Case Study: Business Held Ransom by One Click

True Story: *October – Milton, Ontario*

An employee of a transportation company innocently clicked and opened a "normal looking" email from a "trusted name" on a shop floor computer.

- ✓ *Unknown to the employee, this action activated malicious software (i.e. malware) on their computer system called CryptoWall Ransomware.*
- ✓ *Behind the scenes the CryptoWall malware immediately began encrypting all the company's data files. Soon they would not be able to access any of their business information. Accounts, production and HR information would be inaccessible to them.*
- ✓ *Normally, the CryptoWall malware would ask for a ransom payment of $700 USD per infected computer or server in order for the user to get their data back. In this case they would be paying the equivalent of over $2000 USD per computer.*

Months earlier the company, in conjunction with HSL, had created a data recovery plan. ***HSL's "RS Level 52 data protection solution"*** *was chosen to be the heart of the transport company's data recovery plan. HSL's policy of plan testing proved invaluable once again as this gave everyone confidence that they could deal with malicious software.*

The Result:

The client avoided being completely shut down, had the malware removed and recovered the data within one day without paying any ransom.

What is your Current Business Recovery Position?

- ✓ How long would it take to get your business back to normal if you lost all of your data today? Has your current plan been tested?
- ✓ Would having a proven recovery plan give you peace of mind knowing you are protecting your business by being prepared?

Get a Free Copy of How to Create a Data Recovery Plan - request a copy via email joe@hardsoft.ca

HardSoft Systems Ltd. 1376 Plains Road East, Burlington, ON L7R 3P8
P: 905 320 3295 www.hardsoft.ca email joe@hardsoft.ca