North Star CMM
Small Business Data/Cyber Protection Awareness

Critical Information

Data or information vital to successfully accomplishing daily operations that, if compromised or obtained by bad actors, could be used to cripple/stop operations, or harm you, your employees, customers or stakeholders.

Critical Information Examples...

- Intellectual Property (IP), Market Intelligence and/or Research & Development Data
- Strategic Data *(Board Meeting Notes, Strategic Plans, Security Plans)*
- Regulated Info./Systems *(SPI, PII, PCI, HIPAA, ITAR, Sarbanes-Oxley)*
- Operational Data *(Customer Records, Employee/Payroll Information, Contracts, Accounts Receivable)*
- Contracting Data *(Controlled Unclassified Information (CUI), Federal Contract Information (FCI))*

Critical Information vs. Classified Information

Critical information and classified information are not the same thing. A lot of critical information is not classified. Information can be designated "classified" by a governing body but critical information does not need a designation to be worthy of protection. It is very possible the exposure of critical information could lead to compromised classified information.

Why Should I Protect It?

It's The Law... Every state has a cyber breach law that dictates what efforts should be taken to protect critical information and what reporting is required if a breach should occur. In addition, each business is unique and there may be additional legal/regulatory requirements depending on what type of critical information you work with and who your stakeholders may be.

Competitive Advantage... Many small businesses overlook or discount the importance of protecting critical information. Business owners that implement processes to protect critical information are in a much better position to work with government and private sector organizations that require cyber security awareness.

Your Reputation Depends On It... Being the victim of a cyber-attack can be a public relations nightmare. In many instances, businesses navigate through the physical and financial impacts of a breach only to fail due to their loss of respect and credibility in the market place.

The Domino Effect... Not protecting critical information within a business can lead to a compromise of data in other parts of the larger supply chain. Data, like networks are interconnected and a seemingly small breach of lesser value information can be just what an attacker needs to step up to the next, larger target.

It's Expensive If You Don't... Most basic procedures needed to practice good cyber awareness and protect critical information come at little or no cost. The cost of a data breach, on the other hand, can be financially devastating and in some cases, lead to the closure of the business.

What Are Common Threats To Critical Information?

Cyber Attack - Viruses, Spyware, Trojan Horses (Malicious Code), DDoS, Phishing, Ransomware, Brute Force, Social Engineering (The number and sophistication of attacks compounds daily.)

Natural Disasters - Earthquakes, Extreme Weather Events (Hurricanes, Floods, Tornadoes), Fire

Man-made Events - Terrorism, Civil Unrest, Theft, Corporate and State-Lead Espionage

AMERICA'S SBDC