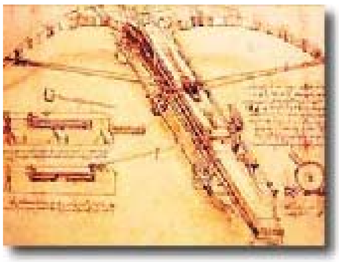
The natural choice for information security solutions



A Corsaire White Paper:

Secure Development Framework

Author	Glyn Geoghegan
Document Reference	Secure Development Framework.doc
Document Revision	V1.0 Released
Date	05 April 2004

Table of Contents

1 Introduction

In order to achieve business goals, organisations frequently have to develop bespoke application solutions or customise commercial off-the-shelf (COTS) packages. These range from complex back-office database applications, CRMs and asset management systems to customer-facing fat and thin applications. Corporate web-applications offer anything from a simple brochure request to a full e-business implementation.

Increasingly, these bespoke systems are exposed to larger and less trusted user-bases, from extranet business partners to the general public at large. Not only are they providing access to key assets and data, in many cases they *are* the business critical assets. In the case of software or service providers it is therefore vital that the security regime applied to the IT infrastructure is matched, and indeed exceeded, by that applied to the applications themselves. If not, then the applications may prove to be the Achilles Heel in an otherwise secure environment.

2 Defining Secure Development

In order to mitigate the risk of attack through the bespoke applications in an environment, it is vital both to build secure applications and regularly validate their security through testing.

Secure development is the term largely associated with the process of producing reliable, stable, bug and vulnerability free software. There are a number of ways that this can be undertaken within traditional application development, but the most common procedures involve phased security assessments and reviews that encompass knowledge share; design and implementation assessment and regular security health checks.

3 The Requirements

It is important to understand the risk the application presents. In the standard risk equation, *Risk = Threat x Vulnerability x Cost*, we consider risk to be a product of the likelihood of a successful attack together with the frequency of such attacks and the associated cost to recover from it.

An insecure application clearly increases the vulnerability of the organisation and therefore likelihood of success. The frequency of attack is increasing as more attackers focus on the application interface when faced with a secure infrastructure. The value of the application and therefore the cost of recovery will clearly vary from organisation to organisation, but it is fair to say that applications provide access to, or are, valuable corporate assets.

The risk associated with an insecure application is already high, and is rising so there are several reasons why organisations choose to follow a secure development program;

- To mitigate the risk of a serious application flaw exposing the organisation or its data.
- To provide a better quality in the completed product or service, thereby reducing any risk of liability or negative publicity.
- To reduce IT security costs after implementation and ultimately provide a better return on IT security investment (ROSI).
- To improve maintenance time by reducing the effort needed to fix bugs after delivery.
- To improve productivity and allocation of resource. Less development work is required to engineer solutions to problems identified early. Their root causes may be determined, resolved and adapted to prevent reoccurrence.
- To shorten delivery times by reducing the time spent in the integration and system test/debug phases.

Retrospective identification and remediation of risks in applications can be a time-consuming and costly exercise. It is far easier to build a secure application that to fix an insecure one.

IBM reported that the cost to fix an error found after product release was 4 to 5 times as much as one uncovered during design, and up to 100 times more than one identified in the maintenance phase. Figure 1

shows the relative cost to fix problems identified in the *Design*, *Implementation*, *Testing*, *and Maintenance* phases as identified by IBM[1].

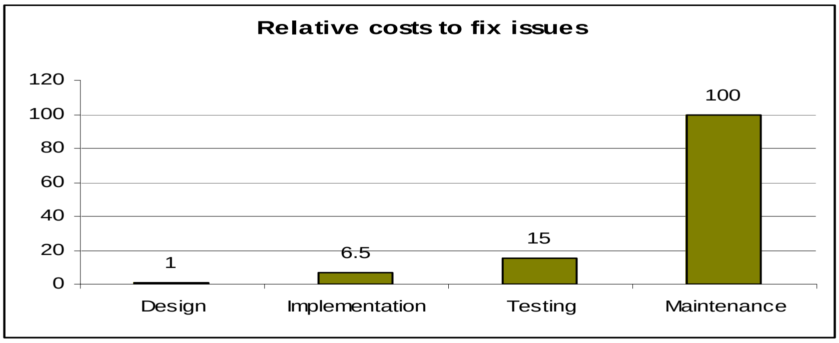


Figure 1

Research by @Stake demonstrated that on average an organisation caught only a quarter of its software security holes and had typically seven significant bugs within its enterprise software. Their findings verified that fixing the same defects during the testing phase cost around seven times less than after deployment. They concluded building security into software engineering at the design stage would net a 21% ROSI; waiting until the implementation stage would reduce that to 15% and at the testing stage, the ROSI would fall to 12%.

4 Successful Implementation

A Secure Development Programme should be integrated with all phases of the organisation's software development lifecycle. It ensures that security is a consideration at all stages of a development project – from risk analysis of the business objectives through design and implementation to deployment in production environments.

Secure Development involves the systematic analysis of the security controls already in place in the organisation's lifecycle. It will typically involve the integration of phased security workshops, reviews and assessments during the development process.

4.1 Drawing on Expertise

Application security, and insecurity, is a rapidly evolving area. In order to successfully integrate security to the development process a comprehensive understanding of the potential issues and failures is required, together with intrinsic knowledge of the existing development processes.

The objectives of quality assurance and user acceptance testing are often at odds with those of security testing. Acceptance testing is performed with a mind to ensuring that the application behaves as it was designed to, from the point of view of a user. Tests from the point of view of a user with malicious intent, are often not carried out and form the core of the security testing mindset.

Through drawing on a security specialist to provide knowledge and experience to complement internal skills, a successful balance may be achieved. Once the processes are defined and integrated, the security role becomes a periodic one, providing knowledge sharing and assessment consultancy when required.

4.2 Agreeing Deliverables

As with all risk management, development of secure applications requires a delicate balance between investment and tangible return. As mentioned before, applications *can* be secured

[1] Implementing Software Inspections, *IBM Systems Sciences Institute*

before, during and after development, but re-architecting to remove serious flaws discovered in production systems may be prohibitively expensive.

Figure 2 below illustrates how the security phases may integrate with a simple recursive waterfall development model. It is assumed that a *Business Risk Audit* will have been conducted during the business requirements phase.

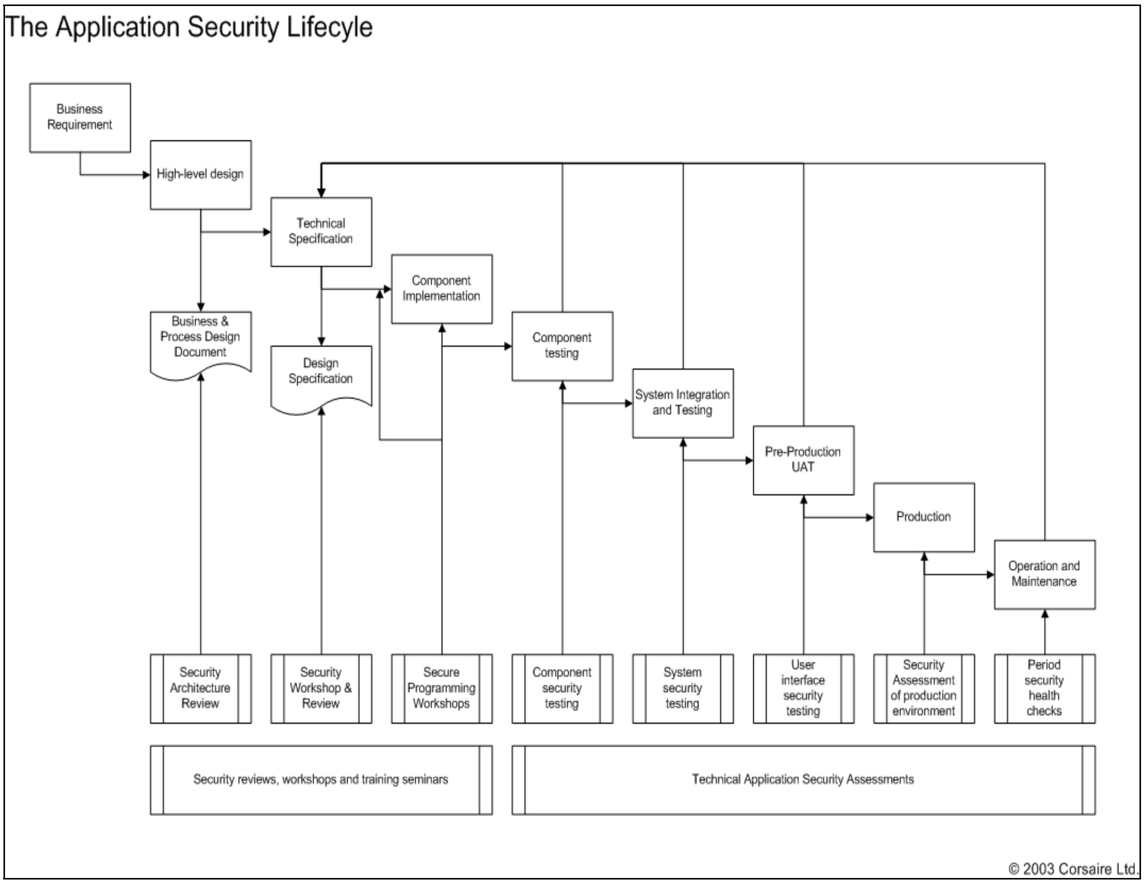

The Application Security Lifecycle
Business Requirement
High-level design
Technical Specification
Component Implementation
Business & Process Design Document
Design Specification
Component testing
System Integration and Testing
Pre-Production UAT
Production
Operation and Maintenance
Security Architecture Review
Security Workshop & Review
Secure Programming Workshops
Component security testing
System security testing
User interface security testing
Security Assessment of production environment
Period security health checks
Security reviews, workshops and training seminars
Technical Application Security Assessments
© 2003 Corsaire Ltd.

Figure 2

4.2.1 Security Architecture Review

The Security Architecture Review is a logical review of the high-level designs and processes associated with the project and how it integrates with the existing environment and third parties. Through this phase, process design flaws and intrinsic security risks are identified and presented to the business in order to find resolutions prior to implementation. Systems and software architects are primarily concerned with the functionality of the application and whether or not it meets the business needs. Security considerations, and particularly, defending data from users with malicious intent is often overlooked.

4.2.2 Security Workshop and Review

The next phase occurs during the technical specification development phase, and consists both of logical reviews of designs and interactive workshops with the project stakeholders. Potential security issues and design flaws can be engineered out of the technical design specification prior to the costly implementation phase. The workshops also raise security awareness in the project team prior to decisions being made which may be difficult to reverse later.

4.2.3 Secure Programming Workshops

Early in the implementation phase, secure programming workshops provide the developers with specific advice relating to typical insecure implementation practice and common flaws. These workshops are tailored to the specific project and environment, e.g. the type of software being developed and the development technologies.

Workshops include discussion on defining the data sets and common security libraries and routines that will be used by the application. Possible attack scenarios and areas of risk within the application are identified and mitigation techniques planned.

4.2.4 Application Security Assessments

The preceding phases have focussed on logical reviews of processes and designs, together with knowledge share workshops. Subsequent testing phases involve technical security assessments of the software components and system as a whole.

An Application Security Assessment is designed to identify and assess threats to the organisation through bespoke, proprietary applications or systems. These applications may provide interactive access to potentially sensitive materials, for example. It is vital that they be assessed to ensure that, firstly, the application doesn’t expose the underlying servers and software to attack, and secondly that a malicious user cannot access, modify or destroy data or services within the system. Even in a well-deployed and secured infrastructure, a weak application can expose the organisation’s crown jewels to unacceptable risk.

4.2.5 Component Security Testing

Typically, each component of the application will be rigorously tested as it is completed. Security testing of the component interfaces and functionality will also be performed on each discrete piece of software.

4.2.6 System Security Testing

After the components and system integration have been completed, further security testing of the system as a whole is undertaken. This takes into account interaction between the completed system and the existing environment.

4.2.7 Interface Security Testing

During UAT and/or Load-Testing phases, security testing is undertaken from the user’s perspective. An Application Security Assessment should be undertaken concurrently with user acceptance testing to ensure that changes made to the security of the application do not adversely impact the business requirements of the application. The assessment will produce a more accurate map of the risks associated with the application if real (or as close to real as possible) data is used in the testing environment. Providing a testing environment that closely matches the live environment will ensure that maximum benefit is gained from this phase of testing.

In less mature security models UAT testing is often the only form of application testing undertaken (if any). Typically, problems identified at this phase without the preceding phases having been undertaken may be difficult, prohibitively costly or impossible to engineer out of the application.

4.2.8 Production Security Assessment

The final stage of security testing is undertaken once implemented in the production environment. This involves re-testing of the user interface to validate fixes applied as a result of earlier advice, and identifies any new security problems introduced as a result of migration to the production environment.

4.2.9 Security Health Checks

Security, attacks and vulnerability types are constantly evolving and changing. As such, regular security health checks will be performed on production applications. This ensures that the applications are tested for resilience against new attack techniques, and provides assurance that changes within the application or environment as a whole have not adversely affected security within the organisation. Given the structured secure development process, this maintenance phase testing is likely to demonstrate that the strong security implementation has provided a stable and secure platform resilient to existing and future attacks.

4.3 Application Security Timeline

In practice, the phases will be performed in a largely linear timeline as shown in Figure 3 below.

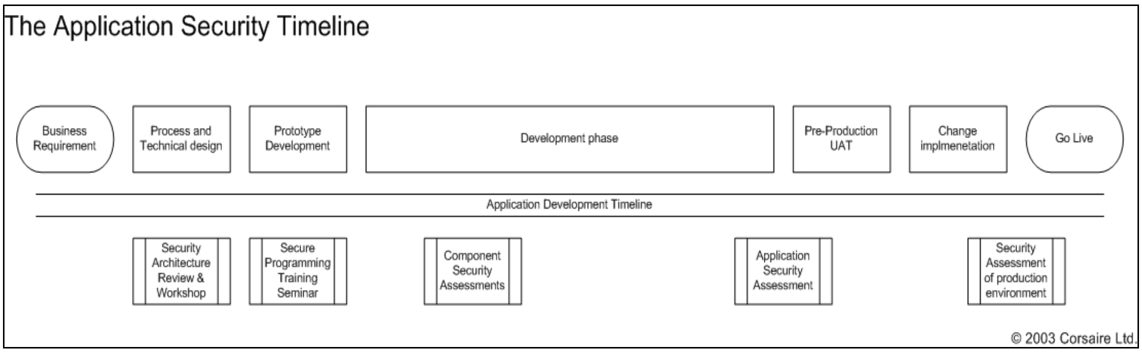

The Application Security Timeline
Business Requirement
Process and Technical design
Prototype Development
Development phase
Pre-Production UAT
Change implmenetation
Go Live
Application Development Timeline
Security Architecture Review & Workshop
Secure Programming Training Seminar
Component Security Assessments
Application Security Assessment
Security Assessment of production environment
© 2003 Corsaire Ltd.

Figure 3

4.4 Preparation Prior to Implementation

One of the first steps to ensure that your project is a success is in preparing your organisation for the process; the second will involve determining which supplier to use.

4.4.1 Transforming Organisational Attitudes

- Prepare Software Managers for the program; they should appreciate the value of the process and understand the importance of allocating time in the schedules for the software developments team participation in certain aspects of the phased security assessments.
- Build phased security assessments into the project schedule and remember to factor in time for the inevitable rework that will follow each phase.
- Inform the participants and if appropriate your customer on the benefits of secure development implementation.
- Encourage a team culture of mutual respect; the process of secure development should be seen as non-threatening. Some developers are concerned that the process might be used against them at performance appraisals time. Assure them that this won't be the case. Teams should recognise that a secure development program can support both individual and team efforts for continuous improvement. Further, that learning can be enhanced as knowledge is automatically exchanged about programming language features, coding and commenting style, program architecture, design notations, ways to document requirements and all other aspects of the software development process.
- Have local champion who preaches the merits of a security development program, trains others as they get started and strives to improve the overall software development process.

4.4.2 Choosing your Secure Development Partner

When considering a security supplier, first outline your goals for the project and your expectations of the supplier. You will want to choose a supplier with experience in your industry and one that has all the expertise you require. Speak to at least two references; both those that have worked with the supplier and those that are still working with the supplier.

In order to assist in your secure development program, the supplier must have experience of integrating security controls with organisations existing development processes. They must have extensive experience of assessing and auditing application security at all levels – from design and architecture through prototyping and coding to analysis of full production environments.

Equally important is the supplier's understanding of the relationship between business demands and security concerns, and how to mitigate risk within the boundaries set down, including required functionality and time-scales.

Detailed below are several questions to ask your potential suppliers; the information gained will help you determine whether they are appropriate. The reasons for asking these questions will be explained accordingly.

1. Is the supplier a specialist first and foremost, or is the security practice a secondary concern?
2. Does the supplier offer a comprehensive suite of services, tailored to your specific requirements?
3. Do the supplier's methodologies follow and exceed those such as OWASP?
4. Does the supplier have a policy of employing ex hackers?
5. Are the supplier's staff experienced security professionals, holding recognised certifications such as CISSP, CISA and CHECK?
6. Can they distinguish and articulate between infrastructure and application testing?
7. How many technical consultants does the supplier have that work on security and assessments, and how many of those are dedicated solely to security?
8. Does the supplier present the deliverables, such as the final report, in an informed manner, with concise and practical information for technical and non-technical parties?
9. Is the supplier a recognised contributor within the security industry?
10. Are references available to attest to the quality of past work performed?

4.4.3 Checking the Quality of your Supplier's Consultants

The quality of the security assessment service that you will receive is the direct result of the quality of the consultants that will be supplied for the project.

A phased security assessment of software development will examine design and implementation, and assess the impact on both the technical and business infrastructure. This requires the consultancy team to possess a broad spread of experience and also detailed knowledge of the areas under scrutiny. It is clear that these kinds of skills cannot be obtained without years of experience in a variety of complementary IT fields, such as development, systems administration or consultancy.

When considering a security assessment supplier, a good measure of their worth is to qualify how they contribute to research and development within the security industry. Research demonstrates a profound understanding of current technologies and a proven ability of the supplier's team to assess, review and audit infrastructure and provide trusted solutions. What is more supplier's that operate in this way are able to deliver real value-add by identifying, remedying and disseminating details of new security flaws discovered; allowing their customers the opportunity to gain both increased security and gain an instant competitive advantage.

A commonly heard complaint when embarking on a security assessment project is that a high-level consultant will come to the pre-project meetings, but when the project starts a junior consultant or trainee is used. To avoid this kind of issue when choosing a security assessment partner, insist on being provided with the CV's of all the consultants that will be working on your project, prior to commencing.

References

Implementing Software Inspections, IBM Systems Sciences Institute

Tangible ROI @stake - http://www.sbq.com/sbq/rosi/sbq_rosi_software_engineering.pdf

Acknowledgement

This White paper was written by Glyn Geoghegan, Principal Consultant at Corsaire Limited.

About the Author

Glyn Geoghegan, CISM, is a Principal Consultant in Corsaire’s Security Assessment team. He holds an honours degree in Mathematics and Computer Science from Imperial College, London. He has worked in IT Security and Internet related roles since graduating in 1996, and has specialised in security design, deployment and analysis since 1997.

He has spent the last four years focused on Ethical Hacking, Security Assessment and Audit at Corsaire and previously at Internet Security Systems where he was co-founder of their EMEA X-Force Security Assessment Services team and lead author on the ISS Ethical Hacking Training course.

Glyn’s past roles have included that of Senior Network Security Analyst at a leading City of London Financial institution where he was involved in the corporate security at many levels. He was responsible for consulting on the paper security policies and procedures, designing, budgeting, procuring, deploying and supporting the Security infrastructure of the organisation and its business partners and building a permanent team to continue the ongoing security strategy and its support.

As an Internet and Security Consultant at a Global Internet Service provider he provided design and deployment advice and implementation on Security Technologies (Firewalls and other border control devices, encryption, content management, anti-virus, DR, strong authentication etc.), ISP scale network and routing design and security, and Internet related services (mail, DNS, web, e-commerce, UNIX etc).

About Corsaire

Corsaire are experts at securing information systems. Through our commitment to excellence we help organisations protect their information assets, whilst communicating more effectively. Whether they are interacting with customers, employees, business partners or shareholders, our sound advice can help our clients reduce corporate risk and achieve tangible value from their investments.

Privately founded in 1997 and with offices in the UK and Australia, Corsaire are known for our personable service delivery and an ability to combine both technical and commercial aspects into a single business solution. With over eight years experience in providing information security solutions to the UK Government's National Security Agencies, Government departments and major private and non-profit sectors, we are considered a leading specialist in the delivery of information security planning, assessment, implementation and management.

Corsaire take a holistic view to information security. We view both business and security objectives as inseparable and work in partnership with our clients to achieve a cost-effective balance between the two. Through our consultative, vendor-neutral methods we ensure that whatever solution is recommended, an organisation will never be overexposed, nor carry the burden of unnecessary technical measures.

Corsaire have one of the most respected and experienced teams of principal consultants available in the industry and have consistently brought fresh ideas and innovation to the information security arena. We take pride in being a knowledge-based organisation, but we don't just stop there. Through a culture of knowledge-share, we are also committed to improving our client’s internal understanding of security principles.

It is this approach to knowledge that differentiates us from most other information security consultancies. As a mark of this, we are known globally through our active contribution to the security research community, publishing papers and advisories on a regular basis. These we share freely with our clients, providing them with immediate access to the most up-to-date information risk management advice available, allowing them to minimize their exposure and gain an instant competitive advantage.

Whilst it is imperative for us to offer a high level of security to our clients, we believe that it is of equal bearing to provide a high level of service. At Corsaire our clients are not only protected but valued too. We work hard at building strong relationships that are founded on the cornerstones of respect and trust. With 80% of our customer base deriving from referrals we are certain that our clients value the quality, flexibility and integrity that partnering with Corsaire brings.

For more information contact us at **info@corsaire.com** or visit our website at **www.corsaire.com**