

Compliance Today – June 2023



Brian Burton (brian.burton@healthicity.com, [linkedin.com/in/brianburton/](https://www.linkedin.com/in/brianburton/)) is Chief Compliance & Privacy Officer at Healthicity, Brentwood, TN.

How to cultivate strong collaboration between cybersecurity and compliance teams

by Brian Burton

Friends, foes, or strangers: How would you characterize the relationship between your compliance and cybersecurity teams?

Compliance professionals understand that developing open and resilient lines of communication is an instrumental component of any compliance program. By leveraging this responsibility and creating strong cross-functional relationships between the compliance and cybersecurity teams, compliance professionals can increase an organization's ability to optimize its data security and compliance efforts.

HIPAA was just the start of the compliance/cybersecurity relationship—and as digital threats become more sophisticated, the necessity of this high-functioning collaboration is tremendously amplified.

A recent study from Fortified Health Security found that nearly 80% of healthcare data breaches reported to the U.S. Department of Health & Human Services Office for Civil Rights in 2022 were the result of IT incidents and/or hacking, a 45% increase from only five years ago.^[1] Cybercriminals exploit the fact that healthcare organizations have access to confidential patient information and can't afford the lengthy downtime often associated with a ransomware attack.

As healthcare organizations stare down an ever-increasing onslaught of digital threats, one approach to strengthening an organization's security posture is leveraging the combined expertise of cybersecurity and compliance professionals.

Key questions about your compliance and cybersecurity teams

Before we jump in, let's take a step back and consider how your teams work together today—and how you hope they will work together in the future.

Here are some key questions that should hopefully inspire some reflection on the current state of your team's collaboration:

- How do your cybersecurity and compliance teams manage HIPAA requirements?
- How often do the teams collaborate?
- Do you have a formal onboarding process to cross-functionally introduce new team members and their roles?

- Have the two groups worked together in a tabletop exercise?
- How do your compliance and cybersecurity teams address evolving risks together?
- Does each team have a dedicated liaison to the other team to help facilitate communication?
- Has your organization experienced any issues or communication breakdowns because of a lack of team collaboration?

Now, let's think ahead about the future state of your departments. These questions are designed to get you to contemplate how both teams (and your organization) could benefit from deeper teamwork.

- How could better alignment between compliance and cybersecurity strengthen your organization's goals?
- In an ideal world, how often would the teams meet—and what would be on the agenda?
- What policies and procedures could benefit from the combined efforts of both teams when reviewing and updating?
- What would a proactive relationship between compliance and cybersecurity look like to you?

To consider these questions carefully and with veneration, use them as a conversation starter with colleagues. Ask your compliance and cybersecurity teams and collect their input on your organization's current and future state.

Imagine what is on the horizon from both teams' perspectives. From the compliance view, how are teams learning about changes to privacy laws or regulations? From the cybersecurity perspective, what technologies exist in the current environment, and how do these technologies impact administrative policies and workforce education?

A more profound, productive cross-departmental relationship can start with a single question. This is an opportunity to involve colleagues in designing the roadmap for stronger, more effective teamwork across your organization, thus better protecting from and responding to the threats presented to the organization.

This document is only available to members. Please [log in](#) or [become a member](#).

[Become a Member](#) [Login](#)