ITP 251 Team Project

LFCC Cyber Security Website

Oral Interview

Fall 2014

Interview Subject: Doug Shrirer: Information Security Officer LFCC

Interviewed by: Mike Haynes

Interview and Location: LFCC

Transcribed by: Donna Becker

Doug Shrirer, the Information Security officer at Lord Fairfax Community College. Among his duties are the protection of the computers and the computer network here at LFCC. This is a task that requires knowledge and know how.

Question: *So tell me Doug, where did you get your education and experience in information security?*

Answer*: I have a masters degree in computer science from Shenandoah University, I have several certificates from Microsoft Corporation on various operation systems and technology, I have about fifteen years teaching experience, as well as other certificates from other vendors and also a CISSP License that needs to be renewed every year. CISSP stands for Certified Information Systems Security Professional.*

Question: *The field of information security is ever expanding, and new graduates are entering the field every year though the demand continues to outweigh the supply. That said, is there any one security professional that you look up to within the field of information security? Why?*

Answer: *I don't think there was any one person that started me out on Information Security. My back ground here at the college started off as a faculty member teaching math courses and communication courses as well as some computer classes; from there I moved over to Administration and IT Technology support services department then went into information security. I do rely a lot on my colleagues*

throughout the state we talk frequently whether it be through list serve, or email, or in person there are a lot of conferences a lot of us go to all the time.

Question: What exactly is your job description here at LFCC?

Answer: *I kind of ran out of paper. I manage user account, that means create user account currently have about eight hundred of those. That means modifications as people change jobs their responsibilities change, they leave their position or new people come on so that is part of it. I also conduct a BIA that's a Business Impact Analysis as well as an RA or Risk Analysis that is an annual event. I interview thirty something department heads and staff members annually and we go through a very detailed list of all the applications and sensitive data they have and how it is protected.*

Question: Everyday can pose a new threat to the network, and those threats can come from external sources as well as internal sources. What can you do to mitigate the risks associated with these potential threats?

Answer: *I don't think anyone can mitigate one hundred percent all risk, there is some risk you have to accept. That is what a BIA – Impact Analysis does identify those risk some you can live with and some you can't the ones you can't I believe in the phosphia defense in depth where you have multiple layers like an onion where you slow people down and their access bad guys and hopefully one of those trick wires will send off an alert and we can catch them.*

Question: For students, faculty, and administration, access is granted by a username and a password. However, passwords can become an issue. Most of the time, a user will select a password that is weak making it susceptible to attack. What measures can you take to help negate this issue?

Answer: *For employees and systems that I directly manage we set up complexity rules what is called a GPL and Global Rule Policy. That requires they have a complex password and if they don't adhere to those rules than you cannot change your password, you cannot do anything.*

Question: *So when they select a password they have to run it through the system to see if authorized?*

Answer: *Correct.*

Question: *Does LFCC have a security policy detailing acceptable use policies and firewall policies?*

Answer: *Yes it does, there is one on the colleges website and the came from VCCS so we adopted as our own we also have that in a written from. You can also go out to the VCCS website to see as well.*

Question: *What processes do you use to handle incident response and disaster recovery?*

Answer: *Those have to be formal documents approved, they are detailed processes that accompany those standards their annually audited. That means I have to view them and also test them, they are not just table top exercises but we actually have to go through the processes. The auditors, state, and other agency do look at those as well. I have to verify with them with examples and screen shots to prove I followed the steps.*