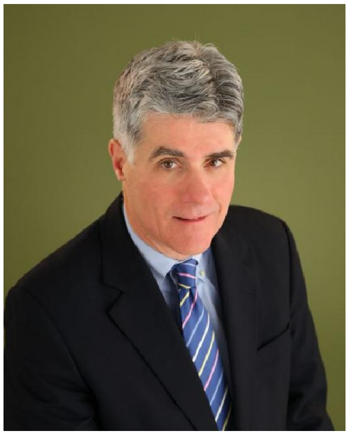
WHY SECURITY CONTROLS DON'T WORK……….AND WHAT TO DO ABOUT IT*

Dr. Frederick Scholl

Monarch Information Networks, LLC



My Brentwood, Tennessee neighbor's business recently lost over $300,000 to Eastern European hackers. Only after several days of feverish work was the money recovered by the FBI. This is definitely getting too close to home. The response to incidents of this type from many people in the security community amazes me. Not long after the hacking incident I was sitting in a booth at RSA 2010 where the CTO of an unnamed vendor was telling listeners that we should pull out all our perimeter security hardware and replace it with his latest appliance. Another technological magic bullet. I don't know about you, but his recommendations don't make me feel at all secure about my small business bank account, health information privacy or credit card data.

Published reports aren't any more reassuring regarding the scope of the problems we all face. Consider the recent USA Today headline: "Banks seek help to stop online thieves"[1]. Or the earlier CNN headline: "Jackson dies, almost takes Internet with him"[2]. More scientifically, the 2009 Internet Crime Report reports $559 million in losses for 2009, an increase of 100% over 2008[3]. Now that 500 million people and whole economies are depending on the Internet, are we heading for a security meltdown?

My recent experience with a consulting client implementing ISO 27001 has convinced me that the solution to today's security problems is a focus on *process*, not static controls. While this is not a new idea ("people, process, technology"), most businesses still focus on technology solutions and give only lip service to people issues and process issues. Partly this is because regulations and audit standards have developed into detailed control objectives and controls and those businesses often measure success

[1] USA Today, July 30, 2010.

[2] CNN, June 26, 2009.

[3] Internet Crime Report, 2010, www.ic3.gov.

by “passing the audit”. While compliance requirements have improved security, in my opinion, they are focused on maintaining the status quo, while security threats are constantly changing.

This article looks at the security issues we face today in business and government and makes the case that we can make significant progress towards remediating those issues through a focus on security processes. By focus on process, I am asking for two things: engineer security as a set of continuous, interconnected processes that make up a system; and establish a continuous improvement mentality or tone at the top to drive this system to improved security.

The problem with depending primarily on a static control framework today is that it is impossible to keep up with changes in the technical and business environment. The frameworks themselves, whether SOX, HIPAA, PCI, or other also have a difficult time keeping up with changes in security threats. Change is the enemy of security, but change is constant today. I was reminded of this when working for a client when their outsource vendor upgraded the OS platform running the firm’s web filter. The filter software then crashed and employees were therefore able in theory to browse porn sites. It took months to fix this problem because it had not resulted in a service outage and sat at the bottom of the priority list. The problem was fixed by the time of the annual audit, however. An expert witness client had a similar problem. Sometime after the firm purchased a smaller competitor, it discovered that the smaller firm had no web filter and employees of both firms were then able to download porn or surf to offensive sites. This fact was noted by plaintiff’s counsel in a subsequent Title VII lawsuit against the firm. I’m not sure what these stories say about my consulting clients but they clearly illustrate the effects of change on security controls.

Major security breaches often point to process breakdown, not specific control breakdown. Although any process breakdown could be explained as a control failure somewhere, a too myopic view of security as a portfolio of independent controls can lead to an unexpected process breakdown caused by a failure elsewhere in the system.

I am a big believer in learning from past events. If we go back 3000-4000 years, we can learn from the original Trojan horse security breach. The Trojans clearly had engineered good perimeter security; they held off the Greeks for 10 years. The Greek’s horse got into Troy through a combination of social engineering and risk assessment process breakdown[4]. The wall around Troy was still intact. Today's Trojans follow the same path in many cases.

How can a process focus bring benefits to security? By looking at security as a system, we can understand how a change at one point may affect other areas. Increasing password length may cause employees to use more Post-it notes. The laptops containing voter information and stolen from Metro Nashville in December 2007 unfortunately had their passwords taped to the bottom. That theft by a homeless man cost the city almost $1M. As another example, I have seen how more rigorous application access controls can actually cause poorer access control if those granting access are not well trained in how to grant access according to the more granular set of controls.

The big benefit to the systems and process approach is that we are able to incorporate the effects of feedback and organizational learning. Feedback can be used to drive the overall system to better security, year over year. One source of this feedback is the incident response process, where timely review of all incidents can enable improvements and eliminate big disasters. Annual audits also provide feedback, but in the best case should be confirmations of the expected security status.

The process focus also makes it easier to align the security program with business objectives. Security is not so much about guarding assets as much as giving more control over business processes to senior managers.

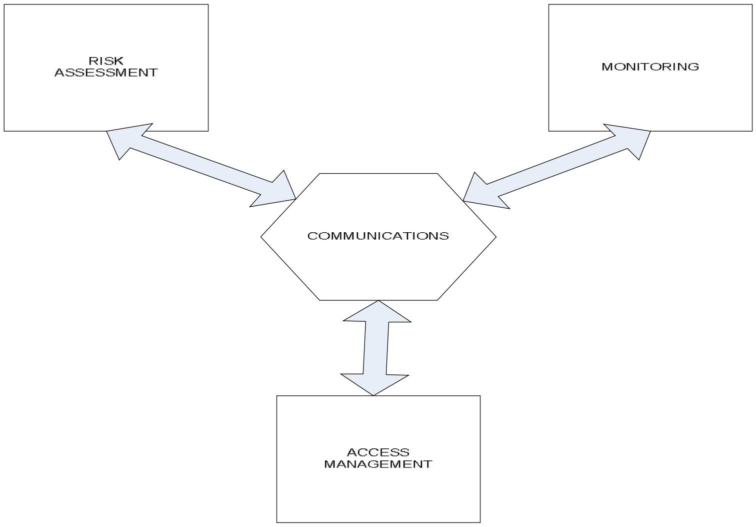
There are at least two templates that can be used to help implement a process based security program: ITIL and ISO 27001. Both are process oriented and focused on the idea of continuous improvement. ITIL is unique among frameworks in its strong business process focus, to wit: "To be effective, security must address entire business processes from end to end and cover the physical and technical aspects. Only within the context of business needs and risks can management define security"[5] Unfortunately the ITIL security framework has not become as popular as the other ITIL processes. While ITIL v2 had a separate 93 page book on security management, the topic warrants only a 9 page section in V3.

[4] Mythology, Edith Hamilton, 1942.

[5] ITIL V3, Service Design.

ISO 27001 is part of a whole ecosystem of security standards developed by ISO/IEC SC27. It too is focused on the idea of continuous improvement of security, with regular compliance auditing. Although my client is not yet certified, I have seen their entire security program turned around in one year by focusing on 27001 compliance. There is a clear perception of improved security in this business as control objectives are met.

Underlying both of these frameworks is the concept of security as quality control for information. As ITIL v2 Security Management states: "information security must therefore form an integral part of an organisation's overall quality management and quality assurance procedures."[6] The three core concepts of quality: control, measurement and continuous improvement[7] are readily applicable to any information security management program.



SECURITY PROCESSES

[6] Security Management, ITIL, 1999.

[7] Quality Planning and Analysis, J.M. Juran, Frank M. Gryna, 1993.

To illustrate some points of this article, I created the diagram above, which shows four critical information security processes. The point is, they are all interconnected on a *continuous* basis to achieve *continuous* improvement of security. The more traditional PDCA model seems to support improvement on an annual basis (tied to annual budgets or audits) or at best on a project basis. I also show "Communications" as the center of the process diagram. Communications process failures are the cause of many information security failures. It isn't enough to present great Powerpoint shows or schedule presentations when the CEO is in a good mood. It isn't enough to rely on traditional corporate communication resources or HR resources. Presenting results of risk analyses is extremely challenging. Look what happened to the Trojan's risk assessment team. The priest Laocoon and his two sons were swept out to sea by serpents after presenting their report. Modern brain science offers some ideas on how to do better.[8]

While working on this article, I may have been lulled into a state of complacence. Maybe it has been the 100 °F heat. Or has security been improving here? While Tennessee used to be #1 on the HHS breach site, with 998,000+ records breached, the Volunteer state has since been surpassed by Florida, with 1,220,000+ records breached. Now we are only #2. The five breach notification letters I received literally brought home the cost that must be paid to deal with one of these incidents.

Our local newspaper has been quiet about data breaches this summer. Until yesterday's headline: "Data Breaches Plague Metro."[9] In this latest incident, after Nashville flood victims applied online for property tax breaks, their banking information was freely offered on the site. Yes, even bank account numbers and routing numbers. According to the article: "The city also will conduct regular audits to make sure their systems are secure". What were they doing before?

I don't think our local government or healthcare providers are unique. The Internet infrastructure and application portfolios used by almost everyone are plagued with 25+ years of *cumulative* security patches. Newly discovered vulnerabilities seem to be holding steady, with Secunia reporting an average of 4,000-5,000 new vulnerabilities per year, for the portfolio of applications they are tracking[10]. I believe we will continue to employ and rely on this error filled system for many years. To secure it, we cannot just

[8] Management Rewired, Charles Jacobs, 2009.

[9] Tennessean, August 13, 2010.

[10] "Secunia Half Year Report 2010", www.secunia.com.

rely on check lists of controls and control objectives. These must be incorporated into a process based system of continuous improvement. Without this approach, the vulnerabilities and patches will aggregate to major outages that will affect all of us.

Frederick Scholl is a Global Senior Information Security Risk Manager qualified by 20+ years of experience and accomplishments in multiple industries. Dr. Scholl earned a Ph.D. in Electrical Engineering and a Bachelor of Science in Electrical Engineering from Cornell University. He also completed an Internet Law Program at Harvard University, and holds CISM, CISSP, and CHP security certifications. He advises trusted businesses in financial services and healthcare on how to protect their information and provides expert witness services on matters involving Internet technology.

* Reprinted from ABA Information Security & Privacy News, Autumn 2010.