# Defining Risk Management

When we talk about cybersecurity today, the big part of that discussion revolves around business risk.

**How do we secure our IT infrastructure?**

How do we ensure the integrity of our data while making the employees able to access everything they need to?

Before we dive into all things cybersecurity, let's make sure we have a good understanding of some of the foundational concepts.

**Let's start with assets, threats, and threat actors.**

We'll review internal and external threats, as well as introduce you to the crucial CIA triad of cybersecurity.

Think of cybersecurity as the art of protecting a treasure chest. Now imagine this treasure chest represents your computer or your smartphone. Inside of it are your golden coins representing your personal information, photos, bank information, and whatever else you want to keep secure. These golden coins are what we call assets in the world of cybersecurity. But wait, there's a pirate sneaking up hoping to get his hands on those coins. This pirate represents a threat.

**Threats:** are anything or anyone that can cause harm to our assets. Now observe the rusty hinge on our treasure chest. The hinge is weak. It's crumbling. It's going to be what we call a vulnerability.

**Vulnerabilities:** are the weaknesses or gaps in our security that allows threats to access our assets. If our pirates use this rusty hinge to their advantage and successfully open our treasure chest, they're going to pose a **risk**. In cybersecurity terms, risk is the potential for a threat, to exploit a vulnerability and to cause harm to our assets.

**Let's tie this all together.**

We have our treasure chest, our asset, the pirate, which is going to be our threat, who's eyeing our treasure chest? The chest has weaknesses, which we're going to call our vulnerabilities. When the pirate can actually exploit whatever weakness there might be, they get access through these vulnerabilities. If they do, then there's a risk our golden coins might be stolen.

*But here's the exciting thing when it comes to cybersecurity, we can change the game by replacing that rusty hinge with a new one, a stronger one.*

We've reduced the vulnerability and therefore the risk. And that, in essence, is what cybersecurity is all about understanding and protecting our assets, recognizing risks, addressing vulnerabilities, and minimizing the risks. Always remember the treasure chest is only as secure as its weakest hinge. Keep it safe and you'll keep your treasure intact. The fact is that there are too many different types of threats and dangers in cybersecurity for us to respond to them all without having some type of foundational understanding that helps us classify and respond to them in a formal, consistent manner. To support the business to handle this problem in cybersecurity, we have the **CIA triad**. *The CIA triad is an acronym that represents the backbone principles of cybersecurity. It stands for confidentiality, integrity, and availability, and each component represents a cornerstone of security objectives that professionals should address to ensure a secure environment.*

**Confidentiality**: ensures that data is only accessible to those who have the authority to view it. Protecting the secrecy of information is going to be the most important thing, especially when it comes to personal data, financial data or any type of sensitive business intelligence. Unauthorized access can lead to data breaches, which can have devastating consequences both legally and reputationally.

**Integrity:** ensures that data remains unaltered and genuine. This means that the information is accurate and hasn't been tampered with without the guarantee of integrity, systems and data cannot be trusted. For example, in a banking system, integrity ensures that the amount deducted from one account matches the amount added to another one. Tampering can lead to mistrust, financial loss, and incorrect data driven decisions.

**Availability:** ensures that systems, application and data are available and operational when people actually need them. Even the best and most secure system has no value if it's not accessible when necessary. Imagine a hospital. The database of patients is going to be the most important thing with treatments and everything else,

it has to be available, especially when there's an emergency. Downtime can result in financial losses, hinder operations, or even endanger lives in critical situations.

*The CIA triad is our trusted shield when it comes to dealing with these pirates and the threats they represent.*

*Since you paid attention, no one is going to walk the plank.*

# Threat Actor, Part I

Building on our treasure chest analogy, let's explore the different types of pirates or threat actors that roam the digital seas, hoping to get their hands on our precious assets. When we're talking about threat actors, we're going to be talking about not only who they are and what they can do, but why they're going to really be a threat or not. So we're going to be looking at a few things for each one.

* We're going to be considering whether they're going to be internal or external to the company.
* We're going to be talking about the type of resources they have access to.
* Are they someone who's on a budget, or do they have a government sized budget that they can actually use for attacking us? That's going to be the funding.

When we're talking about resources, how many different people can they allocate for this? That's going to be really making a big change between it being a small operation and a large one, even the sophistication of it. Are they going to be someone who wants to come in low and slow as an advanced, persistent threat? Or is it going to be someone who's just trying to do a drive by attack that they just downloaded off the internet?

That's really going to help us understand what their sophistication is as well as their their capability.

**Unskilled:** hackers are the rookie pirates in rickety boats. They might use basic maps and often hope for an easy catch using readily available hacking tools. They may not always know what they're really doing, but they can still cause damage if they stumble upon our unguarded treasure. Unskilled hackers are always going to be external to the company. Their resources are going to be low, their funding definitely on the lower end of things, their sophistication also low, and their capability is going to be low as well.

**Hacktivists:** are pirates that sail for a cause. They're not just after gold, but want to send a message. Think of them as pirates trying to overthrow a tyrant or make a political statement in the digital world. They hack to promote a political or social agenda. These hacktivists are always going to be external to the company. Their resources are going to be low, their funding is going to be low, sophistication is going to be low, and their capability is going to be low as well.

**Insider threat:** Pirates are going to be the trickier ones.They're part of the ship's trusted crew, maybe even trusted with guarding the treasure.Their intimate knowledge of the chest secrets make them particularly dangerous.Insider threats are going to be internal to the company.Their resources are going to be the company's resources.It's going to be high.Their funding may be low, but their sophistication is going to depend on what their job may actuallybe.Their capability is going to be high since they're going to already be inside.

*Imagine pirates using unauthorized tools or secret routes that the captain doesn't know about. That's what we're going to be calling* ***shadow it*** *in companies.*

This happens when employees use unauthorized apps or services, often inadvertently creating vulnerabilities. When it comes to shadow it, they're going to be an internal threat. Their resources are going to be high. Funding might just be low. It's going to be whatever can come out of their pocket. But sophistication depends on where they're at in the network. Because of this, their capability is going to be considered high.

Remember that treasure chest we talked about before?

*Now imagine there's a special gate that leads to it. And at this gate stands a diligent guard. This guard has a special list. Call an application. Allow list. Only the pirates or the applications on that list are going to be allowed through the gate. Everyone else is going to be turned away.*

By only allowing trusted pirates or applications, we minimize the chance of letting anyone or anything malicious in. It's like handpicking who can approach our treasure, keeping the unknown or potentially dangerous ones at bay. An application allowed list is our gatekeeper in the world of cybersecurity. It ensures only the known and trusted get access, bolstering our defenses against unwanted intruders. Keep your treasure safe and allow only the familiar faces in.

# Threat Actor, Part II

**Advanced persistent threat:** Think about these as someone who's going to be highly skilled. They're going to be well financed attackers, and they're going to have all the time in the world to have all of the effort focused right on attacking our sacred treasure chest as many times as they want for as long as the want. They don't even care if they even get caught. This isn't just going to be one pirate, but a relentless group often backed by nation states. They don't raid and leave. They linger, watching, learning, and striking silently. Their attacks are prolonged, sophisticated and stealthy. They are the ghost ships of the digital seas, always watching and waiting. Apts are going to be external forces that resources are going to be very, very high. Their funding is going to be high, their sophistication is going to be high, and their capability is also going to be high. A few different examples of Apts could involve the following **organized crime**, nation states, or even corporate competitors. Organized crime are going to be our mafia pirates, a tightly knit crew with a clear hierarchy out to steal and trade treasures. They're organized, professional, and profit driven when it comes to organized crime, they're going to be external. The resources are going to be high. Their funding is going to be high, their sophistication is going to be high, and their capability is also going to be high.

**Nation states**: are the state sponsored pirates. Imagine a massive ship funded by an entire kingdom. They're sophisticated, resource rich, and have specific agendas like espionage or destabilizing rivals. They'll stop at nothing to achieve their goals. Now nation states are going to be external. They're going to have high resources, high funding, high sophistication and high capability. In the vast oceans of the digital world.

*Understanding our adversaries these pirates is the first step in defending our treasure. Recognizing their ships, their tactics, and their motivations. Help us fortify our defenses and sail safely.*

# 2.7 Threats Intelligence

***Threat Intelligence Source:*** *As a cybersecurity expert, you need to be aware of the latest threats, and this is where* ***threat intelligence*** *comes into play.*

One reason this is important is because we need to be aware of what's happening so that we can prevent it from happening to our systems, so protect our assets. It can also help us do things like reduce incident response time. If we have a sense of some kind of a threat and what it can do, what kind of an impact it can have on assets, we can then come up with an incident response plan proactively and so that when it does occur, we can contain it much quicker. So often what will happen when we look at threat intelligence sources?

* It won't always just say this is the end result.
* This is the impact.

Often depending on the threat intelligence source, it will step through how attacks actually occur so that we can look at all of the levels involved in that attack and apply security controls along the way. So there is a team in cybersecurity.

It's called adversary tactics, techniques and procedures, otherwise called TTP.

And this is exactly what we just described.

Going step by step through all of the methods used by attackers to gain access to a system, or perhaps

to crash it, whatever their goal is.

So the other thing that we should be able to think about is tools that will give us a graphical representation

of something relevant, related to threats, like a live geographical map.

That gives us a sense of where malware threats are currently active.

Let's take a look at that.

There are plenty of tools like this out on the internet.

What we are looking at is the activity for virus software out on the internet.

And what's interesting about this is we get a sense not only of where it is geographically, but as

we go further down, we can start viewing some additional details.

So besides the countries, if I start clicking at the very bottom, we can see the type of sectors that

are being affected by these attacks, whether they're in the education sector, government and so on.

If we keep drilling down a little bit further, we can see the nature of the malware.

Is that a botnet?

Is it a collection of infected machines targeting another individual server or network?

And if we go even a little bit further, we can get a sense with the graph of the number of daily attacks.

So when cybersecurity people talk about the fact that there are attacks continuously against government

agencies and so on, it's true.

It actually is happening.

You can gain threat intelligence through closed source or proprietary information sources.

These would be private sources that you might have to sign up for with a particular vendor in order

to get a feed of the latest threats and the details related to them.

But there are also open source intelligence sources, otherwise called Osint, Osint.

These would be things like government reports, for example, in the United States, the National Security

Agency or the NSA continuously publishes a lot of information about threats and how to protect against

those impacts.

There could be media reports, academic reports.

Also, there are some freely available tools that provide us with lists of a lot of these threats online.

Let's take a look at the Google Hacking exploit database.

So here in the Google hacking database we have an example of open source intelligence.

It's available to anybody for free over the internet.

Its focus is really on how to use the Google search engine itself as a way to receive information that

probably shouldn't be disclosed, private information.

So on the Google hacking database, let's say I were to scroll down to where we have this web user login

entitle.

Entitle is a keyword you can search for in the Google search engine.

That means I want to search for pages that were indexed by the Google crawler, where in the title bar

of the web browser window, when that page is active, it would have web user login.

I'm going to go ahead and copy that.

And we're going to open up a new web browser.

And I'm going to paste that in here.

So we can actually do a little search on that.

What we're going to get is a list of search results where there are web page logins.

And if I click on any one of them to follow it through, it's going to bring up some kind of web page

login, which means that that's one less thing that attackers have to figure out from this point.

They might run brute force attacks or something along those lines to try to break into this particular

website.

Of course, we never do that against sites that we don't have, express written consent from the system

owners to run those kind of attacks, or it could be a site that you have under your control that you're

using for testing.

That would be okay, but don't try to break into things just because they show up in your Google search

results.

Now that's an example of open source intelligence.

We also have closed or proprietary.

That would mean that you might have to sign up with a subscription to some threat intelligence source

before you can start receiving that information about those threats.

The other thing to think about is there are other locations out on the internet that are also free,

like GitHub.

There are file and code repositories, again where we have information related to threat intelligence.

So you've got both open source and closed free versus signing up with a subscription to gain access.

We also have common vulnerabilities and exposures or CVEs.

So a CV is a uniquely numbered threat that is known internationally and this is freely available.

So this is an example of Osint.

Again the idea is we can become aware of threats, see how they work and protect against them.

So for example, if I were to search the CVE list and I'm going to search it for something that was

used in the Equifax hack of 2017, where more than 100 million customers information related to credit

information was stolen because of this.

So I'm going to search for Apache Struts, which is really just a Java web development platform for

website developers.

But if I search for any CVS, any known vulnerabilities related to that, we have a list here of many

of them.

And if I were to go down, for instance, down to 2017 specifically 2017, dash 5638, this is the one

that outlines that specific vulnerability that was actually exploited in the Equifax hack.

So there's a lot of detail that we could learn about this down to the point in some cases where you

can actually get code samples at the programming level of how to create the exploit.

So it's just another example of Osint that is available to us.

Then we get into other threat intelligence sources like the dark web.

Sometimes people call that the dark net.

It's called that because the content on it is not indexed by a search engine like Google.

So you can't just search up for something that you want to display.

Now, the dark net is really something that is used by what's called the Tor network.

The Tor network is an overlay network that sits over the standard internet protocols that we know and

love.

And the idea is that anonymizes your origin location and also encrypts the connection.

So the idea is that we can get to regular websites that are indexed, or some of the more nefarious

bad websites on the dark web that are not indexed.

Now, why is this relevant?

How is that a threat intelligence source?

It can be, depending on who's using it and how they're using it.

Think of journalists that need an anonymous and secured and protected way to send sensitive information,

perhaps to the media or law enforcement or government informants, that type of thing.

So the way that the dark web works with the Tor network is that imagine that we've got the free Tor

web browser program downloaded, and we're going to a website and let's say we're doing that from Canada.

So what happens is our network traffic automatically goes to a Tor network entry point.

So let's say again that's in Canada, my origin location, after which it goes through a whole bunch

of other servers to try to mask where I'm really coming from.

That's called the Tor Relay Network.

These are servers all around the world that are designed for this purpose, and this is transparent.

You don't have to do anything to make this happen.

It just works.

Eventually you get to the Tor network exit point.

Let's say in our case, it's Austria.

And then finally you get a connection to the website you wanted to connect to.

Well, from that website's perspective, it looks like you came from Austria and not Canada.

Let's take a look at the Tor browser for just a second, to see what that looks and feels like when

you're actually doing it.

So after you've downloaded and installed the Tor browser, it's going to show up like any other app

inside your start menu in windows.

So I'm going to go ahead and start the Tor browser from my start menu.

That's going to connect me to the Tor network, after which I can then surf to a website of interest.

So let's say I want to go to the Total Seminars website.

So I just type in the URL if I know it as I normally would.

Now there are some search engines that are available in the Tor browser, but again they can only show

you what has been indexed.

And so there are a lot of dark sites that are not indexed, and you can only get to them by plugging

in an IP address or a DNS name.

Okay.

So we've made a connection to the Total Seminars web page over the Tor network using the Tor web browser.

Let's take a look by clicking the padlock in the upper left at the path that we took to arrive there.

So from our browser, we went through Germany three times before we finally ended up at the Total Seminars

website.

So from the Total Seminars website perspective, such as with logging, this connection was initiated

from Germany and not from where I really am in Canada.

Now.

While all those threat intelligence sources are fantastic, we have to go to them to learn about them.

There must be some automated way that threat intelligence information can be shared among many different

software programs and many different enterprises, and that's called automated Indicator sharing, or

AIS.

This uses a specialized format called the Structured Threat Information Expression or Styx Styx format.

It's a special format for packaging up threat intelligence information that is understood among many

dissimilar systems.

So the next thing is, how do we transmit that specially formatted threat intelligence information across

a network that uses the trusted automation exchange of intelligence information or taxi standard Taxii.

So this is built into a lot of security monitoring tools where you get up to date threat indicator feeds

automatically without you having to go out and get it yourself.

So we now know that we have a couple of different ways that we can get threat intelligence information,

both at the open source level and at the closed source level.

Autoscroll

Course content

Overview

Q&AQuestions and answers

Notes

Announcements

Reviews

Learning tools