At present there are 4 areas of risk, at Twitter, that are the most critical for the Twitter Board and Risk Committee to understand: Access Control, Patches and Software Updates, Software Processes and Compliance, and Incidents.

It is imperative that the Risk Committee have a clear and accurate understanding of these areas. The understanding needs to be defined through quantified measurements, not qualitative descriptions or isolated projects, and placed into larger context. What does each risk poses? How does the compare to peers (what values should we be at presently)? How do these values compare to what regulators and the larger public, and our Customers, expect? What is the priority of addressing each area?

Access Control – the total scope and breadth of our challenge at Twitter around access to information and systems.

Where is Twitter in relation to peers and expectations of regulators and Customers? What is the impact of our current situation? Where do we need to be, by when, and how are we tracking?

Patches and Software Version Compliance – Keeping Operating Systems and software correctly patched and current is considered one of the most fundamental and basic components of security hygiene. In addition to essential protection against security vulnerabilities, and disruption of operations, regulatory agencies specifically look at this to understand if an organization lacks maturity in the most rudimentary of security practices. Where is Twitter in relation to peers and expectations of regulators and Customers?

Processes and Compliance (SDLC / SDL) – Software and service development and deployment needs to go through mature uniform processes (SDLC) and be methodically evaluated for security and privacy risks through a mature Security Development Lifecycle (SDL). Decisions regarding security and privacy need to be made at the appropriate level and with global context for value v risk to the company. that decisions made in regards to security and privacy concerns

Incidents – The number, type, and frequency of issues related to security hygiene, controls, and integrity of systems and processes indicate risk that is being realized and risk that is forthcoming. This is the gauge measure whereas access control and patches and updates are levers. version compliance are levers

Access Control

Twitter is significantly behind peers and below acceptable (and industry) standards in access control. To quantify this statement Twitter is at a point analogous to where Google was in 2005-2007. Peers, and companies in general, block employees from accessing systems (and data) in production. This has been the norm for years in the industry. Production environments are sacrosanct at most companies. Not only is this because of security concerns due to live customer data and direct customer interactions but also to avoid outages and disruptions in service. A non-insignificant number of outages and operations disruptions at Twitter are due to testing and development happening in production instead of testing or staging environments.

How excessive is the access to production systems and data at Twitter? Each engineer Twitter hires (approximately half of all employees and equaling more than five thousand employees at the end of 2021) is provisioned with the ability to connect and communicate with production systems. This includes the ability to directly log in to systems in this sensitive environment.

Twitter data centers and may launch services that directly interface with production data. A range of outages at Twitter have been attributed to failed tests because they occur in production with live systems. These outages are expensive to Twitter even when not highly visible externally. They consume meaningful resources internally and interrupt other work. Numbers for outages, disruptions, and of all sizes, related to a lack of a testing and staging environment should be considered

Edge case – IPMI + SUDO + … versus main risk.

Risk Committee Misalignment Concerns

Access control is a critical path item for Privacy. Data deletion, and other regulatory obligations, require appropriate, mature, access control. Regulators and our Customers/Users are under the belief that Twitter has more mature, and enforced, access controls than are present. At the end of 2021 there is not a concrete plan to address access control on which IT, Engineering, Privacy, and InfoSec are aligned.