Checking In with CISOs

We spoke to CISOs we previously profiled and asked them to update us on their goals and challenges.

CISOs are battling an uphill climb while playing an increasingly important role as safety officers in the digital transition of the enterprise. The job is tough, and sometimes it can be hard to see the progress through all the work. But, in the years we have been profiling CISOs we have seen the role evolve from a transactional program within IT to increasingly a strategic element of the company, with impact on innovation.

In the PWC Cyber Security 2017 study, David Burg said, “We’re seeing more and more that cybersecurity can actually become a remarkable way to help a company innovate and move faster.” Compared to two years ago, this is major progress for our industry. Here we check in with the CISOs we have profiled already, to gauge their own progress on solving security challenges, aligning with the business, and carving out a strategic role with executives and in the Boardroom.

Boardroom and Roadmap

During my first year at Webster Bank, board awareness around information and cybersecurity was a hot topic. Today I have consistent “face time” with a dynamic group of directors, no less than six times yearly. Strengthening an already talented Board of Directors and realizing Webster’s need to remain relevant at every level, the bank recently brought on an extremely talented and forward leaning technology Board Director.

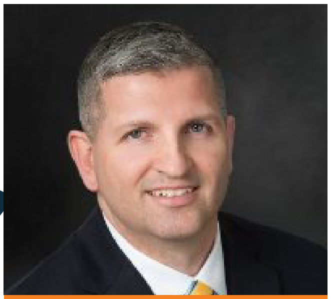
Over the past three years, one consistent topic for the Board remains cybersecurity insurance.   Discussions center on limits, types of coverages, carriers, risk transfer strategies, and retainers.

Our talented and relevant Board of Directors and Executive Leadership has supported a 75% growth in staff, doubling of expense, and significant influx of capital into the Information Security Program over the past three years. Thanks to this outstanding support, my department is able to defend against current threats, plan for regulatory change, and anticipate potential future threats and mitigate them in advance while working in tandem with the lines of business.

Moving Away from MSSP

One of the most significant information and cybersecurity accomplishments over the past 12 months has been the institution of a Technology Operations Center (TOC) at Webster Banks. The TOC has two primary goals, 1st combine elements from the Security Operations, Service Desk, Infrastructure, and Applications group into a specially designed, centralized, and collaborative work area and 2nd to use this collaborative group to better respond to and resolve mundane and line of business technology needs and provide faster and more effective incident response.

As this group begins its journey to 24X7 operations, the next major milestone is the elimination of our currently underperforming and costly outsourced Managed Security Services Provider (MSSP).



Damian Laviolette
CISO
Webster Bank

Putting Plans in Place

Last time we spoke, we did not have a formalized plan for the information security management program. I have since developed a formal plan that addresses mission, goals, and overall strategy including cyber security systems, business continuity and incident response, data management, awareness and training, and policy management. After establishing a clear mission and strategy, I developed a management process designed to accomplish them. This was a major milestone that strengthened my relationship with the Compliance and Audit Committees. We also launched a comprehensive audit plan and implemented a Governance Risk and Compliance (GRC) system.

Increased Visibility

When I started here, it was my desire to create a culture of information security awareness. I was asked to be a member of the Audit Committee. This transition allowed me to successfully promote and raise awareness of our information security program. Ultimately, it served to inform the Board of Directors of the challenges facing the security team and the organization and the measures we've taken to address those challenges. I firmly believe they now have a realistic sense of the risks and are very supportive of our program.

Challenges & Wins

As a smaller company, we are challenged with not having the resources that a large company has to staff a security program, yet we have the same security requirements. Planning and doing can't occupy the same space and operations (doing) will always take the priority. Therefore, having a solid strategy and plan in place is essential to keeping staff focused on what is most important. This helps us overcome the resource issues.

We are going through the HITRUST certification process right now. Attaining certification will be a major win for us because it provides so many benefits to the organization.

Steve Bartolotta
CISO
Community Health
Network of CT

Board-Focused

I consistently meet with the Board and brief them on a regular basis. Most recently, we brought in someone from the New Jersey Cyber Security Communications Integration Cell (NCCIC) who shared what they are seeing in the healthcare industry and suggestions for information security programs. One of these suggestions was encryption at rest, which could have a significant impact on the physicians treating patients.

I now update and explain to my Board on how we have been training our staff to recognize things like phishing email scams, as well as what we've done from a patching and back-up program, so the Board understands the steps we are taking to mitigate risk.

It continues to be important that our board drives information security down throughout Cooper so we may ensure this becomes part of the culture.

Strategic Plan

I've been focused on understanding my strategic plan and continuing to keep focused on that plan.

Phil Curran
CISO & CPO
Cooper University
Hospital

Kevin Hamel
CISO
COCC

Growth Outside of COCC

I worked with the founders of the CISO Executive Network and started up a Hartford chapter. Through reaching out to many of my CISO peers in the area, we got the chapter up and running and now get together six times a year to have meaningful conversations about information security in today's world.

I also participated in the eight week Citizens Academy run by the FBI. This program gave me a behind the scenes, in depth look at the FBI, which has really helped to strengthen our relationship with them and the DOJ. It's really beneficial for us as an organization, because if our clients experience financial fraud or experience a cyber breach, I can reach out to federal law enforcement on their behalf and potentially get our clients some help from federal agencies.

Working with Boards

My strong relationship with our Board and CEO has opened up opportunities for me to speak to our clients' board of directors about cyber security. I've also been asked to speak at a number of other venues such as local chamber of commerce events, audit associations, and even hospitals' board of directors meetings. Board members and business leaders are trying to get their arms around the challenging issue of cyber security.

Focus on Business Risk

Our information security program continues to evolve to a more risk-based focus. We look at info sec findings and translate them into business risk. Also, our employees continue to have a healthy focus of exactly how they play a role in protecting the organization.

Sales Closer

A big part of my role has shifted relative to sales enablement. I now work with our sales organization to assist in being a "closer" from information security perspective. My involvement comes in the late stages of the sales cycle, where security becomes a key differentiator against our competition to help us win the deal. This has been particularly effective when I am utilized with larger enterprise accounts to help them close those opportunities.

Decentralized Security Model

We have really strengthened our risk management program over the last year by pushing a decentralized security model out to the business. We are actually ensuring the business understands, is aware, and takes ownership of the information security risk they truly own. This allows my team to act in more of an oversight and management role, and pushes accountability out to the business.

Agility with High Growth

We are a high growth, fast moving company, so I ensure we have an agile approach to roadmap and planning activities. Things can change quickly, so we must be flexible since new priorities and challenges can come from every business deal. One of my biggest realizations was that narrowing down the horizon for the roadmap to the current quarter and projecting two quarters out provides more responsiveness versus being locked into a one year roadmap. I no longer push my team to predict the future that far out, as priorities can change.

Vanessa Pegueros
CISO
DocuSign

Transition into Healthcare

Seven months ago I transitioned from my role as CISO in retail to a VP, Information Security (CISO) at a large healthcare organization. Something that drew me to this industry is that you have an opportunity to address risks across many industry verticals within a health system. There is healthcare information risk, regulatory risk (HIPAA, PHI etc.), credit card risk (PCI), operational technology (OT) risk, medical device risk and ultimately every other vertical within a growing health systems. I've found having an information security background in other verticals has assisted me lowering risk across our health system large eco-system.

One of the draws to this organization was the CIO openness to partnering with security. Along with his proactive approach to lowering cyber risk and driving security awareness at all levels. I saw this would be a great opportunity to use my executive security experience to build a risk based security program to enable secure innovation to assist in saving lives.

Boardroom Discussions

I have found this organization to be more Board-driven than any industry I have ever worked within. I have attended seven different types of Board meetings with maybe 45% of the same audience. Each Board has a different mission statement and reason why they are interested in the security risk we have across our organization, including the strategic direction information security is taking to lower risk. There is a high expectation of continual updates on how their security investments are lowering cyber risk.

Healthcare before Information Security

Although some areas of healthcare may be slightly behind other industries when it comes to cyber protection, healthcare is more in tune and has been doing security for far longer than information security has been around. In many cases you could say information security's terminology was derived from healthcare. Our information security methods of remediation, containment, isolation, monitoring and triaging risks is how hospitals have been successfully addressing health incidents for years.

Darrell Keeling
CISO
Parkview Health

WHAT HAVE WE LEARNED?

CISOs are executing on their goals and accelerating their information security programs. Great progress has been made with Boardroom alignment and communication through business-focused conversations and strategic discussions.

Every CISO discussed specific goals they accomplished since we featured them in our magazine. They track their progress through metrics and roadmaps, and present this information to both their teams and the Boards. Many of the CISOs we spoke with have grown and improved their teams to act as business enablers.

Overall, CISOs continue to grow from their successes and failures, learn from one another, and push forward to protect their organizations while aligning to the business.