Viewpoint Blog

When the Unthinkable Happens: Contractor Shares Lessons Learned from a Ransomware Attack

5 Questions with E.R. Snell's Justin Snell on how his company addressed a data security breach and why it modernized to protect the business

Some 68% of construction companies have only minimal, or even no construction cybersecurity measures in place.

Recent reports have shown that the construction industry is among the most targeted for ransomware attacks. In fact, contractors of all types and sizes are among the leading businesses impacted by targeted data and cybersecurity threats like phishing scams, malware, wire and electronic fraud, and more. Given that the average cost of a data breach in the United States is around $9 million, doing business without the proper technology and data protections in place can be a risky venture.

Although large companies that generate more revenue tend to attract more hackers, small companies are also appealing to hackers because they usually do not have the most modern technologies or robust construction cybersecurity protocols in place. According to a 2021 GlobalData survey, more than half of all construction executives believe their firms will be hit in the

future, yet 68% of firms have no security measures in place, or minimal security.

Read More:

Why It’s Important to Have a Sound Construction Cybersecurity Strategy

E.R. Snell's vice president of technology, Justin Snell, shares his company's own story and how it took proactive measures to prevent future attacks.

E.R. Snell Contractor, Inc. is a premier contractor for road and bridge construction, with a focus on concrete and asphalt construction of roads, bridges, and culverts. In 2020, before moving to the cloud, it was the target of a ransomware attack.

E.R. Snell’s vice president of technology, Justin Snell, recently spoke with Trimble Viewpoint to share the company’s story about the attack for the benefit of other contractors, and the changes made to protect against cyber risks. Here is a segment of that discussion:

Trimble Viewpoint: How did you discover E.R. Snell was the victim of a ransomware attack?

A ransomware attack that took place over a holiday weekend prompted an emergency repsonse by the E.R. Snell team.

Snell: During the Labor Day weekend, we started receiving alerts that our antivirus software had been disabled so we immediately went into the office to determine what was going on. Upon closer inspection, we realized that all of our files were being encrypted and our servers had been hacked. The next morning, I was on the phone with the FBI to report the incident.

At the time of the attack, only 10% of our data was hosted in the cloud with the majority of data hosted on-premise. Luckily, both our cloud and on-prem servers were backed up daily so that we could access our data in case of an emergency. However, the hackers had deleted almost all of the cloud backups, likely to provide even more leverage for us to pay the ransom.

The hackers got in via an employee's email account and had placed a key-logger on the on-prem mail server to gain administrative access. Through the chat service, they then demanded a ransomware payment through bitcoin.

Trimble Viewpoint: What steps did you take when you discovered your servers were compromised?

E.R. Snell moved to the cloud with Trimble Construction One to take advantage of more robust construction cybersecurity protections.

Snell: In the first 24 hours we hired an incident response team and attorney. Fortunately, we had cybersecurity insurance, so we were able to quickly file a claim. We then engaged Trimble Viewpoint to help move our Vista ERP to the cloud and to the connected Trimble Construction One suite of solutions. They jumped into action immediately, helping to move our data and getting everything set up so we could continue to work. All of our critical services were back up within a week.

We also set up multi-factor authentication on all critical accounts, including email. During these processes, the backups being held for ransom were recovered so we were able to ignore the ransom demands.

Watch the Video

Learn about E.R. Snell's Cybersecurity Breach and Why It Modernized Operations

Trimble Viewpoint: How did the ransomware attack disrupt your operations?

Snell: With the lack of available software, multiple departments had to utilize manual processes, which required extra time and resources. Throughout the three weeks of triage, we paid out insurance and betterment fees, hired an outside accounting firm to rebuild five months of data and hired an outside IT firm to rebuild more than 200 computers.

From beginning to end, it took three months to completely rebuild all of our missing data.

Trimble Viewpoint: Have you made any changes to your operations since the ransomware attack?

Snell: We've made several companywide adjustments. One of the biggest changes was moving 80% of our systems to the cloud. In hindsight, it's something I wish we had done sooner.

Trusting our data to Trimble Viewpoint's Vista in the cloud is an insurance policy in itself and mitigates a lot of risk. We now have peace of mind knowing that our data is more secure in the cloud with encrypted, user-level permission controls, multi-factor authentication and single sign-on.

Trimble Viewpoint: What advice would you give other contractors who may not have the right technology and processes in place to minimize the risk of a ransomware attack?

Snell says one of the best things contractors can do-aside from modernizing-is to have robust construction cybersecurity and disaster recovery plans in place.

Snell: Technology evolves so fast. You have to not only stay ahead of the competition, but stay ahead of threat actors. If anything, this was a sobering experience of understanding the threats, which are growing more severe by the day.

In addition to moving to the cloud, create a written disaster recovery plan and regularly review and test it. We conduct an annual in-depth review of our plan and run monthly and quarterly reviews and DR tests where we simulate all of our servers going down and restoring the backups.

Education is also key. Everyone in your company should be aware of the importance of data security and be on the lookout for threats when they open every email, visit every website and perform any action on their computing devices. Host training sessions and show employees exactly what they should look for to prevent an attack.

All high-security logins should require employees to verify their identities in more than one way with multi-factor authentication. Employees should use an entire phrase when creating a password and include spaces between a minimum of four words. Adding in characters, numbers and case-sensitive words will make it even more complicated and thus harder to crack.

Looking back at why we were targeted, it makes perfect sense that a construction company may not have the best security protocols in place but today, we do.

How to Protect Your Construction Business from Ransomware

Is your company equipped with the right technology solutions to connect and protect your business and workflows when an attack occurs?

Trimble Viewpoint can help you modernize your operations and future-proof your organization by leveraging a cloud,-connected construction and business management suite of solutions, and a commitment to best-in-class data security. Reach out andconnect with us today to learn more.

Posted By

Andy Holtmann

Andy is Marketing Content & PR Manager at Viewpoint. He has worked in the construction software arena since 2011. Previously, he netted multiple awards as a newspaper and trade media editor.