UNITEL

Responsive Technology Partners

Steven McComas MPA, MBA, CGMA, CPA
Chief Executive Officer – Responsive Technology Partners, Inc
Chief Financial Officer – Pineland Telephone Cooperative, Inc.

Mike Reed
Risk Advisor—UNITEL Insurance

Technology support when you need it, not just when it's convenient.

Responsive Technology Partners

a joint venture between

Wilkes COMMUNICATIONS

Pineland

Steven McComas *MPA, MBA, CGMA, CPA*

Chief Executive Officer – Responsive Technology Partners, Inc

Chief Financial Officer – Pineland Telephone Cooperative, Inc.

(912) 601-7110
steven.mccomas@responsivetechnologypartners.com

Scan Here
to download my virtual business card.

Our Mission

To provide world-class customer service through industry-leading IT solutions that make every customer feel as if they are our only customer.

Core Values

INNOVATION

EXCELLENCE

INTEGRITY

SERVANT'S HEART

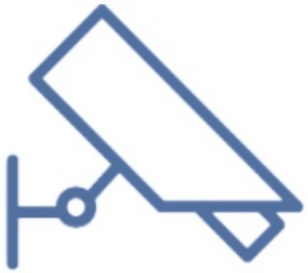
OUR SERVICES

IT Support

Cybersecurity
& Compliance

VoIP Phones

Infrastructure



Access Control
& Camera Systems

Cabling

Our Locations

GEORGIA

VIRGINIA

FLORIDA

NORTH CAROLINA

Our History

1951 — Pineland Telephone Cooperative established in Metter, Ga.

2008 — Pineland Computer Services established.

2017 — Purchased 1st MSP, Broadtech Solutions, in Vidalia, Ga. In lead Pineland's CLEC expansion efforts

2019 — Pineland's 100% ILEC fiber build February 2019, Pineland continues MSP expansion efforts via 2nd acquisition of Cogentes and rebranded to establish Pineland Cogentes.

2020 — Pineland Cogentes named to Inc. 5000. at #630 fastest growing US private companies, #18 for IT Management.

Our History

02/20

Pineland Cogentes acquired with First Service Carolina in Raleigh, NC.

08/20

Pineland Cogentes rebranded as Responsive Technology Partners and acquired Professional Network Services in Roanoke, VA.

10/20

RTP acquired Compunet LTD in Tampa, FL.

02/21

RTP successfully provided cybersecurity for Super Bowl LV.

Results from Pineland's Diversifying Revenue Strategy into the MSP Market

Revenue Mix	2010	2020	Projected 2021
ILEC	89%	59%	51%
CLEC	0%	12%	12%
RTP MSP	**1%**	**24%**	**29%**
Alarm & Fire	6%	8%	6%
Other Investments	3%	-2%	2%
Total	100%	100%	100%

“When it comes to running a business, the most important decisions a leader makes are not about products or locations – they’re about people.”

Dee Ann Turner, A 33-year veteran of Chick-File-A Inc as Vice President of Talent.

Our Executive Team with 250+ years of MSP and business experience.

BACK ROW: LEFT TO RIGHT

- **David Topping** - Director of Business Development Virginia
- **Jeff Lunsford** - Director of Operations Virginia
- **Alex Muzafarov** - Director of Operations Georgia
- **Dustin Durden** - Executive Vice President
- **Gary Klik** - Director of Operations Virginia

FRONT ROW: LEFT TO RIGHT

- **Brad Revels** - Director of Operations North Carolina
- **Eric Cramer** - Board of Directors Member
- **Steven McComas** - CGMA, CPA, Chief Executive Officer / Board of Directors Member
- **José Remon** - Director of Business Development Florida
- **Tom Glover** - President Georgia
- **Mike Abbott** - President North Carolina

Responsive
Technology Partners

Inc. 5000 — America's Fastest-Growing Private Companies

2020

Inc.5000
N° 18 2020
IND IT MANAGEMENT

Inc.5000
N° 630 2020
AMERICA'S FASTEST-GROWING PRIVATE COS

2021

Inc.5000
N° 509 2021
AMERICA'S FASTEST-GROWING PRIVATE COS

Inc.5000
N° 14 2021
IND IT MANAGEMENT

HIPAA SEAL OF COMPLIANCE
COMPLIANCY GROUP
HIPAA VERIFIED

Inc.
Best in Business
2020

LV
SUPER BOWL
cyber security provider

IT Sales & Marketing "Boot Camp" 2021

- 14th annual Sales and Marketing Boot Camp with Robin Robins and the Technology Marketing Toolkit, **the world's #1 Marketing Consulting Agency for MSPs**, held in Orlando, FL.

- Tom Glover, Georgia President, presented in the top 5 MSP's Better Your Best Competition.

- MC Tracy, Marketing Manager, won first prize as the Marketing Manager of the Year 2020-2021.

Kevin "Mr. Wonderful" O'Leary

- Spoke with Mr. O'Leary about the top 5 problems businesses are facing post-pandemic.
  - Businesses were forced to operate remotely
  - Businesses faced an accelerated adoption of technology
  - Businesses enhanced their focus on direct-to-consumer strategies
  - Businesses reassessed real estate investments and costs
  - Businesses see a potential for long-term operational enhancements

https://www.responsivetechnologypartners.com/2021/06/01/5-things-shark-tanks-mr-wonderful-taught-me-the-day-we-met/

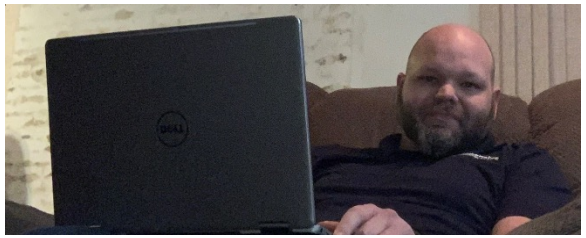
National Exposure and Increase Franchise Value for RTP

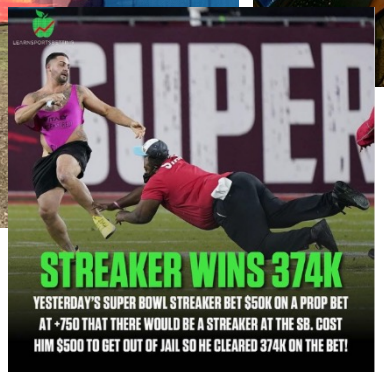
- VP of Business Development for our Florida office, Jose Remon, Senior System Engineer for our Florida office, Alex Mane, supported by some of our senior leadership and outstanding engineers from our Virginia and Georgia offices, successfully provided secured IT support for Super Bowl LV (“55”) in Tampa, Florida. Several months in the planning resulted in our clients, the Tampa Sports Authority and NFL, hosting a successful global sporting event during troubled times with no IT issues!

RAYMOND JAMES STADIUM
SUPER BOWL LV

NFL CYBER SECURITY
LV
SUPER BOWL

NFL CYBER SECURITY




STREAKER WINS 374K
YESTERDAY'S SUPER BOWL STREAKER BET $50K ON A PROP BET AT +750 THAT THERE WOULD BE A STREAKER AT THE SB. COST HIM $500 TO GET OUT OF JAIL SO HE CLEARED 374K ON THE BET!

Key take-aways from Pineland/Wilkes' MSP Journey

- **Pineland and Wilkes investment business objective with RTP is simply a pure investment play with the goal of generating long-term contributory cash flows with above rural telco market EBITA margins.**

- **The MSP model is a culture of its own. This is not an extension of your telco operation's department.**

- **Having existing MSP experts run and drive the growth strategy is critical. Involvement = Commitment. Don't let your Boards get into the details.**

Key take-aways from Pineland/Wilkes' MSP Journey

- **Don't overpay for an existing MSP. It's about a return on cash invested. Value is not a multiple of recurring revenue.**

- **MSPs control commercial IT relationships in competitive markets. Targeted and careful MSP acquisitions are a good approach to land immediately on the beach for CLEC expansion.**

Thinking about getting into the MSP Space? Are you already representing yourself as an IT expert by your actions?

- Make sure you have solid internal controls and tested risk management policies and procedures for MSP work. Communication with your advisors is critical – Attorney, Auditors, Insurance Brokers, and Technology Consultants.

- Cybersecurity is the #1 IT issue for your clients. Don't represent third party IT solutions and provide advice outside your level of expertise and risk tolerance. If so, approach very carefully! These risks are very high!

"The ransomware threats are comparable to the challenge of global terrorism in the days after the Sept. 11, 2001 attack."

-Christopher A. Wray, FBI Director, *June 4th, 2021*

Cyber Attacks and Ransomware

- **Types of Cyber Attacks:**
  - **Brute-Force Attack**
    - **Trial and error of guessing a password**
  - **Credential Stuffing**
    - **Using stolen credentials**
  - **Phishing and Spear Phishing**
    - **Through malicious links or attachments in emails**
  - **Malware Attacks**
    - **Malicious software downloaded to system**
- **Ransomware:**
  - **Ransomware is a type of malware that threatens to publish the victim's personal data (usually to be sold on the dark web) or potentially block access to it unless ransom is paid. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.**

Largest Ransomware Attacks 2021

1. **Colonial Pipeline Attack**
   - **Hacker group: Dark Side – Eastern-European Russian Group**
   - **150 GB worth of data stolen**
   - **Ransom payout: $4.4 million**

2. **Brenntag (Chemical Distribution Company)**
   - **Hacker group: Dark Side – Eastern-European Russian Group**
   - **150 GB worth of data stolen**
   - **Ransom payout: $4.4 million**

3. **JBS Foods (One of the largest meat processing companies worldwide)**
   - **Russia-based hacking group**
   - **Ransom payout: $11 million**

What The FBI Director Has To Say About Recent Cyber Attacks

- Russia is harboring some of the most dangerous ransomware groups.
- The FBI is investigating 100 different software variants that have been used in ransomware attacks, demonstrating the scale of the problem.
- Large concerns after food processing plants, hospitals, and fuel pipelines are forced to shut down.
- "As attackers continue chipping away at our nation's critical infrastructure, significant disruptions are to be expected. Without a clear direction on how to build a more robust defense, those disruptions become disastrous."

byte

J

Paid registration

0

4 posts

Joined

09/19/20 (ID: 108611)

Activity

кардинг / carding

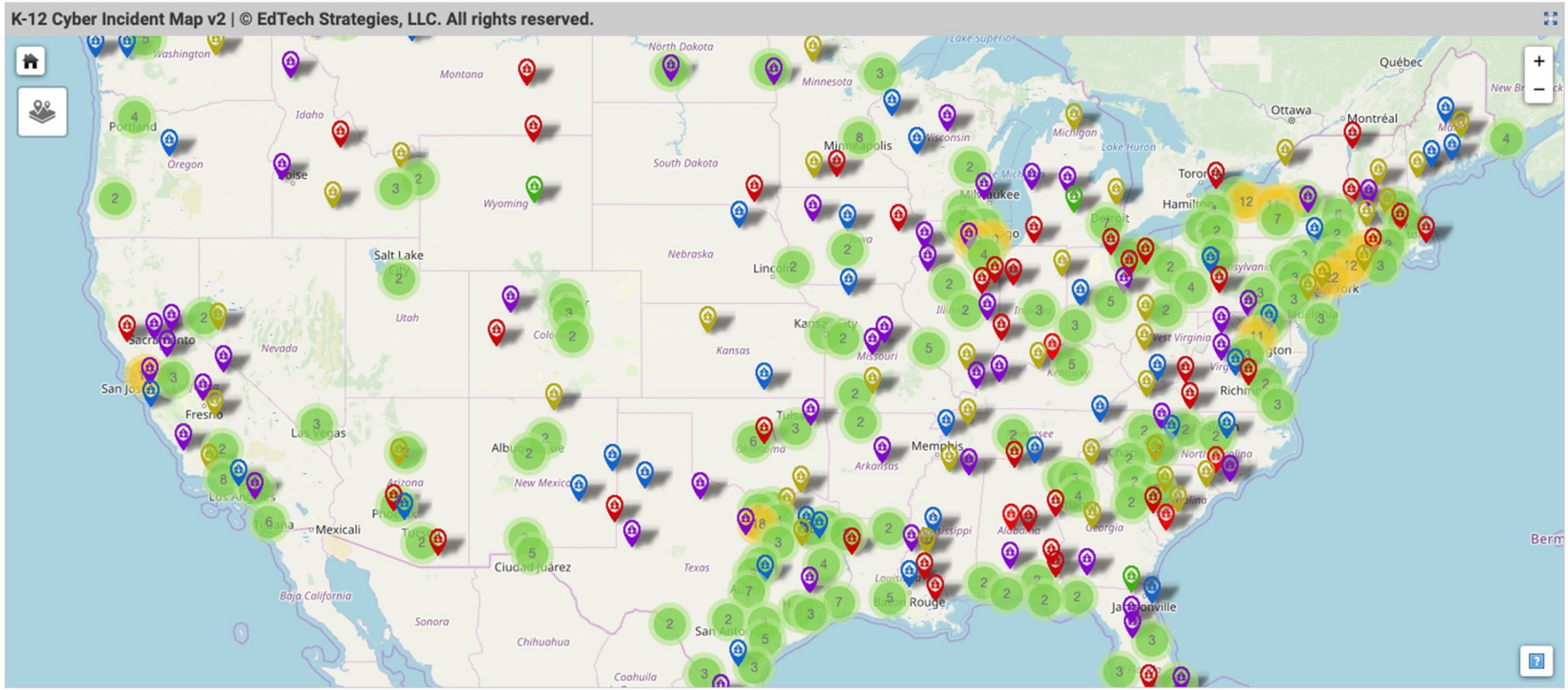
Posted 16 hours ago

Selling login email:pass for Office 365, login.microsoftonline.com of people in position C-Levels
CEO - chief executive officer
COO - chief operating officer
CFO - chief financial officer or chief financial controller
CMO - chief marketing officer
CTO - chief technology officer
President
Vice president
executive assistant
Finance Manager
Accountant (but not always good, sometimes very small transactions in it)
accounts payable (the best)
Director
Finance Director
Financial Controller
Accounts Payables
Accounts Receivables

text me for your request only DM here on exploit. Deals through guarantor

Actual seller's ad on Exploit.in

2019 School Cyber Attacks



How does cyber security fit into your risk management plan?

UNITEL

Cyber Risk Management

Mike Reed
UNITEL Risk Advisor
402-434-7200
mreed@unitelinsurance.com

Companies Are Diversifying

- Focus on larger enterprise customers
- Implementing of acquiring new business strategies
  - MSPs
  - Tech services
  - CLEC
  - Security
  - Strategic partnerships
  - Software and tech subsidiaries

The Effects of Diversification

- New exposures
- New skill sets
- New type of customers
  - More sophisticated including demands
- Need for updating processes and procedures
- Different types of company structure and management

White House Order

- June 12th – ransomware notification
- Implement best practices from executive order
  - MFA: multi-factoring authentication
    - Passwords are routinely compromised
  - Endpoint detection and response
    - Malicious activity on network
  - Encryption
    - Protects data if stolen
  - Implement and empower security team
    - Handle proactive processes and procedures

What We Are Seeing

- Claim amounts and frequency of claims increasing
  - Ransomware average claim now approaching $300,000
- Carriers forms are changing:
  - First-party – “You”
    - 90%+ claims are happening to “you”
  - Third-party is “others”
- Carriers are all concerned of risk
  - Upward rate pressure
- Liability concerns with MSPs
  - SolarWinds
  - Kaseya
- Additional risk controls and supplemental apps
- Need for additional sub-limits
  - New coverages such as
    - Contingent bodily injury/property damage
    - Bricking
    - Invoice manipulation
    - Crypto jacking

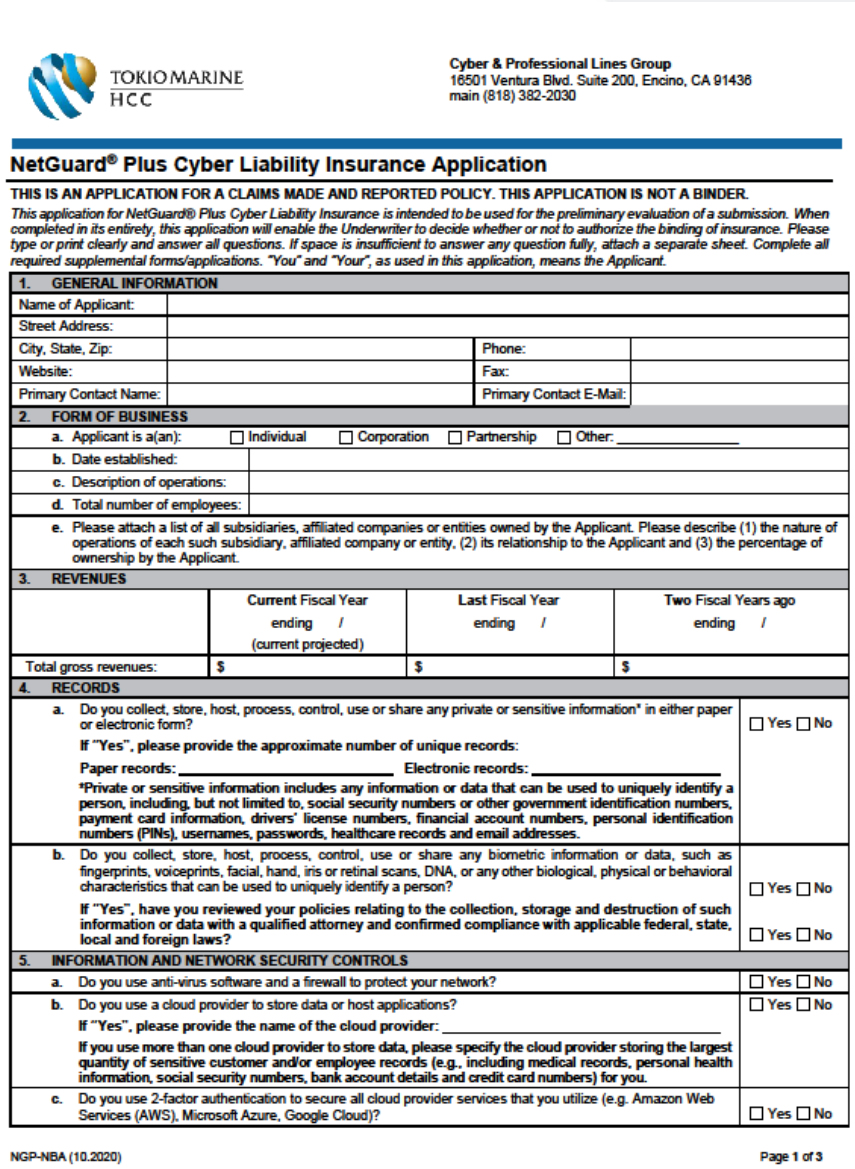
Claim Trends in Telecom

Top Claims

- Ransomware
- Social engineering
- Invoice manipulation
- MSP exposures

Underwriting Concerns

- Additional supplemental apps
- Additional risk controls
  - Multi-factoring authentication
  - Offsite backups
  - Vendor selection



TOKIO MARINE HCC

Cyber & Professional Lines Group
16501 Ventura Blvd. Suite 200, Encino, CA 91436
main (818) 382-2030

NetGuard® Plus Cyber Liability Insurance Application

THIS IS AN APPLICATION FOR A CLAIMS MADE AND REPORTED POLICY. THIS APPLICATION IS NOT A BINDER.

This application for NetGuard® Plus Cyber Liability Insurance is intended to be used for the preliminary evaluation of a submission. When completed in its entirety, this application will enable the Underwriter to decide whether or not to authorize the binding of insurance. Please type or print clearly and answer all questions. If space is insufficient to answer any question fully, attach a separate sheet. Complete all required supplemental forms/applications. "You" and "Your", as used in this application, means the Applicant.

1. GENERAL INFORMATION

Name of Applicant:			
Street Address:			
City, State, Zip:		Phone:	
Website:		Fax:	
Primary Contact Name:		Primary Contact E-Mail:	

2. FORM OF BUSINESS

a. Applicant is a(an): ☐ Individual ☐ Corporation ☐ Partnership ☐ Other: _____

b. Date established:

c. Description of operations:

d. Total number of employees:

e. Please attach a list of all subsidiaries, affiliated companies or entities owned by the Applicant. Please describe (1) the nature of operations of each such subsidiary, affiliated company or entity, (2) its relationship to the Applicant and (3) the percentage of ownership by the Applicant.

3. REVENUES

	Current Fiscal Year ending / (current projected)	Last Fiscal Year ending /	Two Fiscal Years ago ending /
Total gross revenues:	$	$	$

4. RECORDS

a. Do you collect, store, host, process, control, use or share any private or sensitive information* in either paper or electronic form? ☐ Yes ☐ No

If "Yes", please provide the approximate number of unique records:

Paper records: _____ **Electronic records:** _____

***Private or sensitive information includes any information or data that can be used to uniquely identify a person, including, but not limited to, social security numbers or other government identification numbers, payment card information, drivers' license numbers, financial account numbers, personal identification numbers (PINs), usernames, passwords, healthcare records and email addresses.**

b. Do you collect, store, host, process, control, use or share any biometric information or data, such as fingerprints, voiceprints, facial, hand, iris or retinal scans, DNA, or any other biological, physical or behavioral characteristics that can be used to uniquely identify a person? ☐ Yes ☐ No

If "Yes", have you reviewed your policies relating to the collection, storage and destruction of such information or data with a qualified attorney and confirmed compliance with applicable federal, state, local and foreign laws? ☐ Yes ☐ No

5. INFORMATION AND NETWORK SECURITY CONTROLS

a. Do you use anti-virus software and a firewall to protect your network? ☐ Yes ☐ No

b. Do you use a cloud provider to store data or host applications? ☐ Yes ☐ No

If "Yes", please provide the name of the cloud provider: _____

If you use more than one cloud provider to store data, please specify the cloud provider storing the largest quantity of sensitive customer and/or employee records (e.g., including medical records, personal health information, social security numbers, bank account details and credit card numbers) for you.

c. Do you use 2-factor authentication to secure all cloud provider services that you utilize (e.g. Amazon Web Services (AWS), Microsoft Azure, Google Cloud)? ☐ Yes ☐ No

NGP-NBA (10.2020) Page 1 of 3

Being Proactive

- Documents
  - Cyber Response Guide
  - Cyber Security Prep and Response Guide

Takeaways

- Be proactive – processes and procedures
- Align your team with the insurance carriers
  - Service plans understand your carriers and forms are changing all the time
- Utilize 3rd party resources
- Review cyber protocols/procedures with risk management team
- Rates and risks are both climbing
- Before you sign a contract – check with carriers
- Cyber forms are different and are changing!

UNITEL

Responsive Technology Partners

Steven McComas MPA, MBA, CGMA, CPA
Chief Executive Officer – Responsive Technology Partners, Inc
Chief Financial Officer – Pineland Telephone Cooperative, Inc.

Mike Reed
Risk Advisor—UNITEL Insurance