

## USE CASE

## WHEN LATER BECOMES TOO LATE

If you're looking for ways to create value for your company in 2022, pushing off data security isn't the astute option. Here's a look at what happens when "later" becomes too late — and what you can do to address security right now.

If you're interested in learning about the empowering services that Certitude Security<sup>®</sup> can offer, [visit our website or coordinate a time to speak to a team member today.](#)

## Diminishing Equity

Inadequate planning and measurement cause gaps in data security. Criminals focus their resources to locate these gaps, leveraging [weaknesses](#) in your strategy and execution to profit at your expense. These business disruption events have multiple negative impacts:

- Eroding equity.
- Increasing liabilities.
- Increasing your [cost of capital](#).
- Decreasing demand for your products and services.
- Dropping stock values.
- Creating excessive stress.
- Loss of trust that triggers changes in employment.

## Protect Against Loss Events

Even seasoned executives shy away from practical strategy discussions about connecting data security to digital platforms.

In truth, investing in targeted cyber security makes your organization more challenging for criminal enterprises to successfully attack, which, in turn, protects revenue, cash flow, and equity.

Start with these fundamental actions to reduce the risk of [compromise](#):

- Apply software updates promptly.
- Isolate, secure, and encrypt data backups.
- Require multifactor authentication (MFA).
- Secure your Virtual Private Network (VPN) and disable Remote Desktop Protocol (RDP), if possible.
- Use strong, unique passwords.
- Train users regarding suspicious links and attachments.

To learn more about financial stability, read [this blog post](#).

As a proud supporter of American companies, Certitude Security<sup>®</sup> works diligently to inform leaders and facilitate [essential](#) asset protection priorities for businesses throughout the United States.