

# CYBER INCIDENT RESPONSE: A Critical Business Function

## *I was hacked! What do I do now? How do I respond?*

If you're reading this, you probably aren't in the middle of a cybersecurity emergency. But you may be wondering, ***"I haven't been hacked ... why should I be concerned now?"***

### The Problem

Organizations are under attack in the United States every moment of every day. Size doesn't matter. IBM's 2020 Cost of a Data Breach Survey illustrates that the financial impact of cyber incidents to companies under 500 employees averaged \$2.64 million, and the impact to enterprises above 25,000 employees averaged \$5.52 million.

Clearly, successful attacks result in immense financial loss. They also halt business operations and result in lost intellectual property, compromised client information, failed confidence, and lower corporate valuations.

Combine the dire outcomes of a successful attack with the worldwide shortage of security professionals, and we all have a grim reality to face.

In our experience, there are three types of organizations:

- Those who have been breached and know it
- Those who have been breached and don't yet know it
- Those who haven't been breached yet

Which one are you?

### The Solution

How do you reduce your risk? There are a few key steps that will help you avoid most attacks and to recover quickly after an incident:

1. Implement a standardized security framework such as National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), etc. Follow the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Payment Card Industry (PCI), and other regulations.
2. Ensure you have reliable data backups, redundancy for critical systems, and an incident response plan.
3. Know who to call for help when it happens.

### How We Help

Working with Ardham Technologies, Pendulum offers audits and implementation of security frameworks and recovery solutions. Ardham has a Cyber Security Incident Response Team (CSIRT) available 24 hours a day to help when you need it most.

The CSIRT is a specialized team who can triage, isolate, mitigate, investigate, and assist in recovering your information technology systems so you can continue regular business operations. Throughout the process, the CSIRT maintains constant communication with your stakeholders to align with your business priorities.

What you can do today: Be prepared. Get an Incident Response Plan in place now. Call us now to schedule a free consultation. We'll discuss your unique issues and how we can help you create a plan or help you work through an incident.