datto

The Journey To Cyber Resilience

Becoming cyber resilient is not an overnight endeavor—it's a journey that requires careful evaluation of an organization over time. As an MSP, cyber resilience starts with your own business and extends outward to your clients. So where do you start?

People, Process, and Technology

A successful cyber resilience strategy requires a holistic approach to building capabilities that are composed of people, process, and technology.

1. People

Hiring or developing security experts and building security awareness throughout the organization.

2. Process

The series of actions that need to happen in order to achieve a particular outcome.

3. Technology

Solutions that empower People and support Processes for robust capability.

When evaluating your business, look for gaps in your security capabilities from people, process, and technology perspectives. For example, if your staff lacks security chops perhaps they can benefit from training or you might hire a tech with a security background. Are your processes repeatable and measurable? If not, that should be an area of focus. Finally, look at the technology you have in place. Are you using what you already have to its full potential? If not, then start with getting those tools operating effectively, then you can start looking at technology to fill gaps in processes or that fills the needs of your people.

In our experience with MSPs, most cyber resilience issues are not technology based. That's why we recommend starting with People and Processes. Technology investment flows from people and process requirements.

Cybersecurity Frameworks For MSPs?

For many MSPs, cybersecurity frameworks can seem overwhelming, but they don't have to be. Cybersecurity frameworks are simply guidelines for achieving security objectives that lead to maturity, and ultimately risk reduction. In fact, many organizations use specific aspects of frameworks or combinations of frameworks to meet their cyber resilience goals.

In this document, we'll refer to the Center for Internet Security (CIS) Security Controls and the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Rather than an exhaustive look, we'll focus on some of the key tenets of each.

CIS Controls are a prioritized set of actions to identify and protect your organization and data from known cyber-attack vectors. There are many controls. Many MSPs focus on either Control Groups 1-6 (previously known as Basic), or Implementation Group 1 to get started. You may not be sure which path to take, that is ok. Remember, identifying and implementing all the controls that are applicable to your organizations' needs is the ultimate goal. We've identified the essential CIS controls to focus on that support **both** paths:

- **Hardware Asset Inventory**
- **Software Asset Inventory**
- **Patch Management**
- **Privileged Account Management**
- **System Configuration Baseline and Images**
- **Log Management System**

By putting these controls in place, you'll know what you have that is worth protecting, get your patching game up to par, manage privileged identity and access management credentials, implement secure baseline configurations on protected hardware and software assets, and assure that you have basic logging in place. The beautiful thing is that you can accomplish these objectives with technology you already have and some process creation. In addition to setting you up for either CIS Controls patch, all of these controls map directly to NIST CSF, so you're moving in a direction that helps you

conform with the two most common frameworks used by MSPs.

The NIST Cybersecurity Framework compiles industry standards and best practices into a cohesive format to help businesses manage cybersecurity risks. It is based on five functions: Identify, Protect, Detect, Respond, and Recover.

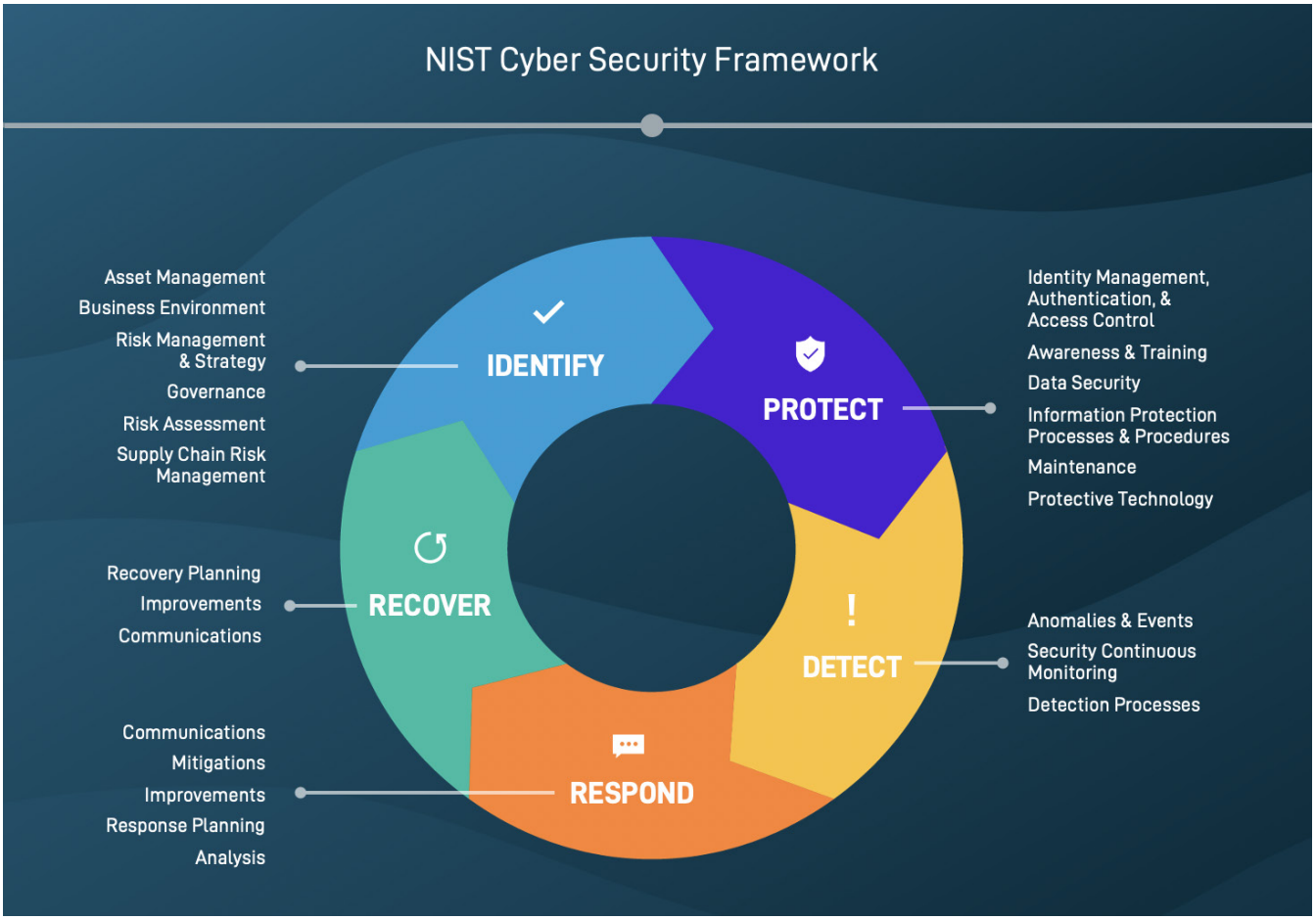
- **Identify** capabilities help you understand your environment to manage cybersecurity risks to people, data, assets, and systems.
- **Protect** capabilities that limit and contain impacts resulting from a cyber event.
- **Detect** capabilities help discover the occurrence of a cyber event in a timely manner.
- **Respond** capabilities allow you to act upon a cyber incident and contain the impacts.
- **Recover** capabilities permit timely recovery to normal operations and reduce the impacts from a cyber incident.

Establishing and/or strengthening the capabilities outlined in each of these functional areas enables businesses to effectively limit the potential for bad outcomes, but also respond to and recover from cybersecurity incidents that will happen, analyze root causes, and make improvements over time.

How Datto Can Help

As your clients' trusted technology advisor, you are in a unique position to help them become more resilient to cyber threats. This might mean educating employees on ways to avoid attacks, assisting in risk assessments, or introducing new processes or technologies that protect against attacks or mitigate the impact of business downtime when they do occur.

Datto solutions solve key technological problems, support the creation of repeatable, measurable processes, and reduce administrative burden. From Datto RMM's Ransomware Detection and automated patching capabilities to Datto Continuity's point-in-time restore and Cloud Deletion Defense, our solutions help MSPs build their clients' cyber resilience. Autotask PSA enables MSPs to track adherence to processes and procedures that build their own cyber resilience.



Asset Management

Asset management is critical to identify risks and eliminate application vulnerabilities. Datto RMM's asset discovery, tagging, inventory, and policy-based patch management capabilities increase client security while increasing MSP efficiency. **#Identify**

Ransomware Detection

Datto RMM Ransomware Detection is designed to mitigate the impact of ransomware attacks. It monitors for ransomware, triggers an alert if it is detected, and prevents further spread by isolating infected devices. **#Detect #Respond**

Business Continuity

Datto SIRIS uses snapshot and virtualization technologies for fast recovery of server operations locally or in the cloud. In the event of a cyber attack, a backup image can be mounted as a virtual machine, enabling business operations to continue while the primary server is restored. This dramatically reduces business downtime when compared with traditional backup. **#Recover**

Ransomware Recovery

Point-in-time snapshots allow businesses to simply 'turn back the clock' to a snapshot before the attack occurred, reducing time-consuming manual effort and speeding restores. What's more, SIRIS eliminates chain dependencies making backups resilient against ransomware. **#Recover**

Datto Cloud

Owned and operated by Datto, the Datto Cloud is built on an immutable platform that ensures backup security. Our exclusive Cloud Deletion Defense™ protects cloud backup snapshots from accidental or malicious deletion. **#Protect #Recover**

Network Security

Datto Networking delivers intrusion detection and prevention for secure connectivity businesses can count on. Stateful firewall, enhanced web content filtering, WiFi protected access, and advanced encryption prevent attacks and increase business resilience. **#Protect**

Conclusion

There is no single or best way to achieve cyber resilience, as no two MSPs are the same. However, building cyber resilience should be considered essential and the most important thing is to just get started. The good news is that you are not starting from scratch. It is likely that you already have many of the capabilities outlined above in place. Using the frameworks discussed above, you can identify and address gaps in the security posture of your MSP and your clients' businesses. You may even identify new business opportunities in the process.

datto

Corporate Headquarters
Datto, Inc.
101 Merritt 7
Norwalk, CT 06851
United States
partners@datto.com
www.datto.com
888.294.6312

Global Offices
USA: 888.294.6312
Canada: 877.811.0577
EMEA: +44 (0) 118 402 9606
Australia: +61 (02) 9696 8190
Singapore: +65-31586291