Cybersecurity Analyst

Interview by Elizabeth Heubeck

Kyle Forsyth

When Kyle Forsyth started college, the U.S. Department of Homeland Security hadn't yet been created. Now he works as a lead information security specialist at Noblis, protecting against cyber threats for one of the nonprofit's largest government clients: The U.S. Department of Homeland Security. Daily, he and his team of colleagues work to identify and halt cyber criminals from hacking into computer systems that could expose confidential information or even threaten our nation's safety. Here, he explains how he got the job, what it entails, and how others can follow in his footsteps.

STEPHANIE RAYNOR

How did you become interested in a career in cybersecurity?

When I was in college, if you wanted to get into computers, you took programming classes. That was not for me. That is still not for me. What really interested me was tinkering around with computers on the side. That's how I got involved in system design and computer engineering.

In choosing an undergraduate major in college, I found myself leaning toward an engineering track—network engineering with a focus on the infrastructure. I found a program at Shepherd University, majoring in computer and information technology, to suit my strengths. It focused on networks, databases, and system development.

What experiences outside of college helped you get a job after graduation?

While in college, I secured an internship with the U.S. Department of Agriculture, where I worked as a technical customer support representative in a system administrator role. I continued to work there after graduation. Realizing I had a lot of experience on the technical side but not the policy and procedure side, I started applying for security positions, which is how I got into security-related work. I later earned a Master of Science in Information Security and Assurance at George Mason University.

What constitutes a cyber threat and how common have they become?

Threats can be different things: software on the outside, a misconfiguration of a system configuration, or an insider threat—when someone on the inside is doing something nefarious.

Equifax just got hacked. They had a vulnerability in their system that they either didn't know about or decided not to fix, which attackers took advantage of quickly. Because we live in a connected world, it's easy to interface with other computer systems from anywhere. Many systems and networks are constantly under attack because of notoriety or prominence; for example, government networks, large companies like Yahoo or Anthem, and financial institutions like Equifax.

What is the potential range of consequences a cyber threat could pose to our nation's security?

A lot of it can just be defamation of character; you lose trust in an industry or organization. There could also be a leak of information to the general public that could harm other individuals—information that wasn't supposed to be made public, which could lead to harm or loss of confidence in an organization.

So, in a sense, you are part of a team of modern-day warriors, fighting unseen but very real threats to our nation's security. What is that like?

We have our own battlefield; it is very different than a traditional one. We certainly are not risking our lives to do what we do, but we are definitely trying to think how our adversaries are thinking and to mitigate their attempts or stop them. We do work as a team, trying to catch bad people doing bad things.

Your employer, Noblis, is a nonprofit that supports government clients. Do cyber analysts typically work for the government, or are there also opportunities in the private sector?

There are tons of opportunities in the private sector. I know a lot of people starting to work in the financial sector, which is beginning to hire good cybersecurity

people. They're willing to invest a good bit of funding into trying to secure their networks. We also see a lot of people in our industry working for bigger companies, like Google, Amazon, and Microsoft.

Can you share what a day at work looks like for you?

Typically, we have a lot of working sessions and meetings. As government contractors, we're partners with the government. We try to piece together information about what has transpired so we can communicate it back to our clients. We also try to stay sharp with our technical skills, and we routinely have a lot of data management tasks like technical and executive presentations, breach reports, and project management.

Tell me something about your job that people might find surprising.

My position requires a mix of management and soft skills: good communication skills, technically and at an executive level. We have to communicate with our management and clients. The importance of our technical work can sometimes be lost in translation to upper level management, so good communication skills are vital.

How important to your job is the ability to collaborate with co-workers?

We do a lot of collaboration. The team I work with is particularly diverse: We're able to bounce ideas off each other and take different perspectives.

When we find bad things happening, a lot of those bad things are not found in succession. You might find step four, then step two. We develop a context to tell the story of that threat, making the decision as a team.

What is the most challenging aspect of your job?

I think balancing the activities we have to do. We have communication tasks, but we also want to stay in the technical realm. It's like a see-saw. If you don't balance it well enough, you start to lose the technical side or the management side.

What makes you excited to come to work in the morning?

Catching bad guys!

Are the education and training that go into becoming a cybersecurity analyst linear, or are there several different routes to get there?

There are different routes. We have a lot of high-level academic folks—Ph.D.-educated computer science people who look at a lot of theory and cybersecurity overall. We also have a lot of technical folks who look at the development of security applications, or at analytics and large data sets.

Can you share some advice for young people who might be interested in becoming a cybersecurity analyst?

I'm not a very good programmer, but I see a lot of value in programming and understanding how it works. I think you have to have a good foundation of how to program, but that doesn't mean that's what you have to do when you get out of school. There are things to do in the field of cybersecurity other than computer programming, such as infrastructure management, computer forensics, information security analysis, and cryptography. I would encourage people to look at other related avenues of learning such as data analytics and mathematics. It's a very broad field. ■

What cybersecurity analysts do

The primary responsibility of cybersecurity analysts (also referred to as information security analysts) is to protect an organization's computer systems and networks by preventing, identifying, and countering activities of cybercriminals intent on "stealing" confidential information or disrupting computer-related operations.

Where they work

Cybersecurity analysts typically work for the government, in the private sector as government contractors, or in private sector fields.

Education required

Most information security analyst positions require a bachelor's degree in a computer-related field. Professionals with higher-level positions in the industry often possess graduate degrees.

Job outlook

The job outlook for information security analysts is excellent. Growth for these professionals is estimated to be about 18 percent from 2014 to 2024. The demand for information security analysts is likely to continue beyond that period, as an ever-increasing number of organizations seek to prevent hackers from obtaining confidential information and wreaking havoc on their computer systems.

Salary

According to the Bureau of Labor Statistics, the median annual wage for information security analysts was $92,600 in May 2016.

Learn more

Association for Computing Machinery
http://www.acm.org

Computing Research Association
cra.org

IEEE Computer Society
computer.org

ISTOCK.COM/HYWARDS