VAcorp

Cyber Liability: Lessons Learned

2023 VASBO Conference

Agenda

- Industry Trends
- Today’s largest cyber threats
- Mitigation strategies
- Incident Response

VAcorp

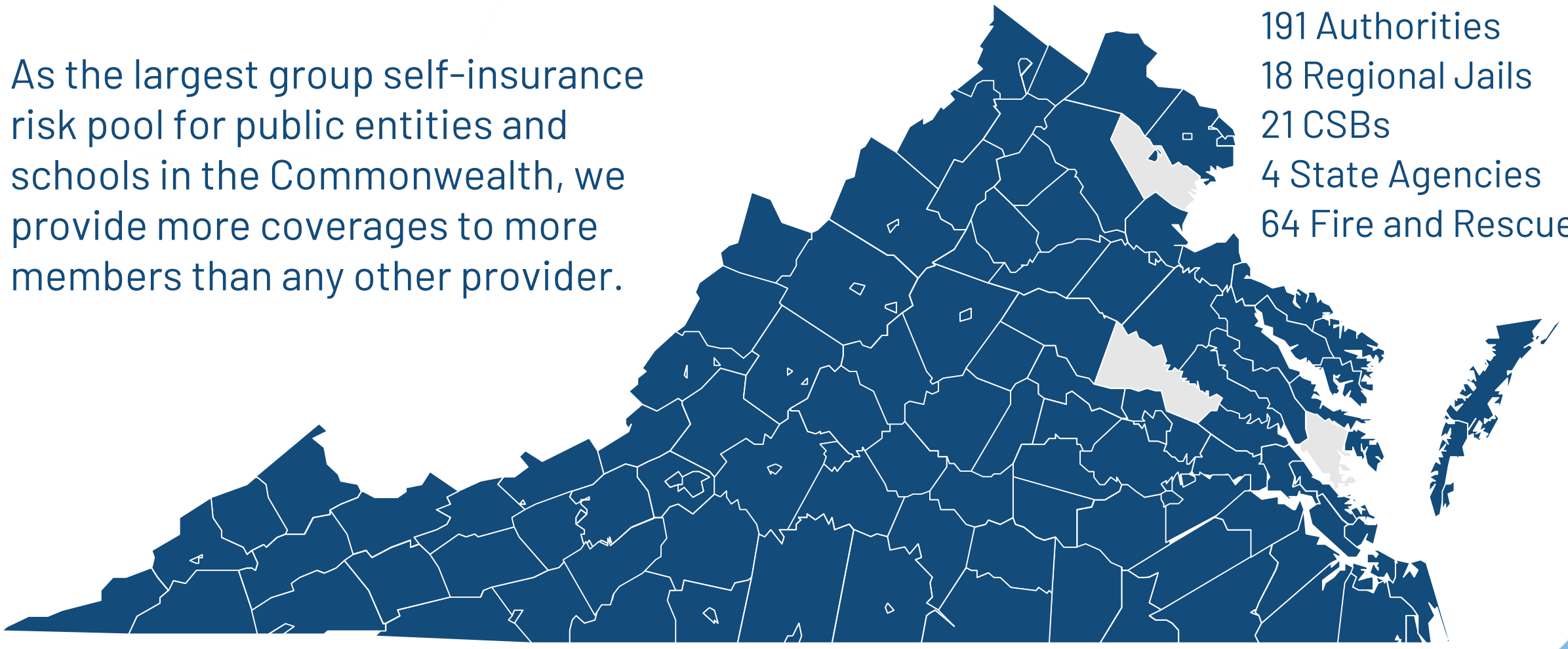
- Formed in 1993
- Self-Insurance Risk Pool
- Property & Casualty and Workers' Compensation
- Risk management services
- Owned and governed by our members

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

VAcorp

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.



548 Members
89 Counties
128 School Divisions
33 Municipalities
191 Authorities
18 Regional Jails
21 CSBs
4 State Agencies
64 Fire and Rescue

Coverages

- Property
- Auto
- Environmental Liability
- Inland Marine
- General Liability
- Cyber Liability
- Equipment Breakdown
- Public Officials Liability
- Workers' Compensation
- Crime
- Educators Legal Liability
- Excess Limits
- Volunteer Accident
- Student Accident
- Security Risk Management

Cyber Liability

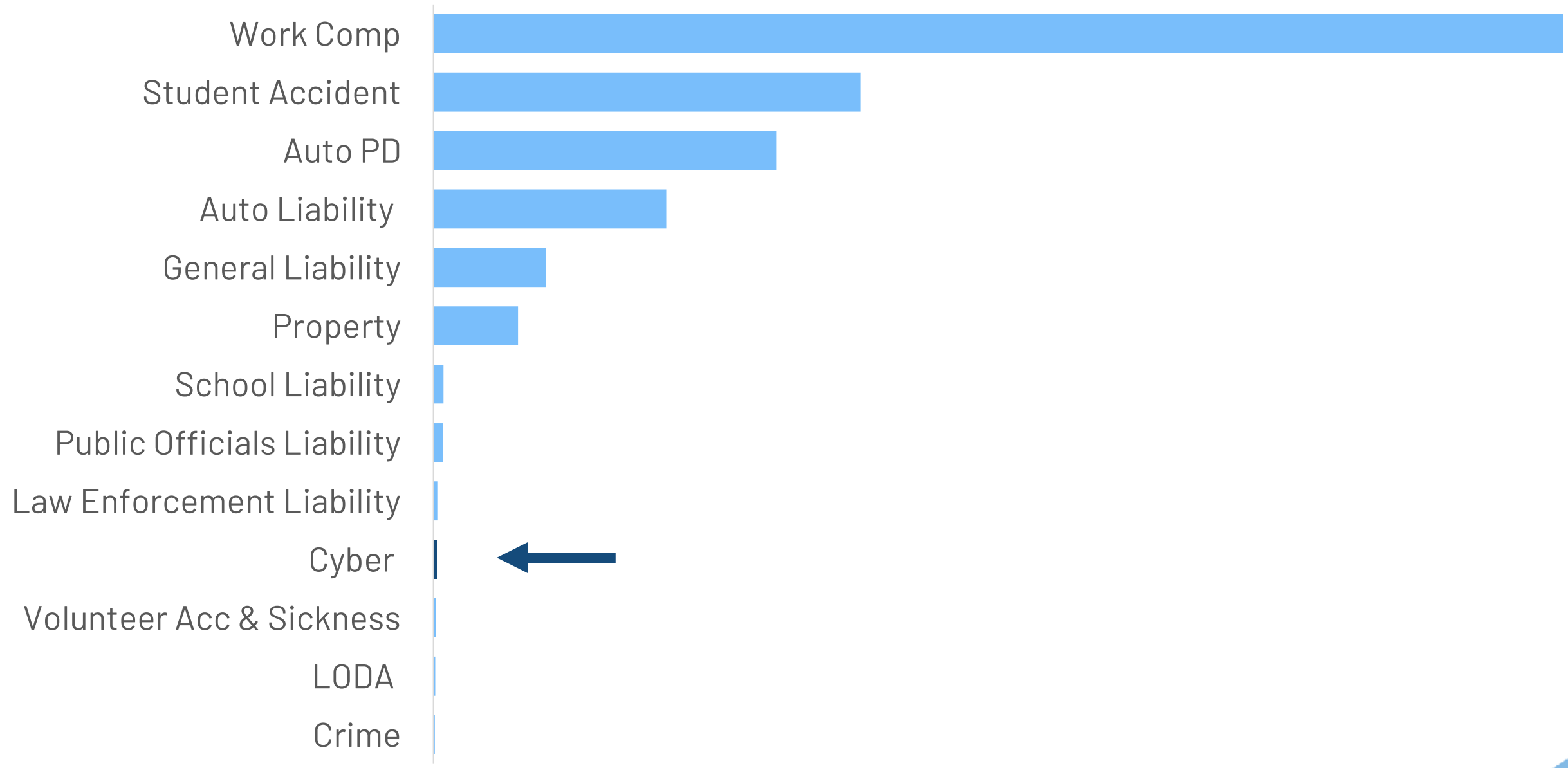
Designed to protect from the consequences of various cyber attacks

- First Party Coverages
  - Legal expenses
  - IT forensics expenses
  - Data restoration
  - Breach notification to public
  - Regulatory Fines
  - Public relations expertise
- Third Party Coverages
  - Privacy and security liability
  - Multimedia liability – plagiarism, defamation, copyright infringement

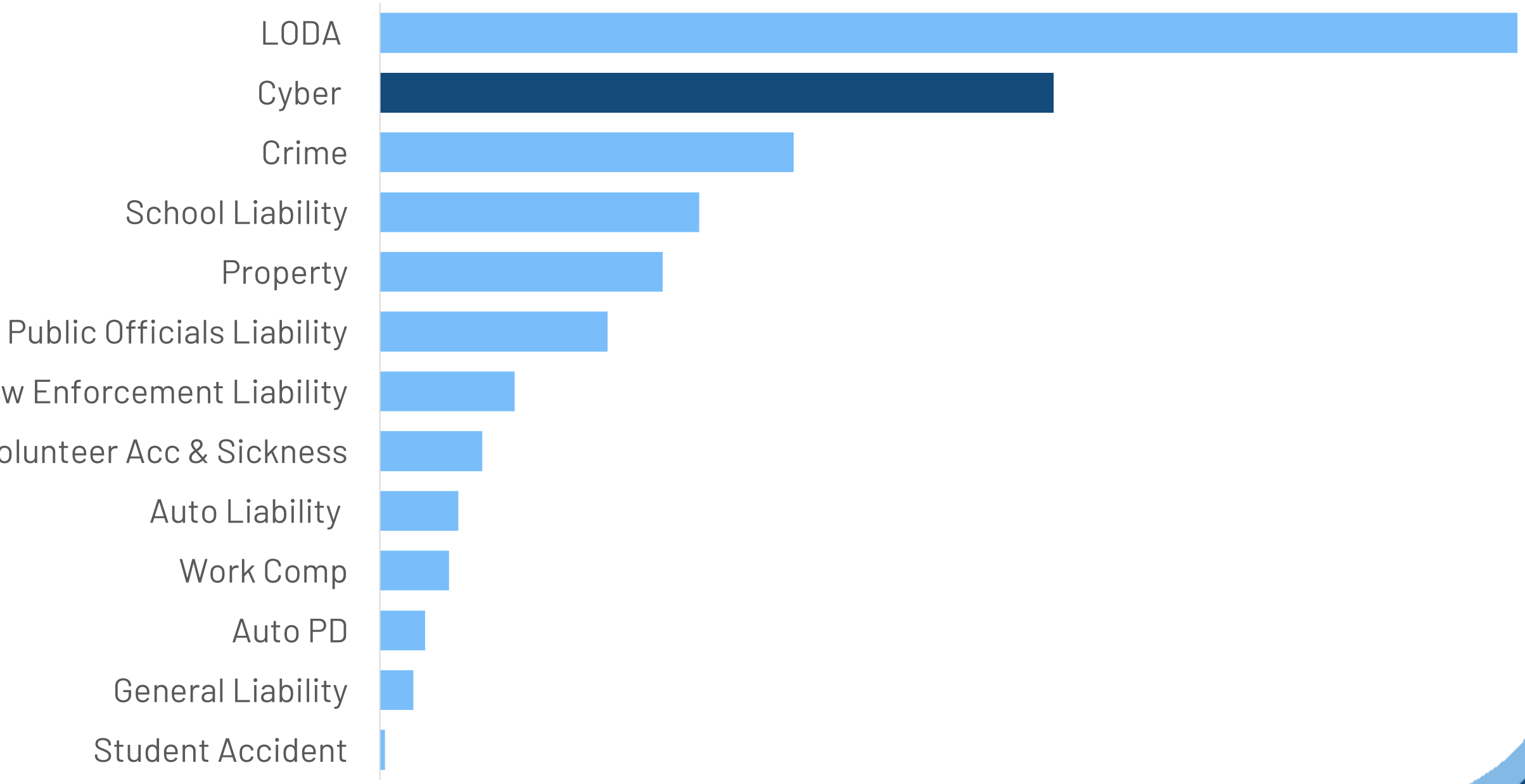
VAcorp Cyber Coverage

- Data Breach Liability
- Privacy Liability
- Network Liability
- Internet Media Liability
- Regulatory Liability
- Security Coverage
- Social Engineering Fraud
- Telecommunications Fraud
- Ransomware
- Fraudulent Instruction
- Regulatory Liability
- Data Breach Incident Response
- Data Restoration
- PCI DSS Fines
- Public Relations Event Response

Number of Claims



Average Cost per Claim



Insurance Industry Market Trends

- Local government cases have been large
- Escalating Professional Services costs
- Tightening underwriting guidelines
  - Changes to exclusions
  - Addition of sublimits
  - Removal of coverage
  - Elevated deductibles

Cyber Crime on the Rise

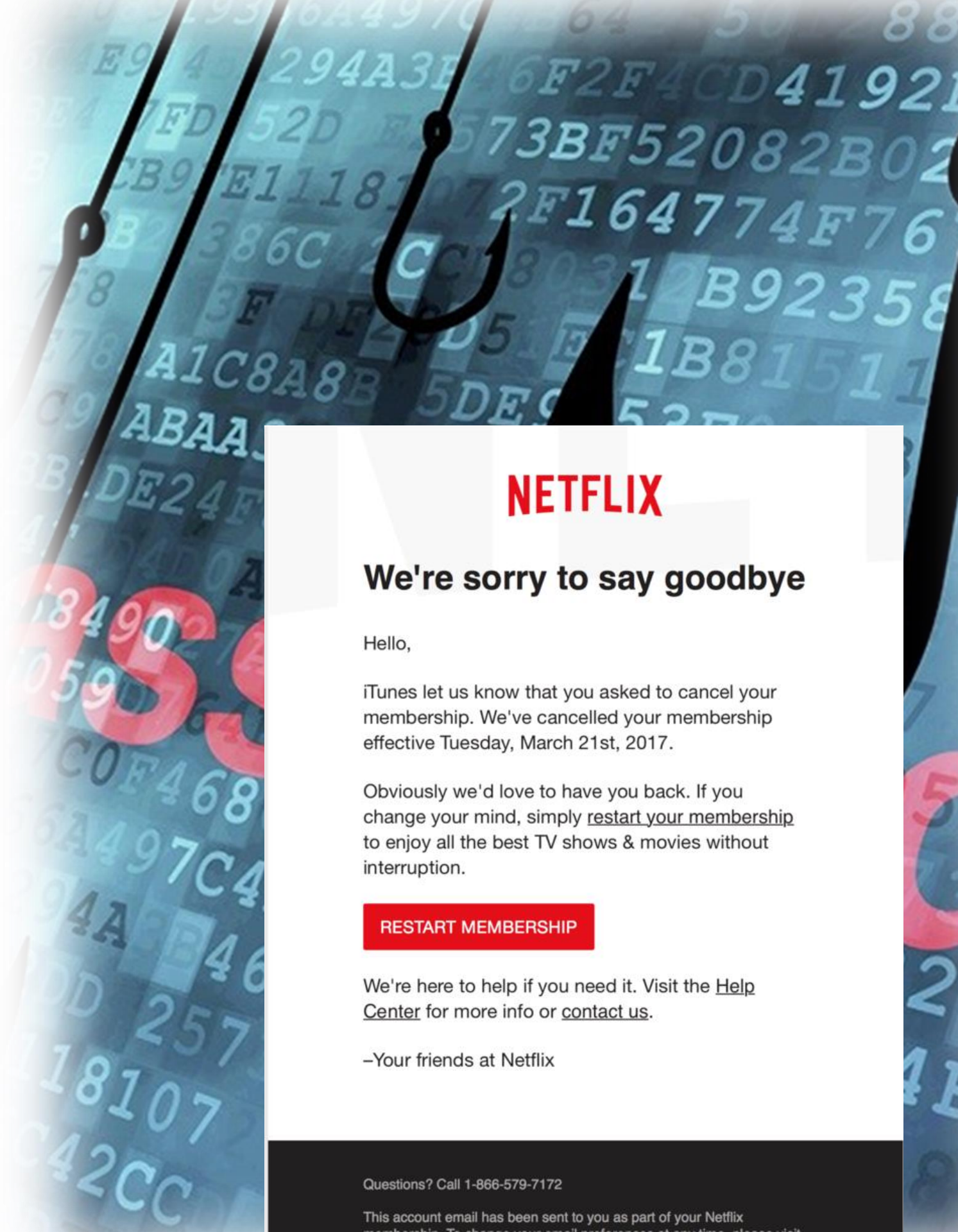
- Cyber crime continues to increase each year
  - Attacks are becoming more sophisticated
- Public sector entities are often targeted

Key Exposure for Schools - BEC

- Business Email Compromise
  - Threat actor obtains access to an email inbox
  - Type of Social Engineering attack
    - Broad term that connotes using psychological manipulation to trick users into making security mistakes or giving away sensitive information
  - “Phishing” is a social engineering attack

Phishing

- Majority of cyber attacks begin with a phishing attack
  - Designed to look familiar
    - Prey on trust
  - Email with Links
  - Requests Action (renew account; keep from being cancelled; confirmation of order)
  - Seeking personal information
    - Accounts
    - Passwords
    - Activation



Phishing Terminology

Phishing vs. Spear Phishing vs. Whaling

Phishing

Uses **mass emails** to trick **individuals and groups** into revealing sensitive information.

Spear Phishing

Uses **personalized emails** to trick **individuals** into revealing information.

Whaling

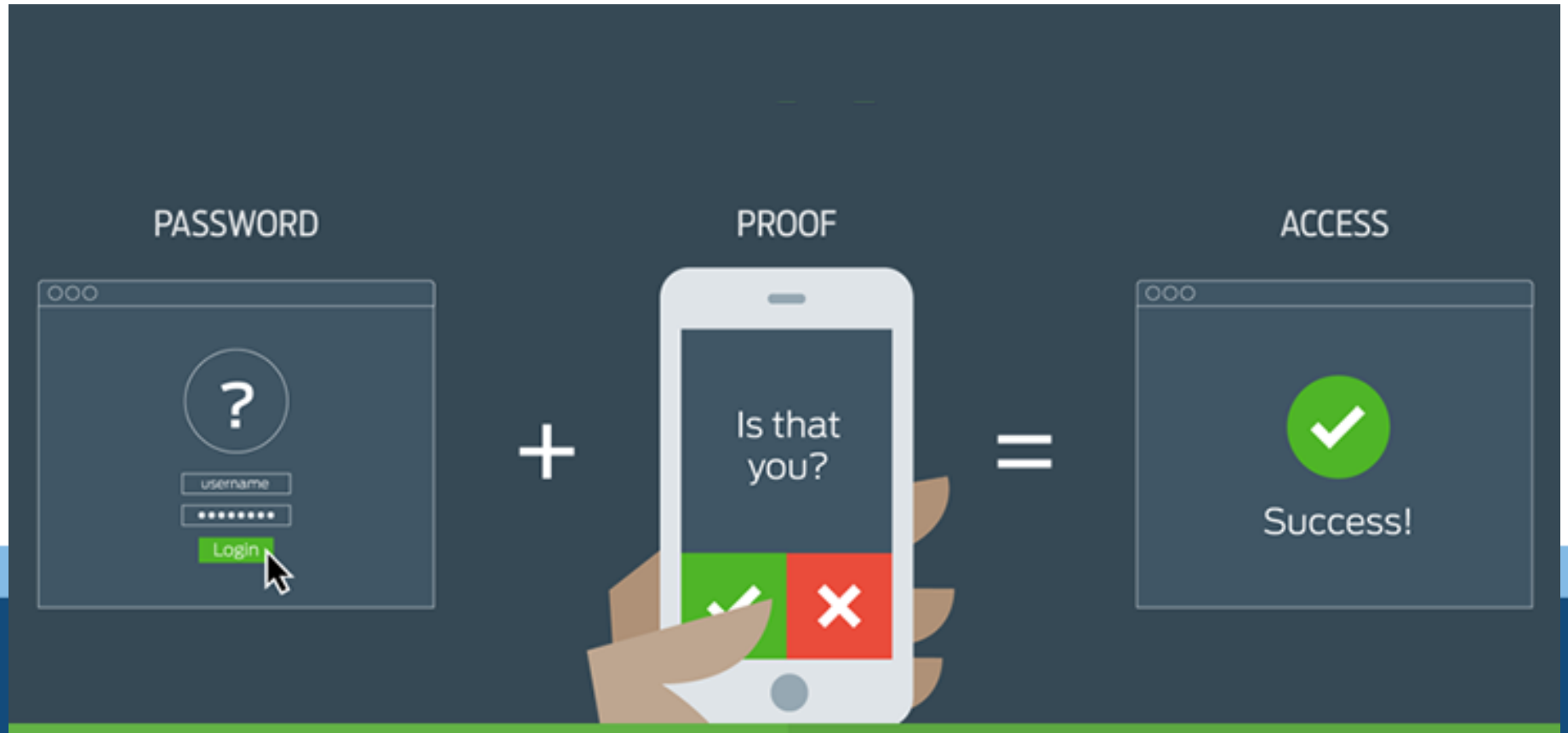
Uses **personalized emails** to trick **high-value targets** into revealing information.

Key Exposure for Schools - BEC

- Business Email Compromise
  - Target specific individuals (spear phishing)
  - Typically involve advance research and personalization
  - Do not contain malware or malicious links
    - Bypass security filters

Key Exposure for Schools - BEC

- Business Email Compromise
  - Threat actor obtains access to an email inbox
- Who is at risk?
  - Schools not using MFA on Microsoft 365/Google



Key Exposure for Schools - BEC

- Business Email Compromise
  - Threat actor obtains access to an email inbox
- Who is at risk?
  - Schools not using MFA on Microsoft 365/Google
    - Employee enters credentials into a spammed message or Google form
  - Schools using MFA without adequate training

Why was MFA ineffective?

- MFA Fatigue
  - In some cases where schools had MFA in place, the end user accepted the prompt to admit access
  - Employees may not have understood that the system only sends the prompt when someone is attempting to access the inbox and simply accepted it
- Example: Some employees accepted 10+ attempts in a row
  - Mitigation: System should trigger a lock after 3 bad attempts

BEC Examples

- Ex. 1: Email “from principal” requesting change in direct deposit account. Change effected.
  - Principal called after not receiving payroll deposit.
- Ex. 2: Email stating, “contractor no longer accepting checks.” Send bank account information.
  - $285,000 transferred

- Prevent this by:
  - Require in person payroll changes
  - Reach out by phone to confirm

BEC Consequences

- Instructions from trusted source
- Information is at stake
  - PII (personal identifying information)
    - Notice given to 12,000 individuals
  - PHI (protected health information)
    - Triggers Virginia Medical Record's Breach Statute
      - Difficult to navigate

"Medical information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:

1. Any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or

2. An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

Double Extortion

- Typically introduced via spoofing email to change payroll or third-party payments
- 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
- Locks systems/threatens to release information on the dark web

>_ CL0P^_- LEAKS

HOME HOW TO DOWNLOAD? MVTEC.COM NFT.CO.UK INRIX.COM EXECUPHARM.COM

TWL.DE PLANATOL.DE INDIABULLS.COM PROMINENT.COM NETZSCH.COM PRETTL.COM

SOFTWAREAG.COM ALLSTATEPETERBILT.COM NOVABIOMEDICAL.COM PARKLAND.CA

ELANDRETAIL.COM SYMRISE.COM AMEY.CO.UK THE7STARS.CO.UK EAGLE.ORG

FUGRO.COM SINGTEL.COM DANAHER.COM PENTAIR.COM JONESDAY.COM STERIS.COM

CGG.COM TRANSPORT.NSW.GOV.AU BOMBARDIER.COM CSAGROUP.ORG FLAGSTAR.COM

CSX.COM NOWFOODS.COM KINZE.COM MMOSER.COM QUALYS.COM WRIGHT.COM

EDAG.COM COLORADO.EDU MIAMI.EDU RACETRAC.COM MARNELLCOMPANIES.COM

YU.EDU UMD.EDU UNIVERSITYOFCALIFORNIA.EDU **STANFORD.EDU** SHELL.COM

PNCPA.COM NIPRO.COM DURHAM.CA TRAVELSTORE.COM SIUMED.EDU FOODLAND.COM

BOUTINEXPRESS.COM RFF.ORG SGS-LAW.COM AUROBINDO.COM UTILITYTRAILER.COM

Akira Ransomware

- Launched in March 2023
- Basic functionality:
  - Exfiltrates data
  - Deletes Windows Volume Shadow copies (back-ups)
  - Encrypts virtual server environment
    - All files with extensions:

.abcddb, .abs, .abx, .accdb, .accdc, .accde, .accdr, .accdt, .accdw, .accft, .adb, .ade, .adf, .adn, .adp, .alf, .arc, .ask, .avdx, .avhd, .bdf, .bin, .btr, .cat, .cdb, .ckp, .cma, .cpd, .dacpac, .dad, .dadiagrams, .daschema, .db-shm, .db-wal, .dbc, .dbf, .dbs, .dbt, .dbv, .dbx, .dcb, .dct, .dcx, .ddl, .dlis, .dqy, .dsk, .dsn, .dtsx, .dxl, .eco, .ecx, .edb, .epim, .exb, .fcd, .fdb, .fic, .fmp, .fmp12, .fmpsl, .fol, .fpt, .frm, .gdb, .grdb, .gwi, .hdb, .his, .hjt, .icg, .icr, .idb, .ihx, .iso, .itdb, .itw, .jet, .jtx, .kdb, .kdb, .kexi, .kexic, .kexis, .lgc, .lut, .lwx, .maf, .maq, .mar, .mas, .mav, .maw, .mdb, .mdf, .mdn, .mdt, .mpd, .mrg, .mud, .mwb, .myd, .ndf, .nnt, .nrmlib, .nsf, .nvram, .nwdb, .nyf, .odb, .oqy, .ora, .orx, .owc, .pan, .pdb, .pdm, .pnz, .pvm, .qcow2, .qry, .qvd, .raw, .rbf, .rctd, .rod, .rodx, .rpd, .rsd, .sas7bdat, .sbf, .scx, .sdb, .sdc, .sdf, .sis, .spq, .sql, .sqlite, .sqlite3, .sqlitedb, .subvol, .temx, .tmd, .tps, .trc, .trm, .udb, .udl, .usr, .vdi, .vhd, .vhdx, .vis, .vmcx, .vmdk, .vmem, .vmrs, .vmsd, .vmsn, .vmx, .vpd, .vsv, .vvv, .wdb, .wmdb, .wrk, .xdb, .xld, .xmlff

Akira Ransomware

- Drops ransom note into every folder with encrypted files
  - "Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will study in depth your finance, bank & income statements, your savings, investments etc. and present our reasonable demand to you. If you have an active cyber insurance, let us know and we will guide you how to properly use it. Also, dragging out the negotiation process will lead to failing of a deal."
  - "We will try to sell personal information/trade secrets/databases/source codes - generally speaking, everything that has a value on the darkmarket - to multiple threat actors at ones. Then all of this will be published in our blog."
- Extortion ranges from $200,000 to millions

Common Culprits

- Out-of-date patching
- Legacy systems
- Software updates often contain critical security patches— **unpatched systems are a major vector for attacks**
- Periodically restart the computer

Suspected Cyber Incident

- **Notify VAcorp**
- Act quickly
- Implement your Incident Response Plan
- Protect your data
  - Take machines off networks and information offline
  - Preserve all logs
- Document as much as possible

Suspected Cyber Incident

- 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
  - 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 or contact third parties without consulting Coach**

Breach Coach

- Skilled, Specialized Attorney
- 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

Beth Waller
540-983-7625
bwaller@woodsrogers.com

WOODS ROGERS
VANDEVENTER BLACK
ATTORNEYS AT LAW

Attorney-Client Privilege

- Protects from FOIA and discovery requests
- Important that all communications are protected
  - All email traffic concerning the incident must copy counsel
- Clear all public statements with counsel

Incident Response

1 Investigation

- Determining what happened and the scope of affected systems and data

2 Recovery

- Containing the attack, eradicating malware, and returning to normal operations

3 Legal Operations

- Providing required notices and meeting other legal requirements, as needed

Guidance from the Treasury on Ransomware

On October 1, 2020, the Treasury issued guidance threatening sanctions against any organizations or financial institutions (insurers) that makes ransom payments to certain criminal groups.

Incident Response Plan

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

Educate Employees

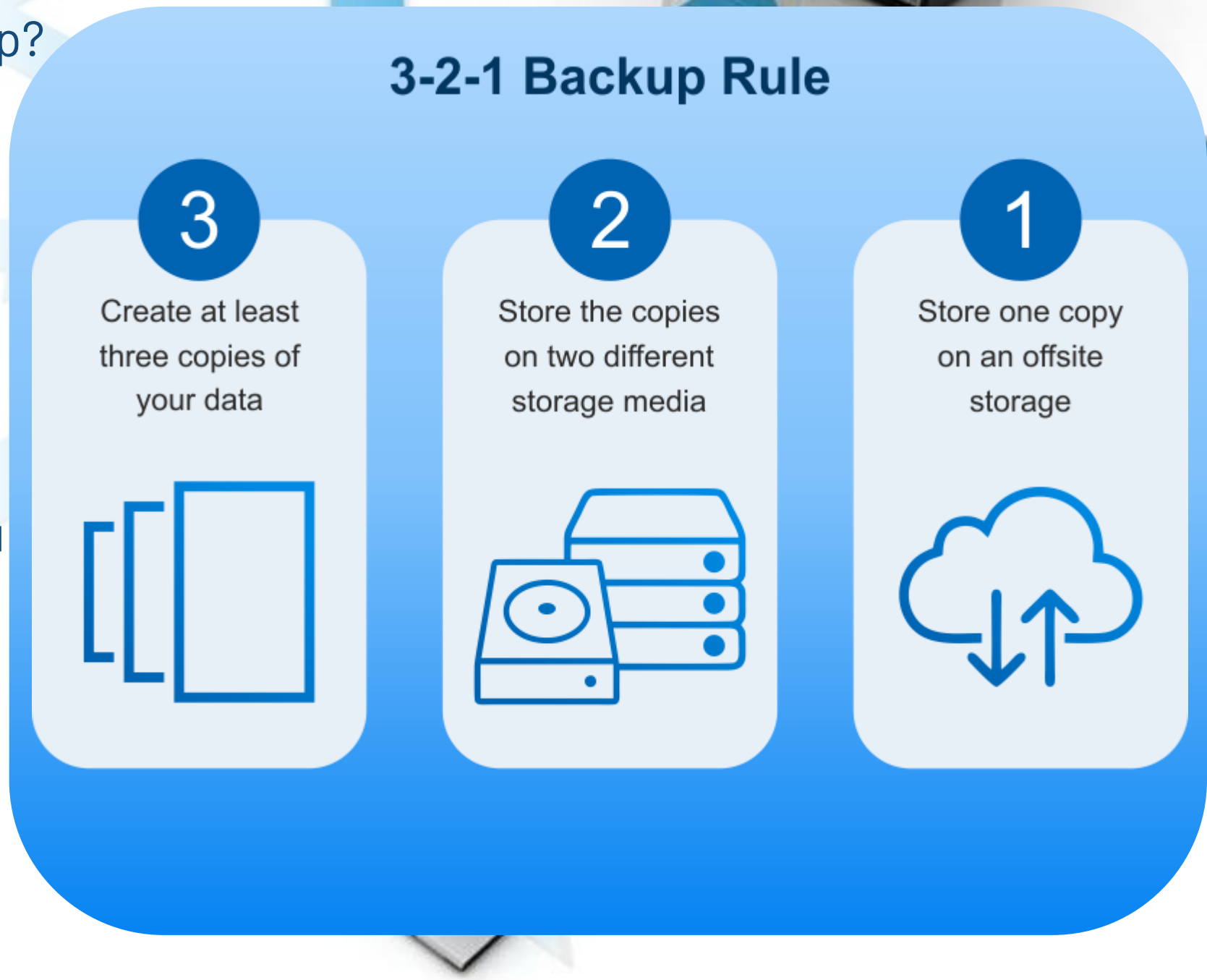
- Provide exposure training
    - Share what is out there
    - Include examples
- Notify users of the systems in place
- Stress importance of notification
    - Create a safe atmosphere
- Include in response team if appropriate
- Provide assessments
- Perform mock drills

Turn on/Preserve Logs

- One of the first things forensics and attorneys will ask for
- Do not let logs roll over/overwrite
- Log review is best way to confirm that constituent data is only encrypted and not exported
- Capture logs at a centralized location with periodic offline copies

Back Up Your Data

- Are your systems backed up?
- Where/How many?
  - Onsite/offsite
  - Third-party
  - Cloud-based
- How often are they backed up?
- When was the last time you checked viability?
- Have you ever restored anything from them?
- Follow 3-2-1 Rule



3-2-1-1-0 Rule

3 copies

2 media types

1 off-site copy

1 offline copy

0 errors

The (un)likelihood of backups

5%

Backups Operational

Majority of the time, the backups (whether onsite / in the cloud / outsourced / internal) are not functional. It is rare to have a functional backup.

95%

No Backups - All Backups Corrupted / Non-Functioning

The common issues include: threat actor is able to utilize the same credentials to access the backup array and is thus able to encrypt the backups as part of its overall strategy.

In other tragic circumstances, the backups fail due to configuration error that is not discovered until after the incident.

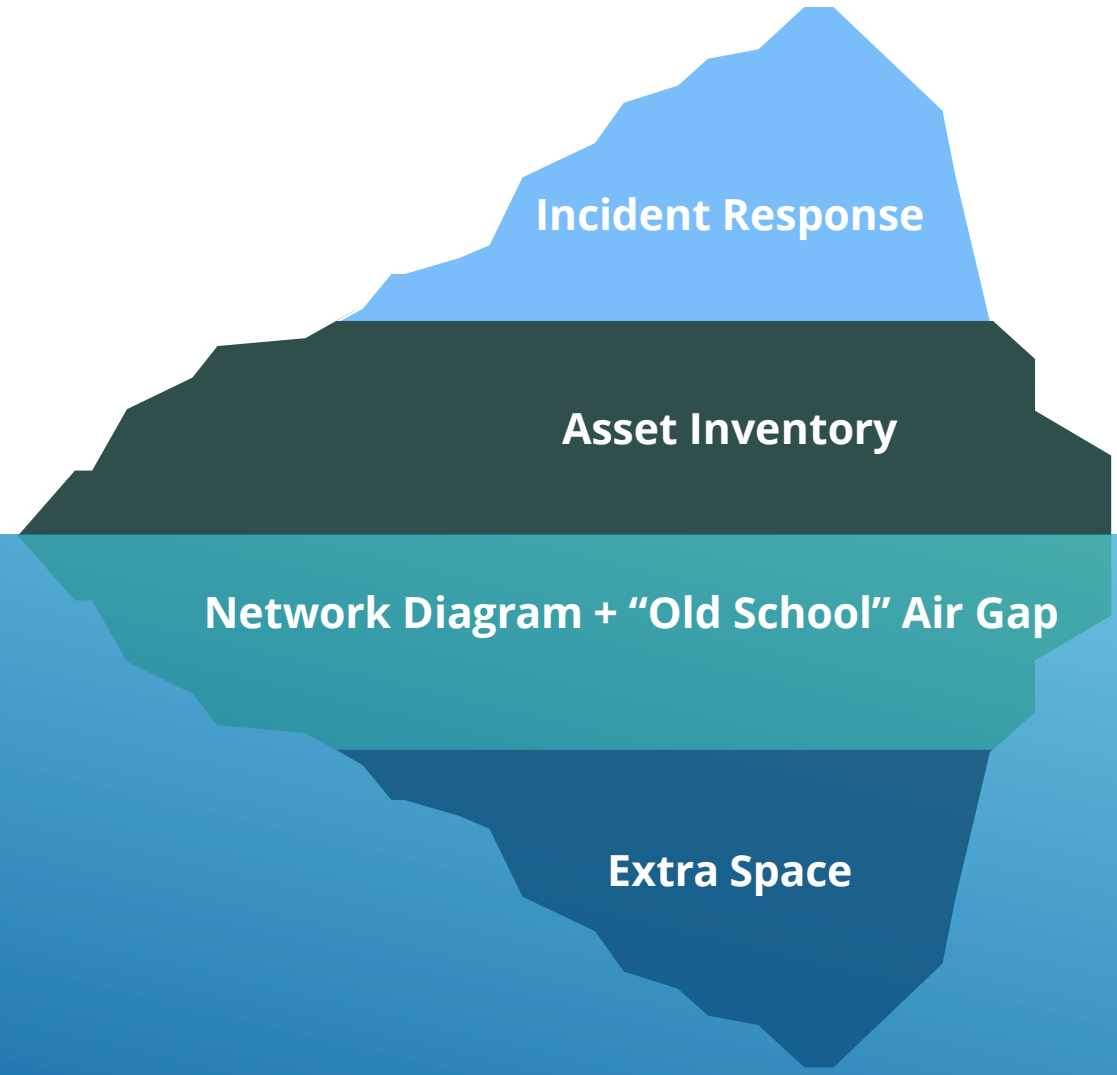
Managing the Rebuild: A Strategy

Current Focus: Above the Water

Focus is often on the surface level issues: having an up-to-date incident response plan.

True Need: Below the Surface

The real effort should be spent here: thinking through what could happen if the backups all fail. Do we have an old school air gapped drive with critical info / applications locked away? Do we have extra slack space to rebuild into if we had to stand up a parallel network?



Other Lessons Learned

- Many school divisions/counties have shared finances through VPN
  - How is your coordination?
  - How will you function when the connection is severed during an incident?
  - Is payroll in the cloud?
    - Can you run it outside the shared network?
- How will you function if you are hit during SOLs?
  - Schools shut down because door locks were affected
    - Would have to be propped open
- Do you have slack space to rebuild without deleting?
  - Do you have an up-to-date asset inventory and network diagram?
- Do you have air-gapped backups?
  - What will you do if the backups fail?

You're in Good Hands

VAcorp

- First to offer cyber coverage
- Most comprehensive cyber coverage available
- Approached by over a dozen state pools for consultation
- Cyber Breach Attorney guidance on each claim
- No deductible
- No sublimits
- No pooled aggregate when purchasing $1 mil limit or greater

Claim Contact Information

VAcorp

Business hours phone number: 888-822-6772

After-hours phone number: 540-265-8021

Email: KJustice@riskprograms.com

JMullen@riskprograms.com

Breach Coach: Beth Waller, Esq.

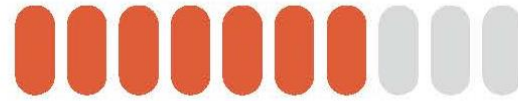
Woods Rogers PLC

BITSIGHT®

The Standard in **SECURITY RATINGS**

4 of the **Top 5**
Investment Banks
use BitSight for
Vendor Risk Management

120+ Government institutions
across 30 countries use BitSight



7 of the **Top 10** Global
Cyber Insurers use BitSight to
make underwriting decisions

20% of Fortune 500
Companies use BitSight

4 of the **big 4**
Accounting Firms
use BitSight

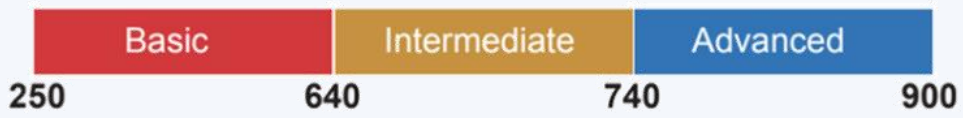
50% of global cyber insurance
premiums are written by BitSight
customers

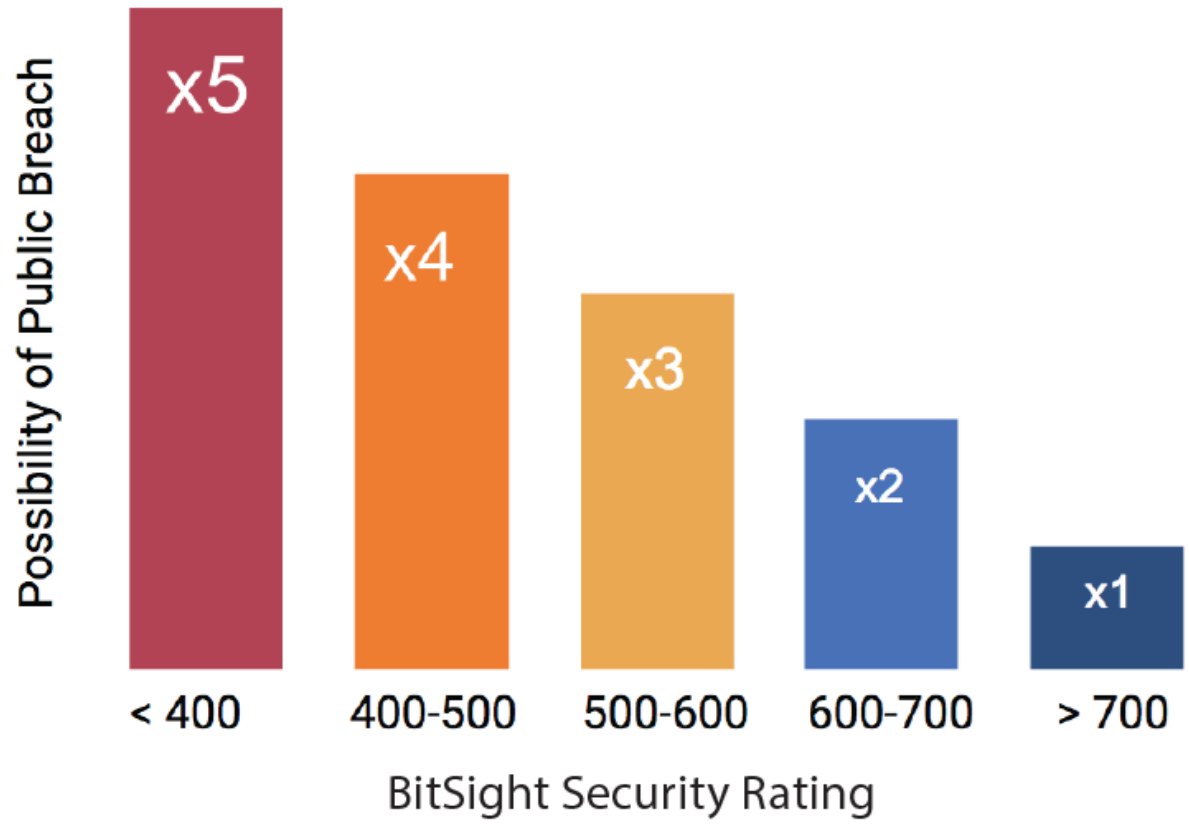
BITSIGHT®

The Standard in **SECURITY RATINGS**

BitSight transforms how companies manage information security risk with objective, verifiable and actionable Security Ratings.

The BitSight Security Ratings Platform applies sophisticated algorithms, producing daily security ratings that range from 250 to 900, to help organizations manage their own security performance; mitigate third-party risk; conduct financial diligence; and assess aggregate risk. With the largest ecosystem of users and information, BitSight is the Standard in Security Ratings.





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

VAcorp Member Portal

per.vacorp.org/VACoRP/VACoRP_Home.aspx

orp

Home | Report a Claim | Resources | Site Tools | About Us

- Media
- Risk Control
- Workers' Compensation
- eRiskHub
- Safety Source Videos

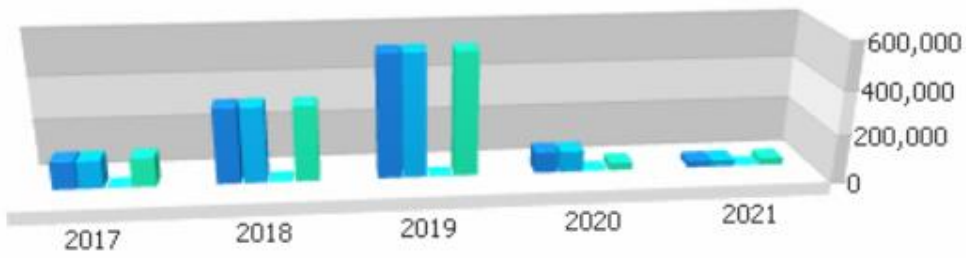
You have 15 open claims.

View Now

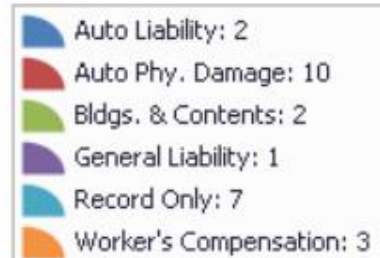
Your last visit was on 2/9/2022 5:00:38 PM.

Logout

Financial Data for past 5 Years



Current FY Claim Type



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

Risk Control

- Secure offsite backups
- Up-to-date security patches
- Restrict ability to spread laterally via network segmentation
- Secure passwords
- Multi-factor authentication
- Encrypt sensitive data
- Disable unneeded functionality to reduce attack surface

Key Takeaways

- Invest in cyber security
- Follow your procedures
- Preserve logs
- Test back-ups
- Train staff
- Notify VAcorp immediately
- Follow Breach Coach guidance

VAcorp

Thank You!

888-822-6772 | www.VAcorp.org