NTCA Cybersecurity Series
(Part 1)
The Fundamentals of Cybersecurity
Dear Colleagues:

It is my pleasure to introduce you to the NTCA Cybersecurity Series. In response to our members telling us they need more resources to improve their cyber posture, we have updated our Cybersecurity Bundle and turned it into a series of informative cybersecurity webcasts with helpful printable materials.

Cybersecurity threats, from phishing attacks targeting unsuspecting employees to nation-state supply chain compromises, are relentless. The Cybersecurity Series is designed to arm you with tools to help you develop a comprehensive, companywide approach to identify, assess and manage your cyber risks. But participating in this series is just a start. You must remain engaged and diligent to adjust your defensive strategies to respond to the evolving threat landscape and to protect your network and company assets.

To further enhance your cybersecurity posture, 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, as federal legislators and regulators explore action to protect the nation’s critical infrastructure, 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 subscribers 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/cybersecurity for the latest information and resources.

Shirley Bloomfield
Chief Executive Officer
NTCA–The Rural Broadband Association
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 four components designed to help teleco executives, board officers and operational staff develop a risk-management approach to cybersecurity.

The four components of the NTCA Cybersecurity Series are designed to work together to help improve your company’s cybersecurity posture and will complement a series of webinars.

**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: Protecting Your Network and Data** will examine the most common vulnerabilities in your workplace and networks and offer practical advice on addressing them. You will receive a printable poster to share with your employees to help them strengthen their cybersecurity skill sets.

**PART 3: 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 1.1 of the NIST Cybersecurity Framework to their operations, while simultaneously providing flexibility for individual companies to suit their unique needs, characteristics and risks.

**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.

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.
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 information technology (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. Security breaches have increased 67% since 2014. In 2019, the average time to identify a breach was seven months and 28% of breaches involved small business victims. Yet 45% of those small businesses had no understanding of how to protect against cyberattacks.

When these cyberattacks happen, they can be costly. It is estimated that small and medium-sized telcos spent an average of $170,000 to resolve a single cyber breach.

Companies must lay a foundation for a meaningful cybersecurity understanding.

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. 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.


**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 & Infrastructure Security Agency (CISA) Security Tip (ST04-015)—Understanding Denial-of-Service Attacks provides information on common DoS attacks, what is distributed through a DoS attack, how to avoid being part of the problem, how to know if an attack is happening and what to do if you think you are experiencing an attack.

• 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 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 Security Tip (ST13-003)—Handling Destructive Malware contains information on malware potential distribution vectors, best practices and planning strategies, recovery and reconstitution planning, and incident response strategies.

• 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 to click a link or attachment. The recipient may be persuaded to divulge personal or company information. Phishing is a leading threat action for more than 30% of small companies due to the use of stolen credential and password dumpers.

• The CISA Phishing Tip Card contains phishing examples and tips.

• The CISA Security Tip (ST04-014)—Avoiding Social Engineering and Phishing Attacks provides information about common indicators of phishing attempts, how to avoid being a victim and what to do if you think you are a victim.

• The FTC Cybersecurity for Small Business—Phishing 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.

RANSOMWARE

Ransomware is a type of malware that attempts to deny access to a user’s data until the ransom is paid. It is a moneymaking technique that can be installed through links in an email or a website.

• The CISA Insights—Ransomware Outbreak contains information on CISA’s role as the nation’s risk advisor, ransomware mitigations, actions for today, actions to recover if impacted and actions to secure your environment going forward.

• 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.

• The FTC Cybersecurity for Small Business—Ransomware provides information on how ransomware works, how to protect your business, what to do if you are attacked and the opportunity to quiz your knowledge.
SPYWARE

Spyware is a type of software that is secretly installed into a system to gather information.\textsuperscript{14} It may cause your device to become slow as it gathers sensitive information.

- The CISA Security Tip (ST04-016)—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's STOP.THINK.CONNECT. Small Business Resources
- CISA's Regional Offices
- FCC's Cybersecurity for Small Business
- FTC's Protecting Small Businesses
- NIST's Small Business Cybersecurity Corner
- NIST's Small Business Cybersecurity Corner Glossary
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 execs 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 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.

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.
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.
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.

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, updated in 2017 and 2018, 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 telco’s 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.

Of import, 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 most 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.

Revised in 2017 and 2018, NIST has come out with version 1.1 of the Cybersecurity Framework. The framework is voluntary, based on existing standards, and designed to help owners and operators of critical infrastructure manage their cyber risk. Part 3 of the Cybersecurity Series will provide an overview of the NIST Framework and include 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:

- **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 23 specific “categories” and 108 “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 pre-eminent guide to cybersecurity risk management. Therefore, as policymakers look to install 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 President Trump in his May 2017 EO.

**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 Deloitte, 40% of manufacturers had their operations affected by a cyber incident in 2019. 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:

- The NIST *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry* provides a set of key practices that companies can use to manage cybersecurity associated with their supply chain.

- The NIST *Impact Analysis Tool for Interdependent Cyber Supply Chain Risks (NISTIR 8272)* is a publicly available tool for filling the gap between an organization’s risk and supply chain risk posture by providing a basic measurement of the potential impact on a cyber supply chain.

- The NIST *Criticality Analysis Process Model: Prioritizing System and Components (NIST 8179)* identifies systems and components that are vital and may need additional security or protections in a company.
CISA CYBERSECURITY ASSESSMENTS

The 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 that there are a variety of venues, and many overlap.

- The **NTCA CyberShare: The Small Broadband Provider Information Sharing and Analysis Center (ISAC)** provides you 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.

- 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 the 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.

• **The NTCA Cybersecurity Working Group** offers a venue for association members—network operators and technical consultants—to communicate and offer direction on cyber policy matters. The group meets virtually on a monthly basis. To learn more, contact NTCA.


Ponemon Institute, pg. 8.


Verizon, pg. 57.


Verizon, pg. 36.

NIST


Verizon, pg. 81.

Id.


Id. pg. 5.

Id.
