NGS Consulting
Next Generation Security Software Ltd.

Slotting Security into Corporate Development

Introduction

Technology trail-blazing organisations such as large financial institutions have been working to secure their custom applications for several years, but the second-tier "technology following" organisations have been slow to follow. This is now rapidly changing due to recent bad press following many highly publicised security compromises.

In many of today's software environments security has traditionally been viewed as an after thought, sometimes an add-on or even an inhibitor to business. Coding faults, implementation issues and fundamental architectural flaws are still found in abundance in a diverse range of custom applications. Driven by business demands, organisations are finding that additional functionality and application diversity are increasingly required to fit within a secure development process. Combined with a fuzzing of the organisational perimeter and increasing pressures on providing more timely information to customers, businesses must now ensure that security is built into any custom application. As previous "internal only" applications and systems continue to evolve and take on functionality that is linked to Internet based clientele or geographically distributed users, lax security procedures often prove pivotal in the malicious compromise of data integrity and confidentiality.

With headlines reporting various phishing and account hijacking attacks that potentially affect their own customer base, many organisations have started to realise that they are once again behind the technology curve and require urgent and expert assistance. In many instances these organisations are initially seeking advice on where to begin the process of securing their custom applications.

The cost of "bolting on" security is obviously a substantial outlay for any organisation. The amounts can vary wildly depending on how and where organisations exert their efforts as does the security assurance.

This document outlines the relative business significance and security benefits for deploying different strategies dependant upon the specific requirements of the development project. Analysis is made of the different security services that are available and how they fit within the different phases of the corporate development lifecycle – in particular, understanding how these services can be slotted into current development procedures. Depending upon their internal development processes and security awareness, there are many areas where Next Generation Security Software Ltd. (NGS) can assist organisations in the complex process of securing their applications.

NGS are renowned for assisting many of the world's largest commercial organisations with the provision of technical security guidance at all stages of the development lifecycle. Based on our experience, it is a well proven fact that the earlier secure functionality is built into the development lifecycle, the more secure, efficient and cheaper the end solution will be. Using our comprehensive wealth of experience, NGS is able to work with organisations large and small at all stages of development thereby maximising the integration of secure processes and techniques to protect against both current and future threats.

The Software Development Cycle

Rapid development timelines, requirement changes and additions, and even risk based business models have shifted large software development cycles from the traditional document driven paradigm of the "Waterfall" model to the more flexible "Spiral" model – a risk management based solution. The linear Waterfall model tends to be used for specific component development within an application solution, whereas the spiral model tends to be deployed at a holistic level for the entire project. In any cases most software development cycles can be depicted as special cased spiral models.

Each stage of a development cycle within these models is commonly addressed with their deliverables, relationships, milestones, transitions, and reviews. Typically the following phases are used when modelling a software development cycle:

1) ***Requirements:*** Definition of the problem or need which should be satisfied by the project. This is normally an information gathering exercise designed to capture all the business requirements, as well as identifying project risks and problems than need to be solved.
   - *Security tends only to be included here if there is a specific security need in the requirements, e.g. One of the problems is to solve user authentication and session management*

2) ***Specification:*** Stringent definition of all components, data flows, features and limitations are assessed during this stage and should yield all the project goals and milestones.
   - *Security can greatly affect decisions in this phase as specific technologies are often selected as a basis to fulfil defined requirements. This is sometimes influenced by time and cost restraints, but more often as a result of not wanting to "reinvent the wheel" for every component of the application. Lack of security or in-depth knowledge at this crucial stage often leads to complex and expensive problems in later phases.*

3) ***Design:*** Once the 'What' has been established in the two prior stages, the 'How' needs to be fully defined in this phase, the objective is to have a complete specification of itemized components in minute detail which can be handed to the development team for implementation.
   - *At this stage security is fundamental as decisions on application logic, system integration, user interfaces, core technologies and policy & procedures are all designed in this phase. Designing applications without security in mind leads to security being added in later phases and sometime limits what can or can't be introduced because of redesign costs.*

4) ***Implementation and Development:*** Construction of the designed application is completed in this phase. Details from the design phase are sometimes disseminated into smaller modules to enable various parts of the design to be completed concurrently.
   - *The application of poor security practice has affected this stage of the development cycle more consistently than any other phase in recent history. Several recently published security advisories are a direct result of developers implementing insecure solutions. This is often due to human error, but typically, it is due to lack of education into the security issues and implications of what they are producing.*

5) ***Integration:*** Integration of multiple components and modification of legacy environments to incorporate the new application can make this one of the hardest phases to complete within the development cycle. Backward compatibility issues, lack of documentation and in-depth knowledge of legacy applications, as well as availability issues with mission critical infrastructure can all significantly hinder the timeliness of this stage.
   - *Security components of the developed application are very often removed at this stage to circumvent issues with compatibility, permissions and day to day running of the core business units of the end customer. As well as removing security within the new application, the inclusion of the new application within an existing environment can open new vulnerabilities or attack vectors to previously secure products.*

6) ***QA & Testing:*** QA and testing is key to ensuring that the application meets its requirements from a functionality, reliability and security perspective, and operates

correctly outside of the development environment.

- *Each area is equally important, yet often a development team will bias their testing towards one objective. Functionality, reliability and security are interlinked in the respect that the security testing makes use of atypical or boundary conditions. Reliability and functionality issues need to be carefully factored into security review processes as part of any delicate compromise negotiations.*

7) ***Deployment:*** The Deployment stage encompasses the migration of approved code and application components to the "Live" environment. Sophisticated applications often encounter problems within the hosting environment due to topology, patch management, version control, account permissions and regional distribution of physical assets.
   - *Ensuring that the actual deployed implementation of the application fulfils all the agreed security requirements is vital at this stage. Dependencies on other software components and interaction with hardware in a live environment can often throw up unforeseen security hurdles.*

8) ***Maintenance:*** Maintenance is required to ensure the infrastructure that hosts the application is as secure as possible. Furthermore as components on which the application depends continue to evolve there is a need to append to and modify the application code base.
   - *The continual evolution and mix of new code elements to an already deployed application place greater demands upon internal security validation processes. Appropriate policies, procedures and safeguards are used to manage maintenance processes and help ensure that security mechanisms keep up with, or outpace existing or emerging threats.*

Adding Security to the Mix

The various models representing the development lifecycle are all technically correct, but they are overly complex when trying to understand how "security" fits in. Taking a less complex route, there are three key areas in which NGS excel when securing critical business applications – put simply they are the beginning, the middle, or the end.

Starting in reverse order, "the end" refers to applications that are currently live or about to be deployed within a live environment. Here NGS tends to utilise a Grey-box testing strategy to identify probable security weak points from a hackers perspective. Once a weakness or vulnerability is discovered NGS will attempt to see if it is exploitable and then advise the development team of the steps necessary to secure their environment. Quite often "user-level" testing is carried out in conjunction with classic penetration testing processes and onsite infrastructure security assessments. The disadvantages of trying to secure applications at the end of the development cycle is that any necessary fixes tend to be patched on thereby delaying deployment as they are more complex to implement robustly.

For organisations that out-source the development of their applications, or where their live applications are under a constant change cycle, NGS helps to implement security features and processes during the "middle" stage. Here consultants work closely with the client's security or QA and testing teams to secure the code as it gets applied to the live systems. This typically requires high volumes of native code review and identification of poor coding practices, followed by event driven instruction on secure coding practices for the developers.

As many organisations already enable their QA or testing teams with the power of veto over code changes to the live systems, they are ideally placed to police the security of new application changes. Unfortunately many of these teams are not particularly security aware (at least from a technical level), and must be trained to identify insecure coding practices and increase their security skills in order to provide guidance to wayward developers.

NGS have found it extremely valuable in the past to add one or two security consultants to the team initially (ideally to implement secure practices immediately) and to participate in knowledge transfer exercises with the clients development team. After a month or two, the QA and testing team will have developed the necessary processes and procedures for validating new code as well as understand the core aspects of a secure application.

The final area where security consultants typically get involved is in "the beginning". NGS

defines this as everything that happens before real code development begins. Consequently the types of services NGS have found valuable to their clients at this early stage focus around specialist technical workshops.

Technical workshops that bring together the clients core development specialists and technical authorities, along with one or two external security specialists, enables frank and open discussions of key aspects of the application currently under development. Topics under discussion revolve around business requirements for the application, how these can be met through code development technologies and what these decisions mean from a security context.

For instance, the application may require users to authenticate using web-based forms. The development team discuss how they intend to implement this, while the security consultants make them aware of how attacks techniques such as automated account brute-forcing attacks are conducted. They would then provide guidance on how their code should respond to occurrences such as failed logins and initial password allocations to users.

The end result is that not only does the application become more secure, but the developers themselves learn more about the threats their application is likely to encounter and how to respond. While some may argue that the developers could pick up much of this information from traditional “ethical hacking” training courses, NGS have found that the focused approach of a workshop provides greater opportunities for security dialogue. Instead of being “talked to” as in a training course, the free flowing form of the workshop allows all members to participate in the security design and to better grasp the security principles that will be applied to the application.

For the applications security itself, having workshops early on in the development process ensures that security is built into the core. This not only makes the application more secure, but also makes it much easier to code – both during the development process and post deployment. There is of course another benefit – particularly for security departments. By ensuring that the security consultancy occurs earlier in the project lifecycle, security departments typically find that the release of budgetary funds is easier, and more commonly comes from the project sponsor’s pot instead of theirs.

How NGS can help

The specific type or combination of application services that NGS provides to our clients is dependent upon their current stage in the development lifecycle. Many of the services can apply to one, two, or all three major application development stages.

NGS often find that the mix of appropriate services is driven by how the client manages their development teams and the business context of the application (e.g. does the client outsource all development? Is the new application destined to replace a legacy system or provide integration with critical business information systems?). The following table provides a high level view of these common services and their general applicability.

Service	Beginning	Middle	End
Security Training	***	**	*
Secure Code Development Workshops	***	**	
Understanding Application Threat Workshops	***	*	*
Design Review	***	*	
Design Authority	**	**	
Secure Coding Authority	*	**	*
Staff Supplementation for QA and Testing		***	
Code Reviews		***	**
Source Code Change Review		***	**
Application Testing Workshops		**	***
Application Penetration Testing		*	***

* represents applicability

The Beginning of a Project

The ideal place for ensuring that a business application will be as secure as technically

possible is at the beginning of the cycle – even before the developers begin the first iterations of release code. At this stage, the emphasis is upon ensuring that the security functions and technologies are appropriate given the nature of the application and are efficiently integrated into the application solution.

With regards to the Development Lifecycle, this stage often encompasses the Requirements phase, the Specification phase, the Design phase and sometimes Implementation and development phase.

Typical services NGS are tasked to deliver to our clients at this stage include:

- Workshops on security skills and techniques
- Workshops on topology and secure application data flow
- Design of application auditing and control functionality
- Infrastructure (both hardware and software) design
- Development of secure coding manuals
- Development of secure function libraries
- Secure Application Design training

The Middle of a Project

Having already committed development and infrastructure resources to the application development project and embarked on code delivery, the "middle" security stages of a project focus upon ensuring current code elements are sound. NGS will typically be involved in validating and helping with code elements that must be made secure, and providing milestone guidance on completed or upcoming components of a sophisticated application.

In the context of an application that has already been developed but is under continual "renewal", or developed by an external third-party, NGS have found that adding security controls to the QA & testing teams can provide immediate security improvements.

With regards to the Development Lifecycle, this stage often encompasses the Implementation and Development, Integration, QA & Testing phases, and sometimes Maintenance.

Typical services NGS are tasked to deliver to our clients at this stage include:

- Workshops – milestone reviews and summaries of completed phases
- Systems integration workshops
- Code review
- Application schematics and security logic reviews
- Staff supplementation for QA & Testing departments
- Application-level penetration testing of new code elements to live systems
- Specialist "knowledge transfer" exercises for operational support teams
- Milestone application security reviews
- Secure code development – providing technical authority, team leaders or actual coders

The End of a Project

This stage focuses upon applications that have been, or are about to be, deployed into live environments – after all development processes have essentially been completed. This stage encompasses the Integration, Deployment and Maintenance phases.

Typical services NGS are tasked to deliver to our clients at this stage include:

- Code review
- Application-level penetration testing
- Application schematics and security logic reviews
- Black-box, closed system testing

High Level Service Overview

Workshops

The purpose of workshops is to facilitate non-confrontational discussions about security issues and help address specific application concerns. NGS have found that workshops often represent the best "value for money" in addressing application security. By bringing together a maximum of 10-12 key client staff (e.g. developers, technical architects, technical project managers, etc.) the free-flow topical discussions facilitate an exchange of ideas and understanding. When focused upon a specific issue (such as understanding current application threats or how to implement single sign-on procedures) the workshop format enables all attendees to "work through" a problem and tackle the issue head on – resulting in greater understanding and more efficient solutions. Depending upon the workshop requirements, a typical workshop would last between 2-4 days and result in the creation of a final report detailing the discussions and all technical findings.

A workshop focused upon secure coding will typically increase the level of security awareness amongst developers and technical project managers – resulting in an all-round improvement in the quality of code produced – thus ultimately reducing the business risk of deploying new applications. Improvements in code quality can also have a marked effect on application reliability.

- **Secure Coding Workshops -** One of the most popular and efficient workshops, NGS can provide a bespoke secure coding workshop to improve the security awareness of developers and to demonstrate the theory and practice behind typical pitfalls. The workshop typically takes the form of interactive lectures designed for maximum knowledge transfer and relevancy and will therefore be tailored to the platforms on which developers operate. NGS believe it is vitally important that developers understand the true requirement for secure coding in addition to how to apply best practice standards. This workshop is ideally supplemented by the Application Testing Workshop, which demonstrates the methodology behind performing a security audit, and the techniques used in real attacks of which the application may well have to contend with.
- **Application Testing Workshop –** NGS can provide a bespoke application testing workshop that demonstrates the NGS methodology for performing a thorough application-level audit. The workshop takes the form of a demonstration application review and a discussion of the underlying methodology. The application testing workshop is of benefit to both developers and Testing personnel.
- **Application Design Workshops** – In some cases, organisations have identified an issue or business practice that could be addressed through the development of a custom application but do not know where to start. NGS is able to work through the application requirements and utilise the workshop format to understand the current infrastructure configuration. Working hand-in-hand with key personnel, NGS helps develop an integrated application solution that efficiently utilises current client resources and skills.
- **Threat Analysis Workshops** – Depending upon the nature of the application and the necessity to better understand the threats it may be exposed to, the Threat Analysis Workshop may prove beneficial. Typical audiences include security staff, key infrastructure managers and technical project managers. NGS consultants lead an open forum on the current threats and attack vectors with an emphasis on explaining not only the nature of the attack but the real likelihood. Attendees gain insight into the threats their applications are exposed to and help evolve solutions that will integrate into the current client environment.

Security Training Courses

In many circumstances instructor led security training courses may be used to address key application security issues for a greater number of developers and interested personnel. These courses are designed to impart a wealth of background security information to all participants – information that can be applied to current and future application developments. The instructor driven courses typically cater for class sizes between 8 to 40 attendees and can range from 1 to 4 days in length. Smaller classes make use of interactive examples,

while larger classes tend to be more lecture based.

These training courses can be delivered at the client premises or externally. In the majority of cases clients prefer to allocate a room on their own premises to cut down on expenses.

- **Secure Coding** – Tuned to address the development languages in use by the client, this course covers secure coding practices. Content ranges from understanding the necessities for content validation procedures and on to implementing content validation procedures in specific languages, through to efficient error handling and avoiding buffer overflow coding flaws.
- **Secure Web Application Design** – A suite of courses geared towards three streams of participants – application designers and coders, QA and testing personnel, and finally web application security authorities. These comprehensive courses cover all areas of web application design, examine common failings, and carefully explain the art of security compromise including how to thwart current attack vectors.
- **Bespoke Training** – Most commonly, clients ask NGS to deliver specific courses designed to address known deficiencies in their developer's knowledge base. These courses typically run for 1-2 days.

Design Consultancy

Utilising the experience of consultants that continually provide technical security advice to many of the worlds largest and most demanding organisations, NGS is capable of applying proven techniques from the cutting-edge of application design. The design consultancy services focus upon ensuring appropriate development techniques and procedures are incorporated efficiently within the applications. Working closely with the client's technical authorities, NGS is able to help design robust and secure functions capable of thwarting both targeted attacks and malicious threats.

Design consultancy engagements are typically scoped relative to the project size and application sophistication. For large projects, clients often find that having a skilled NGS consultant onsite for the first few weeks of application design help to bring order to nonexistent or chaotic security implementations. In many cases, even a few days invested in having NGS review proposed application designs can save many weeks of potentially lost development time or partially secured application functionality.

- **Design Authority –** NGS would typically provide experienced consultants to act as design authorities to ensure that the design phase of the development cycle produces a proactively secure application. Throughout this phase a strong emphasis is placed on knowledge transfer. This stage is ideally supplemented with NGS consultants acting as a secure coding authority during the implementation phase.
- **Design Review –** NGS can review design documentation and models to ensure that the application is secure before the implementation phase begins. This approach prevents the need to retrofit security, catching potential problems before they are implemented. Retrofitting security can be extremely expensive; it is therefore critical to the success of the project that it is designed securely from the ground up. Secure coding cannot mitigate against underlying design flaws.
- **Milestone Security Reviews –** For long-term software development projects that encompass multiple coding groups and project phases, clients find that milestone security reviews ensure a consistently high level of security integration. By ensuring that phase completion reviews include experienced security consultants, NGS clients have benefited from the identification of slipping security processes and open discussion on the significance of current security conciliations.

Code Reviews

Whether the application be web-based, compiled, or a combination of both, NGS maintains world leading skills in secure code development review. Globally renowned for their vulnerability research, NGS researchers and experienced consultants apply cutting-edge knowledge and development techniques to client application code reviews.

Many organisations rely on business critical applications developed by third parties with little knowledge of the quality of the code, nor the security awareness of the developers. This

introduces a business risk that is hard to quantify. A source code review provides a third party evaluation of the code that can be invaluable in calculating risk.

Using an efficient mix of automated discovery tools, optimised procedures and secure coding experience, NGS consultants regularly provide technical application code reviews designed to identify and uncover insecure development practices or potential attack vectors. The services are designed to identify security flaws and, just as importantly, provide detailed guidance on securing the applications code.

- **Source Code Change Review –** NGS offer a full or partial source code review to ensure developers are following best practice coding standards. Whilst security is a lesser priority to many developers, it is the main objective of a source code review. Depending on the findings, the review can be supplemented with a Secure Coding Workshop.
- **Source Code Review of Changes to Code Base –** Invariably the requirements for a project are likely to change often during the development cycle. Modifications should be subject to strict change control, documentation, security testing and regression testing. NGS often provides a partial source code review to ensure the changes will not adversely affect the system. This is an ideal supplement to a full source code review.
- **Secure Coding Authority –** NGS can provide experienced secure development consultants to act as a coding authority and ensure that the implementation phase of the project produces a secure code base that meets the design specifications. As with the design authority, a strong emphasis is placed on knowledge transfer.

Application Testing

NGS offers a range of services designed to assess the security of the application within test or live environments. These services focus upon identifying security failures within the deployed application and enumerate any application dependencies that could be exploited by an attacker. NGS consultants work to uncover these issues and provide detailed information about the application attack vectors that could be used to exploit the vulnerability, as well as providing comprehensive technical security advice on mitigating the issue.

These services are commonly applied to applications in their final state, and typically take between 5 and 20 days to conduct. The services are ideal for finding vulnerabilities in the final deployed application that could be exploited by malicious attack. In many cases clients use these services to validate the security of the application before going “live”.

- **Application Penetration Testing –** NGS provides best-of-breed application testing to catch both design and implementation flaws. NGS consultants take a holistic view of the security mechanisms in place and rigorously audit all aspects of application behaviour that contribute towards its overall security.
  Testing of any changes to the application codebase is critical since they could impact the functionality, reliability and security of the application. A follow on source code review of the changes ensures the full impact is understood.
- **Application Penetration Testing of Changes to Codebase –** In addition to, or in place of a source code review of changes to the application codebase, NGS consultants can also test a specific part of the application. This is an ideal supplement to a full application review, ensuring that the security of the application is not undermined by recent modifications.
- **Black-box Testing –** When clients have a new commercial application, or client software that will be deployed globally, NGS can provide “Black-box” testing facilities. The task of this testing is to identify vulnerabilities or installation security flaws that could be discovered and exploited by malicious attackers should they actively invest substantial time to “hack” the application. NGS consultants utilise a structured testing regime to identify probable flaws and then work closely with the application development teams to review the flawed code elements and devise robust solutions. This two-pronged approach enables a rapid turnaround for vulnerability classification and remediation information.

Staff Supplementation

In some circumstances clients may find themselves needing to apply security knowledge to an on going development project immediately, or are not are able to locate sufficiently skilled resources within their own organisation. In these cases NGS can provide the necessary skills by directly supplementing the clients existing technical staff with experienced professionals.

NGS are often contracted by clients to provide security expertise "on the ground" within key departments. This may be initiated through a compelling event (e.g. a recent successful attack against an application) or technical findings from another security project.

- **QA and Testing –** For organisations that outsource large components of their application development requirements, they may discover that their QA and Testing department has appropriate control procedures and powers to validate and authorise new code deployments. As such, for high priority projects, our clients sometimes find that adding security validation and review functions to this team provides an efficient method of ensuring only secure code makes its way to production systems. NGS can provide security consultants to immediately initiate these processes and embark on a knowledge transfer exercise to train internal QA and testing resources in to doing the same. The typical duration for such an exercise is of the region of 2-3 months.
- **Code Development –** Some application components require additional effort or technical skill to integrate critical security functions. NGS consultants are able to leverage the skills and experience of having developing their own award winning security software solutions and work with their clients to code important application components.
  In these instances, NGS effectively acts as an external software development facility – focused on developing technically demanding components. Examples of this service include the development of code encryption and watermarking processes for high value intellectual property components, development of network services and interfaces, and on to Internet distributable client-focused financial transaction components.

Knowledge Transfer Exercises

At any stage of the development lifecycle, NGS consultants may be called upon to provide expert advice on specific issues and attack vectors. Working hand-in-hand with our client's technical staff, we can ensure that not only does the issue get resolved, but also that the personnel who raised the issue fully understand the threat and remediation processes. These client personnel can then become technical authorities within the organisation and help to raise the overall level of security knowledge.

Next Steps

NGS are committed to working closely with our clients and actively strive to become their trusted security advisors. Any consulting engagement conducted by NGS emphasises knowledge transfer and is custom tuned to meet our client's specific requirements.

NGS can provide greater detail about all the professional services contained within this document and help develop a security solution that fits any business requirement. For more detail please contact us.

Email: appsecurity@ngssoftware.com
Phone: +44(0) 20 8401 0070
Web: http://www.ngssoftware.com

Authors: Gunter Ollmann, Sherief Hammad, John Heasman, Chris Anley -- June 2004