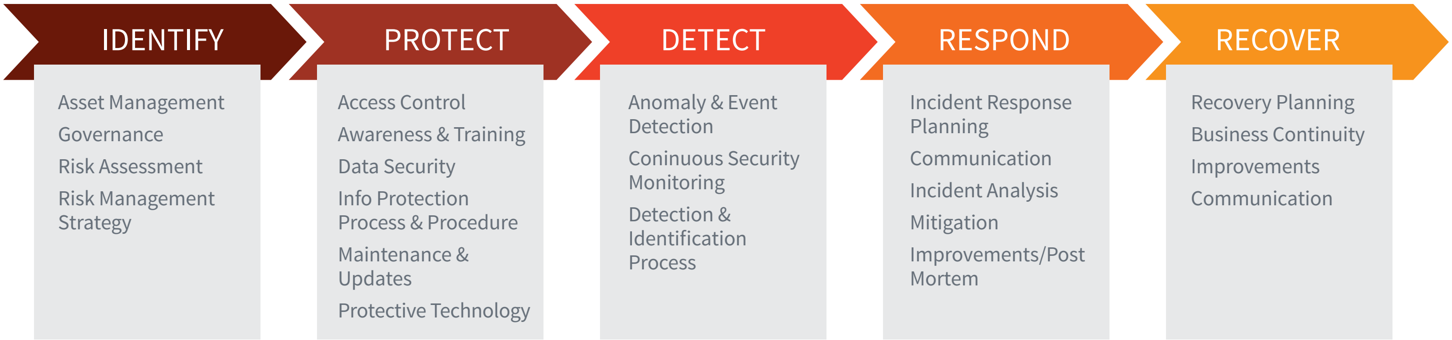
National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity



IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	Access Control	Anomaly & Event Detection	Incident Response Planning	Recovery Planning
Governance	Awareness & Training	Coninuous Security Monitoring	Communication	Business Continuity
Risk Assessment	Data Security	Detection & Identification Process	Incident Analysis	Improvements
Risk Management Strategy	Info Protection Process & Procedure		Mitigation	Communication
	Maintenance & Updates		Improvements/Post Mortem	
	Protective Technology			

The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure.

IDENTIFY: RISK ASSESSMENT

Understanding your risks is an essential part of an effective cybersecurity—and overall business—strategy for your MSP. Here are the five main steps that your risk assessment should contain:

- **Identification.** First, you need to identify the exact risks for the given area, such as a ransomware attack, accidental data deletion, or downtime due to a natural disaster.
- **Analysis.** Evaluate the severity and the probability of the risk, define which business function(s) could be harmed in which specific case, and prioritize the risks.
- **Mitigation.** Once the risks have been identified and prioritized, you need to create a set of policies and frameworks to reduce their probability. For example, if your risks are in the IT-security area, you should prepare for possible breach scenarios, including malware attacks, human error, or hardware failures.
- **Treatment and damage control.** Sometimes it's not possible to evade the unwanted, and then the risk becomes reality. Treatment and damage control, from your customers' perspective, is just as important as risk mitigation. Develop your disaster recovery and data breach incident response plans with care, discuss and verify them with your clients and review them regularly. Remember that only by acting thoughtfully during a disaster or other unwanted situation can you avoid losing a client.
- **Monitoring.** Once you have created solid MSP risk management workflows and frameworks, you should constantly monitor the risks from your priority list, and review and recheck your plans.

MSP RISK MANAGEMENT BEST PRACTICES

- **Pay attention to the top 5.** Risks are literally infinite, so it's important to focus. For example, the most common IT-security risks for all clients in all verticals are backup loss, hardware failure, end-user error, ransomware and phishing attacks. These risks are both common and complex, and you should first create a workflow to mitigate them and only then turn your attention to more unusual ones.
- **Start with yourself.** Some managed service providers keep forgetting about their own security while pursuing that of their clients. However, no matter how secure the premises of your clients are, if you get breached, their data will no longer be secure.
- **Create end user training programs.** You should create both internal and client-oriented training programs. Your team should understand the whole concept of MSP risk management. Your clients, in turn, should at least know how to avoid the most common issues and how to contact your support team.
- **Check your backups.** Yes, really. Some managed IT providers don't verify their backups and, as a result, lose their clients during a disaster in which they cannot recover the data. That is a huge reputational loss.
- **Create documentation.** Don't rely on your own knowledge or your team's expertise. You should create and update your documentation regularly. Document each successful attack or breach. The post-mortem process is especially helpful in mitigating future unwanted events.
- **Legal risks.** If you have clients that fall under compliance, discuss that with your attorney. You need to be sure that, if they fall victim to a data breach, you are safe from prosecution. Also, review all your SLAs, MSAs, and SOWs with your attorney. This will secure you in the event of a lawsuit by an unhappy customer. The final thing you need to do to mitigate the legal risks is to understand how to use general and cybersecurity insurance.

CONCLUSION

MSP risk management is a mindset that you need to support with commitment and actions. If it's truly a part of your culture and operations, it can be a real competitive advantage in a highly competitive MSP market.