Network and System Security for Small- and Medium-sized Businesses

Part 2 – Risk Assessment

Part 2: Assess Any Special Risks and Requirements

Step 1: Identify any special adversaries
Step 2: Identify all critical data assets
Step 3: Identify where critical data is stored and transmitted
Step 4: List threat scenarios for critical data
Step 5: Calculate Risk to Prioritize Cybersecurity Efforts
- How to identify risk
- How to prioritize risk

Step 6: Implement strong security controls for sensitive data based on risk

---

Part 2: Assess Any Special Risks and Requirements

Rationale: After implementing fundamental security controls (as addressed in Part 1 above), each business must further assess their situation to understand any special risks to their information. This "risk assessment" will make sure they account for potential negative impacts arising from the compromise of any particularly sensitive information. It will also account for any elevated threats (or threat actors) they may need to protect against.

Frequency: Comprehensive risk assessments of all information should be done regularly (probably annually), but at least any time major changes take place in your infrastructure, equipment, or operating systems. Furthermore, you should be doing regular risk assessments of all new hardware or software as it is introduced into your environment.

Start Here: As you read the steps here, just start with what you know. You may immediately recognize some of the most critical data you have, know where it is stored, and know who might want to access it. With that knowledge you can easily identify an area of greatest concern (or threat scenario). Write it down. Choose what security controls would help minimize the risk of that happening. The things you are most concerned about may indeed be the greatest risks to your organization. Start there and then reiterate through the process!

Outline of Major Steps (as detailed below):

1. Consider if you have any special adversaries
2. Identify all critical data assets
3. Identify where this critical information is stored and how it is transmitted
4. List out various Threat Scenarios for critical data assets
5. Calculate Risk to Prioritize Cybersecurity Efforts
6. Implement strong security controls for sensitive data based on risk (How to identify risk, How to prioritize risk, Select security controls to mitigate risks)

NOTE: If you or your people are working in a foreign country I strongly suggest you take the training found at www.expatdigital.com in order to live and operate securely and effectively. This site focuses on helping you understanding your risk situation and applying appropriate security controls.

Step 1: Consider if you have any special adversaries

Think about any adversaries you might have (beyond opportunistic criminal hackers) who would be actively seeking your information (or in whose hands your information would be especially damaging), such as antagonistic individuals/neighbors, militant groups, or hostile governments.

1) If you identify special adversaries, you need to further consider both the motivation and capabilities of these adversaries. If they have sophisticated hacking capabilities, and if they have strong motivation to obtain your information, then the likelihood of them accessing your data is greatly increased and you will need to apply more stringent security controls.
2) If you identify special adversaries, then you will need to implement further security controls and precautions (beyond those in Part 1 above).

Step 2: Identify all critical data assets

Take time to identify and list all the important information that you keep in your environment. Consider: personal contact information, email, company plans, financial information, emails, photos, etc.

1) The value of this information should be considered in terms of the following:
    a) Confidentiality - what damage would you suffer if the information was made known to unauthorized individuals (like special adversaries, or just posted on the Internet)?
    b) Availability - what if the data were lost (by hardware failure, encrypted by ransomware, accidentally deleted, etc.) and was not able to be restored/recovered? Even if the data could be recovered, would there be serious problems during the time it took to restore?
        i) Consider the impact if you lost connection to the Internet, due to a hardware outage or a Denial of Service attack? What data would inaccessible? How would that impact to your business?
    c) Integrity - what if someone erroneously changed the data, intentionally or unintentionally?
2) If applicable, interview all relevant individuals in your organization, to understand *what* information you have and *where* it is stored.
3) **NOTE:** Make sure to strongly protect this list of data assets as it can be a map to your most critical information if the list itself were to fall into the wrong hands. Consider if your situation is too risky to even keep a list of your valuable information written or listed anywhere. It should at least be encrypted and possibly only be a mental list.
4) **NOTE:** If you have information stored on your computer systems that may endanger others (like getting people killed or imprisoned), most likely it should NOT even be stored electronically!
    a) If you must store highly sensitive information, make sure it is strongly encrypted.
        i) Even if strongly encrypted, it is usually operational mistakes (people and process) that leak data, not the weakness of the encryption technology.
    b) AND Consider storing it in a way that would need two documents for it to be useful for an adversary or criminal hacker, such as listing pseudonyms in one file, but people's real names in another file, without an obvious connection between the two. These real names would be kept *very* secure (such as by using steganography along with encryption, and/or kept in different locations, or only kept on paper and hidden, etc.).

NOTE: If you don't have any special adversaries or any especially sensitive information, then the rest of this risk assessment may be considered optional for very small businesses (but still helpful for disaster recovery purposes).

Step 3: Identify where this critical information is stored and how it is transmitted

You need to identify where your information is stored and where/how it is transmitted. These storage locations or transmission channels represent points of vulnerability and must have extra security controls applied to ensure the security of the data.

Consider if information is stored and transmitted in the following technical "containers":

1) Stored on local file servers or file sharing areas (such as networked attached storage devices)?
2) Stored on local computers or laptops?
3) Where is this data backed up to? (The primary data may be secure, but then stolen from the backup location.)
4) Is it stored online or with a Cloud provider?
   a) Make sure to take note of all information stored in the Cloud, as this will have special security implications.
   b) Consider encrypting all files before they are put in the Cloud, or at least use a Cloud Service Provider that has very strong security controls, practices, and policies.
5) Is this data transmitted via email?
6) Is the information transferred to other locations via any other means?
7) Is the information stored on removable media, such as a USB flash drive or removable disk?

Step 4: List out various Threat Scenarios for critical data assets

Based on the information you have gathered so far, you should now be able to identify threat scenarios where certain threat actors could try to compromise your data where it is stored or transmitted. You should first just consider security situations that you are aware of and concerned about. These areas of concern are most likely some of the highest risk situations that should be addressed. Once you have listed these areas of concern as the first threat scenarios, you should go through a more rigorous or methodical process to identify other threat scenarios that give rise to cybersecurity risk.

Step 5: Calculate Risk to Prioritize Cybersecurity Efforts

Risk is measured by understanding the impact of a negative security incident (e.g. breach) combined with the likelihood of the event. i.e. RISK = IMPACT * LIKELIHOOD (Or in other terms, Risk = "consequences" * "probability".) The greatest risk exists for events that would cause the greatest negative impact (based on the value of the information) and have the greatest probability of happening (based on the motivation and capabilities of attackers). Understanding your greatest risks helps to prioritize your cybersecurity efforts, since the greatest risks should be addressed first.

A) <u>How to Identify Risk:</u>

Once you have:

- identified what information you have that is sensitive to you and your people,
- considered what would be the negative impact if this information was exposed to unauthorized individuals or if the data were lost or inadvertently changed,
- understand where this data is stored and how it is transferred,
- have an understanding of the capabilities and motivation of your adversaries,
- Then you can combine these elements to create a detailed list of threat scenarios

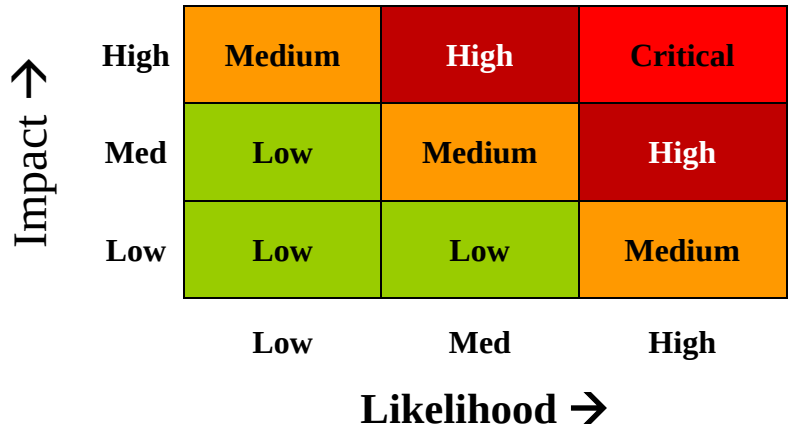
THEN you can better understand the risk to your organization and can decide to apply appropriately robust security controls to minimize the risk of this information being lost or compromised.

B) How to Prioritize Risk:

By mapping out which negative events (threat scenarios) are most likely to occur (based on adversary capabilities and motivation, vulnerability of systems, etc.) and which information is the most valuable (and thus would create a greater impact if compromised), then you can set priorities based on highest risks. As likelihood and potential impact both increase, the risk is greatest. In general, greatest risks should be addressed first.

Although there are sophisticated methods to accurately calculate and quantify risk, the best place for most people to start is by using a qualitative method to calculate risk. This can be done by assigning the values "High", "Medium", or "Low" to both Impact and Likelihood of each threat scenario you have identified, starting with your highlighted Areas of Concern. If the likelihood that a certain event could occur, and the negative impact of that event would be considered "high", then the overall risk would be considered Critical. You should prioritize your cybersecurity efforts based on the highest risks identified.

See this **Risk Matrix** as a visual way to map out the highest risks to your organization:



For example, consider this threat scenario. You may have a list of contacts, which represents some critical and important part of your operations. You know that this information could greatly impact your business if this list got into the hands of your competitors. Thus the **Impact** of this data being breached is High. Furthermore, if you know that your competitors are highly motivated to obtain this list, and you believe they may have considerable computer skills (including time and money), then the **Likelihood** of this data being accessed is also High. Thus, this would be considered a **Critical** risk and should be addressed first. To protect this data and reduce this risk, you must consider where this information is stored and how it might be transmitted. These technical containers would be the place to implement strong security controls to protect this information.

Step 6: Implement strong security controls for sensitive data based on risk

One way you can decrease your risk is by applying further security controls to decrease the likelihood of a security incident/breach, and/or increase your ability to quickly detect a possible breach/incident. In general, the quicker you respond to a breach, the less the damage.

First, list any existing security controls in place for each threat scenario (or overall, per container, etc.) These security controls help to decrease the risk of a negative security incident. Then consider which areas (or data) still have unacceptable risk, where the likelihood and resulting impact of a negative security event still pose more risk than you as an organization are willing to accept. You then should consider what further security controls need to be applied to reduce the risk (by making it harder to exploit a vulnerability).

Please note that you can deal with risk in a number of ways. The most common way is to reduce risk by applying mitigating security controls. You can also avoid a risk by choosing to not keep certain kinds of data or not run certain kinds of systems. (For instance, there is no reason whatsoever to store full credit card numbers. Further, there may be sensitive data about your employees that should not be kept in electronic format based on the risk of harm.) Some risk can be transferred to others by purchasing insurance or by allowing a more capable organization store and secure your data.

Part 3 of this paper will give ideas for security controls to address these risks. (Don't hesitate to engage with third-party cybersecurity experts to help reduce these risks and move forward in your security journey.)

Resources for Further Research

Risk Assessments:

1) The information security risk assessment: identifying threats: www.vigilantsoftware.co.uk/blog/the-information-security-risk-assessment-identifying-threats/
2) Software to Help do Risk Assessment: www.vigilantsoftware.co.uk/product/vsrisk-standalone
3) Creating a Threat Profile for Your Organization (Note: But don't get bogged down in details) www.sans.org/reading-room/whitepapers/threats/creating-threat-profile-organization-35492

Incident Response Planning:

1) Cybersecurity Incident Response Planning: digitalguardian.com/blog/incident-response-plan
2) Responding to IT Security Incidents: technet.microsoft.com/en-us/library/cc700825.aspx
3) 10 steps for a successful incident response plan: www.csoonline.com/article/3203705/security/10-steps-for-a-successful-incident-response-plan.html