MICHAEL CHARLAND

GLOBL ISO, HARTFORD STEAM BOILER, A SUBSIDIARY OF MUNICH RE

HEADQUARTERS: Hartford, CT (Hartford Steam Boiler) and Munich, Germany (Munich Re)

EMPLOYEES: 41,400+ (Munich Re)

REVENUE: $52 billion (Munich Re)

After spending 21 years working in emergency services, Michael Charland moved into a number of IT roles, eventually leading him to a more security-focused career track. As Charland worked in security roles with increasing levels of technicality and responsibility, he transitioned into managerial positions where he had an opportunity to leverage his communication and business skills. As he matured in his career, Charland had exposure working with other C-level executives to help drive security maturity and grow programs to meet the demanding needs of the business.

Currently the Global Information Security Officer at Hartford Steam Boiler, a Munich Re subsidiary, Charland has responsibility for a global organization inside of a larger global organization. He says, “My organization has seven subsidiaries and two additional business units acting as self-standing business organizations. I currently lead information security in the verticals of finance, hospitality, IoT, insurance/reinsurance, cybersecurity, energy, inspection and engineering of building and other services. I’ve also led information security in the healthcare and banking verticals in the past.”

Charland was attracted to his current role at Munich Re/ Hartford Steam Boiler not only due to the global nature, but because of the numerous subsidiaries in a variety of verticals and the emphasis the organization put on the importance of information security. Reporting into the Global CISO, Charland says it was evident security had a clear vision of direction and defined path for growth.

STRATEGIC SECURITY GOALS

For the year ahead, Charland is focusing on three main goals: increasing security awareness, gaining buy-in and participation from IT and the business, and continuing to grow the program by providing strong information security.

Charland explains, “The basic root of my goals this year is to increase security awareness and bring the organization fully online with the understanding that it takes each and every one of us to protect the organization and its assets. We need to get back to basics as well. I understand that we all enjoy the new flashy devices and “Next Gen” toolsets, but if we don’t manage our assets or properly patch, the fancy tools will not increase our security posture. Information security can be a difficult topic for people because your individual goals are constantly changing with the landscape. Security changes moment by moment, new vulnerabilities are found each day, ways to bypass antivirus and other security tools are developed or released into the wild daily, if not more often. It reminds me of being in law enforcement. We work continuously to learn new skills then train to develop and deploy these skills, but often, our methods become outdated almost as quickly as we deploy them."

THE PEOPLE FACTOR CHALLENGES

In order to accomplish these goals, Charland believes the top challenge he must overcome is the people factor. He believes it is vital to get buy-in from everyone within the organization, so they understand the key role they play in protecting the brand.

He comments, "We need to get the buy-in from people, because I can put tools in all day long. We could do logging and put things in place to help protect us, but if one person clicks on a phishing attempt, then we're chasing the path of being under attack. If one person goes to a website and puts information in that they shouldn't, there are so many avenues that are open to the person being socially engineered."

Communication as the Key to Success

Charland believes communication is critical to his success. In his current role, not only does he communicate with peers in the senior leadership area, but he also communicates regularly with line-staff to understand where they are facing challenges. He says the more everyone speaks with each other, the more open they are inside the organization, and in turn, the more successful they will be.

Building relationships and communicating with other C-level security leaders is also crucial to Charland. He explains, "Communication is one of the ways criminals have always stayed ahead of us. In law enforcement, criminals do not have to follow work hours or rules, and they will use anyone and anything they can to achieve their goal. On the other hand, we must work within rules, laws, and parameters. Our hands are tied because the privacy laws of some countries do not allow tracing of certain end user activities. To combat the fact that we have limitations, we all need to communicate regularly. Build up your CISO and information security network and be there for others when they call you at 10pm on your vacation saying they need a helping hand. We all need to help each other, discuss our pain points, and share solutions we are using to resolve them freely inside our community. That is the only way we stand a chance to keep up. I have had the opportunity to make connections and build relationships with some amazing and incredibly talented individuals in our field. All it took was reaching out, being myself, and being willing to help them in any way. Take the time to build your network. Trust me, it is great to have a network to reach out to and assist in problem resolution."

BUDGET BUY-IN AND APPROACH

Before budget allocations, Charland works to determine where to make investments that will make the greatest impact for the security program. This comes following partnership with IT and the business to determine how the business and IT landscape may change in the coming year.

Charland approaches budget discussions in a strategic manner, especially due to the global reach of the organization. He says, "First I have to have local buy-in. In our case, the local is actually global. It's local to me, but global for all of our organizations. And then budget even rolls up from there to the mother company, who also must have buy-in to the budget. So it not only happens here, but then goes up an additional level to the global level (CIO, CEO, and CISO). It's an interesting situation because we're a global company inside of a global company. You don't see that very often."

He balances current needs with the needs of the year ahead and understands that an over-reliance on tools may not be the right answer. He explains, "You can't just drop a tool in to solve a problem. A new tool requires resources to run it and evaluate the output. Also, that resource needs a backup. It is a balance based on the current needs and those of the upcoming year. In 2008 the IT industry began laying people off and not replacing them, but instead having individuals do more in their roles. This trend has continued. So, I do my best to run with lean teams utilizing highly effective individuals who openly communicate within their team and outside."

MANAGING SECURITY FOR THE CLOUD

"Although many organizations have already begun moving to the cloud, they often have not taken time to provide training to their IT and/or security teams on the differences of how to manage security for cloud. There are many changes in how we manage security in the cloud based on whether the solution is SaaS, IaaS, or PaaS. When moving to cloud, we need to make sure that compliance is in place for our cloud configurations. Automation must be used as much as possible and we must regularly confirm that a person has not accidentally opened a hole causing a security vulnerability. Several times we have seen a person accidentally cause an opening that results in a breach. We need to understand and automate processes with policy and automation in place prior to moving to new technologies."