Don’t be a statistic. Take cybersecurity seriously.

Heed this warning! Failing to invest the time and resources in preparing for a cybersecurity incident could be the death knell for your business. Various studies and reports indicate that a significant number of small companies are unable to sustain their businesses over six months after a cyber attack. What can we do and where can we turn to avoid becoming a statistic?

The NIST Cybersecurity Framework, with its practical set of guidelines, has been structured and published to help businesses become more resilient. The framework became a federal act in August 2018, requiring all federal agencies to implement and follow this structure. While this may be voluntary for small businesses, this program provides a set of standards, guidelines and best practices to manage cybersecurity-related risk.

Due to the increase in cybercrimes, small businesses are increasingly adopting the NIST framework to provide the structure for assessing and implementing their own security practices and systems. Managing cybersecurity lands squarely on the business owners—those who are directly responsible for the survivability of the organization.

There are five logical functions, each embedded with categories, subcategories and references to guide business owners and staff to build security and resiliency into their organization.

IDENTIFY – “Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.”

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy

PROTECT – “Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.”

- Access Control
- Awareness and Training
- Data Security
- Information Protection Processes
- Maintenance
- Protective Technology

DETECT – “Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.”

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

RESPOND – “Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.”

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvement

RECOVER – “Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.”

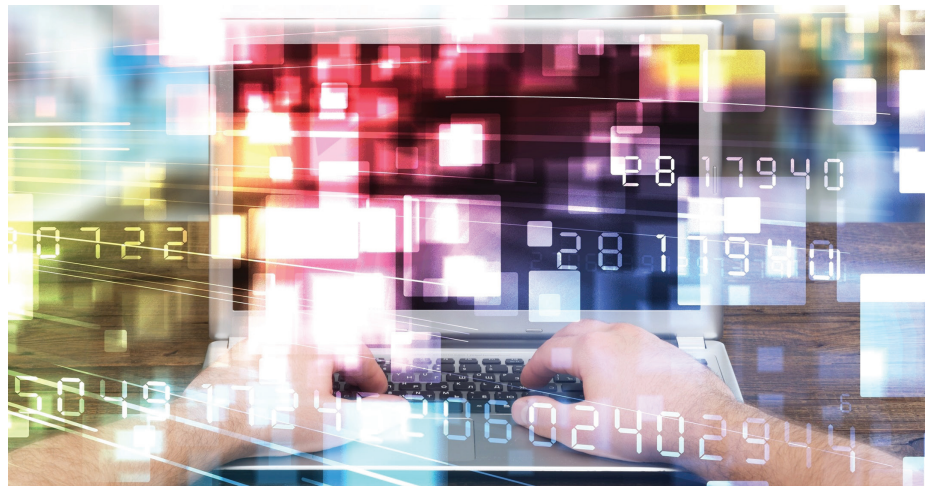
- Recovery Planning
- Improvements
- Communications

To be completely transparent, there is no destination when it comes to cybersecurity. However, if we follow a plan like the NIST CIT Framework, it can lead us to a better and more secure place by providing:

- A comprehensive set of cybersecurity policies and procedures
- A remediation plan for present vulnerabilities
- Guidelines for regulatory compliance, if required
- A plan for implementing a security infrastructure to detect and protect your digital and financial assets

The first step is to develop a Framework Profile that identifies the outcomes your business will develop based on your risks, needs, market sector and your industry.

In developing your Framework Profile, you will want to start with an assessment. The simplest and best first step will be a self-assessment. The goal will be to arrive at a quick sense of your strengths and weaknesses and to provide advice as to what improvements you should consider. Think about an assessment that will measure your results against the NIST model for cybersecurity for small business. Some sample questions may include:



- Do you require Information Security training for your employees?
- Are recovery processes and procedures documented and reviewed?
- Are potential impacts from third parties identified and documented?
- Are you using an email filtering solution?
- Do you have web filtering or website blocking set up?
- Do you have a threat detection product in place today?

The answers to these and other questions will establish your current state and your current security posture, both from a technical and an organizational standpoint. It will also be useful to have an understanding and comparative analysis of how your business stacks up overall by industry, size and location.

The results of the assessment should establish the gap analysis for the systems, policies and procedures that will require remediation and improvement. Understanding the importance of each of these and other factors will also help to set your priorities, the plan and budget for what will create the best results with the greatest impact and return on investment.

With the results of this assessment in your hands, you will meet with the trusted advisors who can then counsel you on the subsequent steps, including reviewing results and running through the assessment together to get a deeper look. Cybersecurity is very dynamic. Your business is likely changing from month to month and year to year. The marketplace and economic environment is ever-changing. Certainly, the vulnerabilities and threats to the security of our digital assets are changing daily with new forms of attacks.

THE FINAL WORD... OF WARNING

We have all witnessed the U.S. government and large corporations with highly-staffed, world-class, expert security teams fall victim to data breaches costing millions of dollars. It is very clear that no one organization is 100 percent immune from cybercrimes. We also know that attacks directed at small businesses are on the rise. Please pay extra due diligence to planning for the fifth function: Recover. Have systems and a plan in place to recover your systems, recover your data, recover your reputation and recover or insure against any financial loss.