CORPORATE COST CONTROL

Data Security Special Bulletin

On September 7, 2017, Equifax announced a data breach that impacted 143 million people. The following week, they announced the source of the security breach: An unpatched server running compromised software. Although a patch had been issued for this flaw, it appears that patch was not applied timely.

Many of our clients are understandably seeking assurances that Corporate Cost Control is not affected by this vulnerability, and more importantly, what we are doing to prevent a similar problem. Although the vulnerability was in a software framework not utilized by CCC, the true, underlying issue in this breach appears to be a failure to follow best practices.

CCC has a well-established, repeatable, and auditable process for managing software patches. CCC maintains a complete inventory of our servers, which allows us to ensure that all are patched timely. We have a dedicated environment for testing purposes. When a patch is released – either as part of Microsoft's regular update cycle, or for "zero day" vulnerabilities – the patch is applied to our testing environment first, on the day of release, to ensure that it creates no other issues.

Once we've established there are no issues, the patches are immediately applied to all production servers. As defined in our security policy, this task is the responsibility of our System Administrator, who works closely with development and IT management to ensure patches and updates are applied timely.

There are other factors that we believe enhance our security posture. Corporate Cost Control's systems have all been developed internally over the past eight years. C3, Hamlet and CCC Verify – our core applications – are bespoke systems developed by CCC personnel and hosted on hardware that we have configured and that we maintain.

CCC's servers, database and applications are built entirely on the Microsoft stack. By keeping our environment homogeneous, we significantly limit the number of operating systems and libraries that we need to monitor and, more importantly, we limit the number of vulnerabilities that our systems may be exposed to.

Finally, unlike other companies in our industry, CCC has largely grown organically. While we have made a few smaller acquisitions, our first step after each acquisition has been to evaluate the acquired systems and ensure they are properly patched. As soon as possible, we replace those systems. This is a top priority with any acquisition, as it allows us to be certain the systems running within our network are properly secured.

The steps outlined above protect us against the specific attack vectors involved in the Equifax breach. Some of the additional steps we take to protect data are:

- An annual web vulnerability scan of all CCC systems;
- Annual SOC audits;
- Continuous intrusion detection monitoring;
- Centrally-monitored antivirus and malware protection on all company IT assets;
- Annual disaster recovery testing.

The Equifax data breach has served to remind everyone at CCC that security can never be taken for granted. If you have any questions or concerns at all, I am happy to discuss them. Please feel free to contact me at dtienes@corporatecostcontrol.com. And as always, we appreciate the trust you place in us, and we take our responsibility to preserve that trust very seriously.

Respectfully,
Dan Tienes
Chief Technology Officer
Toll Free 800-207-6926 ext. 411