Secure Customer Trust By Protecting Your Business From Cyber Attacks

This article was originally published on Huffington Post Canada.

Trust is everything when it comes to our money. As customers, we need to know that every transaction is secure and that our personal information and money are both safe. Ensuring this reality is an ongoing challenge for organizations tasked with managing network security, especially considering the number of non-cash transactions that occur worldwide every year — 390 billion in 2014, a nine per cent increase from the year before. With this in mind, here are six ways to protect your business from cyber-attacks, presented in partnership with Cisco.

Make it a priority

A security breach is expensive – $3.79 million on average and climbing. And that number doesn't even cover the real damage, which is the cost of lost revenue and the erosion of customer trust. For businesses in the financial services sector, investing in network security is not just good defence – it's aggressively forward-looking. Using security products including Cisco solutions is the first step for business that are increasingly using technology to better their business – from mobile devices, to guest wi-fi – cybersecurity needs to be a priority at the highest level of the organization.

Gathering support and aligning the necessary resources is the first step to protecting your business from cyber-attacks. Organizations that manage to transition from a reactive security strategy to one that is proactive and predictive will be the ones with a clear competitive edge.

Create a plan

While the specifics of your cybersecurity plan will vary depending on many factors, all effective cybersecurity plans should address three critical elements: people, processes and technology. A breakdown in any one of these areas can have catastrophic results.

A number of industry groups, vendors and government agencies provide resources and frameworks to help businesses create effective plans. Examples include the NIST Cybersecurity Framework and Cisco SAFE. The NIST Cybersecurity Framework was developed in part by the United States Department of Homeland Security and is endorsed by Public Safety Canada.

Conduct regular backups

The importance of backing up sensitive corporate and customer information on a regular basis cannot be overstated. Whether using hard drives, servers or the cloud, ensuring that data is stored safely and backed up consistently helps protect the business in the event of a data breach. Conducting complete and incremental backups on a daily, weekly and monthly basis ensures information isn't lost or compromised. Using Cisco products that help automate and centralize the process can help make securing sensitive information a hassle-free affair.

Update aging IT networks

The 2016 Cisco Annual Security Report reveals that too many businesses have older IT infrastructure that runs on outdated operating systems. In the financial services sector, 20 per cent of network components have passed their Last Day of Support – the highest obsolescence level. While institutions like major banks are well-resourced to invest in security expertise and threat protection, mid-sized financial services organizations like credit unions, wealth management firms, and accounting firms are struggling with the challenge of protecting customers' data. Updating the network infrastructure using products such as Cisco firewalls, identity management and intrusion protection products, for example, can assist in detecting unauthorized users attempting to access the network, while ensuring safer network access from staff and end users alike.

Establish a strong culture of security across the organization

Establishing a strong culture of security – one that encourages staff to be ever mindful of security risks and threats – can go a long way in protecting the business. This can include enforcing acceptable website policies, encryption, and remote access policies that help employees select stronger passwords.

Don't be afraid to ask for help

Research indicates there will be a global shortage of two million cybersecurity professionals by 2019. This means many organizations will have to look externally to find the necessary talent to develop and implement their cybersecurity strategy. Vendors with deep security expertise like Cisco employ teams of cyber security professionals and offer customers advisory, implementation, or even managed services to help close this gap.

These five tips can set a solid and secure foundation for protecting the business from cybersecurity risks. In addition, using Cisco technologies and services can help provide a comprehensive security architecture, simplifying security management and bringing faster threat detection and containment. At the end of the day, it's about ensuring the security network helps grow the business, ensure customer safety, and maintain that all-important competitive edge. Learn how you can combat security threats here.