Article

May 2023

Cyber Security Preparedness: 8 Questions Your Organisation Must Answer

From identifying critical systems and data assets, to having business continuity and disaster recovery plans, to understanding legislative obligations for reporting cyber security incidents, we will cover it all.

Charlie Hales
Managing Director, Australia

Email charlie.hales@waterstons.com
Linkedin https://www.linkedin.com/in/charliehales/

With the increasing frequency and sophistication of cyber-attacks, it can be overwhelming to know where to begin in terms of protecting your organization.

The good news is that we have done the work for you. In this article, we will provide you with a breakdown of the 8 essential questions that your organization should be asking to not only respond to a cyber-attack, but also to prepare for it.

From identifying critical systems and data assets, to having business continuity and disaster recovery plans, to understanding legislative obligations for reporting cyber security incidents, we will cover it all.

By asking these questions, you will gain valuable insight into your organization's current level of cyber security preparedness and identify areas that require improvement. Implementing the necessary measures and protocols to address any vulnerabilities can help safeguard your business from potential cyber threats and ensure the continuity of your operations.

So, whether you are a small business owner or a Fortune 500 executive, this article will provide you with the knowledge and tools necessary to develop a comprehensive cyber security plan.

What Data Do We Hold?

Failing to identify the critical data assets that require protection can leave your organization vulnerable to potential cyber-attacks. Knowing what data your business holds is the key to implementing effective cyber security measures.

By conducting a thorough analysis of your organization's systems and data assets, you can determine which areas require the most protection. This could include sensitive customer information, financial records, or intellectual property. Once identified, you can prioritize your cyber security efforts and allocate resources accordingly.

What Does Our Cyber Plan Currently Look Like?

Having a cyber plan in place is essential to protect your organization from the increasing threats of cyber attacks. However, it's important to understand that cyber security is not just the responsibility of the IT department, but of the entire organization. It involves a collaborative effort from all employees, as well as implementing the right processes and technology to ensure a strong security posture.

To evaluate where you're at on your cyber journey, it's important to take a holistic approach and assess not just your technology but your people and processes as well. This means analysing your employees' knowledge of cyber security, identifying potential weaknesses in your processes, and assessing the effectiveness of your current technology solutions.

Implementing a cyber security plan isn't an option anymore, it's a necessity to an organisations protection.

Do We Have an Up-To-Date and Regularly Tested Incident Response Plan?

Having an up-to-date and regularly tested incident response plan is crucial for any organization to effectively manage and respond to cyber security incidents. Without a plan in place, an incident can quickly spiral out of control, causing significant damage to the organization's reputation, finances, and overall operations.

An incident response plan outlines the necessary steps and procedures to be followed in the event of a cyber security incident. This includes identifying the incident, containing and eradicating the threat, assessing the damage, and restoring normal business operations as quickly as possible.

It is not enough to simply have an incident response plan in place, as it must also be regularly reviewed and tested to ensure its effectiveness. Cyber threats are constantly evolving, and a plan that worked in the past may not be effective in addressing new threats. Regular testing helps to identify any weaknesses in the plan and provides an opportunity to make necessary improvements.

By having an up-to-date and regularly tested incident response plan, organizations can ensure that they are able to respond quickly and effectively to any cyber security incidents, minimizing the impact on their operations and reputation.

This also helps to demonstrate to customers, partners, and stakeholders that the organization takes cyber security seriously and has measures in place to protect their data and information.

What Is The Role of Our Service Providers & What Do They Cover?

To ensure that your organization is prepared for a cyber breach, it is important to assess the cyber security provisions of your third-party service provider agreements. If your service provider does not have the capability to detect, respond, manage and report on a cyber-attack, it might be time to re-think your agreements.

Additionally, it's important to evaluate the readiness of your internal IT team and their ability to handle a cyber-attack. Don't hesitate to ask your team about their plans and whether they have the necessary resources and expertise to respond effectively.

Finally, it can be beneficial to seek the opinion of an additional third party like a reputable cyber security organisation. These organisations can provide valuable insights into your organisation's security posture and use techniques like penetration testing to evaluate your resilience against cyber threats.

By taking these steps, you can ensure that your organization is well-prepared to respond to cyber security incidents and protect your valuable assets.

Are We Equipped To Identify Potential Cyber Security Incidents?

After going through the information in this article and conducting an evaluation within your organization, you should be able to determine your level of preparedness for potential cyber security incidents. Typically, if you're asking the question, "Are we prepared?" it's an indication that there is room for improvement in your cyber security posture.

However, don't lose hope if you find gaps in your current cyber security plan. The important thing is to start somewhere and take proactive steps towards improving your organization's cyber security resilience.

What Is The Efficiency of Our Access To Relevant Resources to Respond to Incidents?

The efficiency of access to relevant resources in response to a cyber security incident is critical to minimizing damage and reducing downtime. The ability to quickly access and utilize the appropriate resources can be the difference between a minor inconvenience and a major crisis.

To evaluate the efficiency of your access to relevant resources, it's important to consider factors such as the speed of response, the availability of resources, and the adequacy of training and support for staff involved in the incident response process.

Regularly testing your incident response plan and ensuring that all staff are familiar with their roles and responsibilities in the event of a cyber security incident can help to improve the efficiency of your access to relevant resources. Additionally, working closely with service providers and regularly reviewing service level agreements to ensure that provisions for reporting and responding to cyber security incidents are in place can also help to improve efficiency.

Ultimately, the efficiency of your access to relevant resources in response to a cyber security incident will depend on the level of preparation and planning within your organization. By regularly assessing your preparedness and addressing any vulnerabilities or gaps, you can help to ensure that your access to relevant resources is efficient and effective when it matters most.

What Are Our Legal Obligations?

Failure to comply with reporting requirements can result in hefty fines and reputational damage. It is important to understand the laws and regulations specific to your industry and location, as they may vary.

If your organization is unsure about its legal obligations for reporting cyber security incidents, it is important to seek the advice of a third-party cyber security organisation who can provide the right support for your sector.

It’s worth noting that in a post-Optus society, the Australian Government are swiftly updated, changing, integrating and implementing new fines, consequences and frameworks to keep organisations accountable.

Have We Developed A Plan for Public Communications?

A plan for public communications is crucial in the event of a cyber security incident, as it can help to manage the impact on your organization's reputation and public trust. It's important to ensure that your organization has a well thought out plan in place that includes designated spokespeople, clear messaging, and protocols for responding to inquiries from the media and other stakeholders.

If your organization hasn't yet developed a plan for public communications in the event of a cyber security incident, now is the time to do so. This plan should be written in collaboration with your public relations team and board.

When developing your plan, consider factors such as the size and scope of the incident, the type of data that may have been compromised, and the potential impact on stakeholders. Your plan should also consider any legal or regulatory requirements for reporting the incident and communicating with affected individuals.

Having trouble getting started? We can help.

info@waterstons.com.au 02 9160 8430