

# Living with Insecurity: A Practical Philosophy

## **Executive Insight Series**

*Jonathan G. Gossels*

---

### **Introduction**

Security is different from many other computer-related topics. It is as much a process or way of thinking about your systems, networks, and applications as it is a set of technologies.

Too often we see organizations focus on certain technical details and miss the big picture entirely. In today's networked world, we have to accept that our systems cannot be 100% secure if we still expect them to be useful in the conduct of our business. That means we have to learn to live with *insecurity* and manage our risks.

This brief white paper addresses five essential concepts. Since 1994, these practical ideas have helped hundreds of organizations make the right business decisions regarding the IT security initiatives.

### **Balancing Act**

A computer is completely secure only when it is powered off and disconnected from the network. Since a computer in such a state is not very useful, we have to accept up front that networked computers have inherent risks. At the same time, 100 percent security in a distributed network is unfeasible for businesses with finite budgets --which is to say, *every* business.

It is important to balance risk with a level of security that makes sense in any given application environment. The answer is to *look to compensating controls rather than deploying overly expensive or invasive security mechanisms*.

### **Security as Enabler**

Too often, security groups view their role as issuing policies and mandates that have the effect of telling business units what they *can't* do. *Security should never be an obstacle to business*. The challenge is to figure out how to offer the required services securely. Losing ground to competitors is not an option. In fact, organizations that embrace security as a business enabler have found that their environments are more flexible, more resilient, and more extensible than they would have been otherwise. These organizations find they are better positioned to offer new services and respond to new customer demands.

### **Think Layers**

Breaches happen. In designing your environment, start from the network perimeter and work your way inward. All the while, ask yourself, "If my security measures failed right now, what would be at risk? How would I even notice that I had a problem? What additional compensating controls or security mechanisms would I need to protect myself?"

In today's business environment, the boundary between inside and outside is constantly shifting. So think about the layering not in terms of inside vs. outside, but in terms of the level of authentication and authorization required.

### **Prevent and Detect**

People new to security often think in terms of keeping a bad guy out or of preventing something from happening. Prevention by itself is limiting. Many problems are better solved with detection, rather than prevention.

### **Start Off Simple**

*Incrementalism is good*. Too many organizations try to cover all the bases at one time, and only end up paralyzing themselves. They see how much needs to be done to become truly secure, and are overwhelmed by the costs in time, money and organizational angst. So, they decide to ignore the problem for a while longer.

Remember, security is a process, not a destination. Making steady progress, even with simple solutions, vastly improves your security profile. Every vulnerability you address, every security policy or practice you implement, makes you just that much better off and reduces your organization's risk.

## 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 technical conferences around the world. Our courses on penetration testing, wireless security, secure electronic commerce, intrusion detection, firewalls, VPNs, and NT/Windows 2000 security at Usenix, SANs, Network-Interop, CSI, and InternetWorld are among the most popular and 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 and we wrote the authoritative reference work on Windows® 2000, the Windows® 2000 Security Handbook (Osborne McGraw-Hill).

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.*

### Security Consulting

Our experts conduct network and host security analyses and a wide variety of penetration tests. In addition, using our signature workshop-style methodology, our consultants will work with your team to review the security of applications or systems in their full environmental context. During these comprehensive reviews, we will thoroughly explore the business as well as technical issues and we will balance the cost, schedule, and operational constraints of each technical alternative. Many of our clients include these reviews as the jumping off point for planning and prioritizing their security initiatives each year.

### Security Blanket & Emergency Response

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 and web sites or critical business resources are compromised, 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.

### Intrusion Detection and 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.

### Technical Skills at the "Guru" Level

Sometimes getting the details right is all that counts. We help our clients to resolve the toughest firewall, VPN, wireless, PKI, authentication, authorization, networking, and configuration problems in NT/Windows 2000, Unix, and heterogeneous environments. In addition we frequently perform code reviews of critical applications and web sites.

### Security Policy & Best Practices

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.

### Security Stolen/Lost Laptop Analysis

Many organizations expend considerable effort and resources to secure their internal networks, key computing resources, and connections to the Internet. Few recognize that a significant amount of their most proprietary information is traveling around the country on the largely unsecured laptop computers of road warriors and senior executives. SystemExperts' laptop analysis will help you to understand the potential risk of a lost or stolen laptop and what measures you can take to mitigate those exposures.

### VPN and Wireless

Certain technologies like VPN and Wireless are becoming ubiquitous and yet most organizations don't know how to properly secure them. We do - and we can help you.

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

**Boston   Los Angeles   New York   San Francisco   Tampa   Washington DC   Sacramento**  
**www.SystemExperts.com   info@SystemExperts.com**