HOW TO THINK ABOUT CYBER RISK AND ORGANIZATIONAL RISK

It's easy to think of cybersecurity as a matter of defending against the various types of threats all organizations are exposed to. This is commonly referred to as **cyber risk**.

But leaders responsible for managing risk and protecting their organizations need to consider a different kind of risk

Organizational risk.

Organizational risk refers to whether or not you can properly implement processes, systems, controls, vendors, or strategies that secure your company and reduce your cyber risk.

It's often ignored but should be considered just as much as threats. We put together a cheat sheet for you that lists out what makes up **cyber risk** and what makes up **organizational risk**.

CYBER RISK

Vulnerable software
Bad actors are always looking for ways to exploit devices or software. If you miss an update, you might miss an important security fix.

Ransomware
This type of malware holds critical files at ransom until your organization pays the perpetrators.

Insider threats
Employees or contractors may steal valuable data or disrupt infrastructure.

Phishing
Hackers will often impersonate a trusted person and send out an email containing a malicious attachment or link as a precursor to an even worse attack.

Brute force attack
Hackers might try to get into your network by compromising one of your employee's accounts, using password data from past data breaches or obtained in another manner.

Leaks
An employee may accidentally expose sensitive information without knowing it — if it's found or falls into the wrong hands, it can end up hurting an organization.

Misconfigurations
Misconfigured databases can lead to inadvertent data exposure, especially for bad actors who are looking for publicly accessible databases.

ORGANIZATIONAL RISK

Budget
A new tool, vendor, or partner may cost too much or their pricing model makes it difficult to properly budget in the future.

Implementation
Without the time, resources, or staff available to properly implement a new tool or vendor, you won't be able to fully realize the benefits, reducing effectiveness.

Staffing/headcount
New tools or vendors might require additional staffing or individuals trained for that specific tool.

Integration
It's not worth considering a tool or vendor incompatible with your infrastructure and client configurations.

Vendor management
More tools and vendors require more vendor management. If it overloads your department, you might be putting your organization at risk.

Department /Organizational consensus
Major vendors and partners require sign-off from various department-heads and teams. Lack of consensus often leads to a non-starter.

Lack of effectiveness
Have you done your due diligence and set up a way to measure effectiveness? If not, you may not be able to properly assess whether you're actually building up your security posture.

HOW A MODERN MSSP SOLVES BOTH

A managed security service provider, or MSSP, can address **cyber risk** and **organizational risk**. When partnering with the right MSSP, you're purchasing an outcome (i.e. as protecting your organization), rather than tools or a partner that can possibly achieve an outcome.

You're also reducing your operational risk by choosing an MSSP that has a clear pricing structure, brings their own set of curated security tools, and works with you to effectively increase your cyber resiliency in a proactive manner.

This will help you budget effectively, streamline implementation and integration, and reduce the level of effort required by you and your employees.

To learn how SolCyber helps organizations stay protected, reach out to us at **hello@solcyber.com**

SolCyber

solcyber.com