Farmers Telecommunications Cooperative and NISC: Navigating the Complex World of Cybersecurity – And Defending Mission-Critical Data

Five Elements of a Strong Cybersecurity Plan and a BSP That's Doing It Right

Broadband service providers (BSPs), utility companies, and municipalities are all responsible for protecting not only their own data, but their customers' data, too. Cybersecurity is not a new topic, but many industry professionals still struggle to understand the breadth and evolution of cyber threats and what it takes to establish —and maintain —a strong cybersecurity plan.

In this white paper, we'll briefly discuss the latest cybersecurity threats, discuss the five critical elements of a solid cybersecurity plan, and tell the story of a BSP, Farmers Telecommunications Cooperative (FTC), that is prioritizing cybersecurity and taking measures to protect their network from attacks.

The rise and sophistication of modern cybersecurity threats

Modern cyber threats are increasingly sophisticated, making them difficult to detect and prevent. Cybercriminals develop new tactics constantly. Here are just a few you may have heard about, but whose developments, prevalence, or variations may be new to you:

- **Social engineering** preys on human users, hoping to gain authorized access to a network by tricking someone into revealing secure details. One of the most common types of social engineering is ***phishing emails***, which may include malicious links or lead to a form where a user is prompted to enter sensitive information. ***Spear-phishing*** is a more sophisticated technique in which those emails appear to come from a trusted source (like another staff member).

- **Malware** is constantly evolving to be more dangerous. The latest, most advanced malware preys on ***zero-day*** issues—new vulnerabilities in software or a computer system that have not yet been discovered—to gain network access.

- **Ransomware** blocks access to your network or data until you pay an (often exorbitant) amount of money. While you may have heard of ransomware, you may not know how common it's becoming. The U.S. Department of Health and Human Services recently reported a 278% increase in ransomware attacks in the last four years.

These are just a few types of cybersecurity threats. Having a solid cybersecurity plan and protective tools in place is the only way to maintain a constant defense against these attacks.

"At NISC, we often say that there are two types of companies: the ones that know they are compromised, and the ones that don't know they are compromised," said Jeremy Schoneberg, NISC Team Lead of Information Security. "In other words, when it comes to cybersecurity, we operate on the assumption that there's no such thing as a company that isn't compromised in some way. While that may not be strictly true, the mindset allows us and our Members to be proactive about protecting critical systems."

The five elements of a strong cybersecurity plan

What does that protection look like? It starts with building a solid foundation for cybersecurity. Here are the five elements of a strong cybersecurity plan:

1. **Perimeter Defense**. Firewall protection is the standard first line of defense for a network. Think of it as a stone wall around an ancient city—vital protection, but not sufficient by itself. A firewall should include 24/7 monitoring and reporting, so you're notified as soon as there's a threat or a breach. Firewall systems should be redundant, so if one firewall fails another is there to provide security.

2. **Endpoint Protection, Incident Detection & Response, Vulnerability Management and Patch Management & Automation**. The biggest cybersecurity risk is human error. Endpoint protection offers security for the endpoints of your network—the laptops, computers, mobile devices, etc. that are accessed by your staff and other users. Modern endpoint protection uses machine learning and AI to keep abreast of the latest threats and protect you against attacks. Incident Detection and Response is a 24/7 Security Operations Center (SOC) that monitors assets for anomalous activity. Once a threat is detected, appropriate actions are taken to neutralize the threat and investigate the incident. Vulnerability Management scans for vulnerabilities, telling you what needs to be patched so your software and hardware can be brought up to date as quickly as possible. Patch Management & Automation allows your organization to automate the patching process so you can patch vulnerabilities as they are detected.

3. **Backup Management with the 3-2-1-1-0 rule**. Backing up data is, of course, a cybersecurity must, and may be the only true protection against ransomware. But all backups are not created equal. At NISC, we believe in the 3-2-1-1-0 rule: When you backup, make at least ***three*** copies of your data. You should use at least ***two*** types of storage media (e.g., cloud and disk/tape). ***One*** of those copies should be kept offsite, away from your own facilities. ***One*** copy should be completely offline, meaning it can't be accessed or modified if someone gains access to your network. Finally, backups should be completed with ***zero*** errors.

4. **Identity & Access Management**. Make sure the people using your network are who they say they are. Identity management allows organizations to verify users by requiring a combination of credentials. Multi-factor authentication can be done in seconds by using another source—like a text to a user's phone or a unique token—before granting access to critical data. Access management segments your network so staff members have the user access privileges they need to do their job, and nothing more.

5. **Education via user training and testing**. Educating your staff about cybersecurity threats like phishing and social engineering is an important way to mitigate the risk of human error. Think of your network users as human firewalls. They are the most common targets of a network breach, so it's vital to maintain a level of vigilance among your staff. Software is available that sends simulated phishing attacks to your team, regularly testing how alert your staff is and training them to scrutinize all communications for legitimacy.

"When NISC evaluates a Member's cybersecurity risk, the tools above are considered foundational to a strong cybersecurity plan. NISC also practices what we preach, using these tools and others for our own systems and data," says Schoneberg. "Whether or not a Member uses the entire suite of NISC's cybersecurity services or handles some aspects of their cybersecurity plan in house, we work in conjunction with the Membership to ensure all are knowledgeable and protected, period."

Case study: Farmers Telecommunications Cooperative (FTC)

Farmers Telecommunications Cooperative (FTC) has been a NISC partner for more than 25 years, relying on NISC for operations, service tools, and other enterprise software. In the last ten years, FTC turned to NISC to implement more robust cybersecurity tools. The cybersecurity partnership between FTC and NISC started with a more sophisticated firewall system. Although FTC had a firewall before using NISC's cybersecurity tools, they had no firewall redundancy—if their firewall was breached, no backup systems would kick in.

As time went on, FTC became a beta user in NISC's Incident Detection and Response service and starting using NISC's Backup Management service. When FTC implemented Incident Detection and Response, Information Systems Analyst Mike Gilbert says he breathed a sigh of relief. "Incident Detection and Response was a game changer," he says. "[Before Incident Detection and Response] we had nothing to tell us somebody was messing around in the network or something was going on."

Today, FTC relies on many of NISC's cybersecurity offerings, while managing some aspects internally. The decades-long relationship between FTC and NISC allows a holistic approach to protecting FTC's systems and an open dialogue to ensure they are keeping up with the ever-evolving threats. While cybersecurity is a relatively new offering in the context of NISC's 50-plus-year history, Members like FTC know that finding the right solution has always been part of NISC's culture. If NISC doesn't have a service FTC needs, we draw from our vast network of partners to recommend a vendor that does.

In the time FTC has used NISC's cybersecurity services, FTC has had no major breaches or security incidents. In an instance when another FTC vendor had a data breach, NISC and their partners informed FTC about the breach and said they were already monitoring for any issues. Working with NISC brings peace of mind to the FTC team. "We're a small telecommunications provider—we don't have the staff to do it all ourselves," says Mike Gilbert. "They have eyes on my network 24/7. Two years ago, we didn't have a policy for responding to cyber threats, and as of today we have that in place."

Summary

The ever-evolving landscape of modern cybersecurity threats necessitates a proactive approach to protecting critical systems. Regardless of how—or with which partner—cybersecurity plans are implemented, BSPs and other providers must recognize their responsibility to safeguard both their own and their customers' data.

Establishing a strong cybersecurity foundation is paramount. This includes robust and redundant firewall defenses, advanced endpoint protection, patch management, reliable backup practices, identity and access management, and ongoing employee training.

Follow the example of FTC, which takes a multi-pronged approach to cybersecurity. As cybersecurity threats persist and advance in sophistication, the importance of a detailed and proactive cybersecurity plan cannot be overstated. If you want to learn more about NISC's cybersecurity tools, we invite you to visit **cybersecurity.coop** or contact us at **866.999.6472**.