Has Your Data Security Kept Pace with Work Force Changes?

85% Security Risks Are Up 85% Since Covid-19 Hit – Are You Prepared?

It's no secret that your company's data is your most valuable asset. Protecting it from hackers and scammers should be every employee's #1 concern. But since many people are working from home, they're often accessing confidential company files in an unsecured environment.

In fact, a recent poll showed that **76% of organizations** surveyed state they have experienced a data breach involving sensitive information this past year.

And of those data breaches:
80% impacted customer PII (personal identifiable information)
32% of the time, intellectual property was compromised

The cost of recovery after such a breach can wreak havoc on an organization's bottom line:

- On average, a data breach cost to mid-sized organizations was **$3.86 million in 2020**
- For Mega Breaches (1 million records or more) this cost grew to **$50 million**
- Since the start of the Covid-19 pandemic, surveys have shown that employees are **85% more** likely to leak files than they were in the pre-Covid days.

Think it can't happen to your company?

You might be surprised to learn the most common SOURCES of data breaches:
42% Malicious or criminal insiders (Rogue employees)
38% Employee carelessness (Careless/Uninformed employees)
36% External attack (Hacker)
28% System glitches

Only about ⅓ of breaches come through hackers, yet most company CEOs think it's always from the outside-in. What about the other **⅔ of breaches that originate internally – intentionally or otherwise?**

Here are key areas you need to consider:

Business Impact

CRITICAL ASSETS: Which apps, files, systems and communications are most vital?

ACCESS PROTOCOLS: How are your employees accessing them, and are those systems secure?

REGULATIONS: Based on your industry, are you in compliance with all security requirements?

SERVICE INTERRUPTIONS: If an attack occurred today, how would your business be impacted?

Your Environment

LOCATION: Where is your data physically located, and do you have multiple back-up servers?

ROCK-SOLID PROTECTION: Does your current technology assure easy restoration?

VIRTUALIZATION: Do you have systems in place to put everyone back on the same page?

SPEED: Can the speed of your current systems be restored after an attack, and how soon?

Your Support Teams & Processes

TEAM ASSIGNMENTS: Do you have tasks assigned by team members, with alternates?

RESPONSIBILITY: Does each team member know the critical tasks they must handle?

PROCESSES: What priorities does your plan give to critical business functions?

COMMUNICATION: How soon can you get everyone "singing off the same sheet of music?"

As you can see, there's **SO MUCH MORE** to consider than just getting your systems back on line! That's why at Lunavi, we focus on protecting both your data AND your procedures, through a highly- detailed review of your business. We focus on building resiliency, whether the source of the potential breach is physical damage, user mistakes, or malicious attacks.

IT PAYS TO BE PREPARED. Your IT Department is tasked with ensuring data availability and integrity 24/7, but they need the latest in technology and processes to maintain that integrity.

DISCOVER how Lunavi can help keep you safe every step of the way.
CONTACT LUNAVI.COM and experience the peace of mind that TOTAL protection can provide!

Sources:
2021 Data Exposure Report | Code42
IBM Cost of Data Breach Report 2020