Advisory For Cybersecurity

What is cybersecurity?

Cybersecurity is the protection of your organization's data from both internal and external bad actors. It can refer to a collection of technologies, methods, structures, and practices used to safeguard networks, computers, programmer, and data against unwanted access or harm. Any cybersecurity plan should aim to secure data confidentiality, integrity, and availability.

There is no “silver bullet” in cybersecurity. In other words there is not one single thing that organisation need to do to prevent being compromised by adversaries. The solutions and processes for a good cybersecurity posture are multiple and it requires skilled professionals to assess the organisation’s cyber defences and provide solutions for technical controls as well as strategies and process improvements.

Recent example of a major cybersecurity breach:

***Date:****September 2022*

***Impact:****9.8 million customers*

*Cybercriminals believed to be working for a state-sponsored operation breached Optus' internal network, compromising personal information impacting up to 9.8 million customers. According to Optus CEO Kelly Bayer, the oldest records in the compromised database could date as far back as 2017.*

*Personal information included in this compromised data set includes:*

* *Names*
* *Birth dates*
* *Addresses*
* *Phone numbers*
* *Passports and driver's license numbers (in some cases*

*It’s speculated that the criminal group gained access through an unauthorized API endpoint, meaning a user/password or any other authentication method wasn't required to connect to the API...*

*Source -* [*https://www.optus.com.au/about/media-centre/media-releases/2022/09/optus-notifies-customers-of-cyberattack*](https://www.optus.com.au/about/media-centre/media-releases/2022/09/optus-notifies-customers-of-cyberattack)

User Case:

**SCENARIO:**

An executive manager at a federal contracting firm was told that a dark web auction was offering access to their firm's commercial data, including access to their corporate client’s database. After an initial assessment, the executive quickly realised that the data being ‘sold' was out of date and unrelated to any government agency clients. Although the organisation is in not in any immediate danger, this incident has raised concerns with executive management and the board.

A limited internal investigation discovered that the potential cause may have been that an employee had downloaded a malicious email attachment, thinking it was from a trustworthy source. This could have been one of the reasons but it has left doubt on whether the organisation has a good cyber posture, if their systems are protected and if their business processes are appropriate for ensuring good practices and allow for good defences against cyber-attacks.

The board decided that they need help to guide them through steps on what need to do to ensure there are improvements and overall a good cybersecurity posture for the organisation. The have assign this task to the Chief Operating Office and given her three months to come back to the board with reconditions, a strategy on cybersecurity and a roadmap towards significant improvements.

The COO has a challenge, not sure where to begin, she reached out to Deloitte group for some high level estimate on engaging a Cybersecurity advisor and was shocked on cost which they could ill afford.

Where Fortify can help

Fortify is a not-for-profit organization with cybersecurity expertise, resourced by volunteer professionals. We provided Cybersecurity advisory services at minimal, or at no cost, to assist organizations such as yours that have limited resources.

Fortify will provide a self-assessment guideline and questionnaire so you can assess your requirements in this area.

* Depending on your needs we will then assign a professional consultant whom will assess your organization and provide a roadmap toward the desired improvements
* If you require assistance with completing the questionnaire, a Fortify consultant will identify gaps with your environment and provide necessary guidance toward completion.
* Our consultant will be able will be able to assess your cybersecurity defenses based on frameworks and standards such as Essential 8 and NITS, and audit your business processes to manage risk.
* If technical solutions are required, our consultant will able to design solutions, scope project and assist you with procurement activities if required.
* Our consultant will assist you to develop a cybersecurity strategy and provide a roadmap of required improvement.
* A fortified consultant will able to assist you in meeting compliance as part of IT governance, audit and risk management, and standards.
* Our consultants will provide a post-engagement reports summarizing in detail any remediation work completed and highlighting risk factors and recommendations for security control improvements

How to engage Fortify

There are a few simple steps to follow in engaging our services

1. Go to the website: fortify.com.au
2. Register your organization
3. Read the guidelines and start to complete the self-assessment questionnaire. Please allow 50 minutes to complete the questionnaire as some areas may be complicated and require some careful thought
4. If you required assistance to complete the questionnaire, please submit a request via the “require assistance” button or go to fortify.com.au/assistance.