PROFILES IN *Confidence*

KATHRYN BURGNER

Information Security Lead, Strategic Advisor

known**well**

Headquarters: Boston, MA

Employees: 100+

Annual Revenue: Private

Kathryn Burgner brings a perspective shaped by the realities of healthcare, where trust and patient data are tightly connected. In a rapidly evolving environment, her role requires balancing innovation with responsibility, ensuring that security supports both patient outcomes and business growth.

Her leadership reflects a broader shift in cybersecurity. It is no longer just about implementing controls. It is about prioritizing risk, enabling the business, and building a culture where security is understood and embraced across the organization.

PRIORITIZING WHAT MATTERS MOST

In a time defined by economic pressure and geopolitical uncertainty, Kathryn's approach is grounded in focus and discipline. "We are really trying to prioritize ruthlessly based on risk exposure, impact, and third-party dependency," she explains.

Rather than trying to address every possible threat, her team concentrates on what is most relevant to the business and its patients. This includes evaluating current risks and aligning security efforts to where they will have the greatest effect. At the same time, efficiency is critical.

"We are always trying to be cost efficient and make sure we are scaling in a way that is smart and right-sized for where we are at in our journey as a company," she says. This balance between focus and efficiency allows her team to move forward with clarity, even in uncertain conditions.

SECURITY AS A BUSINESS ENABLER

Kathryn sees a clear shift in how security leaders must operate today. "We really need to focus on risk reduction and measurable results," she says.

That focus is closely tied to partnership across the organization. Security is no longer a standalone function. It must be integrated into how the business operates and grows.

"Being an enabler, not just an enforcer or just a cost center," she explains, is essential to building credibility and driving impact.

In healthcare, that alignment is especially important. Trust is directly connected to patient experience, making security a core part of delivering value to the business and its customers.

AI AND THE RISE OF HUMAN RISK

When it comes to AI, Kathryn's perspective is centered on its impact on people. "It lowers those barriers," she says, referring to how AI makes it easier for both innovation and malicious activity.

While AI creates opportunities for automation and efficiency, it also increases exposure to human risk. Phishing, social engineering, and other attacks become easier to execute, expanding the threat landscape beyond traditional boundaries. For Kathryn, this shifts the focus of security.

"We are going to need to think about how quickly we can operationalize defenses to human risk while using AI to combat AI," she explains. This includes proactively identifying exposed data, understanding where risk exists, and building defenses that can keep pace with evolving threats.

BALANCING SPEED AND SAFETY

One of the biggest challenges with AI is balancing rapid adoption with responsible use. "Anyone can use it," Kathryn says.

The question is not whether AI will be used, but how safely

and effectively it is implemented. “If we focus too much on the regulatory side, we may miss the speed,” she explains. “But those regulations are there for a reason.”

For Kathryn, the answer lies in balance. By prioritizing risk and evaluating use cases carefully, organizations can move quickly while still protecting sensitive data and maintaining trust. In healthcare, that balance is critical. Patient data and regulatory requirements create a higher standard for how technology must be deployed.

BUILDING A CULTURE OF SECURITY

Rather than relying solely on policies and controls, Kathryn emphasizes culture as a key driver of security success. “The biggest thing we are trying to do is create a culture of security that is transparent and collaborative,” she says.

Her goal is to make security approachable, not intimidating. “Security is not looked at as an enforcer or punishment, but more of an enabler,” she explains.

This approach is particularly important in healthcare environments, where clinicians and providers are focused on patient care and do not have time to navigate complex security processes.

“We need to make it very easy for them to be successful,” Kathryn says. By building trust internally, her team is able to reduce human risk and encourage collaboration across the organization.

EVOLVING SKILLS IN THE AGE OF AI

As AI continues to evolve, Kathryn sees a shift in the skills required for security teams. “I do not think roles will simply be replaced,” she says. Instead, professionals will need to adapt, developing new capabilities around data analysis, modeling, and working effectively with AI tools.

“How can we teach the skills to work with AI,” she explains, rather than focusing on specific tools that may quickly become outdated. This shift reflects a broader change in the workforce. The ability to adapt and apply new technologies will be more important than any single technical skill.

A FRAMEWORK FOR GROWTH

To guide her program, Kathryn relies on established frameworks that provide structure without limiting flexibility. “We use NIST CSF 2.0 as a strategic security enabler,” she says.

This allows her team to measure progress, define maturity, and align security with the company’s growth. “We think about how we are scaling our business and then scaling our security at the right ratio,” she explains.

By focusing on incremental progress, her team avoids becoming overwhelmed while still building a strong foundation.

FOCUSING ON IDENTITY AND PREVENTION

Looking ahead, Kathryn is prioritizing areas that directly reduce risk, particularly identity and human behavior. “Identity and access management is still an important area,” she says.

In addition, her team is focused on preventing attacks before they occur by making secure behavior the easiest path. “We need to make it very easy for them to do the right thing,” she explains.

This approach reflects a shift toward proactive security, where the goal is to reduce risk at its source rather than simply responding to incidents.

BALANCING INNOVATION AND TRUST

For Kathryn, the future of cybersecurity will be defined by balance. “The continued balance between the speed of using new technologies and prevention is going to be so important,” she says.

Organizations must move quickly to remain competitive, but they must also maintain the trust of their customers and stakeholders. At knownwell, that trust is central to everything.

“Our core focus is earning and maintaining patient trust while still enabling growth and innovation,” Kathryn explains. This balance between speed, security, and trust defines her approach to leadership, and positions her team to succeed in a rapidly changing environment.