Read Chapter 17: Surviving Progress and Comment on key insights from the chapter.

Future Crimes book Chapter 17: Surviving Progress discusses various topics. First, it addresses concerns regarding bad software, its consequences, and software damages. Pertaining to these issues, the author explains how most software developers carry the mindset of trying to release their software in a timely manner while sacrificing the quality of their service. The result is what we continue to witness: exploitable vulnerabilities, zero-days, and the massive number of bugs that can often lead to breaches of users’ data. Unfortunately, Software companies are currently not liable for the damages incurred by those who use their software. These companies are not responsible for the damages that their products cause due to the terms of service agreement that users often breeze past, the first time they install the product.

The chapter also discusses the importance of secure passwords and encryption. That is, we have witnessed that passwords in the form of letters and numbers are no longer secure enough on their own to be used as a password. Hence, companies have been taking steps to increase security by requiring multiple forms of identification in addition to basic passwords. However, when it comes to these basic passwords, I also firmly believe that NIST’s latest password guidelines (passphrases) are something to consider with advancements in computation power to compromise passwords easily. Following this discussion, the author also emphasizes the idea of Encryption by Default to protect sensitive personal data on our mobile devices.

Furthermore, the author brings up the human factor, the weakest link in the information security chain. As a result, security awareness, technical education, and human-centered design to security are critical. This idea is becoming more and more relevant as we connect more and more devices to IoT. This criticality arises due to the fact that most security software is designed in a way that is not understandable to the general public. Many of the issues that these programs solve require the user to have a baseline knowledge of how to apply the software to their specific situation properly.

Lastly, the chapter indicates how much technology will play a part in digital criminal forensics. As a result, police officers and investigators, for example, need to be technologically savvy to follow the trail left behind by intruders. Plus, they must even be a bit creative in acquiring unaltered evidence considering that international jurisdiction laws sometimes prohibit law enforcement from accessing resources of another country.