With increased number of incidents and data breaches in current times, organizations are now redefining their approach to cyber security. Risk of cyber incidents can be a decisive factor towards an organization’s future, demanding organizations to take new skill sets and practices. Ensuring cyber security, data protection and overall system privacy can be applied under the same principle as ensuring the real world security of a building. It works best when implemented right in the start at the entry point. Taking security precautions in the initial design stage helps minimize potential threats to the organizational information and embed privacy and cyber security right into the organizational system’s architecture. It would be wrong to say that implementing cyber security at a later stage is impossible, but, there is no doubt that such a measure will not only create more difficulties but also create more errors and glitches.

Many organizations still take cyber security under the context of IT department. This mindset needs to be changed and cyber security be understood as a part of design process along two parallel paths. The technical path ensures that coding actually works how it should. The process path ensures that all requirements are fulfilled and problems are resolved. The end result of this approach may not result in perfect security, as it is not possible in the real world. However, it will ensure robust protection to build basis for improvements in cyber security.

We at Stickman believe in “Cyber Security by Design – the key to long term protection”. We believe that cyber security should be at the heart of every organizational structure and be made an integral part of the system from the beginning. We are positively inclined to develop satisfied customers and hence believe in their long term protection by helping them develop secure system from the start till end. Our “by design” concept recognizes that all companies are different and one size does not fit all. Cyber security landscape is changing constantly. Surviving in a competitive market and to stay ahead of the game requires organizations to adapt and change according to this changing landscape.

The concept of “cyber security by design” does not only involve technology. It also ensures that we train the people the right way to equip them with a “cybersecurity-aware” behavior. An attacker who is persistent may eventually end up getting into the system and acquiring critical information, but, making this difficult for him at each and every step is what makes up for a successful design. We provide our customers with secure options that they can prefer over less secure ones. We look at our long term protection plan cybersecurity by design from the perspectives of product development, technology development, IT hardware and software changes and brand equity.

**Product Development**

It is important to understand that during the initial phase of product development, organizations should make penetration testing as an integral part of the software development lifecycle. What we normally see is the opposite trend, i.e. making a product and then conducting its security assessment in the end to look for vulnerabilities. The issues are usually fixed with a patching software, but it turns out to be much more costly than addressing the real issue.

If issues are fixed during the software development process, much of the costs can be reduced by avoiding multiple cycles of testing – patching – retesting the software at the end. Ever since the threat landscape has changed, organizations are now looking forward to providing more secure applications that are able to sustain their profitability and attractiveness for the customer. As information is getting more fragile at the hands of malicious attackers found everywhere over the internet, measures to counter such attacks also need to be improved. Malicious hackers look for all routes to enter into the network and one of these routes is the application host. Hence, the applications hosted by your organization must not be vulnerable, or else information can be easily compromised. Employing a team of penetration testers during the SDLC phase helps avoid costs that may result otherwise in case of breach of data.

**Technology Development**

When developing new technology, our long-term protection design ensures that cybersecurity is kept at the forefront and not considered as an afterthought. It is important to have a thorough knowledge of infrastructural components like hardened host, network segregation and public key infrastructure for ensuring that the new technology will not weaken existing environment in terms of its security. It is also important to understand what technology is used in building a new software, to help make decisions in favor of security. Security testing and security code review must be used to validate controls used in securing a new technology. This security code review must be performed before a software is released for testing and is being reviewed for its functionality. Though code reviews can be both manual and automated, we ensure that our clients get maximum security by performing manual or human reviews.

**IT Hardware and Software Upgrades**

Hardware and software updates affect PCI DSS and ISO 27001 compliance. Any upgrade should be managed with compliance in mind. All standard requirements show the word “maintaining”, which means that compliance is not a one-time activity and rather an ongoing one. Many organizations have looked at PCI compliance as annual requirement in the past, but now it is mandatory to consider it as a continuous process. Stickman consulting helps you continuously monitor your applications for updates and changes, as well as new vulnerabilities and remediates them as soon as they are found. We perform tests through all stages of development lifecycle.

**Brand Equity**

Gaining new customers and attaining them is ultimate strategic goal of every organization. Brand equity is achieved only if an organization is able to maintain its customer base. For online retailers in particular, maintaining brand equity can be a challenge as even a single data breach incident can result in heavy loss of finances and customers. With rapidly evolving digital landscape in the retail industry, retailers usually find themselves under constant threats from sophisticated and escalating cyber attacks. As the customer is now more knowledgeable and conscious about security breaches, retailers now need to come up with new approach towards cyber security. Security issues can no longer be ignored by retailers, however, they do face obstacles such as employee turnover, inadequate IT resources, limited staff and distributed operations.

Stickman consulting understands that retailers need to embrace technology and adopt new approaches to their business and information security. We address the security and compliance challenges faced by retail industry in the market. We give our customers the solutions that they need for securing, standardizing, automating and simplifying transactions and operations right from the beginning till the end.