# Transcript: IT Podcast - Ep 123 - C706 with Ronald Mendell\_default

*The following transcript is a verbatim account of the video or audio file accompanying this transcript.*

Speaker: Ronald Mendell

WGU's IT audio series, flexible, portable, profound.

Welcome to the podcast on C706, secure software development. I'm Ronald Mendell, your host. The theme of today's podcast, why bother with C706? I frequently have students ask me, why should I take this course? I'm really not interested in software or in doing information security and software. The purpose of this podcast today is to go over that issue and explain how the course is very important for any information security person to learn regarding how to best protect software. Regardless of the student's personal feelings or perceptions, an information security professional may find him or herself on a software project assigned by the management team. Their function there will be to ensure that the software is developed in a secure fashion and that there's appropriate controls in place to protect. It's important that an information security student understand the precepts for reasonably secure software. Those precepts include, what is the secure development life cycle? What is the software development life cycle and how do they differ? One enforces the business mandate for the software and that is the SDLC. But in addition to, let's say, creating a payroll program that properly generates the payroll that's meeting a business mandate, you also have to consider things like security, privacy, and compliance with regulatory requirements. That's what the SDL or the secure development life cycle involves. That is why there's a twofold focus in developing software. You want to make sure that the software is functional, that it accomplishes its business mission. But at the same time, you also want to make sure that it's reasonably secure. Other important precepts covered in the course include the importance of threat analysis. Threat analysis is universal throughout information security and the focus that's given to it in the software course really can improve your understanding of the topic as a whole. Taking the course could be very beneficial and increasing your ability to analyze potential threats and understand their possible impact and the extent of damage that they can cause if they are able to compromise your software. Also, of course, makes you aware of the role of testing in the various stages of development of the software. It points out how to identify vulnerabilities and how to develop appropriate countermeasures. Taking the course on software security aligns with the rest of information security. For example, the concept of separation of duties is very important when it comes to testing software. You don't want the same person to develop the software to do the security testing on it. That violates the doctrine or basic security principle of separation of duties.

Finally, software security aligns with the rest of the information security on such things as defense in depth in terms of protecting the perimeter of a network and least privilege. This privilege is a real key concept in software security. You don't want anyone to have access to different parts of the program without proper authorization. With these concepts in mind, I just want to leave you with the final note that taking the course on secure software development is very important. It's going to add extra items to your information security toolbox. We look forward to having you in the course and wish you well when you do take the course. Take care, this is Ronald Mendell signing off for WGU.

Schedule time with your instructor to explore more deeply. WGU, a new kind of you.