MX

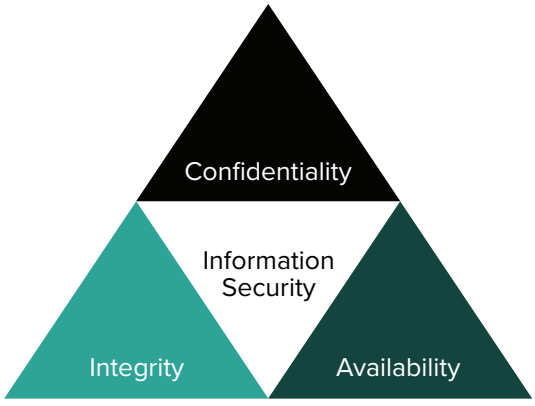
SECURITY PRIMER

FOR FINTECH COMPANIES

Consumer privacy concerns as they relate to the digital world continue to grow. Consumers not only want to know what data points you are collecting, they also want to know what you intend on using them for and for how long. It is for this reason that the intent of the data's use must be made clear to the end user. Historically, it has been assumed that obtaining consent to harvest a specific data point is all that is needed for proper disclosure. Today, it is important that users have a clear and transparent understanding of how their data will be used to benefit them, and also how it might benefit other parties.

SECURE DATA HANDLING

Data security encompasses two fundamental areas, ensuring that data 1. retains its integrity and 2. is only accessible to those authorized to access it. Proper understanding of the access requirements and requisite sensitivity of the data involves taking the time to develop data classifications and corresponding security controls.



To develop these controls, it is important to understand that data security involves two contexts as well – data-at-rest and data-in-transit. While the need for confidentiality and integrity remain for each context, achieving this in each case requires specific strategies. Data-at-rest security often involves field level or full disk encryption while data-in-transit relates to encrypted protocols for data transmission.

Encryption of data alone is not enough; proper implementation and key management practices are pivotal in ensuring data is properly secured. It is for this reason that well-respected encryption libraries and protocols should be used for each context.

PURPOSEFUL DEVELOPMENT

The excitement that comes from innovating and trailblazing can often lead to making hasty unplanned choices that we intend to address in the future. Purposeful development involves developing systems that have a specific focus and function. Leveraging discrete units of software with a specific function, inputs and outputs facilitates proper architecture, development, integration and testing. Building software in this manner requires planning and discipline and reduces your attack surface area. This practice liberates you to make changes quicker and with more confidence that your platform will remain stable. In the event that security issues are detected issues can be quickly isolated to the affected service and changes rapidly deployed that remediate the issue.

The keystone of purposeful development is establishing a software development lifecycle (SDLC). DevOps style development allows for small incremental changes which can be quickly reviewed by security teams, ensuring that security issues are addressed in their infancy and can be easily remediated. Follow advice from OWASP, NIST and SANS to develop an appropriate SDLC for your organization.

PRIVACY AND AUTHORIZED ACCESS

Consumer privacy concern as it relates to the digital world continues to grow. Consumers not only want to know what data points you are collecting, they also want to know what you intend on using them for, and for how long the data will be used. It is for this reason that the intent behind why, data is used must be made clear to the end user. It's assumed that only obtaining consent to harvest a specific data point is all that is needed for proper disclosure. Instead it is important that users have a clear and transparent understanding of how their data will be used to benefit them and also how it might benefit other parties.

To round this out, it's important for systems to be developed in such a way that users can clearly see what they have consented to. This framework should also allow users to grant and revoke access as they see fit. Clearly defining the intent behind the data points they are granting access to will empower consumers to understand where they are sharing their data and why. This fosters a relationship of trust and enables a user to take ownership of their data.

MONITORING AND RAPID RESPONSE

A good security program is one that understands its risks and associated threats. This is evidenced by thoughtful monitoring and response planning. Controls should continually be monitored for their effectiveness and layered in such a way that one failure cannot cascade through the organization. Monitoring should include not only control status, but active security events. These events should be reviewed and related back to the organization so as the threat landscape evolves, changes can be made to controls.

Building out systems which can accommodate change in a rapid manner are essential in architecting for rapid response to security instances. To do this, an organization has to invest the time and resources necessary to gain clear situational awareness in all aspects of the organization. Coupling this with tools that enable flexible data acquisition and analysis is the difference between being in command of a security incident, or the victim of one.

CONCLUSION

Many organizations get caught up in the regulatory burden that comes with maintaining, storing, and manipulating financial data. Caution must be exercised to ensure decisions are made to guarantee the needle continues movingforward towards what is best for our patrons and not only what checks off the most regulatory boxes. This mindset ensures our efforts best serve our end users. Doing the bare minimum doesn't cut it. Waiting for appropriate legislation or regulation puts an organization into a situation where they will be told what to do, instead of doing what is best for themselves. The friction which can arise from this approach, at best, hampers innovation and, at worst, can cripple an organization.