WHITE PAPER

CHR Solutions

CYBERATTACK:

IT'S A QUESTION OF **WHEN**, NOT IF

INTRODUCTION

Cyber incidents and attacks are on the rise and there doesn't seem to be an end in sight. The number of devices already connected to IP networks is roughly three times the global population. Furthermore, approximately 70 percent of the global population has mobile connectivity—and that number continues to rise. ISPs and hosting providers, teetering at the leading edge of this internet-connected tsunami of online users, have become prime targets for cybercriminals.

Nearly a decade ago, guidelines were introduced to help companies protect themselves against cyber threats and cybercrime. However, rather than acting, too many companies continue to waste time talking about the need to take action. And, in this case, talk can be very expensive.

Small telecom and internet providers need to take action now before it's too late.

THE CYBERSECURITY LANDSCAPE FOR ISPS IN 2023

Obtaining reliable data regarding the true scope of cyberattacks is difficult; when these attacks happen, many companies forego reporting the crime and simply accede to the attackers' demands—usually in the form of cryptocurrency payments—and say as little about it as possible. There is a general sense that reporting the crime will publicize both their weaknesses and increase the perception of the public at large that they are vulnerable.

The information that is available on the scope and nature of the problem doesn't look good:

$449.1 MILLION

DOLLARS PAID TO RANSOMWARE GROUPS IN THE FIRST SIX MONTHS OF 2023

According to Wired Magazine, victims have paid ransomware groups $449.1 million in the first six months of this year. If this year's pace of payments continues, the total figure for 2023 could hit $898.6 million—nearly $400 million more than 2022[1].

AT&T, T-Mobile, Verizon, and Dish Network have had to deal with serious cybersecurity incidents within the first six months of this year that ended up exposing private information on millions of customers.

Regional telcos and ISPs continue to represent prime targets as serious service outages or DDoS (Distributed Denial of Service) attacks for each could have a profound impact on their business, as well as their customers' welfare—and, with their limited resources, they frequently offer the least resistance in terms of cybersecurity preparedness.

[1] | *Wired.com, "Ransomware Attacks Are on the Rise, Again," www.wired.com/story/ransomware-attacks-rise-2023/*

THE MOVEMENT TOWARDS A SOLUTION

In 2013, in order to address potential weaknesses in our critical national infrastructure, President Obama directed the Department of Commerce's National Institute of Standards and Technology (NIST) to develop a voluntary risk-based cybersecurity framework. The result, issued roughly one year later, was the NIST Framework, a set of industry standards and best practices, designed to lay the groundwork for helping companies focus their efforts on maintaining secure networks.

However, today, almost a decade after the NIST Framework was initially published, many companies in the telecommunication industry continue to lag behind in their cybersecurity efforts, making them especially vulnerable.

> *While being in compliance with the NIST Framework can't guarantee your network is 100% secure (currently, nothing can do that)* ***it can make a significant difference in reducing the risk of a security breach.*** *It can also play a substantial role in lowering the insurance costs for your network.*

A QUICK OVERVIEW OF THE NIST FRAMEWORK

Designed to help organizations identify, implement, and improve cybersecurity practices, the NIST Framework is composed of five core functions designed to operate on a concurrent and ongoing basis:

- ***Identify*** helps organizations gain an understanding of how to manage cybersecurity risks to systems, assets, data, and capabilities.
- ***Protect*** helps organizations develop the controls and safeguards necessary to protect against or deter cybersecurity threats.
- ***Detect*** are the steps organizations should consider taking to provide proactive and real-time alerts of cybersecurity-related events.
- ***Respond*** helps organizations develop effective incident response activities.
- ***Recover*** is the development of continuity plans so organizations can maintain resilience—and get back to business—after a breach.

Each organization has unique risks and the NIST Framework recognizes that no one-size-fits-all solution exists for managing cybersecurity risk. But that's one of the strengths of the framework: rather than being a simple checklist, it represents a compilation of forward-looking cybersecurity practices that companies should consider when building their cybersecurity programs.

While many large organizations have the necessary budgets and the staff to address these issues, Trent Martin, Director of Information Technology Services at CHR Solutions, says, "Most small telecom companies simply don't have the IT staff available to manage the type of informed cybersecurity strategy that the NIST Framework calls for.

"In many cases, their best strategy is to seek a good partner, ideally, one with a strong managed services capability that will allow them to leverage a much larger staff than they could otherwise afford on their own. Without that kind of assistance, they're living on borrowed time and are at much greater risk of a cyberattack, from anything like a phishing scam or malware strike to a complete lockdown of their system followed by a ransomware demand they're unable to meet."

As the available statistics show, vulnerabilities like these are being exploited daily and with increasing frequency.

HAVING A STRONG MANAGED SERVICES SOLUTION CAN MAKE ALL THE DIFFERENCE

A robust managed services partner can aid you in reducing the level of cyber threat you face, as well as significantly ease the strain on your resources by leveraging a shared team of experts to manage your cybersecurity issues.

Within the NIST Framework's five core functions, a good managed services team can help you **identify** threats and risk with continuous vulnerability scanning and annual penetration testing. They can also work with you to **protect** yourself with multifactor authentication, continual cybersecurity training, friendly phishing campaigns, and email phishing filtering, and manage how you **detect and respond** to cyberthreats with advanced or next-generation endpoint protection, such as EDR (Endpoint Detection and Response) or XDR (Extended Detection and Response), which might include commercial solutions, such as CrowdStrike Endpoint Protection or Datto RMM Ransomware Detection—each of which are significantly stronger that attempting to rely on traditional anti-virus solutions.

> *"Having access to a Security Operations Center (SOC) that's monitoring your devices, your network activity, all the event logs for your servers, with 24/7/365 coverage, can be a game-changer.* ”

According to Martin, "Having access to a Security Operations Center (SOC) that's monitoring your devices, your network activity, all the event logs for your servers, with 24/7/365 coverage, can be a game-changer. Most ISPs don't have the critical staff that's needed to comprehensively review all of this information; a good SOC has the resources needed to handle these details at a fraction of the cost you'd pay to appropriately increase your staff or manage a cybersecurity breach."

NO CYBERSECURITY SOLUTION IS 100%

In the unlikely event you were still to fall prey to a cyberattack, a good managed solutions provider would be instrumental in helping you **recover** and return your systems status to a time before the attack.

Relying solely on physical onsite backup options can leave you vulnerable to a variety of issues. In a data-ransom scenario, users often find themselves locked out of their own backup servers, whereas a managed solutions partner can ensure that you have sufficient cloud storage and efficient back-up systems in place that will allow you access to your data regardless of what's happening locally. In some cases, they might even be able to help you regularly capture an Immutable Snapshot, a record of your stored data that can't be edited or overwritten, giving you the ability to roll your systems back to an earlier point in time before the crisis occurred.

A good partner might even be able to assist your transition to a more secure office productivity environment, such as the one offered by Microsoft 365, which allows you to have your communications and documentation separated from your local infrastructure. This can play an invaluable role in helping to recover your critical information after a cyber strike. For instance, in a ransomware event, where your entire local infrastructure gets taken down, Microsoft 365 would still allow you to have communications outside of your local channel, while your key documentation stays separate and safely stored on the cloud.

The right partnership can save you time, stress, and money while helping you create a cyber-secure environment without putting unnecessary strain on your internal resources and budget.

CONCLUSION

There’s no way to sugarcoat the problem: lax cybersecurity continues to be a leading issue for many companies, particularly regional telcos and ISPs. Those with limited resources and IT staff are waiting too long to take necessary steps to protect themselves, but attempting to do it on your own can be expensive and can overtax your available IT resources.

The stakes are high. Waiting to take action is no longer viable. This might include beefing up your existing IT team or it might require taking on a cybersecurity partner with a dedicated team of experts.

There’s no denying the warning light is flashing on local telcos and ISPs.
The time to act is now.

CHR Solutions

713.351.5111
info@chrsolutions.com
chrsolutions.com