NH-ISAC
DARE TO SHARE

NH-ISAC Monthly Newsletter September 2016

What does serving as a Board Member entail…

Over the past 3 months, we have featured interviews with current NH-ISAC board members to provide insight and information on being a board member and what you can do if you are interested in serving. This is the last one in the series.

This interview features Terry Rice (VP, IT Risk Mgmt. & CISO, Merck & Co., Inc.), Board Member.

How long have you been working with the NH-ISAC?

While I have been on the board of directors since October 2013, my association with the ISAC goes back at least two years earlier. Only Josh Singletary and until recently, Reid Stephan, had more time with the group. Back then we had about a dozen companies participating, we didn't have a listserv, we didn't have summits, and we had very limited threat information sharing. But we did have a vision on what the NH-ISAC could be and we have taken tremendous steps over the last five years to get to where we are today. We still have a lot of work to do, but it is amazing to see how far things have progressed in that time.

What prompted you to get involved?

Each of us is a product of our experiences. There are at least two memories I recall that made me passionate about collaborating with peers in the cybersecurity area. The first was early in my career; I started my professional journey in the military after attending college at West Point. At that time, I anticipated having a career in the military, so I took a lot of classes on national security strategy, international relations theory, and foreign policy matters. One of the interesting lessons I took away from those classes was how groups of people throughout history have worked together to repel significant and often existential threats. From the earliest bands of hunter-gatherers to the emergence of nation-states and on through to the modern era, communities have formed alliances to respond to adversity of all types. These alliances often paired together entities that competed vociferously in other areas, but when faced with a common challenge they bonded together for the good of all. Within the field of national security specifically, the notion of collective defense has been a primary tenet since at least Thucydides and the Peloponnesian Wars. In most cases, collective defense arrangements have allowed defenders to stave off, or at least substantially counterbalance and reduce the effectiveness of, threats posed by a strong adversary.

I believe these lessons are applicable to the field of cybersecurity. To me it is not surprising that as cyber threats continue to grow and increasingly represent critical risks to companies, industries, and even nations, that these same entities are beginning to work collectively to reduce the likelihood and impact of this growing menace. I believe collective defense arrangements, especially real-time threat intelligence sharing through the ISACs and shared utilities like those recently launched as part of the CyberFit program, represent some of the best ways that companies and governmental agencies can work together to respond to the growing cybersecurity challenge. While "cyber" is clearly a new domain with lots of unique problems, history can actually be a useful guide in how we prepare and respond.

The second memory that pushed me to get involved was the experience I had shortly after starting as the director of global security operations at Johnson & Johnson in July of 2003. I started the day before Microsoft released the infamous MS 03-26 patch that corrected a vulnerability in the ubiquitous Microsoft Windows RPC service. I remember reading the bulletin the day it came out and thinking we really need to move fast to get this patch out. But like many, if not most, entities at the time, we just didn't have enough capability to get the new code installed across 120,000 computers before Blaster (aka Lovesan) was released nineteen days later. As we implemented a response plan which included me sleeping on the floor of my office for three nights in a row, I regularly reached out to a small, ad-hoc group of cybersecurity peers and friends that I knew from my days as a consultant. We shared notes on what we were seeing, talked through our respective response plans, and most of all tried to give each other the motivation necessary to go back and deal with the issues as new variants of the worm were released on an almost daily basis. Most of these sessions were via telephone and most were 1:1. As a result, none of us got a full insight into what everyone else was seeing and doing.

I remember thinking after the incident subsided that there had to be a better way. Too many of us were doing exactly the same thing independently, learning from our individual mistakes, and ultimately responding in an inconsistent and haphazard way. While it would be another eight years before I learned about and got involved with the NH-ISAC, I immediately focused my efforts on expanding my network and finding other security people that I might be able to call upon in a crisis. Most of these efforts were cross-industry since the ISAC concept had not matured outside of the financial services, yet I met and gradually became friends with many of the people who now form the NH-ISAC board of directors. I never want to go back to those very lonely days and I never want a cybersecurity colleague to face the discomfort of stepping into a role as challenging as the ones we hold without having a peer network with which they can interact.

Top 10 Health Related Cyber Events This Month:

Massive Cyber Attack at Banner Health Affects 3.7M Individuals

Advocate Health Hit with Record $5.5 Million HIPAA Penalty

Patient Info from Missouri Clinic Hacked By The Dark Overlord Remains Online And Available. Why?

655,000 Bon Secours Patients Exposed to Data Breach

St. Jude: Pacemaker Hacking Claims 'Absolutely Untrue'

Personal Information of Pulse Victims, Survivors Breached, Orlando Health Says

Tackling Medical Device Security as a Public Health Issue

FDA Clarifies When Medical Devices Should Be Re-Approved

Healthcare Hacker Attack Victim Tally Soaring

Hospitals Gravely Concerned on Mobile Device Security

NH-ISAC is pleased to publish this monthly member newsletter. The newsletter is designed to bring events and other important ISAC information to your attention.

If there is something you would like to see included email: contact@nhisac.org

Board interview continued….

Speaking of experience, you have had held cybersecurity positions in a number of different industries. What is unique about the healthcare industry and how should the NH-ISAC handle these unique challenges/opportunities?

The healthcare industry is an extremely wide and diverse ecosystem which makes up more than 17% of US GDP. The healthcare industry is also one of the largest employers in US; one that is growing at a reactively fast pace and well ahead of its peers. The industry is also the leading investor in research and development with nearly a quarter of the nation's total R&D spend going to healthcare related activities. It is an industry where recent advances in biology, chemistry, and information technology offer tremendous potential for us to revolutionize patient care in so many ways. But most importantly, the industry is one where everyone involved gets to have a small part in saving lives and improving the health of countless people across this nation and around the world. This last point is what separates our industry from every other.

That responsibility comes with a significant burden for those of us in the cybersecurity space. We must help bring new life saving technologies and health information services to market while ensuring these capabilities do not put patient information, patient safety, or critical healthcare functions at risk. We are challenged with allowing legacy technology to continue well beyond its intended life as a way to help curtail cost. This must be done while ensuring the legacy applications stay secure and don't impact other parts of integrated healthcare network. We are constantly asked to interconnect partner networks because our industry, unlike others, requires the sharing of a massive amount of extremely sensitive information between many different organizations including primary care, specialists, insurance companies, labs, EHR vendors and others. Cybersecurity professionals must help to implement those connections while ensuring the security of all that are connected.

While all of these are difficult, perhaps the biggest challenge is the fact that the vast majority of healthcare in the United States (some estimates say more than 75%) is delivered via small and mid-sized businesses (SMBs). We know that in general SMBs have a hard time defending their networks because they often lack the capital to buy and implement the latest cybersecurity solutions. Even if they can afford the tools, they have an even harder time recruiting and retaining an adequate amount of appropriately trained staff. It is this situation that presents the NH-ISAC with its greatest opportunity. Our organization has done well attracting large pharma, medical device, insurance, and integrated healthcare delivery networks to the ISAC over the last few years. Both the community and each of these entities have benefited from the collaboration. But the area that needs the collective capabilities of the ISAC even more are the SMBs. We need to focus our energy on making the ISAC accessible, affordable, and appropriate for the SMBs. This has become a major focus of the board of directors.

What are the responsibilities of a board member and what are the skills one must bring to be an effective board member?

While it might sound like fun to be a board member of the NH-ISAC, it is actually a lot of work, most of which must be done during personal hours since each of us have extremely demanding day jobs. The work is often mundane and boring. Yes, I said it. The vast majority of our time is spent on governance issues, budgeting, member recruitment and retention, staff support, legal matters, insurance, and a whole host of topics that have seemingly nothing to do with the sharing of real-time intelligence. But these are important and often critical items that are required to ensure the ability of the NH-ISAC to stay viable as an association.

Yes, we do deal with matters related to the core NH-ISAC mission. We work with the ISAC leadership to develop a strategic plan, select additional offerings, and seek member feedback on what additional features should be added. We also spend a lot of time working with the full time members of the NH-ISAC to help them be more effective in their roles by removing any obstacles to their progress.

I believe that to be an effective board member, the most important quality is an irresolute commitment to "servant leadership." These roles are about giving back to the healthcare ecosystem and the cybersecurity community. As a board member, your first responsibility is to the current and future members of the ISAC. You need to have a passion for putting your own wants, desires, and needs aside and searching for ways to benefit the community even when that causes discomfort, frustration and fear within. At times I have felt all of these emotions.

Despite all the work, the role is deeply satisfying. The joy of seeing a capability come together when you thought at times that it just wasn't going to make it is remarkable. The short acknowledgement from a peer who was able to work through an incident with minimal impact because of a tip passed on by a fellow ISAC member is inspiring. The opportunity to serve next to and work with some of the most experienced and knowledgeable people in the industry is humbling. And the knowledge that all of us across the ISAC family are working to do our part so that our industry can continue to save lives and improve the health of patients is a just reward.

Open Call for NH-ISAC Board Elections

The NH-ISAC Board of Directors is pleased to open the 2016 Board election nominating program. Each year, the terms for several current Board member seats come to a close and NH-ISAC members have the opportunity to select the successor by popular vote. The process begins with an open nomination period, where members are encouraged to self-nominate or recommend another member for consideration.

The 2016 election cycle is unique in that the Board recently approved a term shift to 3 years (from 2), so that each year 1/3rd of the Board seats will be subject to member election. In addition, two seats were vacated during the year by resignation. As a result, there are 9 Board Director positions that will be opened to member nominations for the election cycle later this fall.

Important Dates:

Nomination Deadline: (September 2nd, 5pm Eastern) – Submit nomination by reply to: nhisac@nhisac.org. The only requirement is that the nominee is representing a current NH-ISAC member organization in good standing.

Biography Submission: (September 6th, 5pm Eastern) – Submit brief biography and photo to be provided in the ballot election package.

Voting Period: (September 19th- 28th) – Votes tallied and elected members notified to begin term at the October Board meeting.

Action: The Board encourages self-nominations. If you are interested in helping continue to build the NH-ISAC as a world-class, industry-led sharing organization, please reply to: nhisac@nhisac.org with your expression of interest. You may also nominate another member in good standing, however we encourage you to discuss with your proposed nominee in advance.

Medical Device Workshop Registrations:

Monday, September 26, 2016
Workshop: 8:30am – 5:15pm CT
Evening Reception:
6:00pm – 7:30pm CT

Tuesday, September 27, 2016
Workshop: 8:00am – 2:00pm

Breakfast and Lunch Included

Details to be sent upon registration.

The Kahler Grand Hotel
20 Second Avenue SW
Rochester, MN 55902

Click Here to Register

Don't forget about the Ransomware 101 Workshop…..coming to a city near you!

To register go to https://www.regonline.com/ransomwareroadshow

Washington, DC - September 13, 2016

Seattle - September 14, 2016

Los Angeles - September 15, 2016

San Francisco (Foster City) - September 16, 2016

Altanta - September 19, 2016

Minneapolis - September 20, 2016

Denver - September 21,2016

Houston - September 22, 2016

San Antonio - September 23, 2016

Chicago - October 12, 2016

New York - October 20, 2016

There is no cost to attend this event!

Have you registered? Don't wait too long as space is limited!

Early Bird Registration ends 9/30/2016