towerwall

Table of **Contents**

From the **Towerwall** Team

Cyber risk rarely announces itself dramatically. Increasingly, it blends into daily operations — calm, routine, and ordinary.

This month's edition explores what happens when risk stops looking suspicious and **starts looking familiar**. From impersonation attacks that bypass detection, to funding assumptions that shape exposure, to regulatory expectations under GLBA, the throughline is clear:

Security leadership requires clarity about how risk actually behaves, not how we assume it behaves.

News & Thought Leadership

10 Things I Know About IT Risk Assessments

In the Worcester Business Journal, Janelle Drolet shares a practical leadership perspective on the role of IT risk assessments in modern organizations.

Her message is straightforward: risk assessments are not compliance exercises. They are operational safeguards.

Among the key themes she highlights:

- Prevent costly downtime before it disrupts operations
- Identify hidden vulnerabilities created by “spaghetti IT”
- Map your full attack surface, including vendors and cloud systems
- Classify and protect sensitive data appropriately
- Make assessments routine, not one-time events
- Prioritize fixes based on business impact, not noise

Perhaps most importantly, Janelle emphasizes that risk management is a team effort. Leadership sets priorities, internal teams execute, and outside expertise provides an independent perspective.

The takeaway: risk assessments are not about finding problems. They are about creating visibility so organizations can make informed decisions.

Read Janelle's full article

Threat & Vulnerability Spotlight

When Phishing Looks Routine

Phishing is not loud anymore. It is normal.
A higher education institution was recently impacted by an impersonation attack that worked precisely because it looked routine.

The email appeared to come from a senior campus leader and referenced a student report. It used a file-sharing link. No urgency. No financial request. No obvious red flags.

Leadership later told us what stood out most was how simple it was. This was not the old stereotype of phishing. It looked like an everyday academic communication, and it blended in well enough to pass their email defenses.

Users who followed the link were walked through a familiar process that ultimately led to a convincing university login page. After credentials were entered, the site displayed a message claiming the interaction was part of a phishing test. That reduced the chance the event would be reported.

The attacker then moved quickly. Payroll details were changed. Mailbox rules were created to permanently delete the notification emails. Because the activity landed right before payroll processing, detection was delayed and the institution experienced measurable financial impact.

What security teams should pay attention to:

- Messages that are calm, brief, and routine
- File sharing workflows that lead to authentication
- Pages that pretend to be internal security testing
- Administrative or payroll changes after login activity
- New inbox rules, especially deletes or redirects
- Testing users with realistic, low drama scenarios instead of obvious traps

Attackers are succeeding more often by looking ordinary. If the strategy depends on catching obvious phishing language, it will miss what is actually working right now.

Valuable Insight:

Utility Text Scams:
When Fear Is the Trigger

Winter outages create anxiety. **Attackers know this**.

As Michelle Drolet recently shared, scammers are sending text messages that appear to come from utility providers, warning of power outages and linking to an “outage map.”

These messages are designed to provoke urgency during freezing weather, encouraging recipients to click without verifying.
The discipline is simple:

- Do not click links in unexpected outage texts
- Visit your utility provider’s official site directly
- Be cautious of alarmist or urgent language
- Pause before acting

Real utility providers do not rely on unsolicited text links for critical updates. Scam awareness is not just about technology. It is about behavioral discipline. **Leaders reinforce this mindset by modeling verification before reaction.**

For ongoing security awareness insights

Follow Michelle Drolet on LinkedIn

Feature Article

The Assumption Your Security Budget **Already Makes**

Most cybersecurity funding conversations begin with a familiar set of questions: Are we spending enough? Are our tools modern? Is insurance sufficient? Is our program adequately resourced? As **Daniel Rathbun** recently outlined, security budgets often encode something deeper, an assumption about how risk behaves.

The real issue is whether incidents fail independently or together. Modern organizations operate in interconnected ecosystems shaped by vendor consolidation, shared cloud infrastructure, common identity platforms, and unified tooling. Each decision is rational on its own. Collectively, they concentrate exposure.

When risk is correlated, such as cloud outages, identity provider disruptions, or supply chain events, impact doesn’t occur once. It propagates. Detection may function and insurance may respond, but recovery demand compounds across systems and departments simultaneously.

This reframes the leadership conversation. The question is no longer simply whether the security program is funded adequately, but whether the funding posture aligns with how risks actually behave. That distinction moves cybersecurity from a cost-center discussion to an exposure governance discussion, one that belongs at the executive and board level.

For CISOs and CFOs alike, **alignment matters more than sufficiency.**

Read the full article

Compliance & Regulatory Update:
GLBA: What Financial Institutions Must Continue to Prioritize

The Gramm-Leach-Bliley Act (GLBA) Safeguards Rule continues to evolve, reinforcing expectations around data protection for financial institutions and organizations handling nonpublic personal information (NPI).

Recent enforcement patterns highlight emphasis on:

- Documented risk assessments
- Multi-factor authentication
- Encryption of sensitive data
- Vendor oversight and third-party risk management
- Formal incident response planning
- Ongoing security monitoring

GLBA is not just a regulatory checklist. It signals federal expectation that cybersecurity governance be operationalized and measurable.

For leadership teams in financial services and related industries, the question is not whether controls exist, but whether they are documented, monitored, and defensible under scrutiny.

Towerwall continues to support organizations navigating GLBA requirements with structured assessments, gap analysis, and ongoing vCISO guidance.

Events & Education

BrightTalk Session with Malwarebytes CEO Marcin Kleczynsk

There is still time to register for tomorrow's Fireside Chat with **Michelle Drolet** and **Malwarebytes CEO Marcin Kleczynski**. In this 30 minute discussion we will touch on topics such as:

- The evolution of modern cyber threats
- AI's role as both weapon and defense

- How organizations without large security teams can defend effectively
- Lessons from building a global cybersecurity company

We will focus on **practical, real-world defense**, not vendor hype. Join us tomorrow at 1:30 PM EST.

Register Now!

Leading Through **Ordinary Risk**

This month's theme is simple:
Risk is increasingly quiet.

It blends into normal communication.
It hides in dependency concentration.
It operates inside routine workflows.

Strong security programs are not built on alarm. They are built on visibility, governance alignment, and leadership discipline.

As threats evolve, Towerwall remains committed to helping organizations operationalize security in ways that reflect how risk truly behaves.

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

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