

Regulation and Information Security

Can Y2K Lessons Help Us?

Regulation. The mention of the word often sends shivers down the spines of business executives and IT professionals. Yet, a recent rash of crippling worms and viruses, coupled with the continued threat of a serious cyber attack on our information infrastructure,

information security continues to be viewed, in many cases, as a technology issue, rather than a management and governance issue in the context of sound business practices. It's critical that we elevate network security to senior management and board-rooms in the private sector.”
—Congressman Adam Putnam

JEFFERY E.
PAYNE
Cigital

has once again elevated the notion of federally mandated security regulation to the forefront. Will regulation solve this problem? What has regulation done to help in the past? Why are technologists wary of regulation? These are some of the questions I'll explore in this issue's installment.

Department of Homeland Security (DHS) Secretary Tom Ridge and Securities and Exchange Commission (SEC) Chairman William Donaldson met recently to discuss the possibility of requiring that SEC filings include information on corporate security “efforts” (www.promag.com/eparchive/index.cfm?fuseaction=viewarticle&ContentID=4238&websiteid=):

“I think we need to talk about some kind of public disclosure, what are you doing about your security, physical and cyber security. Tell your shareholders, tell your employees, tell your communities within which you operate.” —*Department of Homeland Security Secretary Tom Ridge*

Congressman Adam Putnam (R-Fla.) drafted but never submitted legislation that would require all publicly traded companies to annually assess information security and report the results. Under this legislation, public companies would be required to “assess the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems,” and to “determine the levels of information security appropriate to protect such information and information systems.”

Instead of proceeding with this legislation, Putnam formed the Corporate Information Security Working Group (CISWG), which has members from the corporate, trade association, and academic arenas. CISWG will work to develop a private-sector-driven approach to securing the nation's information and infrastructure. Putnam had this to say about his efforts (www.house.gov/putnam/pressreleases/cswg.doc):

“I have visited a variety of companies, and have determined that the matter of in-

History tells us that some sort of government intervention or regulation is almost a certainty for the information-security industry. Whether we justify such action on product safety (automotive, electrical appliances, and nuclear reactors areas, for example) or on national economic stability (public company disclosure, Y2K remediation disclosure, and so on), items of national importance often become regulated. I believe that given the economic risks associated with a concerted cybersecurity attack on the United States, some form of regulation will be thrust upon our profession in the next several years.

But regardless of what is likely to happen, questions remain: Is regulation good for information security? Good for the US? Can we do it in a way that will have an actual impact on security? What forms of regulation make sense? What criteria for being secure is sufficient? Where can we get answers?

Regulation pros and cons

Security experts have mixed opin-

ions about whether regulation has a positive impact on our profession and on information security in general.

Regulation pros

Here are some reasons in favor of regulation.

Improved security. We can debate how much improvement regulation actually can provide and the extent to which improvement will unfold over time. However, it's common knowledge that regulation improves quality and security because it forces those who don't do anything to at least do something. The question is how much? The reason is simple—many companies have little information-security protection beyond a firewall and antivirus software. There is so much room for improvement that we're likely to achieve it even if we do a bare minimum.

Positive economic impact. If we can demonstrate that security regulation adequately addresses security concerns, publicly disclosing this information would provide comfort and confidence to consumers, corporate investors, and the federal government. In any case, there is no reason we shouldn't crow about progress (as long as we're making it).

More sophisticated security awareness. Regulation makes any topic a board- and executive management-level issue. There is little question that getting corporate management and boards of directors to understand information-security's risks and rewards will elevate security professionals in the eyes of the corporation. Over the last few years, they have become more important and more valuable, moving from operational to more strategic roles. The chief security officer position will continue to gain importance and regulation will only accelerate the process.

Regulation cons

On the other side, there are minuses to consider.

Cost. Regulation costs money: corporate dollars to stay in compliance and tax dollars to audit and regulate the compliance. For example, 48 percent of public companies say they will spend more than US\$500,000 per year complying with the new Sarbanes-Oxley Act (*CFO* magazine; www.cfo.com/article/1,5309,10546||1,00.html). Such expenditures affect return-on-investment (ROI) and other bottom-line results.

How much is enough? Security professionals disagree about what level of rigor and detail makes sense for information-system security regulation. If all we need are network-centric system-level assessments, how much confidence do we gain when most of today's attacks are the result of software security risk? Why regulate security and not software, which often comes with no manufacturer's warrantee?

Disagreements about metrics. Currently, security experts disagree over security metrics. Simply put, we don't know what to measure and how much of whatever we need to measure is sufficient to call a system secure. Security is a process, not a product, and there are always things that we can improve. How do we set the passing-grade bar high enough to produce reasonable confidence but low enough to be affordable? What is security's ROI?

The lack of definable boundaries. Cybersecurity is an international issue. Today's networks do not have physical boundaries. In fact, the Internet is available in countries even while they are at war. All of this makes implementing regulations to protect our homeland a difficult proposition. Any competent security professional will tell you that secure

components can integrate in insecure ways. How can we secure anything connected to the Internet? Much of it is outside the US government's purview.

These pros and cons raise some seriously thorny issues. The strong points on both sides of the issue exacerbate the problem of arriving at an informed opinion. So, what is a thinking security person to do?

One worthwhile exercise involves studying how the Year 2000 Problem was handled from a regulatory perspective. Y2K makes a reasonable case study because it's probably the closest example we have to the problem at hand. Perhaps, by understanding how a set of very similar pros and cons played out in a related area, we can learn some lessons and apply them to our problem.

The Y2K bug: a regulatory case study

Many computer professionals were well aware of the impending Y2K Problem by the mid-1990s, but few corporations were working actively on it. We're in a somewhat similar position now. Many technologists understand the security problem's implications, but most nontechnologists have only the vaguest understanding. In 1997, the US Subcommittee on Financial Services and Technology of the Senate Committee on Banking, Housing, and Urban Affairs called on the Securities and Exchange Commission (SEC) to address public companies' Y2K disclosure obligations. Brian Lane, director of the SEC's Division of Corporate Finance, testified that under current law, investment companies and advisors must disclose any Y2K problems that could not be corrected by 1 January 2000 and would materially affect the company's or advisors' abilities to fulfill their contractual obligations.

The SEC testimony, and similarly compelling testimony from other concerned parties (Hearing on Y2K

Liability and Disclosure, 22 October 1997; www.senate.gov/~banking/97_10hrg/102297/witness/witness.htm

firms that were not Y2K-compliant by December of that year.

While the SEC ultimately didn't

The irony is that it was precisely the hand-wringing exercise and Y2K mitigation that made sure that nothing happened. Today, successful security is in a very similar situation; if it works nobody notices.

htm and Oversight Hearing on Financial Institutions and the Year 2000 Problem, 10 July 1997; www.senate.gov/~banking/97_07hrg/071097/witness/witness.htm/), convinced Congress to take the Y2K problem seriously. By late 1997, Senator Bob Bennett (R-Utah) introduced legislation requiring public companies to disclose their Y2K readiness in quarterly financial statements to the SEC. Although this legislation never passed, it was a driving force behind pushing the SEC to consider holding all public companies accountable for their Y2K readiness—not only financial and investment firms. This all sounds somewhat similar to our security regulation discussion.

During the next two years, the SEC moved from suggesting general guidance on what public companies should disclose regarding their Y2K readiness to detailing information that must be included in financial statements to adopting a new temporary rule under the Securities Exchange Act of 1934. This rule required many in the securities industry to file specific reports on Y2K work and readiness and established a schedule of fines for non-compliance. To ensure that companies took the rule seriously, the SEC promptly fined numerous organizations for not adequately complying with the temporary rule. A final SEC rule enacted in July of 1999 let the agency shut down brokerage

subject other industries to these fines, a combination of increasing pressure to disclose from the SEC, hearings by Congress targeting critical infrastructure industries, and pressure from customers pushed all businesses to address Y2K concerns and publish statements regarding their Y2K preparedness. A similar groundswell might be building in the security case, but with less of a date-driven impetus for solution. Y2K had a clear and present endgame. Security does not.

Liability concerns regarding public statements on Y2K readiness and antitrust concerns surrounding sharing Y2K problems and solutions within industries prompted Congress to pass several laws in the late 1990s that removed these hurdles and sped the problem's mitigation. The Year 2000 Information and Readiness Disclosure Act of 1998 promoted Y2K information disclosures and exchange by relaxing antitrust laws around information sharing. The Y2K Act of 1999 limited companies' liability associated with Y2K when they made full and proper public disclosure of their status.

Then, nothing happened. Some critics called into question how technologists could be so wound up, spending over US\$5 trillion worldwide on a problem that seemingly fizzled out. The irony is that it was precisely the hand-wringing exercise and Y2K mitigation that made sure that nothing happened. Today, suc-

cessful security is in a very similar situation; if it works, nobody notices.

There still is much debate regarding whether Y2K preparedness was a waste of money. Critics point to the lack of problems that actually materialized on and after 1 January 2000 as evidence that the entire issue was blown entirely out of proportion by Y2K consultants and government regulators. Proponents believe that the reason so few problems were identified is directly related to the intense focus on identifying and correcting problems prior to the date. Both agree that the impact of date problems in embedded systems was greatly exaggerated and resulted in a mistaken belief that critical infrastructure around the world was much more likely to fail than was actually the case. Does a similar amount of hype (or appearance of hype) surround cyber security?

An estimated US\$100B was spent on Y2K in the US. Established in April 1998, the Senate Special Committee on the Year 2000 Technology Problem held 34 hearings and heard the testimony of 150 witnesses. The federal government alone spent US\$8.5B assessing, fixing, and testing for Y2K problems (GAO Report, "Year 2000 Computing Challenge: Lessons Learned Can Be Applied to Other Management Challenges," (AIMD-00-290). <http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.88&filename=ai00290.txt&directory=/diskb/wais/data/gao/>).

The early days of Y2K sound very similar to today's discussions regarding information security. There is talk of public disclosure, talk of government regulation, talk of critical infrastructure. Mostly just talk. So, what can we learn from the Y2K experience and how can we apply it to assure that if and when our federal government gets involved, we get more secure systems and not just red tape and fees?

Three

lessons learned

What can we learn from this Y2K experience? I think there are three broad lessons regarding regulation that we should consider when thinking through how to regulate information security: the SEC's role, congress' role, and the overall approach to regulating technology.

Lesson 1: The SEC is an effective change agent

Y2K demonstrated that SEC information-disclosure guidelines and regulations are a surefire way to get corporate America to sit up and pay attention. The Sarbanes-Oxley Act hammers this point home. It is little wonder that DHS Secretary Ridge is focusing some of his attention on convincing the SEC to consider rules regarding information-security preparedness. It is also little wonder that the (activist) SEC is listening.

Today, our business successes rely much more intimately on our information systems' integrity and security than ever before. As information system failures often are the root cause of significant business disruptions and revenue losses, you would expect that the SEC would look to increase our information systems' reliability and security regardless of national security implications.

Because the SEC was so successful at affecting Y2K change—beginning somewhat subtly and ending with a hammer—we're likely to see that happen again. The SEC makes a good corporate change agent.

Lesson 2: Congress is an enabler, not a regulator

Congress should work to clear hurdles for businesses to share information and work together instead of mandating specific types of security regulation. We must manage disclosure problems carefully—especially those involving privacy. Congress should not create laws that dictate specific measures, especially when

we consider what current laws actually say about “digital signatures,” terms with murky definitions.

Laws are not flexible enough to shift and change as needed by a rapidly changing and advancing industry like IT. We should welcome legislation that lets companies share security vulnerability data and best practices. (Although a controversial opinion, I believe that any law that reduces liability associated with security breaches when certain acceptable standards are met might help our industry tremendously.)

Lesson 3: Regulation doesn't have to be all or nothing

Rather than developing formal, structured regulations around Y2K, the SEC's approach of starting with simple guidance that ratcheted up as necessary over time was particularly effective. We should adopt this approach.

Of course, information security is a much more difficult problem than Y2K. This is not a simple software bug to be fixed with static analysis and some Cobol patches. We need to start any government involvement slowly and as simply as possible. I suggest that the government would be wise to leverage industry efforts to define and abide by security best practices. Subtle economic incentives, such as working with the insurance industry to reduce premiums if adequate security measures are in place, are excellent market drivers. The notion of directed tax breaks to reinforce a positive security direction also might help.

Holding our collective breath

When an impending problem can cause significant economic damage or harm to the homeland, some form of regulation will happen, so it looks like we're in for it. It is up to us to think through this issue carefully, and ensure that

any regulatory move does more good than harm. Our best strategy is to engage the government now, teaching it the subtleties of the problem and making suggestions that can only serve to help us all.

Jeffery E. Payne is president, CEO, and cofounder of Cigital, a software quality management company. He is a software expert and speaks to companies about the business risks of software failure. He has testified before Congress on issues such as intellectual property rights, cyberterrorism, and software quality. He has a BSc. in computer science from Allegheny College and an MSc in computer science from The College of William and Mary. He is a former ACM National Lecturer and the cofounder of the Northern Virginia Chapter of the IEEE Computer Society. Contact him at jepayne@cigital.com.