SECURITY REPORT

RIHAM AHAMED ABDUL RAHEEM
HND COMPUTING IDM

Contents

Introduction

UniCare is a leading insurance company with its roots entrenched deeply all around Sri Lanka with 5 Branches Island wide. As the company's primary goal has become to spread its influence more due to higher customer demand and several other factors, within this journey the security risks, threats, protection acts and how to protect UniCare will be documented in this report.

The primary scope of this document will be to specifically identify what risks and threats the company will face, what regulations and protection acts are expected to be made, how ISO 31000: Risk Management can be utilized, the impact of an IT security audit on the security of the company and what responsibilities and tasks employees must follow in order to ensure the safety and security of information within the company.

All information stated here is backed by research, properly evaluated and have been extracted from information grounds with sole purpose of research and reporting as such therefore will not be used to make any profit or claims to the information or materials used unless claimed by the writer himself.

IT Security

In today's world, data and protecting that data are critical considerations for businesses. Customers want to ensure that their information is secure with you, and if you can't keep it safe, you will lose their business.

Many clients with sensitive information actually demand that you have a rigid data security infrastructure in place before doing business with UniCare. With that consideration as the backdrop, how confident can the company be when it comes to the organization's IT security?

In order to have a strong handle on data security issues that may potentially impact your business, it is imperative to understand the relationship and differences of three central components – Threat, Vulnerability and Risk.

Frequently these technical terms are used interchangeably, but although related, they are distinct terms with different meanings and implications.

Identification of risks

A risk refers to the potential for loss or damage when a threat exploits vulnerability. Examples of risk include financial losses as a result of business disruption, loss of privacy, reputational damage, and legal implications and can even include loss of life. (Watts, 2020)

Risk Assessment

- **Identify Hazards:**

  This step consists of simply listing which business risks a particular company might face. These could include acts of nature, fires, mechanical breakdowns, and even cyber-attacks.

- **Identify assets that could be at risk:**

  This step consists of identifying which business or external assets might be damaged by one of the hazards listed above. Some common examples are employees, customers, buildings, a business's reputation, and the environment.

- **Analyze the impact:**

  The last step consists of figuring out what sort of harm could be done to the company assets.

After analyzing all of these reports, whoever acts as the company's risk manager can try to mitigate each risk.

For example, a safety program, smoke detectors, and fire extinguishers might reduce the risk of accidental fires. Better security could reduce the chance that hackers can steal valuable data.

Of course, no company can take steps to totally eliminate every threat, but these are examples of good first steps.

Next, this assessment will help companies buy the right insurance to protect them against the things that they cannot control.

The more steps that companies do take to minimize threats, the cheaper that insurance premiums are likely to be. Risks assessments and impact analysis can help prevent losses and result in lower insurance premiums. (Watts, 2020)

How can UniCare mitigate risks

You can reduce the potential for risk by creating and implementing a risk management plan. Here are the key aspects to consider when developing your risk management strategy:

- **Assess risk and determine needs:**
  When it comes to designing and implementing a risk assessment framework, it is critical to prioritize the most important breaches that need to be addressed
- **Include a total stakeholder perspective:**
  Stakeholders include the business owners as well as employees, customers and even vendors. All of these players have the potential to negatively impact the organization (potential threats) but at the same time they can be assets in helping to mitigate risk.
- **Designate a central group of employees:**
  who are responsible for risk management and determine the appropriate funding level for this activity.
- **Implement appropriate policies** and related controls and ensure that the appropriate end users are informed of any and all changes.
- **Monitor and evaluate policy and control effectiveness:**
  The sources of risk are ever-changing which means your team must be prepared to make any necessary adjustments to the framework. This can also involve incorporating new monitoring tools and techniques.

Identification of threats

A threat refers to a new or newly discovered incident with the potential to do harm to a system or your overall organization.

There are three main types of threats

1. Natural threats.
2. Unintentional threats
3. Intentional threats.

There are many examples of intentional threats including spyware, malware, adware companies or the actions of a disgruntled employee.

In addition, worms and viruses are also categorized as threats, because they could potentially cause harm to your organization through exposure to an automated attack, as opposed to one perpetrated by humans.

Although these threats are generally outside of one's control and difficult to identify in advance, it is essential to take appropriate measures to assess threats regularly.

Here are some ways to do so:

- Ensure that your team members are staying informed of current trends in cybersecurity so they can quickly identify new threats.
- They should subscribe to blogs (like Wired) and podcasts (like Techgenix Extreme IT) that cover these issues as well as join professional associations so they can benefit from breaking news feeds, conferences and webinars.
- You should also perform regular threat assessments to determine the best approaches to protecting a system against a specific threat, along with assessing different types of threats.
- Penetration testing involves modeling real-world threats in order to discover vulnerabilities.

Top threats to a business of Unicare's scale

1. Employee Negligence

Possibly the biggest positive impact to securing your critical data can be employee awareness training for modern security threats. Opening malicious attachments, clicking dangerous advertising links and weak passwords all pose commonly exploited risks.

Conduct security training at the time of hire, regular company-wide training, and attack simulation. Require regular password changes and enable two-factor authentication for additional security.

2. Malware

Your employee training should conform to a strict security policy which you've created in advance.

But unsupported operating systems, unauthorized software and inadequate patch management also create ripe opportunity for malicious code to take hold. Automatically update and patch your systems.

3. Bring-Your-Own-Device

More and more employees are bringing their own devices to work where they are storing important data. Are these devices under the control of your Systems Admin? A BYOD policy which includes, encryption and remote backup is critical.

4. Lack of a System Admin

Businesses often struggle with both security budget, and numerous shared responsibilities among employees. This can mean that suspicious activity or breaches may be taking place on the network, and nobody is monitoring these events.

Whether it is a single body or multiple people managing the IT at your business – make it clear who must be aware of new threats and implement as well as enforce safeguards.

5. Ineffective Disaster Recovery Plan

Sure, most businesses are backing up some data in some form or another. But does this mean that there is a clear plan of action in the event of catastrophic data loss?

What is the level of confidence that you can get back to "business as usual" within a reasonable time frame.

6. Unlimited Access

Many businesses seem to are either unaware or don't understand the danger of giving all employees unlimited access to data. Access should be restricted to the minimum required for them to function in their position. Understand where the most sensitive data is kept, and how it is accessed by which specific employees.

Data Protection Act

The Data Protection Act (1998) is a UK law that governs the processing and handling of personal information. The main purpose of the Data Protection Act is to protect individuals from having their personal details misused or mishandled. The Data Protection Act does this in two ways:

- By establishing rights for individuals
- By creating responsibilities for businesses, organisations, and the government and setting guidelines for the way they handle and store 'personal data'.

The 8 Core Principles of DPA

1. Processed fairly and lawfully
2. Processed only for specified, lawful, and compatible purposes
3. Adequate, relevant, and not excessive for the intended purposes
4. Accurate and up-to-date – individuals have the right to have inaccurate personal data corrected or destroyed
5. Kept for no longer than necessary
6. Processed in line with the rights of the individuals
7. Secured against accidental loss, destruction, or damage against unauthorized or unlawful processing
8. Not transferred outside the European Economic Area (EEA) unless there is adequate protection.

UniCare should establish a data protection policy in your business to ensure your legal obligations are met.

The policy should take into account the particular personal data needs of the business as well as the way it processes this information. The policy should also address areas where personal and sensitive data might inadvertently leak in contravention of your obligation under the law. (James, 2020)

It is of UniCare's safety that a policy like such should be implemented as:

- Keeping the information you have about your customers secure will help protect your and their information;
- Sending out a mailing from incorrect or out-of-date records could not only annoy your customers but also wastes your time and money;
- Good information handling can improve your business's reputation by increasing customer and employee confidence in you;
- Good information handling should also reduce the risk of a complaint being made against you.

IT Security Audit

An IT security audit involves an IT specialist examining an organization's existing IT infrastructure to identify the strength of its current security arrangements and pinpoint any potential vulnerability.

Using specialist tools to gather data from the various systems that a business uses to carry out their digital day-to-day tasks, whomever is carrying out the audit will conclude by putting together an in-depth report that covers the aspects where the infrastructure is strong and where it is perhaps more vulnerable.

How an IT Security Audit is performed and what impact it has:

This is followed up with a number of recommendations to bolster the business' network security arrangements, with tasks identified to be carried out in the short, medium and long term.

A large enterprise may have its own internal audit team; if not, then employees nominated to perform the audit will need some formal training and must be cleared to have access to any sensitive locations or data covered by the audit.

Obviously, for the audit to be impartial, the people involved must be independent from the business unit being audited.

To further minimize disruption and the resources required, self-assessment audits are best conducted in two stages:

- Adequacy audit: a document-based review of the adequacy of policies and procedures for protecting data and managing information risk.
- Compliance audit: an evidence-based assessment of the implementation and effectiveness of the policies and procedures.

By conducting an adequacy audit first, much of the work can be completed off-site and recommendations for corrective actions to address shortcomings can be completed prior to the start of the compliance audit.

There is no point checking if a unit or system is compliant if there aren't sufficient documented policies and procedures already in place for it to adhere to.

All documents should be fit for purpose.

On the other hand, poorly written policies, where scope, responsibilities or requirements aren't crystal clear, can be given the benefit of the doubt as long as they are flagged as a minor non-compliance or observation in the audit report.

Once the adequacy audit is completed satisfactorily, then the compliance audit can begin.

This mainly involves questioning the key stakeholders identified in the audit plan.

If serious problems are identified during this stage of the audit, a corrective action plan should be drawn up so they can be tackled without having to wait for the full report, where they should appear as non-compliances.

Ideally, an audit should assess compliance with every mandatory measure in scope.

In many instances, this isn’t going to be realistic, in which case, audits should focus on higher-risk areas: a single location, business unit, system, application or project.

If the workload is still too much given your resources, consider sampling, focusing on the key security controls.

Auditing is an iterative process for assessing compliance and supporting continued improvement.

Future audits should obviously cover areas that have not been sampled or have previously been identified as weak, and where hardware, software, policies or procedures have changed.

The real benefits come from implementing an audit's recommendations and dealing with any reported concerns.

Use the current level of compliance as a benchmark to be improved upon ahead of formal and third-party reviews. This type of goal setting will help to promote a culture of continuous review and improvement.

References

James, A., 2020. *Hutsix.* [Online]
Available at: https://www.hutsix.io/what-are-the-eight-principles-of-the-data-protection-act/
[Accessed 29 March 2021].

Watts, S., 2020. *bmcblogs.* [Online]
Available at: IT Security Vulnerability vs Threat vs Risk: What are the Differences?
[Accessed 2021].

Watts, S., 2020. *bmcblogs.* [Online]
Available at: IT Security Vulnerability vs Threat vs Risk: What are the Differences?
[Accessed 29 March 2021].