AOC ASSOCIATION OF OREGON COUNTIES

February 15, 2023

Joint Legislative Committee on Information Management and Technology

Co-Chair Woods
Co-Chair Nathanson
Senator Taylor
Senator Thatcher
Representative Hartman
Representative Mannix

Thank you for this opportunity to address you this afternoon about the cybersecurity threat facing Oregon. For the record, I am Tillamook County Commissioner David Yamamoto while also the County Commissioner representative to OBAC (Oregon Broadband Advisory Council) and Co-Chair of AOC's Governance, Revenue and Veterans Steering Committee.

My testimony today may be unlike previous testimony you have heard since I was subject to the horrors of a ransomware attack on Tillamook County a few short years ago and I would like you to understand the issues involved in these attacks.

Over the Martin Luther King Junior holiday weekend of 2020, Tillamook County was hit with a cyber-attack. When I entered the Courthouse that first morning, our IS Department staff were busy unplugging every bit of equipment we had. Yet, by the time we determined that we were hit, most of our servers had been encrypted, many with multiple layers of encryption. Our backups had also been compromised and were unusable as restore issues, including our off-site backup repository. Per our insurance procedures, we were provided a breach coach who arranged for an outside company to come onsite and provide recovery and remediation support.

Due to the backup failures, we had no choice but to pay the ransom of over $300K to recover our data. The county was completely offline for about 2 weeks while we cleaned and scanned all servers and desktops, ran decryption tools repeatedly on every machine to help identify and stop any further malicious activity. It took about 2 more weeks before our network was generally back to normal operation, and months to get back to full operation. Although we had Office 365 for cloud-based email, a day or two after the initial attack, we started to see inbound email sharply drop off and completely stop after 3 days.

All administrative accounts had their passwords reset early in the recovery, and 2 accounts, the administrator who identified the attack when logging in with their account and a new account that was created by the attacker, were disabled and flagged for deletion. When we brought accounts back online, we forced password changes just to be safe in case any passwords had been compromised. All removable storage (USB drives, external hard drives, etc.) were pulled out of service and quarantined. The company who assisted with recovery and forensics was unable to identify how we were infiltrated, though 2 likely causes were identified, a web server and a VPN tool.

One of the interesting things that we found was that the team that hit us was extremely professional (malicious intentions aside) and had better customer service than most legitimate vendors that we work with. As we found new encryption keys, they were prompt to respond with the proper decryption tools once we had paid them. To them, this is a business and if recovery goes awry, future ransomware victims might be reluctant to pay.

Post-incident, we migrated to a new server farm for our infrastructure. We recently made another change to a backup system that stores backup copies on 3 servers in 2 locations, as well as a backup in the cloud that can't be overwritten to ensure that we have viable backups in the event of attack or disaster. We changed to a different VPN protocol that also included multi-factor-authentication to make it much harder to be compromised. We removed the web server from the domain, and as part of a project that had already been planned, moved most of our web services to a hosted solution, which provided additional protection from this type of attack.

We moved to a hosted DNS solution to ensure that cloud services including email would not be disrupted if our internal network is impacted. As we move to more cloud-based services, this will increase the reliability of operations during cyber-attacks and other disaster scenarios that may impact our local servers and with the hosted web services we will be better able to keep the public informed of issues. We have regular vulnerability scans of our network to identify issues and work to address problems as they are detected.

There are several projects that we are working on to further protect us. One is obtaining hardware tokens for all employees to provide a form of multi-factor authentication that can't be bypassed by cell phone hacking or cloning. Another is to identify a tool to help us detect malicious activity including data exfiltration. We are working on getting penetration testing conducted to build on the vulnerability scanning to help develop a more robust plan to harden the network. We also plan to work with our insurance provider to develop a cyber response playbook to guide our course of action and eventually a runbook of scripts and tools to run as we work through the playbook to enable faster response and more efficient use of staff time, which we now know is critical.

As you can see, not only did Tillamook County pay a large ransom to regain access to our own systems, we have spent hundreds of thousands of dollars to upgrade our systems to prevent this from happening again. Please understand that county services were shut down for 2 weeks while all data services were offline.

I need to point out another problem and that is the issue of public records requests that would require us to provide information about the security systems we have in place to protect ourselves. Please support HB 2806 which would provide executive privilege relating to security infrastructure and responses to cyber security threats.

Over time we've learned that holiday weekends are prime opportunities for malicious actors because they have a longer window of opportunity when they're likely to act undetected. A few months ago, we received a letter from the US Department of Justice that the group that attacked us, called REvil, was vacationing in Eastern Europe and 2 of the leaders were arrested and subsequently extradited to the United States where they remain in prison. We were, however, told not to expect any reimbursement since our money had long been spent in Russia where they were based.

Although we're in great shape to survive the type of attack that we were hit with in 2020, we also are aware that things have changed, and the greater threat is that they will steal data before encrypting it and even if we can restore everything from a backup, they can demand a ransom to not leak our data online. This type of ever evolving threat is something that we need to make everyone in the State aware of and offer every evolving solutions to protect our citizens. Unlike many other State, County and other local governments, Tillamook County has been open to assisting any other entities that have questions about how we dealt with our cyber-attack to try to educate and assist in prevention or recovery.

There is a little more of this story to relay to you. Within a couple of months of our disaster, Oregon was hit by the pandemic and we found ourselves spending tens of thousands of dollars to equip our critical employees with laptops so they could perform necessary functions from home. While the Courthouse was closed to the public for months, the Commissioners as well as many department heads continued to perform duties in the Courthouse. The security systems needed for our remote workers was an additional, but necessary, piece of protecting our systems from employees working from less secure areas outside of the Courthouse.

Respectfully submitted,

David Yamamoto