9 Elements of Cybersecurity for Small and Medium-Sized Manufacturers

Small and medium manufacturers (SMM) must manage myriad challenges throughout their ongoing operations, with cybersecurity and available resources among the most significant.

Unfortunately, when these two challenges intersect, it leaves SMMs especially vulnerable to cyberthreats capable of disrupting operations or outright crippling businesses from the resulting damage.

The statistics paint a stark picture and show no SMM is threat-free:

- 43% of cyberattacks target small businesses
- 54% of small businesses think they're too small for a cyberattack
- There was a 424% increase in new small business cyber breaches last year
- 54% of small businesses don't have a plan in place for reacting to cyberattacks
- 47% of small businesses say they have no understanding of how to protect themselves against cyberattacks

To help alleviate the digital burdens SMMs face, we've compiled a guide covering the nine most accessible and proactive cybersecurity measures.

#1 Employee Cybersecurity Training

All cybersecurity depends on people, processes, and technology. These three elements comprise the tripod that supports all IT infrastructure—and when one cannot stand, none can.

Within that trio, people have the most interesting role. They are simultaneously the weakest link in any cybersecurity program—as the most vulnerable and susceptible to threats—and the easiest factor to strengthen into a robust and reliable pillar through dedicated training.

Tactics for Cyber Awareness and Training

Is cybersecurity hard to adopt? Not with the right training.

Employee cybersecurity training helps develop a culture of digital threat awareness and prevention without taxing resources and team bandwidth too severely. It's the most accessible and easiest path toward a more secure workplace.

The key to an effective training program is consistency, followed closely by buy-in. SMMs can't expect employees to learn and adopt numerous best practices in a single sitting alone, and information overload can negate a training program's effectiveness entirely.

Mirroring the tripod of people, processes, and technology, any SMM can adopt a three-pronged training approach across:

- **Annual awareness and new hire training** – At a minimum, thorough sessions should be held during onboarding processes and again annually to refresh or update knowledge. Employees should be reminded of best practices and updated on current threats. Training will also help SMMs consistently meet potential compliance obligations.
    - For example, the CMMC for Department of Defense suppliers requires the protection of federal contract information (FCI) and controlled unclassified information (CUI). Other compliance frameworks may pertain to personally identifiable information (PII), such as health records (i.e., HIPAA) or credit card data (i.e., the PCI DSS).
- **Covering cybersecurity topics in safety meetings** – A few minutes can be set aside for cybersecurity refreshers in regular safety meetings (e.g., weekly, monthly). For more frequent sessions, information should be digestible, building upon previous discussions. Employees are much less likely to retain information if asked to remember too many action points or diverse topics. Instead, consider:
    - Every few weeks, encourage employees to lead the training. Few learning methods surpass teaching others, and employee-led training inherently helps foster buy-in and a proactive cybersecurity culture. Between leading sessions and regular engagement, best practices will stay top-of-mind.
    - To generate further buy-in, recognize and incentivize those who facilitate training. Rewards can relate to time off, upcoming raises, and various eligibilities.
- **Workplace reminders** – Various reminders of cybersecurity best practices and threats can be posted around facilities as passive support. These reminders should be quick takeaways or framed to make them easy to remember.
    - For example, Ernie Edmonds, Sr. Managing Consultant of Cyber Physical Security Services at [REDACTED], has promoted phrases including “passwords are like toothbrushes; you don’t share them.”

    - Remind employees “call and confirm” whenever they’re asked for sensitive data or to perform suspicious financial transactions. It could be a phishing attempt (i.e., impersonation scamming), and calling the sender directly to confirm legitimacy requires hardly any time.

By adopting an effective cybersecurity training program, SMMs can readily enhance 33% of their protections against digital threats—their people.

#2 Small Business Architecture

How an SMM builds its IT architecture (i.e., the foundational design of an organization’s IT infrastructure) dramatically affects its resilience against cybersecurity threats.

The most vulnerable architecture is a "flat topography"—or a lack of hierarchical network and multi-layer resource segmentation. Everything is collectively grouped "within the same bucket," regardless of priority.

Unfortunately, most SMMs’ architecture is flat.

If a digital intruder can be thought of as an invader, establishing hierarchical network segmentation is akin to constructing a series of increasingly insurmountable walls. While most commercially available firewalls will not enforce these barriers, those that do are not expensive, and open source options exist as well (e.g., pfSense, OPNsense).

The Vulnerabilities of Flat-Topography Architecture

In flat IT topographies, all systems, applications, data, and other resources are provided the same level of security and concern on a given network—from mission-critical databases to an Amazon Fire Stick used for entertainment in the employee breakroom.

The dangers are apparent. If a cyberthreat can access or compromise one of the two, managing a hacked Fire Stick is preferred.

Because of how networks are connected, flat topographies mean that once any resource is compromised, any other can be too. They do not enforce any additional barriers regardless of how essential a given resource is.

Start Away from the Technology

The first step of constructing IT infrastructure actually begins separately from technology tasks.

SMMs building or reviewing their architecture should start by assessing their various systems, applications, data, and other resources according to mission-critical importance, sensitivity, and value. As a reference guide for cybersecurity, manufacturing industry members can utilize the National Institute of Standards and Technology's (NIST) "Five Functions" from its Cybersecurity Framework:[1]

- Identify
- Protect
- Detect
- Respond
- Recover

Those categorized as the highest priority must be segmented away from things that will not affect operations nearly as much should they be compromised.

Multi-Layer or "Trust Zone" Architecture

The easiest way to approach hierarchical or multi-layered architectures is with zones named after recognizable traffic light colors: green, yellow, and red.

Essential resources should be secured in a "green zone" that heavily restricts access as needed, so only authorized individuals and devices can interact or communicate with them. All others can be located in more accessible zones (e.g., a "yellow zone," a "red zone"). Since the flow of information can only occur in a set number of ways, it's easier to restrict with designated zones.

For example, resources from the green zone can communicate to those in red, but the reverse is not allowed. In that case, if the red zone is compromised, green remains protected.

If resources or data storage contains information belonging to multiple zones, always secure it within the most protective to be safe.

This architecture is also called "multi-tiered protection layer topology" or "trust zone topology."

It provides an incredibly effective method for enhancing nearly every aspect of cybersecurity, protecting data and resource availability, integrity, and confidentiality. If SMMs don't have the personnel or bandwidth to build configuring trust zone topology, third-party cybersecurity consultants and providers are also available.

[1] NIST. *The Five Functions.* https://www.nist.gov/cyberframework/online-learning/five-functions

#3 Malware Prevention

Malware refers to any malicious software that can infect and damage networks or devices. Common types of malware include:

- Viruses
- Worms
- Trojan viruses
- Spyware
- Adware
- Ransomware

As a simple but essential aspect of any cybersecurity program, all SMMs should implement malware protections.

Tactics for Protecting Against Malware

Although malware remains one of the most widespread digital threats to SMM's cybersecurity, readily accessible and affordable solutions are available:

- **Listing Services** – Listing services allow organizations to differentiate between good and bad programs, websites, or network traffic. They can also be called "default deny lists," "default allow lists," "blacklisting," or "whitelisting." If malware does not match what is allowed by listing services, it will not be able to run. Listing services can be used to restrict access to:

    - Core programs and applications like web browsers and Microsoft Office

    - Role-specific resources—such as Visio for engineers and QuickBooks for accountants—determined by network permissions and group memberships in Microsoft's Active Directory (AD) or via Carbon Black, App Locker, or other services

    - Anything else—including malware or installers for unapproved applications—can be implicitly denied (or unless specific request processes are adhered to)

- **General malware protection software** – Most commonly known as "antivirus software," these programs prevent, detect, and remove malware. Today's malware protection software has evolved far beyond early antivirus programs and can be categorized according to how it operates:

    - Threat signature detection – These programs rely on a database of known malware code and attributes that they scan for and recognize among incoming traffic. While cloud-based or software-as-a-service (SaaS) offerings should update automatically, the database of threat signatures must remain current for this protection to stay effective.

    - Heuristic or artificial intelligence – As the more evolved malware protection software, these programs establish baseline user and traffic behaviors and configurations. Any deviations are detected and addressed or contained for cybersecurity professionals to investigate.

- **Monitoring and response** – Software cannot perform the entire job independently. Dedicated cybersecurity professionals must be available to sift through alerts, check for improperly flagged instances (i.e., "false positives"), and respond or adjust configurations. If full-time, dedicated staff is not possible, SMMs can hire third parties as "managed security service providers" (MSSPs).

#4 Home Office and Mobile Devices

Especially following the rapid rise in remote work, SMMs must ensure that employee devices and home networks are as secure as their own.

Location is ultimately irrelevant to the rigors of cybersecurity. The same network architecture, malware protection, and configuration best practices apply to at-home computers and laptops, as well as personal devices and mobile phones:

- **Network segmentation** – Easily achieved with two Wi-Fi networks, the same trust zone topology segments personal from professional digital activity at home. If either is compromised, the damage won't spread. More complicated measures like traffic forwarding exist, but anyone can recreate it with two different Wi-Fi devices. Merely plug a new Wi-Fi device and ethernet cable into the appropriate port on the old one.

- **Use separate devices** – Once a device is compromised or infected with malware, additional cybersecurity measures such as virtual private networks (VPNs) or multifactor authentication (MFA) may no longer provide protection. If a personal machine or device connected to an SMM's network is infected, so will the network.

- **Implement strict device policies** – The most reliable method for securing IT environments with remote employees is to provide them with all the hardware. While “bring-your-own-device” (BYOD) policies allowing personal hardware for work have become more popular, they significantly exacerbate cybersecurity risk. Instead, SMMs should:

    - Meet all hardware needs employees have and require strict usage policy adherence. With dedicated work devices, management, listing services, and other security configurations are much easier.

    - If SMMs decide to adopt a BYOD policy, they should specify that no "jailbroken" or "rooted" devices will be allowed to connect to company networks. Jailbreaking or rooting refers to gaining full administrative access to the device and its operating system. Any intruder will have complete control over a jailbroken or rooted phone if compromised.

#5 Adopt Zero Trust Policies and Mindset

"Zero trust" simply means adopting configurations and policies where trust is not implicitly granted to users, devices, and network traffic.

Instead of "trust but verify," it's "verify then trust."

If an employee, device, or other traffic tries to access the network or IT resources, the zero-trust approach relies on:

- A policy engine computer – Evaluates whether or not they should have access
- A policy enforcement computer – Grants or denies access

For effective zero trust, the policy engine and enforcement computers must continuously evaluate legitimacy while referencing identified patterns of behavior (e.g., user activity, login dates and times), IP address locations, user permissions and AD group memberships, and VPNs.

Tactics for Implementing Zero Trust

The sudden rise in zero trust adoption is partly fueled by a recent government mandate that will soon require it for all government and third-party contractor activity. As a result, zero trust will become a cybersecurity compliance obligation for SMMs holding government contracts—although it’s critical to note this policy is not yet enforced.

However, cybersecurity and other IT vendors will begin increasingly referencing zero trust, so SMMs should be familiar with the term and concept.

Returning to the adoption of cybersecurity best practices and regular training, a "verify before trusting" approach can be fostered among personnel easily. It *should* be incorporated into any malware or phishing identification training as a rule.

#6 Data Storage and Backups

Especially following the continuous rise of ransomware, SMMs may need to reconsider their data storage and backup processes and policies.

Ransomware involves malicious actors infiltrating networks to encrypt data and resources, preventing owners from accessing them. Encryption works by rendering data unreadable by people or computers without the associated cryptographic keys to convert it back.

Cloud storage platforms (e.g., DropBox) synchronize automatically, so backups are now more endangered. If infected or compromised devices and data are automatically synchronized, the backups probably are as well.

Tactics for Safe Data Storage and Backups

Fortunately, simple adjustments to data storage and backup policies enable full recovery for SMMs who may suffer a ransomware attack:

- **Local backups** – Performing a local backup to network areas that can't be rewritten preserves pristine data. With each backup, new versions of the data are stored—although this may require additional hardware and storage space investments. If rewrite access is never granted, ransomware can't gain the permissions necessary to encrypt backups.
    - This “write once, read many” practice was once referred to as a “worm drive.”

- **“Hot” and “cold” backups** – "Hot" backups are always live and performed in real-time but are difficult to access. They may require 30 minutes to restore, but hot backups enable relatively fast system and network recovery. In contrast, a "cold" backup is only powered on and live during instances where resources are being backed up or restored. It's powered off at all other times to prevent ever being compromised.

  - The best strategy is to run both hot and cold backups—ideally, more than one of each.

Ransomware has affected many organizations so severely that they later closed down from the consequences. Proper, safe data storage and backup practices will help prevent any SMMs from sharing the same fate.

#7 Monitoring and Incident Management

Monitoring activities provide SMMs with greater network and activity insight—from determining normal behaviors used as a baseline against suspicious activity to understanding IT resource usage and identifying cost savings.

Because malware prevention software cannot always catch every intrusion attempt and occasionally flags false positives, organizations need monitoring personnel to review all cybersecurity policies, processes, implementations, and configurations.

Given the statistics on cyberattacks targeting small to medium businesses (and a self-reported lack of preparation), SMMs must determine and adopt incident response policies and procedures.

Cyberattacks are a matter of “when, not if.”

After cybersecurity incidents are identified and assessed as legitimate threats, the personnel responsible for managing them should know their defined roles and tasks to best ensure swift containment, removal, and recovery.

Tactics for Monitoring and Incident Management

For effective monitoring and prompt incident management, cybersecurity teams require:

- **Extensive visibility** – Monitors and responders must have the capability to see and understand what is occurring, where, and who is causing it to make decisions on the appropriate response.

- **Comprehensive control** – Once a potential threat has been assessed, the security team must have the expertise, skills, tools, and permissions (e.g., administrative access) to quickly rectify and restore the situation.

- **Machine-speed orchestrated response** – Prompt responses will require machine assistance, such as from security information and event management (SIEM) systems.

- **Ongoing monitoring** – To proactively identify potential threats and vulnerabilities, SMM's cybersecurity programs should rely on SIEM and similar tools, alongside full-time or third-party professions.

A prompt response can be the difference between overcoming a cyberattack or not, so teams—internal or third-party—need to actively investigate potential threats and be well prepared for genuine intrusion attempts.

#8 Encryption

While ransomware threatens to encrypt organizations' resources and data to prevent access, proactive and well-managed encryption is immensely beneficial for protecting against malicious intruders and data loss or theft—whether it is stored on a network or device or is in transit.

As mentioned, encryption renders data unreadable unless the associated cryptographic keys are present to decrypt it. Since the data is unreadable, encryption can also be relied upon as a potential failsafe measure against compliance violations (e.g., CMMC, HIPAA, PCI DSS). If an intruder has accessed or stolen encrypted data, being unreadable prevents it from being compromised.

Any cryptographic keys should be governed by strict management policies and procedures and replaced periodically as a best practice. The loss of a cryptographic key means someone else may be able to decrypt the data, or—equally damaging—the owners can no longer read or use it.

Tactics for Encryption

Encryption can be applied at three levels, and a combination of each provides robust cybersecurity. Manufacturing industry businesses utilizing those levels, however, must distinguish between encrypting data at rest (i.e., device-level encryption) and data in transit or in use:

- **Data at rest** – "At rest" refers to encrypted data stored on physical or logical mediums (e.g., hard drives, USB flash drives, file servers, databases) and not currently being accessed. This prevents the consequences of theft or intrusive access when physical or logical mediums are powered off or not in use.

- **Data in transit** – “In transit” refers to encrypting data communicated internally or between external network locations (e.g., third-party service providers, processing a credit card payment).

- **Data in use** – "In use" refers to encryption for any data actively being accessed, read, updated, processed, or erased. Some databases support "in use" encryption—from parts of a single field to the entire schema and its contents, and with different cryptographic keys associated with each. Crucially, "at rest" encryption does not protect data in use. Both are necessary.

Although not as effective as encryption, “masking” can also hide data from users lacking the appropriate permissions.

#9 Multifactor Authentication (MFA)

Multifactor authentication (MFA) adds additional security steps to login processes. This ensures users are who they say they are, even if some element of their account or credentials have been comprised. It is sometimes called "two-factor authentication" (2FA), but MFA is predominately accepted as the proper umbrella term.

MFA is an essential cybersecurity measure, as one factor may be compromised (e.g., username and password), but access will not be granted without the other(s). As many platforms now support MFA, it should be considered a baseline cybersecurity measure to adopt.

MFA relies on a combination of “factors,” which identify individuals based on one of the following criteria:

- **Knowledge (“something you know”)** – Users must input a unique value that only they know, most commonly:

  - Conventional usernames and passwords
  - Personal identification numbers (PIN)

- **Possession (“something you have”)** – Users can verify their identity by providing a unique physical item, sometimes featuring time-based expiries (e.g., 30 seconds) before new values are generated, such as:

  - PIV cards or badges
  - Registered mobile phones with authenticator apps or one-time passwords (OTPs)

    - USB tokens.

- **Inherence (“something you are”)** – This factor generally refers to biological identity verification, including:

    - Fingerprints
    - Retina scanners
    - Facial recognition

Two or more of these factors must be used for an authentication process to be considered true MFA. As an example, debit cards provide the most universally relied-on form of MFA—the holder needs both the physical card (even if only for the number) and the associated PIN to make a payment.

While pin codes delivered via SMS or email loosely count as a form of MFA, they are the least secure, as devices can be cloned or messages redirected.

How [REDACTED] can Help SMMs with Cybersecurity

When looking to improve or overhaul cybersecurity programs, expert advice is especially beneficial for overcoming strained resources, knowledge, skills, and bandwidth. Seeking out the right assistance—whether it's from vendors, the government, or grants—is imperative.

As a trusted advisor providing solutions for all aspects of California’s manufacturing industry, [REDACTED] is here to help small and mid-sized manufacturers map out and assess the potential threats and pathways to secure digital infrastructure.

Further information on this topic can be heard by listening to [REDACTED] podcast series. Other technology and cybersecurity podcasts in the series have covered topics such as ransomware and robotics.

Contact us to learn more about our cybersecurity services.

Sources:

NIST. *The Five Functions.* https://www.nist.gov/cyberframework/online-learning/five-functions