

Productivity Up, Risks Down: A Security Firm's IT Makeover



AT A GLANCE



A mid-sized Canadian non-profit security firm, with over 1,500 employees across multiple locations, was facing challenges with its current infrastructure, including slower systems and rising cybersecurity risks that impacted its productivity. Although the firm's sole IT Manager was highly skilled and dedicated, the rapid growth and complexity of the IT environment had outpaced what one person could manage, and they needed additional resources.

Leadership recognized the need for external expertise and **sought a technology partner to help modernize infrastructure, provide strategic guidance, improve the user experience, and strengthen their cybersecurity best practices.**

CHALLENGES



With their current growth rate, the in-house IT Manager needed additional support to sustain the need to update hardware, licensing, network architecture, and ensure their cybersecurity practices were up to date to avoid leaving the security firm vulnerable and putting business continuity and growth at risk.

Through a competitive RFP process, SysGen was chosen as their new IT partner, in collaboration with their IT Manager. During the onboarding process, SysGen offered to conduct a comprehensive assessment of its IT environment to pinpoint potential critical gaps and risks. Based on this evaluation, they would develop a strategic plan that addressed urgent issues, outline a new roadmap for infrastructure modernization, strengthen cybersecurity practices, and provide ongoing CIO-level guidance. This strategy would help the security firm and its in-house IT Manager operate securely, efficiently, and with a foundation for future growth.

SYSGEN'S PROPOSED SOLUTIONS



SysGen won the RFP opportunity through their unique Dedicated IT Support Model[®]. This model rejects call centres and has been proven to be the most proactive IT solutions approach, and is customized to their clients. During this process, SysGen took the time to propose the optimum solutions. Key elements included:



Comprehensive IT Assessment: SysGen proposed this initial step to uncover potential risks and gaps in the security firm's IT infrastructure. This allows their dedicated techs to understand the firm's environment and work flows as well.



Strategic Oversight & CIO-level Guidance: After the assessment, SysGen curated an executive-level IT strategy and guidance while eliminating the cost and commitment of a full-time in-house CIO, while keeping the partnership with the in-house IT Manager in mind.



Infrastructure Modernization: Alongside their IT Manager, SysGen worked together to run system updates, servers, and licensing. This part of the project took partnering directly with the rest of the organization, fostering the collaborative environment.



Improved Security Posture: The next step was to analyze the security firm's current cybersecurity practices, made the necessary updates in systems and hardware, and foster a training environment for their staff to be aware of potential cybersecurity risks.



Flexible Hybrid Environment: Together, SysGen and the security firm combined on-premise systems with cloud services for scalability and resilience.

THE PROCESS



Having completed the aforementioned proposed solutions, SysGen followed a structured process that balanced immediate fixes with long-term strategy. This approach ensured risks within the security firm were addressed quickly while laying the foundation for sustainable growth, stronger security, and better user experiences. **Here are the following steps:**



Assessment & Planning: In addition to the initial assessment, SysGen conducted regular and comprehensive IT audits that identified risks, bottlenecks, and opportunities, which lead to a clear modernization roadmap.



System Reconfiguration: Quick wins such as security patches, account cleanups, and network optimizations immediately improved stability and protection. This was done on a quarterly basis to remain proactive within the IT environment.



Implementation: The core infrastructure was modernized, backups were secured, and updated licensing was brought into compliance to reduce risk and enhance performance.



Strategic Oversight: CIO-level involvement aligned IT initiatives with business objectives, driving governance, compliance, and lifecycle planning. This step was always conducted in partnership with the in-house IT Manager.



Dedicated IT Support: SysGen remains embedded within the security firm's team, providing consistent on-site and remote expertise with proactive monitoring and guidance.

THE OUTCOME



The partnership transformed the security firm's IT landscape, shifting it from a reactive operation into a proactive and strategic enabler of growth. Their current infrastructure and potential cybersecurity risks were replaced with modern systems, robust safeguards, and reliable processes that improved the day-to-day experience for everyone involved.

With their CIO-level guidance, IT decisions became aligned with business objectives, while the in-house IT Manager gained the resources and support needed to focus on higher-value initiatives. This comprehensive approach turned IT within the firm into a driver of productivity and security, delivering measurable results.

40%

By partnering with SysGen, the security firm strengthened security, with up to 40% fewer risks with MFA, security patches and improvements.

60%

Less downtime and improved overall productivity resulted in boosted efficiency across the 1500+ employees within the firm.

30%

More IT projects delivered successfully with partnership and strategic alignment.

50%

Fewer escalations with on-site and remote support, which helped the employees feel empowered and satisfied.