

Hacking the Business Climate for Network Security

Bruce Schneier, Counterpane Internet Security

Computer security is at a crossroads. It's failing regularly and with increasingly serious results. CEOs are starting to notice. When they finally get fed up, they'll demand improvements—either that or they'll abandon the Internet, which seems unlikely.

And they'll get the improvements they demand. Corporate America can be an enormously powerful motivator once it gets going.

This is why I believe computer security will eventually improve. I don't think the improvements will come in the short term or without considerable resistance, but I do think that corporate boardrooms—not computer science laboratories—will fuel the engine of improvement.

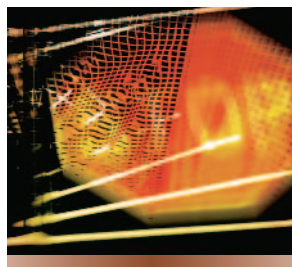
As such, the solutions won't have anything to do with technology. Real security improvement will only come through liability—holding software manufacturers accountable for the security and, more generally, the quality of their products.

This is an enormous change, and one the computer industry is not going to accept without a fight.

BUSINESS RISK MANAGEMENT

But I'm getting ahead of myself here. Let me explain why I think the concept of liability can solve the problem.

Computer security is not a problem that technology can solve. Security solu-



We need to change the economics of security, giving the businesses in the best position to fix the problem the motivation to do so.

tions have a technological component, but security is fundamentally a business problem. Companies approach security as they do any other business uncertainty—in terms of risk management. Organizations optimize their activities as a cost-risk ratio. Understanding these motivations is key to understanding the state of computer security today.

It makes no sense to spend more on security than the original cost of the problem, just as it makes no sense to pay liability damages when spending money on security is cheaper. Businesses look for financial sweet spots—adequate security at a reasonable cost, for example—and if a security solution doesn't make business sense, a company won't implement it.

This way of thinking about security explains some otherwise puzzling security realities. For example, historically, most organizations haven't spent a lot of money on network security. Why? Because the development and implementation costs are significant: time, expense, reduced functionality, frus-

trated end users. On the other hand, the costs of ignoring security and getting hacked have been—in the larger scheme of things—relatively small. We in the computer security field like to think they're enormous, but they haven't really affected company bottom lines.

From the CEO's perspective, the risks include the possibility of bad press, network downtime, and angry customers—none of which is permanent. There's also some regulatory pressure from audits or lawsuits, which adds to costs, but on balance a smart organization does what everyone else does—and no more.

Things are changing—slowly, but they're changing. The risks are increasing and, as a result, so is the spending.

PRODUCTION ECONOMICS

This same kind of economic reasoning explains why software vendors spend so little effort securing their products. We in computer security tend to think the vendors are all a bunch of fools, but they're behaving completely rationally from their own point of view.

Adding good security to software products incurs essentially the same costs as increasing network security—large expenditures, reduced functionality, delayed product releases, annoyed users, while the costs of ignoring security are minor—occasional bad press and maybe some users switching to competitors' products.

Microsoft does not bear the financial losses to industry worldwide due to vulnerabilities in the Windows operating system, so Microsoft doesn't have the financial incentive to fix them. If the CEO of a major software com-

pany told the board of directors that he would be cutting the company's earnings per share by one-third because he was going to address security really seriously—no more pretending—the board would fire him. If I were on the board, I would fire him. Any smart software vendor will talk big about security but do as little as possible, because that's what makes the most economic sense.

Think about why firewalls succeeded in the marketplace. It's not because they're effective. Most firewalls are configured so poorly that they barely work, and technology offers other more effective security solutions, such as e-mail encryption, that have never seen widespread deployment.

Firewalls are ubiquitous because corporate auditors started demanding them. This changed the cost equation for businesses. The cost of adding a firewall includes the purchase, installation, and maintenance expenses as well as user annoyance, but the cost of not having a firewall is failing an audit.

Even worse, a company without a firewall could be accused of not following industry best practices in a lawsuit. The result: Companies have firewalls all over their networks, whether they do any actual good or not.

A BUSINESS SOLUTION

As scientists, we are awash in security technologies. We know how to build more secure operating systems, access-control systems, and networks.

To be sure, there are still technological problems, and research continues. But in the real world, network security is a business problem. The only way to fix it is to concentrate on business motivations. We need to change the economic costs and benefits of security. We need to make the organizations in the best position to fix the problem *want* to fix it.

To do that, I have a three-step program. None of the steps has anything to do with technology; they all have to do with businesses, economics, and people.

Step 1: Enforce liabilities

This is essential. Vendors currently suffer no real consequences for producing software with poor security features. In economic terms, the costs of low-quality security are an *externality*—a decision's cost that is borne by people other than those making the decision.

Even worse, the marketplace often rewards low-quality software. More precisely, it rewards new features and timely release dates, even if they come at the expense of quality.

Rational liability changes everything.

If we expect software vendors to reduce the number of features, lengthen development cycles, and invest in secure software development processes, they must be liable for security vulnerabilities in their products. If we expect CEOs to spend significant resources on their companies' network security, they must be liable for mishandling their customers' data. Basically, we have to tweak the risk equation so the CEO cares about actually fixing the problem. Putting pressure on the balance sheet is the best way to do that.

This could happen in several different ways. Legislatures could impose liability on the computer industry by forcing software manufacturers to live with the same product liability laws that affect other industries. If software manufacturers produce a defective product, they should be liable for damages.

Even without this legislative imperative, courts could start imposing liability-like penalties on software manufacturers and users. In fact, this is starting to happen. A US judge forced the Department of Interior to take its network offline because it couldn't guarantee the safety of American Indian data entrusted to it. Several companies have been penalized for using customer data in violation of privacy promises or for collecting data through misrepresentation or fraud. Judges have issued

restraining orders against companies with insecure networks that cybercriminals use as conduits for attacks.

Alternatively, the industry could get together and define its own liability standards.

Clearly this isn't an all-or-nothing issue. A typical software attack involves many parties: the company that sold the software with the vulnerability in the first place; the person who wrote the attack tool; the attacker who used the tool to break into a network; and the network owner, who was entrusted with defending that network.

One hundred percent of the liability shouldn't fall on the software vendor. Nor should 100 percent fall on the network owner, as it does today.

However it happens, rational liability changes everything. Currently, a software company has no economic reason to refrain from offering more features, more complexity, more versions. Liability forces software companies to think twice before changing something. Liability forces companies to protect the data entrusted to them.

Step 2: Allow parties to transfer liabilities

Once liability forces CEOs to care about security, they will turn to insurance companies for help. Insurance companies are in the business of liability transfer. From a CEO's perspective, insurance turns variable-cost risks into fixed-cost expenses, and CEOs like fixed-cost expenses because they can budget them.

Insurance companies are not stupid. They're going to move into cyberinsurance in a big way. And when they do, they're going to drive the computer security industry—just as they drive the security industry in the brick-and-mortar world.

CEOs don't buy security for company warehouses—strong locks, window bars, or an alarm system—because it makes them feel safe. They buy it because company insurance rates go down. The same thing will hold true for computer security. Once insurance

companies are writing enough policies, they will start charging different premiums for different security levels.

Even without legislated liability, CEOs will start noticing how their insurance rates change. And once they start buying security products on the basis of insurance premiums, the insurance industry will wield enormous power in the marketplace, determining which security products are ubiquitous and which are ignored.

The insurance companies will pay for actual losses, so they have a great incentive to be rational about risk analysis and security product effectiveness. This is different from a bunch of auditors deciding that firewalls are important. Insurance companies will have a financial incentive to get it right. They will demand real results.

And software companies will respond, increasing their products' security to make them competitive in this new "cost plus insurance cost" world.

Step 3: Provide mechanisms to reduce risk

Once insurance companies start demanding real product security, the computer industry will undergo a sea change. Insurance companies will reward companies that provide real security and punish companies that don't. This reward system will be entirely market driven. Security will improve because the insurance industry will push for improvements, just as it has in fire, electrical, and automobile safety as well as in banking and other industry security mechanisms.

Moreover, insurance companies will want security implemented in standard models that help them build pricing policies. Insuring a network that changes every month or a product that is updated every few months will be much harder than insuring a product that never changes. The computer field naturally changes quickly, which makes it different to some extent from other insurance-driven industries. Insurance companies will nevertheless look to security processes that they can rely on.

Actually, this isn't a three-step program. It's a one-step program with two inevitable consequences. Enforce liability, and everything else will flow from it.

Much of Internet security is a *commons*—an area used by a community as a whole. In our society, we protect our commons—environment, working conditions, food and drug production, accounting practices—through laws that punish those companies that exploit them unscrupulously. This kind of thinking is what gives us bridges that don't collapse, clean air and water, and sanitary restaurants. Further, we don't live in a "buyer beware" society; we hold companies liable when they take advantage of buyers.

There's no reason to treat software any different from other products. Today, Firestone can produce a tire with a single systemic flaw and they're liable, but Microsoft can produce an operating system with systemic flaws discovered every week and not be liable. Today, if a home builder sells you a house with hidden flaws that make it easier for burglars to break in, you can sue the home builder; if a software company sells you a software system with the same problem, you're stuck with the damages.

This makes no sense, and it's the primary reason security is so bad today. I have a lot of faith in the marketplace and in human ingenuity. Give the companies in the best position to fix the problem a financial incentive to fix the problem, and fix it they will. ■

Bruce Schneier is CTO of Counterpane Internet Security, Inc., and author of Beyond Fear: Thinking Sensibly About Security in an Uncertain World (Copernicus Books, 2003). Contact him at schneier@counterpane.com.

**Editor: William A. Arbaugh, Dept.
of Computer Science, University of
Maryland at College Park;
waa@cs.umd.edu**