

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS
WHO ARE LEADING THE WAY
FOR CONFIDENT SECURITY
PROGRAMS



KEN PATTERSON CISO, HARVARD PILGRIM HEALTH CARE

HEADQUARTERS: Wellesley, Massachusetts

EMPLOYEES: 1,400 employees; 2,900 workforce

ANNUAL REVENUE: \$2.5 Billion

“We have seen many examples of data breaches occurring at other companies, especially those in health care. We know, as hard as we try to prevent a data breach, if someone wants us bad enough, they will most likely get us. To this end, we make every effort to be prepared to ensure we continue to earn the trust of our members. To me, that’s what it is all about.”

- **KEN PATTERSON**

TRUST - THE COMMON DENOMINATOR IN BUSINESS & SECURITY SUCCESS

At Harvard Pilgrim Health Care since 2000, and CISO during that time, Ken Patterson has the benefit of historical knowledge and years of reputation and relationship building to help advance the company’s security program. During his tenure, his ability to align security imperatives with business goals through risk management has resulted in strong support for the security program within the organization. He says, “Since I began working at Harvard Pilgrim in June 2000, my security staff has grown from one person to seven people, with additional support from co-ops and summer hires. The executive leadership is aware that healthcare is a highly regulated industry and compliance initiatives must be met, as well as protecting against a major data breach. As a not-for-profit healthcare organization, the privacy and security of our members’ sensitive information is a part of our culture, and continuously reinforced through the privacy and security training of our entire workforce, including our employees, contractors, consultants and temporary personnel.”

EXCEEDING STANDARDS

Harvard Pilgrim recently completed its five-year IT strategy in which security played a major role. Patterson is now focused on a three-to-five year roadmap at Harvard Pilgrim. To accomplish these goals, Patterson starts with ensuring he is fully integrated into the business mission, goals, and approach. “We have a top down push of our objectives; our CEO pushes down to our CIO, and she pushes these goals down to

her direct reports. We all try to understand how we can align with those performance goals,” says Patterson. Patterson has put the work in with his executive-level peers to ensure the program exceeds standards. Patterson says, “Today’s CISO needs to be a strong collaborator with all of his or her business units within an organization and needs to integrate their work successfully into the fabric of the enterprise. To help the business make optimal risk-based security decisions, the CISO must have a solid understanding of how the business operates. Leadership, collaboration, communication, and the ability to establish and nurture effective relationships are required for today’s CISO to be successful.”

UNDERSTANDING CORPORATE GOALS

Patterson says, “The mission of Harvard Pilgrim is to improve the quality and value of healthcare for the people and communities we serve.” The Harvard Pilgrim Corporate Business Strategy is:

- **INNOVATE** - Grow membership in selected market segments by using pragmatic innovations in product and network design, provider partnerships and payment models, and customer decision-support and wellness programs.
- **DIVERSIFY** - Continue to diversify by expanding our business geographically and demographically.
- **MANAGE COSTS** - Strengthen our competitive position through a campaign of disciplined cost management.

Patterson aligns security goals with the mission and organizational goals of the company. Patterson states, “Our security goals are to align risk management, governance, and security programs to business goals; and establish principles that executives and business managers can recognize and support during market segment expansions and new healthcare programs. We listen to business stakeholder needs and engage stakeholders in the planning process. We are focused on improving the ability to react to (and potentially prevent) unforeseen security risks and events.”

ADVICE FOR THE NEW CISO

Patterson’s career in Information Security dates back to the late 1970s. He stands out as one of the first pioneers in the industry. When speaking about the leadership role of CISOs, he says, “Empowerment comes from experience, if you don’t have leadership or communication skills you are not going to make it, those are the skills CISOs need to be effective.” He suggests new CISOs should:

- **Integrate with the Business** - Listen to business executives and understand what they want to get done and be a facilitator - help them get to their goals.
- **Increase your Business Acumen** – Similar to what others in the industry have recognized, Patterson points out that CISOs are often promoted for their technical background, but it takes a different skill set to be a successful CISO. New CISOs need to master the skill of business communication and place security within the realm of business goals when articulating strategy and advocating for security budget and priorities.
- **Work your way up to the board** - For many CISOs there are still at least one (and often more) layers of management between them and the Board. CISOs who do not have direct access to the Board should focus on making their case to other executives. Patterson suggests CISOs prove their communication skills and value to CIOs, CEOs, and CFOs to gain access to the Board.
- **Be Prepared** - Patterson says he meets with his CEO before presenting anything to the Board. This way he is prepared for questions, and he has the support of the CEO in the room.

SECURITY-FOCUSED CULTURE

Patterson and his team work hard to improve privacy and security around compliance with regulations, which has helped instill a security-focused culture. “My executives send me emails concerning recent articles they read about security because it often captures their attention. They understand the importance of being prepared and have helped me advocate this to our entire workforce,” says Patterson. Harvard Pilgrim requires security training for all employees, resulting in an organization-wide understanding of the consequences of a breach in terms of financial loss or reputation. “We make good use cases to demonstrate what could happen here and how we build a process to rapidly detect and respond to any incidents that occur. Even if something minor happens, the workforce knows about it,” comments Patterson.

“ Listen to business executives and understand what they want to get done and be a facilitator - help them get to their goals. ”