Thank you for the opportunity to provide testimony today. My name is Nathan Couture, and I serve as the Chief Information Security Officer for The University of Vermont Health Network (UVM Health). I appreciate the Committee's attention to the critical issue of cybersecurity for hospitals and healthcare systems across the State of Maine.

I want to ground my perspective in lived experience. In October of 2020, the UVM Medical Center (the academic medical center within our network) experienced a major cyberattack that resulted in weeks of system downtime and disrupted nearly every aspect of patient care. This was not a theoretical scenario or a tabletop exercise. It was an incident that impacted real patients, real staff, and real communities across Vermont and Northern New York.

Through that experience, we learned lessons that shape how we think about what realistic, durable, and effective cybersecurity policy looks like for hospitals. It is from that vantage point that I strongly support Maine's efforts to focus on response planning, resilience, and recovery rather than prescriptive prevention requirements that, no matter how well intentioned, cannot keep up with the pace and sophistication of modern cyber threats.

The Reality of Cyber Threats in Healthcare

Hospitals are facing adversaries who are:

- well-funded,
- agile,
- globally distributed, and
- increasingly focused on patient-impacting disruptions.

No prevention regime, no matter how robust, can provide 100% protection. Legislation that attempts to mandate specific technical controls will always lag behind the evolving threat landscape. What *can* be legislated effectively, and what will materially improve patient safety, is planning, preparedness, and coordinated response capability.

Key Lessons Learned from the 2020 UVM Medical Center Cyberattack

In the aftermath of our incident, several core lessons emerged, lessons that are directly relevant as Maine considers hospital cybersecurity planning legislation.

1. Traditional Downtime Procedures Are Not Built for Cyberattacks

Most hospitals maintain downtime procedures designed for short-term or localized outages, for example, when a single system or application is briefly unavailable.

But a cyberattack is not a short-term or partial outage.
It can disrupt *all* systems simultaneously, and the downtime can last weeks.

Our experience demonstrated that hospitals need to develop resilience plans that account for:

- enterprise-wide system loss,
- extended durations without core technology, and
- highly manual workflows that strain staff and operations.

2. Emergency Management Assumptions Must Shift for Cyber Events

Traditional hospital emergency management frameworks focus on acute, high-casualty events where triage is based on patient condition.

A cyberattack flips that paradigm.

We were forced to triage care not by medical urgency but by system availability.
For example, imaging, lab, surgical scheduling, and medication administration workflows may be impaired for different durations, making it harder to safely deliver "standard" care.

A cyber event is *not* a mass-casualty surge.
It is a sustained constraint on the entire care delivery ecosystem.

3. Some Clinical Services Cannot Go Fully to Paper

While many inpatient workflows can temporarily revert to paper, certain types of care, such as radiation oncology, require minimally functional technical systems to safely treat patients.

During our cyberattack, we had to quickly engineer temporary, secure technical pathways to safely continue these mission-critical services. Hospitals must plan for these nuances before an attack occurs.

4. Regional Coordination Is as Important as Internal Planning

One of the most important realizations we had was that patient care does not stop at a hospital's physical or organizational boundaries.

During the attack, we relied on regional partners to take on certain patients, share resources, and help maintain continuity of care across state lines.

Cybersecurity legislation should recognize that care networks are interconnected, and preparedness planning must include:

- communication protocols,
- transfer arrangements, and
- joint response frameworks
  across hospitals and regions.

5. External Resources Can Make or Break a Recovery

The activation of the Vermont National Guard, specifically their specialized cyber and technical resources, was a pivotal factor in speeding our recovery and restoring systems safely.

Hospitals alone cannot shoulder the full burden of recovering from a modern cyberattack. States must consider not just mandates, but mechanisms to provide support.

Recommendations for Maine's Legislative Approach

Based on our experience, I respectfully recommend that the Committee prioritize the following areas:

1. Focus on Response and Resilience Over Prescriptive Prevention

Framework-based approaches, such as coordinated incident response plans, are far more adaptive and enduring than lists of mandated controls.

2. Provide Funding, Expertise, and Shared Resources

States can significantly improve hospital preparedness by offering:

- cybersecurity grant programs,
- technical assistance teams,
- cyber navigator programs, and
- surge support resources similar to National Guard cyber units.

3. Incentivize Regional Coordination

Encourage hospitals to develop and exercise regional cyber response plans, including cross-organization communication and coordinated patient movement strategies.

Closing

Cyberattacks against hospitals are not hypothetical, and they are not events that any one organization (regardless of size, sophistication, or investment) can completely prevent. What we *can* do is build stronger, more resilient systems able to protect patient safety even in the midst of disruption.

I commend the State of Maine for approaching this issue with a focus on planning, resilience, and support. I strongly encourage you to pair requirements with the resources hospitals need to implement and sustain them.

Thank you for your time, your leadership, and your attention to this critical matter.

Sincerely,

Nathan Couture
Chief Information Security Officer
UVM Health