

Best Practices: ProveIT Case Study for U.S. Air Force Software Assurance Center of Excellence

United States Government Risk and Protection

MARKET OVERVIEW

#GI217305

Mark Kagan

GOVERNMENT INSIGHTS OPINION

ProveIT case studies provide government end users with assessments of IT solutions. Our methodology enables impact assessments to be comparable, consistent, and independent. Working with government and vendor personnel directly involved in the project, Government Insights analysts gathered relevant information on the project and provided our analysis of the approach, the solution's success in meeting the organization's stated goals, and the project's impact on return on investment, risk, innovation, and transformation. In addition:

- This ProveIT case study examines a U.S. Air Force initiative to implement application security/software assurance practices following the massive breach of an Air Force information system. The breach prompted the Air Force Electronic Systems Center (ESC) to establish the Application Software Assurance Center of Excellence (ASACoE) to raise awareness about the criticality of application security, implement Web- and database-level application monitoring, and train and mentor software developers to identify and repair existing software vulnerabilities and/or incorporate security into coding practices.
- Government Insights believes that the approach taken in creating the ASACoE, its approach to implementing software security, and its growing role in the Air Force to change the information assurance paradigm provide other government organizations and managers with a sound model for emulation.

TABLE OF CONTENTS

	P
In This Report	1
Methodology	1
Situation Overview	2
Business Needs	2
Management Challenges	2
The Approach	3
The Best Practices	11
Future Outlook	20
Essential Guidance	21
Actions to Consider	21
Learn More	21
Related Research	21

LIST OF FIGURES

	P
1 ASACoE Concept of Operations	4
2 Project Timeline	9
3 ROI Impact.....	12
4 Risk Management Impact.....	15
5 Transformation Impact	16
6 Innovation Impact.....	18

IN THIS REPORT

This ProveIT case study examines and analyzes the U.S. Air Force's Application Software Assurance Center of Excellence (ASACoE). The ASACoE was established to help prevent compromises of Air Force software applications, as well as to provide thought leadership and change management in the way the Air Force develops, acquires, implements, operates, and maintains its software.

Methodology

In a ProveIT case study, Government Insights analysts examine a stated business issue in a government organization and the IT approach that it took to address it, and then specifically analyze the return on investment, risk, transformation, and innovation factors involved in this solution. Return on investment looks at the operational costs and business value of the solution. Risk covers the situation complexity of the technology and the execution of the solution. Transformation covers the impact on delivery of an agency's mission, business processes, security implications, lessons learned, and a look back at how to do it better. Innovation involves leveraging best practices for scalability, repeatability, and replicability.

Government Insights interviewed the following people who are or were involved in the creation and operation of the ASACoE:

- Sean Barnum, Principal Consultant, Cigital Inc., which is a subcontractor to the ASACoE (Barnum is also a key participant in the Department of Homeland Security's Software Assurance Program.)
- Dan Bartko, Branch Chief, Application Security and Program Manager, Application Software Assurance Center of Excellence, 754th Electronic Systems Group (ELSG), Maxwell Air Force Base (AFB) - Gunter Annex, Alabama
- Greg Garcia, Director, 754th Electronic Systems Group, Maxwell AFB - Gunter Annex, Alabama
- Bruce Jenkins, Managing Consultant, Fortify Software Inc., which is a subcontractor to the ASACoE (Jenkins was an Air Force major and chief, Applications Security, 554th Electronic Systems Wing [ELSW], Air Force Electronic Systems Center, Hanscom AFB, Massachusetts, when he headed the effort that led to the establishment of the ASACoE.)
- Lt. Gen. Chuck Johnson, U.S. Air Force (ret.), Vice President, Air Force Network and Support Systems, The Boeing Company (Johnson formerly commanded the Air Force Electronic Systems Center, Hanscom AFB, Massachusetts, and began the initiative that resulted in the creation of the ASACoE.)

- Josh Saul, Vice President, Product Management, Application Security Inc., which is a subcontractor to the ASACoE
- Charisse Stokes, Program Manager and Senior Director, Southeast, Telos Corp., which is the prime contractor to the ASACoE
- Roger Thornton, Chief Technology Officer, Fortify Software, which is a subcontractor to the ASACoE
- Anthony Vicinelly, Federal Sales Engineer, Application Security, which is a subcontractor to the ASACoE

SITUATION OVERVIEW

Business Needs

The U.S. Air Force began realizing that it had been losing unknown quantities of data and information in such areas as command and control, logistics, personnel, scheduling, and even in classified research and development areas. These data losses came about as the Air Force moved from using closed systems or client-server systems to the open Web. Like the rest of the federal government, the Air Force was increasingly creating or acquiring Web-based systems or bolting on Web interfaces to legacy systems to open them up to outside systems and users — as well as threats and actual attacks.

As a result, the traditional "M&M" approach to IT security — a hard exterior shell that protects a soft center (i.e., an almost exclusive focus on perimeter and network security) — has become increasingly inadequate. A massive data breach in a major information system in 2005 brought home to one major Air Force agency the fact that serious vulnerabilities existed, requiring a new and long-term security focus.

Management Challenges

Today's Air Force relies heavily on software technologies to ensure the safety and security of its people and its mission. These software technologies are under increasing risks of attack and exploitation. However, the Air Force's approach to IT security, like most government and private sector organizations, has primarily focused on protecting the network and not the software applications and databases *within* the network. Many of these applications, which were originally designed and implemented before the Internet existed, are now connected to the Web and are especially vulnerable to attack and exploitation. At the same time, most Web-based software applications routinely suffer from the problem of vulnerabilities that may have been inadvertently embedded in their code.

In May 2005, a hacker breached the Air Force's Assignment Management System (AMS) at Randolph Air Force Base, Texas, and downloaded the personnel records of 33,000 Air Force officers — nearly half the officers in the Air Force. The AMS, which is managed by the Air Force Personnel Center at Randolph, is an online program used for assignment preferences and career management. The hacker used a legitimate user's log-in to access the system and did a password reset. The records included the names, social security numbers, places of birth, security clearance information, job histories, and so forth of officers from generals down to second lieutenants, making them — and the military — vulnerable to identity theft and social engineering attacks. To date, the Air Force has not been able to determine the hacker's identity or what happened to the information.

One officer whose personal record was compromised was Lt. Gen. Chuck Johnson, commander of the Air Force Electronic Systems Center, at Hanscom AFB, Massachusetts. The ESC develops, acquires, modernizes, and integrates net-centric command and control, intelligence, surveillance, and reconnaissance (C2ISR) capabilities, as well as combat support information systems, and provides warfighting commanders with battlefield situational awareness and accurate, relevant, decision-quality information on a global information grid. Johnson therefore had a professional and personal interest in determining why and how the breach had happened and, as commander of the ESC — which develops, acquires, operates, maintains, and protects thousands of critical IT systems across the Air Force — in doing something about it.

The Approach

Solution Description

The mission of the ASACoE is to:

- Foster security into the software development life cycle (SDLC) and software acquisitions through techniques, tools, and education
- Leverage information technology, through the deployment of practices and automated tools, to support and improve Air Force software development processes
- Take advantage of software assurance state-of-the-art information technology and industry best practices
- Shield and defend applications against potential attacks

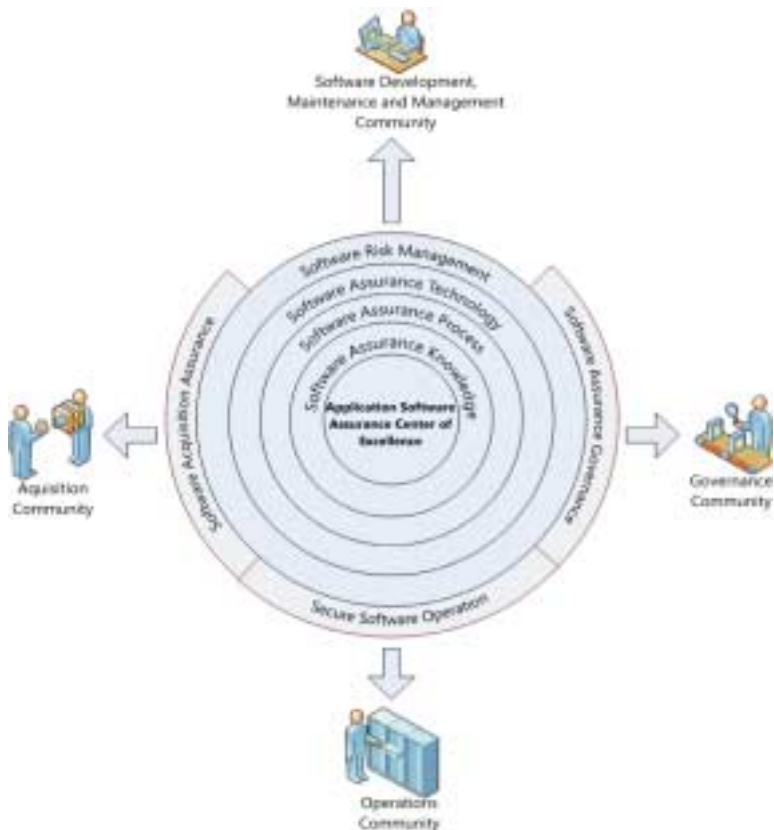
The goals of the ASACoE are twofold: defend against application-level compromises of government-developed/acquired and government-maintained automated information systems (AISs) and combat information systems (CISs); and change the ways in which the

Air Force develops, acquires, implements, and maintains the Air Force's applications by including security throughout the entire software development life cycle.

The ASACoE concept of operations (CONOPS) is to "provide expert guidance and support on software assurance issues to all relevant stakeholders throughout the Air Force and to address the full range of required software assurance capabilities." This is graphically represented in Figure 1.

FIGURE 1

ASACoE Concept of Operations



Source: Government Insights, 2009

The ASACoE program addresses the following comprehensive set of software assurance capabilities:

- **Software assurance knowledge.** Collect, categorize, map, transform, and disseminate relevant software assurance knowledge including policy, standards, and training

- **Software assurance process.** Create a framework to define software assurance best practices and enable their integration into diverse Air Force system engineering processes
- **Software assurance technology.** Research, identify, select, test, acquire, and deploy software assurance tools and techniques for use throughout the Air Force
- **Software risk management.** Partner with the software development community to provide capabilities for identification, mitigation, and prevention of potential exploitable weaknesses
- **Software acquisition assurance.** Support the definition and validation of software assurance requirements to ensure all software-inclusive programs achieve appropriate levels of desired assurance
- **Software assurance governance.** Support the development, integration, and certification of software assurance policy, standards, and compliance processes for systems governance throughout the Air Force
- **Secure software operation.** Support the development and integration of secure profiles, configurations, and processes to assist with secure software operations throughout the Air Force

The ASACoE program provides the following software assurance services and training to support the above capabilities:

- **Centralized project management.** Vulnerability trend analysis and reporting and view multiple projects in all functional areas
- **Portfolio risk assessment.** Understand risk posed by each application in an Air Force portfolio, prioritize for analysis, and prioritize for mitigation/remediation
- **Source code analysis (SCA).** Proactive security with targeted, accurate analysis tuned for low false positives
- **Penetration testing.** Scripted, controlled external probing of the application's security features
- **Database security analysis:** Penetration testing, configuration assessment, and ongoing monitoring and auditing of database activities
- **Code auditing.** Prebuild security auditing and analysis of the application's entire code base

- **Real-time analysis (RTA) and defense.** Monitor, prevent, and report on intrusion attempts against applications/databases
- **Training.** Provide training to diverse audiences on software assurance practices and tool usage

The ASACoE provides multiple levels of services:

- **Triage risk assessment.** Offers three days of training; five days of tool installs, scanning, analysis, and mentoring; and five days of analysis and assessment report writing
- **Training and tools (no assessment).** Offers 3 days of training and 2.5 days of tool installs
- **Assessment only (no training and no tools).** Offers five days of scanning and analysis and five days of assessment report writing
- **Detailed risk assessment.** Offers everything involved in a triage risk assessment plus 5–10 additional days of architectural risk analysis and 5–10 additional days of focused manual code review and targeted penetration testing

The ASACoE can pull, as needed, from a broad software assurance training curriculum. Training provided so far under the program has fallen into two different training packages — one focused on program management offices (PMOs) and the other focused on testing organizations.

Program management office training courses include the following curriculum: defensive programming (one day), Fortify SCA training (one day), Application Security AppDetective training (one/two days), and Fortify Manager and Fortify RTA (one/two days).

Testing organization courses include the following curriculum: risk-based security testing (one day); IBM/Rational AppScan training (one day); and Fortify SCA, Manager and Program Trace Analyzer (PTA), Application Security AppDetective training (one day).

Selecting the Solution

Following the discovery of the data compromise, Johnson initiated an effort to analyze the AMS breach and the entire issue of application security. The ESC created a Crisis Action Team (CAT) to understand and address what specifically had happened and, more broadly, the issue of vulnerabilities and threats inside the network perimeter. It was then tasked with determining how the Air Force could mitigate or reduce the risk of similar breaches in the future to other applications and coming up with a long-term strategy to deal with application and software security.

Part of the CAT effort involved interviewing security officials from the banking, power, oil and gas, and transportation industries to learn how they dealt with application security and data loss. The CAT and Johnson also talked with a number of software companies to acquire insights into how they developed software and what they were doing to ensure the integrity and security of their products. The ESC sought guidance from the software assurance programs sponsored by the Department of Defense and the Department of Homeland Security. It also issued a request for information (RFI) to find out the companies that were involved in the field of application security and that could help the ESC define the problem so it could issue a request for proposal (RFP) to find a solution.

One of the CAT's recommendations was the creation of a center of excellence that would address the issue of application security on behalf of the Air Force. However, prior to the creation of such a center, the ESC tasked the 554th Electronic Systems Wing to conduct a pilot software assurance program during January–November 2006 to evaluate tools and solutions for scanning source code that could be used by software developers to identify vulnerabilities that could compromise systems. After conducting extensive market research, the pilot program did a limited assessment among a variety of different vendors and tools, at the end of which it became evident that there was more to application security than using just source code analysis tools.

Code analysis can identify potential or existing issues within code, but it doesn't change the code itself. The pilot determined that penetration testing was also necessary to assess an application's ability to protect itself. It also determined that it was critical to have a special focus on database security and examine security policies for live database traffic, including legitimate and illegitimate activities.

Finally, the pilot concluded that approaching security as a "bolt on" to application development and security was potentially not the most cost-effective approach. The Air Force would take years to do code scans on all its applications — and it wouldn't really change anything, according to Bruce Jenkins, managing consultant at Fortify Software. He was an Air Force major and chief, Applications Security, 554th Electronic Systems Wing, Electronic Systems Center, Hanscom Air Force Base, Massachusetts, who led the CAT and the pilot.

"Even if we fixed the software, we would still have problems because the developers building software would still be building it with problems," says Jenkins. Therefore, it was necessary to adopt a more comprehensive approach that incorporated understanding of and implementing good coding practices — including planning, risk assessment, and enterprise architecture — and identifying, integrating, and ensuring security in all areas of software development and deployment.

The Air Force also needed to strengthen its abilities to build or purchase software in the future to ensure that its software could defend itself. "We needed to build our software the way we build our planes," says Johnson. "If we don't build them strong and reliable, they are going to fall out of the sky or be shot down when they go on a mission. The same philosophy should apply to our software."

Implementing the Solution

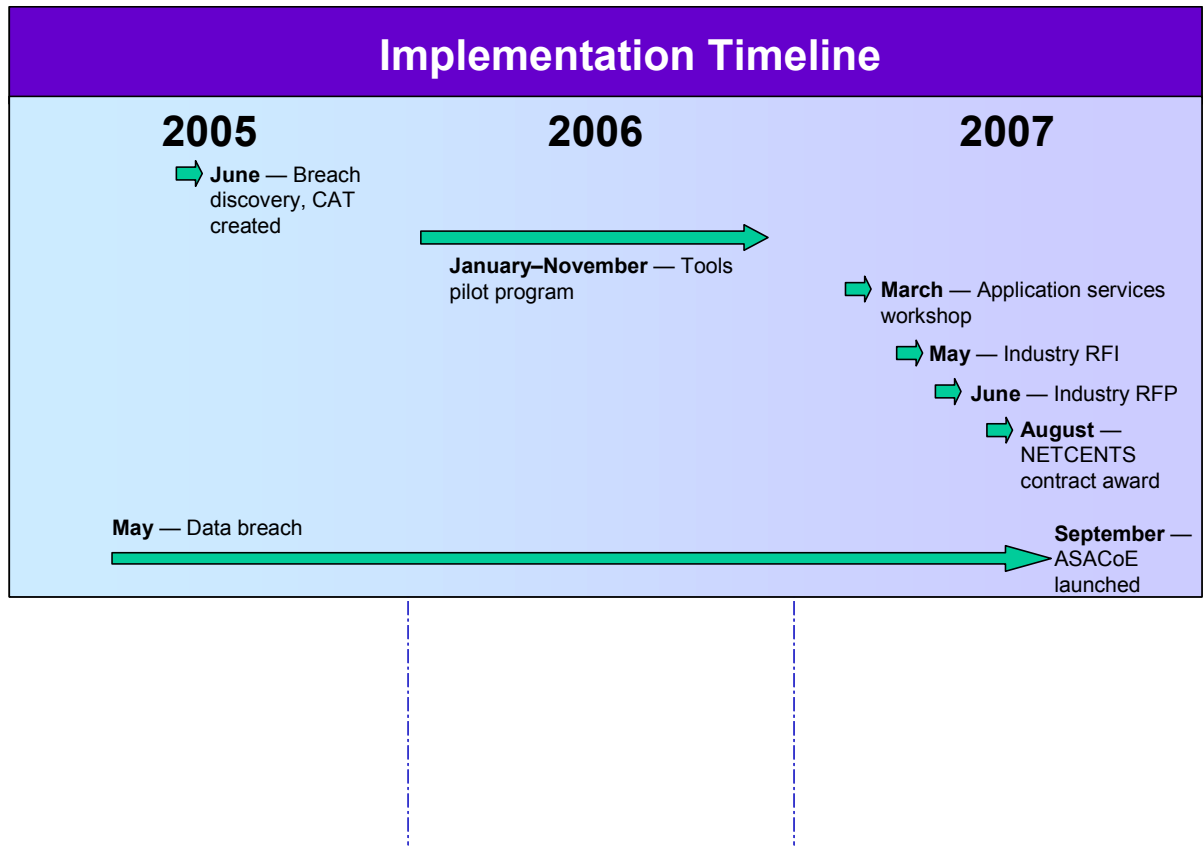
The ESC paid for the initial activities of the CAT and the pilot program by leveraging existing funds from programs that would benefit from a software assurance program. "The process was the same as if we were going to 'mod' an airplane," states Johnson.

The ESC stood up the ASACoE on August 31, 2007, under the management of the 754th Electronic Systems Group at Maxwell AFB - Gunter Annex, Alabama. After receiving half a dozen proposals, the ESC awarded a \$10.2 million contract under the Network Centric Solutions (NETCENTS) procurement vehicle to a team led by prime contractor Telos to provide software assurance tools and services. The award was made on the basis of "best value," that is, the inclusion of tools that would cover the best range of codes and hosting schema, the ease of use of those tools, training, thought leadership, services capability, and the ability to pull all that together and deliver a total solution to the Air Force.

During the next 14 months, the ASACoE identified 2,588 government off-the-shelf (GOTS) applications, collected actionable data from more than 200 applications, and conducted assessments on more than 150 applications in more than 35 program management offices. Initially, the ASACoE started with organizations within the ESC and has since started reaching out to other Air Force organizations, as well as the Air National Guard and Reserve. Figure 2 shows the project timeline.

FIGURE 2

Project Timeline



Source: Government Insights, 2009

As of this writing, the ASACoE has trained 332 developers in mixed Air Force/contractor teams. The training tries to address the full spectrum of application development. "We don't just give them the fish, we teach them *how to fish* when it comes to software coding practices, how to use the tools, and actually running the tools on applications," states Fortify's Jenkins. "We also don't want it to be a one-time snapshot and then you forget about it; we want to build it into a continuous process of assessment."

There are usually four classes held each month, with 20 students in each class. The ASACoE expects to train at least another 300–400 developers, and as many as 480, by the end of August 2009.

The Players

- **Telos.** Prime contractor Telos is a systems integration and services company that provides IT security solutions to government agencies and commercial organizations. Specific offerings consist

of Xacta's Secure Solutions, which include enterprise IT security management solutions, enterprise security consulting services, enterprise messaging, secure networking, and high assurance credentialing solutions. Telos functions as the lead for developing and executing the ASACoE program under Air Force direction and draws expertise from a team of four companies: Application Security, Cigital, Fortify Software, and IBM/Rational.

- **Application Security.** Through its flagship products DbProtect and AppDetectivePro, Application Security provides complete database security solutions that empower organizations to monitor and protect their most critical assets in real time while simplifying audits and automating-compliance requirements. DbProtect is a centrally managed enterprise solution for comprehensive database security, combining discovery, vulnerability scanning, real-time activity monitoring, and auditing. AppDetectivePro is a network-based vulnerability assessment scanner that discovers database applications and assesses their security strength. It uses industry best practices and proven security methodologies to locate, examine, report on, and fix security holes and misconfigurations to protect organizations from internal and external database threats.
- **Cigital.** Cigital, including its wholly owned subsidiary Cigital Federal, is a software security and quality consulting firm focused on helping organizations improve software. Its consultants specialize in programs that empower companies and government agencies to ensure their software applications are secure and reliable while enabling them to significantly improve how they build and deploy software. In addition to being the software assurance subject matter expert for Telos, Cigital is providing the ASACoE with software security analysis and engineering services that include organizational risk assessment and planning, application risk assessments, portfolio risk assessment and management, collaborative mentoring, and other application security supporting services. It is also helping to identify and implement best practices for integrating security into all areas of the Air Force's software development processes.
- **Fortify Software.** Fortify's software security assurance products and services protect companies from the threats posed by security flaws in business-critical software applications. Its Fortify 360 software security suite automates key processes of developing and deploying secure applications. Fortify 360's Real Time Analyzer (RTA) component is being used to apply a shield onto existing applications to block hackers and help the Air Force protect itself from the immediate risk of vulnerabilities in production software. In quality assurance (QA), Fortify 360's Program Trace Analyzer (PTA) is used to find vulnerabilities as a part of the QA process. The Fortify 360 Source Code Analyzer (SCA) examines every line of code and every program path to identify hundreds of different

types of potentially exploitable vulnerabilities early in the development life cycle. It is also used to help developers clean up legacy application code.

- **IBM/Rational/Watchfire.** IBM Rational solutions are targeted combinations of products, services, and best practices based on the open and modular IBM Rational Software Delivery Platform. The IBM/Rational/Watchfire AppScan is an automated Web application security scanner that identifies, validates, and reports on application security vulnerabilities. AppScan offers a solution for all types of outsourced and in-house security testing for all types of users — application developers, quality assurance, penetration testers, security auditors, and senior management. IBM acquired Watchfire Corp. in July 2007 to broaden its security and compliance management capabilities in the software development life cycle. IBM integrated its Rational software quality management solutions with Watchfire's application vulnerability assessment and compliance testing services to enhance and simplify the Web application development process.

The Best Practices

Business Value — ProveIT Assessment

The following ProveIT business value assessments are based upon Government Insights' collective evaluation of the ASACoE solution in the areas of return on investment, risk, transformation, and innovation.

Return on Investment

Return on investment examines the operational costs and business value of the solution.

Return on investment for security is notoriously difficult to calculate, since loss of confidentiality, integrity, or availability of a system is rarely a pure black or white thing. "We can effectively track relative metrics around the increased assurance of software (e.g., number of vulnerabilities found in a baseline analysis that are not present in future analysis) brought about through applying ASACoE activities and contributions," says Cigital Principal Consultant Sean Barnum.

Fortify's Jenkins believes that it is still too early to determine a quantifiable ROI for the ASACoE's awareness, assessment, repair, and training program. "We still need to quantify the costs associated with data compromises and system downtime," says Jenkins. "We are not yet able to show the cost avoidance if we demonstrate problems and then fix them versus what we would have lost."

Nevertheless, 754th ELSG Director Greg Garcia puts it in these terms for program managers in other agencies: "What's the ROI of *not* losing 33,000 names and social security numbers. I don't think I can quantify

that. It's not necessarily the dollar value — it's the mission loss, it's the downtime, and it's the nonperformance of the application that's at risk. I would rather tell them that their application has mission integrity and when they need that mission capability to be there it will be there, and it will perform as designed."

The ASACoE does expect that by September 2009 it will have collected sufficient metrics, including follow-up scans of applications that were assessed, to be able to quantify the cost savings.

One area that should yield a quantifiable ROI is a comparison of the time and costs of manually reviewing software code versus using the Fortify Software, Application Security, and IBM/Rational automated solutions. This would be especially valid in the case of software applications with millions of lines of code.

The ASACoE has been up and running for only 18 months, as of March 2009, and it will not have collected relevant and useful ROI metrics until the fall of 2009. Determining an ROI on security is also complicated because, more often than not, it involves "measuring" a negative or absence, such as system uptime or mission capability versus potential downtime or lack of mission capability — and this case is certainly no exception. Government Insights will revisit this issue in a year and determine if a new — and presumably higher — ROI impact is merited.

The ASACoE solution is relatively immature and we note the inherent difficulties of measuring security ROIs, but our initial assessment comes in just above the midimpact range. Figure 3 shows the ROI impact level.

FIGURE 3

ROI Impact



Source: Government Insights, 2009

Risk

Risk covers the situational complexity of the technology (including specific technology, legacy environment, and scale) and the execution complexity (crossorganizational governance, organizational culture, and program planning and management) of the solution.

According to everyone interviewed for this case study, the biggest risk was — and is — not doing anything about software vulnerabilities. These vulnerabilities exist at each tier of the application infrastructure, including the Web front-end, middleware, and even the back-end database where all the sensitive application data is stored. The ASACoE has been carrying out risk assessments to identify the Air Force systems most at risk to focus limited resources in the most effective ways. In many cases, the risk assessments are complicated by the fact that they involve very complex systems, not just simple Web-based applications, and multiple systems that interact with and/or are part of a larger system.

There are also risks because the tools and solutions used by the ASACoE teams may not catch all the vulnerabilities in an application or system. According to Cigital's Barnum, "the current triage risk assessments are quick and shallow analyses and will inherently not find a broad set of issues (including design flaws) that only a deeper and more detailed analysis could find. Triage risk assessments are a starting point for these programs, not an end point."

The tools are also not designed to assess and/or repair all types and "flavors" of software and such tools may, in fact, not exist at this time, particularly for such "obsolete" software languages as COBOL and FORTRAN. On the other hand, "while it would be great to have and use 100 tools to assess a much wider range of software applications and their potential vulnerabilities, we would never finish the assessments and the training costs would be prohibitive," says ASACoE Program Manager Dan Bartko.

Because there is not yet an Air Force-wide mandate, the ASACoE is relying on those Air Force organizations, which have become aware of the application assurance program to approach the ASACoE, or the ASACoE approaches organizations and asks them if they would like to participate. Assuming that more than one organization is lined up at any given time, the ASACoE uses a portfolio risk assessment methodology to determine the systems that would probably provide greater returns on investment. This is based upon such factors as system sensitivity, mission criticality, and who accesses the system.

The solutions and techniques used by the ASACoE, the training that it provides, and the awareness campaign that it is implementing do not involve a high-risk level, either in the complexity of their technology or their execution. However, there is a level of risk in that the amount of training provided to software developers at various Air Force organizations may not have been sufficient to enable them to make the best use of the tools.

There is a risk that in the absence of a senior-level mandate, some organizations may not cooperate with the ASACoE, which may be explained by one or more reasons. In the absence of current attacks or hacks, an organization may not wish to know about its possible

application vulnerabilities since their identification would require the allocation of scarce resources to repair them. In addition, the ASACoE's heuristic and holistic approach requires changes in the ways organizations operate and do business. These are fundamentally cultural and business process changes that are typically the hardest things for organizations to do.

Organizations may also resist making the changes, even if they welcome the ASACoE teams to assess their applications, because incorporating software assurance processes into their application acquisition and/or development life cycle will most probably lengthen delivery schedules. Thus, organizations will have to modify their approach to costs and benefits and incentives and penalties — which returns them to the issue of cultural and business process changes. For all these reasons, a senior-level mandate and priority is *critical* to the success of a software assurance program.

It must be noted that the ASACoE has so far encountered mostly positive and even enthusiastic responses to its efforts in the Air Force organizations where it has carried out training and assessments. "The usual reaction of developers when we show them what they've been missing and the vulnerabilities in their software is, 'Wow! I didn't know that. No one ever told (taught) me before,'" observes Bartko, ASACoE program manager. "They are always very happy to learn this so that they can get it right in the future."

False Positives and False Negatives

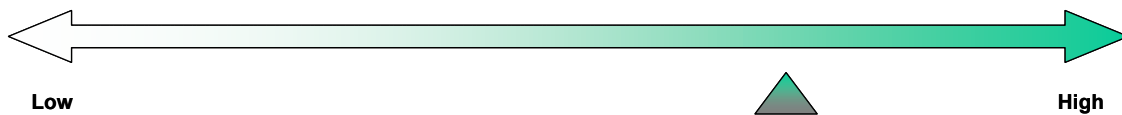
- **Source code false positives.** Static source code analysis tools such as Fortify 360 SCA typically err on the side of inclusion rather than exclusion when analyzing code. This means that they would rather point out issues that "might" or "might not" be problems rather than only report 100% confidence findings and perhaps miss reporting some real issues (false negatives). These false positives reported by the tools require time to evaluate and analyze to rule them out. The Fortify 360 SCA assigns every issue a confidence level and a severity level. The issues are then presented so that the most severe and most likely issues appear first. The ASACoE specifies for the customer a set of filters so that issues can be grouped according to the ASACoE's classified system. Based upon the needs of the customers, entire categories of errors can be disabled. This allows the customers to identify the important bugs more quickly and ensures that false positives never reappear in subsequent scans.
- **Source code false negatives.** False negatives are much rarer, but when one is suspected, relevant data is collected and forwarded to the Fortify Security Research Group (SRG) for evaluation. If the SRG confirms the false negative, it issues a notice to the ASACoE and the issue is tracked as a product defect until it is resolved in a subsequent product version release.

The results of IBM/Rational AppScan penetration testing are compared with the Fortify 360 results to identify whether any penetration test "positive" results are invalid and can thus be filtered out of the results set.

The situational complexity for designing and implementing this solution was relatively low, while the situational execution was higher — but not high. However, the Air Force ESC did not try to reinvent the wheel or invent something to replace the wheel. It used existing best practices and COTS solutions, which effectively reduced the level of risk because they did not require designing and executing a program and technologies from scratch. Figure 4 shows the risk management impact level.

FIGURE 4

Risk Management Impact



Source: Government Insights, 2009

Transformation

Transformation covers the impact on delivery of an agency's mission, business processes, security implications, lessons learned, and a look back at how to do it better.

The creation and operation of the ASACoE represents a transformation in the way the Air Force looks at and implements IT security from a network- and perimeter-centric focus to a more holistic approach. The goal is that in another three to five years, application security will no longer be an "add-on" but will have become a natural part of the way the Air Force develops or acquires and fields and maintains IT systems.

However, it is still a work in progress, and it has been mostly confined to ESC organizations so far. But as the ASACoE's Air Force personnel move on to other positions in the Air Force, it is expected that they will teach others what they have learned and practiced and will "evangelize" the importance of and need to ensure application security.

The ASACoE is holding discussions with the Air Education Training Command (AETC) at Keesler AFB, Biloxi, Mississippi, about providing training to its software development students, either at

Keesler or at Gunter Annex. The AETC software development curriculum does not currently include formal training in software or application security. Providing such training would help to ensure that Air Force software developers include security from the ground up in the software life cycle.

ASACoE teams have discovered in some offices when they come to do an assessment that there are already software assurance tools sitting on the shelf — unused. "To avoid 'shelfware syndrome' it is critical that organizations understand the role that tools will play in their practices and deploy them with an appropriate level of training, mentoring, and process integration," says Cigital's Barnum. "Tools are not silver bullets that 'bring down the werewolf' on their own. They exist to support good practices, not replace them." Therefore, the teams provide the training, mentoring, and follow-up to ensure that after they leave, the techniques and processes will continue to be followed and the tools will continue to be used.

The creation and activities of the ASACoE constitute a paradigm shift in the Air Force's approach to security, which will eventually significantly improve the level of security across the Air Force and potentially other government agencies. The impact could be higher in this case, but it is not higher because it is still mostly confined to the ESC, and not evenly across all ESC organizations. Figure 5 shows the transformation impact level.

FIGURE 5

Transformation Impact



Source: Government Insights, 2009

Innovation

Innovation covers the solution's leveragability to gain value including scalability, repeatability, and replicability.

The ASACoE is spearheading a shift to a heuristically based assessment of application behavior, according to Garcia, director of the 754th Electronic Systems Group, Maxwell Air Force Base - Gunter Annex, Alabama, which manages the ASACoE. "Not only are we working to define the behavior of applications to standards, but we are now monitoring and tracking differences in user behavior."

Garcia has requested that every software program within the 754th ELSG be assessed. The 554th Electronic Systems Wing, which manages the 754th ELSG, is currently considering that this should become a mandatory policy for the wing's programs. The ESC is creating a prioritized list of the ELSW's applications of greatest concern with the goal of carrying out assessments on them.

Scalability

The strategic concept of operations, structure, and processes of the ASACoE are designed to be extremely flexible and scalable in the breadth of capability addressed, depth of analysis provided, and the tempo of service provision.

The ASACoE currently can use the same process to assess and repair very small applications (hundreds of lines of source code) and larger, more complex applications (millions of lines of code and/or multiple programming languages). The only limiting factor is the time it takes to prepare the application for scanning and then conducting the scan (source code, penetration, and database tests). The ASACoE teams generally schedule five days for an assessment, but they can sometimes be completed in one to two days and sometimes in four to five days, depending on the size and complexity of the application.

The ASACoE, which currently has six four-person assessment teams, can handle as few as one assessment or as many as six assessments simultaneously. Scaling up the scope of its operations will depend on the three "Ms" of mandate, money, and man power, although its "training the trainers" activities will have a multiplier effect that should reduce — but not eliminate — the need for additional man power.

Repeatability

The current assessment process is highly scripted and easily repeated. From the moment an assessment engagement is scheduled, checklists are used for everything — from determining the customer's technology to completing the final report. The process is constantly refined by means of weekly "lessons learned" meetings, which are held to identify weaknesses and shortcomings. If necessary, the checklists are then updated to reflect any changes made during these meetings.

Replicability

The ASACoE model appears to be one that could be easily duplicated in other government agencies, including the design, setup, training processes, product installation, coaching/mentoring, and final report writing that includes a mitigation strategy. The ASACoE is also in a position — and more than willing — to provide advice and best practices for all these activities to other government agencies.

The ASACoE program rates very high in all three areas of scalability, repeatability, and replicability. Depending on the applications of mandate, money, and man power, the ASACoE's activities and/or model could be expanded with relative ease across the rest of the Air Force and then across the Department of Defense. It also provides a tested "how to do it" model for the rest of the federal government. Alternatively, an expanded ASACoE could be a "shared services" application security provider for the federal government, or it could assist in setting up additional and similar centers of excellence that would be shared services providers. Figure 6 shows the innovation impact level.

FIGURE 6

Innovation Impact



Source: Government Insights, 2009

Lessons Learned

The ASACoE has derived a number of best practices in the course of setting up the center, choosing its tools, training developers, and assessing and repairing applications and databases. The most important best practice is understanding that security is a continuous process that must be constantly addressed and readdressed. It cannot be viewed as a one-time thing or a snapshot because the threat keeps evolving. At the same time, the ASACoE continually refines its techniques and procedures to improve its total effectiveness.

Some other best practices can be summarized as follows:

- **Think strategically, act tactically.** While it is critical to understand how software assurance integrates into the organization, it is not possible to swallow the entire elephant at once and succeed. Find a couple of areas where you can effect the most change quickly and use them as fulcrums to leverage wider change and which have the greatest chance for success, and tackle these first. Then incrementally deal with the rest of the strategic problem, gradually building capability in an architectural fashion.
- **Create an awareness campaign.** It is absolutely critical that everyone involved in acquiring, developing, and fielding software applications, especially program and acquisition managers, be

made aware of the security risks and what a software assurance effort is all about. They must be made aware of the threats and vulnerabilities to their systems and data and that there are programs to deal with them. The worst thing is for an organization like the ASACoE to walk into an organization and say, "We are here to help" and it says, "Who are you and help with what?"

- **Obtain senior leadership buy-in and mandate.** You need to get the leadership to accept the importance of application security and make it a priority for their organization. They need to tell their organization that it's critical from both a mission standpoint and a business standpoint and that this is how they are going to proceed. Senior leadership needs to tell their people that there will be incentives if they play and consequences if they don't, such as their applications will go offline unless they fix their problems.
- **Provide robust training and education.** The ASACoE currently provides a three-day training program for developers, managers, and quality assurance providers. This may be effective and sufficient in organizations in which the program staff is already familiar with software security concepts and with some or all of the tools, technologies, and techniques. However, stakeholders in other organizations may be unfamiliar with software security concepts and tools and, consequently, three days may be too short. This may lead to inconsistent results.
- **Acquire familiarity with an organization's culture.** Do not assume that an organization understands application security or is willing to participate in assessments. Furthermore, the levels of understanding and willingness vary among organizations. A "one size fits all" approach for training and awareness campaigns may be less than effective in different organizations.
- **Understand the technological landscape.** You can do everything else correctly but still fail in performing an assessment if you don't understand the technologies you may encounter at an organization. Although the ASACoE does technology surveys of organizations prior to doing assessments, the people who answer those surveys may not have a clear picture of what's being used to develop their applications. For example, they may think they have Java applications, but they are actually Cold Fusion and .NET with a little Java. As a result, the ASACoE assessment team may not be able to conduct a full assessment of specific elements embedded in the applications. Knowing this up front increases productivity and helps manage expectations.
- **Collect useful and actionable metrics.** Ensure that the people involved collect the right metrics for the right reasons and understand why they are collecting them. Otherwise, you waste their time and resources and the metrics they collect — if they

don't ignore you — will present an incorrect picture of reality. Ensure that they don't collect too many metrics when all you need is three. You don't want to burn out people by having them spending all their time collecting metrics.

- **Use a toolkit, not a tool.** No one type of tool can cover all aspects of the software development life cycle nor can one type of tool identify and/or repair all application vulnerabilities. Tools from different vendors look for the same issues in different ways or cover different technical contexts. Use at least one tool to support at least one perspective of analysis, although it is better to use more than one tool to cover as many perspectives as possible. Similarly, no one tool is capable of finding all issues potentially identifiable through any one form of analysis. It is important to note, however, that while a toolbox approach is most effective, it is important for effective adoption that it be pursued gradually and not all at once. The ASACoE chose to start with a toolbox covering multiple different perspectives of analysis but only one tool for each perspective.

FUTURE OUTLOOK

Under the FY10 Program Objective Memorandum (POM), the ASACoE will come under the 24th Air Force (Cyber Command) and will expand its efforts beyond the ESC to the rest of the Air Force. This would potentially mean that (increased) funding for the ASACoE would come from the cyber command or from Air Force staff.

The 754th ELSG intends to issue a new RFP in May 2009 and award a contract in August. The ASACoE is considering a contract term of one year with four to five one-year options. It will look for new tools that may be more effective or that can cover additional vulnerabilities, such as in FORTRAN and COBOL, so it can advance closer to the goal of assessing 100% of the code in each application.

The ASACoE is working with the 643rd Electronic Systems Squadron (ELSS), Maxwell AFB - Gunter Annex to incorporate application assurance into systems engineering process (SEP) work. It is also in touch with the other military services (Army, Navy, and Marine Corps), as well as the Department of Homeland Security to increase their awareness of the progress and lessons learned at the ASACoE and within the Air Force. The ASACoE is talking with the Air Force CIO to get a certification and accreditation process for software testing and tools implemented across the Air Force. It is also working to have application software assurance requirements incorporated into the acquisition process, including boilerplate language for future contracts.

ESSENTIAL GUIDANCE

Actions to Consider

Government agencies must proactively address the issue of application security/software assurance and, if they have not already started, begin the process of changing to a more holistic approach to security that goes beyond perimeter and network defense. Data-at-rest encryption solutions that are being implemented under Office of Management and Budget (OMB) mandates will only mitigate part of the problem; they are not a full solution. It is not a question of *if* an agency's applications will be attacked and potentially devastating data losses will occur, but when. Based on the experience of the Air Force's ASACoE, Government Insights recommends that other government agencies start taking the following steps:

- **Make application security a senior-level mandate and make funding available to do more than pay lip service to it.** Without senior executive buy-in and without funding, any application security campaign will go nowhere, while giving the false and dangerous impression that "something" is being done.
- **Create an awareness campaign about the dangers posed by application vulnerabilities and the practices and supporting tools available to counter them.** Part of this campaign should include the concept that security must be seen as an *investment* and not as an expense — a notion that goes far beyond the arena of application or database security.
- **Begin the process of creating a center of excellence.** Whatever name is used, a centralized office is needed to establish and coordinate software security policies, evaluate and choose tools, train developers to assess and repair software applications, and train agency and contractor developers to incorporate security into the entire software development life cycle. To this end, agencies should not try to reinvent the wheel but should look to the example of the ASACoE and seek its guidance in how to go about creating their own centers and training programs.

LEARN MORE

Related Research

- *U.S. Department of Defense IT Security Initiatives, FY09: Overview and Analysis* (Government Insights #GI215453, December 2008)

Copyright Notice

Copyright 2009 Government Insights, an IDC company. Reproduction without written permission is completely forbidden. External Publication of Government Insights Information and Data: Any Government Insights information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate Government Insights Vice President. A draft of the proposed document should accompany any such request. Government Insights reserves the right to deny approval of external usage for any reason.

Published Under Services: Government Insights: United States
Government Risk and Protection