SID: 1810980
Gold Cohort - Case 1

Victor Xu
Professor Simon
MSIS 512: Information Security
October 29th 2018

Checklist vs. Risk: Case 1 [HW]

Introduction:

"There are only two types of companies: those that have been hacked, and those that will be...a breach alone is not a disaster, mishandeling it is." - Robert Mueller (Former FBI Director)

The age of digital transformation has introduced undeniable conveniences in our daily lives. Tools such as FaceTime and social media have rendered the once-fetishized dream of instant communication between global diasporas a reality. Fintech projects like Amazon Go and Google Pay are playing significant roles in an accelerating cashless revolution. In certain cities - Beijing as an example - digital wallets have already become the standardized form of payment, even for simple, everyday commodities like vegetables in a farmer's market or shampoo from that mom-and-pop shop across the street. Suffice to say, gone are the days of relying on snail mail and pigeon posts for communication, or hackling over spare pennies at the store. Our daily interactions have become increasingly immediate and accelerated on a global scale.

In the media, these privileges wrought by technological innovations often overshadow the catch-up game institutional regulations play in easing out the security and ethical considerations lurking beneath the surface. For instance, what are the dangers of having our 'data doubles' - copies of our identities living across social media - copied and manipulated? What would happen to our crytowallets if our phones become physically stolen or hacked? What should be done? These are the types of shadow questions which must be answered by policymakers, across all public sectors and industries evolving to fit the needs of this information age.

The purpose of this paper is to analyze three popular compliance models ranging from healthcare (HIPPA), payment card processing (PCI), to general data protection (EU GDPR); in the process identifying their framework classifications (checklist model, risk management framework, or hybrid model), followed by a justification of why this framework was selected. By 'checklist model' the implication is an audit-friendly method of examining security, in that it is easy to confirm that necessary steps were taken or implemented. In contrast, a 'risk management framework' operates on a scale (risk itself, defined as the product of likelihood and impact) which varies from case to case. The latter takes into account the number of people using a service, the threat (intent of the actor), and vulnerability extent, to deploy the just-appropriate level of action. Finally, a 'hybrid' model applies both the checklist and risk framework depending on the circumstance. Justificatory examples for the above will be drawn from wearables, Square, and Google.

Framework Classification:

Starting with **HIPPA** (Health Insurance Portability and Accountability Act), the most appropriate classification framework would be **risk-based**, although an argument can be made for a 'hybrid' model. At the highest level, HIPPA is concerned with the risk analysis and management of healthcare information. Following HIPPA means performing regular security evaluations - being aware of evolving innovations/techniques - at the necessary level. Note that 'necessary' is synonymous with 'relative', since the risk a public hospital versus a healthcare app faces could look drastically different, despite both handling healthcare information. This language matches a risk-based management framework, with risk being calculated on a scale to determine severity, which then guides the administrative safeguards.

The place where a hybrid model might fit would be the physical (IT/technical) implementation. The process of designing physical failsafes (i.e. How often data is updated or cleaned? What are the levels of privilege?) and securing computer systems (usually Linux-based), could benefit from a structured 'checklist'. Although HIPPA does not provide a super specific list of rules, there is a general IT sector checklist, which covers broad requirements like, "Implement a means of access control...assigning a centrally-controlled unique username and PIN code for each user, but also establishing procedures to release ePHI during an emergency." (Merrell) Ultimately though, HIPAA is not a certificate of compliance or list of fixed methods, but a program that needs to be developed and actively maintained.

Moving into retail transaction and **PCI** (Payment Card Industry Data Security Standard), the framework would be a '**checklist model**'. The Payment Card Industry does not impose regulations, but rather sets an industry practice (norm), which is carried out by credit card companies. Evidence for the 'checklist' can be found in how PCI treats risk using 4 levels, divided by transactional and compliance categories. For example, PCI Compliance Level 1 (defined as having over 6 million Visa and/or Mastercard transactions processed per year, or any merchant that has had a data breach or attack that resulted in compromise) requires on-site auditing by an Qualified Security Assessor (QSA), plus network scanning by an Approved Scanning Vendor (ASV). PCI Compliance Level 2, 3, 4 (decreasing volumes of transactions, so decreasing levels of risk) would fill out a Self Assessment Questionnaire (SAQ), and get quarterly scans from an ASV. This 'four size fits all' approach is procedurally standardized, and thus characteristic of a security 'checklist' being applied.

For legal policy making through **EU GDPR** (General Data Protection Regulation), the framework which best fits would be the '**hybrid model**'. Generally speaking, government regulations expressed through law need to be enforced through objectively measurable aspects. Laws must be applied to everyone in a class, despite the difficulty in developing regulations which supports both broad and specific cases. This is particularly true when considering how the

GDPR is designed to cover the entire European Union (a collective of 28 nations). Hence, a hybrid model allows for some flexibility: using risk management to estimate the severity of what is expected to happen, followed by a checklist for faster auditing.

The 'risk management' component is tied to the notion that GDPR compliance is ongoing, evolving as policymakers make adjustments based on real-world observations. Remaining compliant requires auditing a company (examining current standing), actioning business practices as necessary, and performing regular evaluations down the road. These evaluations account for variance in scale and risk (i.e. a local shop versus an international conglomerate), both of which become reflected in the penalties for non-compliance, defined as "fining of 4% of annual global turnover or €20 Million (whichever is greater)." This means if say, Google (a global powerhouse), breached the GDPR, the amount coughed up would be far greater than a mom-and-pop shop. Logical, considering the relative risk of a data breach from Google (far greater impact if all EU citizens were subscribed to Google services) would be significantly higher as well.

At the same time, the EU GDPR, like any legal regulation, uses 'checklists' (as part of the hybrid structure) to examine general guidelines, for the sake of time-saving. The 'checklist' would contain material pertaining to areas of data protection such as: consent to information handling, data breach notifications, right to access (personal data), right to be forgotten (data removal), and data portability (movement). These general GDPR principles are applicable to all companies, big or small, which process the data of EU citizens.

Examples for each framework:

HIPPA: Wearables Market

Wearables are developing increasingly precise sensors to track vitals inclusive of: continuous heart rate, blood pressure, ECG, calories burned, skeletal muscle mass, sleep health, and blood oxygen level. Advanced models integrate A.I. algorithms to detect irregular behavior for users - triggering the attention of medical professionals or family/friends automatically. These wearables are developed by a range of companies, many which are based internationally (i.e. China/Shenzhen, Korea, U.K.). As part of the service experience, these companies must handle the storage and retrieval of users' data through smartphone apps (typically Android or iOS), with data stored on the cloud. As these technologies ripen, natural questions arise: Who has access to this health data? Furthermore, what could happen if an actor with nefarious intent accessed users' information?

Somewhat surprisingly, HIPPA policies have yet to catch up with the development of medical-grade, connected wearables. Yet broadly speaking, any entity which shares patient information to a third party service provider, is required to have a Business Associate Agreement (BAA) in place; a contract which ensures the business associates will take the necessary measures to safeguard that information. (Donovan) Still, wearables sit in a grey zone which illustrates the speed in which the healthcare space develops, but more importantly, denotes the

importance of a risk-based assessment model. Because advancements are constant and unpredictable, it makes little sense for policymakers to generate a checklist of procedures which might be outdated or completely inapplicable the next day. As such, a system which examines the risk of a entity on a relative scale, before suggesting courses for action, is the most pragmatic. The downside, of course, is the evaluation process will take longer than a checklist to implement (also making auditing more challenging), although it might be the only way to deal with complicated considerations such as administratively, who has access to what data.

PCI: Square

Square is a mobile payment company producing hardware accessories (i.e. card reader which plugs into the headphone jack) and software (reading/directing card transactions) compatible across Android and iOS devices. The platform allows for individuals across the United States, Canada, Japan, Australia, and the United Kingdom, to accept credit and debit card payments. (Square, Inc) It's not unreasonable to say that Square relies on seamless integration of standardized card payment mediums (i.e. major credit card companies such as Visa, Mastercard, American Express) to appeal to small businesses. This integration is only made possible through Square's compliance with the PCI security checklist, such that "Square uses strong encryption on its devices...its cryptographic keys are at least 2,048 bits. Neither card numbers, nor magnetic stripe data, nor security codes are stored on Square client devices...The current technology is Payment Card Industry Data Security Standard (PCI) compliant."

It makes sense for Square to adhere to the PCI checklist because ignoring these practices would likely result in being blacklisted (business-wise) by the entire payment card industry. This would destroy the premise of which Square operates on (seamless integration), if major credit cards are simply unsupported. From a policymaking perspective, this example illustrates how a checklist can be effective when the industry is already powerful and established. A checklist approach reduces costs (eliminating proprietary evaluations), generates even broader adoption, and prevents stricter intervention from the government down the line. Furthermore, being PCI compliant becomes this 'badge of honor', whereby consumers (using Square) are assured proper security practices are being integrated to keep personal transactions safe.

EU GDPR: Google/Android

The majority of Google services - including it's open-source mobile operating system, Android - are offered for free, provided that users are willing to disclose personal information to the Mountainview company. As alluded to in the introduction of this paper, by extracting a corpus of information from search histories/libraries (Google Drive, Google Photos, Maps), Google is able to generate models of our data doubles; the lives we lead on the internet. This information becomes invaluable for the purposes of targeted marketing and ads. With the GDPR, the European Union targets enterprises like Google, through regulatory actions designed to protect users' data.

In nascent news, EU fined Google €4.3 billion ($5 billion) for abusing its Android market dominance in ways such as: bundling Chrome apps and paying "large manufactures and operators" to exclusively pre-install Google search with handsets. (Warren) Google had previously been fined $2.7 billion for manipulated search results generated by users' data. Still, since the GDPR's roll-out, Google has updated it's privacy policies to improve the transparency of data between customers and commercial use. This includes clearer illustrations on how users can access their own data, including security check-ups, and advertisement controls. (Isenegger) The hybrid model is highlighted in this example, because of how the EU GDPR is performing on-going investigations on Google (it's not the same infringement being repeated on the same scale) depending on how the company is using customers' data in relation to the marketplace (constantly evolving). This level of evaluative analysis requires risk-based management to determine the severity. But at the same time, checklists are written to document how specific privacy guidelines were broken, along with their corresponding fines (making processing easier).

Summary:

In this age of digital transformations, it's more important than ever to pay attention to the compliances and regulations taking form to identify complex security and privacy considerations. This paper analyzed three popular compliance models and their framework classifications: healthcare (HIPPA, risk-based), payment card processing (PCI, checklist), and general data privacy (EU GDPR, hybrid). Drawing on examples from medical-grade wearables (as a grey zone), Square readers (operating on seamless integration of industry standards), and Google Android's tempestuous relationship with the EU, this paper illustrated how these chosen framework labels make sense from a policymaking perspective, and to a lesser extent, from the business's perspective. Consequently, we gained a deeper understanding of the implications behind these frameworks, operating on important industries in the world around us today...

Work Cited:

Donovan, Fred. "How Does HIPAA Apply to Wearable Health Technology?" *HealthITSecurity*, HealthITSecurity, 3 Oct. 2018, healthitsecurity.com/news/how-does-hipaa-apply-to-wearable-health-technology.

"HIPAA Compliance Checklist." *HIPAA Journal*, www.hipaajournal.com/hipaa-compliance-checklist/.

Isenegger, Alexandra. "What-Are-the-Effects-of-GDPR." *Quora*, 5 Feb. 2018, www.quora.com/What-are-the-effects-of-GDPR.

Merrell, Eric. "What-Are-the-HIPAA-Security-and-Privacy-Rules." *Quora*, 14 Sept. 2017, www.quora.com/What-are-the-HIPAA-Security-and-Privacy-Rules.

Square, Inc. "PCI Compliance: What You Need to Know." *Square*, squareup.com/guides/pci-compliance.

Warren, Tom. "Google Fined a Record $5 Billion by the EU for Android Antitrust Violations." *The Verge*, Vox Media, 18 July 2018, www.theverge.com/2018/7/18/17580694/google-android-eu-fine-antitrust.