Using NIST Cybersecurity Framework

We often talk about following industry standard best practices. The Cybersecurity Framework from NIST, the National Institute of Standards of Technology, is one of the most widely used and best respected Cybersecurity Standards.

We will look at how to apply the NIST Cybersecurity Framework to your business.

1. Identify

Identification is about knowing what's out there—including people and physical assets like PCs, mobile devices, switches, firewalls, and more.

- **Who has access to the network?**
- **Are all network devices accounted for?**
- **Are any devices using default credentials?**
- **Is software and firmware up to date across devices?**

2. Protect

Protection includes developing and implementing safeguards to prevent security problems and make sure that your computers and network are available for business use.

- **Are users sharing accounts?**
- **Is two-factor authentication enabled?**
- **Are email filters in place?**
- **Are employees receiving security training?**

3. Detect

Detection covers your ability to identify a cybersecurity incident.

- **Is security software installed and up to date?**
- **Are audit logs being monitored?**

4. Respond

Response is about taking action when a cybersecurity incident is detected.

- **Do you have a plan to handle a security breach?**

5. Recover

Recovery is about minimizing downtime—and expenses—if a security incident or breach happens.

- **Do you have full backups of important business data and device configs?**
- **Do you have cyber insurance?**
- **Can your processes, procedures, and technologies be improved?**