Week 6: What are Company X's critical information and threats?

No unread replies.No replies.

As usual, "Company X" is an organization you have worked for and/or understand well enough to analyze. Give us sufficient information to understand what Company X does, but it is not necessary to identify the company.

According to "The Basics of Information Security", first steps in the operations security process involve identification of critical information and analysis of threats.

***Your assignment is to conduct both these actions for Company X.***

**Company X** is an organization that works in providing education, and it currently has approximately 1,500 employees. Of those 1,500, only 30 or so work in the information technology sector of the business. By serving not only students, but also employing teachers and staff, it is a clear target for attackers looking to steal a wide range of information from a single target.

Identification of critical information:

* Employees’ personal identifiable information such as social security numbers, addresses, etc.
* Students’ personal identifiable information such as social security numbers, health records, etc.
* Company bank accounts and payroll information
* Teachers’ coursework stored on company networks and company computers

Analysis of Threats:

I see the biggest threat vector here to be the possibility of a spear phishing attempt aimed at someone in the I.T. department who has significant role authority/permissions in the system. Having worked at “Company X”, I know just how much someone with just an administrative access can do on the entire system. If this were to happen, the attacker would be able to change the permissions roles for others and slow down any attempt at trying to stop them before extracting the information needed. We’re talking about a place that only implemented MFA after a high-level employee was phished and their bank account information stolen.

Another threat vector is the ability for any student worker or worker in the I.T. department to access any employees’ computer remotely without them knowing, including teachers. The way the company had their networks set up, all it took was knowing the computer name, and you can type /$(PC name here) in the run menu on windows or use Remote Desktop on macOS. While the User Support Services places trust in their students to not do anything nefarious, the ability to backdoor into computers on the network is a GIGANTIC red flag that should be addressed.

Lastly, the use of a local admin account on all company computers, with a password that was widely shared throughout the I.T. department is another huge threat. Under no circumstances, should there ever be a local admin account on computers connected to a company network. This gives an attacker a huge window of possibilities to exploit if they were to gain knowledge of that local admin password. I would recommend only having profiles that are connected online, and restrict any set up of local admin accounts.