



Competitive
Enterprise
Institute

Issue Analysis

Cybersecurity Finger-pointing

Regulation vs.
Markets for
Software Liability,
Information Security,
and Insurance

by Clyde Wayne Crews Jr.
May 31, 2005

Cybersecurity Finger-pointing

Regulation vs. Markets for Software Liability, Information Security, and Insurance

By Clyde Wayne Crews Jr.

The only system which is truly secure is one which is switched off and unplugged, locked in a titanium lined safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then I wouldn't stake my life on it.¹

Computer security expert Gene Spafford

Executive Summary

We face unprecedented information security vulnerabilities in our hyper-networked, global economy. Leaving the path clear for private, technical, market, and contractual solutions, and avoiding governmental mandates that impede contractual liability and insurance markets, should take priority. Embracing legislation or mandates can mean locking in collective “solutions” that may be hard to correct, undermining information security rather than enhancing it. Policymakers, along with the computing and infrastructure industries, should think carefully before implementing further federal regulation over risk allocation.

The principle for cyber-risk allocation, as much as one can be defined, is that government's protection function should not overburden the ability of markets to self-insure or self-protect via technology, contractual liability and insurance instruments. Although there is not always a bright line, government must better distinguish between proper public and private responsibilities in information security, and avoid dictates that interfere with these private alternatives as technologies or other conditions change. Interventionist approaches will create jealousies among players, and lead to a politically driven hodgepodge of liabilities and immunities. Uncritical government assumption of responsibility for network and critical infrastructure risks can roll back progress without contributing to information security, cybersecurity or even national security.

because an electronic message was ‘sniffed,’ or ‘spoofed.’ Someone’s health or financial records are going to get into the wrong hands. A design will be compromised; someone will get hurt. And at that point, network television cameras are going to be focused on a lawyer who’s asking a company executive, or a government official, ‘Sir, were there reasonable alternatives at the time?’”⁷

Some politicians and governmental bodies agree. Echoing a National Academy of Sciences panel that proposed an end to software liability exemptions, Rep. Rick Boucher (D-VA) said, “The producers of software should be responsible for any flaws that the software contains” and noted the possibility of congressional action.⁸ Even former federal cyberczar Richard Clarke, while opposing any sort of “cybersecurity police,” did envision government providing a “backstop” for cyber-insurance companies and even assisting in the development of actuarial tables.⁹

Is the shift in attitude toward holding software makers or online services liable a positive development, a suitable answer to today’s security woes? This is a precarious time in software/business history, and caution is warranted before making such sweeping changes. Options more suitable and more adaptable than political mandates do exist, and that flexibility will likely prove even more important as cyber-hazards grow.

Today’s Contracts, or Tomorrow’s Regulation?

Software is generally governed by “End User License Agreements” whereby rights are allocated via disclaimers and the users’ clicked “I accept” agreement.¹⁰ In that sense, these common provisions are simply contracts that courts uphold. Monetary losses are typically governed by such contractual agreements, while physical harm or property damage would be governed by more general product liability law. Thus, software isn’t treated entirely differently from physical products. Software is often sold “as is,” limiting the vendor’s liability, with few express guarantees made regarding performance or security or even possible damage to a customer’s computer or operations. While disclaimers are often criticized with respect to software, such agreements are common in non-software markets as well.

Of course, the full scope of liability in the online world is an unresolved issue, which is not altogether surprising given the many varieties of online transactions that exist, combined with the relative novelty of universal networking itself. Frontier industries and services bring vast benefits—along with their share of headaches and annoyances. An increasingly online customer base will help determine over time what kinds of security breaches various companies in the

This is a precarious time in software/business history, and caution is warranted before making sweeping changes. Security options more suitable and more adaptable than political mandates do exist, and that flexibility will likely prove even more important as cyber-hazards grow.

Contractually driven approaches that treat liability as an evolving relationship should prevail over regulatory approaches that mandate liability, or at the opposite extreme, indemnify companies from liability when technologies fail.

transaction pipeline are accountable for, and ultimately the extent to which they face liability exposure. Disclosure and other business practices that emerge can play a role, as can shareholder suits. For example, according to an *ABA Journal* analysis, disclosure that information was compromised might protect a company from potential liability to shareholders for breach of fiduciary duty when officials were contractually obligated to maintain confidentiality of that information.¹¹

A set of laws called the Uniform Computer Information Transaction Act (UCITA), which would have extended certain additional indemnity to software makers, has been largely abandoned in the state legislatures given the current pro-liability climate.¹² Opposition to UCITA partly stemmed from the concern that certain hardware products heavily reliant on software—like automobiles and aircraft and medical instruments—could try to redefine themselves as software and gain further liability exemptions.¹³

Contractually driven approaches that treat liability as an evolving relationship should prevail over regulatory approaches that mandate liability, or at the opposite extreme, indemnify companies from liability when technologies fail. Limitation-of-liability contracts are commonplace in allocating economic risk, as parties commonly give up certain rights to sue as a condition of receiving services in many contexts.¹⁴ Risk allocation is a complex operation requiring continual renegotiation in the market, and is not well suited to government declarations that one party or another should be liable. Intermediate options exist as well: mandatory arbitration clauses, in response to uncertainties of legal liability and the courts, are on the rise in numerous economic sectors, including online services. While long-standing in fields like stock brokerage contracts, arbitration clauses are finding their way into onto services like cable TV, cell phones, online retailers, gyms, auto financing firms, travel agencies and summer camps as well as high-speed Internet services like those of Comcast and AOL.¹⁵

Assuming a software maker isn't somehow grossly negligent, the *perpetrators* are the ones that should be held accountable for damaging intrusions committed online. One may not enter even an unlocked house—even assuming some software programs leave the security “doors” open. Identity theft is illegal, regardless of whether software or networks are bulletproof, and regardless of whether committed online or offline. Indeed, information security dilemmas encompass non-Internet threats, too, such as identity theft via stolen Social Security numbers. Online victims, whether a company whose network is attacked or an individual whose identity is stolen, are saddled with the costs as real as those of a physical break-in. Society adapts to uncertainties and potential calamities in the offline world (door locks and homeowner's

insurance, for example); adaptations with respect to cyber-invasions include improvements in parallel security technology, as well as insurance. Online or off, strategies for coping with invasions should be harmonious, and lean toward holding the actual criminals accountable. Indeed, the complex interplay between market-driven expansions of insurance and contractual liability is likely to figure prominently in the resolution of cybersecurity concerns.

The proper response is not to legislate and regulate, but to allow changes in industry norms and practices to secure the ends that regulation can only mimic. These changes would entail more than technological advances, but contractual ones. For example, firms reliant upon secure software might increasingly push to alter the nature of end user agreements, thus giving themselves more leeway to sue. Perhaps even “collusion” on the part of industry software buyers to demand better terms is in order; this possibility is one reason why avoiding antitrust interference with industry self-help is important. And favorable changes in software buyer terms that industry buyers obtain might filter down to household users, too, making everyone better off. But a market-driven process of give-and-take is important to the future security environment.

The proper response is not to legislate and regulate, but to allow changes in industry norms and practices to secure the ends that regulation can only mimic.

Legislative Commandments Impede Evolving Cybersecurity and Liability Standards

Unfortunately, the Internet environment allows one company’s network to serve as a platform for attacking others. That has created agitation for governmental intervention, but it also points to an inherent unfairness in automatically pointing fingers at a software maker or service provider. “Your security depends on my security,” as an official at the federally funded CERT Coordination Center put it; “If an intruder can compromise my network, my network and my systems can be used to attack yours.”¹⁶ Yet even with those hazards, those concerned about limitation of liability contracts can, and do, demand better software from companies that are willing to stand behind it, and refuse to deal with those who do not make guarantees. Buyers do not have to accept the status quo in terms of end user agreements, but they need not run to government for relief. If cybersecurity problems are severe, major customers should increasingly exercise their own “market power” to demand certain desired software features. Microsoft, for example, is making changes in its new version of Windows in response to such security concerns, and other vendors are responding to quality concerns in similar fashion. Agitation from industry itself will likely be an increasingly potent driver of cybersecurity.

Legislated liability decrees would also interfere with the resolution of more routine non-security-related liability issues in the computing world.

Since quality improvements and market-driven liability can be expected to play an increasingly important role, sudden government liability mandates would be problematic. Government intervention would complicate the nascent marketplace for advances in contractual liability and recovery, such as guarantees, “quality of service” assurances, and cyber-insurance. Proposals for mandated liability also conflict with the government’s own recent homeland security policies, which would, in some instances, indemnify vendors from liability in spite of what markets might prefer. Indeed, the impact of governments’ explicitly absolving some firms from liability in pursuit of certain homeland security goals arguably should be of more concern than the fact that liability is contractually limited by marketplace licensing agreements. Indeed, the distinction between the “security” we typically expect the market to provide (like door locks, passwords, and firewalls), and the “protection” provided by government as part of its national security and police functions are important, but often overlooked. The centrality of a private-sector role in security innovations ought not be undermined; insurance and liability standards, in their infancy in cyberspace, are tools for bolstering security. Government should allow them to evolve, not legislate them into existence out of well-meant but misguided concerns about national security.

Networking, the linking of one’s computer with others, is a potentially risky activity with costs as well as benefits—particularly on a non-proprietary network like the Internet. In terms of assigning blame if things go wrong, there appear to be two basic targets of culpability at the business level: liability for software makers, and the potential liability of companies who suffer some breach if *their* customers are harmed. (We are setting aside for the moment that a household end-user may fail to perform upgrades.) Lax security practices can unquestionably be dangerous; therefore, better security hygiene by vendors and companies, as well as appropriate professional ethics on the part of vendors, are critical. Among the enablers of that competitive market discipline are emerging insurance products that limit how recklessly companies can behave via audits and premium adjustments (firms that take more precautions may get lower premiums or a prized quality certification, for example). Instead of legislative requirements, appropriate risk allocations should be subject to negotiation, with industry players free to change terms of contracts regarding liability over software use and the acceptable operation of networks.

Legislated liability decrees would also interfere with the resolution of more routine *non-security-related* liability issues in the computing world. Software performance glitches often fall outside the realm of security. Software failures have led to airline crashes, to the loss of 1999’s Mars Polar Lander, and to a vehicle recall (caused by

buggy anti-lock brake software).¹⁷ Another liability-related issue involved claims that America Online's AOL 5.0 software damaged users' computers, which—while damage was at issue—is not the sort of problem that falls within the rubric of cybersecurity.¹⁸ Creating a fertile ground for exploratory liability standards would be more productive than a lurch toward liability mandates in the presumed service of information security. That evolutionary process would prove superior to the rigidity of legislative commandments holding all software vendors, corporate networks that fail to patch, or other “villains” statutorily liable. Court decisions in the case of non-security related failures may be right or wrong, but they can help lead to the improvement of liability contracts over time.

Blame and Liability: It's Complicated in Cyberspace

Even if it were appropriate for governments to assign liability for future cybersecurity breaches, it's not as simple an allocation as one might assume. It is often noted that a single company's network (or even a homeowner's computer) can be used to anonymously launch attacks. The true perpetrator remains masked.

As cybersecurity's importance to our information-based society has grown, the problem of properly allocating liability sometimes lacks easy answers. The root of today's problems are not that business practices have progressed too far down the path of click-licenses and shrink-wrap agreements, making abrupt reversal problematic and counterproductive. Rather, on a public Internet open to everyone, *private parties don't always stand in a position to make comprehensive security guarantees*. The Internet is not a proprietary network on which a given vendor sets all the terms and can eliminate troublemakers who refuse to comply. And as more individuals and businesses adopt cable and DSL broadband (and whatever their successors may be) and leave computers online 24 hours a day with hard drives exposed to the world, swarms of computers become subject to hijacking. Today's misguided effort to impose liability on corporate America overlooks the global, public, unregulated peer-to-peer nature of the Internet that facilitates “borrowing” by anonymous hackers. Targeting vendors ignores the underlying reality that the trouble is *deliberately caused* by troublemakers, rather than software makers, corporations with a less than bulletproof network, or ignorant users who allow their computers to become hijacked.

On a public Internet open to everyone, private parties don't always stand in a position to make comprehensive security guarantees. The Internet is not a proprietary network on which a given vendor sets all the terms and can eliminate troublemakers who refuse to comply.

Blaming the developer of a repeatedly attacked piece of software when it finally succumbs to such insults may or may not be appropriate in particular cases, but generally, the attacker rather than the victimized software maker should be accountable.

Wired News and other technology sites have spilled a lot of ink on stories about user-friendly virus-making kits like the VBS Worm Generator, designed specifically for attacking computers.¹⁹ Blaming the developer of a repeatedly attacked piece of software when it finally succumbs to such insults may or may not be appropriate in particular cases, but generally, the attacker rather than the victimized software maker should be accountable. Granted, some code is more secure than other code. But if a crime akin to breaking and entering has occurred, then imposing vendor liability—unless specified in contract—seems both economically and morally questionable. Indeed, some hackers have a novel perspective regarding other people’s computer files. Unsuspecting computer users can be monitored by ShareSniffer, for example, one of many tools that allows users to “sniff” for files on others’ computers. As the ShareSniffer website told users: “[Y]ou can use your own Microsoft Windows operating system to navigate other computers that have been voluntarily shared to the Internet.”²⁰ Note the clever use of the word “voluntarily.” It’s a safe bet that many of the same agitators for liability on the part of software makers like Microsoft have themselves “allowed” their computers to become a conduit for attacks on others by failing to block spyware or a virus.

Given the public, open character of the Internet, mandates for vendor liability is inappropriate and a diversion, since anyone’s insecure computer can be used as a platform to attack other networks, and since mandates do not alter the basic fact that technological advances along with insurance and risk-allocation instruments are necessary to address security problems. Microsoft’s Windows is a popular hacker target, and hackers even get self-righteous, blaming the company for weaknesses that allow them to succeed. But this is a dubious stance in any venue, as *Money* columnist Allen Wastler helpfully notes:²¹

“You may not like Microsoft. ...But that doesn’t mean you have a right to vandalize its products or its service. Or hurt the people who use those products....I don’t like my commuter train service. Alternatives exist but are limited. They could make the rail service better, but they don’t. Does that allow me or anyone else to exploit holes in the transportation system, which are many, and screw with the commute? Of course not.”

As it stands, on an anonymous Internet, vendors have limited control of what end users do. Even if software ships with vulnerable services or default settings adjusted so that hacker access is (presumably) prevented, users may alter those settings, or hackers may even alter them externally (for example, by guessing a password). In a corporate setting, even if vendors ship software with security features enabled or provide patches, administrators may not follow through.

There is a tradeoff between leaving features in software open for ease of use, and closing those features for security purposes.²² Other downstream missteps are also beyond the software vendor's control, such as accidental exposure of passwords, or selection of passwords that are too easy for hackers to guess. Clearly, better security practices by system administrators and home users can make many incursions impossible, but often in the cybersecurity debate there is a tendency to blame vendors rather than administrators or users for failing to take commonsense steps. Regarding proper roles of the marketplace and government, some experts have rightly noted the need for astute system administrators rather than interference from federal administrators.²³

Clearly software developers can't control everything others do: some individual users will never secure their machines or download each new security update. Software is constantly updated, and its use is not generally within control of the vendor: where earlier software versions seems to work well enough, many users won't bother with updates. Network administrators sometimes make unauthorized changes to proprietary software, often as a shortcut or to carry out a directive from their own bosses.²⁴ Rogue employees with a grudge could induce a breach undetected, with the blame incorrectly falling on the software maker. Even installing updates can create problems: issues raised by new versions of software include negligent or erroneous installation; conflict with a previously installed feature or setting; and possible introduction (whether inadvertent or not) of a security hole.²⁵ This is not to argue that there cannot be honest disagreement over whether there are really flaws in software, or whether it is used incorrectly; but it is important not to institutionalize a regulatory bias that always infers that software is at fault. Note also that even where software vendors are at fault, there would seem to be a responsibility to mitigate one's damages: once a user learns of a flaw, one cannot simply let virus writers do their will and expect to recover from the software maker.

One might also imagine instances in which hardware makers could be held accountable for breaches, whether fairly or not. Related to the risks posed by the peer-to-peer character of the Internet is the simple fact that devices connected to critical networks change over time, and can create uninvited havoc for network administrators. Experts at the 2002 Defcon security conference pointed out the possibility that numerous hardware components, from game devices to office printers to a TiVo recorder, can run code harmful to a network.²⁶

Another problem with liability mandates: Whom would one sue for problems that emerge with open source software? If such software dominated in, say, the operating system market, or becomes

Clearly software developers can't control everything others do: some individual users will never secure their machines or download each new security update. Network administrators sometimes make unauthorized changes to proprietary software. Rogue employees with a grudge could induce a breach. It is important not to institutionalize a regulatory bias that always infers that software is at fault.

more prominent in government computer systems, hackers might inflict serious damage if they redirected their attention to it. Since open source software is freely available in the public domain and can be altered by anyone, responsibility for its potential failures is not obvious.

The security outsourcing business, in which firms contract out their network security monitoring needs to specialists, might be altered by liability mandates on software developers as well. If liability is imposed on software developers, that can lessen the incentives for network monitoring companies to make ironclad guarantees about their services. They might be tempted to point the finger at the software maker if something does go wrong, even if they are at fault. Liability mandates would change the dynamics of this industry, putting it in a more adversarial stance with respect to software makers.

If legislators choose to assign liability, lobbyists will inevitably descend upon Washington, pointing fingers at rivals or even firms that should be partners in information security goals. Apart from software vendors, there are many creative options about whom else to regulate.

Adversarial relationships among key players in the information economy would be an unfortunate development. Occasionally, assumptions about the security of certain seemingly ironclad techniques and procedures will turn out to be false. Consider some surprise vulnerabilities. The email security program Pretty Good Privacy was found to contain a flaw that would allow an uncomfortable degree of control of the recipient's computer, if the sender were inclined to snoop.²⁷ And a hole was discovered in anonymous Web surfing technologies by which an interloper might investigate items in the victim's browser cache.²⁸ Until this discovery, no one had any reason to doubt that websites one visited were private. Unexpected vulnerabilities don't just occur online: Recently, security professionals were surprised by a newly revealed vulnerability in door locks that operate on a master key system, such as an apartment building. (Ironically, the insecurity was discovered using techniques employed by hackers to penetrate computer systems.) Researchers devised an approach by which one can use any given key to create a master.²⁹ When weaknesses are revealed late in the game in longstanding procedures and technologies roundly regarded as secure, it's harder to credit the venom directed at firms like Microsoft or Oracle or AOL. A cooperative environment in which the marketplace can rapidly respond should outperform adversarial regulatory approaches.

Speaking of adversarial stances, imposing liability rather than permitting it to emerge through experimentation can backfire by primarily benefiting big companies relative to small ones, and otherwise can create considerable confusion and disarray. If legislators choose to assign liability, lobbyists will inevitably descend upon Washington, pointing fingers at rivals or even firms that should be partners in information security goals. Apart from software vendors, there are many creative options about whom else to regulate. Web sites that

experience outages and cause headaches for customers—such as an online trading service—could be one option; alternatively, the ISP and backbone providers that support the failed website might be vulnerable to regulation.³⁰ We could end up with a “Superfund-like” fiasco with all suing all, including attack victims who unintentionally help propagate viruses. It’s likely the buck would not stop with software makers, so who might be next? Companies with insecurely barricaded networks? The ISPs? Consumers who fail to install firewalls? (Even the home user may not be immune.) Even without deliberately harmful code, there can be plenty of blame to go around. Unfortunately, as the legislative response to email spam showed, government will act if the industry does not, even if the legislative solution is no real solution at all. The urge to “do something” means industry should react as quickly as possible, or regulation and a tangle of liability findings could soon loom on the horizon, despite the fact that assigning blame to those other than criminals is misguided. As Professor Margaret Jane Radin of Stanford put it, “A court is going to say it is negligent of you not to implement preventative measures if they are reasonably effective and affordable.”³¹ Genuine cybersecurity entails addressing the more fundamental problem of online *authentication*, the lack of which underlies other controversies such as those over online file-sharing and email spam.³² Policymakers should instill cooperation, not blame and fighting, but market players must respond quickly with new strategies.

Unfortunately, as the legislative response to email spam showed, government will act if the industry does not, even if the legislative solution is no real solution. The unattainable ideal is for it to be impossible, not merely illegal, to break into a network.

In the cyber-liability debate, policymakers should bear in mind that the Internet is being used for purposes for which it was not designed. We insist upon using the insecure Internet, demanding ironclad service, all the while knowing, whether we acknowledge it or not, that the Internet is inherently insecure. Liability can and will gropingly emerge in the marketplace even against this perplexing backdrop. But it is not as simple a matter as having government require it. Legislatively providing for lawsuits on an Internet that, at present, is *not capable* of being secure but designed only for exchanging data, is a confused step. After all, if one connects a computer to a network one knows to be insecure (we have never had grounds for claiming the Internet was otherwise) one may not bear responsibility for the resulting havoc; but nor can one claim ignorance of the risks. The unattainable ideal is for it to be impossible, not merely illegal, to break into a network. In such a scenario, one would expect that network owners and vendors increasingly adhere—and require network participants to adhere—to strict security policies. Evolving standards, such as improvements in authentication, membership requirements, cooperative network protocols, improvements in network architecture, biometrics and numerous other technological advances, can increasingly be ways that industry players and end users internalize

and control risks and eliminate the “market failures” that many invoke as justification for security regulation today. Such technical and market improvements can be prerequisites to the security guarantees that policymakers and the public would like to see. But the evolution can not be hastened by law; in a competitive environment, healthy contract-based innovations to establish liability for lapses—along with better methods of protection—stand the best chance of being created. Industry competitive discipline and consumer demand have vital cybersecurity roles to play.

Traditional insurers have responded to cyber-threats by offering coverage against hacker intrusions, virus damage, denial-of-service attacks, identity theft and extortion.

The Emergence of Cyber-insurance

Regulations would tend to hold companies or individuals accountable for things they can’t always control, rather than target the characters who deliberately engage in sabotage. But, barring negligence, the offender is not the software vendor or the network operator, but the hacker. However hackers aren’t always particularly deep-pocketed, meaning that even if they were caught, it may not help anyone much in terms of financial recovery.³³ Enter cybersecurity insurance.

Insurance markets experienced turmoil after the terrorist attacks of 2001. Yet recovery, including new cybersecurity products, is at hand. Following the terrorist attacks, many insurers threatened to drop property and casualty insurance, and warned of the need for government intervention to offer backup terrorism insurance to spread risks: In 2002, for example, Liberty Mutual Group CEO Edmund F. Kelly wrote in the *Washington Post*, “If there is one essential piece of legislation...it is the federal terrorism insurance bill.”³⁴ M. R. Greenberg, chairman at the time of American International Group, Inc., said “[T]he insurance industry does not have the capital to provide adequate insurance coverage against future acts of war...”³⁵

Legislation was enacted, even though markets did begin to adjust, as new instruments emerged for what had been unpriced, unknown risks.³⁶ The problem wasn’t a market failure, as the Cato Institute pointed out; free market pricing needs to include all relevant costs and benefits, and after September 11, 2001 the markets were giving “news we don’t like hearing”: that risks had changed.³⁷ But the existence of risk is the basis of insurance markets. Business columnist Holman Jenkins noted in the *Wall Street Journal* that car accidents, hurricanes and earthquakes don’t end insurance, they are seen as reasons to sell more: Indeed, “[T]he industry would be rebelling against its own gene pool not to take advantage of surging demand and prices for terrorism coverage.”³⁸ Ditto for cyber-insurance. Traditional insurers have responded to cyber-threats by offering coverage against hacker intrusions, virus damage, denial-of-service attacks, identity

theft and extortion.³⁹ Visa offers insurance against identity theft to member banks, which would provide up to \$15,000 for cardholders.⁴⁰ Some homeowner policies now offer identity theft insurance.⁴¹ AIG eBusiness Risk Solutions, after about three years in the cyber-insurance business, had issued over 2,000 policies as of October 2002, costing from \$1,000 to hundreds of times that, with most claims arising from virus damage.⁴² The inadequacy of some traditional insurance policies might drive new cyber-insurance products. Some companies have begun acquiring stand-alone “network risk insurance” costing \$5,000 to \$30,000 annually for \$1 million in coverage, rather than acquiring them within general liability policies.⁴³ Other companies offering various types of cyber-insurance include Chubb and Hiscox (a Lloyd’s of London affiliate) for protection against data loss, and lost sales. The Insurance Information Institute has estimated the cybersecurity insurance market will reach \$2 to \$3 billion over the next few years.⁴⁴

As firms are induced to acquire cyber-insurance as a new cost of doing business, they are seeking to lower those costs by adopting the latest and most reliable security practices; that’s a good substitute for government regulation. Essentially, those businesses that fail to adhere to agreed-upon standards will be denied insurance, forcing a change in internal security practices. The White House, noting that insurers and firms worked together to sort out divergent fire safety and electrical safety standards in the early 1900s, expects businesses to increasingly seek coverage for data and assets in an evolution that mirrors that earlier emergence of standards.⁴⁵ Insurance coverage, perhaps obtained after a security audit to ascertain a company’s network security status, can protect from data theft, viruses, denial-of-service, Web site defacement, credit card fraud and cyber-extortion.⁴⁶ The more precautions companies take, the lower their premiums. For better rates, companies will need to demonstrate compliance with specified practices, such as installing software patches, outsourcing security monitoring and maintaining firewalls. Increasingly, as more broadband users and companies come online, upstream and downstream firms will demand cyber-insurance, security outsourcing, or other changes with respect to security practices. Oracle, for example, as a part of its security efforts, requires that its component suppliers complete a checklist to prevent Oracle’s reputation being harmed by a partner’s mistake.⁴⁷

Security expert Bruce Schneier noted several years ago that computer security is really a branch of the insurance industry:

Eventually, the insurance industry will subsume the computer security industry. Not that insurance companies will start marketing security products, but rather that the kind of firewall

As firms are induced to acquire cyber-insurance as a new cost of doing business, they are seeking to lower those costs by adopting the latest and most reliable security practices; that’s a good substitute for government regulation.

you use—along with the kind of authentication scheme, operating system and network monitoring device you use—will be strongly influenced by the constraints of insurance.... Businesses achieve security through insurance. They take the risks they're not willing to accept themselves, bundle them up, and pay someone else to worry about them. If a warehouse is insured properly, the owner really doesn't care if it burns down or not. If he does care, he's underinsured. Similarly, if a network is insured properly, the owner won't care whether it's hacked or not... The choice of which OS to use will no longer be 100 percent technical... In this future world, how secure a product is becomes a real, measurable feature that companies are willing to pay for...because it saves them money in the long run.⁴⁸

Awareness of security and better professional ethics and computer hygiene are being impelled by marketplace demands. Companies don't want to be put at risk by their partners' lax security practices. Thus, the lack of liability insurance may increasingly be a significant barrier to companies seeking involvement in sensitive commercial or governmental operations.

Schneier elaborated further in congressional testimony in July 2001. "Concerned about denial-of-service attacks? Get bandwidth interruption insurance. Concerned about data corruption? Get data integrity insurance. ... Concerned about negative publicity due to a widely publicized network attack? Get a rider on your good name insurance that covers that sort of event. The insurance industry isn't offering all of these policies yet, but it is coming."⁴⁹

Awareness of security and better professional ethics and computer hygiene are being impelled by marketplace demands. Companies don't want to be put at risk by their partners' lax security practices. Thus, the lack of liability insurance may increasingly be a significant barrier to companies seeking involvement in sensitive commercial or governmental operations. One can envision insurers increasingly offering coverage based on levels to which evaluations or third party audits demonstrate that a company has patched vulnerabilities (perhaps based on lists like the top ten vulnerabilities published by Qualys, a company in the business of certifying networks).⁵⁰ Marketplace alternatives to cybersecurity regulation would likely include an assortment of rating systems before converging on standard practices, but the process is a healthy, necessary one. Security expert Mark Rasch noted the role of insurers in the process:⁵¹

Some insurance companies have already developed rudimentary underwriting criteria for cyber-insurance—no firewall, no insurance. And the principles of good security are no secret. How often is security assessed and tested? Once a year? Every week? How good is the intrusion prevention-and-detection technology? What about policies and training? Incident response plans? Biometric access control for critical systems? Disaster recovery and business continuation? Standards exist,

but they must be coordinated and codified in a way that creates a meaningful ratings system.

Various elements of today's policy debate can be resolved by the coordination process of the market. For example, if information sharing is truly important to reducing risk—consider the debate over whether or not to publicly disclose breaches, for example—then that too will ultimately be reflected in premiums.

Other potential criteria for insurance eligibility are numerous. Policies could emerge based on the fact that most Internet attacks on companies (around 80 percent) exploit vulnerabilities for which patches or fixes already exist—and companies, for one reason or another, have neglected to address them.⁵² Policies might pay only if those patches were installed. (Again, it seems inappropriate to hold a software developer liable for a given breach when a patch had been long available, and insurance markets could reflect that). Mandatory submission to a network audit could be a requirement for liability coverage, as contrasted to mandatory network audits required by legislation. Insurance could also play a role in determining the level of cyber-training needed, rather than relying on the government-funded cybersecurity training. It is often noted that users want functionality and convenience over security; that ethic will likely change, as software makers, administrators, ISPs, and users respond to the new realities and seek to qualify for insurance. Even helping trap the invaders may be a way of qualifying for insurance: more firms are selling “honeypotware” to Fortune 1000 enterprises and government to bait and trap hackers, and insurers are requesting that their customers make honeypots a component of their cybersecurity arsenal.⁵³

In the non-cyber world, the insurance market is rebounding despite warnings that government would have to serve as insurer of last resort. The cyber-insurance market is in its infancy but also shows promise. There will be different liability standards and categories of insurance for different applications. There will be differences in software and hardware insurance policies. There will be differences in insurance products depending upon types of attacks, and upon whether a company was monitoring for possible attacks, installing patches or performing other kinds of self-help. Government over-involvement in cybersecurity and critical infrastructure management could negatively impact this complex insurance product environment.

In the non-cyber world, the insurance market is rebounding despite warnings that government would have to serve as insurer of last resort. The cyber-insurance market is in its infancy but also shows promise.

Government Intervention Impedes Cyber-insurance Innovations

At the same time government is mulling imposing liability for cybersecurity, it is also enacting liability exemptions in the broader homeland security realm, by indemnifying some companies from responsibility when their security related products fail.

We are on the cusp of addressing a range of security problems with new innovations, including contractual liability standards and insurance products. Yet in the post-September 11 environment, Congress has already engaged in interfering with evolving solutions by offering “backup” insurance and by explicitly absolving companies from liability, even though marketplace contracts might better allocate responsibility and risk. Remarkably, at the same time government is mulling *imposing* liability for cybersecurity, it is also enacting liability *exemptions* in the broader homeland security realm, by indemnifying some companies from responsibility when their security related products fail. But if careful risk allocation is what the marketplace needs, indemnification is a curious step. The market’s efforts to negotiate and grapple with cybersecurity threats are complex enough, and are dependent upon the unimpeded emergence of liability standards and insurance products.

Like legislative mandates, exemptions must be very carefully considered given the potential disruptions in the complex, changing relationships between companies, ISPs, users and other players. Consider a recent example: in the email spam debate, one major proposal would have given ISPs the right to sue spammers as well as immunize the ISP from liability in the event it accidentally blocked legitimate mail if done in “good faith.” There are legitimate grounds on which to sue spammers that can be and are pursued without legislation. But the government ought not simply endorse ISP blockages that they otherwise would need to defend (or face consequences) while simultaneously facilitating the blocked party’s potentially being sued. Such complex issues would best be worked out in the marketplace given the potential for a non-spammer’s being blocked. Indeed, given today’s cyber-insecurity, the blocked “spammer” may himself be the victim of a hacker who hijacks the blocked party’s good name. As noted, such complexities abound in the cyber-realm, since it is not always obvious who the bad guys are.

As far as indemnification from liability, new legislation incorporated into the Homeland Security department bill limits liability for manufacturers of products related to the fight against terrorism, by indemnifying them for any losses above insurance levels when their “security technologies” fail in the event of an attack. Manufacturers of items like weapon alarms and bomb detectors want the government to pay if they are sued because of a product failure.⁵⁴ The measure, called the SAFETY Act (“Support Anti-Terrorism by Fostering Effective Technologies”) limits liability of a “qualified anti-terrorism

technology.”⁵⁵ Above a certain floor provided by insurance, companies would be shielded from responsibility for product failure. As a Department of Homeland Security press release put it, “Companies investing in the development and deployment of qualified anti-terrorism technologies will be provided with unique protections that will minimize their risks should they be sued in connection with a terrorist attack. Without the Act, many companies may not invest in potential life-saving technologies to protect Americans.”⁵⁶ Time will tell the extent to which this new intervention will apply to cybersecurity related products—the new rule includes security services, an ambiguous term that will surely create uncertainty over who and what qualifies.⁵⁷ The Homeland Security director is given the authority to indicate which technologies will qualify for such a benefit, and he has discretion in bestowing immunity.

While companies would be indemnified against attacks and not ordinary failures, the interventions are still worrisome. While it is a long-standing and reasonable practice that companies providing defense-related products to the government according to dictated specifications should not be held liable for resulting failures, the new legislation extends this so-called “government-contractor defense” to the ordinary commercial marketplace, in which government-approved terror-defense related products are sold, not to the government, but to the general public.⁵⁸ While for national defense purposes indemnity may be responsibly and appropriately offered, indemnity for private, commercial applications, if they fail against an attack, is something new altogether.⁵⁹

Marketplace self-discipline is all that we have apart from political discipline and regulation, and it is undermined by broad indemnification. Indemnification can interfere with competitive incentives to improve products enough to make valid security guarantees. When government subsidization of or intervention into frontier research takes it out of the realm of private insurability, or even provides immunity, the effects can be significant. The Price Andersen Act, which limits the liability of nuclear power plants, has clearly impacted that industry; it may have helped get the industry off the ground, but the industry is fully regulated by government. Indeed, the way cybersecurity is funded, regulated, and insured will clearly impact safety and the prospects for self-regulation. Risks accompany substituting government responsibility for private responsibility, in socializing what may often be ordinary security functions. In politically managing risk, one removes the incentives (like liability and contractual agreements) that are needed to keep private companies in line. Taken too far, government indemnification can mean vibrant markets in liability and insurance may never emerge.

Marketplace self-discipline is all that we have apart from political discipline and regulation, and it is undermined by broad indemnification. Indemnification can interfere with competitive incentives to improve products enough to make valid security guarantees.

Government “insurance” has led to costly bailouts for federal deposit insurance and federal loan guarantees to airlines. Such interventions allow risk-taking that would otherwise be imprudent, meaning they will weaken rather than strengthen cybersecurity if extended to that realm.

Moreover, indemnification’s impact on cybersecurity could be the opposite of that intended. While indemnification is not a direct dollar subsidy, it is an indirect one. But there is no straightforward way to calculate the costs of (perhaps inappropriately) protecting private companies from the failure of their technologies, or the costs of preempting what could have been superior contractual arrangements. But such costs should be on policymakers’ minds. For example, if the government were to demand distribution of firewall software by ISPs, then both the ISP and the software vendor might be likely to receive immunity. Indemnification has also been proposed with regard to information sharing. But explicit exemption from civil liability for an attack merely by sharing information about a vulnerable or unprepared infrastructure can undermine overarching security goals: As one scholar noted, “If an operator of critical infrastructure knows it can avoid civil liability for a cyber-terror attack by simply submitting information regarding the attack to the Homeland Security Department, it will have less of an economic incentive to invest in preventing future attacks.”⁶⁰

In defense of indemnity in insurance markets after the terrorist attacks, Information Technology Association of America’s Harris Miller said, “The risks involved are so great and so difficult to determine that insurance companies are refusing to provide the necessary coverage. Congress must act now to grant risk sharing so that our leading high-tech companies can get on with the business of protecting the American people.”⁶¹ As one lobbyist in 2002 put it during negotiations over the indemnification provisions in the homeland security legislation, “This is the No. 1 issue...It’s where we’re wearing out the shoe leather.”⁶²

But we must not disregard the risks of undermining competitive incentives. As one scholar noted with respect to the airline bailout after the September 11 attacks, “airlines don’t have a market incentive to implement real measures that will significantly enhance security. They operate on the (plausible) assumption that in the event of another terrorist attack, they will not have to bear its costs.”⁶³ Individuals and enterprises alike will act in a riskier fashion if they believe the costs of their actions will be borne by others. Government “insurance” has led to costly bailouts for federal deposit insurance and federal loan guarantees to airlines. Such interventions allow risk-taking that would otherwise be imprudent, meaning they will weaken rather than strengthen cybersecurity if extended to that realm. Nor is it the case that we won’t be served in product and service markets if the government doesn’t step in to indemnify vendors. One example: a company called MSA, which makes the Response gas mask, has indicated it will continue with the marketing of its mask even if it does not get SAFETY Act protection:

“We have been selling products to protect peoples’ health and safety for 89 years...The SAFETY Act is a nice plus but it doesn’t change our business model dramatically.”⁶⁴

Free markets, in cybersecurity as in other pursuits, are needed to overcome moral hazard problems and reduce risks. There is no regulatory shortcut to genuine security. Assuring that government guarantees not hinder and distort private cyber-insurance markets is particularly important because the field is in its relative infancy. Federal indemnification alters incentives of companies to offer more bulletproof products and software. If government is heavily involved, *then* what happens if there is a widespread failure in the event of some major attack? It’s true that cyber-risks are poorly understood; but also important is to realize that the market is the only tool for properly valuing those risks. Yet instead we find the federal government proposing damage caps on amounts underwriters would bear in the event of a cyber-attack, as well as premium subsidies.⁶⁵ Such moves aggravate the problem of holdout—of waiting for legislation to pass before offering insurance and other improvements. At the very least, if government is in the business of providing what should be a commercial insurance service, it ought to charge the going market rate to prevent driving out private competition.⁶⁶

Professors William Yurcik and David Doss note some key remaining concerns surrounding the development of cyber-insurance markets: (1) the lack of data and audit procedures to quantify risk and loss potential; (2) the lack of a widely established market base to spread affordable premiums (3) the fact that post-9/11 worst-case scenarios are very large; and (4) the fact that insurance is not a priority of a typical technology company.⁶⁷ They note, however, that:

Given that these major insurability problems are not intractable, cyber-insurance is a viable and attractive market solution to the software security problem: (1) insurance companies will facilitate standards for best practices and insurability in order to develop cyber-insurance products; (2) pressure on organizations to reduce insurance premiums provides an incentive to reduce their exposure to software security liabilities in tangible ways including demand for security information about products and “safe” software products themselves; (3) pressure on software companies to deliver “safe” products to a market demand or assume liabilities with valid warranties; and (4) pressure on software engineering practices (requirements, development, and testing) to improve in order to provide “safe” products and decrease exposure to warranty claims.⁶⁸

It’s true that cyber-risks are poorly understood; but also important is to realize that the market is the only tool for properly valuing those risks.

The offering of security guarantees and insurance should remain competitive and market-driven. That even means vendors ought to remain free even to offer software about which they make no guarantees.

The cybersecurity debate abounds with much talk about government standards or interventions. As noted above, though, “standards for best practices and insurability” developed in the market are within reach. Markets need the opportunity to react, especially given that government has no special knowledge of how to quantify and assign cyber-risk. Homeland security is complicated enough without scattering unnecessary manmade policy landmines across the cyber-landscape. The offering of security guarantees and insurance should remain competitive and market-driven. That even means vendors ought to remain free even to offer software about which they make no guarantees. Markets will evolve in new ways to enable insurability and the acceptance of liability, if that’s what customers will pay for. As it stands, software programs typically have 10 errors or bugs per 1,000 lines of code, a huge amount in typical million-plus line programs.⁶⁹ Changing the culture to weed out errors quickly is simply not possible in the short term. But protecting a policy climate in which security initiatives, such as insurance and the third-party certification, can flourish is our best hope for improvement. Government shouldn’t impose liability, but it shouldn’t take steps that impede its development either. Nor should it get carried away with indemnification.

Conclusion

A cybersecurity principle, as much as one can be defined, is that government’s cybersecurity protection activities should not impede or burden the ability of markets to self-insure or self protect (unlike the approach taken with airport security). It is not prudent or safe to take information security down the regulatory road by mandating liability or interfering in cyber-insurance markets. Although there isn’t always a bright line, we must better distinguish between proper public and private responsibilities in information security. Policymakers must avoid imposing cybersecurity dictates over essential economic sectors, especially when those dictates make superior private alternatives impossible as technologies or conditions change.

About the Author

Wayne Crews is Vice President for Policy and Director of Technology Studies at the Competitive Enterprise Institute. His work includes regulatory reform, antitrust and competition policy, safety and environmental issues, and various information-age concerns such as e-commerce, privacy, “spam,” broadband, and intellectual property. He is the author of the annual report, *Ten Thousand Commandments: An Annual Snapshot of the Federal Regulatory State*.

Wayne has published in outlets such as the *Wall Street Journal*, *Chicago Tribune*, *Forbes*, *Atlanta Journal-Constitution*, *Communications Lawyer*, and the *Electricity Journal*. He has made various TV appearances on Fox, CNN, ABC and others, and his regulatory reform ideas have been featured prominently in such publications as the *Washington Post*, *Forbes* and *Investor's Business Daily*. He is frequently invited to speak, and has testified before several congressional committees.

Wayne is co-editor of the books *Who Rules the Net: Internet Governance and Jurisdiction* (2003) and *Copy Fights: The Future of Intellectual Property In the Information Age* (2002). He is co-author of *What's Yours Is Mine: Open Access and the Rise of Infrastructure Socialism* (2003), and a contributing author to others.

Endnotes

- ¹ Quoted in Perri Wilbert, "Getting Serious About Security," *Cape Times Technology Supplement*, October 9, 2001. <http://security.kingsley.co.za/articles/article4.htm>.
- ² The White House, *The National Strategy to Secure Cyberspace*, February 2003. <http://www.whitehouse.gov/pcipb/>.
- ³ Charles C. Mann, "Why Software Is So Bad," *Technology Review*, July/August 2002. <http://www.technologyreview.com/articles/mann0702.asp>.
- ⁴ Mann, 2002.
- ⁵ Robert Lemos, "Top 10 Security Stories of 2000," ZDNet News, December 24, 2000. Available at <http://www.zdnet.com/zdnn/stories/news/0,4586,2668051-2,00.html>.
- ⁶ Ray Ozzie, "The Myth of Cybersecurity," *CNET News.com*, August 14, 2002. http://news.com.com/2010-1071-949678.html?tag=fd_nc_1.
- ⁷ *Ibid.*
- ⁸ Cited in Joseph Menn, "Security Flaws May Be Pitfall for Microsoft," *Los Angeles Times*, January 14, 2002. p. C1.
- ⁹ Patrick Ross, "Former NIPC Chief Calls for 'Soft' Cybersecurity Regulation," *Washington Internet Daily*, April 9, 2003. p. 2.
- ¹⁰ Joseph Menn, January 14, 2002.
- ¹¹ "Disclosing a computer intrusion also can save a company from significant potential liability... Say, for example, that company officials knew about a hole in security, and information was accessed through that hole—information the company had a contractual duty to hold confidential. Shareholders could charge the company with breach of a fiduciary duty." Jenny B. Davis, "Cybercrime Fighters," *ABA Journal*, August 2003. p. 39. http://www.wiggin.com/spotlight/news_sample.asp?ID=7573812003.
- ¹² For a pro/con discussion on UCITA, see Sandeep Junnarkar, "The New Software Controversy," October 17, 2002, <http://news.com.com/2009-1001-962336.html>.
- ¹³ Noted in Stephen H. Wildstrom, "Want to Sue over Buggy Code?" *BusinessWeek Online*, September 22, 2003. http://www.businessweek.com/technology/content/sep2003/tc20030922_0232_tc129.htm.
- ¹⁴ For an overview, see Marc T. Shivers and Andre J. Brunel, "Contractual Limitations of Liability (a.k.a. "LOLs" or Why the Other Party Is Laughing Out Loud)," *Computer & Internet Lawyer*, Vol. 19, No. 5, May 2002. p. 6.
- ¹⁵ Jane Spencer, "Signing Away Your Right to Sue," *Wall Street Journal*, October 1, 2003. p. D1.
- ¹⁶ "Another Massive Net attack Looming?" *MSNBC.com*, August 11, 2000. <http://zdnet.com.com/2100-11-522977.html?legacy=zdnn>.
- ¹⁷ Examples noted in Associated Press, "Spread of Buggy Software Raises New Questions," April 27, 2003.
- ¹⁸ See "AOL Not Entitled to Defense On Loss of Computers and Software, Va. Court Says," *Software Law Bulletin*, Vol. 15, No. 8. August 2002. p. 7.
- ¹⁹ For example see Michelle Delio, "New Kit Renews E-Mail Worm Scare," *Wired News*, Mar. 12, 2001. <http://www.wired.com/news/technology/0,1282,42375,00.html>.
- ²⁰ From ShareSniffer Website, at <http://www.sharesniffer.com>.
- ²¹ Allen Wastler, "Blaming Microsoft," *CNN Money*, August 28, 2003. <http://money.cnn.com/2003/08/28/commentary/wastler/wastler/index.htm>.
- ²² Brendan I. Koerner, "The Security Traders," *Mother Jones*, September 1, 2002.
- ²³ Jay Lyman, "Cyber Security Key to New U.S Initiative," *NewsFactor Network*, October 9, 2001. <http://www.newsfactor.com/perl/story/14015.html>.
- ²⁴ Salkever, "Needed: A Security Blanket for the Net," September 16, 2003.
- ²⁵ Software issues are noted in Gary Audin, "Packetized Voice: It's the Software Stupid!" *Business Communications Review*, Vol. 9, No. 32, September 1, 2002. p. 48.
- ²⁶ Elinor Mills Abreu, "Experts Say Computer Hacking Becoming Easier," *Reuters*, August 2, 2002. <http://ca.news.yahoo.com/020803/5/o1nj.html>.

²⁷ See Robert Lemos, "PGP E-Mails May Become Bullets," *CNET News.com*, September 6, 2002. <http://zdnet.com.com/2100-1105-956815.html>.

²⁸ Ian Austen, "Study Finds That Caching By Browsers Creates a Threat to Surfers' Privacy," *New York Times*, December 14, 2000. <http://www.nytimes.com/2000/12/14/technology/14PRIV.html>.

²⁹ John Schwartz, "Master Key Copying Revealed," *New York Times*, January 23, 2003. <http://www.nytimes.com/2003/01/23/business/23LOCK.html>.

³⁰ Example noted in Carl S. Kaplan, "Can Hacking Victims Be Held Legally Liable?" *New York Times*, August 23, 2001. <http://www.nytimes.com/2001/08/23/technology/24CYBERLAW.html?ex=1072155600&en=7da84f6e8d73d88b&ei=5070>.

³¹ Kaplan, August 23, 2001.

³² For an overview see Clyde Wayne Crews Jr., "Cybersecurity and Authentication: the Marketplace Role in Rethinking Anonymity—Before Regulators Intervene," *Competitive Enterprise Institute Issue Analysis 2004 No. 2*, November 8, 2004. <http://www.cei.org/pdf/4281.pdf>.

³³ Kaplan, August 23, 2001.

³⁴ Edmund F. Kelly, "Sharing the Risk of Terror," *Washington Post*, November 13, 2002. p. A27. http://www2.rmi.gsu.edu/faculty/klein/RMI_3500/Readings/Other/TR_Sharing.htm.

³⁵ M. R. Greenberg, "Government Must Be Insurer of Last Resort," *Wall Street Journal*, November 26, 2001, p. A18.

³⁶ See for example Holman W. Jenkins Jr., "How Big Is the Terrorism Insurance Problem?" *Wall Street Journal*, August 14, 2002. p. A13.

³⁷ As described in Peter VanDoren, Tom Miller and John Samples, "Government Terrorism Insurance: Déjà Vu(Doo)?" *Cato Commentary*, January 23, 2002. <http://www.cato.org/current/terrorism/pubs/vandoren-020123.html>.

³⁸ Holman W. Jenkins Jr., "Bull's-Eye Insurance," *Wall Street Journal*, October 31, 2001. p. A25.

³⁹ Noted, for example, in William Yurcik and David Doss, "Cyberinsurance: A Market Solution to Internet Security Market Failure." White paper, presented at the Workshop on Economics and Information Security, University of California, Berkeley, May 16-17, 2002. <http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/53.pdf>

⁴⁰ Christine Dugas, "Visa Acts To Calm Fears of Identity Theft," *USA Today*, April 22, 2003. http://www.usatoday.com/money/perfi/credit/2003-04-22-visa-id-theft_x.htm.

⁴¹ *Ibid*, Dugas, 2003.

⁴² Donna Howell, "Firms Take Look At Cyberinsurance," *Investors Business Daily*, October 3, 2002. p. A6.

⁴³ Jon Swartz, "Firms' Hacking-Related Insurance Costs Soar," *USA Today*, http://www.usatoday.com/tech/news/computersecurity/2003-02-09-hacker_x.htm.

⁴⁴ "Most Companies Have Cyber-Risk Gaps in Their Insurance Coverage, States The I.I.I. -- Traditional Insurance Policies Not Adequate For Cyber Exposures," Press Release, Insurance Information Institute. August 13, 2003. <http://www.iii.org/media/updates/press.731722/>.

⁴⁵ See Brian Krebs, "White House Pushing Cybersecurity Insurance," *Washingtonpost.com*, June 27, 2002. http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&no_de=&contentId=A55719-2002Jun27¬Found=true.

⁴⁶ *Ibid*. Krebs, June 27, 2002, citing the Insurance Information Institute.

⁴⁷ Noted in Alex Salkever, "Can Software Security Be Certified?" *BusinessWeek Online*, October 1, 2002. http://www.businessweek.com/technology/content/oct2002/tc2002101_6896.htm.

⁴⁸ Bruce Schneier, "The Insurance Takeover," *Information Security*, February 2001. http://www.infosecuritymag.com/articles/february01/columns_sos.shtml.

⁴⁹ Testimony and Statement for the Record of Bruce Schneier, Chief Technical Officer,

Counterpane Internet Security, Inc., Hearing on Internet Security, Before the Subcommittee on Science, Technology, and Space of the Committee on Commerce, Science and Transportation, United States Senate, July 16, 2001. <http://commerce.senate.gov/hearings/071601Schneier.pdf>.

⁵⁰ The Qualys list of highest-risk vulnerabilities is at <http://www.qualys.com/services/threats/current.html>.

⁵¹ Mark Rasch, "This Firm Is Not Yet Rated," *Wired*, January 2004. p. 64-65. <http://www.wired.com/wired/archive/12.01/view.html?pg=1>.

⁵² This phenomenon of lack of adoption was noted in Louis Trager, "DHS Research Official Gives Silicon Valley View of Its Plans," *Washington Internet Daily*, August 1, 2003. p. 5.

⁵³ Michael Schrage, "We Can Trap More Crooks With a Net Full of Honey," *Washington Post*, January 11, 2004. p. B1. <http://www.washingtonpost.com/ac2/wp-dyn/A5056-2004Jan9?language=printer>.

⁵⁴ Examples given in D. Ian Hopper, "Tech Cos. Push Terror Legislation," *Associated Press*, July 10, 2002.

⁵⁵ Robert Block, "Shielding the Shield Makers," *Wall Street Journal*, November 26, 2003. p. B1. <http://online.wsj.com/article/0,,SB106981510038565500,00.html?mod=todays%5Fus%5Fmarketplace%5Fhs>.

⁵⁶ Press Release, U.S. Department of Homeland Security, "Safety Act Regulations Submitted for 30-Day Public Comment Periods," July 11, 2003. <http://www.dhs.gov/dhspublic/display?content=1073>. Coverage at Matthew Weinstock, "Rule Provides Liability Protection for Anti-Terror Technologies," *GovExec.com*, July 10, 2003. <http://www.govexec.com/dailyfed/0703/071003w1.htm>.

⁵⁷ Weinstock, 2003.

⁵⁸ Robert Block, "Shielding the Shield Makers," November 26, 2003. See also Opening Statement of Chairman Tom Davis, "Implementing the SAFETY Act: Advancing New Technologies for Homeland Security," House Committee on Government Reform. October 17, 2003. <http://reform.house.gov/UploadedFiles/TMD%20SAFETY%20Opener.pdf>. Other relevant testimony from this hearing chaired by Davis is available at <http://reform.house.gov/GovReform/News/DocumentSingle.aspx?DocumentID=1653>.

⁵⁹ Hopper, 2002.

⁶⁰ Bret Stohs, "Protecting the Homeland by Exemption: Why the Critical Infrastructure Information Act of 2002 Will Degrade the Freedom of Information Act," *Duke Law and Technology Review IBriefs*, September 20, 2002. <http://www.law.duke.edu/journals/dltr/articles/2002dltr0018.html>.

⁶¹ Patrick Ross, "Clarke Expected to Move Cybersecurity Plan Next Week," *Washington Internet Daily*, September 12, 2002. pp. 1-2.

⁶² William New, "The Ins and Outs of Homeland Security," *National Journal's Technology Daily*, August 12, 2002.

⁶³ Uriah Kriegel, "Prioritizing Security," *Tech Central Station*, August 25, 2003. <http://www.techcentralstation.com/1051/techwrapper.jsp?PID=1051-250&CID=1051-082503C>.

⁶⁴ William M. Lambert, MSA's North American president, quoted in Robert Block, "Shielding the Shield Makers," November 26, 2003.

⁶⁵ See Andrew Goodman, "Federal Government Sees Cyberinsurance as Way to Incentivize Private Sector," *Washington Internet Daily*, August 20, 2003. p. 1.

⁶⁶ Noted by Jenkins, October 2001.

⁶⁷ William Yurcik and David Doss, "Cyberinsurance: A Market Solution to Internet Security Market Failure." 2002. <http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/econws/53.pdf>

⁶⁸ Yurcik and Doss, 2002.

⁶⁹ Peter Svensson, "Spread of Buggy Software Raises Questions," *Associated Press*, April 27, 2003, <http://finance.lycos.com/home/news/story.asp?story=33972514>.

The Competitive Enterprise Institute is a non-profit public policy organization dedicated to the principles of free enterprise and limited government. We believe that consumers are best helped not by government regulation but by being allowed to make their own choices in a free marketplace. Since its founding in 1984, CEI has grown into an influential Washington institution.

We are nationally recognized as a leading voice on a broad range of regulatory issues ranging from environmental laws to antitrust policy to regulatory risk. CEI is not a traditional “think tank.” We frequently produce groundbreaking research on regulatory issues, but our work does not stop there. It is not enough to simply identify and articulate solutions to public policy problems; it is also necessary to defend and promote those solutions. For that reason, we are actively engaged in many phases of the public policy debate.

We reach out to the public and the media to ensure that our ideas are heard, work with policymakers to ensure that they are implemented and, when necessary, take our arguments to court to ensure the law is upheld. This “full service approach” to public policy makes us an effective and powerful force for economic freedom.



Competitive
Enterprise
Institute

1001 Connecticut Avenue, NW
Suite 1250
Washington, DC 20036
202-331-1010
Fax 202-331-0640
www.cei.org

Issue Analysis is a series of policy studies published by the Competitive Enterprise Institute. Nothing in *Issue Analysis* should be construed as necessarily reflecting the views of CEI or as an attempt to aid or hinder the passage of any bill before Congress. Contact CEI for reprint permission. Additional copies of *Issue Analysis* may be purchased through CEI's publications department (pubs@cei.org or 202-331-1010).