How Retail Cybersecurity Can Adapt to the 2021 New Normal

The retail industry, having learned to co-exist with a global pandemic, saw significant changes in 2020. Foremost among them is a major shift to the eCommerce channel. For those smaller retailers new to eCommerce technology, shopping and payment apps, and work-from-home technology, retail cybersecurity challenges have become much more of a concern for 2021.

2021 Retail Cybersecurity Threats

Trustwave's 2020 Global Security Report found that 24% of all cyberattacks targeted retailers, the most of any industry. Alarmingly, the new normal of eCommerce and work from home (for back office staff) makes retail even more of a target than it was a year ago.

Retailers make attractive targets for cyber-criminals. The shift to eCommerce means that retailers must process and store more customer data. Hackers seek to steal personally identifiable information (PID), including credit card and bank data to profit from selling data on the dark web.

Others use stolen credentials and passwords to purchase products from online retailers. Knowing that consumers reuse passwords, they try to login to multiple sites, sometimes using automation to speed up the process (credential stuffing). Payment processes also see numerous attacks.

There's a lot of new territory to protect and the security standards and technology have a hard time keeping pace. The fact that retailers often employ young and inexperienced staff who lack

cybersecurity training complicates the problem. Hackers use social engineering techniques to gain access to sensitive data, knowing that humans are the weakest link.

Retail Cybersecurity Best Practices

To begin the process of evaluating your retail cybersecurity readiness, consider how your company is doing relative to these retail cybersecurity best practices:

The Bare Minimum

1. Don't Retain Sensitive Customer Data – Storing sensitive data such as credit card information multiplies your risk by making you more of a target and exponentially increasing the cost of a data breach. If that information is stolen, your reputation suffers long-lasting damage, and you may be subject to fines and litigation.

Investigate options such as tokenization that substitute non-sensitive equivalents or tokens for the sensitive data on your system through a tokenization system.

2. Perform Regular Verified Backups – Be sure to back up your eCommerce website, POS systems and other applications and data at least daily, more often if possible. Periodically test your backups to verify their quality.

Backups are essential to survive ransomware attacks, natural disasters, and other types of data emergencies. A managed services provider (MSP) can help you automate the backup process.

3. Ensure PCI DSS Compliance – With payment data security standards set by industry experts, PCI compliance is a must to process customer payment data. Consult PCI DSS compliance experts to verify compliance.

4. Regularly Update Your Network, Applications and Website – Hackers want to exploit software vulnerabilities to gain access to sensitive data. When developers discover new vulnerabilities, they update their software. A managed services provider (MSP) can set up automatic security updates to simplify the task.

Additional Recommended Cybersecurity Measures

5. Use a Secure Web Hosting Service – Select a web hosting service for your eCommerce site that places security as its top priority. You'll want to ensure that automatic and verified backups are performed so your site can be quickly restored in the case of an attack.

6. Use Secure Protocols – Upgrade to the current HTTPS secure website protocol with an up-to-date SSL certificate. Doing so protects your customer's data, increases customer confidence, and boosts your search engine ranking.

7. Use a Secure eCommerce Platform – While comparing the features of Shopify, BigCommerce, or Squarespace, be sure to prioritize security. A breach most likely will put you out of business.

8. Protect Admin and User Login Information – Once hackers gain access to your site they can inflict damage in countless ways. It's good practice to educate customers on good password habits, even require them to change passwords periodically.

9. Employ Multi-layer Security – Multiple security measures provide the highest level of overall protection. All the above plus antivirus software, firewalls, cloud-delivered network security and web filtering, email protection, dark web scanning, remote workforce protection, and especially employee training work together to keep customer and company data safe.

#1 Retail Cybersecurity Recommendation

With numerous possible attack vectors in play, retail cybersecurity is complex. The best thing that a retailer can do to ensure their longevity (survival) in 2021 is to hire qualified cybersecurity experts to evaluate their business security posture.

Keep in mind that the doer should never be the checker. Outside expertise will identify those areas in your business that need improvement. Count on the retail cybersecurity experts at eMazzanti Technologies to help you with this all-important task.