8 steps to creating a retail cyber security strategy

Step 1

Review what you have

It's a good idea to bring in cyber security experts who can help you identify where the breaches are most likely to occur and what data is valuable - both to you, and to potential cyber criminals.

Step 2

Create your top-line cyber security approach

It's likely your initial plan will cross multiple departments and teams, with the ability to work across cyber defences and organisational functions, to create or strengthen an integrated cyber security strategy.

Step 3

Complete regular staff training

Many attacks rely on employee negligence or gullibility to steal your valuable data. That's why top of the line and frequent staff training is important. Your goal is 100% compliance with data security best practices.

Step 4

Define user & credential management practices

Best practice today suggests that you start from a place of Zero Trust. Always authenticate and authorise based on all available data points and you should never give more access than is needed for longer than is required.

Step 5

Consider all workers: in-store, head office, and off-site

Hybrid working is a relatively recent shift, so it's easy to forget about the full dispersion of your workforce. Each use case will have different access, security, and training needs. Be sure to account for all in-store, head office and off-site team members in your strategy.

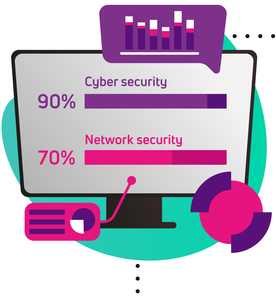
As of February 2022, according to Findstack, "Remote work statistics tell us that across the world around 18% of people work remotely full-time. On the other hand, in the USA more than 4.3 million people work remotely, which amounts to 3.2% of the entire workforce."

Step 6

Source malicious attack protection

At the core, you'll want a solution that allows for different access levels within a Zero Trust framework:

- Patched regularly to protect you from the latest threats
- Swift, real-time response measures
- Learn and adapt to the unique risks your organisation will face



Step 7

Install network security programmes

You'll need to have both cyber security and network security to boost a robust retail cyber security strategy. Many modern security packages offer both under one bundle, so weigh your options carefully.

As explained by Difference Between, "In simple terms, cyber security is the practice of protecting internet connected systems and networks from digital attacks. Network security, on the other hand, is the act of protecting files and directories in a network of computers against misuse, hacking, and unauthorised access to the system."

Step 8

Proactively monitor for threats

Real-time monitoring is the most effective way to reduce your risk. This is done by continually scanning for breaches while providing ITIL-based change and problem management services. Your cyber security advisor can determine if your current solutions are up to the challenge.