There are many mistakes and oversights that startups across all industries have fallen prey to when it comes to cybersecurity. The typical trope that you can never start to consider cybersecurity too soon can apply in many of these cases. However, even startups that implemented cybersecurity early in the design and build of their business have missteps and mistakes that can set them back as they grow or hit explosive growth. So, how does a startup attempt to avoid some of the big mistakes? Invest in cybersecurity, just like the business is going to invest in platform build, going to market, and funding. Make cybersecurity a cornerstone of the business early, so that it becomes a part of the fabric of the business.

# Build a Cybersecurity Strategy

To integrate and make cybersecurity a key foundational discipline, startups should make sure to spend time on a cybersecurity strategy early. While many founders and technology leaders will be focused on disrupting the marketing and building a go-to-market strategy, a key component will be missing, if cybersecurity is not considered. The current climate nearly necessitates startups to consider the requirements of both consumer and business customers’ security requirements. To do this, the startup should consider the following items as the cybersecurity strategy is built.

## Data Security and Data Privacy

Do not mistake data security and data privacy as the same discipline. Data security is focused on protecting the data in transit, at rest, and managing where it is moving to/from. A key component to keep in mind when it comes to data security is that an organization could implement data security in such a way that it puts them in a legally defensible position, if something were to happen. In many cases, data security is less concerned about why the data is being collected and more interested in how it is being collected, where it is being stored, and the controls protecting the data.

Data privacy is the discipline of understanding what type of data is collected, why it is collected, and how it is used, while limiting the collection and storage of that data with the best interest of the data owner in mind. Data privacy requires data security, but data privacy goals are to protect the data owner over the needs of the business.

Not taking the time to understand the business's data security and data privacy requirements could lead to architectural issues that may require a significant level of effort to address later. This can also make it extremely difficult to attract and retain key customers, as the startup grows.

## Disaster Recovery and Business Continuity

Disaster recovery and business continuity should be considered early in the design process of the startup. Knowing what your customer’s expectations might be or what the business can tolerate, due to a disaster or down time is key. Not having a proper plan to account for disaster or business interruption could be a business-ending event for a startup, as it will erode the customers’ trust. Investing in a strong business continuity plan that allows for continued operation or redundancy is a strong investment in the relationship with the startup’s customers.

## Identity Management

This is a very large subject and one that is often overlooked, as part of the strategy for startups. Startups should consider how they want to manage authentication, for both their product and internal resources. This can involve implementing SSO to offload management of passwords and identities to your customer’s identity management platform or a trusted third-party platform (Google, Microsoft, Facebook, etc.).

Another key component to consider when building the identity management strategy is how access is managed for internal users. This includes onboarding, offboarding, and right management through the lifecycle. Overprovisioning access or rights to internal users can leave the startup susceptible to insider threats or data leakage, which has been an issue for many companies in recent breaches. Spending the time to understand the strategy of how to manage identities, authentication, and access management is key to the cybersecurity strategy and will allow for explosive growth.