Do Compliance Requirements Help or Hurt Information Security?

by Rebecca Herold, CISSP, CISM, CISA, FLMI

Once upon a time, before there were any regulatory requirements for protecting information (well, at least very few), information security professionals often lamented, "Oh, if only laws would require information security then we wouldn't beat our heads against the wall trying to secure our networks and systems!" Fast forward to today—now you commonly hear some of these same practitioners moaning, "Oh, there are just too many laws and too many different data protection requirements to feasibly comply with!"

I discussed this issue with seven seasoned information security and privacy professionals to get their opinions about whether regulatory compliance requirements help or hurt information security initiatives. They were wholly in agreement that compliance can help or hurt information security and associated initiatives depending upon the culture of the organization. Key points from each of them are included in the following discussions of how compliance helps and hurts information security.

Our discussion panel includes:

Dr. Peter Stephenson, Associate Director, Norwich University Master of Science in Information Assurance Program

Mike Corby, Sr. Director, Gartner Consulting

Peter Wenham, Director, Trusted Management Ltd. Information Assurance (IA) Consultants

Dr. Gary Hinson, CEO, IsecT Ltd. and www.NoticeBored.com

Pam Poucher, Manager, Business Intelligence & Privacy, Cox Enterprises

Kevin Beaver, Owner, Principle Logic, LLC

Barry Jones, Principal Consultant, Tribridge, Inc.

Compliance Requirements Help Information Security Efforts By…

Legally requiring long-held information security standards and practices

Some regulations requiring information safeguards reference the need to use what are considered industry-leading best practices. For instance, within Section III Analysis of, and Responses to, Public Comments on the Proposed Rule of the Health Insurance Portability and Accountability Act (HIPAA) regulatory text, it is recommended that those implementing the controls should:

> *"…see NIST Special Publication 800–14, Generally Accepted Principles and Practices for Securing Information Technology Systems and NIST Special Publication 800–33, Underlying Technical Models for Information Technology Security."*

Jones: "Most of these standards are the same principles and practices that security professionals have been advancing since the birth of the profession. And most of these principles and practices have been either roundly dismissed or generally lip-serviced by organizations until now."

Not only have the use of existing information assurance standards been referenced, but the various standards themselves—now held up as examples of how to appropriately safeguard information—have also been updated and improved upon. For example, ISO 17799:2000 was updated and made more applicable to today's more challenging technology and business environments with the release of ISO 17799:2005 in June of 2005.

Hinson: "One reason legal and regulatory compliance pressures mostly help is because they have undeniably forced improvements in governance standards."

Increasing management awareness of security and how management handles business risks

When laws and regulations make business leaders personally accountable for implementing information safeguards, business leaders become concerned.

Jones: "Mandates are providing management awareness, support, and budgets the likes of which we InfoSec professionals haven't seen in our entire careers."

The CIO Magazine—PriceWaterhouseCoopers "Global State of Information Security 2005" report indicates information security budgets will increase by 47 percent in all industries, and by 57 percent specifically in the highly regulated financial industry in 2006.

Hinson: "Another reason legal and regulatory compliance pressures mostly help is because they are well publicized and force managers to read-up on governance-related topics."

Sixty-seven percent of the Deloitte 2005 "Global Security Survey" respondents indicate regulatory requirements are "effective" to "very effective" for improving the information security program and reducing information risks.

Corby: “If the compliance needs result in raising the awareness of security as an opportunity to manage several risks that are the thrust of the compliance issue, then security has the opportunity to move on to the next step; as a player with the opportunity to establish good governance and provide strategies for mitigating the risk of non-compliance.”

Sixty-one percent of the respondents to the Ernst & Young “Global Information Security Survey 2005” indicate regulatory compliance requirements have had the most significant impact to the information security practices within organizations.

Stephenson: “Generally compliance requirements have forced executive management to pay attention to information security.”

Forcing information security issues to be addressed that otherwise would not

Beaver: “Most business managers and executives haven't and, for the most part still don't, understand information risks. So, if the HIPAAs, GLBAs, and California Senate Bill 1386s of the world are what it takes to force people to keep private and confidential information private and confidential, then we're still better off in the long run.”

Most information security practitioners agree that if it were not for regulatory requirements, executives would not support or address information security risks and issues because information security costs have always been viewed as a discretionary cost to business and a drain to the bottom-line budget.

Hinson: “Legal and regulatory compliance pressures also help because they force senior management to take their governance obligations seriously (they carry the weight of law).”

Executives now see, as Enron and Tyco executives are led to jail in handcuffs, that regulatory requirements should be taken seriously. Such images have great impact on the motivation of executives to comply with laws to avoid being the next top story on the nightly news.

Wenham: “People do 'security' for one of two reasons: they have been 'had' (that is, been broken into, had stuff stolen, had a hacker in who messed up the Web site, had a disgruntled employee interfere with things, and so on) or they have to (that is, the law, compulsory legislation, or some other external factor means they have no choice).”

Increasing public awareness of information security and privacy issues—the public then demands that businesses address the problems

> Beaver: "I do believe these laws and regulations have brought more visibility to the privacy and security problems we have."

According to Privacy Rights Clearinghouse, more than 53 million individuals within the United States have had their personal information put at risk as a result of a data breach in at least 106 publicized personal information breach incidents in 2005. These breaches were reported largely, and perhaps only, because of state-level regulations requiring notification. The public is reading and hearing about these incidents daily. Public awareness of information security and privacy issues has certainly been raised.

Providing a solid new, or improved, foundation for information security within organizations that previously had no, or insufficient, information security programs

> Poucher: "Compliance requirements can help an organization by providing a framework, a starting point so to speak, to work within to assist in identifying your risks and vulnerabilities."

Many regulations very clearly define the types of information security and privacy safeguards that must be implemented by covered organizations. For example, both the Gramm-Leach-Bliley Act (GLBA) and HIPAA clearly outline the technical, administrative, and operational safeguards those organizations must formally implement. The implementation of these requirements then form the basis for the information security program at many organizations where, up until the regulations went into effect, information security may have just been a function given to a network administrator to help stem the tide of incoming malicious code—or even a non-existent formal business responsibility.

> Hinson: "Legal and regulatory compliance pressures help because they apply a common standard quite rigorously through the efforts of a small army of professional compliance officers, auditors, accountants, lawyers, and, of course, information security managers."

Because of the preponderance of operational, policy, and training requirements, the regulations force information security and privacy professionals to work more closely with the rest of the business; they have to or they will not be in compliance with these personnel and business process directives.

> Corby: "Compliance offers the opportunity to measure, improve, and re-measure. Compliance is not an event, it is a process by which certain expectations are met, and then new expectations can be set and achieved."

Data protection regulations overwhelmingly require organizations to measure risk, provide education, and monitor for threat on an ongoing basis. These actions must be documented to demonstrate compliance. For organizations that never performed these activities before, regulatory requirements are helping them realize their true information security postures and adjust accordingly to better protect their information assets.

Clearly reducing subjectivity of interpretation of specific safeguard requirements when the regulations are written well

> Hinson: "Well-written legal and regulatory compliance pressures help because they are written in formal language designed to reduce ambiguity."

Although portions of regulations can be a bit wishy-washy and subject to a wide range of sometimes creative interpretation, they can also clearly specify compliance requirements. For example, the HIPAA directive to "Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored" and the accompanying regulatory implementation discussion makes it clear that covered entities must create a formal disposal process with appropriate tools and technologies to completely destroy and dispose of information that is no longer needed.

Moving information security higher up in importance and in the organization chart

> Hinson: "Legal and regulatory compliance pressures help information security professionals because they have increased salaries in related professions!"

More executives are paying attention to information security compliance requirements and putting information security functions at a higher role within the organization. As the PWC "Global State of Information Security 2005" finds, companies with the security function at the executive level have budgets and information security policies that are more aligned and ingrained with business, and a higher percentage of personnel comply with information security requirements and policies than in organizations in which the information security function is not at the executive level. Information security professionals may very well be moving up in the organizational chart; the SANS Institute's 2005 Information Security Salary and Career Advancement study found that salaries for corporate security positions rose an average of 5.5 percent from 2003 to 2005.

Requiring organizations to implement controls that are able to track activities for personal and sensitive information

> Wenham: "Regulatory and legal compliance is now starting to put the emphasis on identifying who did what and when to 'information;' this, in turn, will lead to improvements in access control to 'information,' which, in turn, will mean improved audit logs and thus lead to vastly improved 'who did what and when' data, which feeds neatly into regulatory compliance and reporting."

Regulations such as GLBA, HIPAA, SOX, and the European Union Data Protection Directive clearly require covered organizations to log and be able to track activities to sensitive and personal information. For example, HIPAA requires covered entities to, "Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."

Compliance Requirements Hurt Information Security Efforts By…

All is not wine and roses with regard to regulatory compliance helping information security. We need to remove our rose-colored glasses and look at the ways in which compliance requirements can also hurt information security efforts.

Confusing companies with multiple conflicting requirements

Many of the laws at the state, federal, and international levels contain requirements that sometimes conflict with other regulations. This conflict causes confusion, interpretation conflict, and challenges for the business leaders responsible for compliance, often resulting in implementation of safeguards only in areas in which organizations think regulators will check.

> Jones: "However much we may applaud the recent groundswell of state legislation following the example of California's SB 1386, we are seeing an emerging patchwork-quilt of laws that differ enough between each other to become a new headache for us all."

Trying to figure out preemption situations and mapping all the related requirements to the related applicable regulations within an organization can lead to extremes of actions; either the company will implement all the most stringent requirements across the board, regardless of any exemptions that may exist or the organization will throw in the towel and decide that doing nothing is the best course of action—they can always plead ignorance in the event of a noncompliance investigation.

> Stephenson: "Some companies do not know whether they have to comply with regulations. Some will assume the worst case and will do what they think they should to meet compliance, others will do nothing and hope they don't get caught."

Establishing many requirements that are not feasible within most organizations

> Jones: "Because legislative action all too often is forced by reaction to dire circumstances and the outcry of constituents, it all too often is not only reactive but over-reactive. Being over-reactive is the root of all kinds of ills, including requirements that strain at gnats but swallow elephants, focus on the branches but not the roots of the problems, breed new bureaucracies to enforce, and become so onerous that in the end, companies will seek to put forth the minimum to get by rather than embrace the spirit of the law."

Some organizations simply do not have the means or resources to implement some regulatory requirements. For example, many small to midsized healthcare provider environments simply do not have the staff, experience, or budget to implement all the HIPAA Privacy Rule and Security Rule requirements.

> Beaver: "I have a problem with career politicians and their advisors writing legislation on subjects they know nothing about."

Being inadequate or leaving gaping loopholes, ultimately not improving security at all

> Jones: "The legislative process typically involves compromises that have much more to do with expediency than with sound principles of information security.

Unfortunately, many regulations are written in ways that do not really require actions to fulfill the purpose of the law, or they leave significant loopholes and exemptions so that data protection really isn't improved as a result of the passage of the law. Many of the United States' state-level breach notifications laws contain huge exemptions for large percentages of organizations that handle millions of records containing personal information. For example, the Georgia S.B. 230 breach notification law only applies to "information brokers." And, without any penalties for noncompliance, it has no teeth to motivate the comparatively few covered organizations to comply.

Taking resources from more critical initiatives

Many organizations have found that the costs of implementing regulatory requirements for one law take away resources from other, possibly more critical, information security initiatives.

> Poucher: "There are additional costs and infrastructure to manage such as a compliance program that places a burden on an organization and can be an impediment to other projects."

I spoke with several chief information security officers (CISOs) throughout 2005 who were exasperated that significant portions of their already approved information security budget were diverted to the Sarbanes-Oxley Act (SOX) compliance efforts, leaving them with no money to implement their planned intrusion detection systems, hire more staff to handle the overwhelming amount of information security work required by other regulations, or to implement encryption on their mobile computing devices.

> Hinson: "The cost of compliance tends to diminish resources available for discretionary projects, and can be a significant cost for businesses already under pressure from tight margins."

Resulting in compliance efforts that are more costly than self-regulation

> Hinson: "Legal and regulatory compliance are more costly than self-regulation."

According to a study released September 19, 2005 by the Office of Advocacy of the United States Small Business Administration, organizations with fewer than 20 employees spend $7647 per employee each year to comply with federal regulations, and organizations with more than 500 employees spend $5282 per employee annually. The report also indicated that the annual cost of federal regulations compliance in the United States totaled $1.1 trillion in 2004.

Scapegoating compliance to implement security solutions

> Hinson: "Legal and regulatory compliance requirements are sometimes abused to justify unnecessary or ill-conceived controls."

I have heard many business leaders complaining, and vendors gloating, that now information security practitioners are using regulations to justify buying cool technologies that they previously could not get because, before compliance requirements, they could never convince the budget approvers of the business benefit of the requested purchase or show how it would improve security.

> Corby: "If the senior executive discovers that the security people are descending upon the CxO or board member with a host of warnings, cautions, crises, and other concerns, the security program can be dealt a severe blow. The one solid chance to become part of the strategic fabric will have been wasted, most likely forever, and certainly within the career tenure of the security director. A frequent occupational hazard is to promote security to the maximum extent it can be delivered. It can be difficult for someone immersed in the issues of security to remind themselves that security only needs to be good enough to mitigate risk to a certain point, but to do it well. Being 100 percent secure is unattainable, but being 100 percent certain of success at the 80 percent level is within reason. Compliance, as I read it, does not call for perfection across the board."

Creating management duress and ultimately creating the view of information security as a business cost not a business enabler

> Hinson: "Legal and regulatory compliance requirements are complied-with 'under sufferance,' meaning begrudgingly, therefore increasing the general resentment, ill-feeling, and negativism towards information security as a cost rather than a source of business benefit."

There have been dozens, perhaps hundreds or even thousands, of articles bemoaning information security as a huge cost to business. Many fewer articles discuss or demonstrate how information security can be a business enabler when done correctly.

Generating high-priced compliance "solutions"

The rise in numbers of compliance requirements generates new compliance snake-oil solutions and outrageous billing rates that damage the valid information security efforts.

> Hinson: "The small army of professional advisors is seen to be milking their clients of $$$, thereby discrediting consultancy and other professional services."

Fear of jailtime and personal monetary penalties drove huge corporate spending for SOX compliance efforts in 2005. Many vendors placed a "SOX Compliance" label on their products and services and bumped up the price to take advantage of this fear. I have heard many marketers within various information security vendor companies not only encouraging, but also threatening with potential job loss, their consultants and representatives to push the products and services by creating fear, uncertainty, and doubt (the FUD factor) within customers.

> Wenham: "One problem that the industry has is that, within the UK, people/companies are claiming to be InfoSec consultants/suppliers when all they have done is harden OSs, sell/install boxes, set up users and profiles, done some vulnerability assessments (and often sold such assessments as pen tests!!!)."

Interpreting requirements in the most convenient way

Many poorly written regulations result in organizations interpreting them to their own liking, twisting the intended requirements to what is most convenient for them and not addressing the spirit of the law.

> Hinson: "Despite the formal language, there are differences of opinion about their applicability and details, and some organizations are probably intent on 'gaming' (that is, deliberately interpreting or bending the rules)."

I have spoken with several lawyers from many different industries about how they view the implementation of information safeguards to meet regulatory requirements, and many indicate that if the regulations do not explicitly state they have to do something, such as encrypt personal information within email messages, they will not support the purchase or implementation of such solutions or processes.

> Stephenson: "There is a danger that some organizations do not do what they need to do, just what they can get away with for the cheapest cost and for the minimum requirements."

Not addressing important risks outside the compliance requirements

> Hinson: "They may increase the risk of failing to address important areas just outside their scope."

Organizations are focusing so intently on the specific regulatory requirements that important security risks often are not addressed. For example, information security practitioners have told me that they cannot get resources approved to secure the growing numbers of wireless technologies proliferating throughout their organizations because the entire information security budget has been earmarked to support compliance requirements, and no regulations specifically mention anything about wireless computing devices. Even though they fall under the umbrella of network security, business leaders often do not understand this.

Slapping on solutions not supporting business

Many organizations are applying information security solutions in an effort only to meet compliance and without regard to the business.

> Wenham: "The understanding of a business, the information that it contains, and the associated business risks are often missing or paid lip service to. This is one of the reasons, I believe, that spending on 'security' has gone up but that the incident rate has not fallen. Quite the reverse, the incident rate has increased far more than spending (because the money has probably been spent on the wrong things or the priority of spending is wrong)."

When information security tools and processes are applied without any regard to the enterprise infrastructure or business mission and goals, it is likely they will be ineffective. Effective information security is applied based upon risk. Many information security initiatives are based upon fear of fines, negative publicity, and jail time. This reality was demonstrated numerous times by the information security spending for SOX compliance; SOX does not require information security to be implemented based upon analyzing the business risks, so SOX-labeled solutions were widely purchased and deployed without first analyzing risks. These organizations will find how effective those solutions really are.

So, The Answer Is "Yes!"

So the answer to the question "Do compliance requirements help or hurt information security?" is "YES!" The side of the fence where the information security grass is greener, before compliance requirements or with compliance requirements, all depends upon your organization and your information security actions.

> Stephenson: "Take HIPAA as an example. Some companies truly did the right thing; had an outside independent in-depth review of their network and operations, remediated the noncompliance areas, then had another independent review to ensure they were then indeed in compliance. Other companies just did nothing because of the resources it would take, and now they hope they will not get caught."

Organizations must look at the vast array of regulations that apply to them, create a comprehensive compliance plan, and implement it according to the risks within their own, unique business environment, and not based upon a slick high-dollar marketing campaign that catches their attention.

> Corby: "Success is measured in small steps, with new successes just over the horizon. Defining those small steps; achieving success, and setting out for the next milestone is critical in developing a compliance program that becomes a permanent part of the organization, not just a 3- or 6-month project that goes away."

It is ultimately up to each organization how they implement information security activities and requirements throughout the enterprise. Their success or failure will be the key indicator for whether their response to regulatory compliance ultimately hurts or helps their information security efforts.

Compliance Requirements Help Information Security By…	Compliance Requirements Hurt Information Security By…
Legally requiring long-held information security standards and practices.	Causing confusion, conflict, and challenges for complying with multiple inconsistent laws, and leading to security implementation only where organizations think regulators will check.
Increasing management awareness of security and how business risks are managed.	Establishing many requirements that are not feasible within many organizations.
Forcing management to address information security issues that they would not otherwise.	Being inadequate or leaving gaping loopholes, ultimately not improving security at all.
Increasing public awareness of information security and privacy issues; the public then demands that businesses address the problems.	Requiring compliance costs that take away resources from other, possibly more critical, information security initiatives.
Providing a solid new or improved foundation for information security within organizations that previously had no or insufficient information security programs.	Resulting in compliance efforts that are more costly than self-regulation.
Clearly reducing subjectivity of interpretation of specific safeguard requirements when the regulations are written well.	Using compliance to justify unnecessary or poor information security solutions.
Moving information security higher up in importance and higher up in the organizational chart.	Creating management duress and ultimately creating the view of information security as a business cost not a business enabler.
Requiring organizations to implement controls that are able to track activities for personal and sensitive information.	Generating many compliance snake-oil solutions and outrageous billing rates that damage the information security reputation.
	Enabling subjective interpretation of poorly written regulations that allows organizations to bend the requirements to what is most convenient for them and not addressing the spirit of the law.
	Not addressing important risks outside the regulations compliance requirements.
	Applying information security solutions only to minimally meet regulatory requirements and without regard to the business.