Remeasure Cyber Risk

Place Value
$10,000

CERTITUDE SECURITY®

One Thing You Didn't Know

"You have used a tape measure before."
How accurate is this statement?

I realize this claim is not a bold prediction like the future value of Bitcoin at the end of the quarter.

But while you may have used a tape measure before, you may not be aware of everything this tool offers. Did you know that the first inch of the tape is 1/16 of an inch short? Yes, that's right. The first inch of your tape measure isn't an inch.

The design feature is intentional. The tape measure's metal hook is calibrated so that it moves just enough to give you a proper zero measurement, whether you measure inside or outside an object.

It's a tool designed to handle your specific circumstances, just as protecting your assets evolves with the operational effectiveness of your business.

How you manage cyber risk is a crucial intangible to your manufacturing operations. Read on to find out how Certitude Security® can help you save your company from disruption and loss.

However, one of the most common ways to damage the specialized slide on your tape measure's hook is by letting the tape recoil quickly. As a result, the hook slams into the case, loosening the mechanism you use for measuring.

Similarly, it's damaging to your business when criminals exploit your weaknesses and effectively slam your operating profits, cash management, and reputation. Certitude Security members can help you understand the methods of evaluating and prioritizing cyber risk that adapts to your business needs.
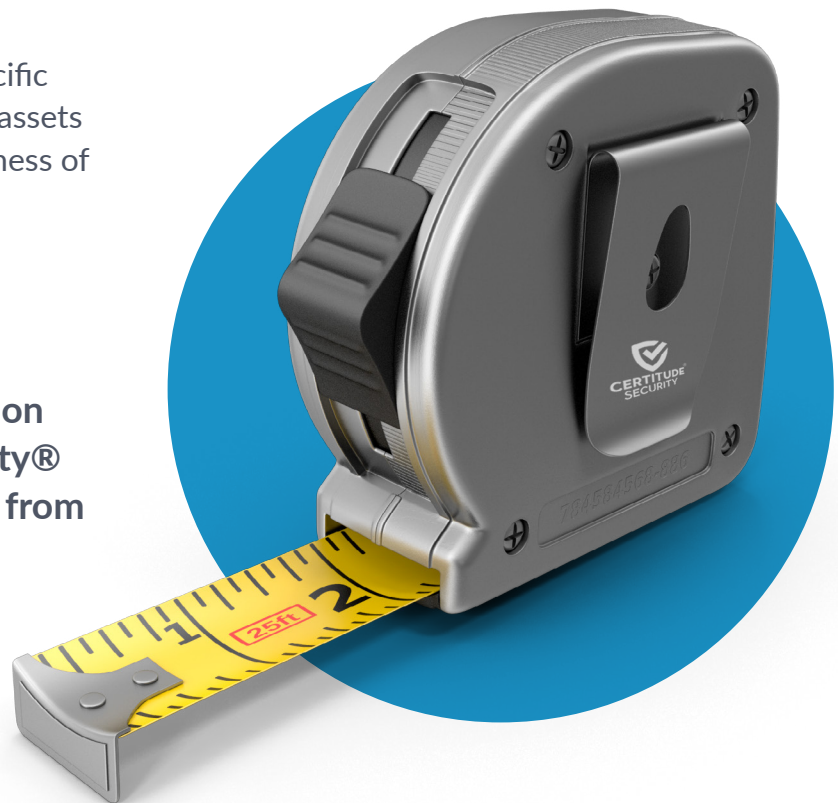
How Costly Is Information Insecurity?

Functions related to manufacturing operations may include designing and developing product lines, purchasing raw materials and components, product design, research and development, production planning, manufacturing of products, quality control, packaging, inventory, and logistics.

Every part of the operation relies on data from workflows within your business. But how are your employees, customers, and vendors impacted by disrupted data flow within your processes? Information security affects vital functions of every organization that provide goods or services to their customers.

How can you be successful when your workflows and processes halt? Costly disruptions to operations — including the inability to receive orders, remit payments, or complete on time and accurate product shipments — limit your progress. Will you pass along the increased production costs?

Reactive decisions, false assumptions, and delays have allowed cyber criminals to develop momentum. These opportunistic thieves see you as an easy means to improve their cash flow. You might succumb to extortion when the criminals state a deadline to release your information to the public.

According to a 2021 IBM survey[1], it takes 287 days on average to identify and contain a data breach. The most common outcome is paying a ransom when you can't access your data or systems. The time and resources you may spend recovering from data breaches can potentially impact your company severely and lead to job loss and stress for your family.

Are your assets secure from probable loss? How do you know?

To prevent or contain significant loss, you need to measure the internal and external exposure to cyber security threats. Developing this understanding and sharing knowledge is essential. Your stakeholders will demand better insights into the risks they have committed to cover.

[1] https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic

What You Don't Know Can Harm You

Your business has exposure to real threats that will lead to harm and loss. How can we make that assertion? Because 100% of the time, we discover process and control issues that fail to protect assets from exploitation during new client engagements. Disruptions impact workflows, impeding your employees' ability to meet your customers' timelines and expectations.

The tendency to pursue the urgent over the important continues at the detriments for many companies. It can be easy to ignore the facts that your exposure to cyber crime increases year over year. The tradeoff in false assumptions is to devote inadequate resources to protecting assets and workflows.

Senior executives within every company need to understand the vital risk decisions they're making. Therefore, a shared understanding of cyber risk and avoidance and data protection acceptance is necessary for sound investment decisions. We understand that you have assets to protect and timelines that must be met, so let's focus on your needs.

A great starting point for team awareness is Inspectionem℠. This confidential business process discussion reveals problems — peeling the onion, so to speak — as we eliminate assumptions and clarify what is most important for the operation of your business.

It is stressful when someone examines your work and choices. Once leadership and IT management understand that we utilize a multi-stakeholder shared purpose approach, commitment improves, and breakthroughs occur.

Why does knowledge of our intent and process change engagement? With the understanding that we focus on helping the team without belittling past decisions and indecisions, fears subside. Great moments take place when open and honest dialogue replaces defensiveness and subversion.

CERTITUDE SECURITY®

How Can You Secure Assets?

Inspectionem℠ provides improved accountability and predictability. The underlying truth supplied by Inspectionem℠ allows leadership to better direct resources (capital, time, people) with confidence. The planning process grinds out years of assumptions as confidential discussions increase shared knowledge.

It's true: You don't know what you don't know. Inspectionem℠ is a trust-building verification process that gives boards and executive leadership the ability to determine risk and reward improvements based on probable loss, cash flow, contractual commitments, and the desired pace of change.

Transparency is key to understanding and preparation, so we encourage responsible leadership committed to collaboration and action. The uninformed receive no mercy from criminals, so there is no excuse and no place for pride.

Rely on guidance from Certitude Security® to help address the security risks that keep you awake at night. Once you arrive at a consensus on the critical assets and workflows to be secured, we can combine our talents with less friction to protect your value for your customers.

Shared understanding is a force multiplier, allowing for higher-value conversations, information, and actionable insights. Improved decision-making awaits you as you transition from assumptions to shared understanding through working with our experts to protect your data. We look forward to collaborating with you.

As a proud supporter of American manufacturing, Certitude Security® is working diligently to inform leaders and facilitate essential asset protection priorities for supply chain businesses throughout the United States. If you're interested in learning about the empowering services that Certitude Security® can offer, visit our website or coordinate a time to speak to a team member today.

CERTITUDE®
SECURITY

Test Your Digital Asset Security Awareness

Are you curious about the depth of your digital security awareness?
Complete and submit this quiz to receive feedback on your understanding.

The choice of answers to be applied to the three questions below are **38%**, **20%**, and **10%**:

1 The average increase in the total cost of a breach from 2020 to 2021: _____

2 Share of total breach costs attributed to lost business: _____

3 Share of breaches initially caused by compromised credentials: _____

Identify which of the following descriptions are threats to your assets:

1 Cloud: _____

2 Social engineering: _____

3 Organized crime: _____

4 Mobile devices: _____

The email address for submitting your quiz answers is info@certitudesecurity.com

LOCATE THE QUIZ ONLINE

CERTITUDE ®
SECURITY