Shielding Enterprises from Evolving Cyber Attacks with a Digital Security Framework

Abstract

As the IT landscape evolves, cyber threat actors also mature in response—developing new techniques to compromise the security posture of enterprises. Some companies take a proactive stance against these breaches, while most adopt reactionary one-off measures. This begs the question: will a predictive approach be more effective? Armed with a well-defined strategy, companies can build a digital security fortress while ensuring their IT infrastructure continues to mature and strengthen in the face of potential threats. Unlike most one-stop solutions, such a process-oriented journey starts with due diligence, moves into thorough security testing, creates an auditory framework, and finally transforms into a robust governance model.

From Reactive to Proactive and Predictive Cyber Security

In recent times, a number of enterprises have fallen prey to cyber-attacks, and reportedly, the damages caused are expected to reach USD 6 million annually by 2021[i]. For hackers, the focus has shifted from targeting network and system level vulnerabilities to running application level exploits across industries, particularly in the financial sector[ii]. Rather than investing in intrusion detection systems (IDS), enterprises should implement a holistic vulnerability management program that ensures fewer security breaches.

Traditional security tools, such as IDS and firewalls, have so far been ineffective in preventing DoS attacks despite regular scans of applications and the overall IT infrastructure. These systems continue to exhibit security defects like cross site scripting (XSS) flaws. These issues are further exacerbated with organizations diversifying their IT portfolio and lines of business, wherein cyber security takes precedence only during the final stages of 'go live' – moving the applications from the testing to production environment.

To define, build, and implement an efficient and effective enterprise security strategy, organizations will need to formulate strong delivery and operational models. These models must have a suitable auditory and governance framework that ensures effective implementation, identifies gaps, and recommends steps for improving the security posture.

Such an enterprise security management program should largely have four stages:

Stage 1: Security Consulting (Due Diligence)

Also known as the 'as is study' and 'process defining' phase, the first step is to correctly asses the enterprise security posture and study existing processes and controls in line with various industry standards such as National Institute of Standards and Technology (NIST). The next step involves developing a detailed threat profile that best suits the enterprise's IT landscape, lines of business, and the overall industry. This will act as the baseline to assess, analyze, and categorize IT assets with respect to potential attack risks and damages. Organizations can then prioritize those assets that require more time and investment. This will help in formulating a prioritized security assessment plan that covers the entire IT

portfolio, and also defines specific delivery models for unique test cases (Figure 1).

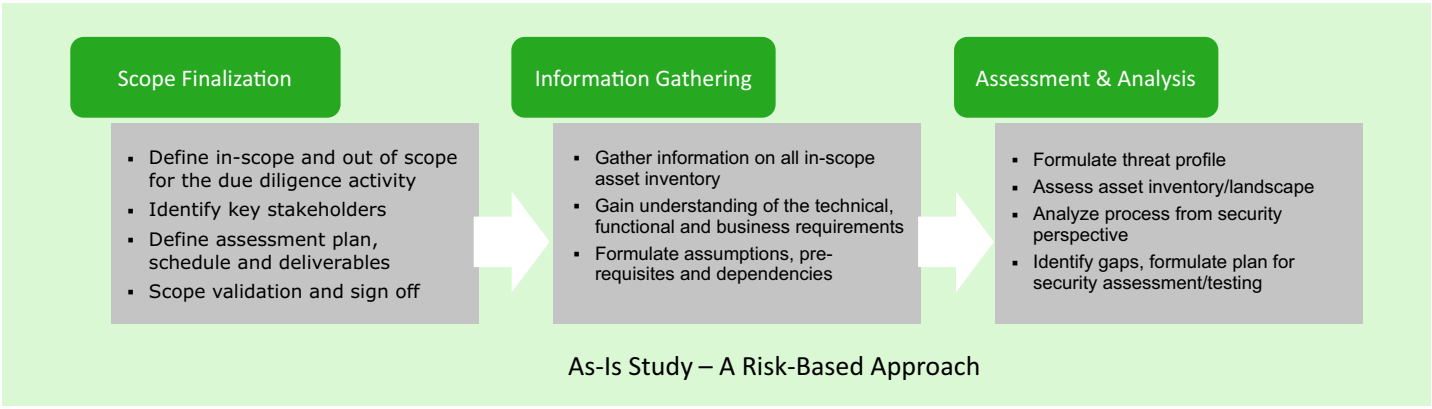

Figure 1: Steps for Due Diligence

Stage 2: Security Assessment and Testing

This stage involves code reviews and tests to identify performance, security, or reliability flaws in applications before they go live. Enterprises will need to perform periodic automated vulnerability scans and manual tests to discover security defects and define remediation measures. Security testing needs to be a methodical approach considering the business, functional, and technical priorities of the in-scope IT elements, which includes web-facing applications, thick clients, desktop application, work stations, and so on.

With the help of a detailed assessment report, enterprises will gain a better understanding of the current security posture and gain insights into specific issues and their respective severity levels, issue reproduction steps, and remediation measures to be implemented.

Stage 3: Auditing, Monitoring, and Training

While periodic assessment and testing is conducted, it is imperative to evaluate the effectiveness of these activities and identify gaps, if any. The auditing process must be in line with industry standards such as Federal Information Security Management Act (FISMA), and the guidelines and scopes will depend on the line of business or industry. Each identified gap must have a corresponding corrective measure along with a specific implementation timeline. This will ensure a holistic closure of the issue not just for the identified instance but also at the application's code or framework level. This would then be revalidated and confirmed by the internal security testing and audit team. The primary aim is to refine and enhance the current testing or assessment activity and improvise.

Based on the findings from these audits, enterprises can plan and conduct security awareness sessions, classroom or web training, and certification programs. These should cover:

- Ethical hacking
- Secure SDLC
- Secure coding
- OWASP top 10
- OSSTMM
- BSSIMM
- Agile security
- DevOps
- Cloud security

Stage 4: Security Governance

The next step is to establish a robust governance program using the open software assurance maturity model (open SAMM) as the baseline (Figure 2). This model will help define the broad business functions and the associated security policies and frameworks, which can be customized as per requirements. This will be followed by formulating detailed security standards and guidelines for every process or work stream according to industry standards.

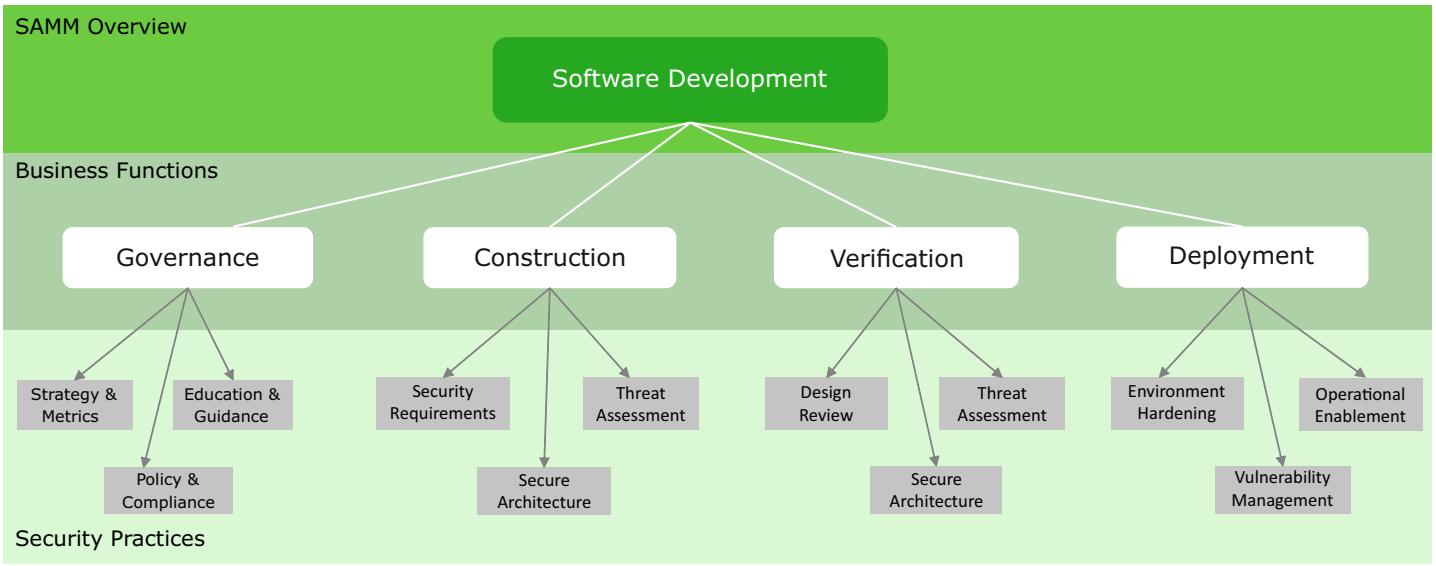

Figure 2: SAMM Overview[iii]

In order to achieve application security maturity, organizations will require policies and guidelines catering to secure SDLC consulting and implementation, as well as agile and DevOps security management as per NIST, ISO, BSSIMM, OSSTMM, and similar standards. Similarly, the infrastructure elements will need to establish security principles based on NIST, ISACA and ISO.

The next step would be to strategize and establish an enterprise wide vulnerability management program which includes IT security risk assessment and management, vulnerability management addressing the application landscape, and infrastructure elements.

This enterprise security governance and compliance strategy must be approved and subsequently supported by senior management for effective implementation. The governing body overseeing the audit and monitoring activities should ideally be accountable to the CISO and the board of directors.

Implementing the Right Delivery Models

The success of such a strategy depends on the effective implementation of a layered delivery mode (Figure 3), supported by either a dedicated team or through SLA-driven shared services.

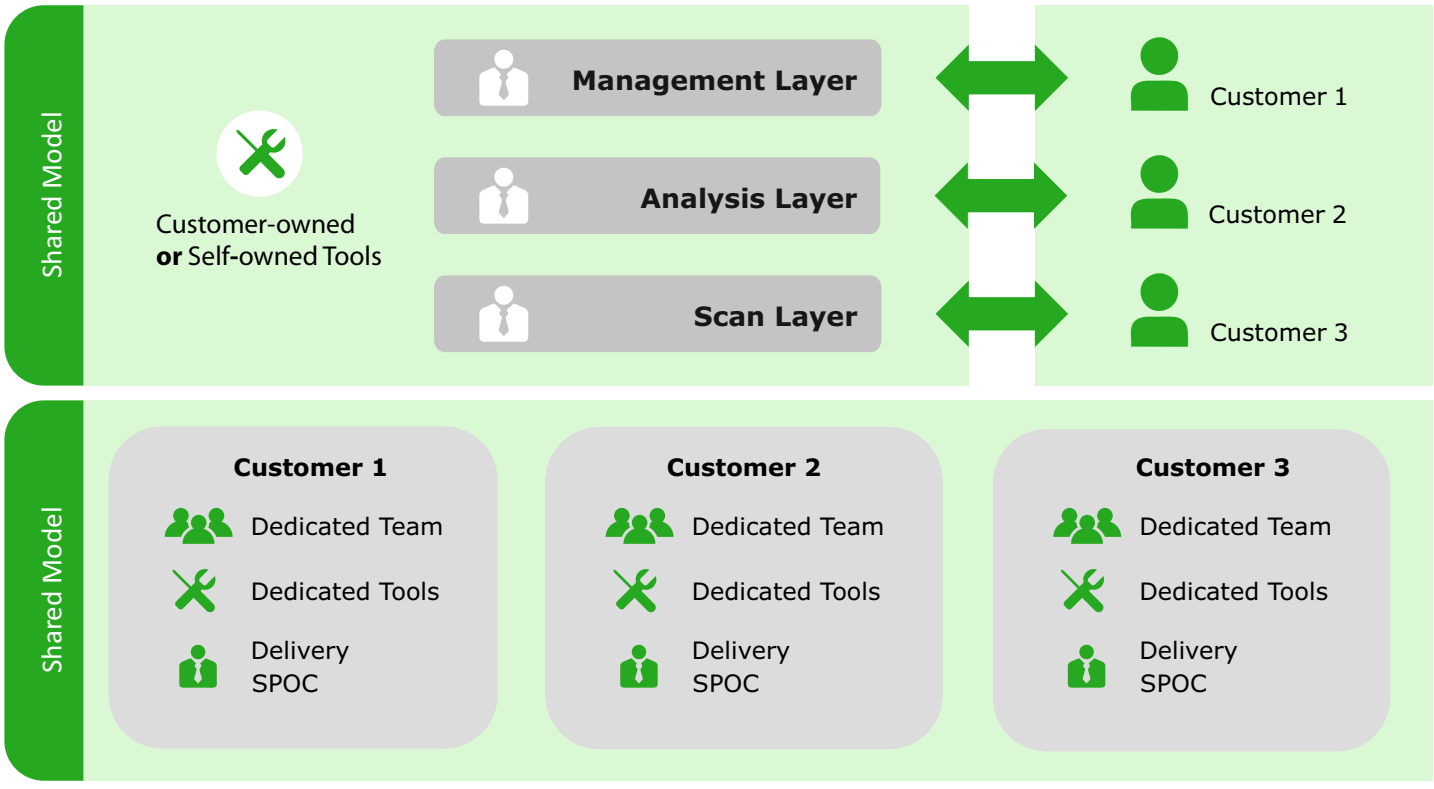

Figure 3: A Layered Delivery Model

Each layer—core operational, functional, and strategic—should be staffed per the skills required to execute the required activities. For handling one-off tasks, individuals with the necessary capabilities can be deployed while for larger programs, an entire team can be assigned. While formulating the delivery model, enterprises must factor in cost, quality, and turnaround time.

Journeying through the Stages of Security Maturity

For any organization, the main objective will be to transition from a reactive to predictive management of information security. The reactive approach tends to be more event-driven, where one establishes a defense mechanism after a breach or attack has occurred. Instead, enterprises need to be more proactive, implement layered security solutions, conduct periodic assessments, and close the gaps before the systems are breached. This will eventually help them move to a predictive model — analyzing threat vectors and metrics, and focusing on building and implementing a more cohesive security solution. These stages have been highlighted in Figure 4.

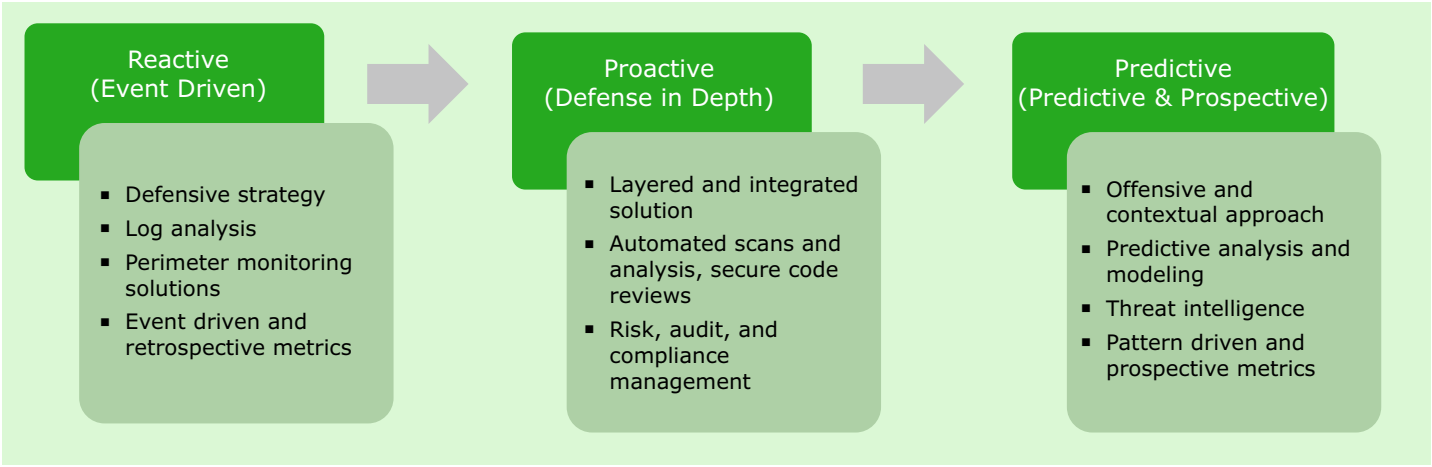

Figure 3: A Layered Delivery Model

Securing the Road Ahead

The security unit within any organization must be empowered with the ability to either remediate or root out cases of non-compliance. This unit must be monitored and complemented by an equally strong audit and governance team, which directly works with and reports to senior management. Enterprises with

a global footprint operating multiple lines of business should adopt a top-down approach to successfully implement such strategies. While there is no silver bullet when it comes to ensuring security, the battle against cyber threats can be won through meticulous strategic planning.

References

i] https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html

ii] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

iii] http://resources.infosecinstitute.com/implementing-secure-software-development-program/#gref

About The Author

Dinesh Sawrirajan

Dinesh Sawrirajan is an Information Security Consultant and Delivery Lead with the Cyber Security Practice at Tata Consultancy Services (TCS). He has more than nine years of experience in application security, risk management, and data security. He has worked with many leading enterprises including one of the Big Four audit and consulting firms, a major Australian retailer, and for the British government. Dinesh is a mechanical engineer and has a double masters in Management – Operations, and Marketing and Finance

Contact

Visit the TCS' Cyber Security page on www.tcs.com

Email: cyber.security@tcs.com

Subscribe to TCS White Papers

TCS.com RSS: http://www.tcs.com/rss_feeds/Pages/feed.aspx?f=w
Feedburner: http://feeds2.feedburner.com/tcswhitepapers

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

Experience certainty. IT Services
Business Solutions
Consulting

TCS Design Services | M | 01 | 18