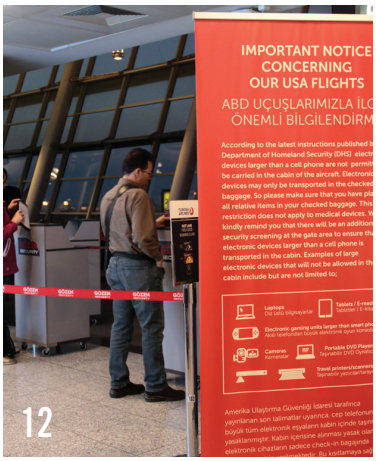
INFRAGARD
MAGAZINE

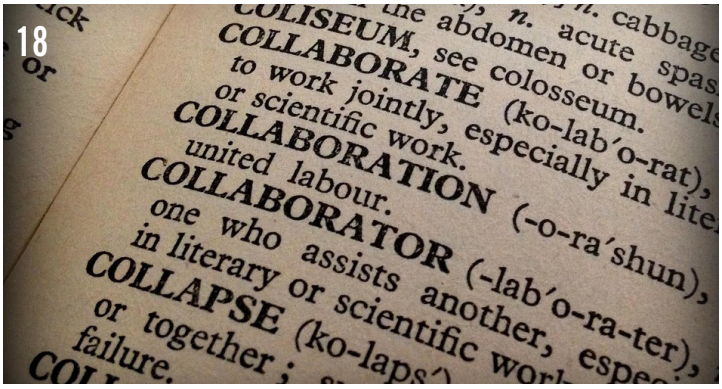
DEVELOPMENTS IN STATE-SPONSORED HACKING
20

APRIL 2017 VOL 3. ISSUE 2.

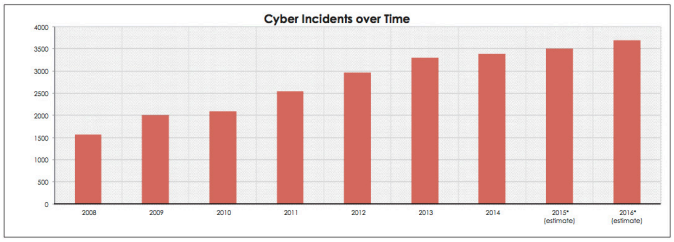
INFRAGARD
MAGAZINE
VOLUME 3 · ISSUE 2

Cover Story:

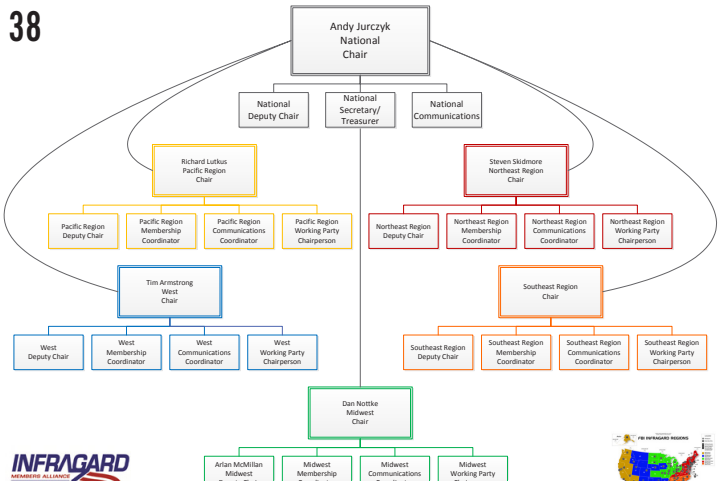




26



38



Cyber Health Working Group Exemplifies Importance of Collaboration Collaboration

By Susan Kahn and Kari Thompson

Around the globe, key players from the public sector, private industry and nonprofit sector are coming together as partners to find long-term solutions to the complex challenges of our rapidly changing world. These partnerships are addressing everything from U.S. infrastructure development to safe drinking water in developing countries. Gilbert Probst of the World Economic Forum has called collaboration "the paradigm of the 21st century."

InfraGard's business model is evidence of this paradigm, and the Cyber Health Working Group (CHWG) is a prime illustrative example. The CHWG is a national healthcare intelligence forum that allows secure peer-to-peer communication for InfraGard-member cyber practitioners across the healthcare domain.

In the spring of 2015, with healthcare cyber breaches making news headlines, the FBI's Cyber Division wanted to bring healthcare IT professionals together for a strategic briefing to share information and mitigate future breaches. Amylynn Errera and Kara Sidener, Special Agents in the Washington, D.C., field office — and their counterparts in FBI field offices across the country, invited cyber professionals from area hospitals, medical billing and medical device companies, health sector nonprofit and trade groups, insurance companies and several federal law enforcement agencies to participate in the briefing.

The meeting between the FBI and the hundreds of healthcare professionals who attended online or in person was a success — but it pointed to a much larger need. Healthcare practitioners were craving peer-to-peer, real-time connection on matters of security. The two enterprising Special Agents determined that a Listserv (an application that distributes messages to subscribers on an electronic mailing list) would be helpful in enabling healthcare IT practitioners throughout the country to connect with one another.

The FBI's partners at the National Cyber-Forensics and Training Alliance (NCFTA), a well-established nonprofit that conducts real-time information sharing and analysis with subject matter experts in the public, private and academic sectors, offered to help the agents establish the Listserv.

More than 500 people indicated interest in the Listserv following a national broadcast message to InfraGard members — underscoring the unmet need, and prompting the development of strict criteria for admittance to the CHWG: Members are required to be current or pending InfraGard members and must work in a healthcare IT position for a relevant organization.

In April 2016, the Listserv went live and members immediately began sharing meaningful information with each other. The knowledge that everyone in the group was vetted through InfraGard provided a baseline level of trust that was further solidified through real-time virtual conversations.

Within three weeks, the staff at NCFTA called the CHWG Listserv "one of the most successful we've ever seen" — so successful, in fact, that they didn't have adequate resources to support it.

Agents Errera and Sidener weren't sure what to do next, knowing they didn't have the capacity to build a Listserv from scratch. They decided to survey the group to validate its usefulness. "We didn't want to re-create the wheel, recognizing there are other sharing platforms in healthcare," said Sidener.

Survey responses from the group resoundingly confirmed that the Listserv was indeed meeting a need no other platform was providing. Members valued the real-time, peer-to-peer connection on relevant, security-related topics. As one member commented, "When I see a message come in from this Listserv, I stop whatever I'm doing to read it."

Knowing the Listserv was fulfilling a need and impacting national cyber security in a very tangible way, the agents kept at it. As is often the case with perseverance, it paid off. Through connections in the FBI's Office of Private Sector, Sidener and Errera were introduced to Sam Khashman, an InfraGard national board member and CEO of Technology Partners, Inc./Imagine Software. Khashman and other InfraGard board members had recently decided to launch an effort to find commonalities among healthcare threats across the InfraGard membership, so the timing was perfect.

"After meeting Amylynn and Kara, I offered — without hesitation — to provide the technology platform to support their effort. It's one way that I can do my part, as CEO of a private sector company, to help the FBI keep all of us safe," said Khashman.

Khashman and his team built a comprehensive portal to replace the Listserv. It was everything Errera and Sidener imagined, with just one flaw. Member conversation slowed dramatically because the portal required members to log in. Members valued the simplicity

and immediacy of the Listserv, and they wanted it back.

The FBI agents, through the partnership with Khashman and his team of tech experts, rebuilt the Listserv and kept the portal to archive conversations and provide a research library for members to contribute to and use. These two platforms, combined with monthly webinars, proved to be the optimal mix for the Cyber Health Working Group.

Today, nearly 300 healthcare cyber practitioners belong to the CHWG — and their participation is making a real difference in healthcare cyber security.

For starters, it's making a difference in the prevention of breaches. Through information shared on the Listserv, combined with the keen observation of a member of Khashman's IT team and swift communication, leaders at one company were able to prevent their systems from being breached — and millions of records from being stolen — by a known hacker. This is just one example of how real-time intelligence sharing and monitoring is preventing cybercrime.
The CHWG information exchange is also making a difference in the day-to-day life of practitioners who are working to strengthen their company's security profiles. In one case, a newly appointed cyber leader at a hospital reached out to the group for help after her senior executives rejected her proposal for a new password policy. Eighty percent of the hospital's personnel were using default passwords, making the company highly vulnerable to attack. She was seeking counsel from more experienced peers about how to convince her leadership to re-consider her proposal. Within minutes, members began offering relevant suggestions to help the new leader persuade her executive team.

"Communication and collaboration at the community level — that is the key," says Gary Gardner, Chairman of the Board, InfraGard National Members Alliance. "Successful public-private partnerships aren't driven by any single person or entity. They're driven by the community. And that has been the real success of the Cyber Healthcare Working Group."

Based on the success of the CHWG, plans are under way to scale the program across sectors.

The team's next priority is to establish a working group at the intersection of energy, transportation and information technology. The ultimate vision is to establish groups for every major sector — and beyond. "The ability to triangulate intelligence across sectors at the community level is important when you consider the interconnectedness of healthcare with other aspects of our economy," said Khashman.

Gardner agrees. "Cyber issues are happening in communities all across the country, so we need to make it easy for community members to engage with each other and with the government," he said.

The Office of Private Sector (OPS) was established in 2014 to coordinate the FBI's engagement with the American business community. OPS works to increase the FBI's understanding of the private sector's risks and needs, increase collaboration and information-sharing between the Bureau and the private sector, and mitigate threats through longstanding, mutually beneficial partnerships between the private sector and the FBI.

Brad Brekke, Director, OPS said, "To address complicated and evolving threats, the FBI and private industry are increasingly engaging in two-way conversation and co-creation. The Cyber Health Working Group exemplifies the future of our partnership."

Errera and Sidener, the special agents at the center of the CHWG co-creation model, offer helpful suggestions for anyone engaging in a public-private partnership. "If you wait to have the perfect model, you're never going to get anything off the ground," says Sidener.

While both agents are capable planners who value strategic roadmaps, they stress the importance of operating loosely in public-private endeavors. "To protect critical infrastructure in the moment, we focused more on getting things done and less on long-term planning," Errera said. They didn't expect their high-tech new portal to halt member conversation; but when it did, they quickly adjusted course and figured out how to re-deploy the effective Listserv tool.

Errera adds that "having the right people involved is essential to build and maintain trust in the effort."

While the journey has had its ups and downs, CHWG planning team members are unanimous in their belief that every step has been worthwhile in helping them learn how best to impact cyber security in the healthcare sector — and in paving the way for future working groups in other sectors.

Through their professional collaboration at 44 Degrees North Partners (www.44degreesnorthpartners.com), Susan Kahn and Kari Thompson design and deliver strategic communication, reputation management and investor relations solutions that engage stakeholders and drive business results. They have been members of InfraGard in Minneapolis, Minnesota since April 2016.