A version of this article appeared in Homeland Security Today ***14****(1), 12-13 (2017)*

Compliance Versus Security

Roger G. Johnston, Ph.D., CPP
Right Brain Sekurity
http://rbsekurity.com

Effective security is not the same thing as complying with security rules and regulations. Sure, there is a certain amount of overlap—deliberately violating security requirements often results in poor security. But in my experience as a vulnerability assessor, a good rule of thumb is that at least a third of security rules and regulations in large organizations actually make security worse. Often, this is because the security requirements don't adequately account for local conditions, human nature, organizational culture, or unrecognized security vulnerabilities.

Many security managers fully understand that compliance does not necessarily equate to good security (though the political or legal need to be in compliance may be unavoidable). Others, however, do not share this view and believe that they can evaluate the effectiveness of their security primarily by auditing compliance with rules and regulations. Nothing could be further from the truth.

I'm often asked by security managers who hold the latter view for examples of compliance harming security. This article gives just a few of many such examples. I have witnessed the majority of these first-hand, often across multiple organizations. I have heard about the remaining examples from other security professionals.

Probably the most common examples of compliance harming security include the following: the bureaucracy, paperwork, records keeping, efforts to interpret and implement complex rules (sometimes confusing and contradictory), time spent preparing for audits, "teaching to the test", memorizing trivia, spending large sums of money on dubious and expensive security measures and consultants, etc. all result in distractions, frustrations, loss of focus and energy, and wasting of security resources. Particularly damaging can be foolish regulations or legislation imposed by naive bureaucrats, regulators, executives, or legislators as a result of over-reacting to security incidents.

Perhaps the second most common example is where all of the above negative attributes of a compliance-based security regime result in security personnel and regular employees becoming highly cynical about security. They come to view security as merely stupid rules and "Security Theater" imposed on them arbitrarily from above by people who don't understand local conditions or what it takes to get the job done properly. Once this happens, a healthy Security Culture and effective security are not possible.

Even when cynicism is not engendered by compliance-driven security, emphasis on compliance rather than real security can create a bad mindset. Security becomes equated with mere bureaucratic busywork, mindless rule following, and the idea that the brass are responsible for security, not me. This inhibits proactive situational awareness, the use of intuition, and taking of personal initiative and responsibility when it comes to security. Poor security results.

In addition, flawed security rules that needlessly harm employee productivity and morale, plus an emphasis on pleasing/conning the security auditors—as so often happens in compliance-based organizations—creates an "us-versus-them" atmosphere, "them" being auditors and higher-ups. This also leads to bad teamwork and a poor Security Culture.

Indeed, it is poor practice to tell employees that security rules and procedures, which they have had zero input in formulating, must be followed or they will be disciplined or fired. The message this sends to employees is that higher ups and security are their enemy. This is bad for the Security Culture, and thus for security. Generally, security rules that haven't passed an employee sanity check are usually bad security rules. Ultimately, all security (like all politics) is local.

Another kind of problem created by compliance are rules that require "Security by Obscurity", i.e., the idea that security is maintained by keeping secrets. In fact, people and organizations are very bad at keeping long-term secrets. Somewhat counter-intuitively, security is usually better when it is transparent. Transparency allows for review, criticism, questioning, accountability, understanding, continuous improvement, and buy-in. It also

allows for access to the best people and the best information. Moreover, the bad guys, whether insiders or outsiders, usually understand the secrets, or at least you have to reasonably assume they do.

Many government organizations require security clearances. The rules usually require personnel with such clearances to report any counseling, even something as minor as brief marriage counseling. As a result, employees with security clearances often avoid getting any professional help at all with their problems out of fear of placing their security clearance at risk, resulting in deteriorating mental health. This may harm security. [It should be noted, however, that the role of mental health in the insider threat (other than workplace violence) is open for debate. None of the spies arrested for espionage against the United States in the last 50 years, for example, were mentally ill. Narcissistic jerks, to be sure, but that is not a mental illness.]

Another common and particularly disturbing example of compliance hurting security is when doing only the minimum required by the compliance rules results in not addressing critical security risks. Carried to an extreme it means that the minimum specified by the compliance rules constrains what is allowed. We won't be allowed to make a significant security improvement not actually required by the auditors. For example, federal requirements for anti-malware on SCADA control systems (such as used for power utilities) mandate measures that are weaker than many SCADA security managers would like to implement but the federal rules prohibit a better security solution.

I know of many cases where an organization had to decide between a real security solution and the minimum standard established by the compliance rules. Guess which one usually wins out? A related problem is bureaucrats and executives vetoing necessary security measures despite the merits because they are satisfied with merely being in compliance. Too often, compliance gives a false sense of security.

Other, more concrete and less "cultural" examples of compliance harming security include:

- An over-emphasis in the rules/regulations on gates, entry points, and fences (which typically create only a 4.5 to 15 second access delay) leads to failure to consider other attack modes and vulnerabilities, resulting in bad security.

- Overly rigid rules, such as requirements for predictable guard patrols, routes, schedules, and shift changes make it much easier for attackers to avoid or negate the guard force.

- Requiring access by numerous auditors, inspectors, overseers, micro-managers, and checkers-of-the-checkers increases the insider threat.

- Over-classifying information. When everything is classified, nothing is. It is much more effective to focus on protecting only the most critical sensitive information, and in the most straightforward manner possible. For example, the federal government

tends to have so many different kinds of classifications and security badges among the various agencies that it is difficult to keep them all straight. (The situation has, however, improved somewhat in recent years.)

- Mindlessly banning new technology, rather than trying to intelligently accommodate it. We saw this kind of "cultural lag" (a term coined by William F. Ogburn in 1922) when thumb drives first came out. All this does is to make makes security the enemy of productivity and employees, engenders cynicism about security, and encourages employees to break this rule to get things done—making later rules easier to break.

- Ill-conceived, overly formalistic use protocols for security devices (especially tags and seals) that offer poor security and/or discourage the users of the device to pay close attention to evidence of tampering.

- Requiring employees to sign at the bottom of a form, swearing that all the information they have provided above is true and accurate. This causes them not to go back and correct inaccuracies, and to continue on in the future with any lies that have written down. Research shows that having the employee pledge at the top of the form to tell the full truth results in much greater honesty.

- Adherence to a given security standard is often used to argue that an organization has overall good security and that no extra security measures are needed when, in fact, the standard speaks to only a narrow subset of security issues. The PCI standard (Payment Card Industry Data Security Standard) is often used in this way, even though it only really addresses security issues for credit card procesding, not broader security issues.

- Security standards and guidelines written by professional organizations are often dominated by input from manufacturers and vendors of security products in a way that helps their business but compromises security. The ISO 17712 standard for freight seals is, in my view, a classic example of a harmful standard. See, for example, RG Johnston and JS Warner, "Vulnerability Assessment Myths", *Journal of Physical Security* **7**(1), 31-38 (2014), http://rbsekurity.com/JPS%20Archives/JPS%207(1).pdf

- Control often gets confused with security, to the detriment of the latter. One form of this is when an organization requires employees to only use one kind of computer, creating a monoculture that is highly susceptible to viruses and other malware. In the 2014 Sony attack, for example, hacked Windows PCs were down for a long time, but the Macs continued to operate just fine.

- The following paper nicely addresses other problems with cyber security compliance (along with some of the advantages): R. Herold, "Do Compliance Requirements Help or Hurt Information Security", http://www.realtimepublishers.com/chapters/1699/esitcv1-13.pdf

In thinking about compliance versus security, perhaps the following joke is illuminating:

An old married couple were watching the news on television. The weatherman said a snowstorm was coming and that cars should be parked on the odd-numbered side of the street to facilitate snow removal. "Guess I better move the car," said the husband has he rose to put on his jacket.

A few days later, the couple heard on television that another storm was coming and that this time, cars were supposed to be parked on the even-numbered side of the street. The old man got up to move the car.

Two weeks later, the couple was again watching the weather report on television. The weatherman was saying, "another huge blizzard is now bearing down on the city and cars must be parked on the....", when suddenly the power failed and the television went blank. The old man turned to his wife and said, "Now what should we do"? His wife said, "Well, dear, maybe you should just leave the car in the garage tonight."

About the Author

Roger G. Johnston, Ph.D., CPP is CEO and Chief Vulnerability Wrangler at Right Brain Sekurity, a company devoted to security consulting and vulnerability assessments. He previously was head of the Vulnerability Assessment Teams at Los Alamos and Argonne National Laboratories (1992-2007 and 2007-2015).