



Table of Contents

1. From the Towerwall team
2. News & Community: Towerwall Cybersecurity Summit 2026. Thank You!
3. Threat & Vulnerability Spotlight: AI Agents for Marketing Are a Security Problem
4. Compliance & Regulation Update: The HIPAA Security Rule Update
5. The Work Continues
6. About Towerwall

From the Towerwall Team

Cybersecurity leadership doesn't slow down between events. If anything, the conversations that start at the summit tend to accelerate everything that follows.

This month, we're reflecting on another successful **Cybersecurity Summit** and sharing insights that carry that momentum forward. From the growing security risks posed by AI agents in marketing and business operations, to an important compliance update that healthcare organizations need on their radar, this edition focuses on what security leaders should be watching, discussing, and acting on right now.

Resilience is built **before the disruption**, not during it. We hope these insights help your organization keep building.

News & Community

Towerwall Cybersecurity Summit 2026: A Look Back at June 11

The **14th Annual Towerwall Cybersecurity Summit**, held June 11 in partnership with **MassBay Community College** at their Wellesley Hills campus, brought together security leaders, practitioners, compliance professionals, and technology decision-makers for a full day of practical conversation and real-world strategy.

This year's keynote, delivered by **Dave Escalante**, Director of Computer Policy and Security at Boston College, set the tone for the entire event:

Assume Compromise: Why Resilience Matters More Than Security

The session challenged attendees to move beyond prevention-first thinking and toward a posture built on resilience, governance, response, and recovery. That theme carried through every session that followed, with speakers and panelists covering:

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

Attendees left with six CPE credits and, more importantly, practical frameworks they can apply across their organizations.

Beyond the content, we're proud that this summit continues to support MassBay students pursuing cybersecurity education and certification. Proceeds go directly toward scholarships, helping build the next generation of cybersecurity professionals in our region.

A Thank You to Our Vendor Partners

*None of this would be possible without the generosity and commitment of the security community that shows up year after year to make this event what it is. Thank you to all 26 **vendor partners** who participated in this year's summit. Your presence, your expertise, and your support of this event, and of **MassBay's students**, make a real difference. We're grateful to work alongside you.*

To everyone who attended, presented, and sponsored the summit this year, **thank you**. These conversations matter, and so does the community that keeps showing up for them.

Presenting Sponsor

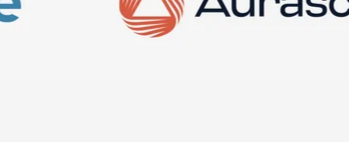


Platinum Sponsor



Gold Sponsors

MARO



proofpoint.

DRATA

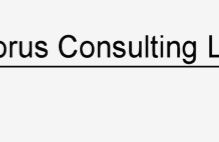


OLIGO



knowbe4

ninjaOne



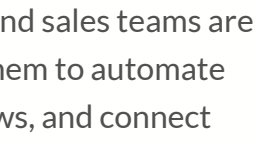
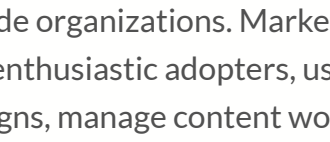
Silver Sponsors

THREATLOCKER

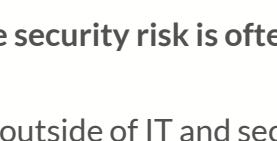


Kiteworks

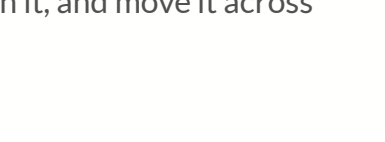
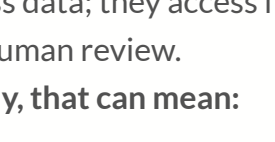
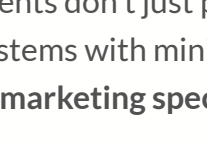
Ultraviolet



VARONIS



FORTINET



Threat & Vulnerability Spotlight

AI Agents for Marketing Are a Security Problem You May Not See Coming

AI agents are moving fast inside organizations. Marketing and sales teams are among the earliest and most enthusiastic adopters, using them to automate outreach, personalize campaigns, manage content workflows, and connect directly to CRM and customer data platforms.

The business case is clear. The security risk is often invisible until it isn't.

When AI agents are deployed outside of IT and security oversight, they introduce a category of risk that's different from traditional software. These agents don't just process data; they access it, act on it, and move it across systems with minimal human review.

In marketing specifically, that can mean:

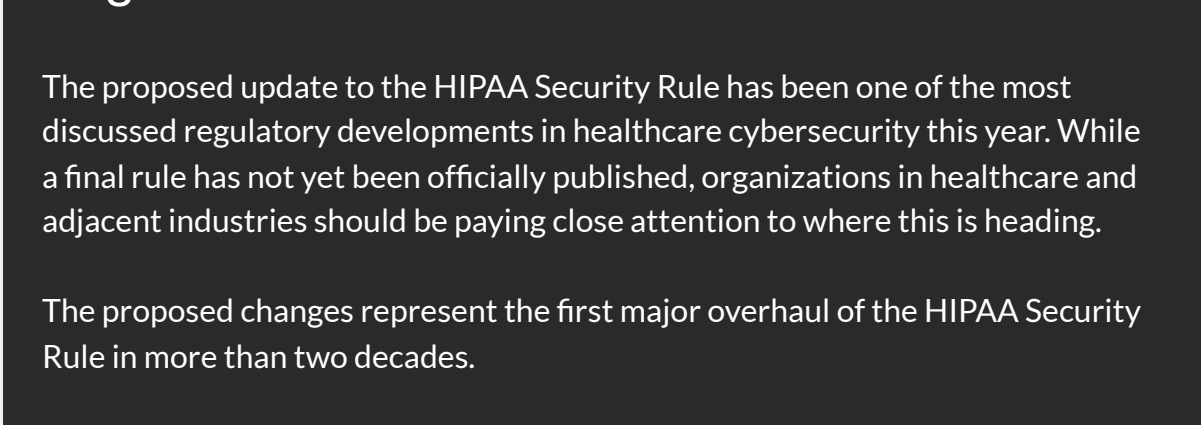
- Customer data shared through AI-powered personalization tools without formal data governance
- Agents connecting to live databases and communication platforms through integrations that weren't security-reviewed
- Prompts and inputs that expose sensitive business logic or customer information to third-party AI systems
- Autonomous actions, such as sending messages or updating records, executed without human approval checkpoints

This is shadow AI in a familiar form. It doesn't look like a threat. It looks like a productivity tool.

The risk isn't in stopping adoption. It's in letting adoption outpace visibility. Security and marketing leadership need to be having these conversations together, and the time to build governance frameworks around AI agents is before an incident, not after.

[Contact Towerwall](#)

to learn how to approach AI agent risk across your organization



Compliance & Regulation Update

The HIPAA Security Rule Update: What Organizations Should Understand Now

The proposed update to the HIPAA Security Rule has been one of the most discussed regulatory developments in healthcare cybersecurity this year. While a final rule has not yet been officially published, organizations in healthcare and adjacent industries should be paying close attention to where this is heading.

The proposed changes represent the first major overhaul of the HIPAA Security Rule in more than two decades.

Key areas of focus include:

- **Mandatory encryption of electronic protected health information (ePHI) at rest and in transit, removing the long-standing "addressable" flexibility that allowed organizations to justify non-implementation**
- **Required multi-factor authentication for systems containing ePHI**
- **Annual penetration testing and vulnerability scanning requirements**
- **Expanded accountability for business associates, with updated BAA language requirements**
- **A 72-hour incident notification requirement to HHS**

OCR enforcement is already trending in this direction, even ahead of a final rule. Risk analysis failures, inadequate access controls, and insufficient encryption have been cited consistently in recent enforcement actions.

For organizations in healthcare, biotech, education, and any sector that handles ePHI or works with healthcare clients, the message is clear: the direction of travel is toward more prescriptive, measurable, and continuously enforced cybersecurity standards. Getting ahead of that curve now reduces compliance risk, reduces audit exposure, and reduces the likelihood of disruption when a final rule does land.

At Towerwall, we help organizations understand where they stand today and what steps make the most sense given their current environment and compliance obligations.

To discuss how the HIPAA Security Rule update could affect your organization:

[Contact Us](#)

The Work Continues

The conversations from this year's summit, the evolving threat landscape, and the regulatory changes ahead all point to the same conclusion: cybersecurity leadership requires sustained attention, not just periodic effort.

The keynote said it best: **assume compromise**. That mindset doesn't end when the summit does. It's the foundation every resilient organization is building on right now.

We remain committed to helping your organization navigate what's ahead with clarity, structure, and a long-term view.

Thank you for being part of the Towerwall community.

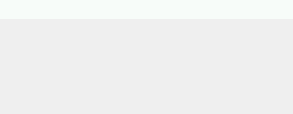
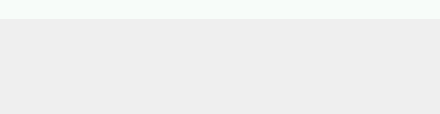
— The Towerwall Team.

[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, 10 Speen Street, 4th Floor Suite 4-01, Framingham, MA 01701, United States, 774-204-0700

[Unsubscribe](#) [Manage preferences](#)