Addressing Continuity Amid Growing Ransomware Threats in Small Business

Protect valuable business-critical data with best-in-class ransomware defence

Small and medium businesses (SMB) are increasingly concerned about the growing threat of cyber attacks, due to the fact that **50% - 70% of all ransomware attacks are aimed at SMB companies**. These outbreaks target employees' personal identifiable information (PII), customer data, financial data, and other critical business information. The impact can be crippling, including downtime from the complete shutdown of data centres, supply chain and business operations, lost reputation with customers and partners, and significant financial ramifications. With Ransomware Containment as part of their cyber security and business continuity protocols, organizations can have peace of mind that their critical, sensitive information assets are protected.

Business Challenges

- Growing threat of cyber attacks, especially ransomware
- Increase in security risks and vulnerabilities associated with remote work and digital workplace
- 200% increase in downtime year-over-year as a result of security breaches
- Recovering from such an attack could be extremely costly – it's estimated that 60%of small businesses fail within the 6 months following a ransomware attack and 80% are likely to be hit a second time

Business Results

- Minimal impact on IT infrastructure and network performance
- Can prevent potential system lock down and avoid significant data recovery and repair costs
- Confidence in ability to manage potential breaches with focus on business continuity
- Countering the impact of additional security threats associated with more staff working from home

RICOH
imagine. change.

Growing cyber security concerns

The growing concerns of cyber threats in SMBs have recently been attributed to the pandemic, with increased numbers of employees working remotely, resulting in the expansion of organizations' corporate networks, this in turn, creates even more entry points for the ever-evolving and increasingly sophisticated cyber criminals. A Coveware report found that the average days of downtime following a ransomware attack was 23 days, and the average ransom payment for mid-sized organizations was $136,576 as of Q2 2021.

Most SMBs may have invested in multiple layers of perimeter and endpoint security to protect their infrastructure and assets from a potential security breach. However, cyber criminals are continuously innovating new and unknown methods to defeat traditional prevention-based security solutions, often spending weeks to months working undetected inside a network before delivering a payload, encrypting up to 10,000 files per minute.

Small and medium-size businesses are continuously adapting to new security risks with employees not leveraging VPN, accessing company data from personal devices, or using infected USB and other removable media to manage files. Being one click away from a possible ransomware breach, employee HR records, customer data, and critical business reports and data are stolen, and devices and files are encrypted. The impact could be devastating to companies of all sizes, ranging from damaging reputation with customers, large financial ramifications from losing thousands of dollars per hour due to ransomware-induced downtime, legal costs including paying the ransom, and interrupted business operations.

When employees are away from the office, they tend to be less mindful of security best practices. Despite robust security systems, organizations recognize that there is a heightened risk with more employees working from home.

Implementing a 'Last Line of Defence'

To help defend against ransomware, the organizations that have implemented the Ricoh Ransomware Containment solution as an additional line of defence get an instant alert, and the solution responds by shutting down the endpoint under attack, including laptops. The solution is an agent-less application that is installed on a virtual server in the central IT system instead of every endpoint and has minimal impact on IT infrastructure and performance. It monitors, in real-time, data across the entire organization. It is intended to spot a ransomware attack – usually via a laptop or desktop – anywhere across the entire network even when it has managed to bypass existing security systems. The solution then locks down the location, isolates files impacted by malware encryption, and stops the ransomware from spreading across the entire network.

As a result, the organization can have confidence in its ability to manage a potential breach with a focus on business continuity. Operations are running smoothly, systems and applications are not locked down, and only a small number of files need to be repaired and recovered. Stopping the ransomware attack would also allow the business to preserve its reputation with customers and partners without financial ramifications such as legal fees, settlement costs, a ransom payout, or other long-term financial liabilities.

1. https://www.inc.com/amrita-khalid/ransomware-hackers-crime-cybersecurity-tips.html
2. https://www.backblaze.com/blog/the-true-cost-of-ransomware/

Learn how you can protect your organization with ransomware containment. **Book a demo today!**

RICOH
imagine. change.

www.ricoh.ca

Ricoh Canada Inc. 100-5560 Explorer Drive, Mississauga ON L4W 5M3, 1-888-742-6417