MEP National Network™

MANUFACTURERS GUIDE TO CYBERSECURITY

For Small and Medium-Sized Manufacturers

Table of Contents

01 **A Growing Threat to U.S. Manufacturing**

04 **Understanding the Risks to Your SMM Firm**

06 **Protecting Your SMM Firm**

07 • Identify

09 • Protect

15 • Detect

17 • Respond

19 • Recover

21 **NIST Cybersecurity Framework Steps**

A Growing Threat to U.S. Manufacturing

If you're like most U.S. small and medium-sized manufacturers (SMMs), you rely heavily on information technology to conduct business. Day-to-day business operations like banking, payroll and purchasing are all conducted over the Internet. Machines on the shop floor are connected to networks and employees use mobile devices to access company information. Have you ever considered how vulnerable your SMM firm might be? Hackers and cyber criminals are focusing their attention on SMMs just like you.

Many larger manufacturers in the U.S. have been putting people, technology and money into protecting themselves from cybersecurity threats. These manufacturers have become more difficult targets for malicious attacks from hackers and cyber criminals. Because SMMs typically don't have the resources to invest in cybersecurity the way larger manufacturers can, many cyber criminals view them as soft targets.

You may not consider yourself a target, but your SMM firm may have money or information that can be valuable to a criminal. Your computer can be compromised and used to launch an attack on someone else (i.e., a botnet) or your firm may provide access to more high-profile targets through your products, services or role in a supply chain.

It is important to note that criminals aren't always after profit. Some may attack your manufacturing company out of revenge (e.g., for firing them or somebody they know) or for the thrill of causing havoc. Similarly, not all events that affect security are caused by criminals. Environmental events such as fires or floods can severely damage computer systems.

61% of small businesses have experienced a cyberattack in the past 12 months.

Source: 2017 State of Cybersecurity in Small & Medium-Sized Businesses, Ponemon Institute

Common Types of Attacks and Breaches

Cybersecurity incidents can have devastating impacts on SMMs, including:

- Damage to information or information systems
- Regulatory fines and penalties / legal fees
- Decreased or stopped productivity
- Loss of information critical in running your business
- Loss of customers
- Damage to your credit and inability to get loans from banks
- Loss of business income

Unfortunately, SMMs often have more to lose than larger manufacturers because an event — whether due to a hacker, natural disaster or business resource loss — can have a major impact. SMMs are often less prepared to handle these types of events. But because SMMs often have less complex operational needs and IT infrastructure, they may be able to take steps to detect and recover from a cybersecurity incident quickly. It is vitally important that you consider how to protect your business before an incident occurs.

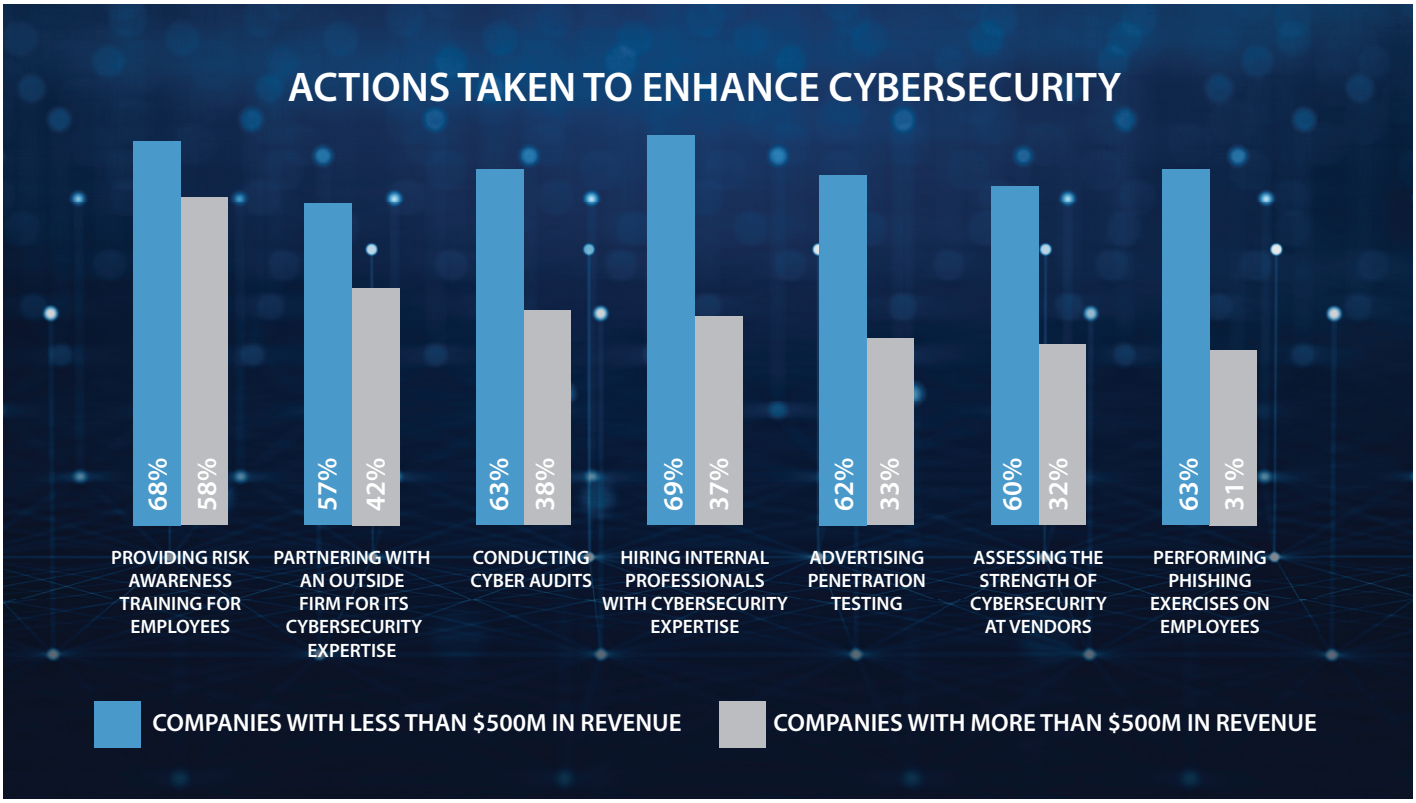
SMMs often see cybersecurity as too difficult or too expensive. It's true that there are no easy, one-size-fits-all solutions. If cybersecurity is considered part of the business's overall risk management strategy, it doesn't have to be intimidating.

> *Cybersecurity can be a key differentiator for your company. A cybersecurity program can help your company gain and retain customers, employees and business partners.*
>
> *Customers have an expectation that their sensitive information will be protected from theft, disclosure or misuse. Protecting your customers' information is an example of good customer service and shows your customers that you value their business, potentially increasing your business opportunities.*

Employees have an expectation that their sensitive personal information will be protected and a cybersecurity program can help employees feel secure. Business partners want assurance that their information, systems and networks are not put at risk when they connect to and do business with your SMM firm.

Demonstrating to potential business partners that you have a method to protect their information can help grow your business relationships. Developing or improving your cybersecurity program will also make it easier for your company to innovate – taking advantage of new technologies that can lower costs while delivering better services to your customers.

It is not possible for any business to be completely secure. But, it is possible — and reasonable — to implement a program that balances security with the needs and capabilities of your SMM firm. This guide provides SMMs with basic practices and tools needed to develop a cybersecurity program.



Source: Sikich M&D REPORT 2019

Understanding the Risks to Your SMM Firm

Risk is a function of threats, vulnerabilities, the likelihood of an event and the potential impact an event would have on your SMM firm. Most of us make risk-based decisions every day. While driving to work, we assess threats and vulnerabilities such as weather and traffic conditions, the skill of other drivers on the road and the safety features and reliability of the vehicle we drive.

By understanding your risks, you can know where to focus your efforts. While you can never eliminate your risks, the goal of your cybersecurity program is to give reasonable assurance you have made informed decisions related to the security of your information.

It is impossible to completely understand all your risks perfectly. There will be many times when you will have to make a reasonable effort when trying to understand threats, vulnerabilities, potential impact and likelihood. For this reason, it is important to utilize all resources available to you, including information sharing organizations (visit the Department of Homeland Security website for more information) relevant stakeholders and knowledge experts.

Three Elements of Risk

Threats

Anything that might adversely affect the information your business needs to operate. Threats might come in the form of people or natural events and they can be accidents or intentional. Some of the most common information security threats include:

- Environmental, such as fire, water, tornado or earthquake
- Business resources, such as equipment failure, supply chain disruption or employees
- Hostile actors, such as hackers, hacktivists, criminals or nation-state actor
- Insider threats - employees and contractors

You may not have considered natural events as threats to your firm's information security, but what would happen if you had a flood in your office? Computers, servers and paper documents can be destroyed by even a small amount of water. If it is a large flood, you may not be allowed in the area to protect or collect the information your SMM firm needs to operate.

Vulnerability

A weakness that could be used to harm the business. Any time information is not being adequately protected it represents a vulnerability. Most information security breaches can be traced back to only a few types of common vulnerabilities.

This guide will help you minimize your vulnerabilities and reduce the impact of a security incident should one happen.

Some threats affect SMMs differently. For example, an SMM that sells products online may be more concerned about website defacement than a business with little or no web presence.

Likelihood

The chance a threat will affect your business and helps determine what types of protections to put in place.

Most SMMs have different types of business information. If a marketing pamphlet is leaked online, it will probably not harm the business nearly as much as if, for example, sensitive customer information or proprietary business data was leaked.

The impact an event could have depends on the information affected and on the nature of the SMM's business.

MEP National Network Helps Small Manufacturers

"Going through this process was great for our organization," said Zach Mottl, Chief Alignment Officer for Atlas Tool. "It's all about developing good habits." As a small business, Atlas Tool was accustomed to creating workarounds to simplify administrative practices, but that is not an option when it comes to cybersecurity.

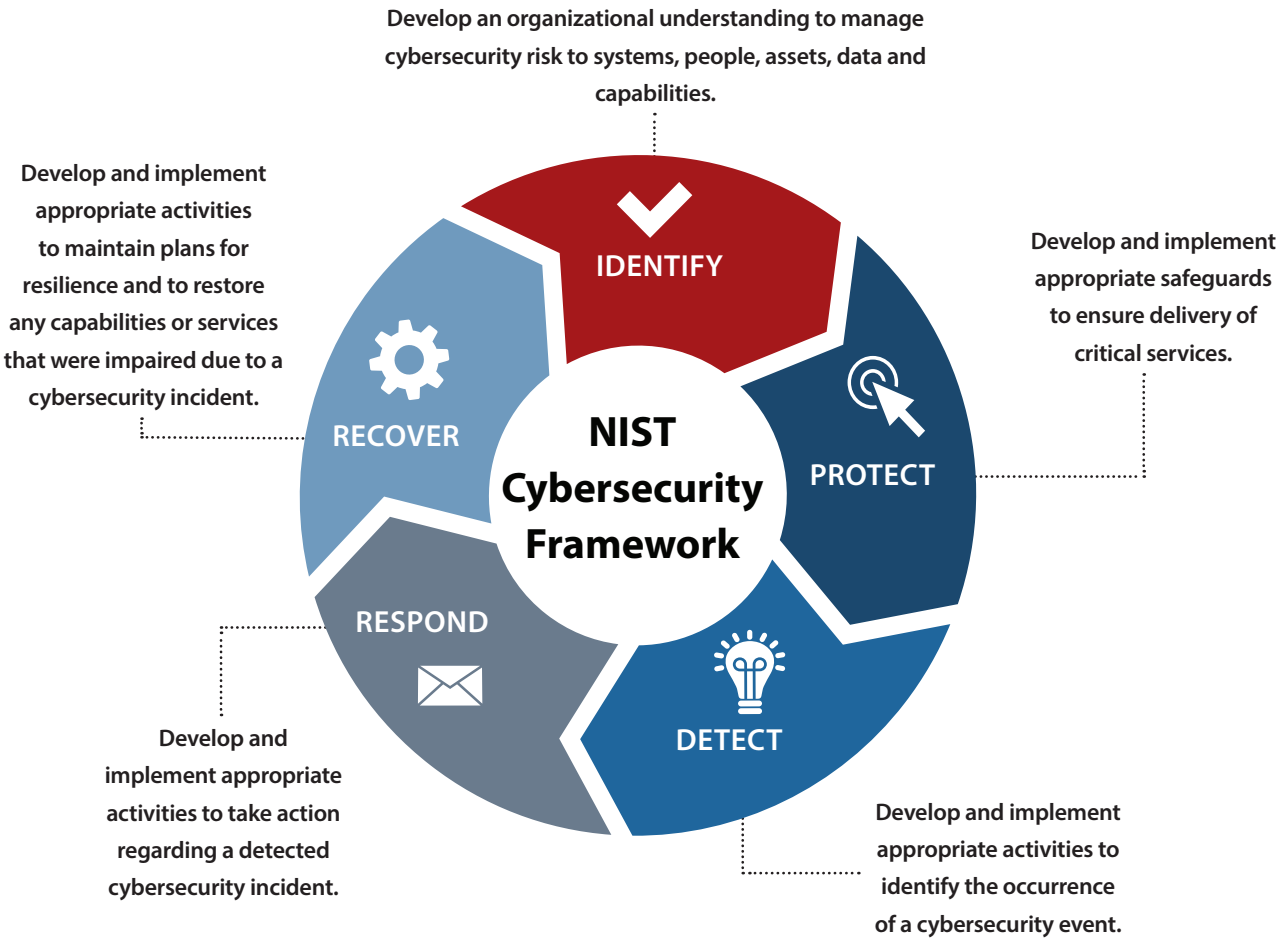
The company worked with IMEC (MEP Center in Illinois) to provide workforce training helping Atlas Tool employees understand the security precautions and reporting protocols. The requirements ensure Atlas Tool is protecting its data, preventing intrusions and notifying the appropriate people in the event of a security compromise.

"Addressing the compliance requirements was important for us to become a more robust and secure organization," said Mottl. "I know all businesses would benefit from the assessment, not just defense contractors."

Protecting Your SMM Firm

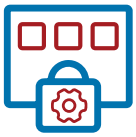
The *Framework for Improving Critical Infrastructure Cybersecurity* (the "NIST Cybersecurity Framework") helps organize the processes and tools you should consider in protecting your information. This is not a one-time process, but a continual, ongoing set of activities.

There are some common practices you and your employees can implement to help keep your SMM firm safe. The specific mitigation activities in this section are grouped into the five broad categories of the Cybersecurity Framework.



IDENTIFY

The activities in the Identify Function help increase your SMM firm's understanding of resources and risks.



Identify and control who has access to your SMM firm's information

Control who has or should have access to your SMM firm's information and technology. Know what type of access each employee has and include both physical and logical access. Employees may have a key or administrative privilege or a password that is required to gain access. To help collect this information, review your list of accounts and what privileges those accounts have. Be aware of anyone who has access to your SMM firm.

> *Do not allow unknown or unauthorized persons to have physical access to any of your firm's computers.*

This includes cleaning crews and maintenance personnel. Do not allow computer or network repair personnel to work on systems or devices unsupervised. No unrecognized person should be able to enter your office space without being questioned by an employee. If a criminal gains physical access to an unlocked machine, they can steal any private or sensitive information on that machine with relative ease.

Physically lock up your laptops and other mobile devices when they are not in use. Use the session lock feature included with many operating systems, which locks the screen if the computer is not used for a specified period (e.g., 2 minutes). Use a privacy screen or position each computer's display so that people walking by cannot see the information on the screen.

*Conduct background checks**

Do a full, nationwide criminal background check, sexual offender check and if possible, a credit check on all prospective employees, especially if they will be handling your business funds.

Consider doing a background check on yourself. Many SMM owners or executives become aware that they are victims of identity theft only after they do a background check on themselves. You may find reported arrest records and unusual previous addresses where you never lived. This can be an indication that your identity has been stolen.

If prospective employees are applying for a job with educational requirements, call the schools they attended and verify their actual degree(s) or certificates(s), date(s) of graduation and GPA(s). If they provided references, call those references to verify the dates they worked for a company and other specifics to ensure the prospective employee is being honest.

**Be sure follow your state's laws regarding prospective employee background checks.*

Require individual user accounts for each employee

Set up a separate account for each user (including any contractors needing access) and require strong, unique passwords be used for each account. **Without individual accounts for each user, you may find it difficult to investigate data loss or unauthorized data manipulation.**

Ensure all employees use computer accounts without administrative privileges to perform typical work functions. This will hinder any attempt — intentional or not — to install unauthorized software. Consider using a guest account with minimal privileges (e.g., Internet access only) if needed for your SMM firm.

More than 2 million cyber incidents in 2018 collectively caused at least $45 billion in losses and it's probably worse than that because many incidents go unreported.

Source: 2018 Cyber Incident & Breach Trends Report - Online Trust Alliance

Create policies and procedures for information security

Policies and procedures are used to identify acceptable practices and expectations for business operations, can be used to train new employees on your information security expectations and can aid an investigation in case of an incident. These policies and procedures should be readily accessible to employees – (i.e. in an employee handbook or manual).

The scope and breadth of policies is largely determined by the type of business and the degree of control and accountability desired by management. Have a legal professional familiar with cyber law review the policies to ensure they are compliant with local laws and regulations.

Policies and procedures for information security and cybersecurity should clearly describe your expectations for protecting your information and systems. These policies should identify the information and other resources that are important and should clearly describe how management expects those resources to be used and protected by all employees. Examples of policies are readily available online and a legal, insurance or cybersecurity professional may have examples of policies as well.

All employees should sign a statement agreeing they have read the policies and relevant procedures and they will follow these policies and procedures. If there are penalties associated with violating the policies and procedures, employees should be aware of them. The signed agreement should be kept in the employee's Human Resource file.

Policies and procedures should be reviewed and updated at least annually and as there are changes in the organization or technology. Whenever the policies are changed, employees should be made aware of the changes and sign the new policy acknowledging their understanding. This can be done in conjunction with annual training activities.

PROTECT

The Protect Function helps limit or contain the impact of a potential information security or cybersecurity event.

Limit employee access to data and information

Don't allow any employee to have access to all of the SMM firm's information or systems, such as financial, personnel, inventory or manufacturing information or systems. Employees should only have access to the systems and specific information needed to do their jobs. **Do not allow a single individual to both initiate and approve a transaction, financial or otherwise. This includes executives and senior managers.**

Insiders – employees or others who work for an SMM – are a main source of security incidents. Because they are trusted and have been given access to important business information and systems, they can easily cause harm either deliberately or unintentionally. Unfortunately, these types of insider threats can be difficult to detect, so protecting against them is very important.

When an employee leaves the SMM, remove their access to the SMM's information or systems. This may involve collecting their ID badge, deleting their username and account from all systems, changing any group passwords or combination locks they may have known and collecting any keys they were given.

95% of all breaches could have been avoided through simple and common-sense approaches to improving security.

Source: 2018 Cyber Incident & Breach Trends Report - Online Trust Alliance

Install surge protectors and Uninterruptible Power Supplies (UPS)

Surge protectors prevent spikes and dips in power from damaging your electronic systems. An Uninterruptible Power Supply (UPS) provides a limited amount of battery power to allow you to work through short power outages and provides enough time to save your data when the electricity goes off. A UPS often provides surge protection as well. Make sure the size and type of UPS meets the needs of your SMM firm.

Ensure each of your computers and critical network devices are plugged into a UPS. Plug less sensitive electronics into surge protectors. Test and replace the UPS and surge protector as recommended by the manufacturer.

Patch your operating systems and applications

Any software application, including operating systems, firmware or plugin installed on a system, could provide the means for an attack. Only install those applications you need to run your SMM firm and patch or update them regularly. Many software vendors provide patches and updates to their supported products to correct security concerns and improve functionality. Update and patch all software on each device you own or use.

> *Vendors are not required to provide security updates for unsupported products. For example, Microsoft ended support for Windows XP on April 8, 2014 and no new patches will be provided for that operating system, even though it has known vulnerabilities.*

When you purchase new computers, check for updates immediately. Do the same when installing new software. You should only install a current and vendor-supported version of software.

It may be useful to assign a day each month to check for patches. There are products which can scan your system and notify you when there is an update for an application you have installed. If you use one of these products, make sure it checks for updates for every application you use. You can check for updates directly with the original manufacturers of the applications you have installed.

Install and activate software and hardware firewalls on all your business networks

Firewalls can be used to block unwanted traffic such as known malicious communications or browsing to inappropriate websites, depending on the settings. Install and operate a hardware firewall between your internal network and the Internet. This may be a function of a wireless access point/router or it may be a function of a router provided by your Internet Service Provider (ISP). There are many hardware vendors that provide firewall wireless access points/routers, firewall routers and separate firewall devices. Install anti-virus software on the firewall.

Malware (short for Malicious Software or Malicious Code) is computer code written to steal or harm.

For these devices, change the administrative password upon installation and regularly thereafter. **Consider changing the administrator's log-in as well. The default values are typically known or easily guessed and if not changed, may allow hackers to control your device and monitor or record all your communications and data via the Internet.**

Install, use and regularly update a software firewall on each computer system used in your SMM firm (including smart phones and other networked devices if possible). If given the option, ensure logging is enabled as this will aid in the investigation of an event by providing evidence. Many operating systems include a firewall, but you should ensure that the firewall is operating and logging activity.

> *You should only use a current (updated), authentic and vendor-supported version of the hardware and software firewall.*

It is necessary to have firewalls on each of your computers and networks even if you use a cloud service provider (CSP) or a virtual private network (VPN). If employees can do any kind of work at home, ensure home network and systems have hardware and software firewalls installed and are operational. Employees should perform regular updates.

In addition to a basic hardware firewall, you may want to consider installing an Intrusion Detection / Prevention System (IDPS). These devices analyze network traffic at a more detailed level and can provide a greater level of protection.

Secure your wireless access point and networks

If you use wireless networking, set up your router as follows (view the owner's manual for directions on how to make these changes):

- Change the administrative password that was on the device when you received it
- Set the wireless access point so that it does not broadcast its Service Set Identifier (SSID)
- Set your router to use WiFi Protected Access 2 (WPA-2), with the Advanced Encryption Standard (AES) for encryption. Do not use WEP (Wired-Equivalent Privacy) as it is not considered secure

If your SMM firm provides wireless Internet access to customers or visitors, ensure it is separated from your business network.

Avoid connecting to unknown, unsecured or "guest" wireless access points, even for performing non-business activities. Access only those wireless access points that you own or trust. If you or your employees must connect to unknown networks or conduct work from home, consider implementing an encrypted VPN capability, which will allow for a more secure connection.

Set up web and email filters

Email filters can help remove emails known to have malware attached and prevent your inbox from being cluttered by unsolicited and undesired email or spam. Email providers may offer this capability. If your SMM firm hosts your own email servers, use filtering if possible.

Similarly, many web browsers allow web filtering, notifying the user if a website may contain malware and potentially preventing them from accessing that website. Enable this option if available.

90% of malware is delivered via email and all it takes is one wrong click to compromise your business.

Source: 2019 Data Breach Investigations Report, Verizon

You may want to consider blocking employees from going to websites that are frequently associated with cybersecurity threats. This may include sites with pornographic content or social media. This can help prevent employees from accidentally downloading malware, wasting business resources and conducting illicit activity using business resources. Many firewalls and routers can be set up to block, or "blacklist," certain addresses or to allow, or "whitelist," certain addresses. Blacklists can be downloaded online or obtained as part of a service.

Use encryption for sensitive business information

Encryption is a process of making your electronically stored information unreadable to anyone not having the correct password or key. Use full-disk encryption — which encrypts all information on the storage media – on all of your computers, tablets and smart phones. Many systems come with full-disk encryption capabilities. Not all mobile devices provide this capability.

Do not forget your encryption password or key! If you lose or forget your key, you will lose your information. Save a copy of your encryption password or key in a secure location separate from where your backups are stored.

If you send sensitive documents or emails at your SMM firm, you may want to consider encrypting those documents and/or emails. Many document and email applications provide for this capability. Typically, the receiver will need to have the same application to decrypt the message or document as you used to encrypt it. If you need to send them a password or key, give it to them via phone or other method. Never send it in the same email as the encrypted document.

Dispose of old computers and media safely

Small manufacturers sell, throw away or donate old computers and media. When disposing of old business computers, first electronically wipe the hard drive(s). Many operating systems provide this capability and there are several downloadable applications that can also do this. If you can't wipe the hard drive for any reason, consider degaussing the hard drive.

After wiping the hard drive(s), remove them and have them physically destroyed. You can sell, donate or recycle the machine after the hard drive has been removed. Many companies will crush or shred them for you. Consider choosing companies that will allow you to watch the process.

Install a remote-wiping application on your computer, tablet, cell phone and other mobile device. If the device is lost or stolen, you can use these applications to wipe all information from the device.

When disposing of old media such as compact disks (CDs) and Universal Serial Bus (USB) flash drives, first delete any sensitive business or personal data. Then destroy the media either by shredding it or taking it to a company that will shred it for you. When disposing of paper containing sensitive information, destroy it by using a crosscut shredder.

You may want to consider incinerating paper and other media that contain very sensitive information.

Train your employees

Train employees immediately when hired and at least annually thereafter about your information security policies and what they will be expected to do to protect your business's information and technology. Have employees sign a statement that they will follow your policies and that they understand the penalties for not following your policies.

Train employees on:

- What they can use business computers and mobile devices for, such as if they can use them to check their personal email
- How they are expected to treat customer or business information, such as whether they can take that information home with them
- What to do in case of an emergency or security incident
- Basic practices

Continually reinforce the training in everyday conversations or meetings. Monthly or quarterly training, meetings or newsletters on a specific subject can help reinforce the importance of security and develop a culture of security.

Employee training is critical when it comes to cybersecurity. Training teaches employees to understand vulnerabilities and threats to business operations.

DETECT

The activities under the Detect Function allow timely discovery of information security or cybersecurity events.

Install and update anti-virus, anti-spyware and other anti–malware programs

Malware (short for Malicious Software or Malicious Code) is computer code written to steal or harm. It includes viruses, spyware and ransomware. Sometimes malware only uses up computing resources (e.g., memory), but other times it can record your actions or send your personal and sensitive information to cyber criminals.

34% of all documented cyberattacks targeted manufacturers.

Source: Global Threat Intelligence Center 2017 Q2 Threat Intelligence Report, NTT Security

Install, use and regularly update anti-virus and anti-spyware software on every device throughout your SMM firm (including computers, smart phones and tablets).

It may be useful to set the anti-virus and anti-spyware software to automatically check for updates at least daily (or in "real-time", if available) and then set it to run a complete scan soon afterwards. Many businesses run their anti-virus programs at some scheduled time each night (e.g., midnight) and schedule a virus scan to run about half an hour later (e.g., 12:30 a.m.); then they run their anti-spyware software (e.g., 2:30 a.m.) and run a full system scan (e.g., 3:00 a.m.). This assumes that you have an always-on, high-speed connection to the Internet. Regardless of the actual times for the updates and scans, schedule them so that only one activity is taking place at any given time.

If your employees do any work from home using their own computers or personal devices, obtain copies of your business anti-malware software for those systems or require your employees to use anti-virus and anti-spyware software.

You may want to consider using two different anti-virus solutions from different vendors. This can improve the chances a virus will be detected. Often, routers, firewalls and IDPSs will have some anti-virus capabilities, but these should not be exclusively relied upon to protect the network.

Maintain and monitor logs

Protection/detection hardware or software (e.g., firewalls, anti-virus software) often has the capability of keeping a log of activity. Ensure this function is enabled — you may want to check the operating manual for instructions on how to do this. Logs can be used to identify suspicious activity and may be valuable in case of an investigation. Logs should be backed up and saved for at least a year and some types of information may need to be stored for a minimum of six years.

You may want to consider having a cybersecurity professional review the logs for any unusual or unwanted trends, such as a large use of social media websites or an unusual number of viruses consistently found on a computer. These trends may indicate a more serious problem or signal the need for stronger protections.

Logs should be backed up and saved for **at least one year** and some types of information may need to be stored for a **minimum of six years**.

RESPOND

The Respond Function helps contain or reduce the impact of an event.

Develop a plan for disasters and information security incidents

Develop a plan for what immediate actions you will take in case of a fire, medical emergency, burglary or natural disaster. The following section highlights elements that should be included in the plan.

Roles and responsibilities.

Who makes the decision to initiate recovery procedures and who will be the contact with appropriate law enforcement personnel.

What to do with your information and information systems in case of an incident.

This includes actions such as shutting down or locking computers, moving to a backup site and physically removing important documents.

Who to call in case of an incident.

This should include how and when to contact senior executives, emergency personnel, cybersecurity professionals, legal professionals, service providers or insurance providers. Be sure to include relevant contact information in the plan.

Many states have "notification laws," requiring you to notify customers if there is a possibility any of their information was stolen, disclosed or otherwise lost.

Make sure you know the laws for your local area and include relevant information in your plans.

Include when to notify appropriate authorities. If there is a possibility that any personal information, intellectual property or other sensitive information was stolen, you should contact your local police department to file a report. In addition, you may want to contact your local FBI office.

Types of activities that constitute an information security incident.

This should include activities such as your SMM firm's website being down for more than a certain length of time or evidence of information being stolen.

You may want to consider developing procedures for each job role describing exactly what the employee in that role will be expected to do if there is an incident or emergency.

RECOVER

The Recover Function helps an organization resume normal operations after an event.

Make full backups of important business data/information

Conduct a full, encrypted backup of the data on each computer and mobile device used in your SMM firm at least once a month, shortly after a complete virus scan. Store these backups away from your office location in a protected place so that if something happens to your office — such as a fire, flood, tornado or theft — your data is safe. Save a copy of your encryption password or key in a secure location, separate from where your backups are stored.

Backups will let you restore your data in case a computer breaks, an employee makes a mistake or a malicious program infects your system. Without data backups, you may have to recreate your business information manually (e.g., from paper records). **Data that you should backup includes, but is not limited to, word processing documents, electronic spreadsheets, databases, financial files, human resources files, accounts receivable/payable files, system logs and other information used in or generated by your SMM firm.** Back up only your data, not the software applications themselves.

You can easily store backups on removable media, such as an external USB hard drive or online using a Cloud Service Provider (CSP). If you choose to store your data online, do your due diligence when selecting a CSP. It is recommended that you encrypt all data prior to storing it in the Cloud.

If you use a hard drive, ensure it is large enough to hold all your monthly backups for a year. It is helpful to create a separate folder for each of your computers. When you connect the external disk to your computer to make your backups, copy your data into the appropriate designated folder.

Test your backups immediately after generating them to ensure the backup was successful and you can restore the data if necessary.

Make improvements to processes, procedures and technologies

Regularly assess your processes, procedures and technology solutions according to your risks. Make corrections and improvements as necessary. You may want to consider conducting training or table-top exercises, which simulate or run-through a major event scenario to identify potential weaknesses in your processes, procedures, technology or personnel readiness. Make corrections as needed.

Make incremental backups of important business data/ information

Conduct an automatic incremental or differential backup of each of your company's computers and mobile devices at least once a week. This type of backup only records any changes made since the last backup. In some cases, it may be prudent to conduct backups every day or every hour depending on how much information is changed or generated in that time and the potential impact of losing that information. Many security software suites offer automated backup functions that will do this on a regular schedule for you.

In general, the storage device should have enough capacity to hold data for 52 weekly backups, so its size should be about 52 times the amount of data that you have.

Backups should be stored on:

- removable media, such as an external USB hard drive;
- a separate server that is isolated from the network, or
- online storage, such as via a CSP.

Remember, this should be done for each of your computers and mobile devices. You may choose to store your backups in multiple locations (e.g., one in the office, one in a safety deposit box across town and one in the Cloud). This provides additional security in case one of the backups becomes destroyed.

Periodically test your backed-up data to ensure that you can read it reliably. If you don't test your backups, you will have no grounds for confidence that you can use them in the event of a disaster or security incident.

You may want to consider encrypting your backups. Many software applications will allow you to encrypt your backups. This provides an added layer of security and is important if your backups contain any sensitive personal or business information. Make sure to keep a copy of your encryption password or key in a secure location separate from where you keep your backups.

Consider cyber insurance

Cyber insurance is similar to other types of insurance, such as flood or fire insurance, that you may have for your SMM firm. Cyber insurance may help you respond to and recover from a security incident. In some cases, cyber insurance companies may also provide cybersecurity expertise and help you identify where you are vulnerable, what kinds of actions you need to take to protect your systems and help you investigate an incident and report it to appropriate authorities.

As you might, with any type of insurance, perform due-diligence when considering cyber insurance. Determine your risks before purchasing a policy. Research the company offering protection, the services they provide, the type of events they cover, ensure that they have a good reputation and will be able to meet their contractual agreement.

NIST Cybersecurity Framework Steps

1. Identify

- Identify and control who has access to business information
- Conduct background checks
- Require individual user accounts for each employee
- Create policies and procedures for cybersecurity

2. Protect

- Train employees and limit employee access to data
- Install surge protectors and uninterruptible power supplies
- Patch operating systems and applications routinely
- Install and activate firewalls on all business networks
- Secure wireless access points and networks
- Set up web and email filters
- Use encryption for sensitive information
- Dispose of old computers and media safely

3. Detect

- Install and update anti-virus, anti-spyware, and other anti-malware programs
- Maintain and monitor logs
- Note unusual password activity

4. Respond

- Develop and maintain a plan for disasters and cyber incidents
- Notify your customers and the authorities

5. Recover

- Make full backups of important business data and information
- Schedule incremental backups
- Improve processes, procedures, and technologies

THE MEP NATIONAL NETWORK

The MEP National Network is a unique public-private partnership that delivers comprehensive, proven solutions to U.S. manufacturers, fueling growth and advancing U.S. manufacturing.

MEP National Network™

100 Bureau Drive, Stop 4800
Gaithersburg, MD 20899

301.975.5020

patricia.toth@nist.gov

WWW.NIST.GOV/MEP/MEP-NATIONAL-NETWORK.COM