certnz

Cyber security **risk assessments** for business

A cyber security risk assessment will help you understand both your business processes, and the systems and data it's important to secure. Knowing your risks can help you prevent — or recover from — a cyber security incident.

1. Know your systems and data ///

Make sure you understand your business processes, and how your systems and data fit into them.

Document the systems and data that support your business processes. Focus on the business processes that are most important to you.

That means the systems that are critical to your business running, and the systems that store your data.

Your systems will be:

- **internal** — those you host, manage, and are responsible for
- **external** — those you access through a web browser, including those managed by a third party.

Your data will include:

- **personal** data (like employee and customer data)
- **financial** data, and
- **intellectual** property.

Example

Accounting and invoicing is an important business process. If you manage this inhouse, you could be using either:

- an **internal** application, like Quickbooks, where data is stored on your on-premise server, or
- an **external** application, like Xero, where data is stored on Xero's servers.

The data stored by these systems is **financial** and **personal** data.

2. Identify threats and vulnerabilities ///

Work out who may want to access your systems and data, and how vulnerable or exposed they are.

Think about who may want to access your systems and data, and the **threats** they face. How easily accessible are the systems and how valuable is the data?

Then, consider how **vulnerable** or exposed the systems and data are. If they're exposed to the internet, or only require basic authentication to access, they'll be more vulnerable to attack.

Consider hiring an IT security professional to help you document threats and vulnerabilities to make sure you don't miss anything.

Remember that not all threats are malicious. A mistake made by an employee can be a threat too.

Example

Your web server has to be accessible over the internet to host your website. The threat of an untargeted attack against it is quite likely, if:

- your IT team leaves a remote access port on the application server exposed to the internet, and
- it only uses basic authentication (username + password).

An attacker could use automated tools to guess your login details and gain access to it without your knowledge.

3. Determine risks ///

When you've identified threats and vulnerabilities, determine the risk each one presents.

A risk is an event caused by a threat and a vulnerability.

There are three different types of security risks. There's:

- **confidentiality** risks —when your system or data is no longer secret.
- **integrity** risks — when your system or data is no longer accurate or correct.
- **availability** risks — when your systems or data are unavailable.

Risk is always going to be a trade-off. Some risks you have to accept, and some you can manage so the risk is not as high. Identifying your key risks is an important first step in finding the right strategy to manage them.

Privacy risks are sometimes considered in a risk assessment. Privacy of personal data, like your customers' details, is a type of confidentiality risk.

Example

If an attacker was able to access your web mail, they could use it to:

- collect sensitive business information, which is a **confidentiality** risk
- direct your clients to make payments into their bank account instead of yours, which is an **integrity** risk.

4. Define the impacts ///

Document the impact of the risks — how they'd affect your business if they happened.

Categorise the type of impact each risk would have.

- **Operational** — how would the risk affect your day to day operations?
- **Reputational** — what would people think of you if the risk happened?
- **Financial** — how much would it cost to recover from the risk?
- **Technical** — how would the risk affect your network or IT environment?

Then, give each one a rating of low, medium or high impact.

This will help you set a risk management strategy and plan for controlling them.

Example

- If an attacker got access to your customer email data and leaked it, it would have a high **reputational** impact on your business.
- If you had a printing company and an attacker brought down the server that runs the printing software, it would have an **operational** impact on the business.

5. Implement controls ///

Define controls that will help prevent, or mitigate, your business risks.

Decide which risks you can:

- **control**, by bringing the risk rating down
- **transfer**, by getting a third party to manage them for you
- **remove**, by shutting down the system at risk, or by not collecting the data at risk
- **accept**, if you can't remove them entirely.

As a business owner, risks are always your responsibility — even if a third party manages them for you.

When you've worked out controls to implement:

- put your mitigation plan in place to prevent the risks happening
- talk to your staff about the risks the business faces, and what they can do to keep it secure
- create an incident response plan so you know what to do in the event of an attack.

Example

If you have a payment system that collects personal data from your customers, you could shut it down and process payments through a third party like Paypal instead.

That **transfers** the risk of the data being compromised to them, without impacting your business or your customers.

Make sure your staff and any third parties you deal with understand your business risks and controls too. And, review your risk assessment regularly — risks can change over time.