ConRes | 50
CONTINENTAL RESOURCES | YEARS

BACK FROM THE DEAD: A Ransomware Recovery Story

Are you confident you can prevent a ransomware attack from infecting your environment? They ignored concerns, and then it happened...

This past summer, ConRes was called into an emergency situation in which a company's entire global network was wiped out and destroyed within minutes.

The company has approximately 70 corporate locations globally, 30 global datacenters, and thousands of customer servers and hosted applications.

Due to rapid acquisition in recent years, this company has many locations with unique customer services that require different customer and IT Policies – often with non-standard hardware and software – all of which connects back to the global network and datacenters.

This led to a patchwork of different companies operating under one umbrella, with minimal security policies and security solutions in place.

The Customer was infected with Petya Ransomware. Rather than attackers collecting ransoms, Petya was intended to wipe, destroy, and cause as much collateral damage as possible, and it did just that.

> **Imagine the unthinkable; 13,000 users and thousands of corporate and customer hosted servers infected globally, all un-repairable.**

This company wasn't even the intended target. The initial infection occurred within an accounting software update from an authorized contractor with remote access VPN.

So we'll ask again, are you confident you can prevent a ransomware attack from infecting your environment? If the answer is no, you need to do something about that today.

How do you bring a company back from the dead following a global ransomware infection? It takes a massive amount of resources and time, leveraging the right partners, and it's expensive.

ConRes played a leading role in the Incident Response, Recovery & Restoration, and the ongoing efforts to secure this company's infrastructure. The initial phase was a month long, 24/7 operation providing Disaster Recovery Services including:

- Quickly assembling a core team of onsite engineers from start to finish and playing a leadership role for the recovery, including overnights, over the weekends, over the holiday.
- Developing Incident Response solution designs and implementation process and plans.
- Building an onsite 24/7 Network Operations Center (NOC) to implement and turn-up security solutions on a global scale. Staffing engineers 24/7 on rotation.
- Providing 24/7 Triage Services to support the restoration of the global infrastructure.
- Working cohesively with other VARs and vendors – ignoring the politics; heads down and executing the plan.
- Providing both internal and 3rd party senior engineers, working together as a unified team.
- Providing project management on all services while working with many PMO teams.
- Developing the recovery mission strategy with unbiased product recommendations.
- Leveraging ingrained vendor partnerships to rush emergency acquisitions and services; flexibility to do what needs to be done to expedite recovery:
  - Flexibility for product purchases during non-work hours
  - Integration center for staging and prepping, international shipping, and all logistics involved

It's not a matter of IF you'll be attacked, it's WHEN. And you need a better plan.

ConRes can develop custom security solutions by identifying the top vulnerabilities specific to your network and provide tangible what-if information if left unaddressed. You need to have a plan in place to tackle both known and unknown Day Zero Attacks. You need to understand the financial ramifications of allowing a lax security policy. Let us help you with:

- Backup Solutions
- Disaster Recovery
- Endpoint Protection & Posturing
- End-to-End Vulnerability Assessments and Penetration Testing
- Security Policies and Pro-active Incident Response Services
- Network Security, Segmentation and Micro-Segmentation
- Next-Generation Firewalls
- Patch Management
- Develop a restoration strategy for a cyber-attack
- Security Monitoring and Analytics

ConRes has experienced first-hand why security is important at a massive scale, how to protect against attacks, and when an attack does occur - how to support you and help remediate. Contact ConRes to get started with a Security Strategy Workshop.

Schedule a meeting: www.conres.com/securityworkshop