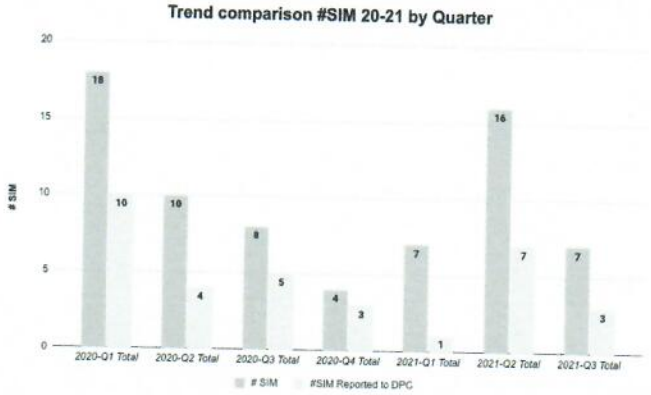
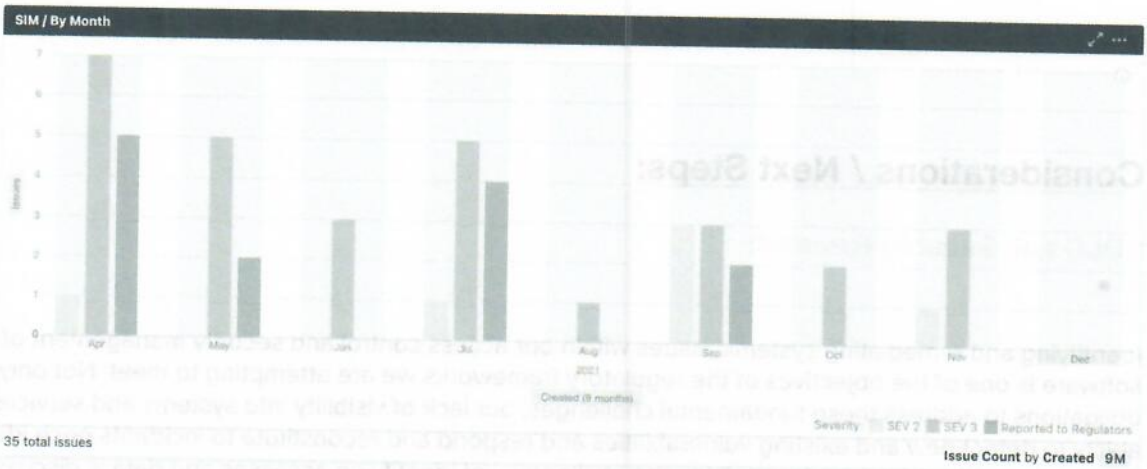
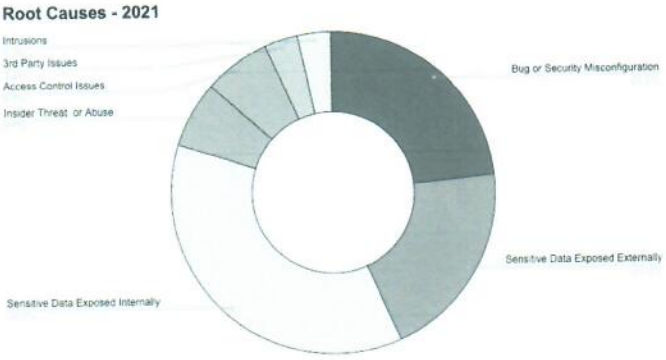




Through the FTC Consent, we are entering into a 20-year obligation that covers everything we do with data as a company. Information Security Incidents we are obligated to report will be under significant scrutiny from regulatory bodies from this point forward. The regulatory bodies will be looking to 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,[5] 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.*

[5] *Q4 2021 is still underway.*



Considerations / Next Steps:

SDLC and Security Reviews:

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.

Access Controls

Excessive (i.e., access that is not needed to perform one's function) access to data remains a significant risk. Work has slowly progressed to create some roles-based access measures but these are not where they need to be. Every new employee has access to data they do not need to have access to for the purpose of their role. Until we have implemented a mature centrally owned and operated system to manage access to data (e.g., entitlements and review, Role Based Access Controls, audits, etc) we are at risk of inappropriate access or use of data. Our inability to delete data compounds that risk, as we retain data that we should not have and which is therefore accessible by people who do not need to have access to this data.

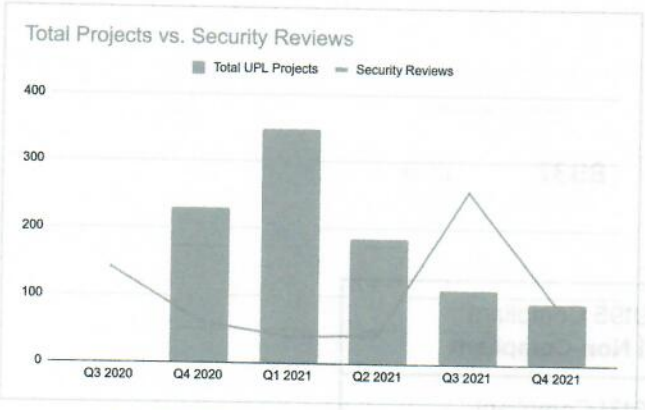
Cookies

[6] SDLC is a formalized process that is imposed and followed in the development of software across the company.

Additionally, out of ~450,000 servers in our data centers, 68% are running out of date kernels (the brains of the operating system)[4]. 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.

SDLC and Compliance

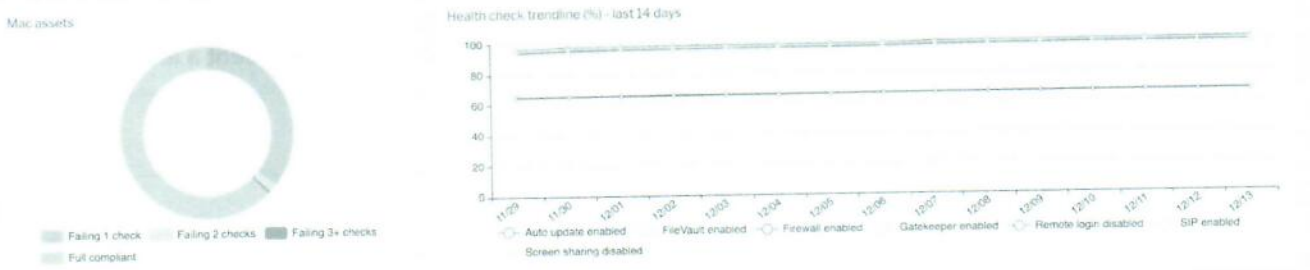
Describe SDLC and Flyway goals and why regulators are requiring these. This includes security and privac reviews. Currently a product needs to go through ~7 different reviews prior to launching. Counsel privacy, privacy engineering , information security, ... - these reviews are numerous and burdensom for the launching team to track down and comply with. We intend to unify the review process to make this a smooth single stop process, easing the burden on launching teams and consolidating the expertise and review functions into formalized, and repeatable, processes.



- It is unknown how many projects are not listed on the UPL. Teams prioritize Run The Business (RTB) projects and there are local projects that do not appear on the UPL as well. The new UPL initiative intends to restrict the UPL to the top 100 company wide projects. While this is useful for
- The highlight of this quarter for SDLC/Flyway is the adoption rate, which is currently at 87.5% against a goal of 100% of projects on the Unified Priority List, down slightly from 92% in Q3 and from 89% at the beginning of Q2 but up dramatically up from 34% at the time of the Q2 board report.

Incidents (Lagging Indicator)

[4] 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.



Application firewall enabled

9195 1

Auto update enabled

6131 3065

Filevault enabled

9114 82

Gatekeeper enabled

9159 37

Remote login disabled

8984 212

SIP configured

9120 76

Screen sharing disabled

8937 259

Application Firewall Enabled	9195 Compliant **1 Non-Compliant**
Auto Update Enabled	6131 Compliant **3065 Non-Compliant**
Filevault Enabled	9114 Compliant **82 Non-Compliant**
Gatekeeper Enabled	9159 Compliant **37 Non-Compliant**
Remote Login Disabled	8984 Compliant **212 Non-Compliant**
SIP Configured	9120 Compliant **76 Non-Compliant**
Screen Sharing Disabled	8937 Compliant **259 Non-Compliant**