Shelby County Treasurer - Erica Firnhaber

From: David Woods <dwoods@mytecsol.com>
Sent: Thursday, June 8, 2023 1:50 PM
To: Shelby County Board Chair - Bobby Orman
Cc: Shelby County Board - Vice Chair - Mark Bennett; Shelby County District 1-1 - Tim Brown; district1-2@shelbycounty-il.gov; Shelby County District 2 - Clay Hardy; district3-1@shelbycounty-il.gov; Shelby County District 3 - Tad Mayhall; cdavis82882 @yahoo.com; Matt Kessler; distrcict5-1@shelbycounty-il.gov; bewallace67@gmail.com; Shelby County District 6 - Heath McCormick; State1947@hotmail.com; Shelby County District 7 - Sonny Ross; district8-1@shelbycounty-il.gov; Shelby County District 8 - Jeremy Williams; Shelby County District 9 - Cody Brands; district9-2@shelbycounty-il.gov; Shelby County District 10 - Martha Firnhaber; district10-2@shelbycounty-il.gov; district11-1@shelbycounty-il.gov; Shelby County District 11 - Julie Edwards; Shelby County Clerk - Jessica Fox; Shelby County Treasurer - Erica Firnhaber; Supervisor of Assessments - Debbie Dunaway; Shelby County Probation - Heather Wade; Shelby County Public Defender; Circuit Clerk - Kari Kingston; States Attorney; Sheriff Brian McReynolds; Charles Baker; Shelby EMA; Shelby County Zoning
Subject: Managed Services & Cyber Security

This sender is trusted.

Good afternoon,

This email is being sent to all department heads and county board members. Please reply to all (if you choose to) when responding so all communications can be transparent.

Most of you know who I am. Have talked with several of you since you took office and feel that you all need to know the situation myself as a company and the county is being put in.

This email may cost me my contract with the county but if that happens just know that what I am doing is what I was hired to do. Protect the county network infrastructure and taxpayer information that resides on that infrastructure. Also note that we have done that successfully for over 23 years without a single breach or outage.

I know there are probably other items that may be more important than this but that is up to you as a board to decide. We have talked with several individuals about this over the past 6 months and tried to resolve this as quietly as possible but that does not appear to be working. Promised multiple times by multiple people that it would be addressed but nothing has happened and it is time for a resolution.

I received the following email last night at 10:29 pm from Judge Ade-Harlow.
It is addressed to the following:
Chief Judge Douglas Jarman judgejarman@fourthcircuitil.com
Associate Judge Allan Lolie judgelolie@fourthcircuitil.com
Board Chairman Shelby County District 7 - Robert Orman district7-1@shelbycounty-il.gov
Sheriff Brian McReynolds sc545@scso87.org
States Attorney Robert T Hanlon statesattorney@shelbycounty-il.gov

Mr. Woods:

Today, I found that you have placed software on judicial use only computers including but not limited to remote access and monitoring software and Webroot Business. These computers include the bench computers in Courtroom A and Courtroom B, judge's chambers computers in Chambers A and Chambers B, and the Lenovo laptop that was used for Zoom in Courtroom B, which is also used as a judicial laptop (my first laptop as a judge in 2016).

I have never given you permission to access any judicial use computer - in person or remotely. I have never given you permission to place any kind of software on any of these computers. I have never given you permission to remotely monitor the business of the judges. In fact, I have refused your program installations since 2015 when I was the Shelby County Public Defender.

I am in the process of uninstalling the three programs that are clear to me that you have installed - Webroot and the remote access and monitoring program (2 downloaded software components - Splashtop and Splashtop-Streamer). I'm not sure if you or your employee(s) also installed Sophos but that has been uninstalled as well. If there are additional programs that you have placed on any of these computers that I have not indicated, I need to know the names immediately so I can remove it all.

Judicial computers are for judges. You and your employees are not judges. You (and/or your employee(s)) installed at least one program on the Courtroom A bench computer sometime after the close of business hours on 6/6/2023 and this morning at approximately 8:15 am or at least it was not apparent of the installation until this morning.

You (or your employee(s)) have also entered Chamber A & B without permission and those doors are locked after business hours. Chambers B is locked even during business hours when no judge is using it.

To be clear, you nor anyone else who is not a judge or has a judge's specific permission are allowed in judge's chambers or on any judicial use computer or technology previously in use, currently in use, or may be installed and used in the future. This includes the court technology upgrades to be installed later this year. You and anyone else in your company, regardless of title, are prohibited from installing, in any manner, anything on all judicial use computers and technology without specific permission from the appropriate judicial authority. If permission is granted, the installation will be done in person and monitored by me during the entire process.

Please advise immediately of any programs installed at any time by you or your employee(s) at any time on any judicial use computer or technology.

Amanda S. Ade-Harlow
Circuit Judge, Shelby County
Fourth Judicial Circuit, Illinois
301 E. Main St., Shelbyville, IL 62565
(217) 774-4212

This is my reply sent to the same people listed previously.

Judge Harlow,

We are under contract and have been for over twenty years with Shelby County to protect the computer systems and network devices within the courthouse and sheriff's offices from nefarious bad actors that are constantly attempting to gain access to any data that it can get its hands on and then hold it for ransom until the entity pays multi millions of

dollars to get the recovery key. That is further clarified within the Cyber Security Insurance policy that the county now has in place. As you are aware, there are several counties around us that have been affected with that exact scenario and several months later still have not recovered all of their data and may never get it 100% recovered.

To insure that does not happen on any system it requires the following:

1. Keeping the computers updated with the latest Microsoft security patches, service packs and anti-virus software.
2. User permissions and passwords set correctly on those systems to restrict access from unauthorized users.
3. Correct operating system is being used for the work environment.
4. Workstation backups performed daily to prevent loss of data and those backups replicated offsite in case of major disaster.

The software that you are referring to was installed on those computers by us at the direction of the county board chairman per our signed contract with the county board. What concerns me now is that you state you are in charge of those systems. Our software has been installed on those systems for months and you are just now realizing that it is there. So much for maintaining the security of those systems.

1. Crtrm-A-Bench was installed on 6/25/2022
2. Crtrm-B-Bench was installed on 6/16/2022
3. Crtrm-B-Yoga was installed on 6/25/22

Myself or none of my employees have ever stepped foot in the judge's chambers to work on computers nor do we have access remotely to them since they are not properly configured for use on the network. The doors are always locked and we do not have keys to those offices.

You stated that software was installed at 8:15 - that would indicate that our software is doing its job in protecting the system and updating itself.

One thing we need to make perfectly clear. We do not monitor anything that is happening on those systems as far as what the judges are doing. We monitor the hardware and software to make sure it is kept up to date and secure. We do not have access to the files that are in the Gems system as we do not have a username and password to access that data. Part of that monitoring solution installs a secure remote access software on the system so when there is a problem we have access to the system and we can repair it. When that happens, we use our own login information not the end-users. That login information does not give us access to any other users information that might be on the system.

We have spoken with Jeff and Kurt at Goodin' and Associates several times over the last 20 years about the services that we are providing and they are in full agreement with what we are doing, it is necessary in today's hostile environment and have actually recommended our services to other companies.

The Illinois Department of Information Technology (DoIT) has audited the county on several occasions and they are also in full agreement with what we provide and stated that the county is very well protected and in good hands. They have written letters of recommendation for us - ask Jessica in the Clerk's office.

Judge Lolie, Judge Kiley, Judge Bennett and every other judge that has been in this courthouse since we have been providing service was not involved in telling us how to do our jobs. We are the networking and security experts and they relied on us to do our jobs. You are preventing us from doing that and in doing so you are exposing the taxpayers of the county to a potential multi-million dollar ransomware attack, voiding the county cyber insurance policy and potentially exposing taxpayer data to hackers worldwide.

We no longer have the logs to prove this but I can assure you that when you were the public defender our management software and antivirus software was installed on every workstation in that office.

The new systems that you purchased and installed have "Home edition" software installed on them instead of "Pro Edition" of the software. Home edition has multiple security vulnerabilities that cannot be patched or properly protected.
The new systems that you purchased and installed are not properly connected to the courthouse network so they are not being backed up as they should be to prevent data loss.

We have removed the following systems from our managed services portal and removed our antivirus software from them:

1. Courtroom A Bench
2. Courtroom B Bench
3. Courtroom B Yoga
4. Law Library

Having done this when the county signed the Cyber Insurance policy we had to fill out a several page questionnaire regarding the setup and configuration of the computer systems and sign an affidavit that the county was in compliance with all of the requirements as set forth in that policy. Those devices are still connected to the network and do not have the approved software installed on them That being the case, we will be notifying the carrier that the network is no longer in compliance. It will be up to them on how to proceed with their coverage.

You are not a county employee and we can find nothing that gives you the authority to override the county board with respect to the computer equipment. We do not feel that we need your permission to install any software on the computer systems in the courtroom or chambers. Those computers were paid for with taxpayer money, owned by the taxpayers of the county and controlled by the county board thru the circuit clerk's office.

You are employed by the State of Illinois and the county is required to provide you with the equipment to do your job when you are here as a judge. That job is to hear cased presented to you in the courtroom and interpret the law as it applies to that case. In order to prevent a conflict of interest you are not to be involved in the day to day workings of the courthouse or any other department within the courthouse.

All that being said, we have removed the software from those systems and will let others decide how they want to proceed from here.

We are available to discuss this issue and others whenever and wherever a time and place can be arranged.

Thank you all for your time.

Thanks

Mytec Solutions, Inc.
David Woods
P.O. Box 178
502 N Cedar, Suite A
Shelbyville, IL. 62565
(217) 774-2525 ext. 1 Phone
(217) 827-0714 Cell
dwoods@mytecsol.com