INSIGHTS FROM THE BDO RETAIL & CONSUMER PRODUCTS PRACTICE

MANAGING GROWING RETAIL AND CONSUMER RISK IN TANDEM WITH INCREASED INNOVATION AND CYBERSECURITY

By Natalie Kotlyar

As digital transformation becomes a core part of overall strategy, retail and consumer products companies should prioritize threat-based cybersecurity. Threat-based cybersecurity is a forward-looking, predictive approach. Instead of (or in addition to) focusing solely on protecting critical data assets or following the basic script of a generic cyber program, threat-based cybersecurity concentrates on investments in the most likely risks and attack points based on an organization's unique threat profile.

For example, this framework looks different for a pure play e-commerce entity than for a hybrid e-commerce or specialty retailer because the most likely attack vectors are different for each. Threat-based cybersecurity approaches go hand in hand with innovation, as security serves as the backbone to digital transformation—and can even be an innovation catalyst.

PROTECTING DATA IS PARAMOUNT IN ACHIEVING PERSONALIZED SHOPPING OBJECTIVES

Retail and consumer products companies have undergone major shifts worldwide due to capitalizing on consumer data as the first step to achieving personalized shopping. But cyber risks grow as data sharing increases.

If organizations in the business are going to sustainably innovate around online shopping, they must be able to safely store and analyze consumer data. Implementing threat-based cybersecurity in conjunction with Payment Card Industry (PCI) standards will be their lifeline and offer them a competitive advantage.

KEY TAKEAWAYS from BDO Cyber Threat Insights – 2019 1st Quarter Report*

Between 2017 and 2018, the **breach rate in the retail sector multiplied by 2.5** as 26% of companies reported being breached more than once.

> 90% of retailers failed to pursue at least 4 PCI DSS key requirements, and an astonishing 98% of them struggled to withhold the key security requirements to maintain secure systems and applications.

64% of insider threats are a result of human neglect (i.e., human error or lack of security awareness amongst employees).

* https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdo-cyber-threat-insights-2019-1st-quarter-repor

UNDERSTANDING THE REQUIREMENTS OF PCI AND THE COST OF COMPROMISED DATA

There are multiple methods to secure information. There are also mandated requirements for protecting information, such as the Payment Card Industry (PCI) framework. If your organization provides technology solutions or services to other organizations; executes transactions using credit card data (process, transmit, or store); or could affect the security of the data that is processed, transmitted or stored (i.e. service providers)—then you are required to comply with the PCI requirements to some level.

ORGANIZATIONS AT RISK

- Retail and consumer products organizations
- Data centers
- Software as a Service (SaaS) solutions
- Infrastructure as a Service (IaaS) solutions
- Hosting providers who offer managed/out-sourced services
- eCommerce providers

BUSINESS COSTS OF COMPROMISED DATA

- Fines as determined by the payment brands
- Increased processing fees
- Removal of your ability to accept payment cards
- Legal costs and settlements
- Loss of customer confidence in your organization

The world we live in requires cost-effective cyber risk management with a PCI component. Retail and consumer products companies should take a holistic approach—making good data security practices and protection part of their overall digital transformation strategy.

IMPLEMENTING THREAT-BASED CYBERSECURITY INCLUDING PCI STANDARDS

Is your data secure? Is your customers' data secure? BDO can help you answer these questions through a comprehensive assessment of your organization's operating environment and its specific business needs. Ultimately, implementing a cost-effective cybersecurity framework includes careful consideration of your risk profile, understanding which digital assets are most critical to protect, and determining your resiliency when incidents do occur.

Once your organization has a better understanding of not just the cyber-attack threats you are encountering, but your email and network vulnerabilities, and the level of real cyber risk you are facing, we can then help you make an informed business investment decision to implement an appropriate threat-based cybersecurity risk management program that fits your respective security needs, schedule, and budget.

We can help you conduct one or more of the cyber security diagnostic services below to determine the cyber threats and risks you are currently facing. We can help you identify and gain process efficiencies, develop realistic timelines, and adhere to milestones along the way, all in conjunction with PCI standards.

- **Email Cyber-attack Detection Assessment**
- **Network Vulnerability Assessment**
- **Penetration Testing Services**
- **Endpoint Cyber Risk Assessment**
- **Spear-Phishing Campaign Services**
- **PCI/DSS – Readiness Assessment**
- **Vendor/Supply Chain Partner Cyber Risk Assessment**
- **Software Application Security Assessment**

"Taking on digital transformation initiatives like adopting an emerging technology, investing in a new technology or even building a new technology are key to operational efficiencies and to bolstering cybersecurity. Incorporating threat-based cybersecurity measures, including PCI into their digital transformation strategy will help mid-market retailers and consumer products companies mitigate risk and focus on more strategic business objectives."

Natalie Kotylar, BDO Retail & Consumer Products Industry Leader

Contact BDO for more details about our qualifications or methodology for ensuring compliance with PCI requirements. You can keep up with the latest news in retail and consumer products by subscribing to the Consumer Business Compass Blog on the homepage here, and follow us on Twitter at @BDOConsumer.

People who know Retail and Consumer Products, know BDO.

CONTACT

GREGG GARRETT
Head of U.S. and International Cybersecurity Advisory Services
703-770-1019 / ggarrett@BDO.com

GREG SCHU
Partner, Payment Card Industry Compliance Leader
612-367-3045 / gschu@BDO.com

NATALIE KOTLYAR
National Retail Industry Leader and Partner, Audit
212-885-8035 / nkotlyar@BDO.com

ABOUT BDO

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 700 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi national clients through a global network of more than 80,000 people working out of nearly 1,600 offices across 162 countries and territories.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.