Research Note

Information Security in the Rise of E-Commerce

Miranda Lin

Published: August 2018
Written: December 2018

Keywords: e-commerce; information security; retail industry; online retail; payment processing.

Abstract: As the popularity and frequency of online shopping (also referred to as e-commerce) rises across the globe, companies selling products and services online are also gathering, storing, and processing an increasingly massive collection of financial and personal information on their customers. In order to ward off hackers attempting to access this sensitive data, effective management of information security is increasingly important to prevent cyber-attacks. Various cybersecurity guidelines are available for retailers to implement, but there are still a handful of companies that are not extracting value from these guidelines. E-commerce companies need to realize that the it is in their best interests to take the initiative.

E-commerce has been growing at a substantial rate around the world, connecting merchants and consumers across countries. Traditional brick and mortar stores are increasing their presence online to offer customers a convenient way to shop without needing to travel to the physical store. Of course, businesses that operate solely online are important players of e-commerce as well. Companies like Amazon and eBay provide the platform for anyone to sell products and services to anyone in the world. Though we are more interconnected than ever, the risks we are exposed to as merchants and consumers have increased. As consumers, we provide personal and financial data to e-commerce companies, which gets stored in their databases. Consider Amazon, whose number of active customers in 2016 was reportedly 310 million; the significant amount of sensitive data stored for the customers makes Amazon's databases a natural target for hackers.[1] Thus, any type of security incident that could possibly occur for online retailers would leave its customers' personal identifiable information exposed, and place the company's operations and reputation at risk. Laws and regulations pertaining to security on e-commerce operations are limited, complicated, and vary depending on location.[2] Regardless of whether there are laws in place that force companies to abide by best practices, it is certainly in the company's best interest to do so to protect their assets and earn the trust and loyalty of customers.

The growth of e-commerce in the U.S., and on the international platform cannot be ignored. In 2016, the U.S.'s e-commerce sales were at 291.8 billion; this is a more than 100 billion increase from 2012, when the sales were at 186 billion.[3] Globally, in 2016, the e-commerce sales were at 1.9 trillion, and by the end of 2017, it's expected to be at 2.3 trillion. By 2021, sales are predicted to be at 4.5 trillion. This would mean that sales are expected to more than triple in a range of 7 years, from 2014, when the sales were at 1.3 trillion, to the predicted 4.5 trillion sales in 2021. The largest e-commerce market in the world is China, with its e-commerce sales at approximately 672 billion. Other countries with a prominent market include the U.S., U.K., Japan, and Germany.[4] According to the Nielsen Global Connected Commerce Survey from 2016 that collected responses from 26 countries, 57% of the respondents "who made an online purchase in the past six months say they bought from an overseas retailer". Evidently, shoppers are "increasingly looking outside their country's borders" when shopping.[5] Though e-commerce operates across borders, governmental agencies have very limited powers to

regulate processes that reach beyond its national jurisdiction. Thus, e-commerce companies themselves need to be deliberate in taking all the necessary precautions to protect its customers' sensitive data. This paper will focus on e-commerce companies' operations in the U.S., the risks these companies are exposed to in the occurrence of a security breach, and recommendations for them to manage their information security.

Managing information security is critical for online retailers to prevent security breaches and to keep their internal informational assets safe, especially with the proliferation of cybersecurity attacks in the e-commerce industry. Over 100 million attacks occurred between July and September of 2017, which is a 100% growth compared to the same period from 2015. Additionally, we can expect to see the "return of the 'Cybercrime Christmas'", when more attacks will occur with the increase in online transactions for the upcoming holiday shopping season.[6] The most common types of cyber-attacks against e-commerce sites include, but are not limited to, denial of service attacks, cross-site scripting, and SQL injections. Denial of service attacks occur when the attacker, often using botnets, floods the e-commerce website with fake traffic to overwhelm the network. This causes the e-commerce site to be extremely slow, and may even bring the whole site down to failure.[7] A successful denial of service attack would be especially detrimental in the holiday shopping season, when interruptions could cause the e-commerce company a substantial loss in revenue. Take e-commerce giant, Amazon, for example; a 20-minute outage on its online store in March of 2016 costed them an estimated $3.75 million.[8] The other two common types of cyber-attacks mentioned, cross-site scripting and SQL injections, both involve the attacker inserting malicious code into the legitimate website. In cross-site scripting, or XSS, the code injected can trick the user's browser into believing that the script is from the website and can be trusted, which allows the script to be executed. Depending on the type of malicious code inserted, consequences vary. For example, a specific script could allow the attacker to access the user's session cookies and use that to impersonate them.[9] Whereas cross-site scripting focuses on obtaining information from the user, SQL injection attacks focus on obtaining information from the company. In inserting SQL commands on a vulnerable website, the attacker can read information from the company's database. For example, a specific SQL command could allow consumers' name, birthday, and postal address to be displayed to the attacker.[7] XSS and SQL injection attacks are well-known and can be prevented by running penetration tests, but, there remains a countless number of other attacks that are more difficult to know beforehand.

Being prominent e-commerce players in the U.S. that have also established an apparent presence in the international e-commerce industry, Amazon and eBay have both unfortunately experienced cyber security incidents that are concerning to their operations. Founded in 1995 in San Francisco, eBay is thriving as an e-commerce company with 168 million active buyers from 190 markets.[10] In May of 2014, they informed the public of a cybersecurity breach that occurred sometime between late February and early March, which had only been detected by the company two weeks before disclosing to the public. In the incident, attackers gained access to three corporate employees' account to obtain 145 million users' information contained in eBay's database. The information retrieved by the hackers include users' name, email address, postal address, phone number, birthday, as well as the encrypted password associated with the eBay account. eBay claimed that they used "proprietary hashing and salting technology to protect the passwords"; assuming this is true, hackers would undeniably have an extremely difficult time in unencrypting the passwords, thus this is less of a concern compared to the other unencrypted data.[11] The unencrypted personal identifiable data is concerning because it could easily be used by hackers to commit fraud outside of eBay, such as registering for various fake accounts online. Now three years after the security breach, there is still a lack of news on how the hackers were able to gain access to the three corporate employees' account. However, some individuals, such as Liron Damri, a former security technologist at PayPal and the current chief operations officer of the security company, Forter, believe that "the breach was likely the result of some form of 'social engineering'", where the employees were

"tricked into handing over critical information to a cyber-crook posing as a trusted person or party within eBay".[12]

Besides massive data breaches like the one eBay experienced in 2014, there are also countless smaller scale cyber-attacks against online retailers that we can expect to be constantly happening. For instance, in April of 2017, news regarding an increase in attacks on Amazon's third-party merchants surfaced. These third-party merchants, numbering roughly two million, account for more than half the sales on Amazon's e-commerce website. Some of the fraudulent activities executed by hackers include changing "the bank-deposit information on Amazon accounts of active sellers to steal tens of thousands of dollars from each", and posting "nonexistent merchandise for sale at steep discounts in an attempt to pocket the cash". The hackers were able to gain access to sellers' account through the dark web, where hackers trade and obtain "email and password credentials stolen from previously hacked accounts".[13] It would be unsurprising to also see some of the information hacked from eBay revealed on the dark web and be used for similar purposes as the attacks on Amazon's third-party sellers.

E-commerce companies share many similar processes and technologies in their operations, making them all susceptible to similar threats. Thankfully, there are some regulations enforced on the companies. One of the well-known regulations enforced is the Federal Trade Commission Act. The FTC Act serves to protect consumers, and it has been "applied to...online privacy and data security policies". For example, the Commission has "brought many enforcement actions against companies failing to comply with posted privacy policies". Other than federal regulations, states have also enacted their own laws involving information security. As of April 2017, every state except Alabama and South Dakota passed laws requiring companies to notify the public of all security breaches that involve the exposure of personal information.[2] Another regulation is the Payment Card Industry Data Security Standard (PCI DSS), which relates to online payment systems. All businesses accepting payment cards such as credit and debit cards, must follow this standard, which includes requirements such as maintaining a firewall and testing security network and systems on a regular basis. In enforcing compliance with the PCI DSS, individual payment brands, such as Visa, determine their own non-compliance penalties.[14] Though these regulations exist, there isn't a federally enforced set of cybersecurity practices that online retailers are required to follow. This makes it possible for companies to lack implementation of even the most basic security practices, such as data encryption. Therefore, it is up to the company itself to research for and embed appropriate security practices in their information security systems. Luckily, numerous guidelines developed by governmental agencies and private parties exist for e-commerce companies to consider. Guidelines specifically for online retailers include the Organization for Economic Co-operation and Development (OECD)'s "Consumer Protection in E-commerce" guideline which was "designed to address the newest developments in e-commerce, such as...mobile transactions and payments, and new platforms that enable consumer-to-consumer transaction".[15] The Federal Trade Commission also has a "Electronic Commerce: Selling Internationally" guideline that provides broad guidance on e-commerce security and consumer protection.[16] The National Institute of Standards and Technology (NIST)'s Cybersecurity Framework also provides a comprehensive set of "cybersecurity activities, outcomes, and informative references" to help organizations "align its cybersecurity activities with its business requirements, risk tolerances, and resources". The Framework was designed for critical infrastructure systems, but e-commerce companies can certainly find value in this document too.[17] From a public perspective, it's difficult to know whether an e-commerce company follows the guidelines mentioned, unless the company itself claims so. However, it's important to note that these guidelines cannot positively impact the company unless it's adopted. When a company chooses not to follow a guideline, these valuable guidelines remain just another piece of document.

Though each e-commerce company operates differently and vary in size of their business, the risks they face in the event of cyber-attacks are similar. One of the major risk is the company's information security. Risks in this area increase when unauthorized individual(s) gain access to a company's informational assets, which may include customer and employee's sensitive data, as well as the company's intellectual property. With data exposed, the likelihood of reputational risks occurring increases, because the public loses trust in the affected e-commerce company. This causes a direct loss for the company because people are less likely to purchase products from them. Stock price may also fall as the public deem the untrustworthy company's stocks to be less valuable. Reputational risks may also occur when an online retailer experiences system failure, which could occur from internal inadequacies or external attacks. Internally, if the company uses weak hardware and/or software filled with bugs, it may cause their web applications to crash. For operations that depends on those systems and are intolerant of interruptions, consequences could be extremely destructive. Externally, when hackers successfully carry out a denial of service attack and slows down or brings down the e-commerce website, customers are unable to shop when they want to. If the system is down for a long period, the online retailer will certainly be labeled with a bad reputation, causing them to lose customers. Lastly, for any of the risks mentioned, whether information security, reputational, or system failure risks, the increased likelihood of them occurring can result from third-party's negligence. E-commerce companies are engaged in close-knit relationships with various third parties, such as manufacturers, payment processing companies, or third-party merchants using the company's e-commerce platform. Each third-party introduces operational risks if they can't deliver their part of the service or if they experience cyber-attacks that puts the information shared between them and the e-commerce company in compromise.

Though it's impossible for e-commerce companies to prevent all cyber-attacks, there are various practices companies need to follow to reduce the likelihood of attacks, and thus reduce their exposure to the risks mentioned. Regarding third party risks, e-commerce companies need to establish clear communication with all third-party vendors to address both parties' concerns. In a study done by Ponemon Institute and sponsored by Shared Assessments, of the 617 individuals involved in the "risk management process in their organizations", only 18% "say they assess the cyber security risks of most third parties". This is concerning, considering that the organizations behind these respondents "spent an average of approximately $10 million to respond to a security incident as a result of negligent or malicious third parties". Thus, it's necessary for e-commerce companies to ensure that third parties are following best security practices, such as embedding up to date anti-virus and intrusion detection technology in their network.[18] If necessary, online retailers need to bind third parties in contract.

Next, strong tone at the top is also of vital importance to e-commerce companies. To build an influencing culture around risk management, companies need to first and foremost, educate employees on the most common types of cyber-attacks and what behaviors they need to avoid to prevent security incidents from happening. For instance, employees need to be aware of phishing scams and the various social engineering techniques used so they can be cautious around suspicious emails or phone calls.

To address system failure risks, e-commerce companies need to establish redundancy. One way this can be achieved is by contracting with a secondary DNS provider. This allows "a domain's query traffic" to be distributed between providers so that if one is unavailable, the other takes over and serves "with virtually no effects to end-users".[19] As for protecting informational assets, e-commerce companies need to have a comprehensive understanding of their assets. This should be done through careful identification, prioritization, and documentation of all data and databases, so companies are aware of what to monitor for suspicious activity. For instance, after identifying a sensitive database, companies should closely monitor that database's logs to detect abnormal logins from unauthorized personnel or authorized personnel who stay logged in to the

database for an abnormal duration. Then, to actively protect these assets, basic preventative controls need to be implemented. This includes encrypting all data and salting and hashing any passwords that are stored. The principle of least privilege should also be applied so only those who need to access sensitive databases for job purposes are authorized. Furthermore, to detect if the assets are vulnerable to attacks, companies need to behave like the adversary and run comprehensive vulnerability scans and penetration tests on a regular basis.

There are also various detective controls specific to the e-commerce industry to protect consumers. Online retailers need to closely monitor all "devices and accounts that have a history of fraudulent activity" and "block these devices from transactions" if necessary. Retailers also need to "screen transactions using previous transaction data" so abnormalities can be detected early. Transactions "originating from a different country or IP address than where the [customer's] account was created" would also require additional monitoring.[20] Lastly, companies need to keep up to date with all the latest cybersecurity breaches by allocating time and resource to research cyber-attacks and preventative methods, as well as time to attend cybersecurity related conferences to discuss current events and collaborate with others in the industry.

In the rise of e-commerce, online retailers are storing more consumers' data than ever, making them targets for hackers. As a result, effective management of information security becomes increasingly important to prevent cyber-attacks to reduce the likelihood of operational risks occurring. Various cybersecurity guidelines are available for retailers to implement, but there are still a handful of companies that are not extracting value from these guidelines. E-commerce companies need to realize that the effects of not adhering to best security practices can be detrimental as cyber-attacks and security breaches result in lost revenue, customers, and a bad reputation. Though no laws in the U.S. force these private companies to follow a predetermined set of controls, it is in the best interest of these online retailers to take the initiative in carefully managing their information security to stay in business.

---

[1] "Number of active Amazon customer accounts worldwide from 1st quarter 2013 to 1st quarter 2016". Statista. 2016. Accessed 28 Nov. 2017 <https://www.statista.com/statistics/476196/number-of-active-amazon-customer-accounts-quarter/>.

[2] Jolly, Ieuan. "Data protection in the United States: overview". Thomson Reuters. 01 July 217. Accessed 20 Nov. 2017 <https://content.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true&bhcp=1>.

[3] "Desktop retail e-commerce sales in the United States from 2002 to 2016". Statista. 2016. Accessed 25 Nov. 2017 <https://www.statista.com/statistics/273424/retail-e-commerce-sales-in-the-united-states/>.

[4] Orendorff, Aaron. "Global Ecommerce Statistics [Infographic] and 10 International Growth Trends You Need to Know". Shopify Plus. 1 Sept. 2017. Accessed 24 Nov. 2017 <https://www.shopify.com/enterprise/global-ecommerce-statistics>.

[5] "Connected Commerce is Creating Buyers Without Borders". Nielsen. 20 Jan. 2016. Accessed 30 Nov. 2017 <http://www.nielsen.com/us/en/insights/news/2016/connected-commerce-is-creating-buyers-without-borders.html>.

[6] *2017 Q3 Cybercrime Report*. ThreatMetrix. 2017. Accessed 25 Nov. 2017 <https://www.threatmetrix.com/digital-identity-insight/cybercrime-report/q3-2017-cybercrime-report/>.

[7] Molitor, Kerri. "How to Protect Your E-commerce Site From Cyber Attacks". Liquid Web. n.d. Accessed 26 Nov. 2017 <https://www.liquidweb.com/blog/how-to-protect-your-ecommerce-site-from-cyber-attacks/>.

[8] Stambor, Zak. "How much did Amazon's outage cost the online giant?" Digital Commerce 360. 11 Mar. 2016. Accessed 30 Nov.

2017 <https://www.digitalcommerce360.com/2016/03/11/how-much-did-amazons-outage-cost-online-giant/>.

[9] "Cross-site Scripting (XSS) Attack". Acunetix. n.d. Accessed 25 Nov. 2017 <https://www.acunetix.com/websitesecurity/cross-site-scripting/>.

[10] "Who We Are". eBay. n.d. Accessed 30 Nov. 2017 <https://www.ebayinc.com/our-company/who-we-are/>.

[11] Finkle, Jim, et al. "EBay asks 145 million users to change passwords after cyber attack". Reuters. 21 May 2014. Accessed 19 Nov. 2017 <https://www.reuters.com/article/us-ebay-password/ebay-asks-145-million-users-to-change-passwords-after-cyber-attack-idUSBREA4K0B420140521>.

[12] Quittner, Jeremy. "How the Once Impregnable EBay Fell Victim to Hackers (And You Can too)". Inc. 30 May 2014. Accessed 30 Nov. 2017 <https://www.inc.com/jeremy-quittner/new-details-emerge-on-ebay-hack-attack.html>.

[13] "Amazon.com's Third Party Sellers Hit By Hackers". Fox Business. 10 Apr. 2017. Accessed 19 Nov. 2017 <http://www.foxbusiness.com/markets/2017/04/10/amazon-coms-third-party-sellers-hit-by-hackers.html>.

[14] "Managing Payment Security". PCI Security Standards Council. n.d. Accessed 25 Nov. 2017 <https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security>.

[15] "FTC Welcomes Revised OECD Guidelines for E-commerce". Federal Trade Commission. 4 Apr. 2016. Accessed 25 Nov. 2017 <https://www.ftc.gov/news-events/press-releases/2016/04/ftc-welcomes-revised-oecd-guidelines-e-commerce>.

[16] *Electronic Commerce: Selling Internationally.* Federal Trade Commission. Mar 200. Accessed 25 Nov. 2017 <https://www.ftc.gov/system/files/documents/plain-language/alt067-electronic-commerce-selling-internationally-guide-businesses.pdf>.

[17] *Framework for Improving Critical Infrastructure Cybersecurity.* National Institute of Standards and Technology. 12 Feb. 2014. Accessed 25 Nov. 2017 <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>.

[18] *Tone at the Top and Third Party Risk.* Ponemon Institute LLC and Shared Assessments. May 2016. Accessed 31 Oct. 2017 <https://sharedassessments.org/wp-content/uploads/2017/06/SA-2016-Ponemon-Study-Tone-At-The-Top-And-Third-Party-Risk-Final.pdf>.

[19] "65% of Top 100 Retail Domains are at Risk of Single DNS Provider Outages". DNS Made Easy. 16 Nov. 2016. Accessed 1 Dec. 2017 <http://social.dnsmadeeasy.com/news/top-retail-ecommerce-domains/>.

[20] "ThreatMetrix Study Finds Nearly 40 Percent of Retail Organizations Have No Online Fraud Prevention". ThreatMetrix. 21 Mar. 2013. Accessed 25 Nov. 2017 <https://www.threatmetrix.com/press-releases/threatmetrix-study-finds-nearly-40-percent-of-retail-organizations-have-no-online-fraud-prevention/>.