

# Retail Cybersecurity Best Practices Ensure a Safe and Profitable 2022



Retailers face daunting cybersecurity challenges in a rapidly evolving business landscape. Omnichannel retailing brings the need to simultaneously address security in the physical store as well as online. Ransomware attacks grow more sophisticated daily. And new privacy laws add increased complexity. Retail cybersecurity best practices help ensure a prosperous 2022.

## Invest in Continuous Monitoring

Effective cybersecurity requires ongoing effort. Businesses should begin with [compliance and security audits](#) to evaluate the cybersecurity landscape and establish a baseline. Identify security vulnerabilities and compliance issues. This helps guide the process of prioritizing a strategy to protect valuable assets and achieve regulatory compliance.

Any effective cybersecurity strategy must include ongoing monitoring and threat detection, as well. Automate continuous monitoring for security anomalies, particularly in the area of login behavior. Additionally, carry out regular penetration testing and security reviews.

## Upgrade Authentication and Access Management Policies

Authentication and access management present a significant challenge for any industry, but especially for retail. High employee turnover means that many short-term employees have access to sensitive

systems. Limit employees to only the access they need to perform their job functions. Then be sure to quickly remove access for employees when they leave.

Deploy multi-factor authentication (MFA) where possible. This includes a combination of authentication measures such as time-sensitive security codes, biometrics, and security questions. Additionally, implement and maintain a [strong password policy](#).



## Take Steps to Protect Customer Data

Retailers gather a host of information from their customers, from name and contact information to shopping preferences, billing data and even birthdates. This data allows businesses to personalize marketing and streamline the shopping experience. But the abundance of sensitive data also poses an attractive target for hackers, as well as a compliance risk.

To protect customers, only store the bare minimum of data necessary and be sure to encrypt all sensitive information. Additionally, solid [mobile data governance](#) aids the regulatory compliance process. Businesses must know what customer data they store and where it resides. And they must be able to demonstrate reasonable data security measures.

## Keep Up with Regulatory Compliance

[Data security and regulatory compliance](#) are tightly intertwined. And for the retailers, the regulatory scene continues to grow more complex as states implement additional data privacy laws.

For instance, over the next year, several key privacy laws come into effect. These include the California Privacy Rights Act (CRPA), an expansion of CCPA. Virginia and Colorado have also passed significant

new data protection laws. And the trend will likely continue. Retailers must include compliance as an integral part of their cybersecurity strategies.



## Ongoing Security Awareness to Address Human Factor

Last but not least, employees play a critical role in any cybersecurity strategy. Due to employee turnover and the rapidly evolving security landscape, annual training will not suffice. Make [security awareness](#) a priority through a multi-faceted training approach.

Present [cybersecurity workshops](#) regularly, with training targeted according to job description. Begin by including security awareness as a critical part of onboarding. Back up the training with just-in-time security reminders such as posters. And conduct phishing simulations at periodic intervals.

## Protect Your Business and Customers with Retail Cybersecurity Best Practices

eMazzanti delivers comprehensive [retail technology solutions](#) for its customers, from multi-layered cybersecurity to point-of-sale technology and more. Our award-winning team will help you implement effective monitoring and authentication tools and achieve compliance. We also offer solutions for security awareness training.

[Contact eMazzanti](#) today to get started with a security and compliance risk assessment. Then work with our retail IT experts to tailor a security strategy to your business needs and budget.

2015 | 2013 | 2012 Microsoft  
Partner of the Year



**Inc. 500** || **5000**  
2016 | 2015 | 2014 | 2013 | 2012 | 2011 | 2010



**ShoreTel Sky**  
Partner of the Year