9 WAYS TO OPTIMIZE SECURITY IN THE NEW CASHLESS COMMERCE CULTURE

Around the world, countries are gradually shifting towards cashless economies. The emerging preference for digital payments is propelling organizations to adapt, and to adopt new cashless infrastructure.

Many companies that have made the move to cashless tech are seeing immense success. They're drawing in customers and increasing revenue. By 2022, US e-commerce revenue is projected to reach $638 billion.[1]

And companies in the cashless infrastructure space are growing at breakneck speed. One such company, Stripe, recently announced that it has secured $600 million in new funding.[2] This boosted the company's valuation to an estimated $36 billion.

These enticing figures encourage organizations to trial and trust cash-free digital payment systems.

Did your organization recently transition to a cashless modus operandi?

If so, you now have thousands or perhaps millions of credit card and consumer identities on file. Cyber criminals see these troves of data as treasure chests. Theft and exploitation of consumer data can result in an avalanche of unexpected consequences.

Restructure your cyber security today in order to preserve your reputation, avoid regulatory penalties, to maintain consumer trust and to prevent lawsuits. These practical considerations can help you innovate, optimize, and meet new e-commerce expectations.

Who's driving the shift?

Consumers are opting for cashless due to contagion-related safety concerns, and organizations are on-board. For example:

- European governments have raised contactless payment limits from 20 euros to 50 euros or more.
- Visa has also lifted certain limits on contactless payments.
- The cost of supporting the end-to-end use of cash is $200 billion per year in the United States. As a result, organizations are pushing for cashless.[3]
- Visa now reports that compared to last year, the US has seen a 100% increase in contactless payments.[4]

[1] The Move to Ecommerce: How Retailers Can Adapt During A Crisis, HubSpot, Ronita Mohan

[2] Stripe, Silicon Valley's Most Valuable Start-Up, Raises New Capital at $36 Billion Valuation, CNBC, Kate Rooney, 16 April 2020

[3] Real-time Payments are Changing the Reality of Payments, Deloitte

[4] Our Cash-Free Future is Getting Closer, The New York Times, Liz Alderman, 6 July 2020

Here's how you can stay secure when digital payments are becoming standard practice:

1 PCI DSS compliance.

Be sure to follow Payment Card Industry Data Security Standard (PCI DSS) guidelines. These suggest that you secure your system using firewalls, strong passwords, anti-virus, zero-trust principles, ethical hacking assessments, and so much more.

2 Network & gateway protections.

An integrated suite of defense-in-depth products can help you prevent identity theft, cyber scams and security breaches. Look for a solution that includes real-time threat intelligence information.

3 Security management tools.

Invest in infrastructure that can offer policy-based security and strong authentication. This can assist you in reducing management complexity, as it eliminates redundant processes, and cuts down on required logins and servers.

4 Endpoint security.

Safeguard point-of-sale machines with reliable VPN connectivity. Get a non-intrusive, compact security appliance that's managed separately from the point-of-sale system, enabling it to support WAN options and to deliver reliable connections.

5 Point-to-point encryption (P2PE).

Point-of-sale cyber security solutions can help ensure that payment data travels securely from a customer's device to your payment processing system. Invest in point-to-point encryption capabilities. While many enterprises rely on transmission-level encryption, this is insufficient when it comes to comprehensive risk mitigation techniques.

6 Multi-factor authentication (MFA):

Consider using multi-factor authentication for payments. Major industry players, such as Apple and Samsung, each use several types of authentication to verify that a payment is coming from a trustworthy, legitimate source.

7 Tokenization..

This refers to the process of converting credit card numbers into random strings of letters and numbers. When consumer data is tokenized, a cyber thief will not be able to use it.

8 Visa 3-D Secure:

Consider adopting Visa's 3-D secure technologies, which can use contextual data to determine potential cases of fraud. A five-step data analysis process provides enterprises with critical information that enables you to flag suspicious transactions.

9 Compliance controls.

Explore security software that can offer real-time information about what's happening within your system. Continually receive updates regarding whether or not your system is in compliance with mandatory regulations.

Cyber criminals will launch more cyber attacks on point-of-sale systems in the coming weeks.

The mega US retail event of the year, Black Friday, is almost here, and the holiday shopping season is just beyond.

Both organizations and consumers see e-commerce as an easy, convenient payment solution. It's here to stay for the forseeable future. Follow security best practices to avoid the egregious damage and disproportionate fallout that can occur in conjunction with cyber crime.

To learn more about protecting retail enterprises, read our e-commerce whitepaper.