15 Risk Management & Data Privacy

During earlier sections you learned about several components of security and steps that can be taken to reduce risk. For example, you can run a vulnerability assessment and if any holes are found take the steps to plug them, or you can set strong password policies and make sure that the users have all been trained to identify phishing attacks. But which should you do first? In this section you'll learn about risk management, which is a process that provides a way to rank risks so the most urgent problems to be dealt with first.

You will also learn about data privacy, which is a key concept that we've been talking about and around in all the previous sections. That is, you've learned that one of the main goals of attackers is to gain unauthorized access to data, because this data may be of some value. If the data didn't have any value, there wouldn't be any need to protect it. In this section you'll take a closer look at some of the main categories of data that need to be protected, some of the laws that mandate protection, and the steps that organizations that handle sensitive data need to take to comply with the laws.

Objectives

At the end of this module students will be able to:

1. Define risk
2. Define mitigation

3. Describe strategies for reducing risk
4. Describe the cyclic process of Risk Management
5. Explain concerns surrounding data privacy
6. List methods for protecting data
7. Create a risk heatmap for their personal devices
8. List the steps for mitigating the greatest risks to their personal devices
9. List the 3 pieces of data required for identity theft
10. Explain how and why many people give away data that should remain private
11. Check their credit scores for evidence of ID theft

Section Content

Introduction

In this chapter you will learn two different subjects, Risk Management and Data Privacy. These two subjects might seem to be unrelated, especially when you're looking at the details and learning the new terminology. But if you step back and look at the big picture the relationship should become more clear. That is, from a cyber security perspective the main thing an organization needs to protect is its data, and the best way to protect data is by using the risk management process.

Risk Management

The book presents all kinds of information about risk management, from defining risks to formulas used for calculating risk impact. This is all good information, but I think it's more important that you understand where risk management fits in the big picture of cyber security, which is determining what you should be doing right now. That is, throughout the class you've learned about many different things that can be done to improve cybersecurity for an organization, things like running vulnerability scans, creating backups, training users to avoid phishing scams, setting password policies, etc. Now you have a huge list of things to do and check, but which should you do first? Helping you make this decision, about what should be done first, is where risk management comes into play in the overall process.

With risk management you rank all the known risks by looking at the relative impacts and the relative likelihood. Once the risks have a rank or score, they can be “managed” by mitigating the ones with the highest scores first. All the risks should be addressed sooner or later, but using the risk management process allows you to focus your efforts where they will have the greatest impact.

The tricky part of this process is creating the risk register or risk ranking. That is, how do you know the likelihood for each risk, and how do you know the impact? This knowledge will come with experience but the numbers will also be related to the specific organization you’re working for.

To help you understand the risk management process let’s look at how you might apply it if one of close friends or family members plans to come to visit for the weekend. They’re bringing their two kids, a 2 year old and a 3 year old. You don’t have any kids at home, and you know there are some things that could be potential safety issues. For example, as you look around your home you see the following:

A. There aren’t any covers on any of the electrical outlets
B. There aren’t locks on any of the cabinets
C. Your home has a basement and there’s no door to the stairs
D. There are exposed cables connecting your TV to your home audio system
E. One of your windows has a latch that doesn’t lock
F. You have a glass topped coffee table with sharp corners
G. You have a decorative bowl of marbles and small rocks in the main room.

If you’ve never had kids then there are probably many other things you should worry about, but this isn’t meant to be a comprehensive home safety check, we just want a few items that we can use to demonstrate the ranking process.

I’m first going to rank these items on a scale of 1-4 by their relative impact. In this case, the impacts would be the severity of the injury to one of the kids, with 1 being no injury, 2 being some tears and screaming, 3 would be something severe enough that it’s requires a trip to the doctor or hospital, and 4 severe injury or death.

Item	Rank	Description
A	2	No covers on any of the electrical outlets
B	2	No locks on any of the cabinets
C	4	No door to basement stairs
D	2	Exposed cables connecting your TV to your home audio system
E	1	Window with a latch that doesn’t lock
F	3	Glass topped coffee table
G	4	Decorative bowl of marbles and small rocks in the main room

Next, I’ll rank the likelihood that one of the kids will be affected by one the safety issues. The numbers will go from 1, meaning it’s highly unlikely, to 4 which means it’s very likely. As I create this set of ranking I’m assuming the children aren’t going to be left unsupervised for more than a few moments. If they were most of the numbers would be much higher.

Item	Rank	Description
A	2	No covers on any of the electrical outlets
B	2	No locks on any of the cabinets
C	4	No door to basement stairs
D	4	Exposed cables connecting your TV to your home audio system

E	1	Window with a latch that doesn’t lock
F	4	Glass topped coffee table
G	4	Decorative bowl of marbles and small rocks in the main room

You might not agree with my rankings, which is ok. We both might change our rankings if we had more information about the specifics. But in any case, remember that we’re just using this as an example. If we use my rankings to create a Risk Heatmap we’d end up with the following:

Relative Impact	4	🟩	🟧	🟥 F	🟥 C G
	3	🟩	🟧	🟥	🟥
	2	🟩	🟧 A B	🟧	🟧 D
	1	🟩 E	🟩	🟩	🟩
		1	2	3	4
		Relative Likelihood			

The rankings and the heat map show that the first things you need to mitigate are items C, F, and G. After you’ve taken care of these items, you should next look at ways to mitigate A, B, and D.

Another thing you should note about the Risk Management process is that it isn’t a one-and-done deal. It’s part of a cyclical process where you periodically rank and then mitigate all the current risks. If we lived in a world where technology never changed you might be able to do everything you needed to provide perfect security and then consider your job finished. But, as you’ve seen, in the real world technology is constantly being updated, and new threats are being discovered on a daily basis, so there will always be new security challenges. Plus, most businesses are dynamic as well, adding or changing services, suppliers, processes, etc.; things that will impact or be affected by cyber security. The only way to stay secure in a dynamic environment is to perform the risk management process on a regular basis. The exact timing can vary, but it’s something that most security professionals recommend doing every few months. Doing the full ranking takes some time, so it's not something you would do every day, but new security issues are found daily, so waiting a year would be too long.

The last thing I want to point out about risk management is that the cyber security risks aren't the only risks a company faces. That is, a company might also face risks from competition, the overall economy, supply chain risks, environmental risks like flooding or earthquakes, etc. This means that the company will integrate and evaluate the cyber security risks along with the overall company risks, which means you as a cyber security specialist you might have to fight for funding. In the "old days" this was a big issue as many companies saw the business risks, but didn't see the cyber security risks. The size and scope of cyber security incidents has increased to where most businesses now know it's an important issue, which is sad for us as a society, but good for anyone working in the cyber security.

Data Privacy

The other subject covered in this chapter is Data Privacy. The book does a good job covering the terminology and security issues associated with data privacy. As you read through this material try to keep in mind that in the big picture, protecting data is the reason cyber security exists. If there were no digital data there wouldn't be any need for cyber security.

The only other thing I have to add is an idea for increasing the motivation for any organization to protect data. This idea came from my friend Donna Starr. Her idea consists of taking the private information for the top earners at any organization, placing it in escrow, and if the organization has a breach and releases customer data, releasing the top earner's data to the public. This would provide the strongest motivation for any organization to take the time and effort to ensure their customer data is protected. And, if a breach occurs, it provides a truly just consequence for the organization's top executives.

Applying What You’ve Learned to Your Home System(s)

When it comes to risk management and your home systems, I don’t have suggestions that I haven’t already made once or twice. The biggest risks to your home systems can be mitigated by ensuring you’re installing updates and patches, using strong passwords, and creating backups on a regular basis.

When it comes to data privacy, I have two suggestions. The first is to ensure that you’re following the common guidelines for protecting your personal and sensitive data. There are plenty of checklists available on the Internet that will guide you through the commonly suggested steps. For example, the following article provides an extensive list of steps you should take to protect your systems and your personal data.

https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe

If this web site no longer exists you can do your own search for something like “how to protect private data”.

My second suggestion is one that’s not found on many checklists, but it’s one that I use frequently. This suggestion has to do with providing your birth date, and using a fake date. Your birth date is one of the three key pieces of personally identifying information that are most commonly used, along with your name and your Social Security Number. For this reason, I suggest only supplying your real birth date to organizations that absolutely need it, like your bank or your employer. For other organizations, especially social media, I suggest making up and using a fake birth date. I also suggest you always use following guidelines to make it easier to remember your new fake birth date:

1. Always use the same fake birth date. Don’t use random dates as you may be asked to supply your birth date if you can’t remember your password. If you use random dates they will be much harder to remember than if you always use the same fake date.

2. Make the month and year of your fake birth date something easy to remember, like your favorite holiday. For example, July 4, or Halloween, or May 4th for you Star Wars nerds. I also suggest picking a date that’s close to your actual birth date. My reasoning for this is explained in item 3.

3. Keep the year of your fake birth date the same as your actual birth year. This will not only make it easy to remember, but may help you on sites that have restrictions or benefits based on your age. For example, I’m involved in some athletic events that use an age ranking. I don’t want to provide these sites with my actual birth date, but I do want my ranking to be correct, which requires that I supply the correct year.

Of course, one of the side effects of this is that many of your social media friends won’t know your actual birthday, and you’ll get birthday wishes on your fake date instead of your real birthday.

And … I know I’ve joked around a bit in the class, so you might be asking yourself if this is a serious suggestion. I want to assure you that this an important thing to do. Like I said, there are only 3 key pieces of information that are used to identify you in most situations, your name, your birth date, and your SSN. If an you’ve used your real birthday on your social media account, you will have given an attacker 2/3 of information and made their attack much simpler.

Ways to Check Your Comprehension

This is the last chapter to be included in the third test. Even though there’s no delay between this chapter and the test, I still suggest that you use the review questions at the end of the chapter, and the practice test, to check your comprehension before taking test 3.

For the test itself, make sure that you leave yourself adequate time to complete it by the due date. Remember that the test must be completed on time to receive any points. The test will lock at midnight on the due date, so if you haven’t finished it by then you will be locked out. Also remember that the test is open book and open note, but you must do your own work.

There is also an optional Test 4 that you can use in case you missed a test, or to replace a low test grade on one of the first three tests. Here are some things you need to be aware of regarding Test 4.

- Taking Test 4 is completely optional, and taking it cannot hurt your overall class grade. Only your highest three test scores will be used towards your overall class grade, so if you take all four tests and your Test 4 score is the lowest of the four, it will be dropped.
- If you decide to take Test 4 note that it must completed by 11:59PM on the due date. Make sure and plan accordingly, and leave plenty of time to complete the test.
- Test 4 is comprehensive, and will have questions from all sections of the class.
- Like all tests in this class, Test 4 is open book and open note, but you must do your own work.

The Activities for This Section

There are two required activities for this section and one optional activity that I strongly urge you to look at and then complete if you haven’t previously completed the steps. The required activities are Hands-On Projects 15-3 and Case Project 15-1 or 15-2. The optional assignment is Hands-On Projects 15-1.

1. [OPTIONAL] Hands-On Project 15-1: Viewing Your Annual Credit Reports

There are several things you should do periodically to check your private data and information. This project shows you how to check your credit reports, but you should also check sites like Social Security and the State Employment to ensure that your information is secure and up to date. Some of the sites, such as the State Employment and Department of Labor sites have caused problems because they let anyone create an account without doing any type of authentication. This has allowed attackers to easily impersonate other people, create fake accounts and steal someone’s identity and do things like file for unemployment benefits, remaining unknown to the actual person.

You should also check these sites for other family members, particularly any minor children. Many attackers target their attacks at minor accounts for things like Social Security, as most people don’t check their Social Security accounts until well into adulthood. This makes it less likely that the identity theft will be noticed, possibly for years.

What to submit for Project 15-1:

- There is nothing to submit for this optional assignment.

2. Hands-On Project 15-3: Online Phishing Training

The purpose of this assignment is to demonstrate the type of user training available to help train an organization’s non-technical users. Hopefully you’re already aware of the information being presented, so the thing you should think about is whether you think this would provide adequate training for non-technical users. It looks like the site specified in the book has changed and now requires an account, which we can't get. To complete the assignment, you can either do your own search for something like "phishing awareness training" or "free online phishing training". I did that and found a few sites you could use including:

https://www.phishingbox.com/phishing-test

What to submit for Project 15-3:

- Take a screen shot after step 2, and another showing the certificate of completion for the training. You'll receive this certificate at the very end.
- Answer question 8

3. Case Project Homework (Writing Assignment)

Choose one of the following Case projects located at the end of chapter 15: 15-1, or 15-2.

If you don't remember what's required you can refer to the Written Project Guidelines document for details on how your paper/report will be graded. You can find the document at:

https://tonysako.com/writingprojectguidelines2021/