- Personnel Weaknesses
  - Lack of awareness/training

**020 Vulnerabilities. The weakness. This is the weakness in a particular asset.

Now remember, scope is important here. Are we looking at the executables on the machine or are we looking a the whole machine?

Are we looking at the protocol? Well the mail server's pretty robust but we're really susceptible to spam. Our weakness is that we don't filter for spam. Let's put in a filtering tool.

This could be default settings. We allow the username to be root and the password to be 'toor'-- root

spelled backwards. That's the standard default.

And what we expect operators to do is once they get this up and running, as they log in to change the root password to something else.

But our machine doesn't force us to do that. It let's us keep on going; because we're root, because we're the senior administrator and if we want to have that password that's fine.

Those default configurations are there to get the machine up and running; and then you have to harden it and secure it. And if you don't go through those checklists you're not actually going to make the machine secure. You could miss one of the pieces in that checklist, by accident.

There are other things, like architectural weaknesses that we have. We decide that we want to use DNS instead of DNSSec; because it's easier on our customer.

We decide that we want to use a single server to solve all the problems of all the other servers. That could be the one weakness.

It could be that the person just doesn't know what they're supposed to do; they're not trained properly. That's a weakness.

Impact

A measurement of the amount of damage or loss that could be or will be caused if a potential threat is ever realized.

Measured with Exposure Factor (EF)

- EF = % of loss of an asset

**021 Okay. When it happens to us, how much do we lose? Now if you don't now how to calculate the Exposure Factor, the impact, what you do is you calculate it as one; in other words 100 percent loss. Because you don't know.

But if a tree falls on your building and crashes through, is the entire building destroyed? And you go: Well no it's not; it's just that corner of the building.

Okay what happens if the fire marshal comes in and says: This building is unsafe to occupy; tear it down? Well now if a little tiny tree

falls on the side of it, it could've caused structural damage.

So if we don't know, and we don't have calculations on this, then what we say is: It's a total loss.

When we look at total losses, by the way, catastrophic losses, this is a really good time to look for insurance to help us with this.

Risk Calculation

Risk Calculation

Risk can be measured *quantitatively* or *qualitatively.*

- Risk is given values so management can decide what to do about the risk.
- The risk assessment should include
  - Criticality of the lost function
  - Duration the loss will persist
  - Tangible and intangible impact on the organization
    - Loss of physical inventory
    - Loss of data
    - Loss of the ability to conduct business
    - Loss of good will and reputation
    - Loss of customers and investors

**022 Risk Calculation. We can do this quantitatively or qualitatively.

So far we've looked at the Exposure Factor and the Annualized Rate of

Occurrence. What we want to know is what our losses could potentially be.

We want to give management some values so that they can make decisions. And that means that we have to be consistent in how we're doing the counting and how we present the information to them.

You've got to figure out what the Risk Calculation is and how this will work for you.

You've got to figure out on that Critical Loss Function how much this will impact you over time. That reaches into business impact assessments and business continuity planning.

Risk Calculation – Common Formulas

Exposure Factor (EF)

- Measures impact - % of loss of an asset

Single Loss Expectancy (SLE)

- EF x Value of asset in $

Annualized Rate of Occurrence (ARO)

- Frequency of occurrence of a threat

  Example: Never = 0.0
  Once a year = 1
  Once every 24 years = 1/24 = 0.04

Annualized Loss Expectancy (ALE)

- Dollar value derived from: SLE x ARO

CERT | Software Engineering Institute | Carnegie Mellon University 23

**023 Okay so how do we calculate this thing?

So here's the easy way to remember this, to start yourself off. ALE, a-l-e. is made by SLE ARO. We're trying to figure out what the Annualized Loss Expectancy is; the ALE.

Okay how do we do that? First off we figure out if this asset were-- how much of a percentage of this asset could be lost? So if we don't know, then it's 100 percent. If we know that it'd cost us 50 percent of our time, then we could go ahead and do that calculation.

Single Loss Expectancy: The Exposure Factor times the value of the asset. How much are those files worth? How much is that filer worth? How much is that intellectual property worth to the organization?

Now this is a tough calculation. If that secret information were released before our initial public offering, that's a serious breach and it causes serious problems. If it's released after, not such a big deal. So it's always a point in time.

So we measure the Exposure Factor against the value of the asset lost. And that gives us our SLE; Single Loss Expectancy.

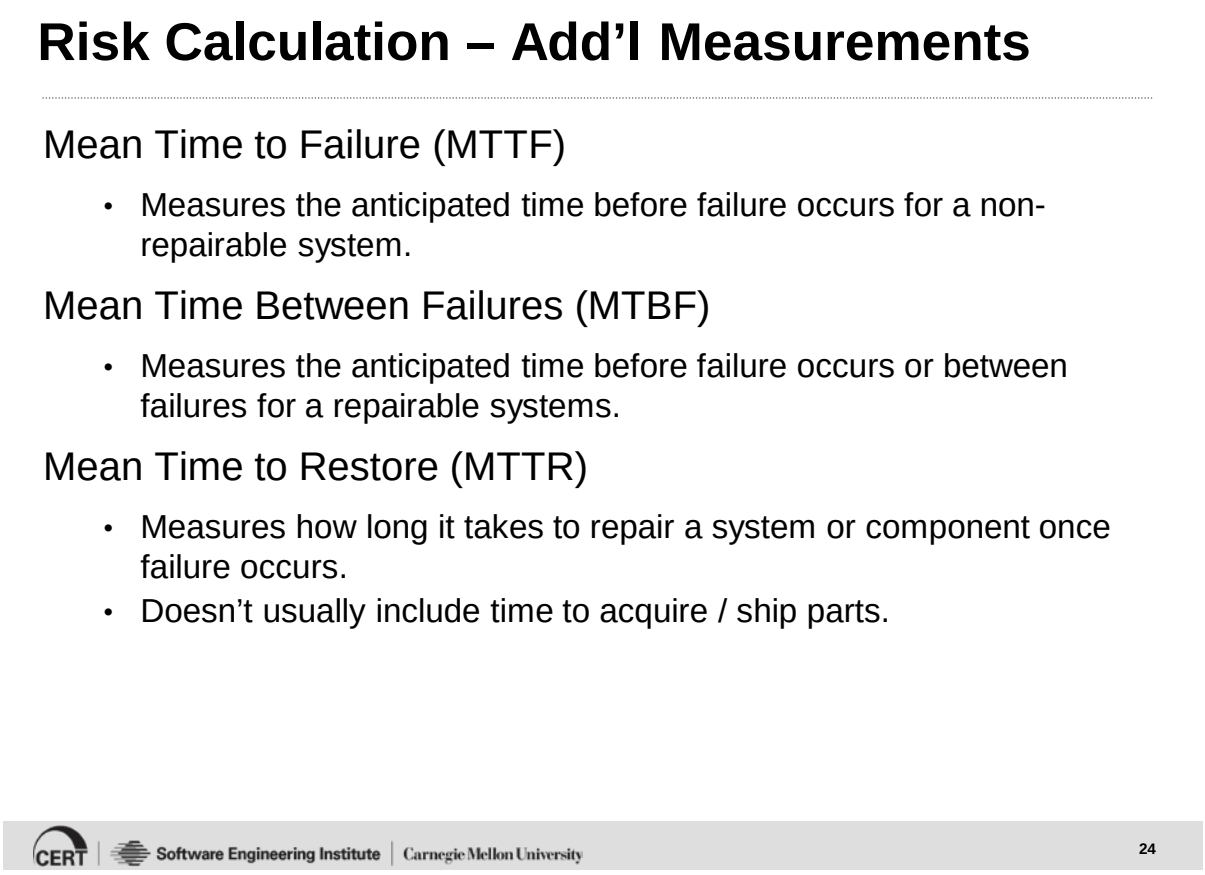
And then we say: How often could this occur? Now if it's for intellectual property release and before the- before the initial public offering, it could happen many different times. The Annualized Rate of Occurrence for this could be 100 or infinite; and you don't know for that.

But let's make it easier. Let's use this tool in a way that we can actually count.

How often are new viruses released? How often is new malware released? Well you can go to databases and get the statistics on that and say: The Annualized Rate of Occurrence for new malware this year was 15,000 instances in the year.
So you take this all and you roll it all up into an Annualized Loss Expectancy. An ALE is the Single

Loss Expectancy times the Annualized Rate of Occurrence. Remember, the Annualized Rate of Occurrence, if it happens less frequently than a year, then we start moving the decimal place.

Risk Calculation – Add'l Measurements



**024 Some other risk calculations that we have to look at; and these really reach- start reaching into business continuity planning.

Mean Time to Failure; measures the anticipated time before failures occur in a non-repairable system.

When the hard drive dies, you can't get-- well you shouldn't be opening it up and fixing the platters. You can; but it's very expensive and you need a clean one.

Mean Time Between Failures; measures the anticipated time before failure occurs or between failures for a repairable system. So could we fix this?

Now how we offset that, by the way, is we have extra drives sitting there and we do backups and we do RAID arrays.

Mean Time to Restore. How long it takes to repair a system or component once failure occurs. Now this doesn't usually include time to acquire or ship.

The perfect example of Mean Time to Restore is in backups. Our system fails here; we need the backup tape. Is the backup tape local? A lot of times what we say is: Well we ship those backup tapes offsite.

Okay so we gave this to the company; they picked it up and they carried it away to the vault, into the mountain. And then what happened was is we say: Well we need to actually restore this tape.

There are two numbers that we have to calculate. One is the retrieval process, calling them, getting the tape, delivering the tape to us. That could be eight hours; it could be off cycle in the middle of the weekend

and you don't have that kind of-- it could be 36 hours because you don't have the type of retrieval system that you've paid for that gives you platinum support, which is right now. You have to wait until normal business hours.

Once it gets to you, how long does it take to replay the tape? That's another piece of the restore value.

So you say: We're down now; it's going to take us 46 hours, if it's on a Friday. If we're down on Thursday it's going to take us-- well normal business hours it's going to take us eight hours to get back up and running, plus nine for the actual restore process.

These are calculation measures that may be available to you. And here's the real trick. I'm giving you all these numbers because what you have to do is you have to say: Are these numbers available to us; and can we get them easily based on the way we do business?

You may have to look at all your different support contracts and see whether it's-- what's it called?-- Bronze, Silver, Gold, Platinum, Diamond or whatever it is; and figure out with all of those contracts that you outsourced these activities, what is the time to restore based on the services that are provided from an outsource standpoint.

Quantitative Risk Analysis

Concrete percentages and real dollar figures

Main steps for a qualitative risk analysis include:

- Inventory assets and assign value (AV)
- Calculate the EF and SLE for possible threats
- Calculate likelihood (ARO)
- Derive the loss potential per threat by calculating the ALE
- Research countermeasures for each threat and re-calculate ARO and ALE based on applied countermeasures
- Perform a cost/benefit analysis of each countermeasure for each threat and asset and select the most appropriate response

CERT | Software Engineering Institute | Carnegie Mellon University 25

**025 Quantitative Risk Assessment assigns a specific dollar value to things. And that's really what you want to do.

So here are the general steps in Quantitative Analysis.

Find out what your asset value is; know what's under the scope.

Calculate the Exposure Factor; how much of it you could lose. Give the Single Loss Expectancy for it.

And then calculate the Annualized Rate of Occurrence.

That should derive all your Annualized Loss Expectancy.

The next thing that you want to do is when you've got that number is you want to perform a cost/benefit analysis on which controls will help reduce the Annualized Rate of Occurrence more effectively for the dollars that you're going to spend.

Qualitative Risk Assessment

Qualitative Risk Assessment

Qualitative risk can be used where $ values are not available.

- In qualitative risk, events are given points for relative loss (from catastrophic to negligible) and likelihood of occurrence (from certain to highly unlikely).
- The process involves judgment, intuition, and experience

TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Source: NIST Special Publication 800-30 Rev1, Guide for Conducting Risk Assessments

**026 Qualitative Risk Assessment however is much easier to do; but also much less accurate.

Here what we do is we don't assign dollar values. We assign orders of

magnitude. What is the likelihood of that event occurring? Very Low, Low, Moderate, High and Very High.

So the likelihoods there, you'd probably do that in percentages. When we say Very Low, that would be like four or five decimal places in. Very Low would be .0001, for argument sake. Low would be .01. Moderate would be--

And see we're assigning numbers there because we want to put it in some sort of level. So it would be between two numbers. But I'm just giving you numbers to work from.

Now what you can say is: Well I don't know exactly what those numbers are; I really don't know. So I'll organize it as best I possibly can for likelihoods. Because Martians landing on the building is very low. But getting viruses on that exact same particular asset are very high.

What's the level of impact? Now I would like to do orders of magnitude again for levels of impact; even though it's Very Low to Very High.

You might say that the level of impact to us is catastrophic; we could lose the entire business. That's a Very High.

The level of impact of one virus means that we- one virus on one workstation means that we're going to have rebuild the workstation. The level of impact on that is Very Low; in this scope.

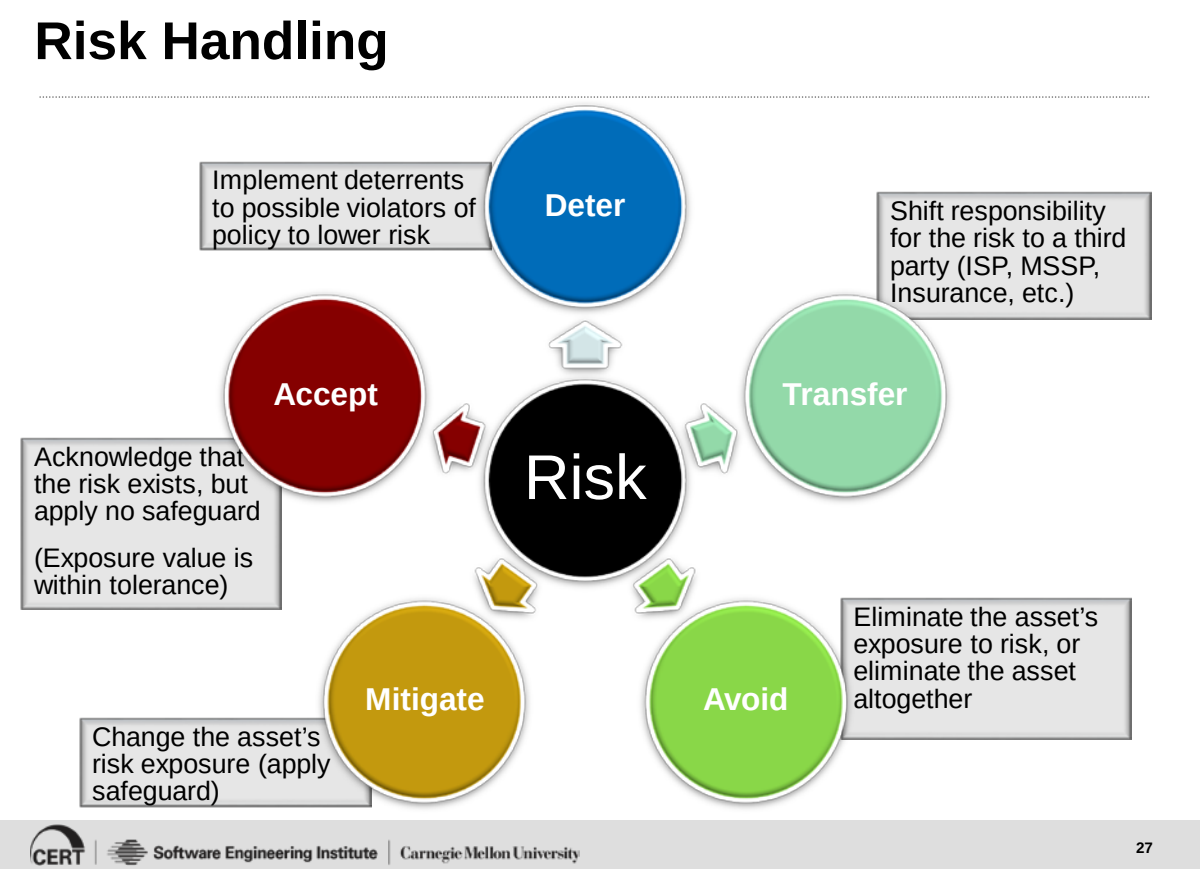
When we take this scope and we add it up with all the other scopes, we need to have some definitions that we give to management about what we mean about Very High and Very Low. This helps us-- and this reaches toward Hubbard-- to help us get better at what we do. He teaches you how to be optimistic, pessimistic, and how to evaluate that.

Now you need some more guidance. Because this isn't enough here. I want you to reach out to the NIST Special Publications.

I like NIST Special Publication 30, 37 and 39 for doing risk assessments and risk management.

You should read all three. Even though you're doing the risk assessment side of things, you should be doing the other ones so that you understand your outputs; the ultimate goal.

Risk Handling



**027 Okay so how do we handle risk?

Well we Deter. We convince our adversary not to attack.

I'm going to climb into that building. Well if there's barbed wire there, hey no that's not going to work out.

I can Transfer. I can insure this.

Now that insurance costs me X number of dollars. It's worth it for me.

I could Avoid. Stop bringing your laptops and all your devices with you.

They have a computer there for you to use; just bring a USB drive with all of your files on it. That creates some other risks.

I could Mitigate. Well what I'll do is I'll create cable locks for all of my systems. I'll engrave them so that you see my name on the back of them; and I'll carry them in a pouch and wherever I go I've always got that pouch on me.

I could Accept it. Somebody's going to steal some of my stuff; and, you know, it's not going to happen that often.

Notices

Notices