WHAT ARE RISK ASSESSMENTS?

RISK ASSESSMENT IS A PROCESS THAT HELPS IDENTIFY:

- Internal and external vulnerabilities
- Threats to business data, systems, software, clouds and networks
- Consequences if threat actors exploit vulnerabilities
- Possibility of harm that may eventually unfold

Failure to conduct regular risk assessments can be costly!

KNOWING YOUR SECURITY RISK ENVIRONMENT

Only about 40% of owners believe there is sufficient risk assessment conducted in their company[1]. If you don't know your risk, you can't fix it.

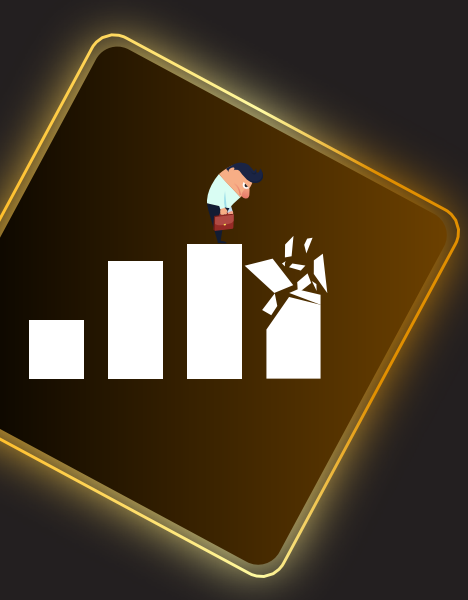
Cybercrime has shot up by 40% since the start of the COVID-19 pandemic[2]. Not being alert can make you the next target.

It is predicted that ransomware attack will occur every 11 seconds in 2021[3]. This leaves no room for complacency.

About 70% of organizations faced a cloud data breach in 2020[4]. Do you still believe your cloud data is completely safe?

THE CONSEQUENCES OF UNDETECTED RISKS

If any business risk goes undetected, it can snowball into a severe breach and cause:



Loss of productivity: Average downtime is close to two hours[5].

Financial loss: Average total cost of a data breach in 2020 is $3.86 million[6].

Reputational damage: One-third of customers will end their association with a business following a major breach[7].

Legal liability: The OCC fined Morgan Stanley $60 million citing failure to comply with standards and secure sensitive data.

Regular risk assessments are a positive and preventative investment in protecting your business.

MAINTAINING REGULATORY COMPLIANCE

To stay ready and compliant with security requirements of most regulatory bodies, regular risk assessments are essential to identifying and measuring potential business impacts.

This is how you classify the risks:

High: High impact risks, if unchecked, could lead to a major breach and have a significant impact on the operations of your business or even result in external monitoring and enforcement.

Medium: Medium impact risks, if unchecked, could adversely affect your business' cybersecurity posture and lead to demand for operational changes by the external enforcement agency.

Low: Low impact risks, if unchecked, might contribute to failure in accomplishing some of your business objectives.

BENEFITS OF REGULAR ASSESSMENTS

01

Identifying your risk profile: Detecting threats and sorting risks based on their potential for harm helps you to focus your efforts on urgent pain points.

02

Asset discovery & protection: With an up-to-date inventory from your risk assessment, you can determine ways to protect your critical assets and vital data.

03

Reduce security spending: Regular risk assessments help you reduce security spending because you know where you need to put money to ramp up security.

04

Actionable analytics: Availability of information that gives enough insights into the future helps you take adequate actions that can improve your business' security.

05

Keeps you compliant: When you handle your business assets and data securely through regular assessments, your business can avoid regulatory violations.

Sources:
1. Security Magazine
2. FBI 2020 Report
3. JD Supra Knowledge Center
4. Help Net Security Magazine
5&7. IDC Report
6. IBM Cost of Data Breach Report

Though it sounds a bit complex, with the right partner by your side, you can run regular risk assessments for your business and prevent a risk from escalating into a full-blown data breach.

CONTACT US NOW!