2021 Information Security Report

Twitter has struggled in the past with matching the right people to the right roles in the areas of Information Security and Privacy. There has been a lot of effort but it has not yielded the impact needed to meet our requirements and obligations. We are addressing this now. This past year Privacy Engineering was pulled out of Information security. Privacy had become so critical to the company we needed to ensure this item received special focus and that we could demonstrate that we can make progress now, whereas we had struggled in the past. We brought in a new leader of Privacy Engineering, one of world class talent and a track record of significant change at scale. With this new engineering leader teamed up with our Chief Privacy Officer (from counsel) we have made more measured progress towards our obligations over the past 6 months than we have since 2018. We do this by distilling the team and their focus down to their core purpose within the company.

We are now embarking on this journey with Information Security as well. The first step, as you will see in this Top Risk document and that has been absent in the past, is that the focus is narrow and the targets are known and quantified. The progress will be modular, methodical, and well understood and tracked. We will have more detailed discussions on this in the upcoming Risk Committee meeting.

To meet regulatory obligations we will be providing quarterly Security and Privacy Risk reports to the Risk Committee focusing on progress against the top risks cited below and related regulatory investigations. Additionally, we will provide end of year reports from the Chief Information Security Officer assessing the state of our Security Program and the Chief Privacy Officer assessing the state of our Privacy and Data Protection ("PDP") Program. These end of year reports will provide evaluations of the respective programs and inform of any changes in "top risks" to the company.

Twitter's Chief Privacy Officer's 2021 review and what to expect in 2022 is complementary to this document and is provided here.

2021 Review

Through the FTC Consent, we are entering into a 20-year obligation that covers everything we do with data as a company. Information Security Incidents we are obligated to report will be under significant scrutiny from regulatory bodies from this point forward. The regulatory bodies will be looking to identify if the incidents we are reporting indicate we have systemic issues in the areas we have stated we have significantly improved or otherwise addressed and remediated. Our incident rate, and the number that met requirements for reporting to regulatory bodies, the past year must be significantly reduced going forward. From Q3 2020 through Q3 2021,[1] Twitter averaged almost 10 incidents per quarter. Over an incident per month (more than 4 per quarter met requirements to be reported to regulators. Each of these events is a significant disruption to our business operations and needs to be made a very occasional exception instead of a constant norm. Many of these issues are able to be traced back to continuing challenges across *access control* and *inappropriate (security) configurations. These risks are the root causes of our FTC and Regulatory risks, which will be addressed here, in the Privacy and Data Protection Report, and in more details at the upcoming Risk Committee meeting.*

Access Control & Exceptional Access to Production Environments

Twitter has a large number of employees with direct access to our production environment. Every Engineer joining the company is provided Production level access. For context about half of all FTE employees[2] are engineers. Best practices are for companies to only allow production access to engineers in very minimal amounts and only in extreme situations (temporarily). Development, test, and staging environments are where engineers should safely conduct the majority of their work. We do not (meaningfully) have such environments. Twitter performs nearly all of

---

[1] *Q4 2021 is still underway.*

[2] *Twitter was just shy of 8,000 FTEs as of November 30,2021, with ~4,000 engineers. A random security issue with an employee or their account would yield credentials that could access production data on average 50% of the time.*

these functions directly in production--thus requiring engineers to have production access. Further to this broad access to production, there are several pockets of exceptional access risk[3]. All of this is a-typical for security mature companies due to the risk associated with providing direct access to live customer data and the systems providing the service.

Strong access management to the various data and systems throughout Twitter's entire organization is the cornerstone to not only security and privacy but to enabling people to develop with velocity. To be explicit, access control is the primary line of defense to protect against a variety of threats (i.e., internal bad actors[4], misuse of data for otherwise legitimate business purposes as occurred in SIM-28--*which were the root cause of the current FTC issues*--accidental data spills, etc.).

Security Management of Systems and Software
Our next top risk we must report to the Board is the state of our security configuration and compliance across our client fleet (laptops and workstations) and servers. We have ~9,000 laptops in our fleet. It had been internally reported that all (about 99%) of our clients correctly have security monitoring software installed on them. Unfortunately this hid the critical aspect of what the security monitoring software was reporting. It has been revealed that more than half (58%) of our entire laptop fleet is out of security compliance, and one-third (33%) do not have software and security updates enabled on them. Additionally, out of ~450,000 servers in our data centers, 68% are running out of date kernels (the brains of the operating system)[5]. Non-patched, out of date, operating systems are present on 70k (15%) of our servers. These issues, clients and servers, represent systems that are vulnerable for exploitation and represent a lack of hygiene that is difficult to justify externally.

FTC & Regulatory i.e., Data Handling & SDLC
Identifying and remediating systemic issues within our access control and security management of systems and software is one of the objectives of the regulatory frameworks we are attempting to meet. Not only are we under obligations to address these fundamental challenges, our lack of visibility into systems and services hinders our ability to detect new and existing vulnerabilities and respond and reconstitute to incidents once identified. The challenges, and our approach to solving the challenges, of identifying accesses and data is discussed in the Privacy and Data Protection Summary and will be discussed in more detail at the upcoming Risk Committee.

A different type of risk, not being compliant with FTC obligations, that we are tracking and reporting to the FTC on is our Software Development Lifecycle (SDLC)[6]. The SDLC ("Flyway") adoption rate is currently at 87.5% against a goal of 100% of projects on the Unified Priority List ("UPL"), down slightly from 92% in Q3 and from 89% at the beginning of Q2. This does not reflect work that is not on the UPL which leaves a significant gap in achieving our overall goal of ensuring that 100% of all work that should be using our SDLC, and verifying that it is in fact doing so. This is critical as the SDLC will be the way we ensure all work that should receive specified reviews to meet our FTC obligations is in fact doing so. In Q1 2022, the team will be pushing all teams to universally adopt Flyway so that we can create better intake mechanisms to capture this work.

2022 Preview

In addition to re-focusing InfoSec on the basics in 2022, to accomplish several of the Run The Business (RTB) reductions of risks mentioned above, we launched a company wide objective (#Protect Objective) that includes critical aspects of these challenges. Combined we will make measurable--via shared dashboards--and verified progress such that:

- Client systems will be brought up to proper base hygiene within the first 3 quarters.
- Production access will be cut in half and extreme risk groups need to be brought to 20% of what they were by the end of 2022.
- Twitter will integrate identity and access management capability by the end of 2022.

---

[3] *320 people have superuser access across all systems and data within production and 250+ can remotely disable ("turn off") hardware within data centers.*
[4] See the statistics in the #Protect presentation
[5] These represent security risks and vulnerable software within the heart of the computer. This is also a PR issue should there be a compromise within our datacenters.
[6] SDLC is a formalized process that is imposed and followed in the development of software across the company.