

Top 10 Security Trends in 2005

Executive Insight Series

Jonathan Gossels

Introduction

This article was prepared at the request of the editor of the CIO Magazine. It is scheduled for publication in January, 2006.

In the autumn of each year, SystemExperts reflects on the hundreds of projects we've completed and the thousands of discussions we've had with clients and prospective clients about their security concerns and attempts to distill key trends. Not surprisingly, in the list below you will notice certain topics that we have noted in the past – that is the nature of trends. That said, because the security space is so dynamic we never fail to see something new.

2005 in Review

2005 saw no earth shaking developments that changed the security landscape. However, it was anything but a quiet year – it was a year in which the security profession made great strides in practicing what it previously only preached. In the United States, the obvious catalysts were regulatory requirements such as Sarbanes Oxley and Homeland Security. These factors were further energized by auditing standards evolving toward continuous compliance monitoring and by natural disasters such as Hurricane Katrina. In the world of security, 2005 has been a year of evolution and progress.

Let's look at five overarching trends and five evolutionary developments.

Overarching Trends

Regulatory Compliance

It is not unfair to characterize 2005 as the year that security and privacy regulations hit home. Whether talking about Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley Act, Health Insurance Portability and Accountability Act (HIPAA), California Senate Bill No. 1386 (sections 1798.29 and 1798.82 of California Civil Code) or the EU's

Privacy and Electronic Communications (Directive 2002/58) and the Data Protection Directive (Directive 95/46/EC), these laws have certain key concepts in common: accountability, protection of personal private information, disclosure of disclosure policies, and integrity of reported information. Taken together, they are changing the way senior corporate managers view security; security is no longer just an arcane function within IT. It is personal and it is relevant.

In this context, the very nature of security reviews and security assessments is changing. Increasingly, organizations want their applications, infrastructure, and operations reviewed against well recognized standards such as ISO 17799 or the relevant sections of COBIT. These standards have value - we've seen even security savvy companies benefit from these more formalized reviews.

Commoditization of Security Tasks

As security tools and products have continued to evolve and as security skills become more prevalent, many activities that were once considered leading edge and required genuine experts to perform have become routine. This has enabled many organizations to do a better job at ongoing security-hygiene.

Other organizations have chosen to take advantage of the corresponding commoditization of these routine services to offload these tasks from their higher paid staff. This has largely been a customer-driven rather than a vendor-driven change. To illustrate, one of SystemExperts's most popular new services in 2005 has been our enhanced Security Blanket service. Its genesis was back-to-back requests by two key clients, not a service we dreamed up and decided to market.

These routine services differ from the traditional managed security service provider offerings which historically, have focused on perimeter monitoring and incident response. Examples of the types of work that these companies

wanted to offload were: tool based Internet perimeter scanning, TCP/IP service monitoring, monitoring for web page defacement, monitoring for OS and product patch availability, Virus-Worm-Trojan alerting, monitoring of hacker communities, and monitoring for domain expiration. These components are often part of a vulnerability management program.

Acceleration of Timeframes

One of the most profound impacts of the Internet on the world of IT has been the acceleration of time frames. Web applications are usually conceived, developed, and deployed quickly. In many cases, organizations bypass their time-tested application development process (design review, code review, unit testing, and integration testing).

Administrative timeframes are compressed as well. While formerly it was acceptable to deploy software patches and updates over a period of weeks and months, that time frame has now shrunk to hours and days. The same holds true for virus protection.

While the old time frames will not come back, many organizations are beginning to formally address the obvious deficiencies. For example, leading financial institutions are once again requiring security design reviews early in the application development process. They are also requiring security code reviews for critical applications. It is important to remember that disciplined processes may seem like they add to the time to market, but they actually help to ensure that good, secure products are delivered more quickly and avoids the high costs of repairing a fundamentally flawed application late in the development cycle.

Transition to Defense-in-Depth

Technological change and evolving business models have made the old concept of an enterprise perimeter obsolete. VPN technology, the use of protocols (like HTTP) that are allowed to pass through firewalls, and the extension of networks to encompass outside service providers and business partners illustrate this point.

While most organizations recognize the inevitability of implementing defense-in-depth, many find themselves in the early stages of transition. A small number of people within these enterprises are beginning to think about security architecture in terms of zones of risk and zones of trust and they are beginning to put plans in place to instrument what had previously been considered *the inside* to detect security problems. The vast majority, however, still

perform their day-to-day roles as if the outside is hostile and the inside is safe.

Managing Complexity

As security becomes integrated into the fabric of an enterprise, keeping track of all of the security-related activities and aligning project priorities across multiple departments becomes a major challenge. Organizations need a way to visualize and manage their security state over time. Many companies have had success in using a color-coded summary chart that is often called a *security-dashboard*.

The security dashboard enables senior management to understand, at a glance, which security-related activities are green, yellow, or red, prioritize spending to mitigate problems, and align security projects with corporate initiatives. It is instructive to keep in mind that the purpose of the dashboard is to help visualize the big picture - is not a mathematical formula that determines risk.

Evolutionary Developments

Renewed Emphasis on Identity Management and Authentication

In many organizations, a significant portion of their SOX Section 404 compliance costs were the cost of accounting for user accounts, entitlements, access to resources, and privileged access. To avoid incurring these costs on an ongoing basis, some organizations are deploying enterprise identity management solutions that will create centralized identity and entitlement repositories with an auditable work flow and access request process.

Other organizations are focusing on this same issue but from a single-sign on perspective. They may have environments that are fragmented: web applications using Netegrity, Windows applications using Active Directory, and Unix applications using Kerberos. These organizations are seeking a consistent single-sign on user experience.

Still other organizations are wrestling with the issue of authentication strength. With AOL allowing people to opt into a higher level of security to protect their email chatter, many financial institutions are wrestling with the issue of meeting investor expectations for enhanced security without overburdening themselves with ongoing helpdesk and distribution costs.

Percolating in the background is the Federal Deposit Insurance Corporation's (FDIC) work on unauthorized access to financial institution accounts and how the financial industry and its regulators can mitigate these risks. The report is entitled, *Putting an End to Account-Hijacking Identity Theft* and can be found at: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf. The report's primary recommendation is that two-factor authentication should be considered as a new security baseline for remote access to computer systems. However, in interpreting this recommendation, it is important to understand that the FDIC staff's definition of two factor authentication is non-traditional and includes the use of Challenge Questions.

Changing Threat Environment & Changing Threats

The security programs in most organizations were never designed to provide protection from the threats they are facing today. Historically, most organizations thought about protecting themselves from a technically skillful young hacker (we actually prefer the term *determined intruder*). While simplistic, that characterization was largely correct; most hacks were intended to show off for the hacker's community and did not do serious damage.

The threat environment has changed. Today, organizations are finding that the determined intruders are often offshore and are sometimes sponsored by organized crime, terrorists, and hostile governments. The attributes that they share are deep pockets and a willingness to spend an *unreasonable* amount of time accomplishing their objectives. These well funded attacks may manifest themselves as internal – which requires a fundamental rethinking of security approaches for most companies.

It is not only the threat environment that is changing, but the nature of the threats as well. A clear example of a pervasive new threat is phishing, tricking users into disclosing private information like a bank account number and PIN and then emptying the account. Other examples of new threats include the myriad varieties of adware and spyware. The cost of removing this malware has become a major headache to businesses around the world.

While we hope that future versions of software will be less susceptible to such attacks, education and vigilance seem to be the watchwords for defending the business against these new threats. Users and employees need to understand the risks of using untrusted sites, responding to unauthenticated request, and installing software to ensure that correct protections are in place.

Outsourcing Application Development & Developing Secure Web Applications

Outsourcing of software development is not new. What is new is the extent of the practice and the post 9/11 political climate. The reason we note this as a hot topic is that many organizations that had jumped on the outsourcing bandwagon expecting to achieve substantial cost savings, are now realizing that by the time they implement suitable security controls (e.g., programmatic and manual code reviews, and extensive testing) to ensure that the received code does only what it was intended, the cost savings is far less. Other organizations, while still outsourcing application development, have become much more selective in the countries they consider for the work.

The vast majority of web applications fail a simple security review. Consequently, it is not surprising that web application exploits are one of the fastest growing intrusion segments. Typical problems include allowing users to escalate their capabilities to perform inappropriate actions on their own account, obtaining information about the accounts of other users, performing any actions on the accounts of other user, reaching back end systems, and impacting the functionality of the server as a whole.

The Open Web Application Security Project (OWASP) (www.owasp.org) is one example of the technical community's reaction to the enormous problem of inconsistent and exploitable web applications. In addition to tools, its documentation includes a list of top 10 web application vulnerabilities and a guide to building secure web applications and web services, and a testing guide.

Securely Connecting to Business Partners

It is not uncommon for organizations to have relationships with dozens of Outside Service Providers (OSPs) or Application Service Providers (ASPs) – we've worked with some clients that have hundreds (we'll use the term ASP for both). The services these entities provide range from internally consumed services like payroll and benefits management to externally consumed capabilities like credit verification and payment processing on web sites.

While the use of ASPs is proving beneficial at a business level - enabling innovative functionality and reducing time to market, integrating these ASPs into the network and processing environment raises obvious security concerns for organizations and their clients. Does the ASP safeguard your confidential data to the same degree that you do? How would you know? Does the connection to the ASP represent an open back door into your network? Can another customer of that same ASP access your con-

fidential data? These are obvious questions yet most organizations can't answer them.

The single biggest problem with ASP security is that it has been neglected. The answer lies in applying the same type of risk assessment and security review process to ASPs as is typical in most companies for internal applications.

Security Certifications

Security is transitioning from a black art to a commodity skill. Increasingly, security services/staffing are acquired by non-technical people (e.g., Purchasing or HR). These two factors have changed the world for security professionals; pseudo credentials and buzzwords are becoming more important than depth of knowledge or actual experience.

A recent survey found 60 vendor-neutral information security credentials and 20 vendor-sponsored or vendor-specific security certifications. This situation is confusing to consumers and practitioners alike. Frankly, it is getting a bit silly. Below you can see a real example of a recent resume we received (name changed of course).

Bruce Walker
Network Security Engineer, A+, Net+, Sec+, FCSE,
CCSA, CCSE, ISSSE, SCSE, CCNA, CCDA, SSCA,
MCSE+I, MCSE 2000

Beyond the confusion, there is a huge hidden cost of these certification programs. Most require well documented officially sanctioned continuing professional education programs, payment of annual fees, as well as periodic recertification.

What to Look for in 2006

Technologies come and go. The security story of 2006 will not be technology. Rather, 2006 will be characterized as the year of widespread *security institutionalization*. Pressure from the audit community for continuous controls as well as the need for ongoing regulatory compliance reporting will change what were historically one-time or occasional security activities (e.g., application vulnerability assessments or policy reviews) into ongoing ones. Budgeting is evolving from funding for distinct security initiatives to including baseline security activities in the enterprise operating budget. Security will know it has arrived at an institutional level when penetration testing is as required and routine a line item in a company's annual budget as buying copier paper and paying the electric bill.

About SystemExperts Corporation

Founded in 1994, SystemExperts™ is the premier provider of network security consulting services. Our consultants are world-renowned authorities who bring a unique combination of business experience and technical expertise to every engagement. We have built an unrivaled reputation by providing practical, effective solutions for securing our clients' enterprise computing infrastructures. Through a full range of consulting services, based on our signature methodologies, we develop high level security architectures and strategies, design and implement security solutions, perform hands-on assessments, and provide a wide variety of both on-site and off-site services.

Our consultants are frequent speakers at conferences around the world. Our courses on penetration testing, wireless security, secure electronic commerce, intrusion detection, VPNs, and Windows security at USENIX, NetworkWorld-Interop, CSI, and many other conferences are among the highest rated because our consultants bring years of practical experience to bear. In addition, our consultants have been technical advisors and on-air guests for CNN, Dateline NBC, WatchIT, and CBS News Radio. Every single full-time staff member is certified in some critical security area.

We provide consulting services on both a fixed-price and time-and-materials basis. We are flexible and we can structure any project so that it is just right for you. You will appreciate the difference of working with genuine experts who are committed to earning a long-term partnership with you by over-delivering and providing unmatched personal attention.

Our consultants provide a wide range of services. Below is a sampling of areas in which we advise our clients. www.systemexperts.com/services.html

Security Consulting

Our experts conduct network and host security analyses and a wide variety of penetration tests. Some of the more frequent tests that we perform include "White Hat" penetration testing, web application vulnerability assessments, dial exposure ("war-dialing") reviews, firewall analysis, host hardening analysis, IP services inventory, wireless LAN inventory, VPN assessments, and denial of service reviews.

Security Blanket, Emergency Response & Incident Response "Scrimmage"

It is not a question of *if* your organization will be the target of a hacker, it is only a question of *when*. Preparation minimizes the impact of an attack and ensures a rapid recovery. Our security experts will work with you so you'll be well prepared and if you are attacked, we have the experience and expertise to respond to the intrusion in a pragmatic, professional manner. Our emergency response teams quickly assess the situation, properly preserve evidence for use by law enforcement, lock out the attacker, and develop and help implement a plan to quickly regain control of the IT environment. We can also help you prepare for these inevitable events by practicing your response through our acclaimed Incident Response "Scrimmage" Training Exercise. With our Security Blanket™, service, you'll be able to sleep at night knowing a team of security experts is on your side and *watching your back*. In addition to performing quarterly penetration tests, we'll notify you of virus attacks and vendor vulnerabilities that affect your infrastructure, and monitor a collection of hacker sites and alert you if your organization is ever mentioned.

Technical Skills at the "Guru" Level

Sometimes getting the details right is all that counts. We help our clients to resolve the toughest intrusion, firewall, VPN, wireless, PKI, authentication, authorization, networking, and configuration problems in Windows, Unix, and other heterogeneous environments. We also provide interim staffing up to the CISO level.

Accelerated Security AssessmentsSM & Code Reviews

Using our innovative and highly interactive Accelerated Security AssessmentSM methodology, our consultants will work with your team to perform a quick but comprehensive review of the security of applications or systems in their full environmental and business context and help you to understand and apply industry best practices. You may use this as the jumping off point for planning and prioritizing security initiatives. Our clients value both the short duration and the immense knowledge transfer that occurs during these intense Accelerated Assessments.

SystemExperts uses this Accelerated Security AssessmentSM methodology in a wide range of services including:

- ISO 17799 Assessment
- Sarbanes-Oxley Security Assessment
- COBIT Assessment
- Wireless Security Assessment
- Best Practices Security Assessment
- Application Service Provider Security Assessment
- Authentication and Authorization Security Assessment
- Application Security Assessment
- PeopleSoft Security Assessment
- Billing System Security Assessment
- Anti-Virus Security Assessment
- Security Architecture Assessment

Security Policy, Best Practices, & Strategy

Security starts with understanding the underlying business and regulatory requirements. Security policy is the means by which these requirements are translated into operations directives and consistent behaviors. We assist organizations in developing and updating policies and identifying where clients' current security practices, policies, or procedures differ from best industry practice. Over the past ten years, we have assisted some of the largest financial institutions in the world in developing their overall security architectures.

Intrusion Detection & Event Management

In security, it is axiomatic that what you can't prevent, you must detect. We have helped dozens of companies (including several of the largest companies in the world) develop comprehensive intrusion detection plans and implement them.

To learn more about how SystemExperts can put its expertise to work for you, contact us today at +1 . 888 . 749 . 9800

Boston

New York

San Francisco

Tampa

Washington DC

www.SystemExperts.com

info@SystemExperts.com

©Copyright 2005 SystemExperts Corporation. All rights reserved.