LAW FIRM IN GREATER TORONTO AREA

ABOUT OUR CLIENT

Our client (thereafter referred to as "The Client") is a law firm in the Greater Toronto Area that has been resolving legal issues corresponding to serious and complex injuries, accident benefits, and tort claims for over 35 years. They have the expertise required to challenge insurance companies and ensure their clients receive the benefits and compensation they are entitled to. They employ over 165 people in 5 office locations, with their headquarters located in Etobicoke, ON Canada. They represent people in 37 languages. They are a true community law firm.

THE CHALLENGES

TCS and The Client have had a strong partnership for decades. We are extremely proud of the trusted relationship we have formed with its Management team.

Recently, The Client was highjacked by Ransomware. The hackers blocked access to their systems and data and demanded payment in exchange for restoring access. Rather than waste time restoring data from backups they chose to pay the hackers and recover their encrypted information. Sadly, in most cases hackers promise their victims they will restore access but don't always following through. This was a risky move for The Client. Fortunately, it worked! However, this incident set in motion a very important mission for the Management team at the firm: *How do we protect ourselves from this type of attack in the future?*

The Client turned to their trusted partner TCS. We assessed their current security posture and found some important components were lacking. We positioned a new FortiGate Next Generation Firewall (NGFW) by Fortinet (one of our trusted technology partners). The next-generation firewall solution included a built-in Intrusion Prevention System and Unified Threat Management to mitigate attacks from the outside.

During the time these new security measures were being implemented, The Client experienced a 3-day power outage within their building. This left the business crippled, as all their communications and server infrastructure were inoperative. This prompted yet another discussion with the Management team: *Would moving our communications to the Cloud provide the reliability, resiliency and redundancy we need to keep our business running?*

TCS performed a technical audit and upon further investigation made the following findings:

- Network security inadequate
- No geo-redundancy measures (applications switching from one site to another in the event of catastrophic failure)
- No failover plan for critical systems

THE SOLUTION

TCS' proposed solution included moving all The Client's critical systems and communication tools (phone and email) into our data-center, and thus into our secure Cloud environment. This would afford geo-redundancy and decrease their IT overhead.

TCS also proposed a TCS Shield security solution, which included implementing a FortiGate NGFW to mitigate external cyber-attacks and threats.

THE RESULTS

Moving The Client's critical systems and communications tools to our secure Cloud environment enabled us to implement geo-redundancy measures. The solution includes built-in continuity and disaster avoidance features to keep their business running in the event of a power outage or any type of event that would cause a significant disruption to daily operations. As part of this process we converted their traditional PRI's into SIP lines which allowed them to realize significant savings in their monthly expense.

With the implemtation of a TCS Shield security solution, The Client now had leading edge security and network protection. We utilized the feature and functionality of the FortiGate NGFW to restrict access to unauthorized sites and online utilities as well as protecting the client from viruses, ransomware and malicious cyber intrusions. The new, secure Fortigate NGFW provided deep visibility and granular control of applications, users and web filtering.