Week In The Life: Brian Heemsoth, Aetna

Fitting The Pieces Together To Handle Cyber Incidents

Brian Heemsoth
Senior Director
Global Security
Innovation

No two days are ever the same in the world of Information Security, nor does any single day ever seem to go exactly as you draw it up in the morning. The dynamic nature of Information Security is exactly what attracted me to the space earlier in my career, and what keeps me energized (although I could go for a few less 3 a.m. Incident Response emergencies). As a leader in this space, I am challenged each day to fit the pieces together to align resources to support handling of critical cyber security events that may arise, and also to not lose sight of our strategic initiatives related to improving security and access to digital healthcare resources for Aetna's more than 37 million members.

This particular week is a busy one. We have three days of SAFe (Scaled Agile Framework) Release Planning to map out the next three months of work related to Aetna's Digital Transformation initiative, a one-day trip to New York City to meet with a group of early-stage cybersecurity companies, and a healthy smattering of cyber security incidents along the way.

> "The dynamic nature of Information Security is exactly what attracted me to this space, and what keeps me energized."

Each day begins in a repeatable manner – review items in our inbox, and take a look at events handled overnight by our Security Operations Center. I also read cyber intelligence briefings from NH-ISAC (National Healthcare Information Sharing & Analysis Center) and other sources, looking for indicators of threats that may impact Aetna. This is normally where the predictability ends.

On Monday a high-visibility cybersecurity event dominates the day. News of a successful ransomware attack at another organization leads to several work streams internally. Members of our Security Operations Center collaborate with our Security Intelligence group to collect indicators associated with

the event so that we can tune our controls to defend against the type of malware involved. Briefings are prepared to share with stakeholders internally, and Aetna's business units are engaged to quantify relationships Aetna may have with the impacted organization, and any resultant risk. Aetna's Cyber Incident Response procedures are invoked to track all of these work streams.

The next few days are spent primarily attending Release Planning for Aetna's Digital Transformation Program. Our Next Generation Authentication program brings risk-based biometric and behavioral authentication capabilities to consumers in a manner that improves their account security and also makes it easier for each to gain access to Aetna's digital healthcare resources. A good deal of the discussions over the course of these three days focuses around technical details of these offerings, and mapping the introduction of features to individual sprints within the release. Over the course of the week we also complete a design for authentication patterns associated with a new product Aetna plans to launch this year.

"THIS WAS A GOOD WEEK. WE WERE PRODUCTIVE IN ENGAGING KEY STAKEHOLDERS IN ADDRESSING RISKS TO THE ENTERPRISE."

On Friday, I take the train down to New York City to meet with a group of Israeli-based cyber security startups who are in town to demonstrate new product offerings. While these companies carry names most of us have never heard of - and in many cases have only a handful of employees - the progressive visions these companies have towards addressing key risks is refreshing. During this particular showcase, a number of companies share some innovative ideas related to helping companies address challenges that are top of mind – involving cloud security, data protection, and analytical tools that help Security Operations Center analysts effectively identify security risks.

Similar to how each day begins predictably, most end in a predictable fashion. Each day the Aetna Security Operations Center facilitates a *Threat & Vulnerability Assessment* call. This meeting is attended each day by several dozen stakeholders from several organizations, including Aetna Global Security, Aetna's IT organization, and our Legal & Privacy teams. Over the course of this call we will review many enterprise indicators of risk, scoring each for impact and likelihood specific to Aetna along the way. Conversations across this wide group of stakeholders provide a conduit for efficient risk and business impact quantification and initial discussions around risk mitigation plans.

This was a good week. We were productive in engaging key enterprise stakeholders in addressing risks to the enterprise, we have mapped out the next few months of work for our Next Generation Authentication team, and we got to learn about some exciting new technologies being introduced. By the end of the week, I am looking forward to a relaxing weekend and to seeing what the next week brings.