DataSure24's February Brainbytes:
2023 Cybersecurity Goals

DataSure24 is your cybersecurity partner, working to help meet your company's specific security needs. Each month, we'll offer bytes of information about emerging risks, news, and protective measures to help keep your data safe and your network secure.

We're a month and half into 2023, time to review your business's goals for the year. If your company doesn't have any cybersecurity goals for 2023, your goal, then, is to implement a comprehensive cybersecurity program.

In 2022, we predicted that, among other things, cybersecurity would be increasingly driven by compliance. In order to ensure the protection of customer information, several industries are facing stricter regulatory requirements regarding cybersecurity, including:

- Manufacturing (CMMC, DFARS)
- Financial (NYS DFS 23 NYCRR 500, NCUA)
- Healthcare (HIPAA)
- Collections Agencies (FTC Safeguards Rule)
- Payment Card Industry (PCI-DSS)

Even if your company does not fall into one of these industries, it too must be prepared for possible security breaches and avoiding gaps in its cybersecurity programming. Fortunately, most business don't realize they have many of the tools already in their environment to help meet compliance requirements AND follow cyber security best practices. The first step, is to assess the organization's security posture.

CyberSecurity Assessment

Completing a Cybersecurity Assessment will allow you to answer the following questions:

- What is my company's critical information?
- What controls are in place for information systems?
- What is the current security posture of information systems?
- Should more or less stringent countermeasures be instituted?
- What is the prioritized security roadmap to follow that addresses high-priority issues first?
- What compliance requirements are met, and what is next on our compliance checklist?

Selecting a Framework

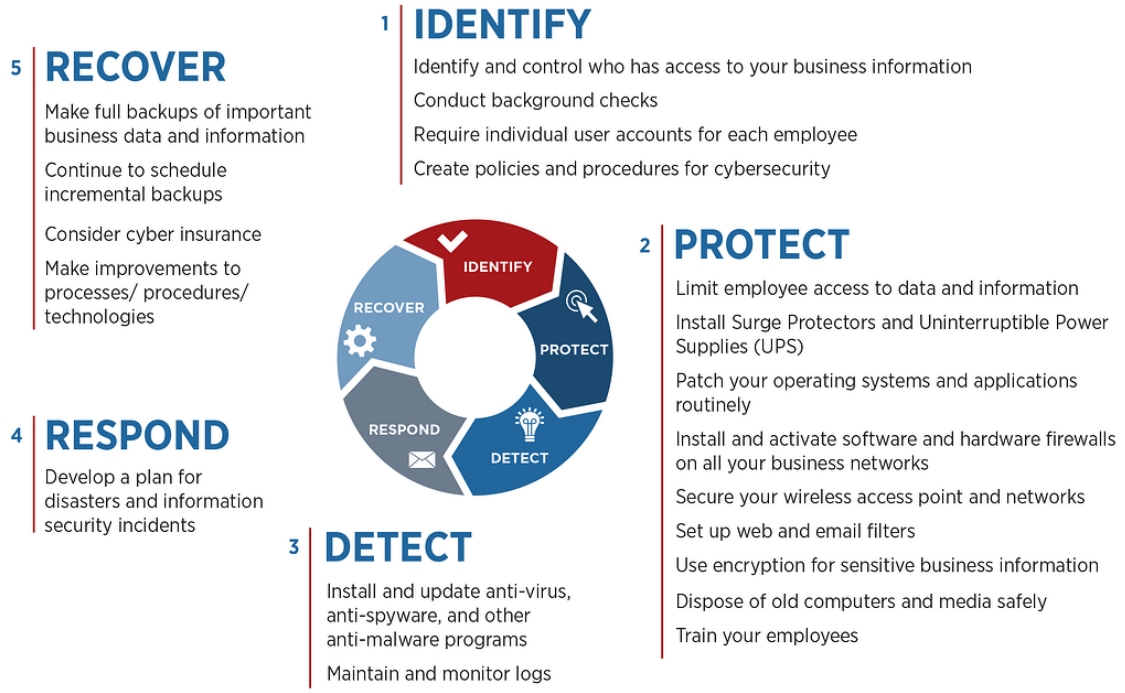
Although all organizations aren't required to comply with the same frameworks, alignment of security and control structures against recognized frameworks is a key step in process maturity and diligence.

Apart from being prepared for possible security breaches and avoiding any loopholes from the organization's standpoint, following a framework helps you approach cybersecurity from an end-to-end risk management perspective. This includes the monitoring activities that occur at all levels and across all departments in the organization.

Implementing a good framework also helps an organization assess itself, its place in the threat landscape, and the loopholes it has to address.

DataSure24's cybersecurity and risk assessments typically follow the National Institute of Standards and Technology (NIST) and Center for Internet Security (CIS) methodology.

NIST, for example, has become the standard for cybersecurity in the manufacturing industry (among others). The Framework is organized by five key functions, and may offer a good starting point for your organization:



Ultimately, your choice of framework depends on your organization's security needs.

A framework is a foundation: a strategic, well-thought plan, offering guidance, and helping protect a company's data, infrastructure, and information systems. The right framework, established correctly, will help to mitigate cyber risks, regardless of the environment.

Cybersecurity should always be a business priority. ***Unprepared organizations will become easy targets for cyberattacks.*** *Now is the time to learn the potential cybersecurity risks for your business, and build a complete cybersecurity plan.*

For more info on developing a cybersecurity program, check out our blog:
[Cybersecurity: Where to Start (or Restart)]

If you would like to speak more about how DataSure24 might help your company meet its security needs, contact us by clicking below, or call (716) 600-3724. We look forward to hearing from you!

Email Us!

DataSure24, 41 Columbia St, Buffalo, NY 14204, 716.600.DS24