Busting Cybersecurity Myths for State & Local Governments

Separating Facts from Fiction to Protect Public Sector Organizations

Vin Curran,
Acrisure Cyber Services

ACRISURE®
CYBER SERVICES

GFOA-PA
GOVERNMENT FINANCE OFFICERS ASSOCIATION OF PENNSYLVANIA

Meet Vin Curran

Head of Sales at Acrisure Cyber Services, advising companies on technology environments and best practices.

- 6+ years of supporting clients across various industries with infrastructure, cloud, and security services.
- Expertise: Industry best practices, regulatory frameworks, carrier requirements, infrastructure, cloud, and security services.

Why Are We Here?

Small Governments, Big Targets

- Cyberattacks against government are increasing – you are a target.
- You protect sensitive citizen data & critical public services.

Goal: Debunk dangerous myths & provide actionable insights for PA government finance leaders

Cybersecurity Landscape for Local Governments in Pennsylvania

Vulnerability: over 2,500 local governments and municipal authorities, many of which are increasingly targeted by cybercriminals due to insufficient defenses

Funding: Local governments in Pennsylvania could soon have access to up to $25 million in federal funding to help them prepare for digital security threats.

Union County - March 2025
- Ransomware attack
- Compromised sensitive data; SSNs, driver's licenses, etc. involved in law enforcement and court-related matters.

Bucks County – January 2024
- Ransomware attack targeting emergency dispatch system
- Disrupted fire call notifications
- CAD system down
- Law enforcement officials also lost access to databases

Myth 2: "We Haven't Been Attacked, So Our Security Is Strong”

The Absence of Detected Attacks Doesn’t Equal Security

Just because an attack hasn’t been detected doesn’t mean it hasn’t occurred. Many attacks go unnoticed due to inadequate monitoring systems.

Silent Threats:

Cybercriminals often infiltrate networks and remain dormant, collecting sensitive data or preparing for larger attacks.

27.6%

of local governments don't know how often they are attacked.

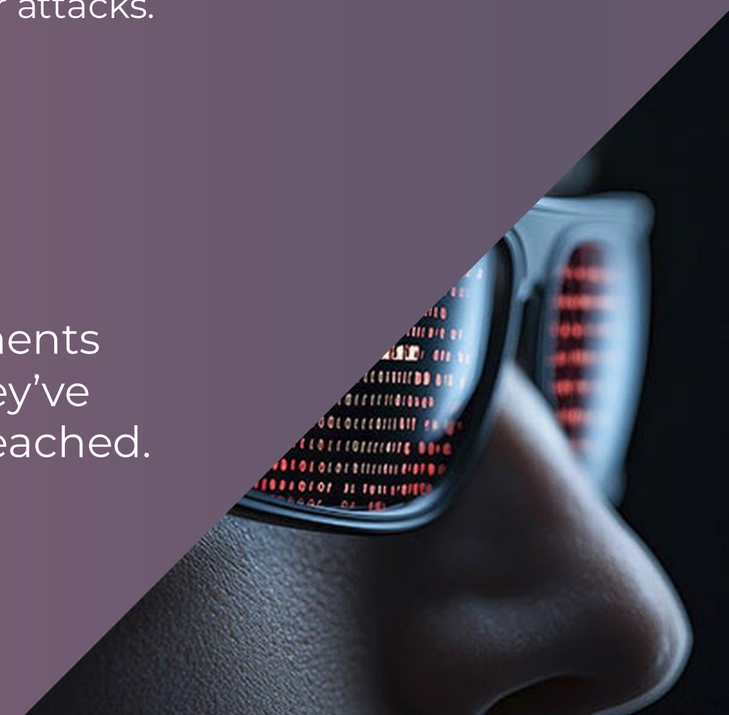
29.7%

of local governments don't know if they've experienced an incident.

41%

of local governments don't know if they’ve already been breached.

- source



Myth 3: "Cybersecurity Is Only the IT Department's Responsibility”

Cybersecurity is a shared responsibility requiring organization-wide awareness and participation.

- Human error is the leading cause of in data breaches.
- Non-technical employees are often the entry point
- Isolated teams hinder unified defense strategies
- **Each department brings unique perspectives**
  - HR can focus on employee training
  - Finance can monitor fraud risks
  - Legal can ensure compliance

~90%

of successful cyberattacks start with phishing emails, especially targeting those outside of IT.

- source

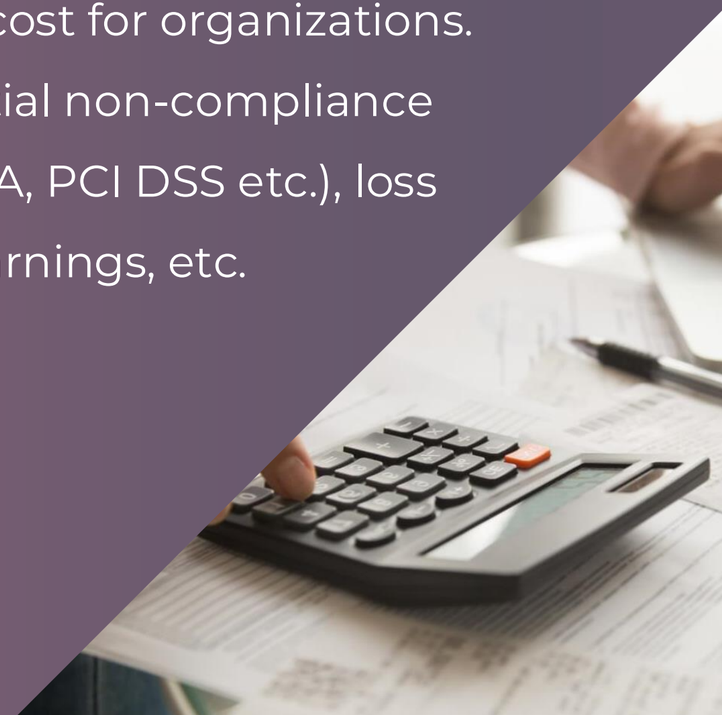
Myth 4: "We Don't Have the Budget for Proper Cybersecurity”

Solutions exist that provide enterprise-grade protection scaled for modest budgets.

- Failing to invest proactively often leads to much higher costs post-incident.
- The sophistication of cyber threats continues to grow, requiring more advanced tools and expertise.
- Prevention pays off:
  - Prevention cost: ~$50,000/year (training, tools, basic monitoring).
  - Recovery cost: $120,000+ per attack

$120K - $1.24M

Is the average cyber attack resolution cost for organizations. Add potential non-compliance fines (HIPAA, PCI DSS etc.), loss of future earnings, etc.



Myth 5: " Strong Passwords Are Enough to Keep Us Safe”

There’s common attack pathways beyond password breaches. Strong passwords are necessary but insufficient on their own.

- Cybersecurity requires a multi-layered approach to protect accounts and systems effectively.
- Hackers use sophisticated tools to bypass password protections.
  - E.g.; brute force attacks, credential stuffing, etc.
- Many users reuse passwords across different accounts/systems.

230 million

Stolen passwords met standard complexity requirements.

- source

Myth 6: “Cloud Services Are Automatically Secure”

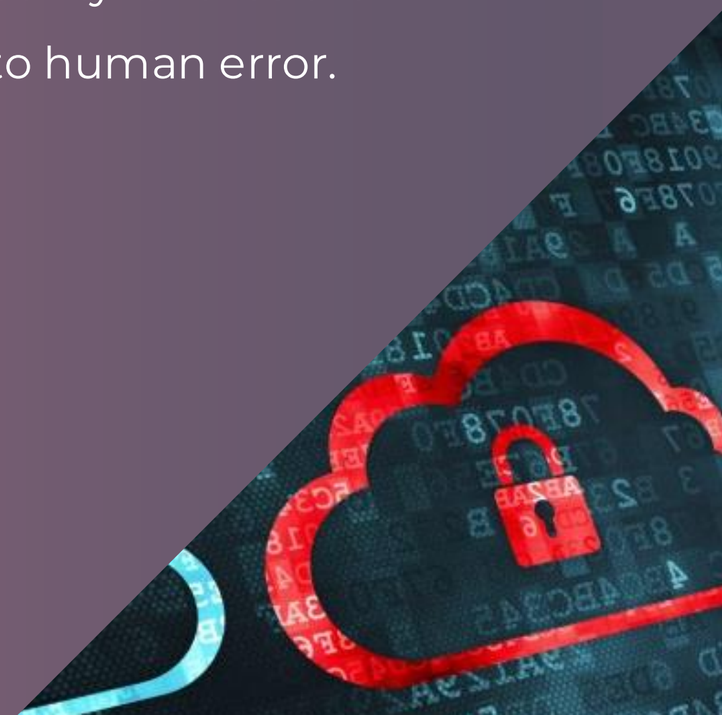
Cloud services are not inherently secure. Security depends on proper configuration and user practices.

- Cloud providers secure the infrastructure, but the customer is responsible for securing their data and configurations within the cloud (Shared Responsibility Model).
- Misconfigurations are common vulnerabilities
- Cloud requires active security management, not passive reliance

99%

of cloud security failures are attributed to human error.

- source



Myth 7: “We Can Handle Cyber Incidents When They Happen”

Reactive measures lead to chaos and higher costs

- Cybersecurity requires proactive planning and defense
- Disaster Recovery (DR) / Backups: Essential for recovery, especially against ransomware. Must be tested & secure (offline/air-gapped)
- Incident Response Plan (IRP): Reduces chaos, ensures critical steps aren't missed. Needed to coordinate internal teams & external experts.

Only 45%

of organizations have an incident response plan (IRP) in place.

- source

Actionable Steps to Protect Your Organization & Community

1. Conduct a Security Risk Assessment: ACS offers a complimentary, non-intrusive cybersecurity & IT risk assessment.

2. Develop or Refine an Incident Response Plan (IRP): Get a free industry-standard IRP template to use now from ACS.

3. Enhance Employee Training: Build a culture of cybersecurity awareness & education; remember, human error is the leading cause of data breaches.

4. Leverage External Resources & Professionals: ACS' certified professionals can fully manage your Cybersecurity & IT 24/7/365 with industry-leading solutions, so you can focus on your core goals.

Who is Acrisure Cyber Services?

We're your **one-stop shop for all Cybersecurity & IT needs**

Advanced
Multi-layered Cybersecurity

Award-Winning
Fully Managed IT Services

Tailored **Cyber Insurance Solutions**

Why do organizations choose ACS?

- ✅ **24/7 Monitoring & Support** by Certified Team of Professionals
- ✅ **Affordable, Complete or Custom** à la carte Solutions
- ✅ **Seamless Integration** with IT Teams & Systems
- ✅ Set-and-Forget **Simplicity**

Learn more at www.Acrisure.com/cyber

ACRISURE®
CYBER SERVICES

Contact Us and Keep Our Contact Info, Just in Case.

We’re here to help.

Email: **cyberservices@acrisure.com**

Phone: **1-877-650-1751**

Learn more at www.Acrisure.com/cyber

GFOA-PA

GOVERNMENT FINANCE OFFICERS
ASSOCIATION OF PENNSYLVANIA