NTCA CYBERSECURITY SERIES

(Part 1)

The Fundamentals of Cybersecurity

NTCA THE RURAL BROADBAND ASSOCIATION®

#BeCyberwise

NTCA CYBERSECURITY SERIES

(Part 1)

The Fundamentals of Cybersecurity

Published March 2024

4121 Wilson Blvd., Suite 1000
Arlington, VA 22203
703-351-2000
www.ntca.org

Disclaimer: The National Telecommunications Cooperative Association d/b/a NTCA–The Rural Broadband Association ("NTCA") is offering the NTCA Cybersecurity Series and/or its individual components for general information purposes only, and nothing contained herein constitutes legal advice or opinions of any kind. You use these documents at your own risk, and you should not use any of these documents without first seeking legal and other professional advice. NTCA makes no representations or warranties, express or implied, with respect to the Cybersecurity Series, including without limitation any warranties of fitness for a particular purpose. NTCA and its affiliates (and any of their respective directors, officers, agents, contractors, interns, suppliers and employees) are not responsible for, and expressly disclaim, all liability for, damages of any kind arising out of use, reference to or reliance of any information contained within the Cybersecurity Series. Although the Cybersecurity Series may include links providing direct access to internet resources, including websites, NTCA is not responsible for the accuracy or content of information contained in these sites.

A Message from the NTCA CEO

Dear Colleagues:

It is my pleasure to introduce you to the NTCA Cybersecurity Series, updated to reflect the most recent version of the National Institute of Standards and Technology (NIST) Cybersecurity Framework released in February 2024 (NIST2.0). Cyber-risk is top of mind for many these days, and it is critical that broadband providers do all they can to protect the security of their networks and customers' information. In fact, recipients of federal funding through programs like the FCC's Enhanced Alternative-Connect America Cost Model (A-CAM) and the Broadband Equity, Access, and Deployment (BEAD) Program are required to make filings describing their cybersecurity and supply chain risk management efforts. And providers of telecommunications services, interconnected Voice over Internet Protocol (VoIP) and telecommunications relay services have data breach reporting requirements, imposed by the Federal Communications Commission (FCC) in December 2023. Federal agencies have proposed cybersecurity requirements in other proceedings and it is a trend we expect to continue, making it even more important that you have a robust cybersecurity plan in place.

To help NTCA members as they consider how to improve their cybersecurity posture, we have a suite of helpful resources and materials available. This includes the NTCA Cybersecurity Series, which is intended to provide initial guidance as you work with your internal teams and lawyers, consultants and other advisors to develop a comprehensive, companywide approach to identify, assess and manage cyber risks. We will continue to update the series as additional guidance becomes available. You can view these resources by scanning the QR code at the bottom of this page.

I also encourage you to consider joining CyberShare: The Small Broadband Provider Information Sharing and Analysis Center (ISAC), our industry's coordinating and communications body created to help protect your facilities, personnel and customers from threats. CyberShare provides you with timely, actionable physical and cyber threat information, and as an ISAC recognized by the National Council of ISACs, it is designed to maximize information flow specifically across the small broadband provider sector and with other critical infrastructures and the government. Additionally, NTCA remains engaged on your behalf in Washington, D.C., to make sure policymakers know that you are proactive in securing your networks and face unique challenges as a small broadband provider.

Thank you for your hard work in seeking to protect your company, your customers and the nationwide network. It starts with you, and we are excited to have you engage with our NTCA Cybersecurity Series as you continue to enhance your cybersecurity posture. I encourage you to visit www.ntca.org/CyberWise or scan the QR code below for the latest information and resources.

Shirley Bloomfield

Chief Executive Officer

NTCA–The Rural Broadband Association

For the latest information and resources scan the QR code

Foreword: About the NTCA Cybersecurity Series

Cybersecurity is not a one-time activity but a continuous pursuit. Cyber-risk is a complex problem, and it is unpredictable. Cybersecurity goes well beyond the responsibility of the information technology (IT) department. It is a companywide responsibility and requires diligence at every level and by every employee. To help you in your efforts, we have created the NTCA Cybersecurity Series as a comprehensive guide consisting of six components designed to help executives, board officers and operational staff develop a risk management approach to cybersecurity.

The six components of the NTCA Cybersecurity Series are designed to work together to help improve your company's cybersecurity posture.

PART 1: The Fundamentals of Cybersecurity is an introductory overview of the cybersecurity realm and the partnership with government in protecting critical resources. It offers tailored resources to help companies examine cyber-risk management approaches and assessments and clarify roles and responsibilities.

PART 2: Sector-Specific Guide to the NIST Cybersecurity Framework helps your operational staff evaluate your company's cybersecurity program at a more granular and sophisticated level. It includes NTCA's updated NIST Framework Evaluation Tool that will help small network service providers digest and apply Version 2.0 of the NIST Cybersecurity Framework to their operations, while simultaneously providing flexibility for individual companies to suit their unique needs, characteristics and risks.

Part 3: Discussion Draft/Template for Cybersecurity and Supply Chain Risk Management Plan is a discussion draft that you can use to begin developing your own cybersecurity and supply chain risk management plan and is intended to spur discussion. It is important to note that: (a) while this discussion draft can be used as a starting point, your company's cybersecurity and supply chain risk management plan should accurately reflect your own cybersecurity challenges and efforts; and (b) this draft is intended merely as an initial baseline for further development and refinement in consultation with your internal experts and external advisors who will need to guide you through specific compliance requirements.

Part 4: Cyber Incident Response Plan is an essential component of your overall cyber risk management strategy. This sample response plan is a resource for your company's senior leaders and cyber risk-management team to help you either create or revise a robust cyber incident response plan.

Part 5: Employee Cybersecurity Training Video is a video you can share with employees to educate them on how to stay safe online.

Part 6: Protecting Your Network and Data will examine the most common vulnerabilities in your workplace and networks and offer practical advice on addressing them. A printable poster is available on the NTCA website to share with your employees to help them strengthen their cybersecurity skill sets.

We encourage you to participate in the full Cybersecurity Series and disseminate the resources to your company's technical experts, senior leaders and risk management specialists as you consider how best to protect your networks systems and assets.

A CONSTANT THREAT

As a telecommunications provider, your company has successfully operated secure networks for many years; cybersecurity already is an inherent part of your business. While the responsibility for protecting your company may have been viewed as a niche task delegated to your IT staff or security consultants, this is not an adequate defense. Within the last few years, cyberattacks have intensified in frequency, sophistication and severity. Corporations, networks and individuals are under constant attack from cyber threats originating within the United States and abroad. Bad actors are targeting all organizations, regardless of their size or business mission, and a cyberattack could adversely affect not only the continued viability of your company but also could put your reputation, your subscribers and your partners at risk. Recent industry statistics help to frame the scope and urgency of the problem. There was a 20 percent increase in data breaches from 2022 to 2023, continuing a longstanding trend of year over year increases, yet less than 40 % of companies say they mitigated cybersecurity risks. In 2023, the average time to identify a data breach was 118 days and 46% of all cyber breaches involved companies with fewer than 1,000 employees. Yet 43% of small businesses do not have a cyber security plan in place. When cyberattacks happen, they can be costly. It is estimated that small and medium-sized providers spent an average of $170,000 to resolve a single cyber breach, according to a 2021 survey. However, most data breaches can be prevented with basic actions such as employee education, vulnerability assessments, patching and proper configurations. To begin, companies must lay a foundation for a meaningful cybersecurity understanding. Some common threats include the following:

DATA BREACHES

A data breach is an incident that involves an unauthorized individual using a company's sensitive information to do harm. The FCC in December 2023 imposed **data breach reporting rules**. Exposed information may include company financial information, employee information, customer data, etc. It is important that companies recognize that the threats to data are not only external. About one-third of data breaches involve internal actors.

- The Federal Trade Commission's (FTC) **Data Breach Response: A Guide for Business** addresses the steps to take once a data breach has happened. Part 4 of the Cybersecurity Series will help you develop your own Cyber Incident Response Plan.

DENIAL-OF-SERVICE (DOS)

A denial-of-service (DoS) attack occurs when legitimate users are not able to access information systems, devices or network resources due to the actions of a malicious actor. Affected services may include email, websites or online accounts. Distributed denial-of-service (DDoS) attacks occur when multiple machines are operating together to attack one target. There were over 13,000 DDoS incidents, according to Verizon's dataset examined in 2020. Attacks typically involved sending junk network traffic to overwhelm systems.

- The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI) and the Multi-State Information Sharing and Analysis Center (MS-ISAC) joint guide titled,

Companies must lay a foundation for a meaningful cybersecurity understanding.

Understanding and Responding to Distributed Denial-of-Service Attacks provides organizations proactive steps to reduce the likelihood and impact of DDoS attacks.

- **The CISA DDoS Quick Guide** contains possible DDoS attack methods per OSI layer, potential impact and the applicable recommended mitigation strategies and relevant hardware.
- The National Institute of Standards and Technology **Advanced DDoS Mitigation Techniques** provides approaches to DDoS detection and mitigation, techniques to test and measure the effectiveness and impact of DDoS/spoofing mitigation techniques and how to develop guidance for such techniques.

MALWARE

Malware is short for malicious software, which is intentionally designed to interfere with a computer or network's normal functioning. A successful malware attack may cause downtime of between 17 and 24 hours.

- The **CISA Malware Tip Card** provides information on types of malware, why you should care, tips and programs to use if you have been compromised.

PHISHING

Phishing is a cyberattack that uses disguised email as a weapon. An attacker tries to trick the email recipient into believing that the message is something they want or need and so they click a link or attachment. The recipient may be persuaded to divulge personal or company information. Phishing scams account for nearly 36% of all data breaches, according to Verizon's 2023 Data Breach Report. And according to a Proofpoint study, 71% of all companies experienced a successful phishing attack in 2023.

- The **CISA Phishing Tip Card** contains phishing examples and tips.
- The **FTC Cybersecurity for Small Business — Phishing Webpage** provides information on how phishing works, what you can do to prohibit phishing, how to protect your business, what to do if you fall for a phishing scheme and the opportunity to quiz your knowledge.
- CISA, NSA, FBI, MS-ISAC **Phishing Guidance: Stopping the Attack Cycle at Phase One** provides insight into malicious actor techniques, as well as technical mitigations and best practices to help prevent successful phishing attempts

RANSOMWARE

Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. According to IBM's Cost of Data Breach Report 2023, ransomware attacks now account for nearly one in four malicious attacks.

- CISA'S **Stop Ransomware Webpage** offers a variety of resources, information, and services for organizations to reduce the impact and likelihood of ransomware incidents and data extortion. The CISA and Multi-State Information Sharing and Analysis Center's (MS-ISAC) joint Ransomware Guide provides information on best practices and ways to prevent, protect and/or respond to a ransomware attack.
- Federal Trade Commission (FTC) **Ransomware-Cybersecurity for Small Business video** explains how ransomware attacks happen and what you can do to help protect your small business from this cyber threat.

SPYWARE

Spyware is a type of software that is secretly installed into a system to gather information. It may cause your device to become slow as it gathers sensitive information.

- The **CISA Security Tip —Recognizing and Avoiding Spyware** contains information on detecting spyware on your computer, how you can prevent spyware from being installed on your computer and how to remove spyware.

Cyber threats come in different forms, and each may be handled differently. To learn more about additional cyber threats, assistance, mitigations and commonly used cybersecurity technology terms, please visit:

- **CISA Cyber Guidance for Small Businesses**
- **FCC Cybersecurity for Small Businesses**
- **FTC Cybersecurity for Small Businesses**
- **NIST Small Business Cybersecurity Corner**

DEFINING ROLES AND RESPONSIBILITIES

It is important to not underestimate the importance of defining roles and responsibilities in managing cybersecurity. It can only take one cyberattack to cause harm to your company. It is not sufficient for senior leaders to simply allocate financial resources to security activities and delegate all decisions to operational and technical employees. Senior executives and the board need to understand key aspects of cybersecurity. This foundational understanding will enable senior leaders to provide sufficient oversight and governance.

THE BOARD

The company's board of directors should understand what the company considers to be its key assets and critical systems, such as employee and customer data, and the central infrastructure necessary to operate voice and/or data network(s). The board also needs to understand significant threats to the security of those assets and systems and oversee the plan that is put in place to identify, manage, and mitigate cyber risks and detect and respond to cybersecurity incidents.

SENIOR EXECUTIVES

Senior executives have the responsibility to make cyber awareness a priority within the company and oversee the development of a comprehensive cybersecurity risk management plan. To promote cyber awareness in a company, team up with your IT staff and create or identify available training resources that your employees can utilize.

To develop a comprehensive cybersecurity risk-management plan, senior executives should convene a cross-functional cyber risk management team to holistically review the company's current cybersecurity plan, identify gaps or areas of improvement and prioritize where to allocate limited resources. An entity's risk tolerance, as set by the board, should inform this process, directing where best to use limited resources to mitigate the risk and how to prioritize activities.

Senior executives and the board need to understand key aspects of cybersecurity. This foundational understanding will enable senior leaders to provide sufficient oversight and governance.

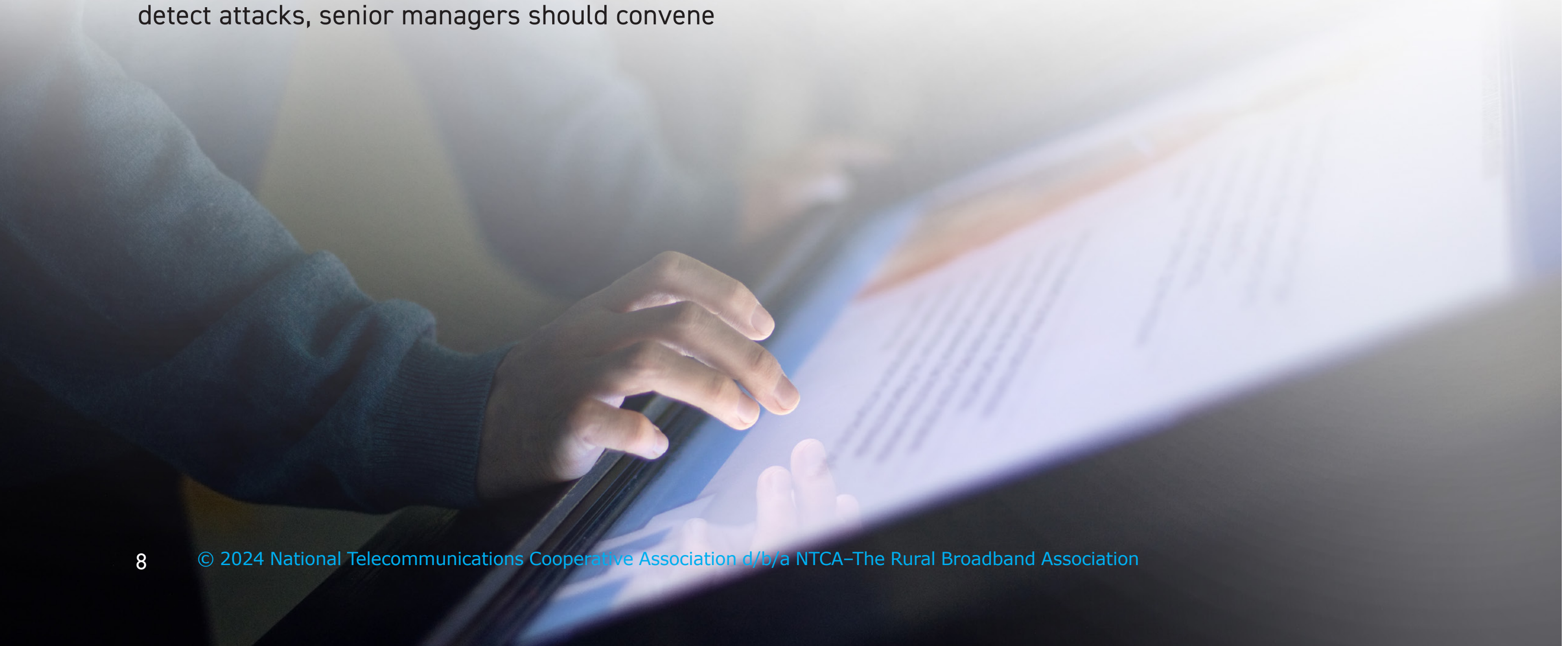
Senior executives also should monitor the company's performance relative to the risk-management plan, making adjustments as needed, and regularly brief the board on how the company is addressing risks and evolving its security posture.

In addition to activities designed to prevent or detect attacks, senior managers should convene a cyber incident response team and related plan to be put into action when or if the worst does occur. Finally, senior executives must ensure there is a companywide culture or commitment to cybersecurity, which starts at the top by modeling good behavior.

STAFF

IT staff members are responsible for the day-to-day, in-the-weeds technical tasks that carry out the vision and direction provided by a company's board and senior executives. IT personnel execute the organization's cybersecurity plan and implement mitigation techniques, including industry best practices, thereby raising the company's overall security posture. Everyday staff responsibility is to adhere to the company's security procedures and refrain from engaging in risky behaviors such as sharing passwords, installing unauthorized software and/or clicking on suspicious or unknown links in emails, etc.

For additional information on developing an actionable understanding of cybersecurity and what roles may look like within your company, please visit **CISA's Cyber Essentials**. It is tailored for leaders of small and medium-sized businesses who may need a helping hand in implementing organizational cybersecurity practices.



CYBER-RISK MANAGEMENT APPROACHES/ASSESSMENTS

Performing periodic cyber risk assessments helps uncover security vulnerabilities that may exist within a network. They are intended to allow a company to optimize and prioritize expenditures, matching its financial investments to relevant security risks.

Further, a risk management assessment enables service providers to evolve and mature their security programs. Cybersecurity is not a one-time event but is an ongoing process whereby continual improvement is the goal. As a result, NIST and CISA provide a variety of cyber and supply chain risk-management approaches and assessments to embed best cybersecurity efforts within your company.

A RISK MANAGEMENT APPROACH TO CYBERSECURITY

In light of the evolving threat landscape, a static, prescriptive, checklist methodology is not an effective defense against cyber threats. Rather, cybersecurity is best addressed using a risk-management approach.

Cybersecurity is not a one-time event but is an ongoing process whereby continual improvement is the goal.

Risk management is an established field, defined as understanding, analyzing and addressing risk to ensure an organization achieves its given objectives. Risk can be thought of as a deviation from the expected, often characterized by how likely a risk is to occur and the subsequent impact on the company and/ or its continued business operations. Enterprise risk management is an integrated approach to managing risk across an organization and its networks. (If you do not already have a risk management plan in place wherein your company holistically addresses various financial, operational, competitive and other marketplace risks, consider researching the field and how it can assist your company.)

The application of risk management to cybersecurity is relatively new. The central resource for this effort is the "Framework for Improving Critical Infrastructure Cybersecurity," commonly known as the NIST Cybersecurity Framework, which was released February 12, 2014, and updated in 2017, 2018 and most recently in 2024, and is built upon a foundation of cyber risk management. (For more on the NIST Cybersecurity Framework, see pages 11–12.) According to NIST, cybersecurity risk management is the ongoing process of identifying, assessing and then responding to risk.

In identifying risk, an organization strives to understand what kind of events can have a negative impact on its continued operations and health. In assessing risk, the company should evaluate the risk, what the impact would be to the service or business and how likely the threat is to occur. Finally, a company has several options to respond to risk, including transferring the risk to another entity, such as via an insurance policy; mitigating risk by placing the right processes or controls in place to reduce the threat accordingly; and accepting or retaining the risk (often a last resort). Note that many small telecommunications providers also may choose to share the risk with an outside vendor or consultant.

In managing cybersecurity risk, the goal is not to eliminate all risk, as this would be an insurmountable task; rather, it is about understanding what security risks threaten the continued health and viability of your company and how you can reduce those risks to a level that is acceptable, as determined by senior leadership, i.e., the board and senior executives. The acceptable level of risk is expressed as your "risk tolerance."

A risk management approach is intended to allow an organization to optimize and prioritize expenditures, matching your financial investments to relevant security risks.

Unlike a checklist methodology, a risk management model is flexible and dynamic to successfully respond to an evolving environment. A risk-management approach is intended to allow an organization to optimize and prioritize expenditures, matching your financial investments to relevant security risks. Most importantly, cybersecurity risk management implies that there is an enterprise or companywide approach, with the senior leaders and board members responsible for determining how much risk an organization is willing to accept.

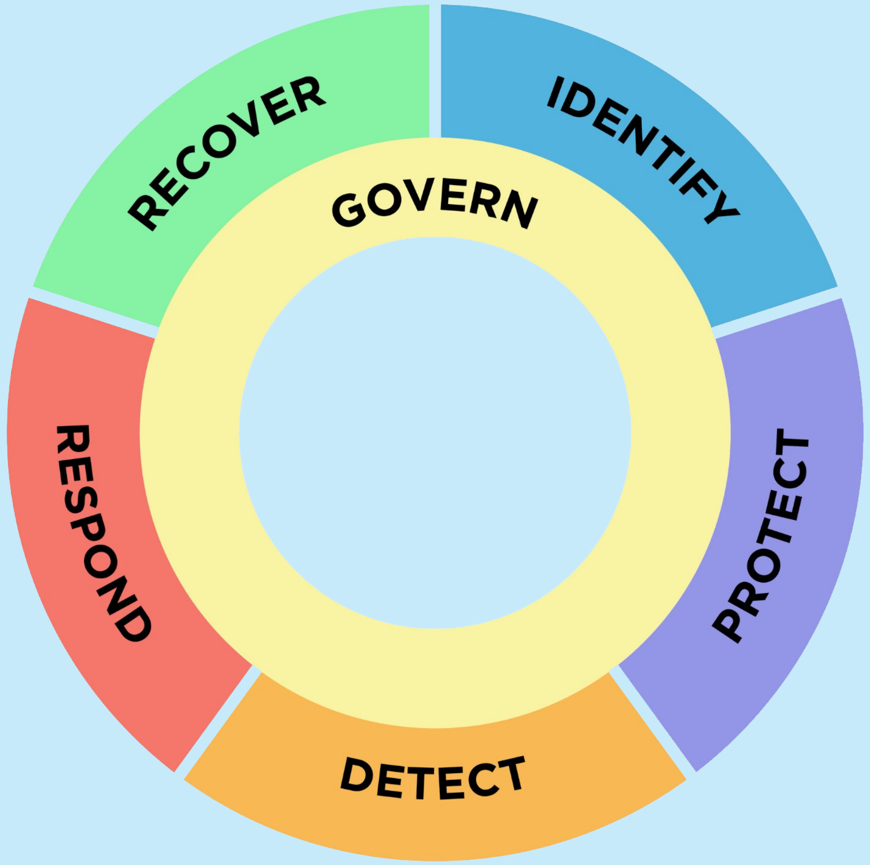
A risk management plan is not a wholesale overhaul of the cybersecurity plan many companies likely already have in place to mitigate threats. Rather, a risk management approach provides a tool for your company to formalize, provide structure to and install governance over your company's existing security efforts. Most often, telecommunications providers, i.e., their IT staff, are focused on installing the nitty-gritty, operational security procedures. Indeed, despite the looming threat environment—and the potential for cyber events to have significant impacts on your business' operations and continued viability—cybersecurity may still be viewed as a job for IT. Most often, cybersecurity governance is what is missing from a company's approach—and a risk management model elevates the overall governance of cybersecurity to the boardroom and the senior executives.

THE NIST CYBERSECURITY FRAMEWORK

In response to evolving and increasing cyber threats, President Barack Obama issued **Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity,** in February 2013. Among other items, the EO directed the National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce, to develop a voluntary framework for reducing cyber risks to critical infrastructure. Released in February 2014, the "Framework for Improving Critical Infrastructure Cybersecurity," version 1.0 (the NIST Cybersecurity Framework), was created to assist all 16 critical infrastructure sectors, including communications operators, with managing cyber risk. The Framework was revised in 2017, 2018, and 2024.

In 2024, NIST released version 2.0 of the Cybersecurity Framework. The Framework is based on existing standards and designed to help owners and operators of critical infrastructure manage their cyber risk. Part 2 of the Cybersecurity Series provides an overview of the NIST Framework and includes NTCA's updated NIST Framework Evaluation Tool.

The NIST Framework provides five main functions that all organizations, regardless of size, can use to evaluate their cybersecurity programs:



- **GOVERN**: Establish, communicate and monitor the organization's cybersecurity risk management strategy, expectations, and policy.
- **IDENTIFY**: Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data and capabilities.
- **PROTECT**: Develop and implement appropriate safeguards to ensure delivery of critical services.
- **DETECT**: Develop and implement the capability to identify the occurrence of a cybersecurity event.
- **RESPOND**: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- **RECOVER**: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber incident.

Within each function, the NIST framework then provides more granular guidance via specific "categories" and "subcategories." The subcategories are then matched with "informative references," which are existing security standards, such as ISO, PCI and COBIT.

The presidential EO specified that the NIST Cybersecurity Framework approach is voluntary. However, the NIST Cybersecurity Framework is the preeminent guide to cybersecurity risk management. Therefore, as policymakers look to adopt or refine risk management guidelines and regulations, use of the Framework is implicit. Further, the NIST Cybersecurity Framework, initially created through an Obama administration action, has since been codified into legislation through the Cybersecurity Enhancement Act of 2014, and the approach was further supported by the Trump and Biden Administrations.

NIST CYBER SUPPLY CHAIN RISK MANAGEMENT RESOURCES

NIST is also responsible for developing reliable and practical guides to managing the cyber supply chain. According to IBM's Cost of Data Breach Report 2023, 15% of respondents reported that breaches in 2022 occurred because of a compromise of business partner and 12% reported that a breach began with an exploited vulnerability in third-party software.

Therefore, it is good to have in mind that cyber supply chain risk management will help prevent compromised components from entering your networks. The following are useful supply chain risk management resources to assist your company:

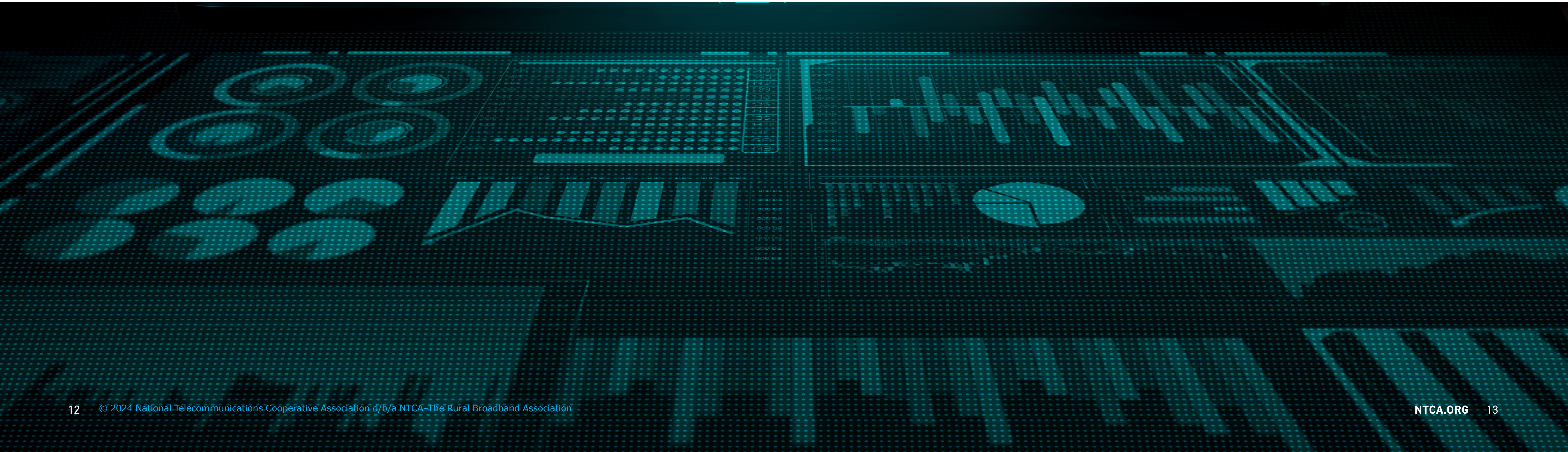
- **NIST Special Publication 800-161Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations**, provides guidance on identifying, assessing and responding to cybersecurity risks throughout the supply chain at all levels of an organization.
- **Empowering SMBs: A Resource for Developing a Resilient Supply Chain Risk Management Plan** a guide to help small and medium businesses develop an actionable supply chain risk management plan to mitigate the risk of disruption to their supply chain.
- **NISTIR 8276 Key Practices in Cyber Supply Chain Risk Management** proving key practices than organization can use to management cybersecurity risks associated with their supply chains.

CISA CYBERSECURITY ASSESSMENTS

CISA provides the community with a variety of tailored assessments through its Cyber Hygiene Services and through its website to determine the cyber health of a company. These assessments are at no cost and consist of the following:

- The Cyber Resilience Review (CRR) is a non-technical assessment that measures the maturity of a company's operational resilience and cybersecurity practices.
- The Vulnerability Scanning evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.
- The Phishing Campaign Assessment is a practical exercise that determines the potential susceptibility of personnel to phishing attacks.
- The Web Application Scanning evaluates known and discovered publicly accessible websites for potential bugs and weak configuration to provide recommendations for mitigating web application security risks.
- The Remote Penetration Test simulates the tactics and techniques of real-world adversaries to identify and validate exploitable pathways.

To get started with the last four assessments, email CISA at **vulnerability_info@cisa.dhs.gov** with the subject line "Requesting Cyber Hygiene Services."



CYBER INFORMATION SHARING FORUMS

Cyber threat intelligence is a critical input into a cybersecurity risk management strategy, as it assists with identifying and assessing current threats and often provides recommended mitigation techniques. In a recent survey of participants in CyberShare, NTCA's cyberthreat information-sharing program created especially for small broadband companies, 93% of respondents said they are receiving information via participation in CyberShare that makes them more aware of and/or helps them manage threats to their enterprise. As your cybersecurity strategy evolves and becomes more sophisticated, you may consider participating in various cyber information-sharing communities.

Listed below are a few venues that your operational and/or technical employees may want to investigate. Note there are a variety of venues, and many overlap.

- CyberShare: The Small Broadband Provider Information Sharing and Analysis Center (ISAC) provides participants with immediate, actionable cyber threat information, and as an ISAC recognized by the National Council of ISACs, it is designed to maximize information flow across the small broadband provider sector and with government. CyberShare participants have access to daily and weekly reports and have the ability to communicate and collaborate in a trusted setting. Learn about and join CyberShare. **https://www.cyber-share.org/**
- The U.S. Computer Readiness Team (US-Cert), part of the Department of Homeland Security, distributes cyber vulnerability and threat information on a regular basis, often several times per week, for free to subscribers. **Sign up for US-Cert email notices**.
- InfraGard is a partnership between the FBI and members of the private sector that expedites the exchange of information and promotes mutual learning opportunities relevant to the protection of critical infrastructure. **Find and join your local InfraGard chapter**.
- State and Regional Fusion Centers operate as state and major urban area focal points for the receipt, analysis, gathering and sharing of threat related information among federal, state, local, tribal, territorial and private-sector partners. **Find your local fusion center.**
- The NIST Software and Supply Chain Assurance Forum (SSCA) provides government, industry and academic participants an opportunity to share their knowledge and expertise regarding software and supply chain risks, effective practices and mitigation strategies and tools and technologies. Forums are held two to three times per year. **Register for the next forum**.

CyberShare

Small broadband providers are committed to helping keep their customers safe online and participate more meaningfully in our digital economy.

As part of this commitment, NTCA introduced CyberShare: The Small Broadband Provider ISAC (cyber-share.org) in 2020, to help small broadband providers protect their networks through an intelligence sharing community. Additionally, NTCA releases cybersecurity communications resources to its ISP members during Cybersecurity Awareness Month (in October) and encourages sharing messages about how to stay safe online with their customers and other consumers.

Helping Communities Stay Safe Online

#BeCyberwise

For more information, visit **www.ntca.org/CyberWise** or email **jill.canfield@ntca.org**.

SOURCES:

Communications Sector Coordinating Council, "Annual Report 2024," available at **https://www.comms-scc.org/2024/03/01/2024-cscc-annual-report/**

Forbes, "Cybersecurity in 2022 – A Fresh Look at Some Very Alarming Stats" (Jan 21, 2022). Available at **https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=5be40376b616**

IBM Security, "Cost of a Data Breach 2023," available at **https://www.ibm.com/reports/data-breach**

Institute of Risk Management, "What is Enterprise Risk Management?" available at: **https://www.theirm.org/what-we-do/what-is-enterprise-risk-management/**

Institute of Risk Management, "Cyber Risk and Risk Management," available at: **https://ww w.theirm.org/resources/find-a-resource/cyber-risk-and-risk-management/**

National Institute of Standards and Technology (NIST), "Glossary," available at: **https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/glossary**

NIST, "History and Creation of the Framework," available at: **https://www.nist.gov/cyberframework/history-and-creation-framework**

ThoughtLab, "Cybersecurity Solutions for a Riskier World; How business and government can protect themselves in the emerging risk landscape" available at **https://thoughtlabgroup.com/wp-content/uploads/2022/05/Cybersecurity-Solutions-for-a-Riskier-World-eBook_FINAL-2-1.pdf**

Verizon Enterprise, "2023 Data Breach Investigations Report 2023" available at **https://www.verizon.com/business/resources/reports/dbir/**

NTCA Cybersecurity Series

(Part 1)

The Fundamentals of Cybersecurity

#BeCyberwise

NTCA THE RURAL BROADBAND ASSOCIATION®

4121 Wilson Boulevard • Suite 1000 • Arlington, VA 22203-1801
703.351.2000 • www.ntca.org