ROGUE NINJA CREATIVE

SMALL BUSINESS CYBERSECURITY

Understanding and Assessing Risks

by Mike Figueroa

Small Business Cybersecurity: Understanding and Assessing Risks

Version 1.0, Published November 2023

Author: Mike Figueroa

Publisher: Rogue Ninja Creative

www.rogueninjacreative.com

Table of Contents

Introduction

If you're a small business owner you've likely found yourself more dependent on technology these days for tasks like customer data management, internal communication, and other critical operations. But while technology offers efficiency and scalability, it also brings an elevated level of risk.

The security of your customer's private information, as well as your own confidential business data, should be a top priority. In October, 2020, a survey by the **Canadian Federation of Independent Business** (CFIB) found that 45% of small businesses have experienced a random cyber attack, while 27% experienced a targeted attack[1]. These attacks are becoming more and more sophisticated over time, and small businesses are increasingly at risk.

This guide is intended to help you conduct an initial cyber security assessment of your small business and evaluate the overall risk tied to your assets, systems, or processes. While not a definitive blueprint, it offers a starting point for exploring the various factors that contribute to risk.

Additionally, it acts as an introductory resource for small business owners who might not yet have the financial means for expensive software or a specialized IT team. By following the recommendations in this guide, you can still mitigate the impact a cyber attack could have on your business. Use it as a starting point for developing more robust security measures that fit your business and team.

At the end of this guide, you'll find links to useful resources, including a helpful Excel workbook based on this guide that you can use to conduct your own initial cybersecurity risk assessment.

So, without further delay, let's get to it!

1 "Nearly Half of Small Businesses Experienced Cyberattacks." CFIB-FCEI, 8 Dec. 2022, https://www.cfib-fcei.ca/en/media/nearly-half-of-small-businesses-have-experienced-random-cyberattacks-in-the-past-year.

Conducting a Risk Assessment

A well-executed risk assessment serves as a foundational element in any cybersecurity strategy. Given its critical importance, large organizations often invest millions into sophisticated systems and specialized personnel for this task. However, even with a smaller team and fewer resources, you can still conduct a robust assessment that effectively identifies and mitigates risks.

This guide follows a risk assessment process that can be outlined in five essential steps:

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5
Identify Assets	Evaluate Vulnerabilities	Identify & Evaluate Threats	Calculate Impact	Calculate Risk

Using sample data, we'll walk through each step to help illustrate the process.

In step 1, we'll take inventory of the data we need to protect and all elements of the business that interact with it.

In step 2, we'll use a custom risk assessment questionnaire to make granular, item-by-item evaluations of security protocols.

In step 3, we'll look at potential threats, such as cyber-attacks, that could exploit our vulnerabilities.

In step 4, we'll use an impact assessment questionnaire to evaluate the potential impacts if these threats successfully exploit our vulnerabilities.

At each step, we'll rate our assets based on their respective risk factors for straightforward comparison and prioritization.

In step 5, we'll calculate total risk scores to guide our evaluation and prioritization of the overall risks associated with our assets.

Step 1: Identify Assets

We'll begin by identifying and classifying our business data. Every piece of information we use to conduct business needs to be identified. We'll need to determine where this data is stored—whether on internal servers, cloud storage, or portable storage drives—and note the levels of sensitivity.

Data Assets

Figure 1.1 shows a table of ten rows containing our sample data. The data is classified and sorted based on its intended audience, ranging from public access to restricted internal or confidential use.

The storage locations for each type of data are also specified, matching

Data Asset	Data Type	Classification	Location
API Keys	Authentication Credentials	Confidential	~/admin/keys (app-server)
Customer Data	Personal Information	Confidential	Salesforce, Encrypted Backup (db-server)
Email Subscribers	Contact Information	Confidential	Mailchimp
Employee Payroll	Financial Information	Confidential	ADP Workforce Now, Encrypted Backup (db-server)
Company Policies	Legal Documents	Internal	Company Intranet, SQL Database (db-server)
Product Inventory	Business Data	Internal	SQL Database (db-server)
Sales Reports	Financial Information	Internal	Encrypted Shared Drive
Website Analytics	Metrics and Statistics	Internal	Google Analytics Service Dashboard
Customer Reviews	Feedback	Public	Company Website Backend
Social Media Posts	Website Content	Public	Public Cloud Storage

Figure 1.1: A partial table of data assets

the hardware, software, or physical spaces that should also be included in our assessment.

For space reasons, this is only a partial table; many other details we should include have been left out. Things like importance of the data's integrity, availability, and encryption, as well as who, if anyone, is responsible for its administration, are all factors that would contribute to our assessment in a real-life scenario. All of these columns are included in the Excel workbook referenced at the end of this guide.

Hardware Assets

So, now that we've located our data, the next step is to list all hardware assets that store, process, or transmit it. We should document the

Hardware Asset	Category	Location	Assigned To	Status
Cisco Firewall	Network Security	Server Closet	Admin	Active
Dell OptiPlex	Desktop	Desk 1	Sarah Johnson	Active
HP LaserJet 4050	Printer	Common Area	Shared	Active
iPhone 13	Mobile Device	Remote	Bob Brown	Active
MacBook Pro	Laptop	Desk 2	Tim Lee	Active
Netgear Router	Networking Equipment	Server Closet	Admin	Active
Raspberry Pi 4	Development Board	Desk 4	Rick Morty	Active
Samsung Monitor	Display	Desk 3	Shared	Active
Windows Server 2019	Server	Google Cloud	Admin	Active
Android Tablet	Mobile Device	Remote	Jane Doe	Inactive

Figure 1.2: A partial table of hardware assets

manufacturer, model number, current location, and status, and identify who has physical or remote access to the equipment.

Our sample hardware data in Figure 1.2 has some typical equipment a small business might own, and includes the physical locations and the team members they're assigned to.

It may seem unnecessary to include something like a printer in a cyber security risk assessment, but even **seemingly innocuous devices can present vulnerabilities**. Printers, for example, are often network-connected and can be exploited to gain unauthorized access to a network. They may also store sensitive information temporarily, which could be retrieved by an attacker. Additionally, if a printer's firmware is out-of-date, it may be susceptible to malware or other security threats.

Also, if members of your team use their **personal devices** for business communications, such as emailing clients or accessing company file, it's essential to include their devices in your risk assessment, regardless of how low you perceive the overall risk to be. Failing to do so can create a significant blind spot in your cybersecurity strategy, one that could potentially worsen over time.

Finally, don't forget to include **decommissioned equipment** in your assessment. Any hardware that is slated for disposal should be carefully tracked, and if it has the capability to store data, it must be securely wiped.

Software Assets

Following hardware, we need to identify all the software assets that interact with our hardware and ultimately our data. This includes applications, databases, and operating systems, both locally installed and cloud-based. All elements involved in storing, processing, and transmitting our data should be listed.

We can use our software assets table to make connections between our hardware and our data. In Figure 1.3, for example, we list the data and hardware that our software interacts with in two adjacent columns.

Software Asset	Purpose	Interacts with Data	Interacts with Hardware
Ubuntu 22.04.3 VM	app-server and db-server	API Keys	Dell OptiPlex, MacBook Pro
Salesforce	CRM	Customer Data	Dell OptiPlex, MacBook Pro
QuickBooks	Financial Management	Employee Payroll	Dell OptiPlex
Mailchimp	Email Marketing	Email Subscribers	iPhone 13, Android Tablet
ADP Workforce Now	Payroll	Employee Payroll	All Desktops, Laptops, and Mobile Devices
Microsoft Excel	Spreadsheet	Sales Reports	MacBook Pro
SharePoint	Document Management	Company Policies	Dell OptiPlex, MacBook Pro
Adobe Acrobat	PDF Management	Legal Documents	Dell OptiPlex, MacBook Pro, Android Tablet
Hootsuite	Social Media Management	Social Media Posts	Dell OptiPlex
Google Analytics	Web Analytics	Website Analytics	None

Figure 1.3: A partial table of software assets

We also sort our software based on its importance. Some are mission-critical, handling sensitive data or core functionalities of our business, while others are less integral but still part of the network. Sorting them helps in prioritizing which assets require the most attention in subsequent steps of our risk assessment.

Keeping Our Assets Lists Updated

It's important to remember that identifying our data, hardware, and software assets is not just a one-time activity, but an ongoing process. As our business evolves, so do the assets we rely on. Maintaining updated asset lists allows for a quick response in case a particular asset becomes a point of vulnerability, as we'll already have an inventory to refer to.

Step 2: Evaluate Vulnerabilities

After inventorying our assets, the next move is to assess the vulnerabilities associated with them. Vulnerabilities can be technical, such as outdated software or firewall misconfigurations, or human, like employees susceptible to social engineering tactics.

Technical Vulnerabilities

Technical vulnerabilities can range from outdated software versions susceptible to known exploits, to firewall misconfigurations that leave your network exposed. Regular security audits, penetration tests, and automated scanning tools are invaluable for identifying these vulnerabilities. Neglecting software patches or using default configurations are also common technical vulnerabilities that can be easily overlooked but can have severe consequences.

Human Vulnerabilities

Human vulnerabilities are inherent risks associated with the behavior and actions of the people in your organization. These can range from simple training lapses, like an inability to identify phishing emails, to more severe issues like potential insider threats. Employees might unintentionally share sensitive information or fall victim to social engineering attacks. Addressing human vulnerabilities often involves ongoing education and training, alongside monitoring tools to catch unusual or risky behavior.

Physical Vulnerabilities

Physical vulnerabilities pertain to the security of your physical locations and the hardware stored there. This includes everything from inadequate surveillance and poorly secured entry points, to unattended workstations and portable storage devices. It's not just about locking doors; it's also about controlling who has access to what and monitoring that access. Physical vulnerabilities can also extend to natural disasters or other events that could physically damage your assets, so disaster recovery plans are crucial here as well.

In our example, we could start by considering the four confidential data in our data table. Summarized in Figure 2.1 below, we can see that the data are stored in different locations. There are three 3rd-party services: Salesforce, HR Software, and Mailchimp. But there are also two locations for backups and credentials storage: db-server and app-server.

Data	Data Type	Classification	Location
API Keys	Authentication Credentials	Confidential	~/admin/keys (app-server)
Employee Payroll	Financial Information	Confidential	ADP Workforce Now, Encrypted Backup (db-server)
Email Subscribers	Contact Information	Confidential	Mailchimp
Customer Data	Personal Information	Confidential	Salesforce, Encrypted Backup (db-server)

Figure 2.1: Confidential data assets from Figure 1.1

If we look at the "Interacts with Data" column of our software table, summarized in Figure 2.2, we can immediately see that our confidnetial data sets are at the top of the list.

Customer contacts, employee payroll, and email subscribers are stored, managed, and accessed via well-known third-party services that you might also be using in your small business. These services often

Software	Purpose	Interacts with Data	Interacts with Hardware
Ubuntu 22.04.3 VM	app-server and db-server	**API Keys**	Dell OptiPlex, MacBook Pro
Salesforce	CRM	**Customer Data**	Dell OptiPlex, MacBook Pro
QuickBooks	Financial Management	**Employee Payroll**	Dell OptiPlex
Mailchimp	Email Marketing	**Email Subscribers**	iPhone 13, Android Tablet
ADP Workforce Now	Payroll	**Employee Payroll**	All Desktops, Laptops, and Mobile Devices

Figure 2.2: A partial table of software assets

hold security certifications such as ISO 27001, meaning they adhere to comprehensive security standards defined by the International Organization for Standardization and are therefore generally considered trustworthy.

About Digital Standards

In Canada, we have the Digital Governance Standards Institute, part of the Digital Governance Council and Canada's only accredited digital governance standards development body. The standards the DGSI provides, like ISO 27001 and others, are comprehensive, detailed, and rigorously structured guidelines that include best practices for risk management, detailed control objectives, compliance checklists, and protocols for ensuring data security, integrity, and confidentiality.

Rogue Ninja Creative follows the guidelines laid out in CAN/CIOSC 104: 2021, Baseline Cyber Security Controls for Small and Medium Organizations, CAN/DGSI 103-1, Digital Trust & Identity – Part 1: Fundamentals, and others. The relevance of these guidelines goes beyond mere best practices; they serve as industry benchmarks that reflect the collective experience and expertise of the cybersecurity community.

While these standards are voluntary, not adhering to them can result in legal consequences, loss of trust from consumers, governments, and business partners. Even if not legally mandated, these standards represent industry best practices. Ignoring them may expose your business to unnecessary risks and harm your reputation.

Your next step after reading through this guide, therefore, should be to visit the DGC website and check if there are published Standards relevant to your specific industry. CAN/CIOSC 104: 2021 is a good place to start. It includes a risk assessment questionnaire similar to one we'll be using here.

Vulnerability Assessment Questionnaire

Authentication and Access Control:

- What authentication methods are used for accessing the data?
- How many people have the necessary permissions to access this data, and what are their roles?
- Is multi-factor authentication (MFA) enabled for all users who have access?
- Are there any instances of shared accounts or credentials, and if so, why?

Password and Key Management:

- How often are passwords or keys changed?
- Is there an enforced schedule or policy that governs this?
- What procedure is in place to revoke access for personnel who leave the company or change roles?

Data Handling and Storage:

- Where is the data physically and virtually located?
- What methods are employed to encrypt this data?
- Who within the third-party service or organization has access to this data?

Monitoring and Auditing:

- Are activity logs available, and how often are they reviewed?
- Is there a system in place to automatically alert the security team of incidents?
- Is there an established process for auditing compliance with security policies?

Security and Compliance:

- What certifications do the third-party services or internal systems have?
- Are these services or systems compliant with regulations that your business must adhere to, such as PIPEDA?
- Have these services or systems undergone any recent security audits, and are the findings available?

Incident Response:

- What are the incident response plans for both third-party services and internal servers in the event of a data breach?
- What is the time frame for notifying you or your security team in the event of a breach?

The preceding questionnaire is primarily focused on the technical aspects of cybersecurity, such as authentication methods, data encryption, and incident response plans for both third-party services and internal servers. It also addresses the roles and responsibilities of individuals who have access to our sensitive data, as well as compliance with regulations like PIPEDA.

We should take our time with this evaluation. A meticulous approach ensures that no detail, however minor, is missed. And no matter how trustworthy we deem something to be, we can't overlook the vulnerabilities introduced by human involvement. Even with an impeccable track record and a thousand security certifications, any system is inherently vulnerable when people are part of the equation.

By thoroughly examining each set of data, along with the corresponding software and hardware, we're making a smart investment in our business.

Scoring Our Sample Data

As mentioned earlier, we'll be calculating the overall risk associated with each particular asset. But before we do, we'll need to somehow quantify vulenrabilities in order to treat them as inputs to this equation.

One way to do this would be to rate each asset's vulnerability on a scale of 0 to 1. Ideally, this would be based on a variety of vulnerability assessments, security audits, and evaluation methods, but for our initial assessment it's okay to keep things simple.

For instance, while using our questionnaire, we might become aware of a lack of multi-factor authentication on one of our business devices. Our initial vulnerability score related to unauthorized access would therefore be high.

You know your business best, so trust your knowledge, your research, and your instincts. The point is to think systematically about security to gain a preliminary understanding of our security posture and make better informed decisions about next steps.

Data	Classification	Location	Vulnerability
API Keys	Confidential	/home/admin/keys (app-server)	0.9
Customer Data	Confidential	Salesforce, Encrypted Backup (db-server)	0.7
Email Subscribers	Confidential	Mailchimp	0.6
Employee Payroll	Confidential	ADP Workforce Now, QuickBooks	0.9

Figure 2.3: Data assets with vulnerability scores

Hardware Asset	Category	Status	Vulnerability
Dell OptiPlex	Desktop	Active	0.5
MacBook Pro	Laptop	Active	0.5
iPhone 13	Mobile Device	Active	0.7
Android Tablet	Mobile Device	Inactive	0.4

Figure 2.4: Hardware assets with vulnerability scores

Software	Interacts with Data	Interacts with Hardware	Vulnerability
Ubuntu 22.04.3 VM	API Keys	Dell OptiPlex, MacBook Pro	0.9
Salesforce	Customers	Dell OptiPlex, MacBook Pro	0.7
QuickBooks	Employee Payroll	Dell OptiPlex	0.8
Mailchimp	Email Subscribers	iPhone 13, Android Tablet	0.5
ADP Workforce Now	Employee Payroll	All Desktops, Laptops, and Mobile Devices	0.8

Figure 2.5: Software assets with vulnerability scores

Figures 2.3 to 2.5 show our preliminary vulnerability scores for our sample data using the aforementioned method.

We can immediately see a major vulnerability: our systems use API keys. Our sample data doesn't specify how, but it does say they're stored on a virtual machine running Ubuntu 22. We'll assume they're being used to authenticate with the various software services our imaginary business depends on. This is a common setup because of its simplicity, often used for logging, automation scripts, and other tasks.

If that's the case, this score is warranted. API keys provide extensive access and a compromised account on that virtual machine could expose these keys, leading to serious data breaches.

Customer Data, Email Subscribers, and Employe Payroll, as well as the associated software, may initially be given low scores based on the security certifications of 3rd-party providers, but in light of the API key storage issue, our vulnerability scores for all assets are affected.

The interconnected nature of these assets, combined with the centralized vulnerability of the API keys, creates a domino effect. Essentially, the vulnerability of one becomes the vulnerability of all, placing the entire operation in jeopardy.

Our hardware assessment identifies another potential weakness: the iPhone 13. Historically, mobile devices pose greater security risks, attributed to their portability and increased exposure to various networks. An elevated vulnerability score for the iPhone might suggest either inadequate security protocols on the device or perhaps past security incidents. Every weak point in our network amplifies the overall risk.

Furthermore, even though the MacBook Pro and Dell OptiPlex might not be as vulnerable as the iPhone, they are still crucial to our operations. They are used every day to handle sensitive data and important tasks, so strong security measures are vital. We shouldn't ignore the Android Tablet either, since any weak spot could become a target for threats.

Step 3: Identify & Evaluate Threats

After assessing our vulnerabilities—albeit tentatively—the next stage is to look into the various threats that could exploit these weaknesses. Threats can come in multiple forms and from different directions. Ignoring this diversity would compromise the integrity of our entire risk assessment.

Categories of Threats

Cyberattacks: This umbrella term covers the variety of methods cybercriminals use to compromise data and systems. Common attacks include phishing, ransomware, and DDoS attacks.

Insider Threats: Sometimes the danger is internal. An employee might inadvertently expose data or intentionally misuse it, posing a threat that's harder to predict and prevent.

Social Engineering: These attacks are aimed not at your technology but at your people. By manipulating staff into revealing confidential information, attackers can bypass even the most robust security measures.

Physical Breaches: Threats are not always virtual. Physical access to servers or workstations can also cause immense damage.

Hardware Failures: Though not a deliberate attack, the threat of hardware malfunctioning, leading to data loss or system unavailability, should not be overlooked.

Evaluating the Likelihood

Understanding the probability of a particular threat exploiting a known vulnerability is crucial. Likelihood can be assessed through past incidents, general statistics, or even educated guesses. For example, if your database server has a known vulnerability, and data breaches are common in your industry, the likelihood is high.

Cross-Referencing Threats to Vulnerabilities

We also need to match each threat to the vulnerabilities we previously identified. For example, if we find that our app-server has a poorly configured firewall, the threat of a cyberattack exploiting this particular weakness becomes increasingly probable.

Documentation

Accurate and comprehensive documentation of potential threats is invaluable. The utility of our risk assessment hinges on the quality of our data. Each threat should be documented, detailing its potential origin, the vulnerabilities it could exploit, and its estimated likelihood.

Scoring Our Sample Data

For our initial assessment, we'll proceed by assigning tentative scores.

The API Keys, stored on the Ubuntu VM, are top targets. If these keys were to be compromised, they could grant unauthorized access to critical platforms, pushing their threat scores upwards.

Salesforce manages our Customer Data and might be secure on its own, but the potential misuse of API keys heightens its vulnerability. Still, an encrypted backup on the db-server acts as a safeguard, resulting in a balanced threat score.

Our Email Subscriber info is in Mailchimp, but it's accessed from devices like the iPhone 13 and an old Android Tablet. This raises its threat score.

The high vulnerability score for Employee Payroll indicates that it's not just about the direct access through platforms like ADP Workforce Now. If the API keys, which may also access ADP, are not securely managed, then this critical data is at heightened risk.

The connections between our data, software, and hardware should play a significant role in these evaluations.

You can see the final threat scores, along with the vulnerability scores from Step 3, in Figures 3.1 to 3.3.

Data	Vulnerability	Threat
API Keys	0.9	0.9
Customer Data	0.7	0.4
Email Subscribers	0.6	0.6
Employee Payroll	0.9	0.7

Figure 3.1: Data assets with vulnerability and threat scores

Hardware Asset	Vulnerability	Threat
Dell OptiPlex	0.5	0.5
MacBook Pro	0.5	0.4
iPhone 13	0.7	0.6
Android Tablet	0.4	0.4

Figure 3.2: Hardware assets with vulnerability and threat scores

Software	Vulnerability	Threat
Ubuntu 22.04.3 VM	0.9	0.9
Salesforce	0.7	0.5
QuickBooks	0.8	0.6
Mailchimp	0.5	0.6
ADP Workforce Now	0.8	0.7

Figure 3.3: Software assets with vulnerability and threat scores

Step 4: Calculate Impact

The next critical step is calculating the impact of the threat-vulnerability pairs we've documented in the previous two steps. This stage allows us to quantify the consequences, generally in terms of financial loss, data compromise, or operational downtime, that may occur if a specific threat exploits a given vulnerability.

Let's consider some impact metrics:

Financial Costs: The direct financial loss due to a data breach, or costs incurred for recovery and system hardening.

Operational Downtime: The time your systems or services will be unavailable, disrupting your business operations.

Data Loss: The loss or unauthorized alteration of confidential and mission-critical data.

Reputation Damage: Although difficult to quantify, damage to your brand's reputation can have a lasting impact on customer trust and market share.

To do this more accurately, we should consider historical data, if it exists, as it provides valuable context. But if we lack that data, we can make educated estimates using industry comparisons. This involves examining how similar incidents impacted other organizations in terms of financial, operational, and reputational costs. By analyzing the repercussions faced by similar businesses, we can better anticipate potential outcomes in our own.

Moreover, it would be helpful to involve key stakeholders from different departments. The IT team may focus on data loss and system downtime, whereas the marketing team might be more concerned about brand reputation. We should include these perspectives to get a rounded view.

To facilitate this process, we can use the Impact Assessment Questionnaire on the next page. After reading through it carefully, we'll discuss how to assign impact scores to our various sample assets.

Impact Assessment Questionnaire

Data Assets

- How would the loss of this data affect operations?
- What legal consequences could arise from losing this data?
- Would a data breach result in reputational damage?

Software Assets

- How critical is this software to operations?
- Would compromise of this software lead to financial losses?
- What would be the downtime if this software fails?

Hardware Assets

- What is the cost to replace this hardware?
- How long to restore normal operations if this hardware fails?
- Does this hardware host sensitive data?

Network Assets

- How would a network failure impact daily operations?
- What is the risk of unauthorized remote access?
- Would a network compromise lead to loss of essential systems?

Personnel

- How dependent is the business on key personnel?
- What would be the impact of losing key personnel?

Business Processes

- How critical is this process to business continuity?
- What are the financial repercussions of a failure in this process?

General Questions

- What is the overall financial impact of a major security breach?
- How resilient is the organization to a major cyber incident?
- What is the likely reputational impact of a significant cybersecurity incident?
- Are there any third-party risks or dependencies that could increase impact?

The impact assessment questionnaire includes targeted questions about data, software, hardware, network assets, personnel, and business processes, aiming to assess operational, legal, financial, and reputational consequences. It can help us pinpoint the specific areas where a security incident could have the most significant impact.

Scoring Our Sample Data

The impacts of our sample assets being compromised vary in severity.

Starting with digital keys, our API Keys have the highest vulnerability, threat, and impact scores, all at 0.9. They act as access points to various systems, and a breach can lead to significant disruptions. Similarly, the Ubuntu 22.04.3 VM stands tall with scores of 0.9, serving as the foundation for many operations.

Salesforce, holding our customer data, has an impact score of 0.7. This data is vital, and a breach could disrupt operations and damage trust. The Email Subscribers data, crucial for communication, comes in with a 0.5 impact score, indicating its importance. Employee Payroll data, with an impact score of 0.8, underlines the severe consequences of its exposure.

On our hardware list, both the Dell OptiPlex and MacBook Pro have a score of 0.5, highlighting their importance in daily tasks. The iPhone 13, with a slightly higher score of 0.6, is used for broader functions, while the less frequently used Android Tablet has a lower impact score of 0.3.

Turning our attention to software, QuickBooks, which manages our financial data, sits at an impact score of 0.7, emphasizing its crucial role. Mailchimp, our bridge to Email Subscribers, holds a score of 0.5, while ADP Workforce Now, crucial for employee data management, stands strong with an impact score of 0.8.

Figures 4.1 to 4.3 show our final set of scores.

Data	Vulnerability	Threat	Impact
API Keys	0.9	0.9	0.9
Customer Data	0.7	0.4	0.7
Email Subscribers	0.6	0.6	0.5
Employee Payroll	0.9	0.7	0.8

Figure 4.1: Data assets with vulnerability, threat, and impact scores

Hardware Asset	Vulnerability	Threat	Impact
Dell OptiPlex	0.5	0.5	0.5
MacBook Pro	0.5	0.4	0.5
iPhone 13	0.7	0.6	0.6
Android Tablet	0.4	0.4	0.3

Figure 4.2: Hardware assets with vulnerability, threat, and impact scores

Software	Vulnerability	Threat	Impact
Ubuntu 22.04.3 VM	0.9	0.9	0.9
Salesforce	0.7	0.5	0.6
QuickBooks	0.8	0.6	0.7
Mailchimp	0.5	0.6	0.5
ADP Workforce Now	0.8	0.7	0.8

Figure 4.3: Software assets with vulnerability, threat, and impact scores

Step 5: Calculate Risk

At last, we've arrived at the final step of our assessment. This is where we tie together all the individual pieces we've analyzed in the preceding sections to get a broad overview of our overall risk profile.

One way to do this would be to assign weights to vulnerability, threat, and impact, and then sum the weighted values to obtain a weighted average for each of our assets:

This approach allows us to emphasize or de-emphasize specific components based on the context and importance in the risk assessment process. For example, if we were in the early stages of implementing a security framework, we could prioritize 'vulnerabilities' by increasing how much vulnerability scores contribute to the total.

In mathematical terms, the weights for vulnerabilities (V), threats (T), and impacts (I), can be expressed as:

$$w_V = 0.4, w_T = 0.3, w_I = 0.3$$

Then we can express our equation as a sum of the product of these variables with our corresponding scores V, T, and I:

$$(V \times w_V) + (T \times w_T) + (I \times w_I) = R$$

The risk value R derived from this formula will be a value between 0 and 1, since V, T, and I are all between 0 and 1 as well. For example, using the values for Customer Data we get:

$$(0.7 \times 0.4) + (0.4 \times 0.3) + (0.7 \times 0.3) = 0.61$$

Applying this formula to the rest of our example data gives us the results on Figures 5.1 to 5.3.

Data	Vulnerability	Threat	Impact	Risk
API Keys	0.9	0.9	0.9	**0.90**
Customer Data	0.7	0.4	0.7	**0.61**
Email Subscribers	0.6	0.6	0.5	**0.57**
Employee Payroll	0.9	0.7	0.8	**0.81**

Figure 5.1: Data assets with vulnerability, threat, impact, and risk scores

Hardware	Vulnerability	Threat	Impact	Risk
Dell OptiPlex	0.5	0.5	0.5	**0.50**
MacBook Pro	0.5	0.4	0.5	**0.47**
iPhone 13	0.7	0.6	0.6	**0.64**
Android Tablet	0.4	0.4	0.3	**0.37**

Figure 5.2: Hardware assets with vulnerability, threat, impact, and risk scores

Software	Vulnerability	Threat	Impact	Risk
Ubuntu 22.04.3 VM	0.9	0.9	0.9	**0.90**
Salesforce	0.7	0.5	0.6	**0.61**
QuickBooks	0.8	0.6	0.7	**0.71**
Mailchimp	0.5	0.6	0.5	**0.53**
ADP Workforce Now	0.8	0.7	0.8	**0.77**

Figure 5.3: Software assets with vulnerability, threat, impact, and risk scores

Final Analysis

Our assets present a spectrum of risk scores, evident upon examining the various categories.

For data assets (Figure 5.1), the API Keys are most at risk with a score of 0.9, demonstrating their critical nature. Employee Payroll follows closely at 0.82, emphasizing the consequences of any breach. Customers and Email Subscribers have respective scores of 0.61 and 0.56, showcasing their importance.

In the software category (Figure 5.2), ADP Workforce Now holds the highest risk at 0.77. QuickBooks isn't far behind with a 0.73 score. Salesforce and Mailchimp have more balanced risks at 0.62 and 0.53, respectively.

Shifting to hardware (Figure 5.3), the iPhone 13 stands out with a score of 0.64, reflecting its broader use. The Dell OptiPlex and MacBook Pro have scores of 0.5 and 0.47, respectively. The Android Tablet, with a 0.37 score, remains on the lower end.

It's essential to understand the interplay between assets. For instance, a breach involving the API Keys could have ripple effects on other assets. A tool with a moderate risk score can become riskier if combined with a high-risk asset. This dynamic emphasizes the need to consider both quantitative values and real-world implications when evaluating risks.

Methodology Limitations

It bears repeating that the approach taken in this guide, while a useful conceptual framework, should only serve as an initial baseline rather than an definitive method for risk assessment. Let's see why next.

Qualitative Nature: we're using are largely based on qualitative measures, which could lead to subjective interpretations. For instance, "How critical is this software to operations?" could be interpreted differently by different personnel.

Granularity: the questionnaires capture a breadth of security domains, but lack depth in specific areas, like the nuances of encryption methods.

Adaptability to Change: we focused primarily on current known risks and might not be effectively accounting for evolving threats, unseen vulnerabilities, leading to potential blind spots.

False Positives and Negatives: answering the questions affirmatively doesn't ensure complete safety, while negative responses don't necessarily equate to high risk. For example, MFA might be enabled, but if it's not regularly tested, it could be ineffective.

Operational Context: while the questionnaires aim to understand context, they don't capture the full complexity of specific operational scenarios, leading to potential gaps in the assessment.

Dependency on Accurate Reporting: the validity of the risk scores is highly dependent on the accuracy and honesty of the questionnaire responses. There's room for human error or bias.

Complexity of Interactions: while the threat scores consider interactions between assets, they might not fully account for the intricacies of these interactions or the cumulative risk they could introduce.

Incident Response Limitations: while response plans are queried, the effectiveness, readiness, and regular testing of these plans aren't deeply analized.

Lack of Continuous Monitoring: risk isn't a static measure. The current methodology provides a snapshot but doesn't account for the dynamic nature of cybersecurity risks.

Understanding the limitations of our methodologies is just as important as recognizing their strengths and potential benefits. This balanced perspective ensures that we make informed decisions and continually refine our approach for optimal results.

With that in mind, our approach, while not perfect, has still yielded valuable insights. So, let's now take look at what we can do next.

Translating Risks into Actionable Steps

After conducting an initial assessment, it's imperative to translate the findings into actionable steps. Assessments uncover potential vulnerabilities and risks, but strategizing will help prioritize and mitigate those risks effectively.

Begin by categorizing and ranking the risks identified. Those with the highest potential impact and likelihood should be addressed first. For example, in our sample data, the API Keys had a notably high risk score, suggesting they need immediate attention.

Based on the risk rankings, apply tailored security measures. It's more effective to use targeted solutions rather than generic ones. Referring to our sample, the iPhone 13, due to its higher risk score, might benefit from enhanced mobile device security such as biometric locks.

It's vital to educate all stakeholders, particularly employees, on the risks and implemented safeguards. This goes beyond mere top-down instructions. Handling confidential customer data requires comprehensive training for all staff to protect it.

Cyber security is a dynamic field. New vulnerabilities emerge, and old ones can become obsolete. Therefore, periodic reassessment of the cyber landscape is necessary to stay ahead. For instance, tools such as Salesforce, QuickBooks, and Mailchimp in our sample had varying risk scores, suggesting they may need different update frequencies and security considerations.

Taking action post-assessment is about being proactive rather than reactive. By understanding the vulnerabilities, prioritizing them, and addressing each with a targeted approach, a robust cyber security strategy can be crafted and maintained.

Security Recommendations Checklist

1. Adopt Secure Secret Management:

- [ ] Transition to trusted services like Google's Workforce Identity or HashiCorp Vault for API keys.
- [ ] Restrict and log access to essential personnel.

2. Enhanced Mobile Device Security:

- [ ] Implement biometric locks on mobile devices, particularly the iPhone 13 due to its high risk score.
- [ ] Regularly update mobile OS and applications.

3. Employee Training and Awareness:

- [ ] Conduct security training, underscoring the importance of data like Customer Contacts and Employee Payroll.
- [ ] Update staff on current threats and mitigation best practices.

4. Software Security Updates:

- [ ] Consistently update tools, including Salesforce, QuickBooks, Mailchimp, and ADP Workforce Now.
- [ ] If needed, consider more secure software alternatives.

5. Hardware Security Protocols:

- [ ] Install updates for anti-malware and firewalls on devices like the Dell OptiPlex and MacBook Pro.
- [ ] Control physical access to vital hardware.

6. Centralized Access Management:

- [ ] Introduce a centralized access system to regulate data and software access.
- [ ] Regularly review and audit access logs.

7. Backup and Recovery:

- [ ] Establish routine backups for essential data and store them securely.
- [ ] Periodically test recovery processes.

8. Vet Third-Party Providers:

- [ ] Assess security protocols of third-party providers associated with high-risk assets.
- [ ] Ensure their adherence to strict security benchmarks.

Conclusion

We've looked at a lot of risks in this eBook, but there's still much more to explore. It's a bit like patching up the big holes in a boat but not checking it all over for smaller ones.

That's where the Digital Standards we mentioned earlier come in. They're comprehensive guidelines ensuring our online securitye. By using them, we can catch any issues we might have missed. This not only helps keep our data safe but also builds trust with the people we work with. It's really worth taking the time to understand these standards and check that we're doing things right.

For those wanting to dig deeper, there are a variety of open-source assessment tools available. Tools like OpenVAS, Security Onion, and ZAP offer in-depth scans and insights that can further strengthen our cybersecurity measures. They're valuable resources for those looking to take a more hands-on approach.

But diving deep into that is a topic for another time. The topic of cybersecurity is vast and constantly evolving with new challenges and solutions.

I hope for now this eBook has given you a good starting point. Be sure to check out the various resources on the next page, as well as the short glossary at the end.

Get in touch at rogueninja.com/contact

Resources

Digital Standards

CAN/CIOSC 104: 2021, Baseline Cyber Security Controls for Small and Medium Organizations

CAN/DGSI 103-1, Digital Trust & Identity – Part 1: Fundamentals

ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection

Automated Scanning Tools

Vulnerability Scanners: Use tools like Nessus or OpenVAS to automatically scan for vulnerabilities in your network.

Web Application Scanners: If you have web applications, use tools like ZAP to find vulnerabilities.

Code Review Tools: Use automated solutions like SonarQube to scan your codebase for vulnerabilities.

Monitoring

Intrusion Detection Systems (IDS): Install an IDS like Snort, Suricata , or Security Onion to monitor network traffic for suspicious activity.

Log Management: Implement centralized log management solutions like ELK Stack to track security events.

Excel Workbooks

Risk Assessment Inventory

Glossary

API Key: A code passed in by computer programs to identify the calling program to the website.

Authentication: A process by which a computer, system, or application confirms the identity of a user.

Backup: A copy of data that can be used to restore and recover that data.

Cybersecurity: The practice of protecting systems, networks, and programs from digital attacks.

Data Breach: A security incident in which information is accessed without authorization.

Data Encryption: The process of converting data into a code to prevent unauthorized access.

Digital Assets: Digital content owned by an individual or organization, including text, graphics, audio, video, etc.

Digital Standards: Set guidelines or best practices that ensure security and interoperability in the digital realm.

Encryption Key: A piece of information used to control the cryptographic process, turning plain text into cipher text and vice versa.

Endpoint Security: The process of securing endpoints or entry points of end-user devices.

Firewall: A network security device that monitors and filters incoming and outgoing network traffic based on security policies.

Impact Assessment: A tool or methodology to predict the impact of changes in the current environment.

Incident Response Plan: A strategy for handling and responding to a security breach or cyberattack.

Infrastructure: The fundamental framework of systems and structures for an organization or system.

ISO 27001: A globally recognized standard for the establishment, maintenance, and certification of an information security management system (ISMS).

Malware: Software specifically designed to harm or exploit any device, service, or network.

Operational Diligence: The thorough and detailed process of ensuring that all operations, especially those related to security, are carried out accurately and effectively.

Patch: A piece of software designed to fix or improve a computer program or its supporting data.

PIPEDA: The Personal Information Protection and Electronic Documents Act, a Canadian privacy law.

Risk Analysis: The process of identifying, assessing, and prioritizing potential threats or vulnerabilities.

Risk Score: A quantitative measure of the risk associated with a particular asset, usually calculated using various metrics and data points.

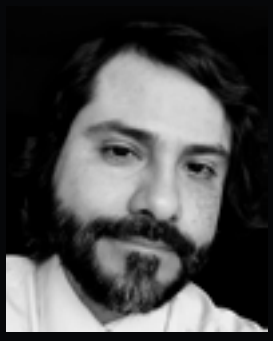
Threat Surface: All the different points where an unauthorized user can try to enter data to or extract data from an environment.

Two-Factor Authentication (2FA): An authentication method where a user is granted access after presenting two separate pieces of evidence to an authentication mechanism.

Vulnerability: A weakness in a system or network that can be exploited by threats to gain unauthorized access.

Zero-Day Vulnerability: A software vulnerability that is unknown to the software maker and has no patches or solutions available from vendor.

About the Author



Mike Figueroa is a full-stack developer based in New Westminster, British Columbia, with over a decade experience in cloud application development. Mike's coding journey spans a variety of languages, from JavaScript to C#, and includes projects like client websites, training management systems, and interactive games.

He also brings to the table a wealth of experience in corporate learning and development. As facilitator and training manager for three provinces, Mike spent over eight years molding minds and fostering growth at one of Canada's leading companies.

Currently, Mike is busy running rogueninja.com and working with amazing clients on exciting new projects.