KOVRR
Cyber Decisions. Financially Quantified.

www.kovrr.com

Applying Cyber Risk Quantification in the Retail Sector

MAY 2022

Retailers are in cyber trouble. Retail and eCommerce CISOs have more to worry about than their peers in other sectors. For one thing, it's an enormous slice of the global economy, with billions of customers moving trillions of dollars moving around—an inviting environment for fraud and mischief. And, a retailer's relationships with its customers can be fragile. A successful cyber attack can have major repercussions for a retail business.

The data is certainly cause for concern. Ever since the 2014 mega attacks that breached tens of millions of customer records at Home Depot and Target, the retail sector has been under pressure to build trust with customers about their data privacy and their vulnerability to fraud. Indeed, the retail industry faces a broad array of cyber threats. According to research from the security software firm Imperva, retailers face a higher level of attempted account takeovers than other businesses (32% of logins for retail vs. 25% in other industries). Retailers also have to deal with more malicious bot traffic than companies in other fields.

For these reasons, retailers are wise to pursue diligent cyber defense strategies. The process of cyber risk quantification (CRQ), which enables a business to put a dollar value on a cyber risk, should be a key part of any retailer's cyber strategy. Cyber risk quantification helps a retailer understand where it is most vulnerable, and hence where it should invest in its cybersecurity program.

One in three retailers see cybersecurity as an obstacle to eCommerce

Retail CISOs have good reason to be concerned about cyber risk exposure. According to Trustwave, **twenty-four percent of cyber attacks targeted retailers in 2020**, for example. This is a higher percentage than any other industry. **A third of retailers claimed cyber worries were their number one obstacle to making the move to e-commerce**, per research from BDO. BDO also found that thirty-four percent of retailers felt that cyber attacks or privacy breaches were the most serious cyber threats they faced.

Money was the motivation of ninety-nine percent of cyber attacks on retailers, according to Verizon. And, as Verizon also found, when data is breached in an attack on a retailer, forty-two percent of it comprised payment information, while forty-one percent was personally identifiable information (PII).

As these data points suggest, retailers are vulnerable for a variety of reasons. A hacker can steal merchandise or money from a retailer. They can steal credit card information, which the retailer may store in its systems. They can also get ahold of PII, which is valuable for other types of fraud.

Damage to brand and loss of customer relationships

Retail is a competitive business, one in which it takes time to build customer loyalty, which can be quickly lost. A cyber attack can damage customer trust. Breaches of personal or payment information thus tarnish retail brands. And, given the size of some retail breaches, the damage can be extensive. A large retailer can easily experience a data breach affecting tens of millions of customers. Cyber risk quantification can help calculate brand damage in money terms.

Risk of failing to comply with privacy laws

Retailers must abide by consumer privacy laws, such as the California Consumer Privacy Act (CCPA). Violations can lead to fines and legal liability for retailers. For this reason, retailers need to protect PII they store on their systems. Cyber risk quantification can help a retailer model the financial impact of a data breach that affects compliance with privacy laws.

Losses due to fraud

A hacker can steal money, merchandise, or both from a retailer. This might be achieved through account takeover attacks, which enable a malicious actor to order merchandise and have it shipped to an address other than the actual customer's. The attacker can also defraud retailers with stolen credit or debit cards or through unauthorized use of coupons. As retailers move toward omnichannel customer relationships, where people can buy online, through mobile devices, in-store, or through kiosks, the attack surface area grows larger.

What is Cyber Risk Quantification?

The challenge for retailers is to understand where they face the greatest cyber risk. It is not possible to invest in security equally across all areas of digital operations. Instead, there needs to be a priority of defense. A retailer should put the maximum investment in areas of cybersecurity where the company expects to experience the greatest potential financial losses from cyber attacks.

Cyber risk quantification makes this happen. The process enables enterprises to assess and manage their cyber risk by stating the risk in terms of revenue, profit and cost. This is necessary because most retailers do not have a clear understanding of where they face attacks. They may not know how frequent or severe various types of attacks are in their IT estate. Nor do they usually have a good sense of what it will cost them to deal with an attack.

Cyber risk quantification solves these problems by analyzing an individual retailer's unique cyber risk profile. The process looks at a retailer's specific systems and data, and how vulnerable they will be given the possible frequency and severity of attacks. For example, what will the financial losses be in the event of a major data breach? This would include the costs of addressing the attack in technical terms, legal costs, customer notification costs, litigation costs and so forth. It also evaluates typical loss data from a retailer's industry peers.

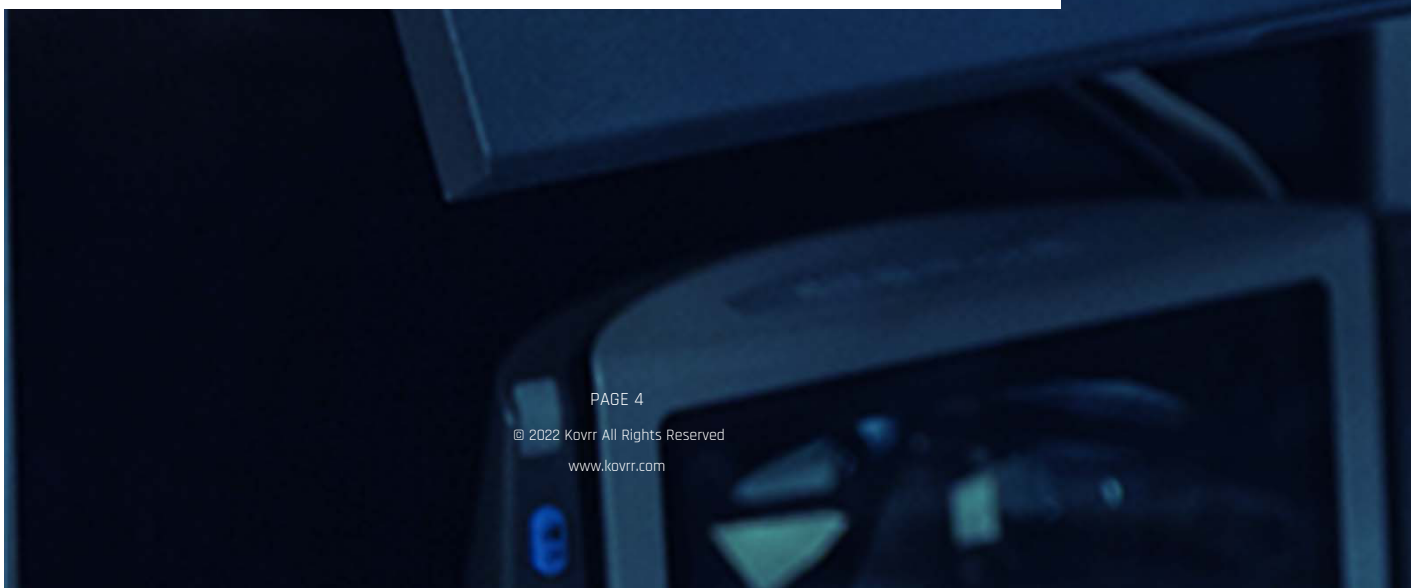
The cyber risk quantification process looks at the retailer's potential for cyber resiliency, along with the strength of its security controls. From this multi-model analysis, cyber risk quantification will arrive at an estimate of potential financial loss by attack type. With this information, IT and security managers can determine the optimal areas for cybersecurity investments and discuss them with business stakeholders.

Cybersecurity Risk Use Cases

Retailers face the same types of threats as other businesses, though the nature of retail and e-commerce make risk exposure more serious in a few areas. Retailers have to deal with cloud-based botnets, which can cause denial of service (DoS) attacks, as well as misuse of near field communications (NFCs), which are used for payments. The point of sale (PoS) system used by retailers is a distinct locus of vulnerability. A lack of point-to-point encryption (P2PE) in PoS systems can expose them to attackers.

Other cybersecurity risk use cases affecting retailers include:

- Phishing attacks—targeting employees and partners of the retailer, with the goal of gaining access to customer data. Customers can also be tricked by phishing attacks that purport to be from the retailer, which can enable account takeover.
- Ransomware—making critical data unavailable to the retailer, which threatens to disrupt the business until a ransom is paid.
- Data breaches—targeting customer PII and payment card data. Hackers can use this information for account takeovers and fraudulent purchases. They can also sell the PII on the dark web.
- Attacks on devices—exploiting vulnerabilities on network endpoints like IoT sensors, security cameras, PoS systems and hand-held computers used in the retail business.



Introducing Kovrr for Financial Quantification for Enterprise Cyber Risk

Kovrr offers a solution for quantifying cyber risk. Kovrr Quantum is a groundbreaking on-demand solution that leverages global threat intelligence and financial impact data from cyber incidents—giving users the ability to drill down into cyber event examples, including risk vectors associated with an attack, types of damage and other relevant data.

Quantum leverages multiple modeling technologies with the goal of differentiating between systemic or targeted attacks and failures. Its approach covers hundreds of thousands of simulated cyber events to output the most accurate quantification metrics possible. Users can also enact simulated scenarios to understand where their cyber security risks are concentrated. The solution offers details of an attack scenario's financial impact on the business.

Using Quantum, security, IT and business stakeholders can quickly and efficiently identify the underlying issues that drive financial exposure from cyber threats. They can assess the return on investment (ROI) for cybersecurity investments. They can also prioritize cyber risk management decisions. The overall approach cuts down the time required to make risk management decisions and contributes to the realization of greater value from the process.

Retail Shifts in the Approach to Cybersecurity Moving Forward

Retailers are taking the increasingly hostile cyber threat landscape seriously. In response, they are taking actions like deploying secure software-defined wide area networks (SD-WANs), which reduce network attack vulnerabilities. They are embracing the zero trust (ZT) model of security, which limits user privileges, especially for those that access retailers' networks remotely. Authentication controls are getting stronger, too, among many other enhancements to security countermeasures in the retail sector.

With Cyber risk quantification, a retailer can decide which technologies will make the most sense to improve its security posture. Stakeholders from security, business and IT can come together to discuss cyber defense strategies using a common business language of risk and money. With this approach, a retailer can make progress toward becoming more secure—and then measure how well the plan worked out.

> Want to see how Kovrr can help your company financially quantify cyber risk? Get a free ransomware analysis today!

The Author

Gil Hazaz

VP Sales

About Kovrr

Kovrr's cyber risk modeling platform delivers global (re)insurers and enterprises transparent data-driven insights into their cyber risk exposures. The Kovrr platform is designed to help chief risk officers, chief information security officers, underwriters, exposure managers, risk professionals and catastrophe modelers understand, financially quantify and manage cyber risk by utilizing AI-powered risk models. To learn more please contact the Kovrr team: contact@kovrr.com