Welcome to the IT Standing Committee Meeting
Housekeeping

- Please stay masked unless actively eating or drinking
- Use standing microphones for questions and comments
- Virtual attendees may “raise hand” to be recognized or ask questions and make comments in the chat
- Slides and all materials will be emailed to the Committee after the conference!
Run of Show

11:00am: Opening remarks and introductions, Chair Matelski
11:05am-11:15am: Cyber Landscape, Serge Jorgensen
11:15am-11:50: Evolving to the Cloud, Jayson Dunn
11:50am-12:30pm: Ransomware, Colin Bowers, Frank Johnson
12:30pm-1:00pm: Identifying Cyber Improvements, Kim Johnson, Todd Ulses
1:00pm-1:30pm: Vulnerable Populations, Ken Wolsey
Opening Remarks and Introductions

Chair Matelski
CIO DeKalb County, GA
Cyber Landscape

Mr. Serge Jorgensen
CTO and Founding Partner, Sylint Group
2022 NACo

LEGISLATIVE CONFERENCE

FEBRUARY 12-16 | WASHINGTON HILTON | WASHINGTON, D.C.
Sylint Group

Accredited by NSA for Incident Response
Approved by Payment Card Industry for Forensic Investigations

Provides Thought Leadership & Guidance in
- Data Security & Privacy
- Cybersecurity Architecture & Posture

Federal, State & Local Governments
Fortune 50 & Private Companies
NGO & Non-profit organizations

Serge Jorgensen
CTO
Cyber Threat Landscape
Threat Landscape & Objectives

- Nation State Resources
  - North Korea – Funding Nuclear Program
  - Russia – Destabilizing Democracy
  - China - Economic Dominance & One World, One Dream

- Organized Crime Motivations
  - Credit Card Theft - $50M/month
  - Business Email Compromise – $1.8B in 2020
  - Ransomware – Payments of $40K to 40M

- Hacktivist Disregard
  - DDoS Tools for $10
  - SSN for $1.50
  - Passwords for free
Russia's SVR intelligence service in the spotlight for SolarWinds hack

by Jerry Dunleavy, Justice Department Reporter | April 15, 2021 01:33 PM

Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks

OCTOBER 11, 2017 // AUTHORS: DONGHUI PARK, MICHAEL WALSTROM

UK says Russia's GRU behind massive Georgia cyber-attack
[Ransomware] **LockBit 2.0** is an affiliate program.

Affiliate program LockBit 2.0 temporarily relaunch the intake of partners.

The program has been underway since September 2019, it is designed in origin C and ASM languages without any dependencies. Encryption is implemented in parts via the completion port (I/O), encryption algorithm AES + ECC. During two years none has managed to decrypt it.

Unparalleled benefits are encryption speed and self-spread function.

The only thing you have to do is to get access to the core server, while LockBit 2.0 will do all the rest. The launch is realized on all devices of the domain network in case of administrator rights on the domain controller.

**Brief feature set:**

- port scanner in local subnetworks, can detect all DFS, SMB, WebDav shares;
- automatic distribution in the domain network at run-time without the necessity of scripts;
- termination of interfering services and processes;
- blocking of process launching that can destroy the encryption process;
- clearing of logs and self-clearing;
- windowed or hidden operating mode;
- launch of computers switched off via Wake-on-Lan;
- print-out of requirements on network printers;
- available for all versions of Windows OS;

![Time spent for downloading of 100 GB](19M 58S)

![Time spent for encryption of 100 GB](4M 28S)
Our company is truly grateful for being our loyal customer for a long time, so we would like to send you a $500 gift card. You can spend it on any goods from the list that you will find on the USB stick. Thank you again for choosing us!
LockBit 2.0 Ransomware

Your data are stolen and encrypted

The data will be published on TOR website
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion and
https://bigblog.at if you do not pay the ransom

You can contact us and decrypt one file for free on these TOR sites
http://lockbitsup4yezcd5enk5unncx3zcy7kw6wlllyqmiyhvanjj352jayid.onion
http://lockbitsap2oaqhcun3syvbq6t6n5nzt7fqosc6jdlmsfleu3ka4k2did.onion
OR
https://decoding.at

Decryption ID: B2BCDXXXXXXXXXXXXXXXXX93E181B2F29E710A
Operational Security

- Cover the Basics
- Ensure Expectations match Reality
Tactical Security

- Add Force Multipliers
  - Audit
  - Legal
  - Emergency Services
Strategic Security

- Introduce Security by Design
- Key Performance Indicators for Leadership
Questions

Serge Jorgensen
sdj@sylint.com
Evolving to the Cloud

Jayson Dunn
AWS Executive Government Advisor,
Former Director of Hamilton
County Communications Center & Former
CIO at the City of Cincinnati
E-FOR ECONOMIC OPPORTUNITIES:
EVOLVING TO THE CLOUD

Jayson Dunn | CISSP, MBA, CPC
Executive Government Advisor
Worldwide Public Sector
jayadunn@amazon.com
DISCUSSION TOPICS

• UNIQUE PUBLIC SECTOR INNOVATION CHALLENGES

• THE FUTURE OF PUBLIC SECTOR IT SERVICE DELIVERY

• THE EVOLVING ROLE OF CLOUD
  o FACTORS DRIVING CLOUD ADOPTION
  o CLOUD MYTHS

• CUSTOMER SUCCESS STORIES

• CONCLUSION / Q & A
UNIQUE PUBLIC SECTOR INNOVATION CHALLENGES
UNIQUE PUBLIC SECTOR CHALLENGES

MULTIPLE LINE OF BUSINESS NEEDS TO SATISFY

PUBLIC SAFETY TOOLS
ERP
FINANCIAL SYSTEMS
CITIZEN ENGAGEMENT
PUBLIC INFORMATION

COUNTY ADMINISTRATION
BUDGET & FINANCE
COUNTY AUDITOR
PURCHASING
HR
ECONOMIC DEVELOPMENT
LAW

WATER / SEWER
PARKS & RECREATION
PUBLIC SERVICES
COUNTY ENGINEER
BOARD OF ELECTIONS
BUILDINGS & INSPECTIONS

COUNTY SHERIFF
JOB & FAMILY SERVICES
CLERK OF COURTS
COUNTY PROSECUTOR
HEALTH & HUMAN SERVICES
PUBLIC SECTOR INNOVATION CHALLENGES

- Frequent operational budget reductions
- Governance / policy development
- Aging infrastructure assets
- Increased demand for remote access
- Silver tsunami / declining skills
- Dependence on capital funds
- Scrutinized expenditures
- Persistent cybersecurity risks
- Forced risk acceptance
THE FUTURE OF PUBLIC SECTOR IT SERVICE DELIVERY
THE FUTURE OF PUBLIC SECTOR IT SERVICE DELIVERY

- BREAK FIX → RE-IMAGE & RE-DEPLOY
- SOFTWARE LICENSES → SOFTWARE SUBSCRIPTIONS
- DATABASES & DATA WAREHOUSES → DATA LAKES
- BUSINESS NETWORK → INTERNET OF THINGS
- RACK & STACK → VIRTUALIZE & CONTAINERIZE

© 2021, Amazon Web Services, Inc. or its Affiliates.
PUBLIC SECTOR TECHNOLOGY NEEDS ARE EVOLVING

- Mobile access to civic data and services
- A/I, machine learning, and data analytics for business decisions
- IoT enabled networks for agile business
- System access beyond firewalls
- Citizen and business needs
IT LEADERS ARE FACING INCREASED PRESSURE

CYBER EVENTS AND OUTAGES ARE NOW FRONT PAGE EVENTS

CIO ROLE IS EVOLVING

IT DIRECTOR
- PREPARING BUDGETS
- PERSONNEL & PROJECTS
- STRATEGIC PLANNING
- ENTERPRISE INNOVATION

CIO
- INNOVATION CHAMPION
- FACE DURING CRISIS
- STRATEGY ARCHITECT
- PARTNERSHIP CREATOR
- CUSTOMER ADVOCATE
- POLICY ENFORCER

© 2021, Amazon Web Services, Inc. or its Affiliates.
THE EVOLVING ROLE OF CLOUD
## FACTORS DRIVING CLOUD ADOPTION

<table>
<thead>
<tr>
<th>Factor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AGILITY</strong></td>
<td>Admins can quickly spin up resources as they need them, deploying hundreds or even thousands of servers in minutes.</td>
</tr>
<tr>
<td><strong>COST</strong></td>
<td>Only pay for IT as you consume it. Becomes variable expense, less expensive than purchasing assets &amp; maintaining infrastructures.</td>
</tr>
<tr>
<td><strong>ELASTICITY</strong></td>
<td>Provision only the amount of resources you need. Can instantly scale up or down as needed.</td>
</tr>
<tr>
<td><strong>INNOVATION SPEED</strong></td>
<td>IT resources can focus on customer service, application deployment, and other business needs instead of managing infrastructure and data centers.</td>
</tr>
<tr>
<td><strong>AVAILABILITY</strong></td>
<td>Customers can leverage 81 AWS Availability Zones across 25 geographic regions worldwide.</td>
</tr>
</tbody>
</table>
AWS has 25 Regions comprised of 81 Availability Zones. Applications and data are replicated in real time throughout each Zone.

A Region is a physical location in the world containing multiple Availability Zones.

An Availability Zone holds multiple data centers with redundant power, networking, and connectivity.

High Availability
Full Scalability
Fault Tolerance
FACTORS DRIVING CLOUD ADOPTION

TRADITIONAL INFRASTRUCTURE

- EQUIPMENT
- DATA CENTER TEAM
- VENDOR CONTRACTS
- LIFE CYCLE COSTS

ON-PREMISE DATA CENTERS LIMIT OFF NETWORK ACCESS

DIFFICULTY EXTRACTING DATA FROM VARIOUS SOURCES

CONTRACT AND PROCUREMENT OBSTACLES CAUSE OVERPROVISIONING

DISASTER RECOVERY AND COOP PLANS INSUFFICIENT DUE LOCATION / ACCESS
FACTORS DRIVING CLOUD ADOPTION

COUNTY ADMINISTRATION
BUDGET & FINANCE
CITIZEN ENGAGEMENT
PUBLIC SAFETY
TOOLS

WATER / SEWER
PARKS & RECREATION
PUBLIC SERVICES

COUNTY SHERRIFF
JOB & FAMILY SERVICES
CLERK OF COURTS
HEALTH & HUMAN
SERVICES

VS

COUNTY ADMINISTRATION
BUDGET & FINANCE
CITIZEN ENGAGEMENT
PUBLIC SAFETY
TOOLS

WATER / SEWER
PARKS & RECREATION
PUBLIC SERVICES

COUNTY SHERRIFF
JOB & FAMILY SERVICES
CLERK OF COURTS
HEALTH & HUMAN
SERVICES
CLOUD MYTHS
MYTH #1: ONCE MY DATA IS LOCKED IN I CAN’T DISCONTINUE

Customers own and are responsible for what is ‘IN’ the Cloud

AWS is responsible for what the cloud ‘IS’
MYTH #2: CLOUD IS LESS SECURE THAN MY ON-PREMISE DATA CENTER

Customers concentrate on systems and apps while AWS manages infrastructure.

AWS

- Facilities
- Physical security
- Compute infrastructure
- Storage infrastructure
- Network infrastructure
- Virtualization layer (EC2)
- Hardened service endpoints
- Rich IAM capabilities

\[+\]

- Network configuration
- Security groups
- OS firewalls
- Operating systems
- Application security
- Proper service configuration
- Account management
- Authorization policies

More secure and compliant systems than any single entity could normally achieve on its own.
MYTH #2: CLOUD IS LESS SECURE THAN MY ON-PREMISE DATA CENTER

AWS Compliance Certifications and Accreditations
# Myth #3: My Data Center Staff Will No Longer Be Needed

## Cost Savings (TCO)
- Infrastructure cost savings/avoidance from moving to the cloud
- Example: 50%+ reduction in TCO (GE)

## Staff Productivity
- Efficiency improvement by function on a task-by-task basis
- Example: Over 500 hours per year of server configuration time saved (Sage)

## Operational Resilience
- Benefit of improving SLAs and reducing unplanned outage
- Example: Critical workloads run in multiple AZs and Regions for robust DR (Expedia)

## Business Agility
- Deploying new features/applications faster and reducing errors
- Example: Launch of new products 75% faster (Unilever)

## KPIs

<table>
<thead>
<tr>
<th>Cost Impact</th>
<th>KPI</th>
<th>Value Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT spend on app per user</td>
<td>VM’s managed per admin</td>
<td>Time to market</td>
</tr>
<tr>
<td>Total IT infrastructure spend</td>
<td>TB’s managed per admin</td>
<td>Time to deploy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operational Resilience</th>
<th>KPI</th>
<th>Value Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application availability</td>
<td>Total monthly incidents</td>
<td>Code deployment frequency</td>
</tr>
<tr>
<td>Critical (P1/P0) incidents</td>
<td>Security incidents</td>
<td>Customer satisfaction</td>
</tr>
<tr>
<td>Security incidents</td>
<td>Mean-time-to-resolution (MTTR)</td>
<td>Employee satisfaction</td>
</tr>
<tr>
<td>App resilience rating</td>
<td>App security rating</td>
<td></td>
</tr>
</tbody>
</table>
MYTH #4: CLOUD COSTS ARE UNPREDICTABLE

Plan
- TCO Calculator
- Migration Evaluator
- AWS Pricing Calculator
- AWS Budgets

Run
- AWS IAM
- Billing Console
- AWS Purchase Order Management
- AWS Budget Actions

See
- AWS Cost Explorer
- AWS Cost & Usage Reports
- AWS Cost Categories
- AWS Cost Anomaly Detection

Save
- Savings Plans
- Reserved Instances
- Recommendations
LA County Call Center Sees 60% Cost Savings With Amazon Connect

Challenge
The county’s legacy contact center was costly to house, maintain, upgrade, and support. It also presented challenges with long hold times and the lack of self-service options available to callers.

Solution
Amazon Connect, a cloud-based contact center solution, solved the challenges presented by the legacy center. Amazon Connect required no supporting infrastructure and offered self-service and automated options to callers.

Benefits
- County estimates 60% annual savings over on-premises infrastructure and licensing costs
- Automating service requests reduces call hold times
- Self-service options drives 17% fewer calls

Amazon Connect is the contact center of the future. It’s an all-in-one, fully cloud-based solution. It changed how we saw our contact center.

Benny Chacko, Deputy General Manager, Shared Services, Information Technology Services, Los Angeles County Internal Services Department

Company: Los Angeles County Internal Services Department
Industry: Local Government & Public Services
Country: United States
Employees: 100,000
Website: isd.lacounty.gov

About LA County ISD
Los Angeles County in Southern California has 10 million residents and more than 100,000 county employees. The Los Angeles County Internal Services Department serves other county departments and provides information to residents.
“What previously would have taken us months, we can now knock out over a weekend and complete testing and piloting over the next week. Our transition and continued investment in the cloud gives us a much more modern system on which we can build for the future.”

—Jack McCarthy, CIO, New Jersey Courts

New Jersey Courts System

Migrated 40 key applications to AWS

- 26,000 virtual court events with 217,000 participants facilitated since March'20
- 99 percent of staff able to work from home
- Turnaround time for select tasks reduced from six months to in 6 days
- Launched its Judiciary Electronic Document System (JEDS) on AWS in just two days

© 2021, Amazon Web Services, Inc. or its Affiliates.
• “We wanted to find a better web publishing platform because the existing one limited what we could do. At the same time, infrastructure was a big factor. We were paying a lot for servers, licensing, and maintenance, and needed to find a way to reduce those costs.”

• “By hosting Drupal on AWS, we’re saving the state of Georgia five million dollars over the next five years.”

Nikhil Deshpande, GTA Chief Data Officer
THE SIMPLIFIED PATH TO CLOUD EVOLUTION

1. INVENTORY ALL ASSETS AND APPLICATIONS
2. IDENTIFY CRITICAL BUSINESS WORKLOADS
3. DETERMINE IF CLOUD OFFERS GREATER BUSINESS VALUE
4. DEFINE YOUR MIGRATION STRATEGY
5. DEVELOP A PLAN AND START THE JOURNEY
Continuous Security Prevents Ransomware and Cyberthreats

Colin Bowers, Director of Cyber Security, Verite Educational Services

Frank Johnson, Former Local Government CIO, current SecuLore Solutions VP Customer Success & Strategy
R for Ransomware
Continuous Security: Prevents Ransomware and Cyber Threats

- The Cybersecurity Challenge
  - Definition of Terms
  - Use Cases
    - Baltimore City
    - Oldsmar, Florida Water Treatment Plant

- Mitigation
- Resources
Introductions

Colin Bowers
Director of Cyber Security
Verite Educational Services

Frank Johnson
Former City CIO
SecuLore Solutions, LLC
Definition of Terms

- Security
- Ransomware
- Cyber threats
- Resiliency
Baltimore City Use Case

- From the perspective of a government cybersecurity leader
- Lessons learned
- What can you do as a leader to prevent ransomware and other cyber harmful events?
Baltimore City Use Case
For Discussion

- Does your county have a disaster recovery plan?
- Does it include cyber incident recovery?
Oldsmar, Florida Water Treatment Plant

- From the perspective of a cybersecurity researcher
- Lessons learned
- Why is this a success story?
For Discussion

- Does your county have a cyber security plan?
- Is cyber security a priority in your county? Why?
Mitigation

- Leadership’s responsibilities
- Holistic approach

- Cyber security lifecycle processes
  - Assess
  - Prioritize
  - Remediate
  - Repeat

Cybersecurity as a priority
Budget
2022 NACo

LEGISLATIVE CONFERENCE

Resources

- NACo Enterprise Cybersecurity Leadership Academy
- NACo Cyber Security Priorities and Best Practices
Contact Information

Erin Kupferberg
Senior Education Strategy Officer
Verite Educational Services
Phone: 703-787-6700 ext. 419
Email: ekupferberg@veriteEDservices.com

Colin Bowers
Director of Cyber Security
Verite Educational Services
Phone: 703-787-6700 ext. 800
Email: cbowers@veriteEDservices.com

Frank Johnson
SecuLore Solutions, LLC
Phone: 410-305-0234
Email: Frank.Johnson@SecuLore.com
What’s My Cyber Readiness Level?

Ms. Kimberly Johnson, VP of Product, BIO-key International

Mr. Todd Ulses, IT Administrator, Curry County, N.M. and New Mexico Counties IT Affiliate Chairman

Ms. Rita Reynolds CIO, NACo
THRIVE “I”:
Identifying Cyber Improvements

2022 NACo Legislative Conference
IT Standing Committee Meeting
Today’s Panelists

Rita Reynolds
CIO
NACo

Todd Ulses
IT Administrator
Curry County, NM
New Mexico Counties IT
Affiliate Chairman

Kimberly Johnson
VP of Product
BIO-key International
The "I" in THRIVE

What cyber improvements does your cybersecurity program need?

- Cybersecurity frameworks and maturity models
- NEW! Quick Check Tool
- Improvement recommendations for IT & county officials
Picking a Framework
Why do you need a framework?

• Structure and methodology to protecting your county

• Different types of frameworks: Control, Program, & Risk

• Most common are NIST, CIS, & ISO
Question for the Audience:
Which cybersecurity framework do you use?
Assessing Your Program Maturity
Don’t miss out on these resources

- **NACo Tech Exchange**: resource for networking and sharing ideas

- **National Cyber Review Survey**: 3 hours to complete and structured around NIST CSF - **closes on Feb 28**

- **CIS Controls**: layman's guide for elected officials vs. IT

- **Security ScoreCard Pilot**
  - Pilot starting at the end of February
  - Quickly see your Security Rating on your publicly facing domain
  - **A few spots remain open to participate**
  - Contact Rita Reynolds at **rreynolds@naco.org**
CISA Cyber Hygiene Services

AVAILABLE AT NO COST:

- Vulnerability scanning
- Web application scanning
- Phishing campaign assessment
- Remote penetration testing

www.cisa.gov/cyber-hygiene-services
## Maturity models to consider

<table>
<thead>
<tr>
<th>MODEL</th>
<th>Cybersecurity Capabilities Maturity Model (C2M2)</th>
<th>NIST Cybersecurity Framework (CSF)</th>
<th>Cybersecurity Maturity Model Certification (CMMC)</th>
<th>FFIEC Cybersecurity Maturity Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maturity Levels/Tiers</td>
<td>3</td>
<td>4/5</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Type of Assessment</td>
<td>Self-assess</td>
<td>Self-assess</td>
<td>Third-party</td>
<td>Self-assess</td>
</tr>
</tbody>
</table>
Assess your program in 10 minutes or less!
Maturity Quick Check Tool

<table>
<thead>
<tr>
<th>Category</th>
<th>Scoring Criteria Names &amp; Definitions</th>
<th>Scores</th>
<th>0 (Very Low)</th>
<th>1 (Low)</th>
<th>2 (Medium)</th>
<th>3 (High)</th>
<th>Scores</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROCESS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SI&amp;G &amp; Metrics</td>
<td>We have clearly defined and shared with all internal stakeholders</td>
<td>Disagree</td>
<td>Neutral</td>
<td>Agree</td>
<td>Strongly Agree</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Management</td>
<td>We have complete asset inventories and processes for managing our assets</td>
<td>Disagree</td>
<td>Neutral</td>
<td>Agree</td>
<td>Strongly Agree</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Governance framework &amp; Policies</td>
<td>Governance framework and security policies are clearly defined and enforced</td>
<td>Disagree</td>
<td>Neutral</td>
<td>Agree</td>
<td>Strongly Agree</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance and Audit</td>
<td>We have mapped and satisfied all regulatory requirements and complete both internal and external audits on at least an annual basis</td>
<td>Disagree</td>
<td>Neutral</td>
<td>Agree</td>
<td>Strongly Agree</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Assessment &amp; Management</td>
<td>We are continuously assessing the cyber risk for our county and third parties</td>
<td>Disagree</td>
<td>Neutral</td>
<td>Agree</td>
<td>Strongly Agree</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disaster Recovery and Business Continuity Plan</td>
<td>We have a clearly defined plan that is understood by all county employees</td>
<td>Disagree</td>
<td>Neutral</td>
<td>Agree</td>
<td>Strongly Agree</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Response Plan</td>
<td>We have a clear plan that includes communications, mitigations, and improvements</td>
<td>Disagree</td>
<td>Neutral</td>
<td>Agree</td>
<td>Strongly Agree</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PEOPLE</td>
<td></td>
<td>SUBTOTAL</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cybersecurity Culture</td>
<td>County employees, including county officials, are aware of our cybersecurity program and share in the responsibility of keeping our county safe</td>
<td>Disagree</td>
<td>Neutral</td>
<td>Agree</td>
<td>Strongly Agree</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mission, Vision, &amp; Strategy</td>
<td>Our program foundation is built on a clear strategy that we communicate to all county employees</td>
<td>Disagree</td>
<td>Neutral</td>
<td>Agree</td>
<td>Strongly Agree</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Educated Users</td>
<td>We have a robust cybersecurity awareness program with continuous training, tests, and simulations</td>
<td>Disagree</td>
<td>Neutral</td>
<td>Agree</td>
<td>Strongly Agree</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TECHNOLOGY</td>
<td></td>
<td>SUBTOTAL</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continuous Monitoring / Threat Detection</td>
<td>We are continuously monitoring for suspicious behaviors, threats, and other abnormalities</td>
<td>Disagree</td>
<td>Neutral</td>
<td>Agree</td>
<td>Strongly Agree</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity and Access Management</td>
<td>We are able to manage identities for employees, suppliers, and citizens and control their access with strong multi-factor authentication</td>
<td>Disagree</td>
<td>Neutral</td>
<td>Agree</td>
<td>Strongly Agree</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Security</td>
<td>Our data is classified based on its level of confidentiality, with the appropriate security measures in place to protect it</td>
<td>Disagree</td>
<td>Neutral</td>
<td>Agree</td>
<td>Strongly Agree</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Download it Now!
Improving Your Cybersecurity
Considerations for IT Teams

Make sure you are taking a multi-later approach and that your security policies “have teeth”.
Considerations for County Officials

Don’t hesitate to ask IT for more information and less technical explanations.
Now what?

1. Use the Quick Check Tool to do an initial assessment

2. Checkout the CISA Cyber Hygiene Services: https://www.cisa.gov/cyber-hygiene-services

3. Familiarize yourself with additional resources:
   - The CIS Center for Internet Security (cisecurity.org) - CIS Controls, Benchmarks, SecureSuite and MS-ISAC
   - NCCoE (nist.gov) National Cybersecurity Center of Excellence is a part of NIST and provides a wealth of guidance on security
   - The NACo Tech Xchange – A community of county IT Leadership that communicates daily through email discussions. A web portal of policies, job descriptions and best practices is also available to members.
Learn more:

Check out more resources and solutions for keeping your county safe:

https://info.bio-key.com/naco-legislative-conference
Thank You

www.BIO-key.com
THRIVE “I”:
Identifying Cyber Improvements

2022 NACo Legislative Conference
IT Standing Committee Meeting
Rita Reynolds
CIO
NACo

Todd Ulses
IT Administrator
Curry County, NM
New Mexico Counties IT
Affiliate Chairman

Kimberly Johnson
VP of Product
BIO-key International

@NACoTweets
#NACoLeg
The "I" in THRIVE
What cyber improvements does your cybersecurity program need?

- Cybersecurity frameworks and maturity models
- NEW! Quick Check Tool
- Improvement recommendations for IT & county officials
Picking a Framework
Why do you need a framework?

- Structure and methodology to protecting your county
- Different types of frameworks: Control, Program, & Risk
- Most common are NIST, CIS, & ISO
Question for the Audience:

Which cybersecurity framework do you use?
Assessing Your Program Maturity
Don’t miss out on these resources

- **NACo Tech Exchange** resource for networking and sharing ideas
- **National Cyber Review Survey**: 3 hours to complete and structured around NIST CSF - **closes on Feb 28**
- CIS Controls: layman's guide for elected officials vs. IT
- **Security ScoreCard Pilot**
  - *Pilot starting at the end of February*
  - *Quickly see your Security Rating on your publicly facing domain*
  - *A few spots remain open to participate*
  - Contact Rita Reynolds at **rreynolds@naco.org**
CISA Cyber Hygiene Services

AVAILABLE AT NO COST:
- Vulnerability scanning
- Web application scanning
- Phishing campaign assessment
- Remote penetration testing

www.cisa.gov/cyber-hygiene-services
## Maturity Models to Consider

<table>
<thead>
<tr>
<th>Model</th>
<th>Cybersecurity Capabilities Maturity Model (C2M2)</th>
<th>NIST Cybersecurity Framework (CSF)</th>
<th>Cybersecurity Maturity Model Certification (CMMC)</th>
<th>FFIEC Cybersecurity Maturity Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maturity Levels/Tiers</td>
<td>3</td>
<td>4/5</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Type of Assessment</td>
<td>Self-assess</td>
<td>Self-assess</td>
<td>Third-party</td>
<td>Self-assess</td>
</tr>
</tbody>
</table>
### Assess your program in 10 minutes or less!
#### Maturity Quick Check Tool

**Quick Check:**
What's Your Cybersecurity Program Maturity?

<table>
<thead>
<tr>
<th>Category</th>
<th>Scoring Criteria Names &amp; Definitions</th>
<th>Scores</th>
<th>Criteria Scores</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROCESS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ILAs &amp; Metrics: are clearly defined and shared with all internal stakeholders</td>
<td></td>
<td>Disagree Neutral Agree Strongly Agree</td>
</tr>
<tr>
<td></td>
<td>Asset Management: we have complete asset inventories and processes for managing our assets</td>
<td></td>
<td>Disagree Neutral Agree Strongly Agree</td>
</tr>
<tr>
<td></td>
<td>Governance framework &amp; Policies: our governance framework and security policies are clearly defined and enforced</td>
<td></td>
<td>Disagree Neutral Agree Strongly Agree</td>
</tr>
<tr>
<td></td>
<td>Compliance and Audits: we have mapped and satisfied all regulatory requirements and complete both internal and external audits on at least an annual basis</td>
<td></td>
<td>Disagree Neutral Agree Strongly Agree</td>
</tr>
<tr>
<td></td>
<td>Risk Assessment &amp; Management: are continuously assessing the cyber risk for our county and third-parties</td>
<td></td>
<td>Disagree Neutral Agree Strongly Agree</td>
</tr>
<tr>
<td></td>
<td>Disaster Recovery and Business Continuity Plan: we have a clearly defined plan that is understood by all county employees</td>
<td></td>
<td>Disagree Neutral Agree Strongly Agree</td>
</tr>
<tr>
<td></td>
<td>Response Plan: we have a clear plan that includes communications, mitigations, and improvements</td>
<td></td>
<td>Disagree Neutral Agree Strongly Agree</td>
</tr>
</tbody>
</table>

**PEOPLE**
Cybersecurity Culture: all county employees, including county officials, are aware of our cybersecurity program and share in the responsibility of keeping our county safe

| Mission, Vision, & Strategy: our program foundation is built on a clear strategy that we communicate to all county employees | |
| Educated Users: we have a robust cybersecurity awareness program with continuous training, tests, and simulations | |

**TECHNOLOGY**
Continuous Monitoring / Threat Detection: we are continuously monitoring for suspicious behaviors, threats, and other abnormalities

| Identity and Access Management: we are able to manage identities for employees, suppliers, and citizens and control their access with strong multi-factor authentication | |
| Data Security: our data is classified based on its level of confidentiality, with the appropriate security measures in place to protect it | |

**Download it Now!**
Improving Your Cybersecurity
Considerations for IT Teams

Make sure you are taking a multi-later approach and that your security policies “have teeth”.
Considerations for County Officials

Don’t hesitate to ask IT for more information and less technical explanations.
1. Use the Quick Check Tool to do an initial assessment

2. Checkout the CISA Cyber Hygiene Services: https://www.cisa.gov/cyber-hygiene-services

3. Familiarize yourself with additional resources:
   - The CIS Center for Internet Security (cisecurity.org) - CIS Controls, Benchmarks, SecureSuite and MS-ISAC
   - NCCoE (nist.gov) National Cybersecurity Center of Excellence is a part of NIST and provides a wealth of guidance on security
   - The NACo Tech Xchange – A community of county IT Leadership that communicates daily through email discussions. A web portal of policies, job descriptions and best practices is also available to members.
Learn more:

Check out more resources and solutions for keeping your county safe:

https://info.bio-key.com/naco-legislative-conference
Thank You

www.BIO-key.com
Vulnerable Populations

Partner, Project Delivery Executive, Health & Human Services,
IBM
2022 NACo Legislative Conference

IT Standing Committee Meeting - Helping Vulnerable Populations to Thrive

Ken Wolsey, IBM
kewolsey@us.ibm.com
Improve outcomes for persons with overwhelming life challenges through enabling technology and safety net collaboration.

Connected Compassion

Child Welfare
Aging & Independence Services
Employment Services
Education & Job Training
Safety Net Collaborative State, County, CBO’s, MCO’s, and IBM

Mobility
Insurance & Medical
Shelter & Housing
Mental Health
Addiction & Recovery
Probation & Justice

Shared Data & Mastered Longitudinal Client Records
Connect360 Intelligent Workflow & Cognitive Tools
Business Objectives

Improve outcomes for vulnerable individuals via increased collaboration between organizations in the health and human services ecosystem in the region.

Shift from program-centric service to person-centered service delivery.

Use technology to enable business process changes, to achieve better outcomes for the most vulnerable.

Use technology partners to modernize custom applications into low code applications while keeping pace with social demands through innovative responses.
Key Executive Findings

Numerous and Complex Programs.
Difficult for clients to navigate, producing partial, suboptimal or poor outcomes.

Service Gaps
Complex needs lead to gaps in services when services are not considered wholistically for persons in crisis.

Program and Organizational Silos
Barriers to access services and collaborate for clients. Produces duplication frustration, mistrust and poor outcomes.

Fragmented Funding
Funding for programs and services crosses between organizational silos and impedes collaboration between organizations.

Lack of Personal Support
Lacks consistent human support, navigational expertise, and advocacy dimensions which a client needs. Clients receive fewer services than they need.

Repetitive Complex Forms and Assessments.
Duplicative efforts for clients and workers. Breeds lack of trust, frustration and trauma.

Time Lag from Application to Service
Critical services unavailable when needed and clients spiral further downward.

Outreach Challenges
Reactive processes. Difficult for workers and providers to identify and reach clients and cohorts who would benefit from additional services.

Documentation Challenges
Difficult and time consuming when clients are in crisis. Impedes progression towards stability and wellbeing.

Client Calendaring & Appointment Mgmt
Clients have difficulty keeping up with all appointments and documentation requirements across multiple providers.

Fragmented, Incomplete and Silo’d Data
Data trapped in program silos. 360° view impossible or difficult to obtain.

Transportation Challenges
Difficult for many clients to access services in person and keep required appointments.
Key Solution Components

Person-centered Service Delivery
Change from a program-centered ecosystem to a person-centered ecosystem of care

Safety Net Organization
Implement a Safety Net Collaborative including the Community Care Coalition

IMDT’s
Implement Interdepartmental Multi-Discipline Teams for case planning and management

Shared Data
Implement a data hub for sharing information across programmatic and organizational silos in support of the Safety Net Collaborative and the IMDT’s

Portals
Implement portals and dashboards to support use cases for different stakeholders: Case Workers, Providers, Clients

© 2022 IBM Corporation
Examples of Recommended Portal Epics

**Case Worker Portal**
- System Access
- Client Registration
- Case Management
- Search
- View
- Assess
- Create
- Annotate
- Refer
- Confer

**Client Portal**
- Anonymous Service
- Register
- Self-Service
- Consent
- Schedule Appointment
- Documents
- Messaging

**Provider Portal**
- Enroll
- Create Account
- Auto-Maintain Profile
- Self-Manage Profile
- Collaborate
- Consent
- Client Data
- Closed Loop Referrals
- Schedule Appointments

**Reports & Dashboard**
- Client Activities
- KPI Metrics
- Case Workloads
- Intake / Assessment Metrics
- Supervisor
- Referral Lifecycle
- Financial Insights
- Aged Reporting
- On-Demand Reports
## SaaS & IaaS based Pay-per-Use or volume discounts

<table>
<thead>
<tr>
<th>SaaS</th>
<th>IaaS</th>
<th>Commercial Connection and Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Application focus for HHS portals and shared data integration fabric</td>
<td>– Infrastructure, database and security with Fedramp Medium, multi-tentant resources and managed services for standard offering</td>
<td>– SaaS based on County population</td>
</tr>
<tr>
<td>– Base offering and common use cases</td>
<td>– Fedramp High dedicated resources for premium or custom offerings</td>
<td>– IaaS for Small Counties pay-per-use</td>
</tr>
<tr>
<td>– Catalog of additional components, services and use cases</td>
<td></td>
<td>– IaaS for Medium and Large Counties pay-per-use or volume discounts</td>
</tr>
</tbody>
</table>
SaaS & IaaS based Pay-per-Use or volume discounts

<table>
<thead>
<tr>
<th>Standard Offering</th>
<th>Premium Offering</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Base standard use cases</td>
<td>– Base use cases plus additions from use case and services catalog</td>
</tr>
<tr>
<td>– Per client configurations</td>
<td>– Per client configurations</td>
</tr>
<tr>
<td>– Multi-tenant IaaS, Security, Data Storage and Managed Services</td>
<td>– Single tenant</td>
</tr>
<tr>
<td>– IaaS pricing: Pay-per-use</td>
<td>– IaaS, Security, Data Storage and Managed Services IaaS pricing: Volume based price</td>
</tr>
<tr>
<td>– SaaS pricing: based on County population parameters</td>
<td></td>
</tr>
</tbody>
</table>

© 2022 IBM Corporation
SaaS & IaaS based Pay-per-Use or volume discounts

Client Code Builds in a SaaS and DevOps architecture

Common Kubernetes Cluster or OpenShift (when Gov Managed Services available)
Standard Data Access & Security in a multi-tenant SaaS architecture

Premium Data Access & Security architecture

Client x
Client y

Client 3 Schema
Client n Schema

Client n Users
Client n Users

Client 2 Users

FedRAMP Medium & Managed Services
Potential Benefits

Counties stay current through technology partnerships and cloud-based strategies

There is reduced need for system customization independent of your technology partners

There is reduced data center, operating and security cost with less vendor lock-in and continuous updates based on the changes in technology and the IT environment

County IT personnel can focus more on IT support functions and less on running proprietary data centers and creating custom applications that are continuously changing to meet evolving business needs and technical innovations.
Discussion Questions

What are the primary portals and use cases for your HHS operations?

- Client portal
- Provider portal
- Care Management portal

Is your County willing to use aaS operational models?

- IaaS
- PaaS
- SaaS

What is the impact of person-centered services versus program-centered services in your County?

- Client outcomes
- Internal efficiencies
- Provider and partner outcomes and efficiencies
Call to Action

• Are you interested to engage with IBM to create/roll out HHS solutions in your County?

• Are you interested to engage with other Counties to create/roll out HHS solutions in your County?

• Send contact information to kewolsey@us.ibm.com
Thank you

Ken Wolsey, IBM
kewolsey@us.ibm.com
Thank you!