How can we quickly recover?

CSC 10: Data Recovery Capabilities

Data Recovery Capabilities **The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.**	
Ensure Regular Automated BackUps	Ensure that all system data is automatically backed up on a regular basis.
Perform Complete System Backups	Ensure that all of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.
Test Data on Backup Media	
Protect Backups	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.
Ensure All Backups Have at Least One Offline Backup Destination	Ensure that all backups have at least one offline (i.e., not accessible via a network connection) backup destination.

http://www.cisecurity.org/controls/

What Boring Solutions we discussed today.

Focused on Implementing Critical Security Controls 1-10

We started with knowing what is in our environment, progressed to discover what it is installed, how it is configured, and what it is doing.

We then looked at the unique challenges of protecting email and browsers, we explored malware defenses, profiling the data flow and ports used by systems, and looked at recovery methods.