

# Is Your Information Security Working?

Bill Young, CCSE, CISSP, Security Consultant, Chesapeake NetCraftsmen, LLC

“Passing an audit is often critical to a company’s continued operation. This puts pressure on engineers to pass the audit at all costs, even if it means covering up known issues.”

Information Security has grown by leaps and bounds. But as types of security devices and techniques grow in complexity and number, is your security actually improving? What about regulatory compliance? Are we on a downward-trending road paved with good intentions?

## Defense in Depth

Ask any Security Engineer what keeps them up at night. More than likely they will tell you it’s a known weakness in their environment that they just don’t have the time to address – something they suspect they might have overlooked, or a vulnerability they strongly suspect exists but simply don’t know about. These are the kinds of thoughts that spook the Info Sec expert.

Security professionals acknowledge these probabilities and attempt to mitigate them using a Defense in Depth strategy to reduce their company’s risk from individual weaknesses.

So, what exactly is Defense in Depth? Put simply, it’s the idea that implementing multiple layers of protection reduces your company’s exposure. If one device or layer in the DMZ is compromised, you can still protect the company’s critical or proprietary data. A successful Defense in Depth strategy requires trained personnel, effective tools and processes, policies and end-user training. While it’s impossible to completely remove the risk of an incident, Defense in Depth is the most effective way to reduce its impact – and sleep better at night.

## Good Intentions

Regulatory compliance and audits in the industry are becoming prevalent, as more companies and industries strive to meet legal and other security requirements. Sarbanes Oxley, HIPAA and FISMA are just a few of the regulations driving organizations to add increased Information Security controls. Successful implementation of these controls should be increasing the effectiveness of Defense in Depth. And indeed we see that these regulations are succeeding in motivating organizations to tackle security with some urgency, rather than a promise to do more next fiscal year.

Every year, the Computer Security Institute and FBI release their Computer Crime and Security Survey. The most current survey is from 2004 and it shows that we may have reached a turning point: we are seeing the first signs of a decline in compromises and the dollars lost per incident. This is heartening and does show that risks can be reduced to manageable levels – but we still have a long way to go. For example, we continue to see an increase in unauthorized access, Web site incidents and viruses. A laundry list of new compromises comes out weekly. Despite the fact that security awareness is at an all-time high, our defensive strategies have significant room for improvement.

## The Devil is in the Details

While Security Engineers share a common goal of protecting their respective organizations, their underlying backgrounds are often very different:

- a. Windows Administrators
- b. UNIX Administrators
- c. Network/Firewall Administrators
- d. Policy Developers and Auditors

Each of these skill-sets is valuable for effective security protection. But human nature compels us to focus on our specific strengths: we tend to spend time on what we understand or find interesting.

This produces a tendency to install security controls in our strongest disciplines, and then configure additional security controls which ultimately protect against the same or similar issues.

The result is that many of the unique Defense in Depth “layers” are often all within the same discipline. A UNIX administrator might configure a wide variety of security controls, but if the company doesn’t have a password policy, that system could still be easily compromised. That’s why it behooves security administrators to *avoid operating in a limited set of security comfort zones* – they need to work across all the relevant areas. Teams can do this better by dividing up responsibilities so that members can focus on what they do well, or what they like doing.

“Every year companies approve budgets for the next greatest security tool. This is often driven by audits, or a breach of the network that occurred in the prior year.”

### It Takes People to Run the Tools

While companies continue to increase their capital budget for security tools, they’re not necessarily increasing the staffing budget to properly deploy and manage those products. The continually rising demand for defensive security strategies has led to a significant increase in the products available. Every year companies approve budgets for the next greatest security tool. This is often driven by audits, or a breach of the network that occurred in the prior year. We have an extensive selection of security tools available to us, including one-time password generators, intrusion prevention systems, system hardening tools and in-line network antivirus appliances.

But security tools are almost always the exception to the “set it and forget it” approach that’s common in computing. It takes a surge of engineering resources to make the products effective by properly installing and customizing the solution to specific environments. Deploying new products also puts a drain on your ongoing support resources. *If your environment is constantly changing, these tools must be constantly updated.* On top of that, new vulnerabilities arise every week, signatures become

available and the tools must be made “aware” of new devices, such as Web servers, that are added to your network.

If inadequate time is put into a deployment, or ongoing support resources are not available, many of these solutions functionally become shelf-ware. It’s common to look to technology to solve our problems. But in both security and in network management, people, time and system integration / tuning are also part of what’s required for effective solutions.

One question that I commonly ask engineers is “why” they last looked at their firewall, system or IDS logs. The response that I almost always get is “because I was troubleshooting a problem.” These tools were installed to monitor, protect and notify us of security incidents, yet we’re not listening.

### The Audit Trap

Audits are arguably the single best thing that has happened for Information Security awareness. Audits often lead to policy development, user education, better patching and an overall improvement in an organization’s security posture. Unfortunately, audits are also training the industry to be better liars.

Passing an audit is often critical to a company’s continued operation. This puts pressure on engineers to *pass the audit at all costs*, even if it means covering up known issues. When an audit is coming, the dust is blown off of a wide suite of tools, many of which were installed purely for audit compliance. Engineers claim that they’ve been reviewing and analyzing the data. The auditor is shown screens of alerts in the NOC when the Intrusion Prevention System sees an issue (a screen that may only have been checked the morning before the auditor arrived to make sure it was functioning). Because the audit covers such a wide range of topics, *the auditor is often not a qualified expert* on each discipline being audited.

Audits also drive us to focus our energies inefficiently. One common audit requirement is that Security Personnel must initial each page of a log. When there are 100 or more pages to be initialed each and every morning, they are seldom being read in detail. Security event correlation and aggregation tools can be used to increase efficiencies here, but they are still resource-intensive and may not meet audit requirements.

After the audit is complete, the results are reviewed, and one of two things occur:

1. If there are no significant findings, the company goes back to business as usual, with a *false sense of security* that no serious issues still exist.
2. If there are problems, the results are waved in front of management, proclaiming that additional capital is needed to buy another tool to ensure that the company can pass the next audit.

“Security tools are almost always the exception to the ‘set it and forget it’ approach common in computing. It takes a surge of engineering resources to make the products effective by properly installing and customizing them to specific environments.”

### Start Sleeping Better at Night

Clearly, we still have a number of issues that need to be addressed even though there have been some improvements. The fundamentals of Information Security require knowing about risks and making informed decisions to react or accept the risks. Skills deficiencies, staffing shortages and audit compliance pressures are preventing many of these issues from being appropriately evaluated and handled.

Often, consultants are engaged to help with the first phase of a new product deployment. Bringing in that initial surge of resources can help make certain that a product is deployed with the due diligence necessary to ensure proper integration. However, to be successful, an effective hand-off and training is required. And, most importantly, there needs to be sufficient full-time staff to manage and maintain these tools.

The bottom line is that Information Security is about discipline and process execution. It’s a constantly changing and improving process, caught between the high costs of effective security measures and the high costs of being hacked. We’ve made industry-wide progress and are beginning to reduce the risk and impact of attacks. But there is no one tool which will solve all security problems. We need to also focus on the “people and procedures” side of things.

The key to Defense in Depth is full cooperation and resolve from security, network, systems and compliance professionals, and their management. With a clear understanding of all the resources necessary – people as well as tools – a truly effective Defense in Depth security program can be both implemented and maintained.

---

**Chesapeake NetCraftsmen, LLC** delivers high-availability solutions for Network Design, Operating Systems, Applications, Security, Storage and IP Telephony with deeply experienced CCIEs who excel at Knowledge Transfer.

Chesapeake NetCraftsmen consultants include some of the most experienced Cisco CCIEs in the country. Most of our technical staff has a minimum of 10 years’ networking experience and many have taught Cisco Certified training. Knowledge Transfer is a key part of every Chesapeake NetCraftsmen engagement, making certain that clients understand how to run and manage their newly implemented or re-structured networks.

**For more information on Chesapeake NetCraftsmen, [click here.](#)**