WHAT HAPPENS AFTER 5PM?

Cybersecurity is no longer about keeping attackers out. It's about detecting them quickly, responding effectively, and maintaining public services when something goes wrong

TOM BRENNAN | CEO & PRINCIPAL CONSULTANT

Coffee with NJ-GMIS • September 3, 2026

YOUR SPEAKER

Tom Brennan, Proactive Risk

A New Jersey Veteran, cyber practitioner who has spent his career building, breaking, and defending systems for public and regulated organizations.

01

OPERATOR

Assessments, monitoring, testing, and incident response. United States Marine

02

COMMUNITY LEADER

Longtime contributor to **OWASP, ISC2, CREST International, SAFECODE** and regional security and technology communities.

03

TRUSTED ADVISOR

Advises leadership teams on risk, compliance, and practical after-hours readiness.

THE REALITY

Cyber risk does not keep municipal hours

Residents, public safety, water, finance, and administration depend on systems that must remain available.

01

After-hours alerts

Signals arrive when staff coverage is thinnest.

02

Fragmented visibility

Endpoints, identity, cloud, email, and vendors tell separate stories.

03

Decision pressure

Leaders must contain risk without unnecessarily stopping services.

The operational gap is not another dashboard. It is ownership, context, and a practiced response path.

OPENING SCENARIO

It is 11:30 PM and the alert just came in

A suspicious overseas login. Ransomware starting to spread. Police need systems online, finance runs payroll tomorrow, and public works needs access to critical infrastructure.

01

Who gets called first?

The person who picks up at 11:30 PM decides how the night goes.

02

Who can authorize?

Isolating a device or disabling an account is a business decision.

03

Does everyone know?

Practiced roles are the difference between response and improvisation.

If the answers are unclear tonight, they will be unclear during the incident.

WHO WE ARE

Proactive Risk: New Jersey-based, veteran-owned, security-first

Long-term expertise for organizations where trust, availability, and compliance matter.

01

LOCAL CONTEXT

Serving New Jersey public and regulated organizations.

02

OPERATOR MINDSET

Advice grounded in real investigations and operational constraints.

03

ONE ACCOUNTABLE PARTNER

Assess, manage, monitor, test, and advise across the lifecycle.

HOW WE HELP

An integrated security and risk lifecycle

Each service can stand alone, but the greatest value comes from connecting findings to action.

MANAGEIT	Managed IT, security operations, MDR, cloud and Microsoft 365
CATSCAN	Penetration testing, vulnerability validation and security audits
MEASURERISK	Framework assessments (CIS, NIST, CMMC, ISO, SOC, WQAA), scoring, evidence and executive reporting
VCISO	CyberAdvisor Strategy, governance, incident readiness and fractional guidance
THIRD-PARTY RISK	Vendor due diligence, continuous oversight and remediation tracking annual due care.

MANAGED DETECTION & RESPONSE

From signal to action, around the clock

MDR works when telemetry, experienced analysis, and authorized response are connected.

1. **COLLECT** — Endpoint • identity • cloud • email • network
2. **DETECT** — Behavior, correlation, threat intelligence
3. **INVESTIGATE** — Validate impact, scope, and business context
4. **RESPOND** — Contain, communicate, preserve evidence, recover

MDR IS NOT A TOOL

Technology, people, and process

Most municipalities already have Microsoft 365, firewalls, endpoint protection, and logging. What is usually missing is 24x7 monitoring, threat hunting, alert validation, and incident response expertise.

01

Common gaps

No after-hours coverage, alert fatigue, false positives, unclear escalation.

02

Ask vendors

Who reviews alerts, how fast, what is escalated, who decides?

03

Where it shows up

BEC, credential theft, ransomware, vendor compromise, account takeover.

Buying the technology is the easy part. Coverage, validation, and authority are what make it work and reduce risk.

PRACTICAL RISK MANAGEMENT

Prioritize the risks that interrupt public service

Use a repeatable method that turns technical findings into funded, owned work.

MISSION

Which public services cannot stop?

EXPOSURE

What paths could an attacker use?

IMPACT

What happens to residents and operations?

ACTION

What reduces risk fastest per dollar and hour?

Outcome: a short, defensible roadmap with owners, dates, dependencies, and measurable residual risk.

PRIORITIZING RISK

Likelihood x Impact = Priority, not CVSS = Priority

Limited staffing and budgets, unlimited requirements. Stop chasing every vulnerability and protect what cannot stop.

ASSETS

CRITICAL ASSETS

Public safety
Finance and payroll
Email and identity
Utilities and elections

SCORING

REAL PRIORITY

A CVSS 9.8 on an isolated system may matter less than weak MFA, excessive admin rights, or untested backups

PATTERNS

TOP RISKS

Weak identity controls and incomplete MFA
Too many administrator accounts
Unpatched internet-facing systems
Untested backups, thin vendor oversight, and poor asset inventory

A short list of funded, owned actions beats a long report nobody can execute.

INCIDENT READINESS

The first hour should not be improvised

A prepared team knows who decides, how to communicate, and what evidence to preserve.

0–15 min	Validate the signal • establish incident lead • protect communications
15–30 min	Scope identities, devices, cloud access, and affected services
30–60 min	Contain with business approval • preserve evidence • notify leadership
Next	Eradicate • recover safely • communicate • capture lessons

https://www.proactiverisk.com/PR-SOP-SOC-001-critical-alert-runbook.pdf

INCIDENT READINESS

How prepared are you when prevention fails?

Most organizations invest in prevention. Readiness is what determines the outcome once prevention fails.

1. Lead — CIO, IT manager, consultant, or administrator — someone must lead and everyone must know who

2. Comms — If Microsoft 365 is compromised: personal phones, alternate email, printed emergency contact lists

3. Restore — When was the last restore test, how long did it take, and did it work? Backups are not recovery

4. Practice — Annual tabletop exercises, executive participation, and technical simulations

CURRENT THREATS

What government organizations are seeing more of

The pattern has shifted from malware to misuse of legitimate access, and from prevention to recovery capability.

Identity	Attackers are logging in, stealing sessions, and abusing legitimate credentials — not dropping malware
Email fraud	Still one of the highest-impact attacks: wire fraud, payroll fraud, and vendor impersonation
Ransomware	Judge readiness by detection speed, segmentation, and recovery capability — not prevention alone
Vendors	Many incidents arrive through vendors, software providers, and cloud services

A RIGHT-SIZED STARTING POINT

90 days to better visibility, lower exposure, and stronger readiness

Start with what already exists, then close the most consequential gaps.

DAYS 0–30

BASELINE

Inventory critical services and coverage
Validate identity, endpoint, email, cloud telemetry
Confirm contacts and escalation authority

DAYS 31–60

REDUCE

Remediate priority exposures
Tune detections and response playbooks
Test backup and identity recovery

DAYS 61–90

PROVE

Run tabletop and technical validation
Measure improvement and residual risk
Brief leadership and set next-quarter plan

No rip-and-replace assumption. Use current investments, clarify ownership, then improve deliberately.

IF YOU ONLY DO TEN THINGS

Top ten actions for resource-constrained agencies

Practical, affordable, and achievable with the staff and tools most municipalities already have.

IDENTITY

CONTROL ACCESS

MFA everywhere
Eliminate shared admin accounts
Monitor privileged accounts
Review vendor access

VISIBILITY

SEE AND PATCH

Enable logging
Patch internet-facing assets quickly
Maintain an accurate asset inventory

RESILIENCE

PROVE RECOVERY

Test backups quarterly
Conduct annual tabletop exercises
Implement an MDR program

Ten actions, owned and dated, will move an agency further than another tool purchase.

QUESTIONS FOR THE ROOM

What happens after 5pm in your organization?

Use these prompts to identify the next practical improvement.

1 Who receives the first credible alert?

2 Who can authorize containment?

3 Which systems must stay available?

4 How do you communicate if email is compromised?

5 When was the last recovery or tabletop test?

6 Which vendor would you call first?

UPCOMING EVENT

Join us at Topgolf Parsippany on October 22, 2026

Clients and prospects are welcome. Bring a colleague, swing a few, and keep the after-hours conversation going.

01

WHEN

Thursday, October 22, 2026.

02

WHERE

Topgolf, Parsippany, New Jersey.

03

WHO SHOULD COME

Clients, prospects, and public-sector technology colleagues.

LET’S MAKE AFTER-HOURS LESS UNCERTAIN.

QUESTIONS & DISCUSSION

Tom Brennan
CEO & Principal Consultant

tomb@proactiverisk.com
973-298-1160
www.proactiverisk.com

SDVOSB — Service-Disabled Veteran Owned Small Business (SDVOSB)
NJ Special Contract 24-T3121-PRI01