International Society of Automation
Setting the Standard for Automation™

Updated September 2024

WHITE PAPER

Industrial Cybersecurity for Small- and Medium-Sized Businesses

A Practical Guide

CONTENTS

Executive Summary

Effective cybersecurity management is essential for all organizations, regardless of size. There are many standards and guidance documents available to help organizations determine a way forward.

This document is intended to provide a starting point for small- and medium-businesses (SMBs), particularly those that manage industrial processes and employ some level of automation. Specific examples include SMBs in the chemical and water and wastewater treatment sectors.

While it is generally accepted that Operational Technology (OT) system security requires different or additional measures than general-purpose Information Technology (IT) system security, it is also true that smaller companies might have difficulty implementing much of the available guidance.

Standards and practices are often based on the assumption that engineering and operations resources are available to define, implement, and monitor the technology, business processes, and associated controls. Unfortunately, this is often not the case. Smaller operations are typically not staffed to include such roles. It is more common to have broadly defined staff roles, with support and operation of IT systems as only part of an individual's responsibilities. Smaller companies may not even be fully aware of the risks they face or that they can contract for cybersecurity-related services. This guide is intended to identify the essential controls that need to be established.

SMBs need to understand their cybersecurity risk and to take action to reduce this risk, just as they do with other business risks. The absence of previous incidents, or the belief that the organization is not a likely target, is not sufficient justification for ignoring this issue.

SMBs can be at risk from a wide variety of threats, including amateur and professional hackers, environmental activists, disgruntled employees or contractors and even nation states or terrorists. In addition, many cybersecurity incidents are a result of accidents or unintentional actions. A company does not have to be a specific target to be affected.

The consequence to an SMB can vary tremendously based on the nature of operations and the vulnerabilities of each. It is essential that the underlying vulnerabilities are recognized and that these vulnerabilities be mitigated to minimize the likelihood of potentially dire events.

This document provides guidance based on well-established frameworks and standards. Further reference should be made to these frameworks and standards, focusing on the recommendations in this document.

Cybersecurity management is not a one-time activity. Like quality and safety management, cybersecurity management is an ongoing activity where continuous improvement must be made in order to manage the risks.

Why Cybersecurity Management is Important

PROTECTING BUSINESSES FROM THE IMPACT OF A CYBERSECURITY INCIDENT

Very few, if any, businesses today operate without some dependence on systems and equipment that are vulnerable to a cybersecurity incident. The impact to the business of such an incident will vary. However, this impact needs to be understood and managed accordingly if businesses are to be able to operate as expected.

There are two broad categories of systems and equipment: Information Technology (IT) and Operational Technology (OT), each with their own characteristics, as shown in the table below.

	Information Technology (IT)	Operational Technology (OT)
Definition	Used in a business or office environment to support day-to-day activities, such as accounting, ordering, human resources, and data analysis.	Used to monitor and control processes in industrial environments, such as factory floors, refineries, oil and gas platforms, and water treatment operations.
Examples of systems or equipment	• User workstations or laptops • File-, email-, or web-servers • Databases • Network devices (routers, firewalls, switches)	• Programmable Logic Controllers (PLCs) • Distributed Control Systems (DCSs) • Supervisory Control And Data Acquisition (SCADA) systems • Historian databases • Protocol and media converters
Cybersecurity concerns	Data confidentiality is the primary concern, followed by integrity of the data and system availability.	System availability is the primary concern, followed by integrity of the data, and finally, data confidentiality. In OT, data integrity and confidentiality are particularly important for device logic or configuration files used in control applications.
Management of Change	Change-control processes are largely self-contained within the IT function.	Technological changes are part of the overall Management of Change process. It can be difficult to take equipment out of service to update.
Other factors	• It is becoming more common for employees to use their own devices, especially mobile technology, to access business systems • New technologies are being adopted with insufficient concern for security	• Equipment and communications protocols tend to be proprietary, and it can be difficult to implement typical cybersecurity controls • Underlying technology can be antiquated and, therefore, more vulnerable to basic cybersecurity incidents • The equipment environment is almost always heterogeneous, with devices of various ages and sources

RISK ASSESSMENT

Cybersecurity-related risks are evaluated using a process that: systematically identifies potential vulnerabilities to valuable system resources and threats to those resources; quantifies loss exposures and consequences based on probability of occurrence; and (optionally) recommends how to allocate resources to countermeasures to minimize total exposure.

In simple terms, risk can be defined as a function of threat, vulnerability, and consequence. Each of these elements must be assessed in order to gain a full understanding of the situation.

Common threats

When considering cybersecurity threats, many consider only deliberate, targeted attacks from professional hackers. As a result, some dismiss the risk to their facilities.

The table below shows that SMBs are subject to numerous types of threats, both deliberate and otherwise. Cybersecurity incidents can arise as a result of accidents or unintentional actions by authorized individuals (employees, vendors, or contractors). Many threats are often non-targeted and SMBs can be impacted as collateral damage.

In all of the examples below, SMBs could be impacted indirectly, simply because they have equipment similar to the primary target.

Table 1 – Threat Examples

Threat	Description	Example
Amateur hackers	With access to many online tools and resources, anyone can find systems connected to the Internet and interfere with their operation, often for the challenge or prestige.	The online community HackForums.net is a popular forum for amateur hackers, and is believed to be behind the PlayStation network attack on Christmas Day 2014, as well as the attack on the Internet Name Servers in the Eastern USA in October 2016.
Professional hackers	Hackers with more skills and resources target organizations with ransom ware and other disruptive techniques and tools for profit.	In 2016, the Lansing Board of Water & Light was forced to pay a $25,000 ransom to unlock its internal communications systems, which were hit as part of a larger attack. The utility estimated the total cost of responding to the attack and strengthening its defenses against future attacks was $2.4M.
Environmental activists	Groups can work with hackers to disrupt the operations of organizations whose business practices they oppose or are contrary to their beliefs.	In 2011, the group Anonymous posted confidential information on 2,500 Monsanto employees and associates and shut down the company's international websites for nearly three days.
Disgruntled employees or contractors	Using inside knowledge or privileged access, to gain revenge by disrupting operations or to steal confidential information to be sold to competitors	In 2012, a male programmer—passed over for promotions at a Long Island power supply manufacturer—created an unauthorized program to harvest employees' logins and passwords. After leaving the company, the person used his credentials to get into the network and disrupt business and inflict damage on the company's operations.
Nation states or terrorists	Organizations with very large resources target critical infrastructure organizations to create instability or to influence their will.	In 2010, a virus known as Stuxnet compromised Iran's nuclear enrichment facility. The virus targeted the control system for the centrifuges in the facility and, while providing pre-recorded data to operators, would cause the centrifuges to operate outside of their normal envelope. Analysts suggest the enrichment program was set back several years as a result of the attack.
Accidents or unintentional actions	The actions of employees or contractors can inadvertently result in a cybersecurity incident.	In 1999, an explosion in a gasoline pipeline in Bellingham, WA, USA, killed three people, injured eight, and caused $45M in property damage. The company was fined $112M. One of the two primary causes of the incident was found to be developers making changes to a live control system.

Common vulnerabilities and key mitigations

A vulnerability is a deficiency that can be exploited by a threat to create an incident. The deficiency can arise from technical (such as a software error), procedural (a lack of policy or standard), or people (lack of training) issues.

A mitigation is an action or solution that is implemented to: reduce the likelihood of a vulnerability being exploited or offset the adverse effects of an incident should that vulnerability be exploited.

There are many cybersecurity vulnerabilities, and each organization possesses different ones depending on the equipment they use and the policies and procedures they have in place. As noted previously in this white paper, SMBs can be impacted by a non-targeted attack, simply because they utilize equipment similar to that used by the primary target. The table below provides a list of common vulnerabilities found in all organizations to some degree, along with key mitigations that should be implemented to control these vulnerabilities.

These key mitigations are essential for all SMBs to provide a basic level of cybersecurity management. It is highly recommended for SMBs to consider additional mitigations. Further guidance is available from several sources, including:

- International Society of Automation (ISA). The ISA/IEC 62443 standards (Security for Industrial Automation and Control Systems) provide detailed guidance on how to create a cybersecurity management system for OT environments. These standards are also available internationally as IEC 62443
- The US Chamber of Commerce [6], Department of Homeland Security (DHS) [7], US Small Business Administration (SBA) [9], National Institute of Standards and Technology (NIST) [10], as well as many business and technology websites [5], [8]
- The Center for Internet Security (CIS). CIS produces the Critical Security Controls [2], which identify the top 20 mitigations that reduce the likelihood and/or consequence of a cybersecurity incident. These controls are referenced in the Key Mitigations table below as CSC"xx" where "xx" is 1 to 20 (for example, CSC17)

Table 2 – Vulnerabilities and Mitigations

Vulnerability	Description	Key Mitigations
Inadequately trained employees	Employees who have received little or no training in the risks of cyber incidents are more likely to: • Be victims of social engineering, such as phishing (the use of faked email messages to extract confidential information or to gain unauthorized access to equipment) • Use removable media without performing virus checks • Fail to observe the signs of a cyber incident This is common in SMBs, where resources for training are limited.	• Provide (internally or using external parties) a variety of training resources for employees, including classroom-based, computer-based training courses/ assessments, informational videos, posters, and email newsletters (CSC17)
Inadequately secured network	Networks that are inadequately secured can: • Allow external users unauthorized access to systems and equipment • Increase the chances of a cybersecurity incident extending throughout an organization SMBs may not have the expertise to adequately secure their network.	• Use standards to define and implement effective network security. In particular, avoid direct connection with external networks, control traffic in and out of the internal network, and between different areas of the internal network (CSC1,2,6,12,13,15,20)

Vulnerability	Descriptions	Key Mitigations
Inadequately secured equipment	Equipment that is inadequately secured can: • Lack appropriate physical security, allowing ease of access to unauthorized users and increase the likelihood of accidental actions • Lack appropriate protection on physical inputs, such as USB ports and DVD drives, making it easier for malware to be transferred • Contain unnecessary applications or run unnecessary services, increasing the possibilities of a cyber incident	• Where possible, keep equipment in locked cabinets or rooms to avoid unnecessary contact • Where not possible, use locks (physical and electronic) to secure access to physical inputs • Remove unnecessary applications and disable unnecessary services on equipment (CSC1,2,3,6,7,11,13,18)
Inadequate anti-virus management	Equipment running without anti-virus protection is vulnerable to malware attack. With some malware, the infection may not be obvious and this can lead to a spread of the malware throughout the organization. A failure to maintain anti-virus protection (with the latest security patches or with the latest malware signatures) makes equipment much more vulnerable to newer malware threats.	• Ensure anti-virus is operational and maintained on all equipment, where possible • Where not possible, ensure equipment is adequately secured to remove opportunity for introduction of viruses • Use standalone machine to perform virus checking on incoming machines and media (CSC8)
Inadequate change management	There are two important considerations for change management: • Making changes to system software or hardware can introduce new vulnerabilities that, if not considered, could be exploited • Inadequate change procedures can create cyber-security incidents. For example, a failure to implement a backup before updating software could result in system unavailability if the update fails	• All changes must be reviewed before implementation. The review must assess the potential impact on system operation (reliability, performance, etc.) as well as any changes to cybersecurity risks • A change procedure must be in place that ensures that all changes are implemented with a step-by-step plan and a means to restore any equipment to its previous state, if required (CSC4,20)
Inadequate security patch management	Equipment running without the latest security patches is much more vulnerable to newer malware threats. The more security patches that are missed, the more vulnerable the equipment becomes.	• Ensure equipment is kept up to date with latest security patches from vendor(s) (CSC3,11,18)
Inadequate backup management	Backups are essential to the restoration of failed hardware or equipment infected with malware. In order to be effective, backups must occur frequently to avoid the loss of significant amounts of data. In addition, unless backups are periodically tested, they can prove to be useless when required.	• Determine what needs to be backed up and how often • Maintain backups to defined regime • Periodically test backups using a test environment (CSC10,13)
Inadequate password management	There are two key issues: • Weak passwords are easy to guess (e.g. 'password') or use only letters or numbers. A weak password can be determined using 'brute force' techniques, within 1-2 minutes • Passwords that are never changed, or changed in-frequently, are much more vulnerable to exploitation	• Enforce use of strong passwords • Enforce periodic change of passwords (CSC5,14,15,16)
Use of shared accounts	There are many problems with sharing accounts between users: • It is no longer possible to verify who took a certain action in a system • Not all users may have the same privileges, so some users may have access to functions or data that they should not • When someone leaves, knowledge of the account details are retained by the person who left	• Avoid use of shared accounts, where possible • If not possible, ensure shared accounts have limited privileges • Enforce a policy to change account details when someone leaves or moves to a new role in the organization (CSC5,14,15,16)

Vulnerability	Description	Key Mitigations
Use of default accounts	Many devices or systems have manufacturers' default accounts. If these accounts are not changed, anyone with knowledge of the default details can gain unauthorized access much more easily. In some cases, default account information is freely published on the Internet.	• Remove or change default account details (username and/or password), where possible • If not possible (e.g. hard-coded by vendor), enforce strict physical access control on equipment (CSC5,14,15,16)
Inadequate incident response	Many organizations have no plans in place to deal with a cybersecurity incident. Organizations that have plans in place may not exercise those plans sufficiently, to validate that they are effective. Without an effective incident response plan in place, organizations can be exposed to major consequences should a cybersecurity incident occur.	• Create an incident response plan that identifies the possible incidents and the appropriate response to each, as well as the key internal and external contacts • Exercise the incident response plan periodically to verify that it is effective (CSC20)

Potential consequences of inadequate cybersecurity management

The potential consequences of a cyber incident will depend on the organization, but the following table outlines the most common consequences for IT and OT equipment and systems.

Table 3 – Potential Consequences

Consequence	IT/OT	Description	Example
Theft of confidential information	IT/OT	Hackers use social engineering techniques to obtain confidential information, such as usernames and passwords that can be used to gain unauthorized access to systems. Hackers with unauthorized access to systems can extract confidential information, such as customer names, credit card numbers, trade secrets, drawings, or plans. In OT environments, the theft of control logic, recipes, production records, and other such information can yield valuable intellectual property.	In 2014, payment card data for 70 million customers was stolen from Target, after hackers gained access using the credentials of a supplier, stolen in a separate phishing attack.
System unavailability	IT	Computer viruses can be downloaded onto IT workstations, laptops, and servers remotely (using unauthorized access or through the use of social engineering), or using removable media, such as USB drives, CDs, and DVDs. Viruses can propagate across a network to infect other machines. Viruses may be used to: • Obtain confidential information (such as usernames and passwords) • Cause excessive network traffic that disrupts normal operation • Wipe an entire hard disk clean • Lock a disk until a ransom is paid	In 2012, a virus called Shamoon infected more than 30,000 office workstations belonging to Saudi Aramco. Business operations were slowed and, in some cases, paused as employees were forced to resort to manual/off-line activities and the use of personal emails for several weeks.

Consequences	IT/OT	Description	Example
Operations or production shutdown	OT	Since operations or production are heavily dependent on the OT systems that monitor and control them, a failure of these systems can result in a shutdown of the plant or process. Typical cybersecurity causes are: • Viruses • Unauthorized access • Lack of backup of system data, program, or settings	In 2013, a virus infected the operational network of the Cook County Department of Highway and Transportation in Chicago, affecting 200 computers. The department was shut down for nine days until normal service could be restored.
Service outage	OT	In a specific instance of operations or production shutdown, the result can have serious ramifications for others. For example, the loss of water or wastewater services, the loss of communications, etc. Typical cybersecurity causes are: • Viruses • Unauthorized access • Lack of backup of system data, program, or settings	In 2015, hackers infiltrated the control system of a Ukrainian power company and took control of the electricity distribution network. Approximately 80,000 homes were left without electricity for up to six hours.
Equipment damage	OT	Production or operational plants are connected to the monitoring and control systems that can be impacted by a cybersecurity incident. Without adequate mechanical or independent shutdown systems, physical damage is possible. Typical cybersecurity causes are: • Viruses • Unauthorized access	In 2014, hackers gained access to a steel mill in Germany and disrupted the operation of the safety system, causing massive damage to the blast furnace.
Environmental damage	OT	Many OT control systems monitor or control processes that, in the event of failure or incorrect operation, can cause harm to the environment. Examples include oil and gas production and wastewater treatment. Typical cybersecurity causes are: • Viruses • Unauthorized access	In 2000, a disgruntled former contractor used stolen equipment to deliberately manipulate a wastewater control system, causing a release of 750,000 gallons of raw sewage into the environment in Queensland, Australia.
Injury or death	OT	Many OT control systems monitor or control processes that, in the event of failure or incorrect operation, can cause harm to personnel or members of the public. Examples include oil and gas production, transportation, and wastewater treatment. Typical cybersecurity causes are: • Viruses • Unauthorized access	In 2008, a 14-year old boy modified a TV remote to change the points on a train network in Lodz, Poland. Twelve people were injured and four trains derailed.

ESSENTIAL CYBERSECURITY ACTIVITIES

Numerous standards and guidance documents are available to help SMBs implement proper cybersecurity management.

The US Cybersecurity Framework, produced by the National Institute of Standards and Technology (NIST) [1], is an excellent starting point for SMBs. The Framework identifies five core functions that encapsulate cybersecurity management. The Framework then further defines all the activities that may need to be undertaken for each function and identifies relevant standards to help identify how to implement these activities.

The table below identifies the essential cybersecurity activities that should be undertaken by all SMBs. These are described in more detail below the table.

Table 4 – Essential Cybersecurity Activities

Framework Functions	Activities			
Identify	Create an inventory of all IT and OT assets	Assess the risk of cyber incident	Define a cybersecurity management policy	Awareness and training
Protect	Secure network and equipment	Protect sensitive information	Manage access to systems and equipment	
Detect	Define methods for monitoring	Define responsibilities for monitoring	Identify improvements	
Respond	Maintain an incident-response plan	Practice response processes	Identify improvements	
Recover	Maintain backups of all systems and equipment	Practice recovery processes	Identify improvements	

IDENTIFY

The identify function focuses on understanding the nature of the systems inventory owned by the SMB and what risks are associated with this inventory.

Create an inventory of all IT and OT assets

This step is essential for all SMBs. Proper cybersecurity management is impossible without a definitive understanding of the assets involved. Organizations that fail to identify equipment or systems leave themselves vulnerable to cyber incidents due to a lack of protection or monitoring.

The inventory of assets should include, as a minimum:

- Make and model of hardware
- Version number of all operating system and application software

Additionally, some organizations identify equipment location, owner, and other useful information.

Assess the risk of a cyber incident

Once an SMB understands what it is protecting from a cyber incident, it must conduct a risk assessment to identify what risks exist.

Risk assessments require the involvement of all key stakeholders (to ensure accuracy) and should identify the likely threats and the vulnerabilities in the asset base. From this, the organization should identify the potential consequences, e.g. loss of confidential information, loss of revenue, environmental impact, injury or death, and so on.

SMBs should rank their risks using a common methodology to allow the identification of risks in priority order.

Define a cybersecurity management policy

Every SMB should have a cybersecurity management policy to define:

- Those responsible for cybersecurity management activities
- The processes and procedures required for operational activities and to reduce cybersecurity risks
- The expectations of employees (e.g. appropriate use of IT equipment, use of personal devices, etc.)

PROTECT

The protect function is a core cybersecurity management activity that an organization must undertake on an ongoing basis.

Secure network and equipment

Securing a network and equipment involves such actions as:

- Physically locking or disabling all equipment inputs to prevent unauthorized use, including smart device charging
- Using only dedicated devices that are kept secure, with anti-virus software scanning before and after use
- Using a quarantine area to check incoming removable devices of unknown provenance and transfer files to dedicated, known devices
- Only allowing a transfer of files from removable devices under strict supervision and in compliance with anti-virus checks
- Applying recommended patches to operating system and application software in a timely manner
- Testing patches before applying to live equipment
- Keeping anti-virus software up to date
- Performing an anti-virus scan regularly and frequently (e.g. monthly)
- Maintaining a record of all updates applied to allow for identification of issues
- Limiting external access to equipment and networks to only those authorized to access them

Protect sensitive information

Protecting sensitive information involves such actions as:

- Keeping confidential information secure (e.g. in locked cabinet or safe) and disposing confidential information in a secure manner (e.g. shredding)
- Being aware of who is around you and taking care to avoid disclosing sensitive information
- Being suspicious of emails if you do not recognize the sender
- Making sure you don't click on links or open attachments unless you are certain the sender is trustworthy
- Making sure you do not download or install anything after following a link in a suspicious email

- Making sure you do not provide confidential information via email unless you are certain the recipient is appropriate/authorized
- Making sure a supervisor or trained expert is available for advice before individuals take any action

Manage access to systems and equipment

Managing access to systems and equipment involves such actions as:

- Maintaining physical and electronic security to ensure that only authorized persons have access to the equipment they require in performing their role
- Securing equipment in locked rooms or cabinets and monitoring access
- Performing background checks on all users before approving access
- Maintaining a register of approved users
- Preventing sharing of login credentials between users
- Removing or changing credentials when a user moves to a new role or leaves
- Removing or changing default accounts
- Enforcing strong passwords and changing regularly
- Providing temporary external access as required, supervise during use, and remove once complete

DETECT

Having established an understanding of its asset base and the risks to it, the SMB must then have methods to monitor for incidents, so that it is able to respond promptly and effectively to minimize the impact.

Define methods for monitoring

Monitoring methods will vary from organization to organization, based on the particular asset base and risk assessment. In some cases, manual methods, such as checking log and system files, will suffice. For larger organizations with more electronic activity, this may be impractical and automated tools may be needed.

Define responsibilities for monitoring

Having defined the methods for monitoring, the SMB must assign responsibilities for these activities.

In addition, all employees should receive awareness training, be instructed to be vigilant for signs of a cyber incident, and be trained to report any type of cyber incident.

Identify improvements

Cybersecurity is an ever-changing situation. Threats, vulnerabilities, and risks change and SMBs need to be able to adapt. In the detect function, SMBs must regularly review their monitoring methods and adjust them to suit changing circumstances and according to incident experiences.

RESPOND

The respond function comes into effect when an incident occurs. However, preparation is essential to a successful response, and so an organization must take actions well in advance of any incident.

Maintain incident response plan

Key to a successful response, with minimal impact, is an effective cybersecurity incident management plan. The plan needs to identify the possible cybersecurity incidents that may occur within the organization and document the step-by-step procedures that should be followed in the event of each one. All employees should be aware of the risks of cybersecurity incidents and their role in avoiding them.

Practice response processes

SMBs must test their cybersecurity incident management plan on a periodic basis. The test must be realistic and exercise as many of the elements as possible, so as to be certain that established procedures will work when required.

Identify improvements

SMBs will need to update their incident management plans in response to changes in the cybersecurity landscape, and also as a result of their incident response tests.

RECOVER

While the respond function comes into effect when an incident occurs, the recover function comes into effect once the respond function is completed. As with the respond function, preparation is essential to a successful recovery, and so an SMB must take actions well in advance of any incident.

Maintain backups of all systems and equipment

Key to a successful recovery from a cybersecurity incident is having the right backups in place. Having the right backups in place requires an SMB to:

- Identify what needs to be backed up
- Determine back-up frequency based on operational requirements (How long can you operate without a working system? How much data can you afford to lose?)
- Store clearly labeled backups securely on-site and off-site, preferably in a fireproof safe

Practice recovery processes

SMBs must test their cybersecurity incident recovery processes on a periodic basis. The test must be realistic and exercise as many of the elements as possible, so as to be certain that established procedures will work when required.

Identify improvements

SMBs will need to update their recovery processes in response to changes in the cybersecurity landscape, and also as a result of their incident recovery tests.

AWARENESS AND TRAINING

The importance of awareness and training for employees cannot be understated. No amount of technical and procedural mitigations will help if an employee takes an insecure action (e.g. inserting a removable drive without performing an anti-virus scan) due to lack of training or awareness.

External classroom and online training courses are recommended for SMBs to give their employees a clear understanding. Internal resources, such as assessment (surveys, tests) and awareness (videos, posters, emails) tools, should be used to complement external courses and provide a constant reminder to employees.

Effective cybersecurity management should be a high-profile business objective that is reported on by management so that employees are constantly reminded of its importance.

The International Society of Automation (ISA) provides training courses and certificate programs based on the ISA/IEC 62443 (Security of Industrial Automation and Control Systems) standard [4].

ASSESSMENT AND CONTINUOUS IMPROVEMENT

Continuous improvement

Effective cybersecurity management requires continuous improvement. The essential activities outlined above are only the beginning.

For each of the five core functions of the Cybersecurity Framework, there are many degrees to which SMBs can go. For example:

- Network and equipment monitoring can be a manual activity in its simplest form, but SMBs can purchase speciality software to assist
- Third-party organizations can provide assessment services, including penetration testing, to validate the effectiveness of cybersecurity mitigations

The degree to which SMBs should go will depend on the level of risk they perceive, and this may vary with time.

In addition, cybersecurity is continuously evolving, with new vulnerabilities, exploits, and threats arising all the time. SMBs must continuously review their risk and adapt their mitigations to suit this changing landscape.

REFERENCES AND FURTHER READING

[1] The Cybersecurity Framework, National Institute of Standards and Technology (NIST), https://www.nist.gov/cyberframework

[2] Critical Security Controls, Center for Internet Security (CIS), https://www.cisecurity.org/critical-controls.cfm

[3] IEC62443 Security For Industrial Automation and Control Systems, International Society of Automation (ISA), https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[4] IEC62443 Training Courses and Certificates, International Society of Automation (ISA), https://www.isa.org/certification/certificate-programs/isa-iec-62443-cybersecurity-certificate-program

[5] 5 Reasons Why Small Businesses Need Cybersecurity, Tech.Co, http://tech.co/should-small-businesses-be-paying-more-attention-to-cyber-security-2016-10

[6] Ten Cybersecurity Strategies for Small Businesses, US Chamber of Commerce, https://www.uschamber.com/sites/default/files/legacy/issues/defense/files/10_CYBER_Strategies_for_Small_Biz.pdf

[7] Cybersecurity Resources for Small Businesses, Department of Homeland Security (DHS), https://www.dhs.gov/publication/stopthinkconnect-small-business-resources

[8] Cybersecurity: A Small Business Guide, Business News Daily, http://www.businessnewsdaily.com/8231-small-business-cybersecurity-guide.html

[10] Small Business Information Security: The Fundamentals, National Institute of Standards and Technology (NIST), http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

[11] Strengthen Your Cybersecurity, US Small Business Administration (SBA), https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity

[12] Cybersecurity for Small Business, Federal Communications Commission (FCC), https://www.fcc.gov/general/cybersecurity-small-business

ABOUT ISA

The International Society of Automation (ISA) is a non-profit professional association founded in 1945 to create a better world through automation. ISA's mission is to empower the global automation community through standards and knowledge sharing. ISA develops widely used global standards and conformity assessment programs; certifies professionals; provides education and training; publishes books and technical articles; hosts conferences and exhibits; and provides networking and career development programs for its members and customers around the world.