

May 16, 2019

The Honorable Ron Wyden United States Senate 221 Dirksen Senate Office Building Washington, DC 20510

Dear Senator Wyden:

This letter is in response to your correspondence dated May 8, 2019. We are pleased to clarify the facts regarding the assertions and questions from your letter.

BACKGROUND ON VR SYSTEMS

VR Systems is a national leader in voter registration software, elections management and electronic pollbooks. Our employee-owned company is headquartered in Tallahassee, Florida, and has worked for over 25 years to develop best in-class products for customers throughout the country. We are proud of our employees, products and security systems. It's important to understand that our product, EVID, is not a vote tallying system. It is a front-end system used to check voters in at the polls and to provide information such as a voter's polling location when they search for it. VR Systems takes its responsibility for elections security seriously. We use best-in-class security systems and protocols, and train not only our staff, but the employees and leaders in elections offices throughout the country in security protocols.

SPEAR PHISHING EMAILS

Like virtually all companies and individuals, we receive spear phishing attempts from time to time and we have security protocols and systems in place to repel them. Our employees are trained to look for phony emails and to be human firewalls. In August 2016, elections officials in Florida, including representatives from our company, were asked to participate in a conference call with law enforcement. On that call, the FBI asked everyone to be on the lookout for certain suspicious IP addresses that might be visiting our websites and they followed up with a Flash Bulletin. We checked our security logs and found that several of the IP addresses had, in fact, visited our website. We notified the FBI as we had been directed to do. At around the same time, our systems quarantined a spoof email that claimed to be from Google, which provides our company with email storage. The email stated that we were out of storage space and advised the intended recipients to click on a link to buy more space. A total of five of these emails came into the company and were quarantined, and an additional two emails bounced because the addresses were incorrect. One of our employees reviewed the quarantined email, and alerted our employee responsible for the gmail system, who advised that this was fraudulent. At no time did anyone from VR Systems click on an attachment in the email. No VR Systems employee email account was compromised and there was no penetration into our system.

We did not know until June of 2017 when the NSA report was leaked that this attempt was part of a larger effort. We did contact the FBI once we learned about the information in the leaked report.

It is my belief that the bad actors were trying to steal network credentials that would have enabled them to send an email from our actual system. Because they were not successful, the cyber actors, as part of their

late October spear phishing attack, resorted to creating an obviously fake gmail account to use in that spear phishing attempt (vrelections@gmail.com).

On November 1, 2016 VR Systems learned from one of our customers of a spear phishing email purported to come from VR Systems that had been sent to elections officials. We were sent a screenshot of the email at 9:24 AM on Nov. 1 and by 10:14 AM, we sent an email to our customers alerting them and telling them not to open the email if they received it. We also called our customers and delivered the same message. We immediately contacted law enforcement in accordance with standard protocol, and they responded.

We were in contact with our customers and each of them told us that they had either not received the email, that it had gone into SPAM or been quarantined by their security systems. No one indicated to us that they had opened the email. We did not hear anything more about this potential threat until we were contacted by a journalist after the NSA document was leaked in June 2017.

REVIEW I

Immediately after learning of the NSA document alleging a breach, we engaged a leading global cyber security firm, to consult, test and monitor VR's systems and servers and they conducted a forensic audit. The results confirmed we were not breached as a result of the spear phishing attempts as had been reported in the leaked NSA document.

REVIEW II

In addition to this private sector review, VR Systems has participated in numerous cyber security programs with the Department of Homeland Security (DHS). The National Cybersecurity Assessments and Technical Services (NCATS) review started in September of 2016 and continues to this day. This includes real-time cyber hygiene testing for web facing networks and systems. In 2017, VR Systems participated in a risk and vulnerability assessment through DHS and was the first elections vendor to complete this assessment. Most recently, DHS led a proactive "hunt" at VR Systems. This cybersecurity and technical analysis of VR's systems spanned two weeks in the summer of 2018 at our headquarters, and was conducted by specially trained forensic cybersecurity experts working on behalf of DHS.

In an executive summary of the review, DHS stated the following: "Over the course of the engagement, and using the available in-scope data, [DHS] did not identify any malicious activity. VR has historically demonstrated continual improvement toward following security best practices, as shown by their use of two-factor authentication for email, their implementation of FireEye HX, their move of systems to the cloud, and their upgrading of servers and workstations to current, patched OSs."

The DHS executive summary makes reference to the series of measures VR has enacted since 2017 as part of its comprehensive cybersecurity program, including:

- Engaging a leading global cybersecurity firm to provide consulting, testing and monitoring of VR's systems and servers;
- Undertaking email specific security protocols, including implementing company-wide, two-factor authentication and Human Firewall training for employees and customers;
- Becoming the first elections vendor to complete a Risk Vulnerability Assessment (RVA) by DHS earlier this year;
- Utilization of secure cloud systems including Amazon Web Services (AWS);
- Offering expanded security products to customers seeking data integrity solutions; and

• Providing customers with media training to help them effectively communicate with the public in the event the integrity of an election is questioned.

Therefore, based on our internal review, a private sector cyber security expert forensic review, and the DHS review, we are confident that there was never an intrusion in our EViD servers or network.

However, we know that no system is ever completely secure and we work tirelessly every day to protect our systems and our customers and remain ever vigilant to protect our network and systems.

I hope that this background is helpful to your understanding of the history of our involvement in this spear phishing attempt. When the cyber actors impersonated VR Systems in emails to elections officials using the obviously fake email address vrelections@gmail.com, it set off a chain of events that is both frustrating and time-consuming for our company to address.

Answers to Questions

- Q1. The North Carolina Board of Elections has stated publicly that it "lacks the necessary technical experience to forensically analyze the computers used in Durham County, and other government agencies declined the agency's requests to evaluate them." Were the VR Systems electronic poll books that failed in Durham County on November 6, 3018 forensically examined for evidence of hackers by cybersecurity experts working for any government agency? If yes, please provide a copy of all reports or assessments shared with your company after the forensic examination of these devices.
- A: VR Systems offered to pay for a forensic analysis to be conducted by the state or its selected vendor, but the state never responded to our offer and instead quarantined the machines in order to do their own analysis. To our knowledge, the state has not conducted that analysis. Durham County brought in a private security firm (Protus3) immediately after the election to conduct an independent analysis. Their report is attached and their findings are logical and, we believe, accurate. We have also attached our attorney's letter which provides a more detailed explanation of our position.
- Q2. Your company asserted in a March 2018 court filing that you had not yet experienced a breach of security. What was the evidentiary basis for this unqualified assertion?
- A: Please see above for a complete response.
- Q3. Have your corporate computer networks and systems been subjected to a forensic examination to determine the scale and impact of the hack by the Russian government described in the Mueller Report? If no, please explain why. If yes, please provide me with all post-breach analysis, including reports created by private cybersecurity companies and government agencies.
- A: Please see above for a detailed response. These reports go into a level of detail that make them business sensitive and for this reason we will not be able to release them as requested. We must protect this information on behalf of our customers in the elections space.
- Q4. On August 1, 2016, did you employ a Chief Information Security Officer, or any other individual with sufficient cybersecurity experience and skills, who was responsible for protecting your systems from hackers? If no, do you employ someone in such a role today?
- A: We employ a team of highly skilled employees who have sufficient cybersecurity experience and skills. Our COO, Ben Martin also has the responsibilities usually associated with a Chief Information Security Officer.

Q5. On August 1, 2016, had you implemented the National Institute of Standards and Technology (NIST) cybersecurity framework? If no, have you now implemented the NIST framework?

A: Yes, we have been following the guidelines of the NIST cybersecurity framework prior to August 1, 2016 and continue to do so today.

Thank you for the opportunity to provide you with this background. If you have any additional questions, please contact me at the address below.

Sincerely,

Mindy J. Perkins, CEO

VR Systems, Inc.