



IT NATION™

SECURE

hosted by  CONNECTWISE

Ransomware Horror Stories

2023 Edition

Presented by Chris Loehr, EVP, CTO



= solis

IT NATION™ **SECURE**

Objective

Provide examples of some recent ransomware cases so that as a service provider you can:

- 1** Speak to your current customers on why they need to improve their cybersecurity risk management.
- 2** Speak to your current customers on why they need enhanced incident response planning and testing.
- 3** Speak to your current customers to learn more about their business so that you may find evidence that their risk footprint is larger than first believed.
- 4** Enhance your conversations with prospects to demonstrate your advanced knowledge of cybersecurity.



THE LIGHT AT THE
END OF THE
TUNNEL ISN'T A
WAY OUT. IT'S AN
ONCOMING TRAIN.
- BRIAN KREBS

Stories are anonymized to protect
the guilty & the innocent. 😊

Healthcare



- Five-person company
- Not patient-facing
- Father and son operation
- Ransomware
- Backups – too many backups
- Security – lacking considerably
- Data – 1M+ patient records
- No data retention policy
- Data received from customers was not vetted
- Moved to pen and paper

Fabrication



- Less than 50 employees
- Metal fabrication
- Single owner
- Ransomware
- MSP had great backups
- Security – good, but turned down adding key controls
- Data – schematics
- No data retention policy
- Small company, small focus by vendors (not anymore)

Financial Services



- Less than 50 employees
- Financial services
- Single owner; daughter involved
- Ransomware
- Good backups
- Security – needed help
- Broad customer base
- No data retention policy
- Compliance challenges because they did not keep up with state regs

What happens when one doesn't have insurance?



- Organization could have to put up a retainer, typically 50%.
- Some firms may turn down the opportunity due to client's financial status or other risks.
- Counting pennies becomes the norm.
- Client is less likely to take the preferred legal path due to cost concerns.
- Whatever budget may have been there for security improvements has now been consumed by the case.
- Getting insurance going forward will have a much steeper path.
- Have seen owners exit a business immediately after an event occurs.

Law Firm



- Less than 100 employees
- Family law, long established
- High wealth clients
- Ransomware
- Good backups
- Security – above average
- No data retention policy
- The data they kept was some incredibly sensitive data dealing with divorce and other personal matters

Shared infrastructure (Communal)



- Three companies
- No legal connections to one another
- Shared servers (domain, file, etc.)
- MSP's idea
- Ransomware
- Three different insurance carriers
- Whose fault was it?
- Please don't do this. I have seen this three times now.

Shared Infrastructure (Communal)



- Small organization <30 employees
- Ransomware
- MSP restored
- MSP advised against insurance, IR or Legal being involved
- Org has no idea if exfiltration occurred
- Org has no idea of root cause
- Saving grace is org really had no sensitive data on systems impacted
- Org trusts MSP 100%
- MSP was defensive

Non-profit



- Small municipality <20 employees
- Ransomware
- One-man IT consultant
- IT consultant notified every law enforcement org he could before calling insurance/IR/Legal
- IT consultant would only perform tasks if the Secret Service approved it first.
- Case last 10X longer than it should
- Destroyed evidence when directed not to so.

CLOEHR@SOLISSECURITY.COM

[HTTPS://WWW.LINKEDIN.COM/IN/CHRISLOEHR/](https://www.linkedin.com/in/CHRISLOEHR/)



Don't forget to fill out your

SESSION SURVEY