ASHWIN SHARMA, *CISO, CTO*
ashwin.sharma@securemation.com https://www.securemation.com/ https://www.linkedin.com/company/securemation/

Securemation have perfected the "Secure-by-Design service over the last 12 years by applying it to local and state Government agencies, financial and health industry organisations, mining and IT companies.

TIP 1. PLAN AHEAD

In a rapidly evolving business landscape, staying ahead of the competition is paramount, and that's where innovative solution comes into play. The key aim is to keep improving.

TIP 2. THE INITIAL CONCEPT

It all begins with the spark of a brilliant idea - a solution to conquer existing business challenges, or to pioneer a new frontier in your industry. Immerse yourself in your vision to craft a cyber resilient business solution that will empower your success.

TIP 3. CREATE A DATA FLOW DIAGRAM (DFD)

This illustrates the different business solution components and the direction of the data flows between them. The DFD identifies where the business-critical information assets live and how it flows to deliver business value. It also identifies the sensitivity of the information that is captured, processed, and stored in the solution.

TIP 4. A CONCEPTUAL SOLUTION

Security is not an afterthought; it should be woven into the very fabric of your solution. You should be dedicated to integrating cyber security resilience into your concept from day one. The most effective and efficient way of securing a solution is by embedding cyber security resilience into the initial design thinking – right from the initial concept. This reduces cost and strengthens the cyber security posture of the business solution. Define the security objectives for the solution and evolve the objectives throughout.

TIP 5 CONSIDER WORKING WITH AN EXPERT

As the solution progresses from a conceptual design to a final design – input from experts in the field can evolve the DFD and the accompanying threats, countermeasures, and residual risk evaluations.

TIP 6. THE END RESULT

As the solution progresses from a conceptual design to a final design – you can evolve the DFD and the accompanying threats, countermeasures, and residual risk evaluations. The security controls will consist of all three dimensions – people, process, and technology controls.

TIP 7. DEPLOYMENT

When the solution is deployed, according to the design, the countermeasure are deployed as part of the package. A final check is then conducted to ensure every countermeasure has been deployed as designed and is therefore reducing the cyber security risks as intended. Compare the result with the initial security objectives for the solution to ensure there aren't any residual risks that are beyond the acceptable tolerance levels.

TIP 8. DESIGNING YOUR DATA FLOW DIAGRAM (DFD)

The initial high-level DFD shows you a very visual and effective way of identifying risk factors in a solution from a "bird's-eye" view. As a solution moves from concept to logical and physical designs, the DFD evolves accordingly, and the amount of detail captured increases proportionately.

TIP 9.

Once the solution is deployed into production: perform ongoing threat hunting by continuous security monitoring. Usually a SIEM & SOAR capability is used in conjunction with dynamic threat hunting on a regular basis. The dynamic threat hunting is performed by looking for threat vectors specific to the technology solution components used. It also includes the people and process elements specific to the technology solution.

TIP 10. SUMMARY

In summary, your approach should never be static. It should improve and evolve several times within a year. The only constant is to embrace change. As new technologies come into play and new attack patterns emerge, your approach evolves in order to keep new business products and services secure.