To start, if you can rebuild I.T., do it.

Before we talk about some Boring Solutions that can improve your security posture, I do have one not-boring thing that I think people need to hear. Everything reaches a point where it is more costly to address the maintenance debt in a high friction environment, then it is to burn it all to the ground and rebuild. So, if you have the opportunity (and of course management and peer buy-in) to burn it all to the ground and rebuild programmatically - **PLAN IT, TEST IT, DO IT!**

20 Critical Security Controls
(these are the first 10 we'll talk about today)

CSC 1: Inventory and Control of Hardware Assets
CSC 2: Inventory and Control of Software Assets
CSC 3: Continuous Vulnerability Management
CSC 4: Controlled Use of Administrative Privileges
CSC 5: Secure Configuration for Hardware and Software on Mobile
          Devices, Laptops, Workstations and Servers
CSC 6: Maintenance, Monitoring and Analysis of Audit Logs
CSC 7: Email and Web Browser Protections
CSC 8: Malware Defenses
CSC 9: Limitation and Control of Network Ports, Protocols, and
          Services
CSC 10: Data Recovery Capabilities

CIS Controls™
http://www.cisecurity.org/controls/
V7