CERTITUDE® SECURITY

USE CASE

EXECUTIVE DELEGATION

Bottom Line:

You don't know what you don't know. MSPs know you lack the skills to assess their performance. Services rendered in secret, without validation, are inherently suspicious. Will you be accountable for preventing harm to your business and customers?

Lesson:

Avoiding delegation mistakes is crucial to building your business and reputation.

We empower leadership teams who desire results. You can delegate cybersecurity responsibilities to competent people, who will help you make informed decisions to avoid disruption, loss, and damage.

To learn more or start a friendly dialogue, visit our website or call (614) 408-0900.

Problem Description

Background:

The act of delegating cybersecurity to your MSP is prone to problems that lead to disastrous results. Business disruption events continue to cause harm as MSPs and IT services companies fail in their duty to protect their customers. Great leaders effectively delegate responsibilities to competent people who commit to transparency and accountability.

Awareness:

Hackers are targeting MSPs and IT outsourcing businesses to attack the service providers' customers, according to a **U.S. Secret Service** alert issued June 12, 2020. Threat actors use compromised MSPs to launch cyberattacks against service provider customers. These attacks include point-of-sale (POS) system intrusions, business email compromise (BEC), and **ransomware attacks**.

Insurance company, Beazley, outlined reported incidents of their policyholders in 2019. Beazley recorded an **increasing number of ransomware incidents** that resulted from attacks on IT managed service providers (MSPs) and other service companies providing organizations with infrastructure and support services. Criminals target MSPs because of their weak security practices and unpatched networks.

Duty and Responsibility:

Leadership is compelled, due to uncertainty, to reconsider information security changes to protect their business, employees, and customers from loss. Limited capital for investing in loss prevention requires planning aligned to your current priorities supporting the future. The lack of clarity limits confidence in making critical security decisions to protect your business and reputation.

Time to Inspect:

Many executives do not **inspect what they expect**. Time constraints and limited knowledge become shortcuts and assumptions that cybersecurity and backups are correct. Without inspection and verification, failure to fulfill obligations causes business disruption. The U.S. Secret Service and Beazley made that clear.

- How do you know if you are reasonably secure?
- Do you cross your fingers and hope that today is not the day that your business is shutdown?
- Are you staking your reputation on their words as validation?

CERTITUDE® SECURITY