White Paper

Updated April, 2018

Every Small Business Should Use the NIST Cybersecurity Framework

By Ola Sage, Founder & CEO, CyberRx

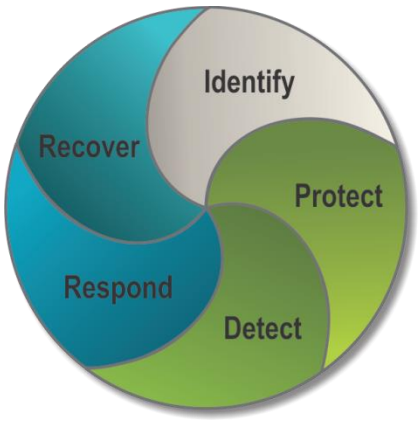
Turn on the TV, or open a newspaper on any given day, and the headlines will scream of another company, large or small, that has been targeted or significantly damaged by hackers. Small and medium-sized businesses (SMBs) are much more vulnerable to cybersecurity attacks than those with large infrastructures and protection investments.

More than one out of five small businesses reported being the target of a cyber-attack, with one out of ten being a target within the last 12 months.[1] Often, these companies have fewer resources to invest in security, putting not just their companies, but also their business partners at higher risk. Not to mention, costs that can exceed $100,000 for a single breach. These costs may not fully reflect all the associated indirect costs such as lost productivity, loss of customer trust, or opportunity costs such as lost revenue or a damaged reputation.

As an SMB, if you feel safe and out of reach from a cyber-attack, you are not alone, but consider this fact. Half of small businesses could remain profitable for only one month if they lost essential data according to the Better Business Bureau's 2017 survey of over 1,000 small businesses. That should give you pause. So, what can or should an SMB do?

There is good news. The *Cybersecurity Framework* released in February 2014 proposes five core functions: Identify, Detect, Protect, Respond, and Recover, to which every organization, large or small, should pay attention and implement to proactively address and better manage cybersecurity risks to their business.

There are five things every SMB should know about the NIST Cybersecurity Framework: 1) It is actionable—and allows you to assess your organization's risks in the five core functions;



2) It leverages industry standards and best practices; 3) It helps you focus and prioritize important cyber-related investment decisions; 4) It can help reduce legal risk with evidence of your organization's good faith efforts to manage cybersecurity risks; 5) It is flexible—and allows SMBs in different industries and of various sizes to adapt the Framework and make it work for them.

Identify Risk Areas within the Company

With a goal of readiness, preparedness, and resilience, every small business should know and understand which organizational systems, assets, data, and capabilities need to be protected.

[1] 2017 State of Cybersecurity Among Small Businesses in North America, Better Business Bureau

Cybersecurity is about risk management; therefore, your C-Suite must participate in identifying and understanding the cybersecurity risks to the organization. This should include the CEO or president as well as the COO, CFO, CIO, CRO (chief risk officer), and CAO (chief administrative officer). For smaller companies that typically do not have the resources for all of these roles, at a minimum, the CEO or president and the individuals who have responsibility for operations and finance should be involved. Since many small businesses outsource their IT operations, it is recommended that companies involve outside experts in assessing the five core elements.

Protect the Company's Assets

One of the easiest and most affordable protections a company can take to protect its assets is to train its people. It sounds simple, but unfortunately many small businesses don't take the time, or think it necessary to make sure their employees understand how they can help protect their company assets. There are also a myriad of industry best practices for safeguards that include recommendations like:

- Make backup copies of important business data and information;
- Change default credentials for all systems, and require individual user accounts for all employees;
- Limit employee access to data and information and limit the authority to install software;
- Change passwords regularly;
- Protect information, computers, and networks from viruses, spyware, and other malicious code;
- Provide firewall security for your IT infrastructure;
- Control physical access to your computers and network components; and
- Secure your Wi-Fi networks. If you have a Wi-Fi network for your workplace make sure it is secure and hidden.

If your business uses an outsourced IT provider, work with them to make sure that these safeguards are implemented. They can also assist with developing or providing training to your employees on cybersecurity do's and don'ts.

> The NIST Cybersecurity Framework is a risk-based approach to managing cybersecurity risk.

Detect a Cybersecurity Event

How do you know if your organization has been attacked? Many times, there are visible signs. Examples may include your website being down or displaying random or negative content that is not authored or approved by your company. Your network may suddenly become unavailable or certain software applications may behave strangely or provide errant information.

There are a variety of products and services on the market today to help your company develop and implement appropriate activities to assist you in identifying a potential cybersecurity event. For many small businesses, the investment needed to procure all of these tools solutions may be cost prohibitive, so some small business may want to consider using a vendor that specializes in monitoring and detecting anomalous activity, rather than doing it themselves.

Respond to a Cybersecurity Event

Responding to a cybersecurity event means taking action to develop or implement appropriate activities in response to a detected cybersecurity incident. It is important that your response processes and procedures are developed before a cybersecurity event occurs. Depending on the type of cybersecurity event, a response may include:

- Taking steps to quarantine the breach, so other systems or users are not affected;
- Implementing a response plan that describes what processes and procedures need to be executed to address the event;
- Communicating the status of response events and coordinating with stakeholders; and
- Performing forensics.

Recover from a Cybersecurity Event

A recovery plan supports your organization's ability to return to normal during or after an attack. The plan does not need to be overcomplicated and should include, at a minimum, lessons learned, which should then be incorporated into future activities. The plan should also address any holes in the communication coordination between internal and external parties such as employees, vendors, and public relations partners, among others.

Key Take Away

The #1 action every SMB should take is to assess where they are most vulnerable to cyber-attacks or breaches so targeted, risk-based actions can be implemented to reduce their cybersecurity exposure.

SMBs should expect cyber-attacks to increase as hackers and other cyber criminals expand from traditional modes of attack to the less expected channels such as social media and mobile devices.

Using the NIST Cybersecurity Framework can help SMBs:

- Become more knowledgeable about their organization's cybersecurity threats and risks;
- Determine areas of vulnerability that may exist with people, processes, or technology;
- Have greater confidence and control to prioritize and determine where to invest cybersecurity resources; and
- Provide evidence of their organization's good faith efforts to manage cybersecurity risks and implement reasonable security measures.

About the Author
Ola Sage is a serial entrepreneur and the founder and CEO of CyberRx. A champion and advocate for cybersecurity readiness, Sage frequently meets with and speaks to business groups and CEOs about cybersecurity and has testified to Congress on issues around cybersecurity insurance, the Cybersecurity Information Sharing Act and its impact to SMBs, and expanded liability protections for small businesses that participate in voluntary information sharing with the federal government to promote stronger cybersecurity. She is the immediate past Chair and a current member of the Executive Committee of the national IT Sector Coordinating Council (IT SCC). The IT SCC, comprised of the nation's top IT companies, professional services firms, and trade associations, represents private sector interests in cybersecurity and critical infrastructure protection to the U.S. government in a public private partnership with the Department of Homeland Security (DHS).

About CyberRx
CyberRx is a cybersecurity risk and compliance assessment software company. Using a unique application of the NIST sponsored Cybersecurity Framework on our software platform, clients assess their risks, create plans, and validate their strategies based on their risk profile and budget. Through our distinctive concierge service, CyberRx connects clients to qualified and vetted products, provides technical expertise to implement or fix problems, performs incident support services, and conducts cybersecurity and awareness training for executives and staff. For more information about **CyberRx,** please visit us at https://cyber-rx.com.