



CYBERSECURITY
EXPERTS ON YOUR SIDE

DATA PROTECTION

for small and medium-sized
businesses



issue 3

Assessing Data Security Risks

In This Chapter

- Looking at the risk assessment process
- Identifying data processing operations
- Determining the impact of a data breach
- Identifying pertinent data security threats
- Implementing appropriate data protection controls

Chapter 3

ASSESSING DATA SECURITY RISKS

In this chapter, you will learn how to apply the risk management process (discussed in Chapter 2) to data security.

Understanding the Risk Assessment Process

Risk assessment is the first phase of the risk management process (discussed in Chapter 2). A risk assessment consists of:

- Identifying your assets (both tangible and intangible)
- Analyzing threats (including impact and likelihood)
- Assessing vulnerabilities (that is, what safeguards or controls are absent or insufficient in a given asset)

Similarly, assessing data security risks involves:

- Identifying your data processing operations (to determine how and where your data assets are used by your business)
- Determining potential business impact (if your data is compromised)
- Identifying possible threats and evaluating their likelihood of occurrence, including frequency
- Evaluating risk (to assess which safeguards or controls should be implemented to protect your data)

Step 1

Identify Your Data Processing Operations

Data within an organization has different risk profiles, not only based on the content of the data, but also due to the way data is used within the organization. Thus, it is important to understand how data is processed within your business as you begin the risk assessment process. For example, a typical SME might have some or all of the following types of data processing operations:

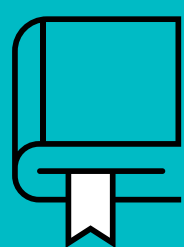
Human resources such as employee payroll management, recruiting and retention, training records, disciplinary actions, and performance evaluations.

Customer management, marketing, and suppliers such as customer information, purchase and sales orders, invoices, email lists, marketing and advertising data, and vendor contracts.

Personnel safety and physical security such as employee security access logs, visitor logs, and video monitoring.

For each data processing operation, consider the following:

- What personal data is being processed?
- What is the purpose of the process?
- Where does the processing occur?
- Who is responsible for the process?
- Who has access to the data?



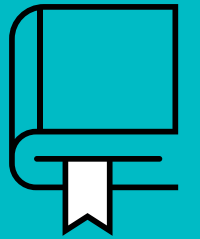
REMEMBER

The principle of least privilege is an information security best practice in which end users are granted only the minimum level of access required to perform a specific job function.

Step 2

Determine Potential Business Impact

Next, you need to determine the potential impact of a data breach or compromise. A breach or compromise may affect the confidentiality (for example, unauthorized access) of data, the integrity of data (for example, unauthorized modification), or the availability of data (for example, a ransomware attack).



REMEMBER

Organizations must protect the confidentiality, integrity, and availability of data. In information security, this is known as the C-I-A triad (see page 14-15).

In a typical risk assessment, the potential impact of a given risk is typically expressed in terms of damage to the organization, such as the loss or destruction of a physical asset (for example, a server, a copier machine, or a vehicle).

The impact of a risk to data security to the business is similar to other risk impacts, but the impact may be indirect. In the case of sensitive personal data, the individual whose data is breached or compromised is the direct victim. In such cases, an individual's identity or financial assets may be stolen and/or their privacy may be violated. The impact to the business is less direct but still very costly and may include (among others):

- Loss of customers and revenue
- Brand damage and adverse public relations
- Regulatory fines and litigation
- Breach notifications and credit monitoring services
- Forensic analysis and recovery



TIP

Business impact can be classified as Low, Medium, or High. However, the actual definition of each of these impact levels will be unique to every business and should involve both objective (quantitative) and subjective (qualitative) measures.

Step 3

Identify Possible Threats and Evaluate Their Likelihood

A threat can be any event or circumstance, either natural or manmade, that has the potential to negatively affect the confidentiality, integrity, or availability of personal or sensitive data. This can include cybersecurity attacks, accidental loss or disclosure, insider threats, fire and flooding, earthquakes and tsunamis, severe weather (such as a hurricane or tornado), civil unrest, labor disputes, and more. Businesses must identify possible threats to their data processing operations and evaluate the likelihood (including frequency of occurrence) of each possible threat. Ensure that you cover threats in well-defined areas including threats from network and technical resources (software/hardware) that are used for data processing, threats from related processes and procedures, threats from involved human resources, and threats from scale of processing.



TIP

For each threat identified, the likelihood can be classified in a manner similar to the business impact: Low, Medium, or High. When evaluating the likelihood of a threat occurring, consider both the likelihood of the threat occurring at all, as well as how frequently it is likely to occur during a given period (for example, over a one-year period).

Step 4

Evaluate Risk

Once you've identified all of your data processing operations (and the data being processed), determined the potential business impact of a data breach or compromise, and identified possible threats and the likelihood and frequency of occurrence, you can evaluate the risk associated with each operation and determine the appropriate data protection control technology controls (discussed in Chapter 4) and organizational/process. According to the risk evaluation, organizational and process controls (discussed in Chapter 5) should be implemented to properly secure your data and data processing operations using a risk-based approach.

Figure 3-1 shows a data assessment template and an example of a data processing operation assessment.

		Impact Level			
		LOW	MEDIUM	HIGH	VERY HIGH
Threat Likelihood	LOW	LOW RISK	MEDIUM RISK	HIGH RISK	
	MEDIUM	LOW RISK	MEDIUM RISK	HIGH RISK	
	HIGH	MEDIUM RISK	HIGH RISK		

Threat Likelihood

For particular data processing operation walk through list of possible data processing threats and evaluate/score threat likelihood. Final likelihood should be based on sum of score from all threats in threat list.

- **Low** – the threat is unlikely to materialize
- **Medium** – there is a reasonable chance that the threat materializes
- **High** – the threat is likely to materialize

Impact Level

For particular data processing operation evaluate possible impact on data confidentiality, integrity, availability (C-I-A triad). The highest impact of the three is the final impact level.

- **Low** – minor inconveniences, which could be overcome without any problem
- **Medium** – significant inconveniences, which could be overcome despite a few difficulties
- **High** – significant consequences, which could be overcome but with serious difficulties
- **Very High** – significant, or even irreversible consequences, may not be overcome

Data processing operation poses

- **Low Risk**
- **Medium Risk**
- **High Risk**

Example

Data processing operation: Marketing/Advertising
Data processed: Contact info (e.g. name, postal address, telephone number, email)
Data classification: Personal Data
Processing purpose: Promotion of goods and special offers to possible customers
Data Subjects: Customers and leads

Threat Likelihood

Network and technical resources (HW, SW) threats: Medium
 processes and procedures threats: Low
 involved human resources threats: Medium
 Business sector and scale of processing threats: Medium
Final likelihood: Medium


Impact Level

Impact level assessment confidentiality: low, integrity: low, availability: low
Final impact level: Low

Data processing operation poses

- **Low Risk** – processing of Marketing/Advertising data pose Low risk – Technical and Organizational measure adequate to this risk should be implemented.

Figure 3-1: Risk Assessment Matrix for data processing operation



YOUR DATA IS YOUR BUSINESS

MAKE SURE YOUR COMPANY IS SAFE FROM DATA BREACHES OR LEAKS. EMPLOY OUR POWERFUL, EASY TO DEPLOY ESET ENDPOINT ENCRYPTION

- ✓ Safely encrypt hard drives, removable media, files and email
- ✓ Boost your information security and comply with the GDPR
- ✓ Add an additional security layer with ESET Secure Authentication

VISIT THE ESET WEBSITE FOR ALL OUR SOLUTIONS.



CYBERSECURITY
EXPERTS ON YOUR SIDE

WWW.ESET.COM



**CYBERSECURITY
EXPERTS ON YOUR SIDE**

WWW.ESET.COM

© 1992 - 2019 ESET, spol. s r.o. - All rights reserved. Trademarks used therein are trademarks or registered trademarks of ESET, spol. s r.o. or ESET North America. All other names and brands are registered trademarks of their respective companies.

We gratefully thank Lawrence Miller for content preparation of this e-book.