towerwall

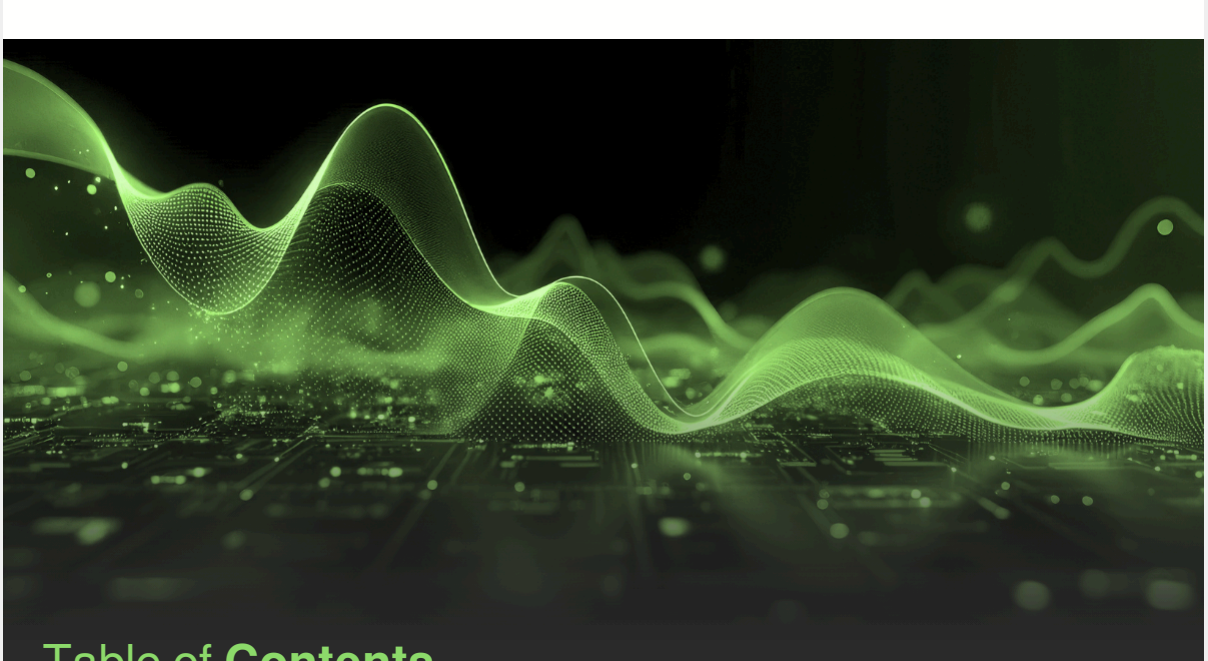

Table of **Contents**

From the **Towerwall** Team

Cybersecurity leadership today requires organizations to balance resilience, governance, operational readiness, and long-term strategy all at once.

Across industries, organizations are navigating growing pressure from evolving ransomware activity, regulatory expectations, and the rapid pace of technological change. At the same time, security leaders are being asked to communicate cyber risk more clearly at the executive and board level while ensuring teams remain prepared for what’s next.

In this edition, we share updates around the upcoming **Towerwall Cybersecurity Summit**, insights into how organizations can strengthen Clery Act support and compliance readiness, and a look at the long-standing partnership between **Towerwall** and **MassBay Community College.**

You’ll also find a recent leadership article from Janelle discussing what every board should understand about cyber risk, along with commentary surrounding the latest ransomware developments and why cybersecurity visibility and preparedness remain critical.

Together, these stories reinforce an important reality: cybersecurity is no longer just a technical initiative. It is a business leadership priority.

News & Events

Towerwall Cybersecurity Summit 2026 | General Admission Now Available

General admission registration is now officially open for the **Towerwall Cybersecurity Summit 2026**, taking place on **June 11, 2026**, in partnership with **MassBay Community College.**

This year’s summit will bring together cybersecurity leaders, practitioners, compliance professionals, and technology decision-makers for a full day of practical insight, leadership discussion, and real-world cybersecurity strategy.

As organizations continue navigating expanding cyber risk, evolving regulations, infrastructure complexity, and AI-driven security challenges, the summit is designed to focus on actionable conversations that help organizations build resilience for the future.

Attendees will hear from industry leaders across topics including:

- Cybersecurity leadership and governance
- Risk management and regulatory strategy
- AI’s growing role in cybersecurity
- Security operations and incident response
- Infrastructure and cloud security
- Zero Trust strategy and implementation
- CMMC readiness and compliance

This year’s keynote speaker, **Dave Escalante**, Director of Computer Policy & Security at Boston College, will present:

“Assume Compromise: Why Resilience Matters More Than Security”

The session will explore why modern cybersecurity leadership must move beyond prevention-focused thinking and prioritize resilience, governance, response, and recovery.

In addition to the educational sessions, proceeds from the summit continue to support scholarships for MassBay’s Cybersecurity Program, helping prepare and empower the next generation of cybersecurity professionals.
We look forward to seeing security leaders, practitioners, and partners from across the region join us for another impactful event.

Register Today!

Threat & Vulnerability Spotlight

Supporting Clery Act Readiness Through Cybersecurity Preparedness

Higher education institutions continue to face increasing pressure to strengthen operational resilience while maintaining compliance with evolving federal requirements.

One area receiving greater attention is **Clery Act readiness**.

While the Clery Act is traditionally associated with campus safety reporting and transparency requirements, today’s digital environment has expanded the conversation significantly. Security incidents, operational disruptions, and cyber-related events can all impact institutional reporting, communication processes, and response coordination.

For colleges and universities, this means cybersecurity preparedness is becoming closely tied to broader institutional resilience. **Organizations are increasingly evaluating:**

- Incident response coordination and communication workflows
- Security monitoring and visibility across systems
- Business continuity and recovery preparedness
- Risk management processes tied to operational disruptions
- Governance and leadership alignment during incidents

As ransomware activity and cyber disruptions continue affecting educational institutions nationwide, proactive preparation is becoming essential not only for security teams, but for institutional leadership as a whole.

Building resilience today requires organizations to think beyond technical controls alone. It requires coordinated planning, visibility, communication readiness, and the ability to respond effectively under pressure.

Read the full article on Campus Technology

Valuable Insight

From a Handshake to a Hub: The MassBay–Towerwall Partnership

Some of the most impactful partnerships begin with a shared mission.
More than a decade ago, Towerwall CEO Michelle Drolet and MassBay Community College leadership came together around a common goal: creating a space where cybersecurity professionals, educators, students, and industry leaders could collaborate, learn, and strengthen the cybersecurity community together.

What began as a modest gathering has since evolved into one of the region’s most recognized cybersecurity events.

The annual Information Security Summit has steadily grown over the last fourteen years, bringing together hundreds of attendees and dozens of cybersecurity vendors and experts from across the Northeast.

The partnership reflects something larger than an annual event. It represents a long-term investment in cybersecurity education, workforce development, and industry collaboration. **Through this continued partnership:**

- Cybersecurity professionals gain access to practical education and leadership insight
- Students receive scholarship support and career exposure
- Organizations strengthen relationships across the regional cybersecurity community
- Industry leaders help shape conversations around emerging threats and resilience

One of the most meaningful aspects of the summit remains its direct support of MassBay students pursuing cybersecurity education and certification programs.

As cybersecurity challenges continue evolving, partnerships like this play an important role in strengthening both today’s security programs and tomorrow’s cybersecurity workforce.

As we continue building that community together,

Join us on June 11, 2026

Leadership Perspective

10 Things Every Board Should Know About Cyber Risk

Cybersecurity is no longer a conversation confined to IT departments.

Boards and executive leadership teams are increasingly expected to understand how cyber risk impacts business operations, reputation, compliance, financial stability, and long-term organizational resilience.

In a recent article featured in the Worcester Business Journal, Towerwall’s Janelle Drolet outlines ten important realities every board should understand when evaluating cyber risk and cybersecurity leadership.

The article explores key themes including:

- Why cyber risk is fundamentally a business risk
- The growing importance of governance and accountability
- The role of executive communication during incidents
- The operational impact of ransomware and disruption
- Why resilience matters as much as prevention
- The importance of continuous preparedness and visibility

As regulatory scrutiny and stakeholder expectations continue to grow, organizations that align cybersecurity conversations with business leadership are often better positioned to respond effectively during periods of disruption.

The article serves as an important reminder that cybersecurity maturity starts with leadership engagement, informed decision-making, and organizational alignment.

Read Janelle's full Article
in the Worcester Business Journal

Compliance & Regulation Watch

AI Governance Is Becoming a Business Requirement

Ransomware attacks continue impacting organizations across healthcare, education, manufacturing, government, and critical infrastructure sectors.

Beyond operational disruption, these incidents are increasingly raising concerns around governance, regulatory readiness, third-party risk, and organizational resilience.

Recent ransomware activity shared by **Michelle Drolet** on LinkedIn highlights an important reality many organizations are facing today: cyber incidents are no longer isolated technical events. They quickly become leadership, operational, financial, and reputational challenges.

Organizations are now being forced to evaluate questions such as:

- How prepared are we to respond during operational disruption?
- Do we have clear incident response and communication plans?
- How quickly can leadership gain visibility into an active incident?
- Are our recovery processes tested and aligned across teams?
- Are we prepared for growing regulatory scrutiny following a cyber event?

These conversations are becoming increasingly important as threat actors continue targeting organizations of all sizes. Cyber resilience today depends not only on prevention, but on visibility, governance, preparedness, and coordinated response.

For ongoing cybersecurity commentary,emerging threat insights, and leadership perspectives:

Follow Michelle Drolet
on LinkedIn

Case Study Spotlight

Building Cybersecurity Resilience in Healthcare: Milford Regional Medical Center & Towerwall

Strong cybersecurity partnerships are built on trust, flexibility, and a deep understanding of what an organization actually needs.
In our latest case study, Nicole Thyne, Executive Vice President and COO at Milford Regional Medical Center, shares how the organization found the cybersecurity expertise their existing technology partners couldn't provide — and how that relationship has grown into an ongoing partnership.

The case study highlights how **Towerwall supported Milford Regional across several critical initiatives**, including:

- **Security posture assessment** and strategic guidance
- **HIPAA** compliance readiness
- **Endpoint protection**, data leakage prevention, and email security
- **Virtual CISO (vCISO) program** tailored to the organization's needs and budget
- **Security awareness training** and privileged access management

For a nonprofit community hospital serving more than 20 towns, getting cybersecurity right isn't optional. The stakes are operational, financial, and deeply human.

"We can depend on Towerwall for anything and everything cybersecurity." — Nicole Thyne, COO, Milford Regional Medical Center

Read the full Case Study

Building Resilience **Together**

Thank you for being part of the Towerwall community.

As cybersecurity challenges continue evolving, collaboration, leadership, and preparedness remain at the center of building resilient organizations. From industry partnerships and cybersecurity education to governance conversations and operational resilience, these efforts continue shaping the future of cybersecurity together.

We look forward to continuing these conversations at this year’s **Cybersecurity Summit** and throughout the months ahead.

— The Towerwall Team.

Book a consultation with Towerwall

Explore our Resource Center

About **Towerwall**

Towerwall is a **trusted, woman-owned information security partner** serving organizations across industries including healthcare, retail, education, technology, and financial services. For over 30 years, our mission has been to help organizations operationalize security, achieve compliance, and protect what matters most.

towerwall