Best Buy:

Risk Assessment and Security Policy Assessment

Jeremy Willett

**Business Model Evaluation**:

Best Buy is an electronics company that utilizes brick and mortar stores and e-commerce to facilitate sales of products and services to its customers. To do this, Best Buy is constantly collecting information on their customer base to perform these sales and better serve their interests. The services provided by Best Buy extend beyond sales to include credit cards and leasing, device trade in programs, technical support services through their Geek Squad brand and installation services of products for homes, vehicles, and businesses. According to Best Buy’s Privacy Policy found on their website, “The information we collect from you includes things such as:

* Name
* Postal address
* Email address
* Phone number
* Payment card number and other payment information
* Your My Best Buy® member ID

In certain situations, we may also collect things like:

* Driver's license number (for example, if you return a product or apply for credit)
* Social Security Number (for example, if you apply for credit)
* Location information (such as when you ask us to tell you about nearby stores or use our digital properties)
* Demographic and lifestyle information (if you sign up for a registry or birthday list)
* Medical and health insurance information (for example, if you use offerings that collect medical information, such as Assured Living)
* Fingerprints (as required by law for fraud detection in connection with Best Buy’s product trade-in program)
* Facial or wrist geometry (if you choose to use Best Buy’s virtual try-on tool, with your permission your camera will scan your facial or wrist geometry. The experience is exclusively done in real time, and we do not retain data after you use this feature.)
* Survey responses” (Best Buy, 2021).

**Organization Analysis**:

Best Buy was founded in Minnesota but operates nationwide. As a result, they must take into consideration both federal and state laws in each of the states they operate in. Currently only three states in the U.S. have dedicated laws regarding Data Privacy: California, Colorado, and Virginia. California has the California Consumer Privacy Act and the California Privacy Rights Act; Colorado has the Colorado Privacy Act; and Virginia has the Consumer Data Protection Act (Data Privacy Laws by State: Comparison Charts, 2022). On a federal level, there is no overarching data privacy laws in the U.S. However, the U.S. has “a mix of laws that go by acronyms like HIPAA, FCRA, FERPA, GLBA, ECPA, COPPA, and VPPA, designed to target only specific types of data in special (often outdated) circumstances” (Klosowski, 2021). Because there are no legal regulations for companies to abide by, it falls onto more ethical standards when it comes to data usage. Companies are free to do what they want with collected data, whether that be use, share, or sell the data collected. While there are no laws dictating what a company may do with collected data, The Federal Trade Commission website states “Statutes like the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and the Federal Trade Commission Act may require you to provide reasonable security for sensitive information” (Protecting Personal Information: A Guide for Business, 2016). This means that Best Buy is obligated to “reasonably secure” the data they collect to prevent it from being accessed without authorization or stolen.

**Organization’s Information Systems**:

Best Buy follows their privacy policy regarding how they handle data. This policy can be found in all stores as well as published on their website. In this policy Best Buy explains what data they collect, what they do with it, and why they collect it. They also have listed their Vendor Privacy and Security Policy Requirements, which dictates what they require any third-party vendors to abide by when accessing any data collected by Best Buy. The website states “These Vendor Privacy and Security Policy Requirements (“Requirements”) are part of Best Buy's comprehensive privacy and security program which seeks to reduce or eliminate risk of loss to Best Buy, its employees, and its customers” (Vendor Privacy and Security Policy Requirements, 2021). Their privacy policy specifically dictates that they do not sell any personal information. The statement on their site says “Best Buy’s purpose is to enrich lives through technology. We will only collect, use, or share your personally identifiable information for that purpose. And we don’t sell (as “sell” is traditionally defined) your personally identifiable information to anyone else” (Best Buy, 2021).

To protect the information that they collect and store, they state “We use a variety of security measures designed, under a risk-based approach, to ensure the confidentiality of your information. However, as set forth in the applicable terms of use for each digital property, we cannot and do not guarantee the security of information transmitted to us” (Best Buy, 2021). While Best Buy does seem to take measures to keep information secure, they were victim to an attack in 2017 because of a cyber-attack on the company they partner with to use their online chat services. As a result of this attack, some customer payment information was accessed. Best Buy worked with law enforcement, vendors, and cybersecurity experts to determine what was accessed and to what extent (Lukic, 2020). This has been the only data breach Best Buy has suffered that has been reported on. Best Buy utilizes HTTPS and a secure SSL certificate on their site and keeps them up to date. Their internal email services are protected by SPF filtering and a DMARC policy exists to prevent fraudulent emails being sent from their domain (Best Buy, 2022).

**Cyberlaw Crimes – Investigation**:

In the result of a cyber-attack, proper response is critical. When a data breach is discovered, companies should contact law enforcement and work with cyber security experts to determine the scope of the breach, minimize the impact, control further damage, and determine the cause and the attackers. Often, companies will not have the resources necessary to do this themselves. It becomes vital for companies to recognize this and employ professionals who specialize in investigating these attacks to get to the root of it and potentially retrieve any stolen information. These professionals will “gather information, run digital forensics and track the authors of cybercrimes by working with internet service providers and telecommunications and network companies to see which websites and protocols were used in the crime” (Cyber Crime Investigation: Making a Safer Internet Space, n.d.)

**Cyberlaw Crimes – Impact**:

Cybercrimes pose a large risk to a company’s business. Failing to protect data from unauthorized and the fall out that ensues because of this can result in a large financial impact to the company. If it is found to be a fault of the company due to poor security, the company can face lawsuits and federal charges as a result. If a company fails to protect data and information, this can translate into the public turning away from the company, resulting in the business losing money over a longer period on top of the immediate financial impact. Losing the confidence of your customer base can be detrimental to a business. The public image it can attach to your company could result in the implosion of the company if things were bad enough. According to Robert Johnson, “Data breaches are one of the top concerns for today’s organizations. The costs of these breaches continue to increase, with the average global cost of a single breach hovering at $3.62 million. Beyond the financial consequences of a breach, network security is also hugely important for any business because an attack can compromise the trust of your customers. In fact, 60 percent of small companies go out of business within six months of falling victim to a data breach or cyber-attack” (Robert Johnson, 2019).

**Cyberlaw Crimes – Information Security Measures**:

Companies need to be responsible with information, especially as they continue to grow. Information must be properly stored in secure servers and protected by firewalls to prevent unauthorized digital access. Policies need to be put in place by companies to dictate how their employees handle and use customer information to prevent mishandling resulting in it being stolen. Malware Protection, Strong Password Policies, Regular review of network alerts, error reports, performance, and traffic, Installing firewalls, Instructing end users to report suspicious activity, File integrity monitoring, Regular risk assessments, and Incident and failure response strategies should all be utilized to combat against unauthorized access and maintain a solid organizational security strategy (Robert Johnson, 2019).

**Cyber-Crime and E-Commerce - Information Systems Security Measures**:

There are multiple ways information can be accessed from Best Buy. Employees can access it as well as third party vendors. Best Buy utilizes internal trainings to educate employees on phishing and malware attempts made through company E-mail addresses. It also has policies in place dictating when customers can and cannot access customer information and how it is to be handled when they do. Customer information can only be accessed when necessary for the service of a customer. It is against policy to freely search this information and must be job related. Any computer or device that can access information must be properly locked when not in use. Computers and devices are not to be left unattended when signed into and accessible. Best Buy also requires any third-party vendor they partner with to abide by strict rules and policies about how customer information is used and accessed. Their Vendor Privacy and Security Policy Requirements state all the requirements a vendor must implement to gain access to this information. Section 3 of this policy states “Vendor will implement appropriate administrative, technical, and physical safeguards to ensure the privacy, confidentiality, integrity, and availability of Best Buy Data and Best Buy Systems, if and as applicable” (Vendor Privacy and Security Policy Requirements, 2021). The document lists all the requirements necessary to gain partnership.

Best Buy also has a reporting form for any person who may find a security bug or vulnerability on their systems or site. This is done to pay any party who finds and reports any security threats missed by Best Buy’s team of security professionals. Their Responsible Disclosure Policy governs anyone reporting to the form and lists the following guidelines:

* Do not disclose the potential security issue to any third party without Best Buy’s prior written permission.
* Avoid privacy violations, destruction of data, and interruption or degradation of our service. Only interact with accounts you own or with explicit permission of the account holder.
* Do not engage in any denial of service.
* Do not engage in any spamming of our customers or potential customers.
* Do not engage in social engineering (including phishing) of Best Buy employees or contractors.
* Do not engage in any physical attempts against Best Buy property or data centers.
* Once a report is submitted, Best Buy commits to provide prompt acknowledgement of receipt of all reports (within two business days of submission) and will keep you reasonably informed of the status of any validated vulnerability that you report through this program.
* Submitted reports are received and processed by a third-party provider of Best Buy.
* You give us the right to use the content of your report for any purpose.
* Submission of a report does not create a consumer, employment, or agency relationship between you and Best Buy.
* Payment of any reward is made at Best Buy’s sole discretion.
* Best Buy may update this policy from time to time.

**Cyber-Crime and Ecommerce - Cyberlaw Protection**:

Best Buy’s utilization of policies to control access of information whether internally or externally has allowed them to protect the information they collect and keep on file. Proper employee training, internal policies regarding how and when information is accessed, prevention against phishing and malware scams and steps taken to keep information secure have allowed Best Buy to maintain a level of protection that was only compromised briefly by an outside source through a third party. While this could have been mitigated by minimizing third party access to payment information, overall, the company has done well to protect against outside intrusion.

**Organizational Security Policy**:

Proper protection of company data is vital to business success and growth. The biggest source of risk is in the brick-and-mortar stores. To protect information, guidelines need to be followed to ensure proper protection of company and customer information. Because each store has multiple computers that double as point of sale stations positioned throughout the store, a “Clean Desk” policy will be in place. “A clean desk policy focuses on the protection of physical assets and information. Ideally, this policy will ensure that all sensitive and confidential materials are locked away or otherwise secured when not in use or an employee leaves their desk” (Zhao, 2022). This policy will dictate that when not in use, all computers are to be logged out of. Whether it is the P.O.S. software of the employee toolkit software, if a computer is not actively in use, it shall be logged out of and inaccessible without employee credentials. This will prevent obvious access to Best Buy systems containing sensitive data. To supplement, no customer information will be accessed unless necessary for the current job function. When assisting a customer, their account data can be accessed when needed to assist this customer however all unnecessary access is prohibited.

The use of non-Best Buy approved devices on company computers is prohibited. No employee shall use a device that plugs into a computer on the company network without prior authorization to do so. If a Best Buy device is issued to an employee, that employee is responsible for maintain that device. In the event that the device is lost or stolen, the employee shall inform their leader and the company Open and Honest hotline as soon as it realized the device was lost or stolen. Leaders will work with the hotline to direct what needs to be done to report this to the proper authorities and the hotline will inform the proper IT staff to try and disable the device remotely and prevent it from being accessed.

To give our employees the knowledge and awareness to protect information, all employees will take information security trainings that cover company policy and best practices to minimize risk from employee error. These trainings will be completed yearly and will be updated with the most current laws and policies. Training will cover best practices and policies on the use of company computers, accessing the company network, recognition of phishing attempts and proper email use, proper internet use, accessing customer data and more as they are deemed necessary. The company will put in place a firewall on the store networks to prevent access to websites that pose threats. While it is understood that it is necessary to be able to search the internet for product information, there are several categories of websites that are not necessary to provide excellent customer service to our clients. Personal email, social networking and some media sites will be blocked from access on the network. This is to ensure that personal emails containing phishing links are not accessed on the network. The same applies to social networking and media sites.

Best Buy will continue to educate employees through training, newsletters, and face to face trainings with leadership in each store. The training employees receive will cover information security policies and practices as well as coaching and training in ethics, customer interaction and product knowledge.

Controlling unnecessary risk is important in minimizing the impact of any data breach that could be suffered in the future. To this end, the company shall only retain unused customer information for a period of 10 years. Any information that has gone un-accessed and unused for this period of time will be deleted from the systems. Any physical copies of information the store may have will be properly discarded of using a company such a Shred-It, who will collect the information and dispose of it securely and properly. The goal of this policy is to minimize risk. Some risk level is always carried when collecting sensitive information; minimization of that risk limits the impact if a data breach were to occur.

While the company and its employees can take every precaution to prevent a data breach, there still exists a chance that it occurs. In the event of a data breach, the company will work with authorities and cybersecurity experts to determine the extent of the breach. The company will be open and honest with the public in the event of such an event and will do everything within its power to resolve the issue. The company will issue an incident response plan to provide guidelines in the event of a data breach. This policy will dictate what needs to be done and how it will be done in the event of a data breach.

Best Buy will ensure any companies partnered with us follow these same rules when it comes to using and accessing Best Buy information and subject them to a Terms of Use contract to ensure these policies are followed.

**Compliance**:

Best Buy is required to comply with the Federal Trade Commission Act section 5 which “prohibits “unfair or deceptive business practices in or affecting commerce.”” (Denny, 2016). The company also complies with the Consumer Privacy Protection Act of 2017. This act “has been designed to ensure the privacy and security of sensitive personal information, to prevent and mitigate identity theft, to provide notice of security breaches involving sensitive personal information, and to enhance law enforcement assistance and other protections against security breaches, fraudulent access, and misuse of personal information” (Federal Cybersecurity and Data Privacy Laws Directory, 2022). Best Buy also must comply with the California Consumer Privacy Act, The Virginia Consumer Data Protection Act and The Colorado Privacy Act, for the stores it operates in those states.

Best Buy has developed its’ security policies around these laws to ensure compliance with these laws. On a national level, these laws are not necessarily broad in their scope, and as an issue of ethics, Best Buy has chosen to go beyond the scope of these laws to ensure customer data is protected for the safety of our clients. By putting data security at the forefront of employee training and putting in place policies that must be followed, the company believes that it goes beyond the necessary compliance of the law and instead seeks to protect customers beyond what is “legally necessary”.

**Risks and Vulnerabilities**:

Best Buy faces risks in protecting client information. The biggest source of vulnerability for the company, as stated earlier, is in our physical stores. Best Buy’s security policy is designed to minimize the risk this poses by protecting the physical assets that allow access to the digital information housed on Best Buy’s networks. This policy expands to our corporate offices as well as any home or mobile employees the company has. Data security is a top-level concern and paramount to protecting our customers and clientele.

**Security Policy Sections**:

This policy has already dictated acceptable use of email and social media websites on company networks. As a general rule, no employee shall use the internet for personal use while on a company network. This is to prevent any preventable issues from arising from unsecure and weak websites being accessed. To further any privacy for the company and customers, no employee shall release any internal news or bulletins without proper consent from management and HR. The goal is to keep data protection and privacy at the forefront of all employees’ minds and ensure that these policies become habits to ensure they are performed every day, every shift, in their entirety to protect our customers.

# References

Best Buy. (2021, September 30). *Best Buy Privacy Hub*. Retrieved from Best Buy: https://www.bestbuy.com/site/help-topics/privacy-policy/pcmcat204400050062.c?id=pcmcat204400050062

*Best Buy*. (2022, April 09). Retrieved from UpGuard : https://www.upguard.com/security-report/bestbuy

*Cyber Crime Investigation: Making a Safer Internet Space*. (n.d.). Retrieved from Maryville University: https://online.maryville.edu/blog/cyber-crime-investigation/#what-is-cyber-crime-investigation

*Data Privacy Laws by State: Comparison Charts*. (2022, February 2). Retrieved from Bloomberg Law: https://pro.bloomberglaw.com/brief/data-privacy-laws-in-the-u-s/

Klosowski, T. (2021, September 6). *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*. Retrieved from New York Times: https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

Lukic, D. (2020, September 29). *The Story of Best Buy Data Breach*. Retrieved from ID Strong: https://www.idstrong.com/sentinel/best-buy-data-breach/

*Protecting Personal Information: A Guide for Business*. (2016, October). Retrieved from Fedreal Trade Commission: https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business

Robert Johnson, I. (2019, January 2). *60 Percent Of Small Companies Close Within 6 Months Of Being Hacked*. Retrieved from CyberCrime Magazine: https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/

*Vendor Privacy and Security Policy Requirements*. (2021, December 13). Retrieved from Best Buy Partner Portal: https://partners.bestbuy.com/-/vendor-privacy-and-security-policy

Denny, W. R. (2016, June 20). *Cybersecurity as an Unfair Practice: FTC Enforcement under Section 5 of the FTC Act*. Retrieved from American Bar Association: https://www.americanbar.org/groups/business\_law/publications/blt/2016/06/cyber\_center\_denny/

*Federal Cybersecurity and Data Privacy Laws Directory*. (2022). Retrieved from IT Governance: https://www.itgovernanceusa.com/federal-cybersecurity-and-privacy-laws

Zhao, J. (2022, April 14). *Build Strong Information Security Policy: Template & Examples*. Retrieved from Hyperproof: https://hyperproof.io/resource/information-security-policy/