

How do I know if I am vulnerable, and what do I do?

The Problem

Catastrophes occur when cyber security vulnerabilities go unknown or uncontrolled. Everyone has vulnerabilities, and it's just a matter of time until someone tries to exploit one of yours. With a Cyber Vulnerability Assessment (CVA), you will gain visibility into your vulnerabilities, and a plan to quickly resolve them.

In a world where more than 146,000 *formally reported* cyber security vulnerabilities exist, security gaps are everywhere. Closing them all is an uphill battle, which becomes more complex every year as the rate of vulnerabilities sharply increases. As new vulnerabilities are discovered daily, and attackers continually enhance their tactics, performing regular CVAs will allow you to control your exposure and risk from vulnerabilities.

Consider the impact if your accounting system was breached or encrypted. What if it was your customer database or a file server with your proprietary research and documentation? More concerning, and often overlooked, are medical Internet of Things devices such as Remote Patient Monitoring (RPM) for glucose, heart rate, and blood pressure, as well as ventilators and pacemakers. The Target retailer hack, which exposed 40 million debit and credit cards, was performed through their heating/air conditioning system. Such network-connected devices can be directly attacked and disabled, or they can be leveraged to breach the computer network storing confidential information. Whether your systems are on-premise, in the cloud, or a mix of both, they must all be protected; it's your business at risk.

The Solution

- Discover your vulnerabilities through a Cyber Vulnerability Assessment
- Understand the practical risks posed to your organization
- Prioritize by risk and impact; plan remediations
- Implement change controls and execute remediations
- Repeat the process annually, at a minimum

How We Help

Working with Ardham Technologies, Pendulum will work with you to budget and implement technology solutions that will properly mitigate the identified vulnerabilities. If you haven't recently performed a Cyber Vulnerability Assessment and Penetration Test, we will. With that data, we confirm your real-world vulnerabilities and assign each of them a priority level to develop the approach and timeline.

Additionally, many risks are simply human behavior. To reduce those risks, we create new policies and provide trainings that improve the cyber awareness of your team and enable them to act as a gatekeeper to common threats.