Honoring Our Past. Innovating Our Future

Tyler Hardison, CISSP, PCI Qualified Security Assessor

Is the chief technology officer at Redhawk Network Security, a provider of world-class security and compliance assessments, managed security services, incident response planning and testing, and network and technical consulting. He plays a key role at Redhawk in leading new product strategies and initiatives and is responsible for developing technology solutions and service offerings for clients. He is highly regarded as a hands-on technologist with a strong focus on regulatory issues, program management and secure implementation. With his extensive knowledge of evolving cybersecurity threats, Hardison leads the development and execution of innovative, robust and secure information technology environments for organizations of all sizes. He has extensive experience and knowledge of security and IT, including regulatory issues and compliance, enterprise architecture, disaster recovery, process improvement, custom application development, and risk management. Hardison is a 20-year technology veteran, with 12 years of experience in the financial services industry, including serving as chief information officer at Stanford Federal Credit Union. He is at the forefront of regulatory changes, with in-depth knowledge of the tools necessary to stay ahead. He speaks regularly on how businesses can meet compliance.

Q: What is it that drew you to the cybersecurity profession? What keeps you in the profession?

A: In 1999, I was a junior systems administrator who had been experimenting with my home lab and Redhat Linux 6.1. I had been using it as a firewall/gateway and, at one point, it had started behaving erratically. A friend of mine pointed out that it might have been hacked. After poking around on the machine, I discovered that it had indeed been the victim of a rootkit. That first experience of discovery and my subsequent dive into operating system hardening awoke the security interest in me. This experience and the regulatory changes within the industries I was working drove a passion in "defeating" the bad guys and a persistent vigilance for all things security related. It is this vigilance and interest that keep me engaged and wanting to protect that sweet data from the wrong hands.

Q: How do you think the profession will change and evolve in the future? How will these changes impact the cybersecurity professional and how will the role evolve?

A: Artificial intelligence (AI) and big data are the biggest drivers in our evolving threat and risk landscapes. The sheer scope and breadth of data collected are far too much for one team to handle on its own. We must become increasingly reliant on our tools to analyze the gargantuan amount of security information data that are flowing our way. We have surpassed the ability of humans to perform sufficient analysis. Therefore, it is incumbent on the security professional to seek out more automation and learn to leverage those tools. This means that the average analyst needs to be proficient in at least one programming language to help extend their ability to automatically detect anomalies in their environment. Additionally, learning penetration testing and thinking like a nefarious agent will help practitioners begin to understand the true solutions for properly protecting data. Cybersecurity cannot be an "armchair" profession. Each individual needs to be constantly learning and vigilant.

Q: What skills will be most important for cyber professionals to develop in the coming year(s), decade?

A: I believe that learning penetration testing and at least one programming language is going to be imperative for any security professional. Effective communication to those who are not skilled in technology is critical. Those with nefarious intentions are exploiting the less technology-skilled population via social engineering. A current example today is foreign governments influencing electoral processes for their gain. The ability to clearly, concisely and effectively communicate critical-thinking skills to the general population can be a game changer.

Q: What cyberthreat keeps you awake at night? How can it be addressed?

A: The intrusion into social media by criminal-minded actors is particularly troubling to me. We live in an era of unfettered access to inaccurate information and extreme viewpoints on all points of the political spectrum. This coordinated attack has been very effective at creating the very powerful emotions of fear, hate and anger. This is very dangerous from a societal perspective as we have turned on each other rather than working toward common goals. Social engineering specifically targets our emotions to create an intended response and action. I believe the fix is to reengage the teaching of critical-thinking skills and encourage people to remove the emotional reaction to information that is designed to specifically elicit an emotional response. Above all, you cannot protect information without protecting the very people who are targeted in the first place.

Q: What do you think are the most effective ways to address the skills gap in the cybersecurity workspace?

A: Information security, aside from what Hollywood tells us, is not a flashy occupation. We need to identify those who have an interest early and provide them with the opportunities for continuing education. I believe that this starts at the primary education level. My early interest in computers grew from my father who was an engineer and a strong proponent of developing my technology interest, to the point that I was learning the BASIC programming language in the third grade. However, not all children who have an interest in technology are given that same opportunity. Instead, we need to encourage teachers to identify those students with an interest early and allow the schools to develop that.

Occupation-focused education may prove to be more successful if applied correctly. As for current technology professionals, it may be up to the employers to address this. Often, we do not give the time or opportunity to our own staff to pursue continuing education. This means sending your people to paid training, giving them time during the workday to complete testing or studying. As others have said, if you give the time to your employees to sharpen their axe, their sharpened axe will help them be more productive.

Q: What do you see as the biggest risk factors being addressed effectively by cybersecurity professionals?

A: I believe we have done an excellent job with perimeter security and providing tools for professionals to identify security issues early. However, it is the application of these tools where we sometimes fall short.

Q: What was the most significant event or experience to date that has impacted the evolution of your career?

A: Switching from being a consumer of security services to being on the service delivery side has opened my eyes to how the consumer side gets it really wrong sometimes. The amount of disinformation, ineffective management decisions, lack of training within insular industries, and just a general malaise among consumers are disheartening. While I believed that I was fairly well educated as a security professional in financial services, it was not until working at a cybersecurity firm that I really began to understand what actually needed to be done. The amount of terrible marketing and disinformation spread by third-party vendors is, frankly, depressing. Consumers rely on their vendors to be forthcoming and honest about their risk when it is applied to their services delivered. However, I quickly learned about how much was actually simply being ignored or, in some cases, actively covered up by software providers. Security vendors are then left to explain these issues, often leading to distrust of the security vendor themselves.

Q: How do you keep your skills and your knowledge current?

A: I sit through a lot of product webinars and demos. I also read a lot of news and security-related websites. Teaching and presenting also help keep my skills sharp.

1 What is the biggest security challenge that will be faced in 2019? How should it be addressed?

Social engineering remains the top issue. We have to teach critical thinking skills to our friends.

2 What are your three goals for 2019?

- Continue to build out my critical-thinking skills and social engineering presentations
- Develop more cloud-based security initiatives for small and medium-sized businesses (SMBs)
- Continue to grow Redhawk Network Security

3 What industry-related sources (blogs, newsfeeds, etc.) do you read on a regular basis?

- *The Register*, *https://www.theregister.co.uk/security/*
- Reddit is a good aggregated source, *https://www.reddit.com/r/netsec/*
- *InformationWeek Dark Reading*, *https://www.darkreading.com/*

4 How do you keep your own information safe? That is, what do you do or not do to protect your own data privacy?

- Dual factor authentication on everything that supports it. I try to eschew those services that do not support it.
- Utilize sites such as *https://haveibeenpwned.com/* to track potential compromises to my data.
- Utilize password managers that generate strong random passwords that are protected by something I know and a second factor.
- My home network has pihole *(https://pi-hole.net/)* implemented.
- I have a stronger firewall at home that has next-generation firewall features.

5 What is your number-one piece of advice for other security professionals as they build their careers?

Never stop learning, use opportunities to educate as much as possible and do not try to master everything.

6 What is on your desk right now?

A notebook with scribbled notes for me to review. A Post-It pad for urgent things I need to pay attention to, a laptop, an old Fortigate firewall, several coffee cups.

7 What do you do when you are not at work?

I am a history buff, so I like to volunteer at my local museum. I am also a reasonably skilled mechanic, so I do my own work on my vehicles. I also enjoy hiking various trails in Central Oregon with my wife.