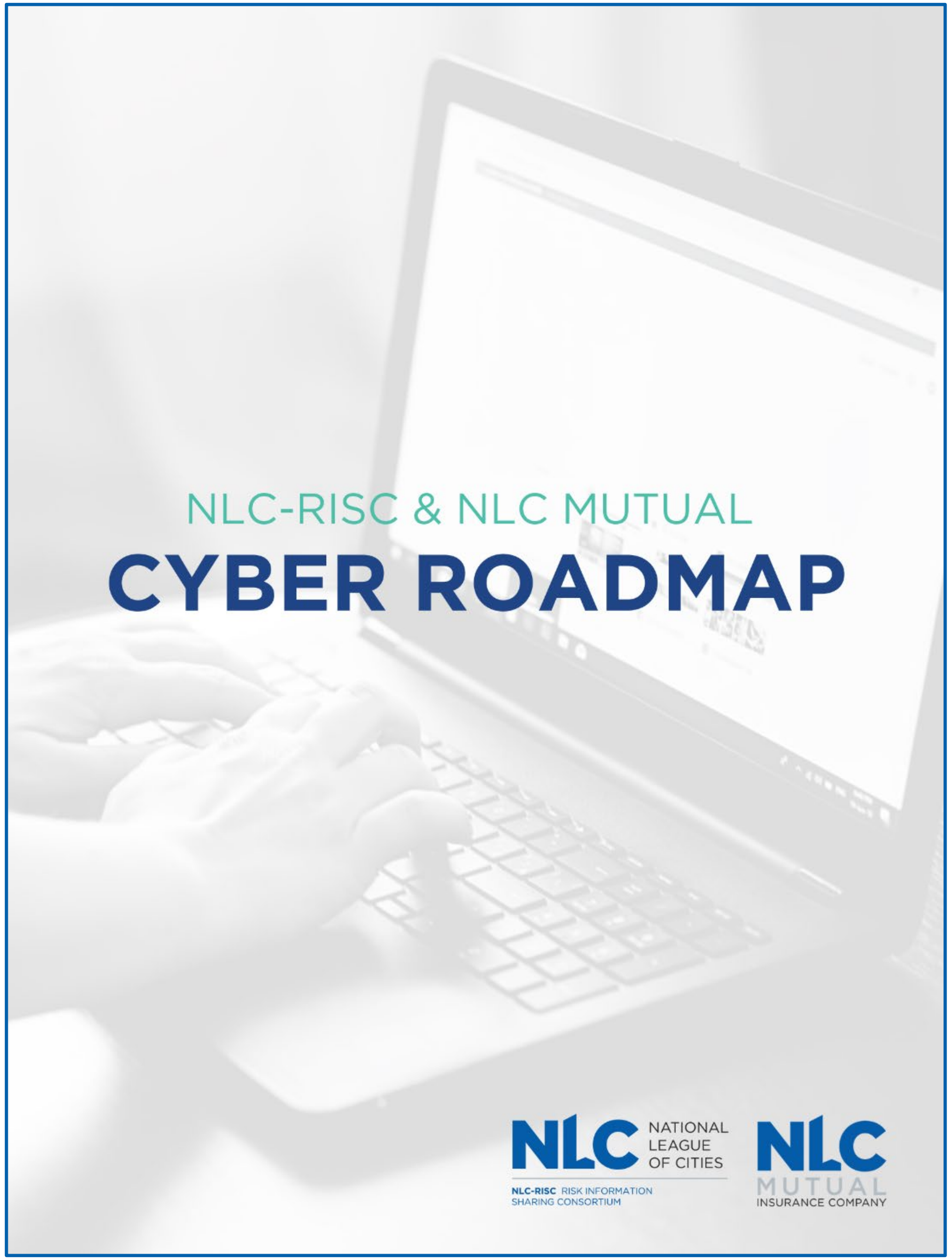
NATIONAL LEAGUE OF CITIES

NLC-RISC RISK INFORMATION SHARING CONSORTIUM

Lessons and Successes from the NLC-RISC and NLC Mutual Cyber Pilot Project

Tuesday, October 22nd| 10:15 AM

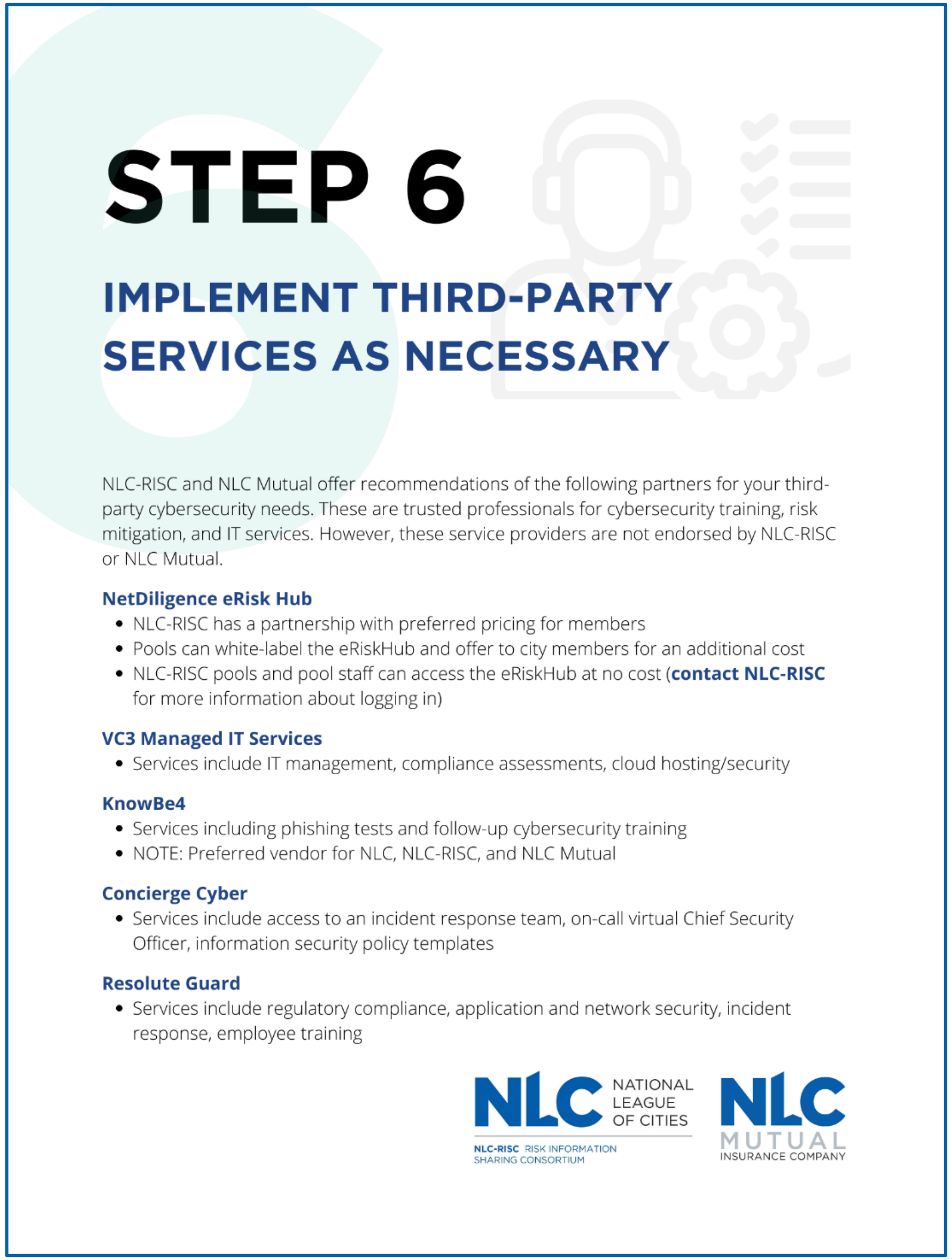


NLC-RISC & NLC MUTUAL

CYBER ROADMAP

NLC NATIONAL LEAGUE OF CITIES
NLC-RISC RISK INFORMATION SHARING CONSORTIUM

NLC MUTUAL INSURANCE COMPANY



STEP 6

IMPLEMENT THIRD-PARTY SERVICES AS NECESSARY

NLC-RISC and NLC Mutual offer recommendations of the following partners for your third-party cybersecurity needs. These are trusted professionals for cybersecurity training, risk mitigation, and IT services. However, these service providers are not endorsed by NLC-RISC or NLC Mutual.

NetDiligence eRisk Hub

- NLC-RISC has a partnership with preferred pricing for members
- Pools can white-label the eRiskHub and offer to city members for an additional cost
- NLC-RISC pools and pool staff can access the eRiskHub at no cost (**contact NLC-RISC** for more information about logging in)

VC3 Managed IT Services

- Services include IT management, compliance assessments, cloud hosting/security

KnowBe4

- Services including phishing tests and follow-up cybersecurity training
- NOTE: Preferred vendor for NLC, NLC-RISC, and NLC Mutual

Concierge Cyber

- Services include access to an incident response team, on-call virtual Chief Security Officer, information security policy templates

Resolute Guard

- Services include regulatory compliance, application and network security, incident response, employee training

NLC NATIONAL LEAGUE OF CITIES
NLC-RISC RISK INFORMATION SHARING CONSORTIUM

NLC MUTUAL INSURANCE COMPANY

Selection of risk pool

- RISC and Mutual sent applications to our member pools in the fall of 2022 with a pre-determined set of selection criteria.

- From our pool of 7 applicants, we selected the Association of Washington Cities.

Master Agreement process

- Next, we worked with our collective legal teams to form a Master Agreement to govern the pilot

- We also crafted an agreement for all work orders to be approved, which includes the participating cities as a signor

Pilot Goals

- Improve pool members' **overall cyber security** and cyber hygiene via best practices that are efficient, sustainable, and solution-based
- **Easily replicated** across a member state and in other pools
- Cyber coverage in place and **improvement of cyber coverage pricing, terms, etc**. over time among participating municipalities

Current Status

- Wrapping up our pilot with AWC and VC3 is **finalizing all member implementations**
- Expect to have a **report on pilot findings** in Q1 of 2024
- **Determining feasibility of replicating** the pilot with another member pool in 2024

RMSA

Risk Management SERVICE AGENCY

AWC RISK MANAGEMENT SERVICE AGENCY

SECURITY | STABILITY | SERVICE

AWC RMSA & Cybersecurity

RMSA offers cyber coverage to our members. In partnering on the Cyber Roadmap Pilot, RMSA's goals include:

- Reducing the risk of cyber claims by offering further cyber protection in an increasingly unsafe digital environment.
- Educating members on cybersecurity Member Standards with an initial pilot focus on small members who may have no in-house or contracted IT staff.
- Fulfilling our mission to proactively provide coverages and resources for our members.
- Showcasing a more appealing pool to cyber reinsurers with these cybersecurity protections in place.

Criteria when choosing members

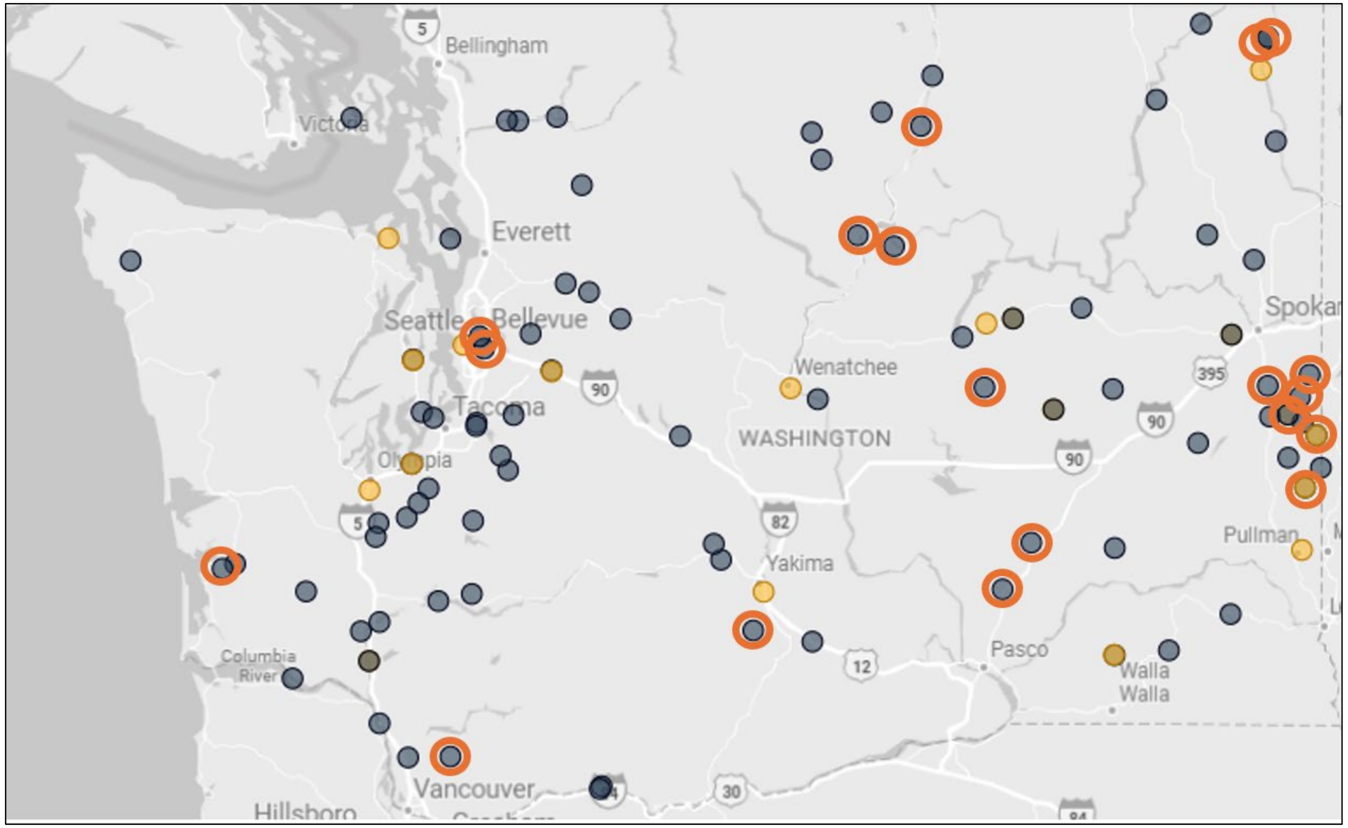
The majority of RMSA's members and 57% of Washington's cities and towns have a population less than 5,000

- Battling the common misconception that cyber-attacks don't happen to small towns.
- Directly correlates to constraints on budget, staffing, and availability to prioritize cybersecurity.

Members from East, West, and Central regions

- Washington's regions vary in cyber and internet sophistication.
- Members with less cybersecurity access need the protection and can provide valuable feedback.

RMSA members, Pilot members encircled



SECURITY | STABILITY | SERVICE

AWC RISK MANAGEMENT SERVICE AGENCY

Recruiting successes

41 RMSA members have been contacted to participate

- 19 members have opted in to the pilot.
- 18 have declined to participate.
- 2 agreed but after discovery decided to withdraw.
- 2 have been removed from candidate list due to staffing changes and availability.

Recruiting successes

- Comprehensive talking points, email template, and FAQs for members.
- Proactive contact with Clerks monthly, in line with Council meetings.
- Working with members that have Councilmembers and Administrators on our Board of Directors and Operating Committee.

Recruiting challenges

Members with existing IT/cyber services

- Desire to maintain member/IT vendor relationship.
- Working with State & Local Cybersecurity Grant Program to implement cyber services.

Members simply busy at the time we reached out

- Recruiting was done partly during '23 budget season.
- Staff already stretched thin.

Staffing challenges

- Staff may only work a few days a week/part time.
- Staff changeover, loss of existing knowledge, focusing on hiring.

Observations

Meet members where they are

- Working along their timelines.
- Connect with them at their cybersecurity knowledge level.

No two members are the same

- Distinctive size, staff, budget, elected officials, and motivations.
- Varying levels of IT and cybersecurity services already in place.
  - Vendor contracts, volunteers, contact from the WA State Broadband Act.
- Member participation and the State & Local Cybersecurity Grant Program (SLCGP)
  - Member with outdated devices, running on Windows 7 which no longer has security updates, patches, or service.
  - Met with member to discuss the SLCGP and assist in grant application process.

Observations

Post deployment and timelines

- Onboarding process longer than anticipated
    - Multiple communication attempts
    - Deployment in waves by geographical region
- Remote tools deployment
    - MFA and Security Awareness Training after onsite visit
    - Coordinating with Clerk, staff, elected officials
    - VC3 and RMSA outreach needed
    - Obtaining access to email tenant from various sources (Service providers, contractors, staff, etc.)
- Surveys
    - Short by design
    - Info and graphics needed
    - Multiple follow-ups

Member	Participation Confirmed	Agreement Executed	Onboarding Kickoff	Onsite Deployment
Hunts Point	9/25/23	10/30/23	11/8/23	11/15/23
Beaux Arts Village	9/25/23	10/30/23	11/8/23	11/15/23
South Bend	9/13/23	10/30/23	11/28/23	11/30/23
Garfield	1/3/24	1/22/24	1/31/24	2/6/24
Spangle	9/14/23	10/30/23	1/25/24	2/6/24
Rockford	9/13/23	10/30/23	1/8/24	2/7/24
Tekoa	10/3/23	10/30/23	1/3/24	2/7/24
Waverly	11/16/23	12/5/23	1/16/24	2/7/24
Metaline	9/13/23	11/8/23	1/18/24	2/8/24
Metaline Falls	11/27/23	1/2/24	1/18/24	2/8/24
Bridgeport	10/3/23	12/6/23	1/24/24	4/17/24
Pateros	9/25/23	11/17/23	3/14/24	4/17/24
Riverside	11/16/23	1/10/24	3/27/24	4/17/24
Fairfield	1/17/24	3/6/24	3/21/24	4/18/24
Mesa	4/15/24	5/1/24	5/1/24	5/23/24
Wilson Creek	1/17/24	4/25/24	5/21/24	7/9/24
Yacolt	5/14/24	6/24/24	7/3/24	7/24/24
Hatton	11/13/23	11/20/23	7/30/24	9/5/24
Harrah	5/29/24	8/28/24	9/5/24	9/17/24

Outcomes

Cybersecurity outreach and awareness

- Cybersecurity services for members.
- General cybersecurity awareness and developing a culture of cybersecurity along with our culture of risk management.

RMSA program improvements

- Currently, no cyber-related claims filed for any pilot member since their deployment.
    - Better rates reflected for members with a reduction in cyber claims.
- Cyber reinsurance premium reduction.
- A more well-rounded comprehensive and competitive risk pool.

Member feedback

What we're looking for:

1. No cyber-related claims or a decrease
2. Satisfaction in services
3. Interest in continuing services after pilot
4. Interest in cybersecurity services as part of RMSA membership offerings
5. Higher level of cyber knowledge; IT service considerations

Feedback from 6-Month surveys:

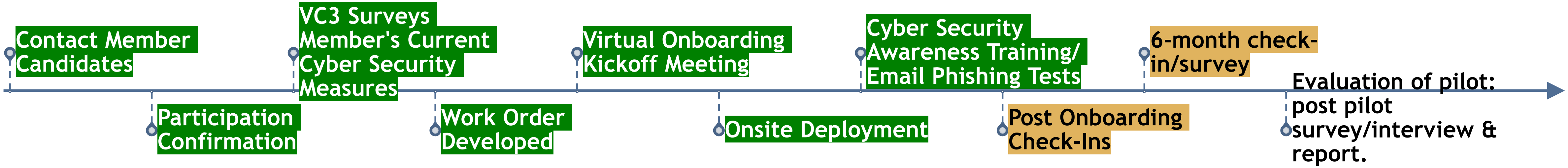
1. No cyber claims or near misses. Cyber services work, members feel more secure
2. Members satisfied with services, minor issues with DUO MFA
3. Most are unsure in continuing services, cost is a major factor
4. A little less unsure if services were incorporated into RMSA membership
5. Most members lack in-house IT staff, moderate interest in hiring IT staff/services

RMSA Next Steps

Check-ins with members, other half of 6-month survey feedback, post pilot surveys/interviews.

Success rates of Security Awareness Training, Phishing Email Campaigns, reduction in cyber claims and near misses.

Evaluating pilot: Feedback from members and reporting from VC3 to help determine future cybersecurity services provided by RMSA.



Contact Member Candidates

Participation Confirmation

VC3 Surveys Member's Current Cyber Security Measures

Work Order Developed

Virtual Onboarding Kickoff Meeting

Onsite Deployment

Cyber Security Awareness Training/ Email Phishing Tests

Post Onboarding Check-Ins

6-month check-in/survey

Evaluation of pilot: post pilot survey/interview & report.

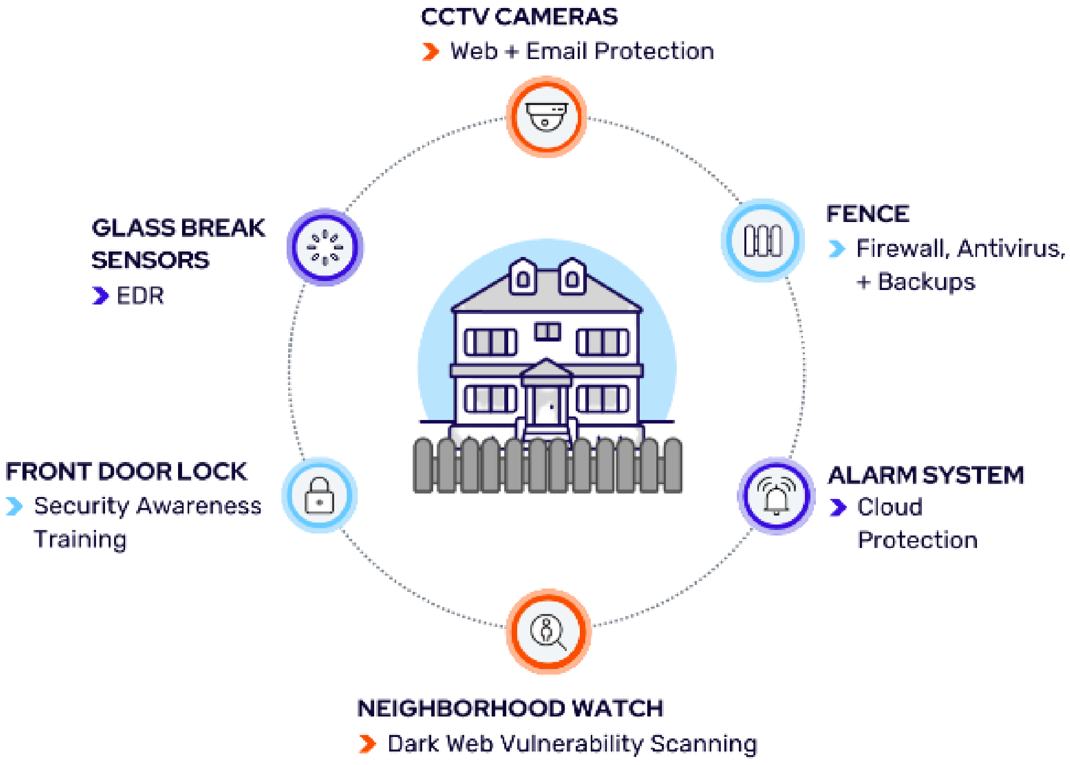
NLC-RISC Staff Conference

- CHECK-IN ON NLC-RISC/MUTUAL AND AWC-RMSA PILOT UNDERWAY TO DEPLOY CYBERSECURITY PROTECTIONS TO RISK POOL MEMBERS

Our cyber pilot was designed to lower municipal risk

LIKE SECURING A HOME, THESE 6 SOLUTIONS KEEP A COMMUNITY'S NETWORK AND DATA SAFE

- **Email Multi-Factor Authentication (MFA)**
  - Configure Microsoft Office 365 MFA for user access to email.
- **Local MFA**
  - Deploy MFA for admin access and remote access to devices (workstations and laptops), servers, and network. Protect user account access for line of business applications and systems.
- **Data Backup and Disaster Recovery**
  - Data Backup of servers, otherwise critical devices, including up to 250GB of cloud storage per computer.
- **Endpoint Detection and Response (EDR)**
  - Advanced threat hunting for endpoints (devices and servers). Includes monitoring agents, 24x7x365 Security Operations Center, and Remote Monitoring and Management (RMM) for endpoint patch management and monitoring, alerting, and support (if needed). Detect suspicious behavior and potential cyberattacks on endpoint devices like servers, desktops, and laptops, before cyber attackers can strike.
- **Email Advanced Threat Protection (ATP)**
  - Configure Microsoft Office 365 Advanced Threat Protection for cloud-based email filtering. Encrypt your email, scan it for malware, and stop most phishing and spam attempts from ever reaching your employees.
- **Security Awareness Training (SAT)**
  - Monthly Phishing Emails, Training, and Reporting. Help keep employees sharp, skilled, and smart to counter cyberattackers.



The low cost per user will allow for ~25 members to participate

19 MEMBERS HAVE SIGNED UP, REPRESENTING 69% OF THE BUDGET

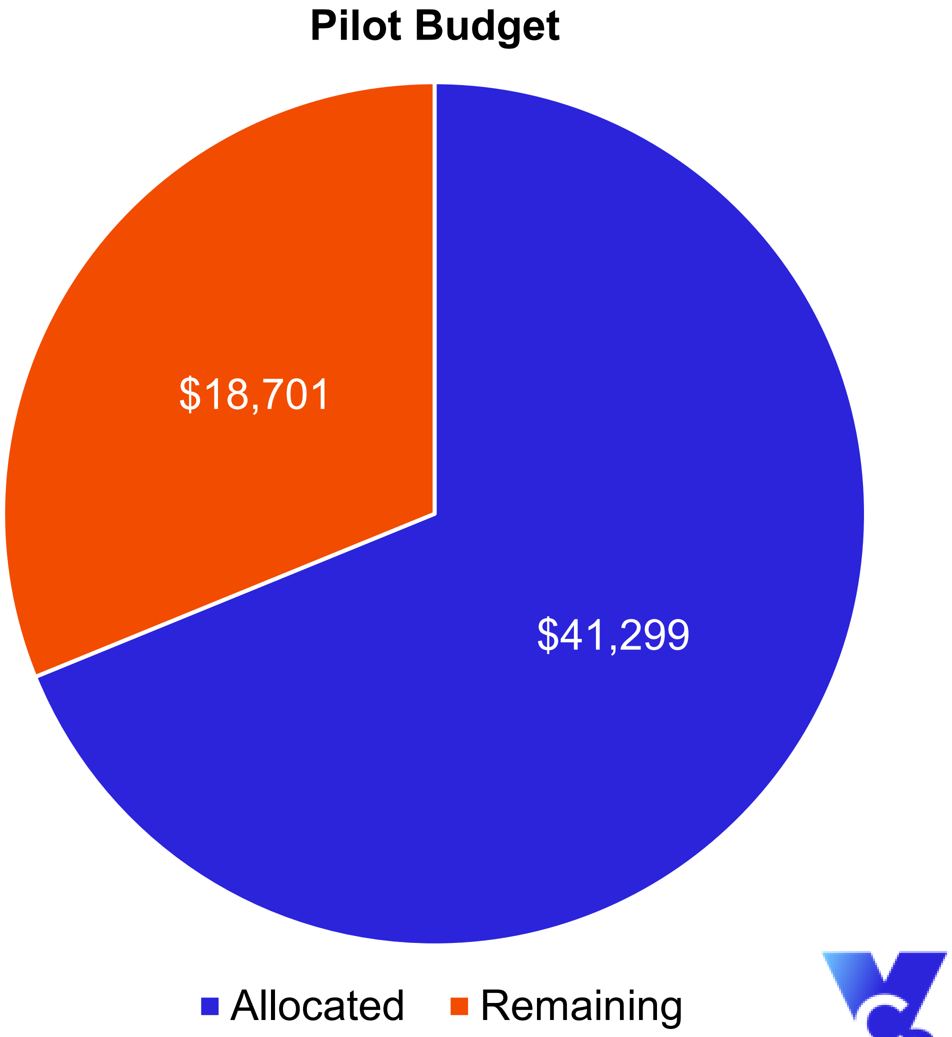
Low-cost, inexpensive solutions, scalable to address cyber risks

Cost/mo	Solution	Comment
$121.40/server	Data Backup	Servers
$56.99/device	Data Backup	Critical devices/PCs
$8.80/device	EDR	Includes patch management
$4.25/user	Local MFA	Admin access and Remote Access
$1.50/user	SAT	
$0.00/user	Email ATP	Included w/ O365 subscription
$0.00/user	Email MFA	Included w/ O365 subscription

This approach has allowed us to stay within budget

$60K pilot budget

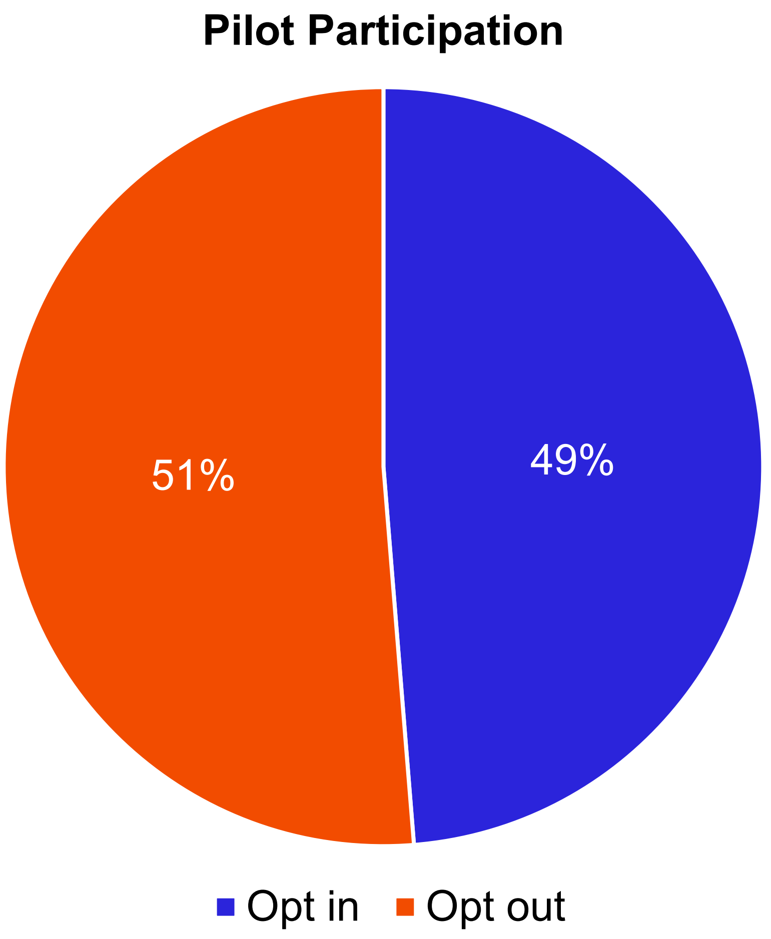
$41K (69%) allocated to-date for 19 participants



Removing/lowering the cost barrier has increased coverage

49% OF THE INVITED MEMBERS SIGNED UP WITH COST NO LONGER A FACTOR

- 39 members invited to the pilot with 19 participating
- The pilot removed cost as a reason for non-coverage
- Other opt out reasons continue to include:
  - Internal IT/cyber services
  - Too busy
  - Staff turnover



We have made the onboarding process simple

AVERAGE 6-7 WEEKS TO COMPLETE ONBOARDING

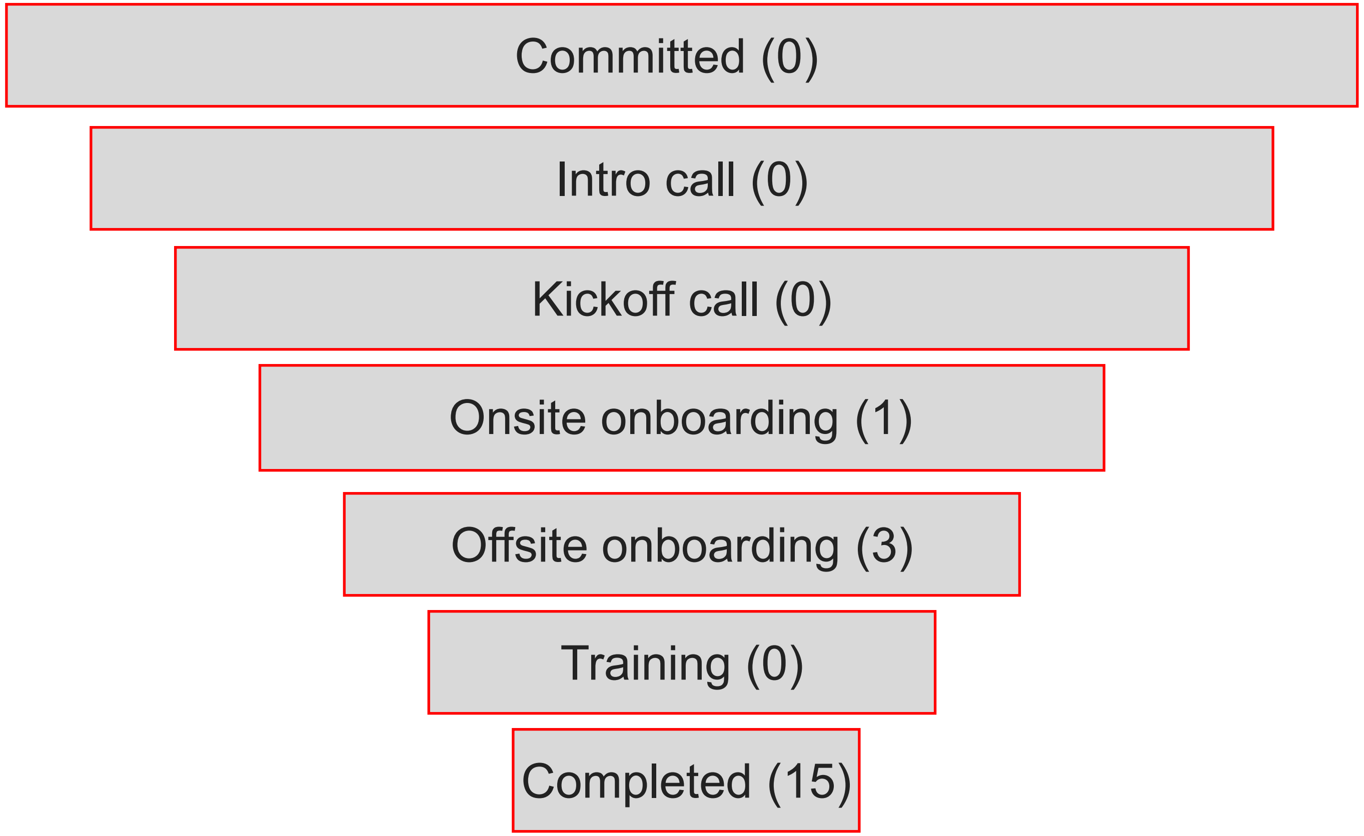
Process

- Intro call (10 minutes)
- Kickoff call (30 minutes)
- Onsite onboarding (2-4 hours)
- Offsite onboarding (4-8 hours)
- Training
- Completed

Time to complete onboarding is 6-7 weeks

- Coordinating with city (part-time, meetings, work schedule, holidays)
- Grouping multiple cities geographically for scheduling onsite onboarding (multiple onboardings in a week)

Onboarding funnel



Committed (0)

Intro call (0)

Kickoff call (0)

Onsite onboarding (1)

Offsite onboarding (3)

Training (0)

Completed (15)

Quick to onboard once coordinated and scheduled.

*3 participants paused: Windows 7 devices, POC turnover, responsiveness, ...

What coverage existed before we started?

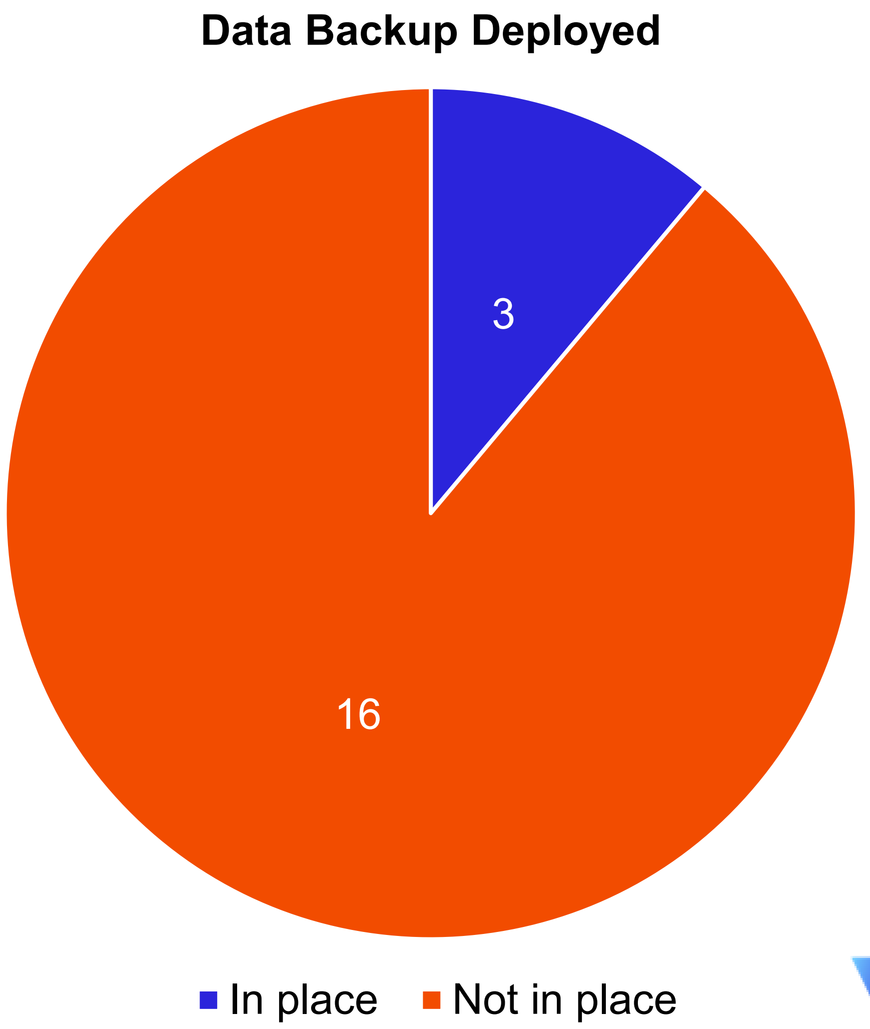
PRE-ONBOARDING STATUS

Only 3 members had data backup and disaster recovery

Data Backup of servers, otherwise critical devices, including up to 250GB of cloud storage per computer

- 84% (16 of 19) of participants did not have adequate data backup in place

21% of companies that were breached, paid the ransom yet still didn't get their data back from the cyber criminals



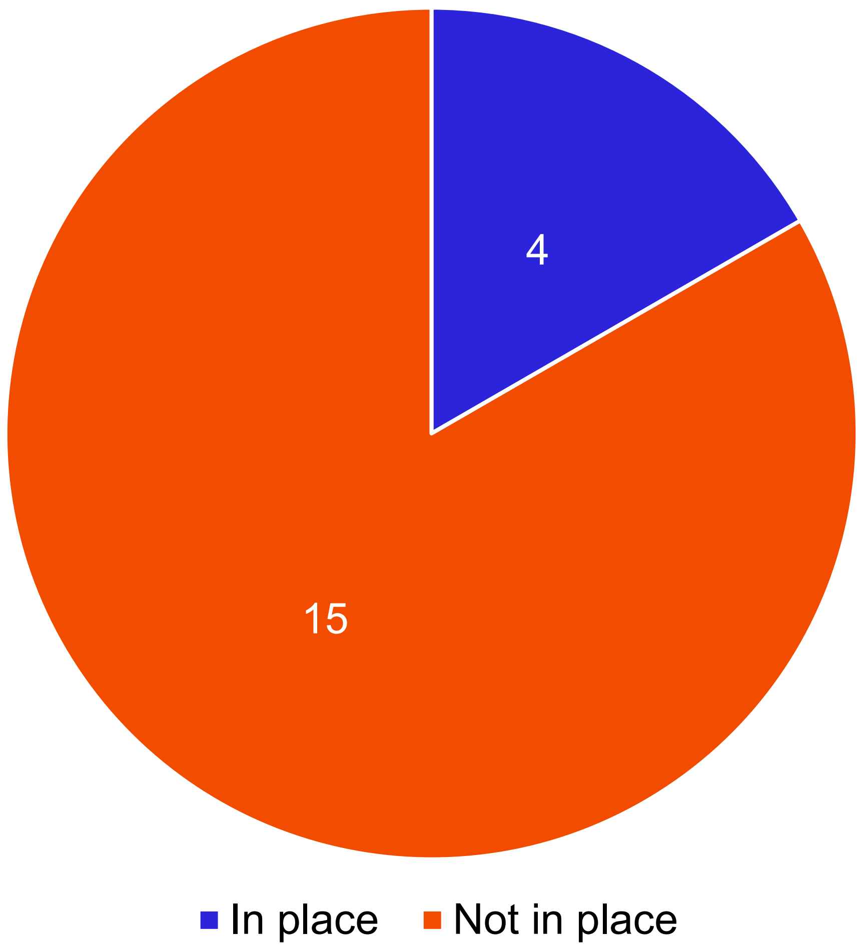
Only 4 members had endpoint detection and response (EDR)

Detect suspicious behavior and potential cyberattacks inside your systems on endpoint devices like servers, desktops, and laptops, before cyber attackers can strike

- 79% (15 of 19) of participants did not have EDR in place

The average dwell time is over 200 days

Endpoint Detection & Response Deployed

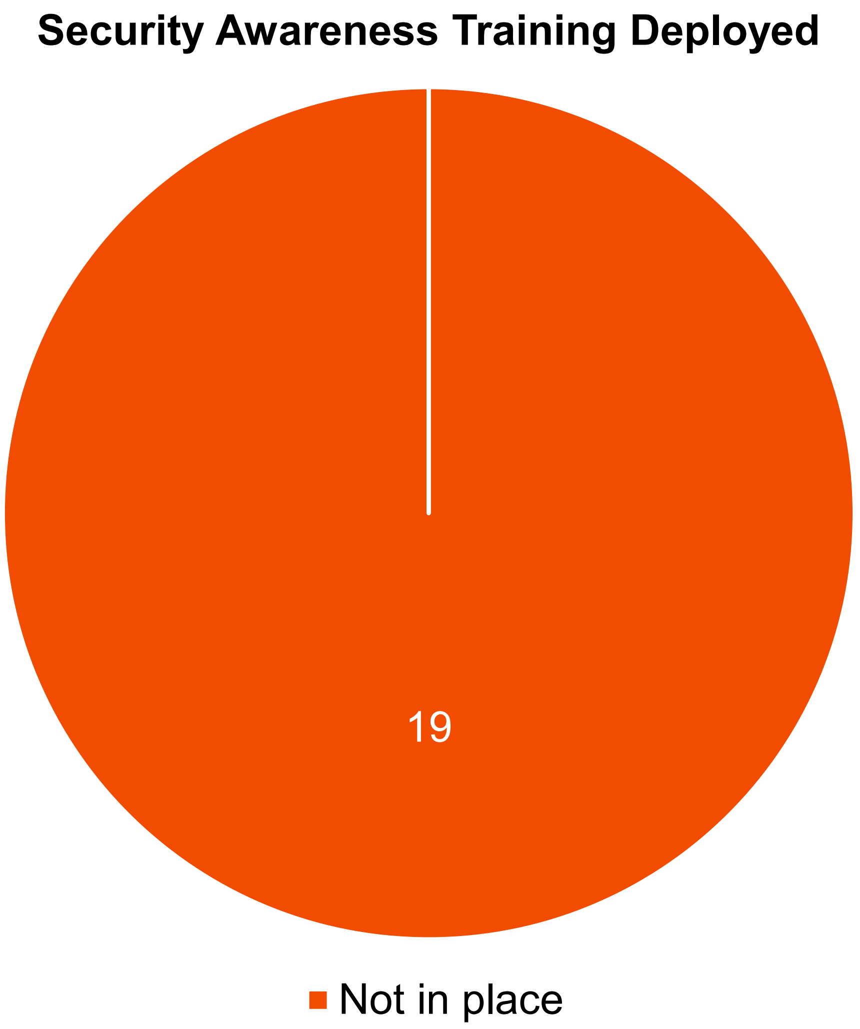


There was no security awareness training (SAT)

Monthly Phishing Emails, Training, and Reporting

- 100% of participants did not have SAT in place

Quarterly SAT reduces the chance of a phishing compromise by 53%

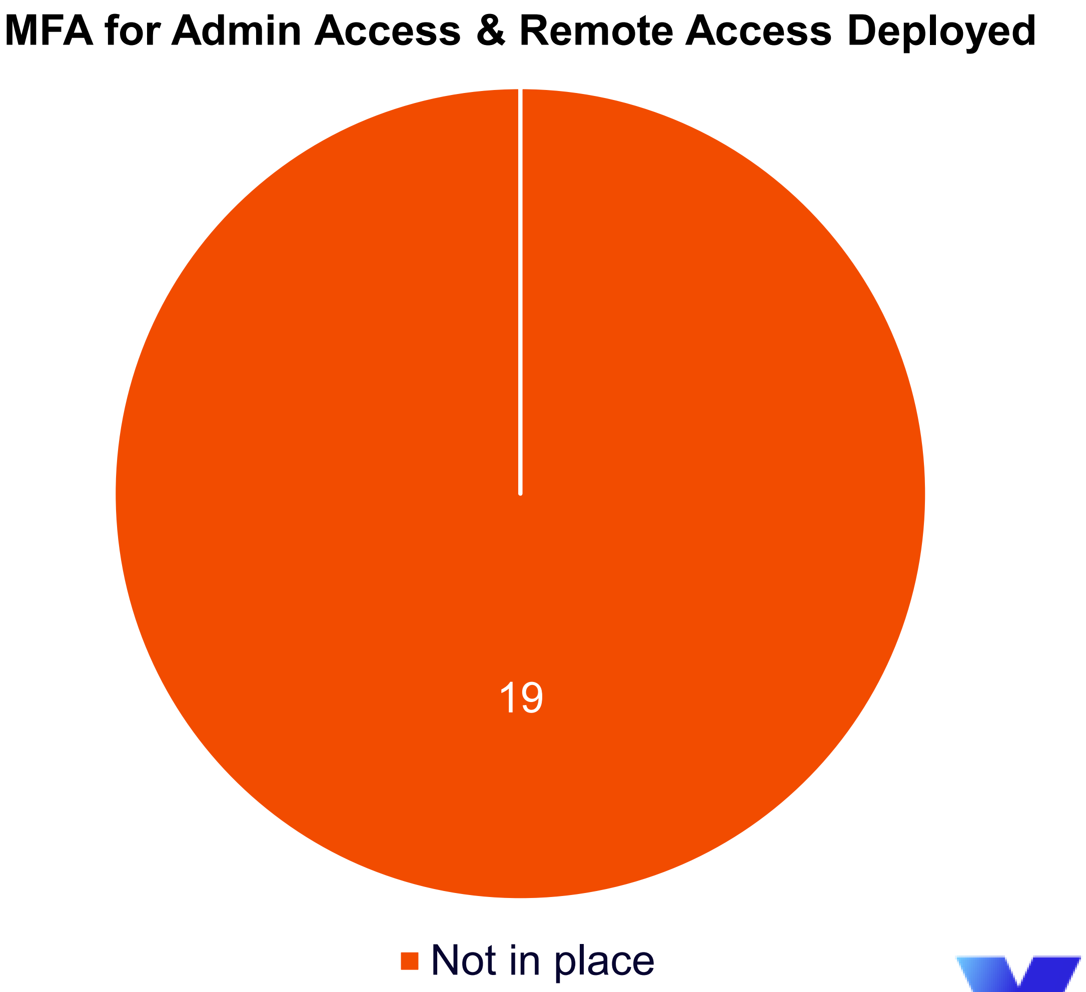


MFA for admin access and remote access was non-existent

MFA for admin access and remote access to devices (workstations and laptops), servers, and network

- 100% of participants did not have MFA in place for admin access and remote access

Microsoft reported that 99.9% of account compromise attacks can be blocked by MFA

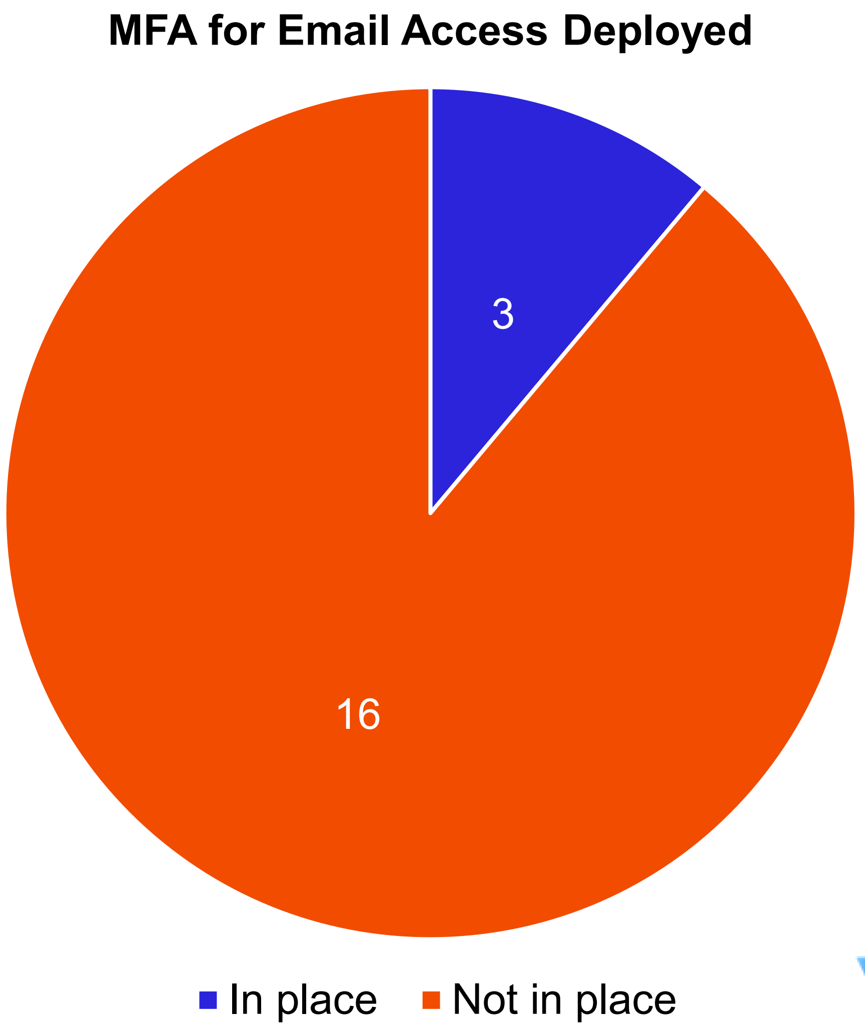


Only 3 members had MFA for email

Microsoft Office 365 MFA for user access to email

- 84% (16 of 19) of participants did not have MFA in place for email access

90% of successful cyberattacks start in email



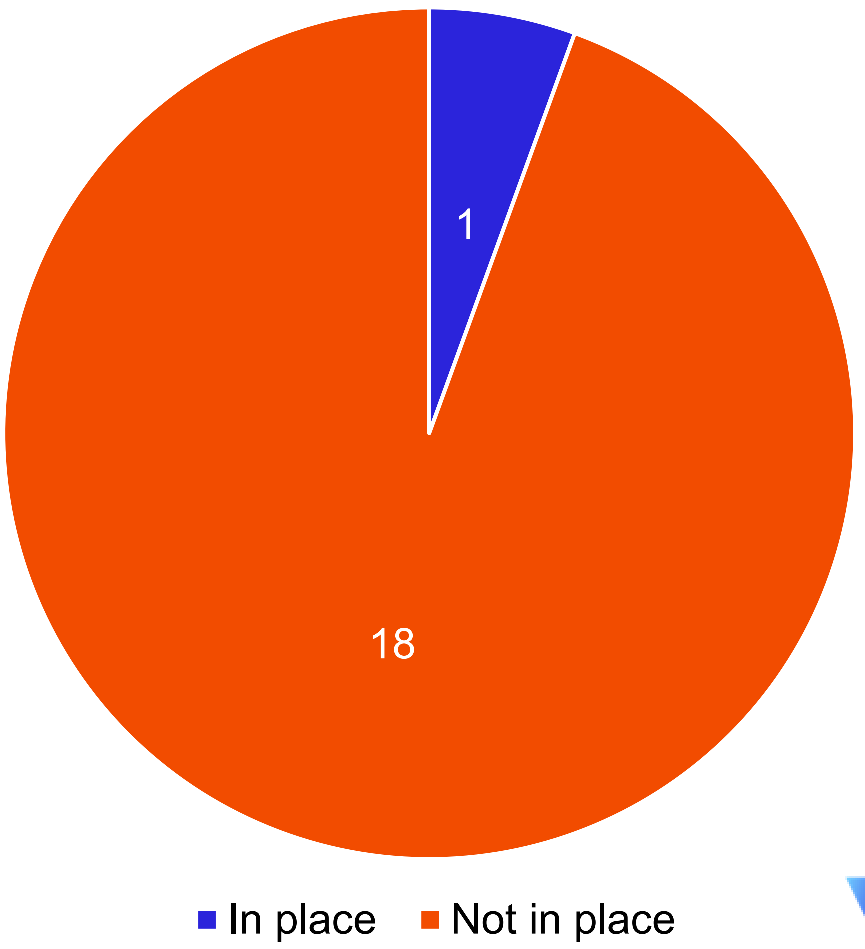
Only 1 member had advanced threat protection (ATP)

Encrypt your email, scan it for malware, and stop most phishing and spam attempts from ever reaching your employees

- 95% (18 of 19) of participants did not have ATP in place

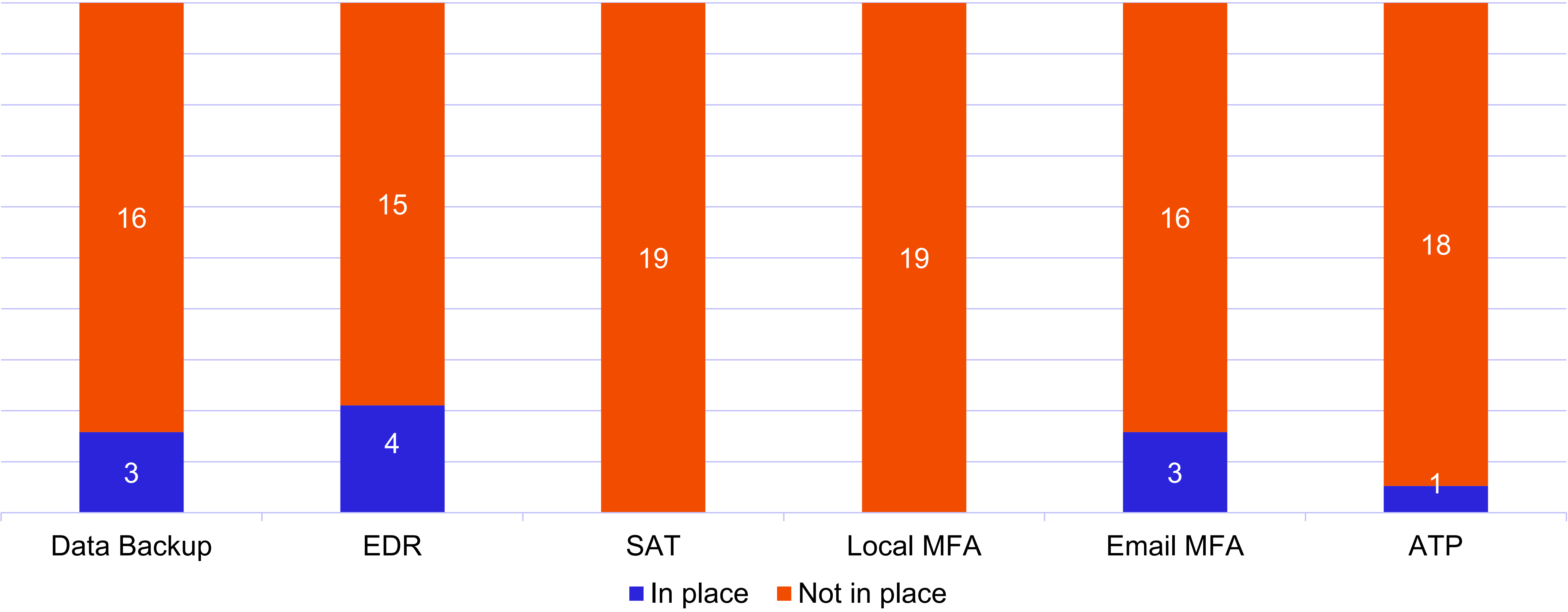
90% of successful cyberattacks start in email

Email Advanced Threat Protection Deployed



All toll – the members were at high risk!

LIMITED SOLUTIONS WERE IN PLACE BEFORE ONBOARDING



What have we learned so far?

CURRENT STATUS

The pilot closes gaps for members with supported environments

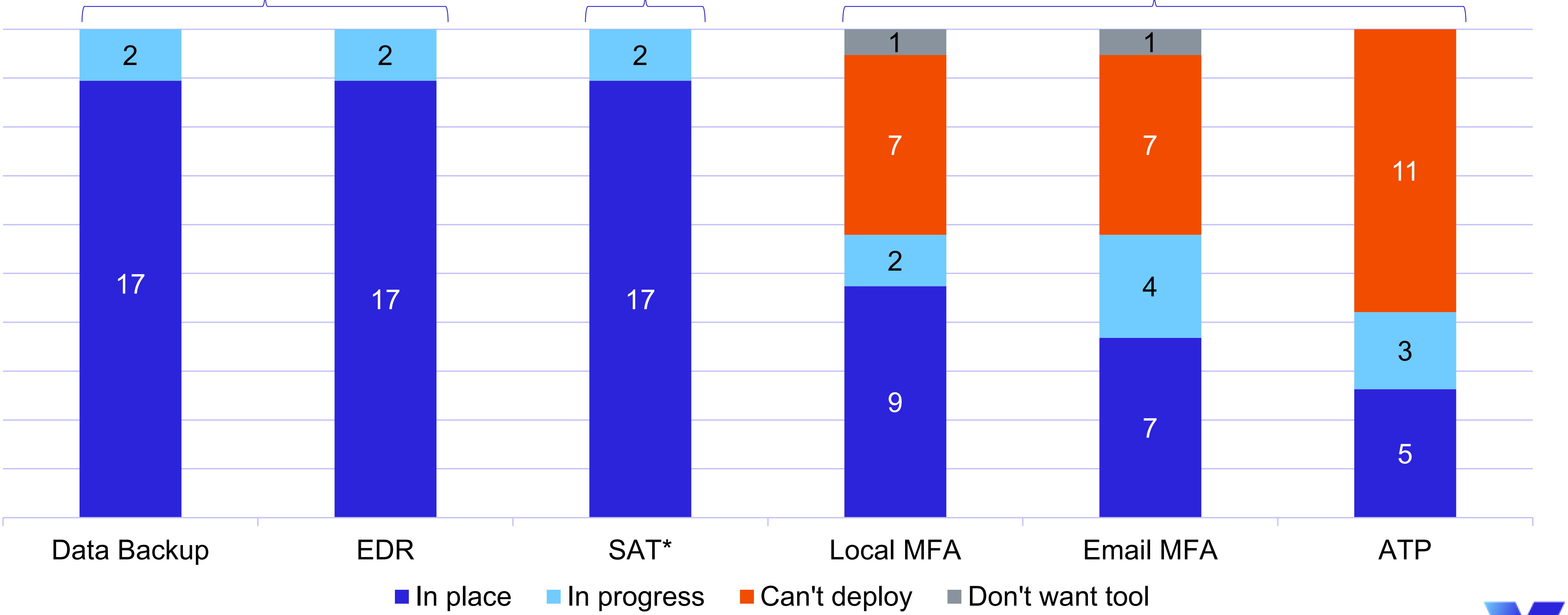
AND AS EXPECTED, NOT ALL MEMBERS WILL HAVE SUPPORTED ENVIRONMENTS…

2 OBSTACLES THAT MUST BE ADDRESSED BEFORE A MEMBER CAN REACH FULL DEPLOYMENT

- **Dated operating systems and hardware**
  - The use of dated, unsupported, operating systems and hardware, like Windows 7, limits what cybersecurity tools can be deployed
  - RECOMMEND: Apply for the State and Local Cybersecurity Grant Program (SLCGP)
- **Personal emails and No domains**
  - The use of personal emails or not having a domain limits the cybersecurity tools and the level of support that can be put in place for
    - Security Awareness Training (SAT)
    - MFA for admin access and remote access
    - MFA for email
    - Email Advanced Threat Protection (ATP)
  - RECOMMEND: Procure Microsoft Office 365 Emails and .GOV domains

Pilot has lowered the risk of the participating members

DATED OPERATING SYSTEMS AND HARDWARE, PERSONAL EMAILS, AND LACK OF DOMAINS ARE OBSTACLES TO GETTING ALL SOLUTIONS IN PLACE



Dated operating systems and hardware limited deployment at all sites

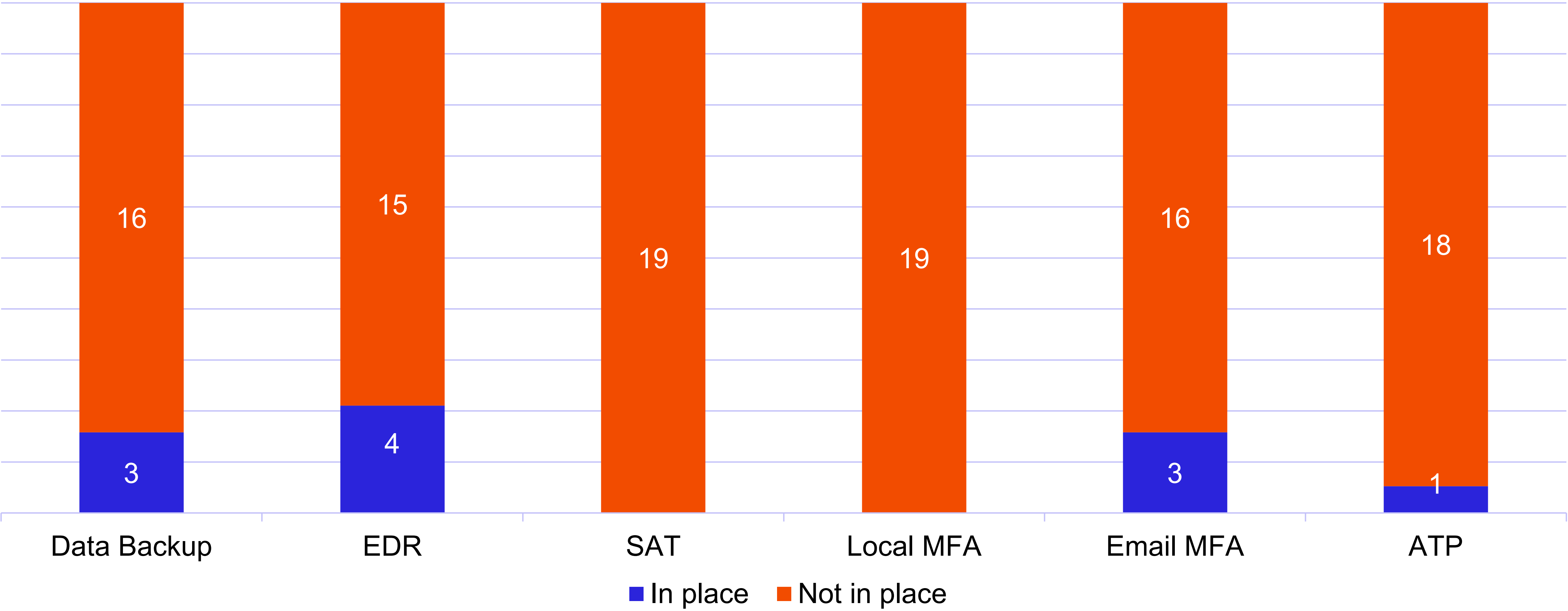
Personal emails and/or no domain led to partial deployment

Personal emails and/or no domain limited deployment at all sites

*Because of personal emails and/or no domains, some of the “In place” deployments for SAT will only have security awareness *training* but no phishing campaigns.

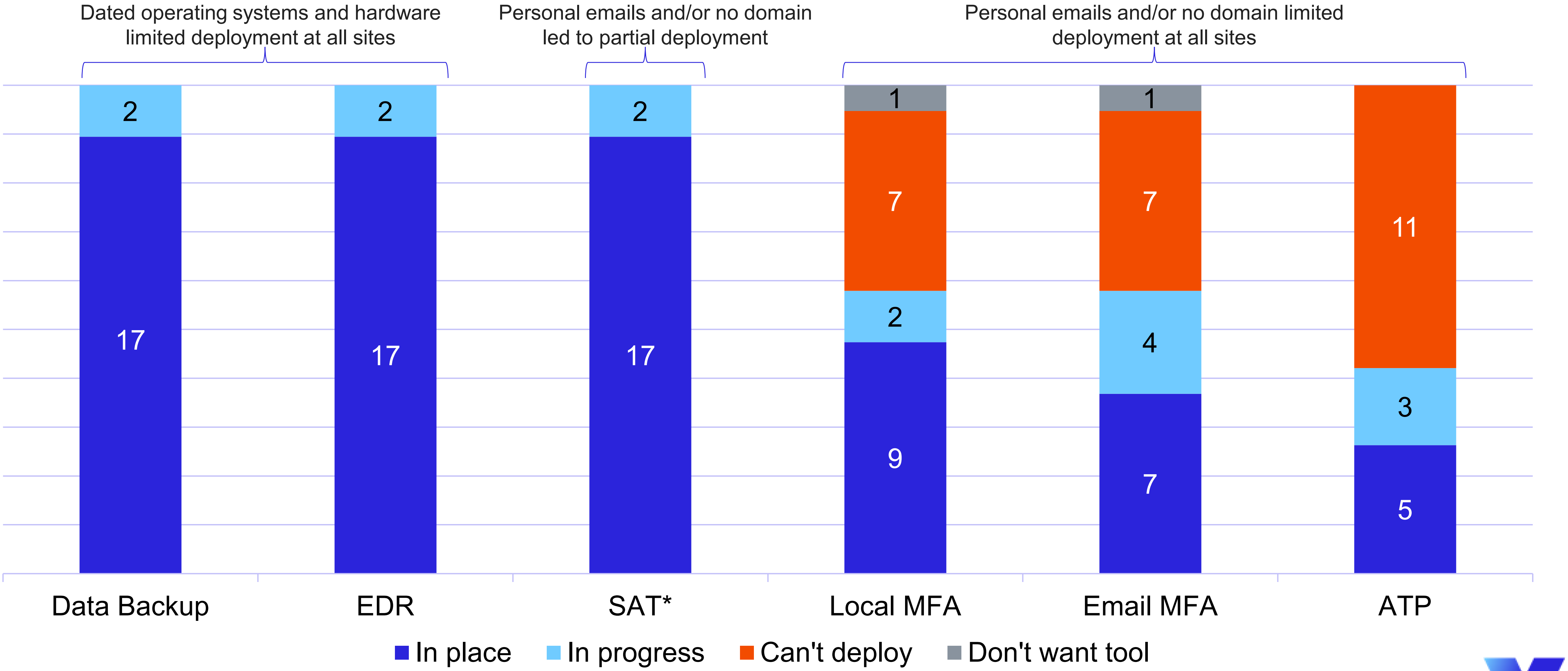
Remember, this is where we started!

LIMITED SOLUTIONS WERE IN PLACE BEFORE ONBOARDING



Pilot has lowered the risk of the participating members

DATED OPERATING SYSTEMS AND HARDWARE, PERSONAL EMAILS, AND LACK OF DOMAINS ARE OBSTACLES TO GETTING ALL SOLUTIONS IN PLACE

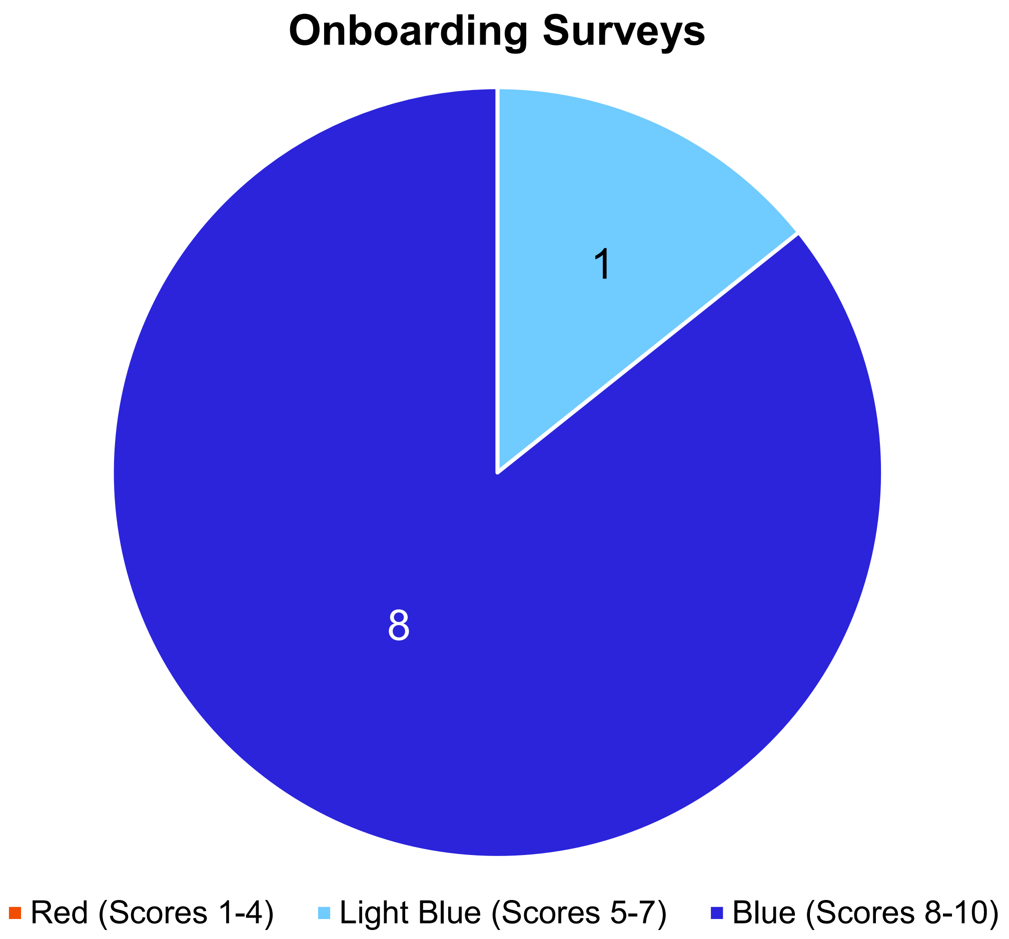


*Because of personal emails and/or no domains, some of the "In place" deployments for SAT will only have security awareness *training* but no phishing campaigns.

And there was support for the approach taken to the pilot

PARTICIPANTS THAT MAY HAVE HISTORICALLY REJECTED CYBER EFFORTS HAVE APPRECIATED THE PILOT

- Survey questions:
  - How would you rate your onboarding experience?
  - Would you recommend VC3 to other members?
  - Was your understanding of services aligned with what was delivered by VC3?
- Key points:
  - 9 surveys completed
  - 5 scores of a 10
  - 2 scores of a 9
  - 1 score of an 8
  - 1 score of a 7



Where do we go from here?

GOING FORWARD

How can you help members lower their cybersecurity risk?

KEY TAKEAWAYS FOR RISK POOLS AND MEMBERS

- Ensure all 6 cybersecurity solutions, that most underwriters will require, can be deployed at every participating member
  - Replace dated operating systems and hardware
  - Replace personal emails with Microsoft Office 365 emails
  - Procure a .GOV domain
- Encourage participation with these low-cost, quick to onboard, cybersecurity solutions
  - Leverage the State and Local Cybersecurity Grant Program (SLCGP)
  - Remind members that having these cybersecurity solutions in place leads to lower premiums

We expect to wrap up the Cyber Pilot in Q1 of 2025

WE LOOK FORWARD TO CONTINUED PARTNERSHIP WITH NLC-RISC/MUTUAL AND AWC-RMSA AS WE PROGRESS THE PILOT

- Complete onboarding for 4 members in progress
- Develop a roadmap for those members that have personal emails, no domains, or dated operating systems and hardware

AIM
HIGHER