PROVISION INFOTECH

CASE STUDY: FROM COMPROMISE TO CONTROL: RANSOMWARE INCIDENT RESPONSE AND RECOVERY IN A CRITICAL OT NETWORK

What We Did

During the fall turnaround season, a gas-processing plant's SCADA network was hit by a ransomware attack introduced via an unmanaged vendor modem. Within minutes, all HMI workstations were locked, cutting operator visibility into compressors, tanks, and safety systems. With daily throughput exceeding 500 MMscf/d, each hour of downtime risked major financial loss and regulatory exposure.

Provision Infotech was called in while the attack was ongoing. Our OT response team quickly isolated infected segments and blocked data from leaving the plant network. Using our proprietary PacketProof™ tools, we traced the breach path - from vendor modem to maintenance laptop - and cataloged all impacted assets for investigation.

Thanks to clean, tested backups from a Provision-led disaster recovery drill three months earlier, core systems were restored in under four hours - well within the plant's 8-hour outage limit. Critical controls were verified against a commissioning checklist, avoiding a full process shutdown and saving an estimated CA $850,000.

Post-recovery, we overhauled remote access with firewall segmentation, MFA, and automated logging. Offline backups and quarterly penetration testing were added to ensure future resilience. What began as a live crisis became a same-shift recovery and infrastructure upgrade, giving the client renewed confidence in their cyber defense strategy.

Highlights

4-Hour Recovery from Active Ransomware Attack

Full operator control was restored within four hours—avoiding shutdown and meeting all operational uptime requirements.

Root Cause Identified with PacketProof™ Tools

Provision traced the attack path from a vendor modem to infected assets, enabling a complete post-incident investigation.

CA $850,000 in Downtime Costs Avoided

Rapid recovery helped the client avoid major throughput loss, restart costs, and potential regulatory impacts.

Long-Term Cyber Resilience Built In

Remote access was rearchitected with MFA and firewall segmentation, and new backup and pen-test protocols were implemented to meet insurer and regulatory standards.

Ready to see these results for your business?

Contact Us

info@provisioninfotech.com

provisioninfotech.com

PROVISION INFOTECH

Empowering the **Energy Industry Through IT & OT Excellence**

We bridge the gap between corporate IT and front-line operational technology (OT), delivering reliable, hands-on, facility based secure technology solutions that keep Western Canada's energy infrastructure operating safely and efficiently.

Who We Are

Provision Infotech has supported energy producers across Alberta, British Columbia, and Saskatchewan since 2015. Our team brings together corporate IT engineers and deep OT expertise, safety-certified field technicians, making us equally effective in head offices, control rooms, and remote well sites.

What We Deliver

OT & IT Specialists
One team that speaks both languages.

Certified On-Site Support
Our COR-certified, ISNetworld & ComplyWorks-verified field technicians are embedded onsite in remote field locations, providing consistent, boots-on-the-ground support

Cybersecurity & Risk Management
Threat hunting, patching, and compliance for industrial networks assessments.

Control & Industrial Networks
Design, build and maintenance for SCADA, PLC, and HMI.

Secure Remote HMI Access
Encrypted, role-based connectivity for dispersed operations.

Why Choose Us

Purpose-built IT & OT team
A uniquely blended skill-set designed expressly to support both corporate offices and field operations for Western Canadian energy producers

Aligned with your production goals
We plan and act to minimize downtime, control costs, and respond rapidly to critical field issues and emergencies.

Deep dual-domain expertise
Seasoned in enterprise servers, networks, and cybersecurity and in SCADA, PLC, and control-system environments - bridging the gaps between IT & OT.

Proven Field Experience
Delivering real-world and hands-on reliability across 300+ Western Canadian sites.

Safety you can Trust
Comprehensive HSE program, COR certification and full ComplyWorks & ISNetworld registration; every technician holds H2S, First Air, CSO, WHIMIS, and more.

Contact Us

 info@provisioninfotech.com

 provisioninfotech.com