VAcorp

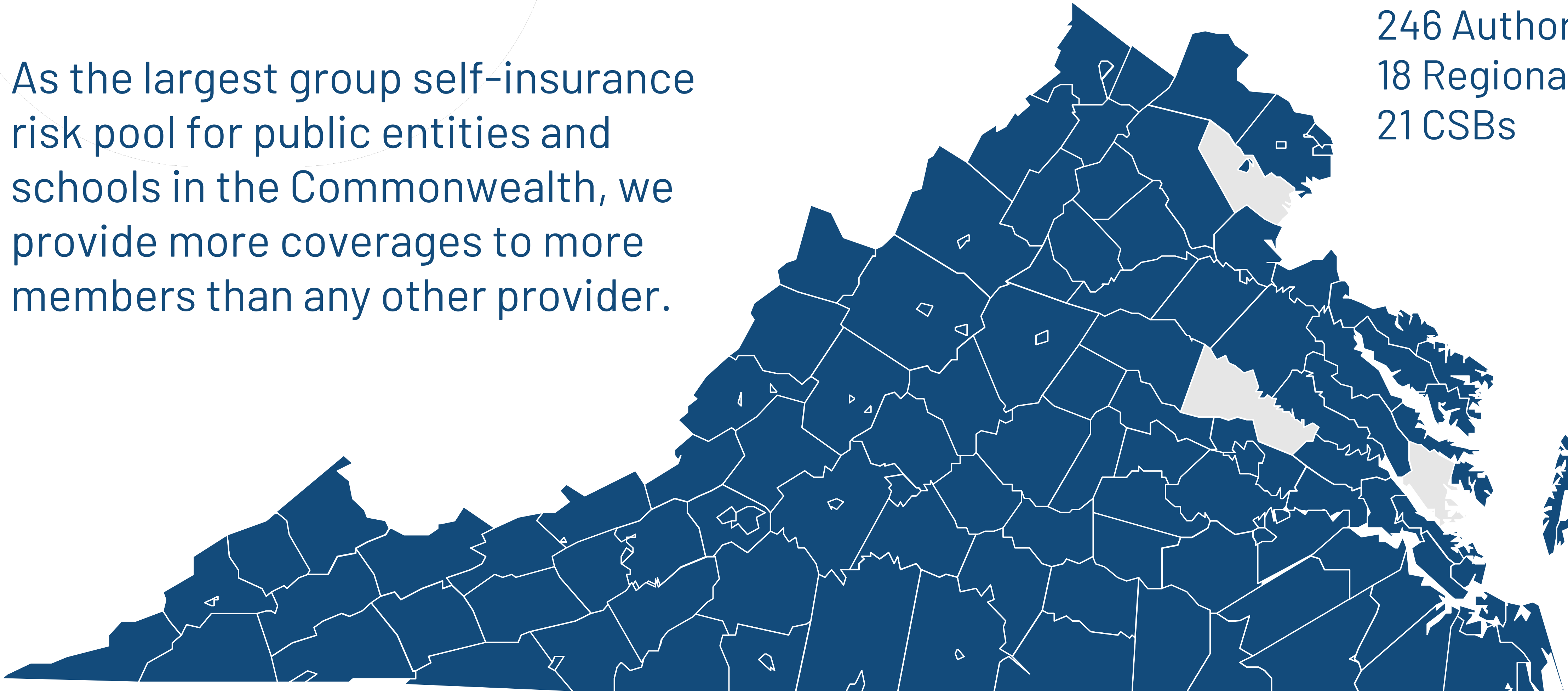
Cyber Security Exposures

Innovation Meets Cybersecurity

We know the unique risks you face. We know how to respond.

Our strength is in our numbers.
Our stability is in our members.

As the largest group self-insurance risk pool for public entities and schools in the Commonwealth, we provide more coverages to more members than any other provider.



527 Members
88 Counties
126 School Divisions
28 Municipalities
246 Authorities
18 Regional Jails
21 CSBs

VAcorp

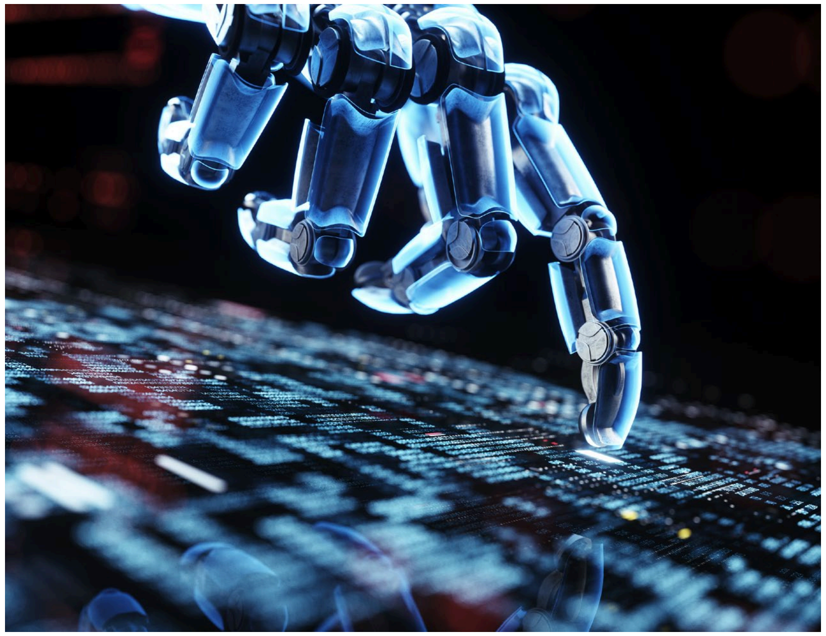
We've got you covered.

Cyber Breach:

It’s Not **If**
It’s **When**

Phishing

- Email with Links
- Requests Action (renew account; keep from being cancelled; confirmation of order)
- Obtains personal information
  - Accounts
  - Passwords
  - Activation



- Designed to look familiar - trust
- Gateway to systems (protected and unprotected)
  - Malware

Phishing

- Email seeking update of streaming user information. “*Click Here* to review and update user profile. Your subscription will expire without this important action.”
  - Asked demographic information
  - Sought to reset password – asked for old and new
- Email confirming online order. “You must *Follow Link* to confirm order prior to shipping.” No order ever submitted – not a patron of that organization.

Social Engineering

Intentionally misleading a person by means of a dishonest transfer statement or misrepresentation of a material fact via electronic or telephonic communication.

The Fraud:

1. Good faith transfer of funds by someone who was misled by Social Engineering communication believing a payment request was valid.
2. Theft of funds due to unauthorized access to a network.

Social Engineering

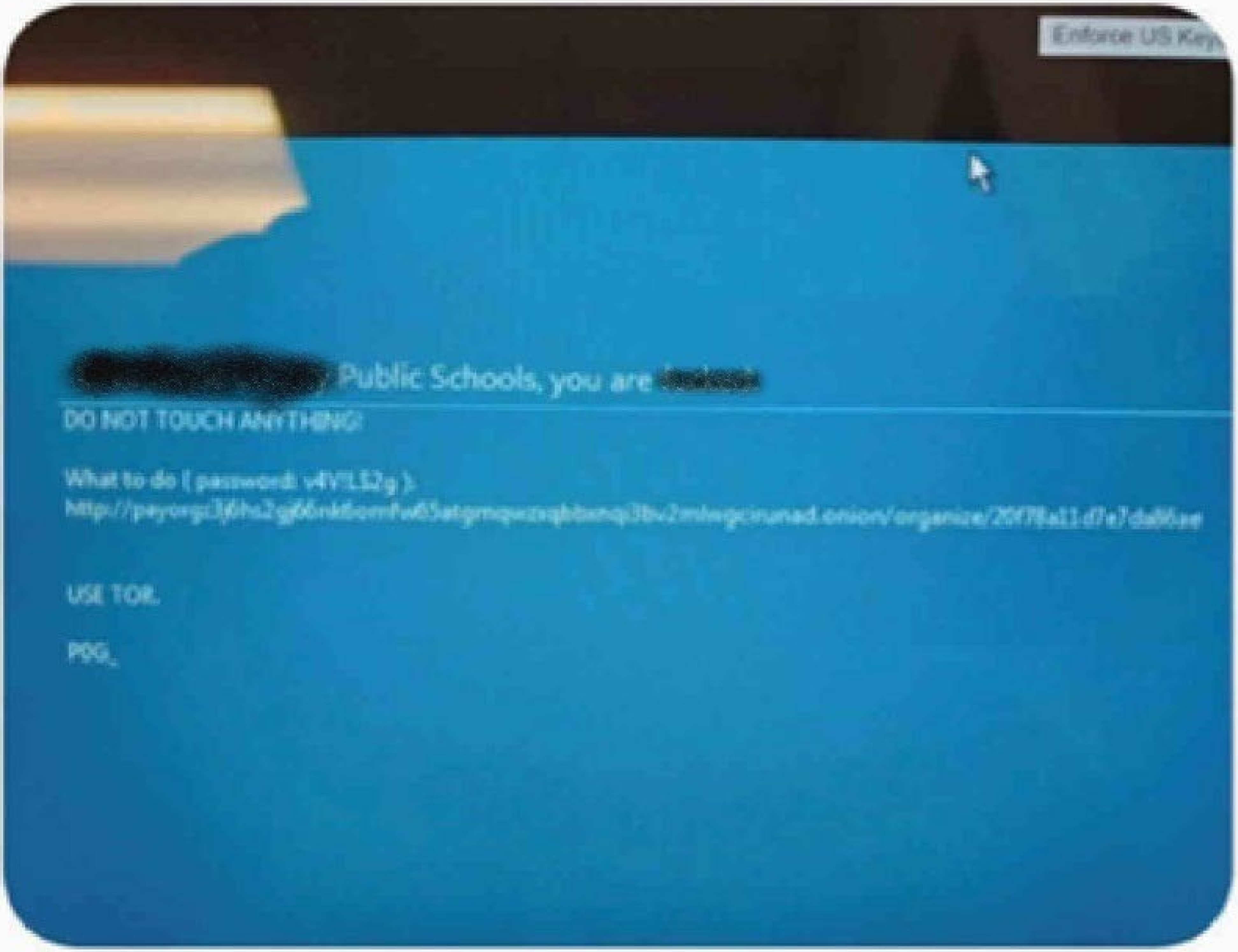
- Email stating, “contractor no longer accepting checks.” Sent bank account information.
  - $285,000 transferred

- Email from purported employee stating, “need funds to be transferred quickly.” First was sent. Subsequent requests for more funds. Real employee got involved.
  - $10,000

Double Extortion

- As name implies – two elements:
  - Embedding code/exfiltrating data for ransom
  - Locking systems and engaging ransomware
- Actors covertly enter system
- Period of weeks or months
- Bad actor may not know whose system it is
- Chooses to lock systems – Threaten to release information on the dark web
- Sends “customer service” email

Delivery



[redacted] Public Schools, you are [redacted]

DO NOT TOUCH ANYTHING!

What to do (password: v4V!L52g):
http://peyorgc3j6hs2gj66nk6omfw65atgmqwzxqbbxnqi3bv2mlwgcirunad.onion/organize/20f78a11d7e7da66ae

USE TOR.

PDG_

This message contains an information how to fix the troubles you've got with your network.

Files on the workstations in your network were encrypted and any your attempt to change, decrypt or rename them could destroy the content. The only way to get files back is a decryption with Key, provided by (us).

It's not a threat, on the contrary - it's a manual how to get a way out.

(Threat Actor) doesn't aim to damage your company, our goals are only financial. After a payment you'll get network decryption, full destruction of downloaded data, information about your network vulnerabilities and penetration points.

If you decide not to negotiate, in 48 hours the fact of the attack and all your information will be posted on our site and will be promoted among dozens of cyber forums, news agencies, websites etc.

To contact our support and start the negotiations, please visit our support chat.
It is simple, secure and you can set a password to avoid intervention of unauthorised persons. …LINKY LINKY…

- Note that this server is available via Tor browser only.

P.S. How to get TOR browser - see at…

Operations and Services

1. General Operations (local gov't; education)
2. Private Health Information (PHI)
3. Law Enforcement (911, Sheriff, etc.)
4. Voting
5. Utilities

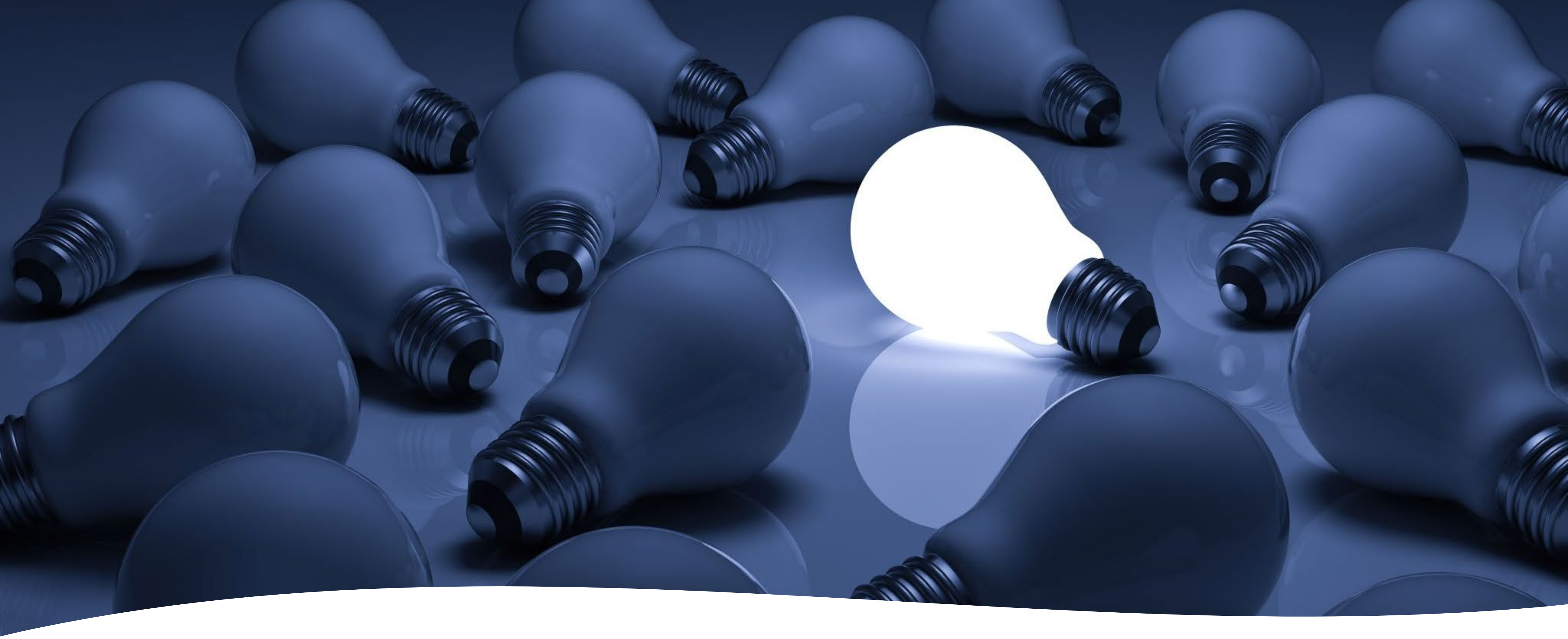
Cyber Liability Coverage

- Coverage designed to protect organizations from the consequences of various cyber attacks
- Excluded on typical GL or Property policies
- No standard cyber policy

Insurance Industry Market Trends

- Local government cases have been large
  - $1,500,000 Ransom event
  - $700,000 Social Engineering Event
- Escalating Professional Services costs
- Evolving Sophistication of Threat Actors

- Tightening underwriting guidelines
- Changes to exclusions
- Addition of sublimits
- Removal of coverage
- Elevated deductibles



VAcorp’s Solution

1. Broad Coverage for the widest array of exposure
2. Zero Deductible
3. No Sublimits
4. Cyber Breach Coach/Attorney
5. Training – Staff and Supervisory Levels

A Guide You Can Trust

Cyber Breach Coach

- Skilled Attorney -Today’s Threats and Tomorrow’s Risks
- Secures Attorney Client Privilege
- Engages Necessary Third Parties
  - Law Enforcement, Forensic Firms, Public Relations
- Identifies Reporting Necessity
- Knows Specialties of Forensic Firms
- Accessible Throughout Event

Coverage Elements

- Data Breach Incident Response

  Data Breach:
  Electronic acquisition, access, or disclosure of Personally Identifiable Information or non-public corporate information in the one's care, custody, or control by a person or entity (including a rogue employee) that is unauthorized by the entity.

Coverage Elements

- Data Breach Incident Response
  - Forensic Services
  - Legal Services
  - Notification Services
  - Fraud Monitoring and Resolution
  - Call Center
  - Public Relations

Coverage Elements

- Data Restoration
  - What is still viable
  - Are there backups – layers?
  - Data upload

Coverage Elements

- Ransomware
  - Extortion costs
  - Negotiations
- Media Liability
  - Release of Content – violations, liabilities, etc.
  - Through Website or Social Media

Coverage Elements

- Breach Liability
  - Network Security
    - Access
    - Malicious Code
  - Privacy
  - Data

Payment:

- Expenses – defense, inv., appeal, etc.
- Damages to third parties

Coverage Elements

- Regulatory Liability
  - Claim expenses – Defense, Investigation
  - Penalties – levied by a governmental agency
  - Regulatory Proceedings
- PCI Fines and Assessments
  - Obligation for Merchant Services Agreement
    - Accepting Payment via credit/debit cards
  - Penalties – Gov't agency or regulatory authority

Coverage Elements

- Social Engineering Event

  Transfer Fraud

  Caused by Fraudulent Instruction

  Loss of funds by entity making transfer

Incident Response Plan

- Define a team
- Determine roles and responsibilities
- Create internal communication path
- Train all levels
- Establish Single point of contact
- Review plan at least annually
- Test the plan

Suspected Cyber Incident

- Act quickly
- Implement your Incident Response Plan
- Notify Provider
- Protect your data
  - Take machines and information offline
- Document as much as possible

```
ce;z-index:999;
}.gbrtl .gbm{-m
block;position:a
;*top:-2px;*left:
px\0/;left:-6px\0
isplay:inline-bloc
block;list-style:n
;line-height:27px;
;display:block;tex
index:1000}.gbts{*
right:9px}#gbz .g
```

Provide Information

- Main contact/conduit at entity
- Log Information
- Name/Contact of ISP, Contract IT, and Third Party email/web support
- Copy of email and/or ransom message
- Wire transfer information
- Known users on affected machine(s)
- Email: cloud-based or on site (365, Gmail, etc)

Suspected Cyber Incident

- VAcorp members will be assigned a Breach Coach based on event type
  - Determine other players to get involved
    - Legal counsel
    - Forensics
    - Law enforcement
  - Assist with Public Relations
- Make no public statement without consulting Coach

Suspected Cyber Incident

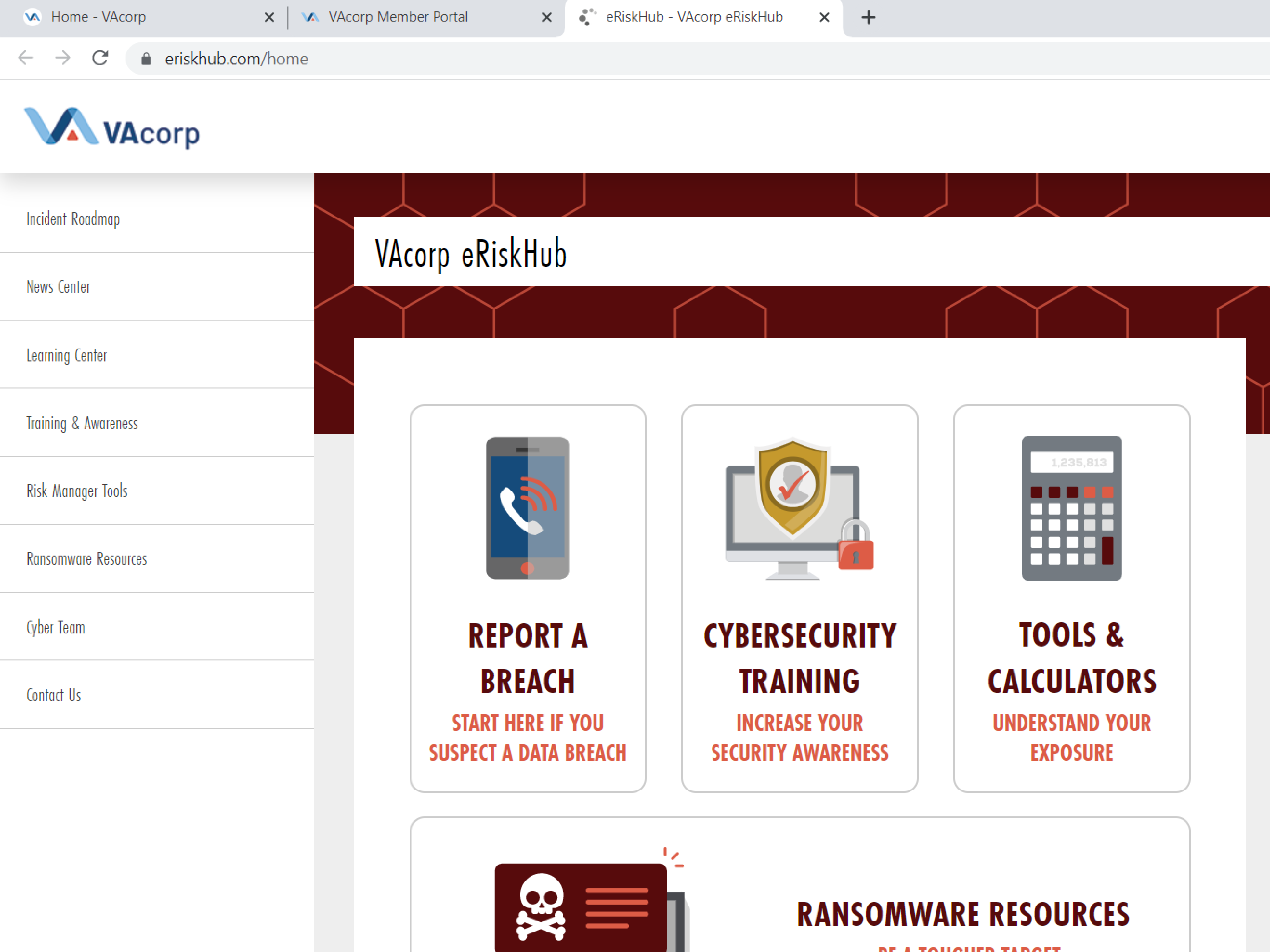
- Speak with provider before anyone else
    - Do not enter into an agreement with an outside provider for an event before obtaining authority
    - The law does not require notification if the compromised data is encrypted

```
ce;z-index:999;
}.gbrtl .gbm{-m
block;position:a
;*top:-2px;*left:
px\0/;left:-6px\0
isplay:inline-bloc
block;list-style:n
;line-height:27px;
;display:block;tex
index:1000}.gbts{*
right:9px}#gbz .g
```

Additional Support

- Additional Cyber Security training for members available at www.VAcorp.org

- Talk to your Member Services or Risk Control representative for more information on your coverage or additional resources



Home - VAcorp

VAcorp Member Portal

eRiskHub - VAcorp eRiskHub

eriskhub.com/home

VAcorp

Incident Roadmap

News Center

Learning Center

Training & Awareness

Risk Manager Tools

Ransomware Resources

Cyber Team

Contact Us

VAcorp eRiskHub

REPORT A BREACH

START HERE IF YOU SUSPECT A DATA BREACH

CYBERSECURITY TRAINING

INCREASE YOUR SECURITY AWARENESS

TOOLS & CALCULATORS

UNDERSTAND YOUR EXPOSURE

RANSOMWARE RESOURCES

BE A TOUGHER TARGET

VAcorp

Thank You!

888-822-6772 | www.VAcorp.org