NetCov

Case Study: Construction Management Company Faces Ransomware Attack

Services:

- Emergency Network Security Services
- Virus Eradication
- Data Recovery & Restoration
- Network Security
- Data Backup & Recovery

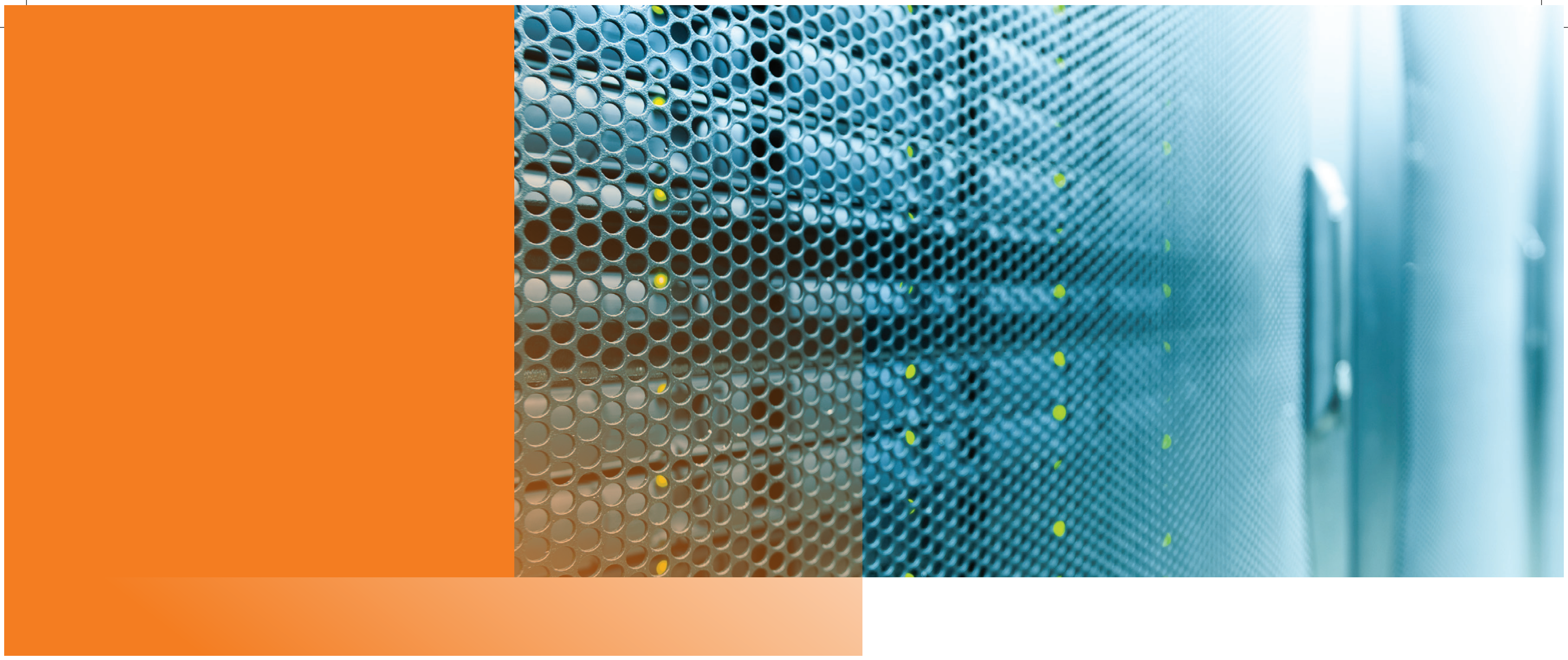
A construction management company hired Network Coverage to recover from a devastating ransomware attack that resulted in over $160,000 of financial losses and 10 days without full operations. Network Coverage eradicated the ransomware virus and recovered and restored data and operations within 24 hours.

Situation: Ransomware Attack

A construction management company suffered a devastating ransomware attack infecting their backups and internal work stations, paralyzing the company's ability to function at capacity and leaving 30 employees unable to work for 10 days while having their data held for ransom.

The company's existing network security and data backup/disaster recovery provider did not have the safety measures in place to prevent the attack. In addition, while the company was under the impression their data was being backed up regularly and securely in multiple locations, this was not actually the case. The attack resulted in over $100,000 in lost productivity and business as well as $60,000 in bitcoin ransom to restore their data.

The construction management company sought the help of Network Coverage during the attack when their previous network security and data backup/disaster recovery provider was unable to remove the infection or restore data.



Approach: Eradicate, Restore, & Prevent

Network Coverage went in immediately to take action against the ransomware attack. Network Coverage first worked to remove the infection from the network. With all on-site backups compromised and no off-site backups in place, the company was forced to pay $60,000 in bitcoin ransom to restore their data. Network Coverage facilitated recovery, regaining access to the data, and encrypting and restoring the data for increased protection in the future.

Network Coverage was able to help the company resolve the infection, restore data, and get back up and running at full capacity within 24 hours.

After recovery was complete, Network Coverage assumed control of the security ecosystem, putting more secure protections in place and establishing a reliable backup and disaster recovery strategy. In the future, should such an attack occur, the construction management company with the network security and data backup/disaster recovery services of Network Coverage, is equipped to restore data and operations within one hour or less.

1. Remove ransomware infection from internal workstations and backups
2. Analyze existing data and backups to determine level of loss and how to proceed
3. Facilitate data retrieval from attackers
4. Encrypt and restore data
5. Implement detailed security measures to prevent future attacks
6. Designed and implemented a thorough, automated, and secure data backup strategy that provides regular backups in multiple secure locations (backups are continuously monitored and tested for reliability and recency)
7. Provided impactful employee education to improve internal security measures and avoid phishing scams
8. Ongoing monitoring and security management to mitigate issues before they occur

Results:
Restore Operations Within 24 Hours

The construction management company's existing network security and data backup/disaster recovery company was unable to eradicate the infection, leaving the company with over 10 days without use of their computers and without access to data, resulting in over $100,000 of lost productivity and business.

Network Coverage was able to restore data and operations within 24 hours to get the construction management company back up and running at full capacity and to mitigate continued financial impact.

In addition, Network Coverage put network security measures in place to better protect against future ransomware attacks. Network Coverage also implemented a secure, automated, reliable backup system to prevent data loss and protect against the impact of future threats.

1. Eradicated ransomware virus
2. Recovered and restored data within 24 hours
3. Increase security measures to protect against future attacks
4. Implement reliable automated data backup & disaster recovery plan

About the Network Security Attack

Phishing scams are network security threats that work to attain sensitive information such as usernames, passwords, or network access through the disguise of seeming like a trusted source. These scams use the human element of trust and lack of information to trick the recipient into granting access. Some of these attacks can be prevented through security technologies that better prevent phishing scams from reaching their targets, while others can be prevented through prioritized data systems and protocols, as well as employee training.

Network security threats are evolving at a rapid pace, making it essential to companies of all sizes to maintain security defenses against them. However, equally important is the disaster recovery plan to recover and restore data in case of emergency. Being able to restore data in the face of loss can take losses down from days or weeks to only hours. This significantly minimizes short- and long-term financial impact.

It is important to take action to prevent against these attacks before they occur. It is almost always more costly, time-consuming, and devastating to a company to attempt to recover from an attack than it is to prevent the attack in the first place.

4 Tips for Preventing a Network Security Attack.

1

Conduct a network security audit (we offer free IT security audits).
Are all of your security measures functional and up-to-date? Are there any weak links in your network? Do you need to make any updates based on personnel or information changes?

2

Educate your employees.
Do you have standards in place for educating employees against threats and taking basic measures—changing passwords, avoiding phishing scams, backing up data, preventing lost or stolen hardware—to prevent security risks and data loss?

3

Check and monitor data backups.
Are backups being made regularly? Is all essential data being backed up? Are you able to access backups when needed?

4

Perform a disaster recovery drill.
If you were to lose data, do you know the steps that would need to be taken to restore that data?
It's helpful to do regular dry-runs to audit the process, as well as to know how long recovery would take in case of emergency.

NetCov

info@netcov.com | www.netcov.com | 888-800-0433