

Time for Change

Imagine a perfect world, where things only changed when you wanted. We could analyze current threats and implement security countermeasures, taking our time to test them thoroughly. When we were satisfied these solutions took care of the problem, we would implement them, and then relax. We would be confident that our organizations were perfectly secure and nothing bad would happen.

Like the commercial says, we don't live anywhere near "Perfect." We are barraged with new threats every day, and vendors struggle to meet crisis after crisis. The bulk of my email are alerts covering the full range of current technologies. An overwhelming amount of them are critical. Our operations technicians are diverted daily from their maintenance and enhancement tasks to implement product patches, and are lucky if they can keep up. In their rush to plug these holes, patches are applied without proper evaluation and testing. Even well tested patches can cause unexpected problems, and some companies simply opt to ignore the barrage in an effort to push forward with business. This is a dangerous game we're playing, and it gets more dangerous every day.

One major company I know had several hundred backlogged patches sitting in the queue. Is this a bad thing? Maybe not.

Companies that choose to ignore patches without qualifying them are simply irresponsible. But if patches are carefully evaluated against potential risks, and informed judgments are made about them, then the company is not remiss in its due care/due diligence duties. They are being smart.

Good security depends almost entirely on good judgment. A company may use Microsoft technologies, but opt to not use the native SQL Server or its services in its environment. Should the company apply an OS patch related to SQL Server? Maybe, maybe not. These are judgment calls that if properly investigated, could result in reasonable deferral of a recommended patch.

The investigation part is paramount. Companies must have a fast way to determine if a recommended patch is relevant—and if relevant, how relevant. Not every patch is mission critical to every company. It could be very relevant, and very necessary. It could be very relevant, but potentially highly disruptive to business. And it could be completely nonessential. The Patch process must include procedures for evaluating and prioritizing patches as they relate to the specific infrastructure. And that's where the hard part is.

Let's expand our thinking a little, beyond patches. In a perfect world, we could be completely secure as long as nothing inside or outside our environments change. But we know that things are always changing. New business requirements demand adjustments to existing infrastructure, implementation of new vendor and custom solutions, and business function transition and retirement, from time to time. On the outside, sophisticated hackers who want to do real damage to our companies and customers are

constantly coming up with new ways to challenge us. Instead of existing in “perfect” we exist in a state of perpetual chaos, operating in reactive, rather than control mode. Like rats in a maze, we are constantly being tested, scurrying from one solution to another, rather than stepping back to see the big picture, which would reveal the futility of this approach and what really needs to be done.

We think we are doing the best we can, but we are really just reinventing the wheel every day. We look to security standards and best practices for guidance, thinking these will push us a little farther along. However, taken literally, these recommendations can become a hindrance rather than a help, diverting us from the real tasks we know need to be accomplished, that should have been accomplished long ago. We need to measure and weigh business risks imposed by technology.

You can't measure if you have no baseline. Without a baseline you can't see what has changed or how. A technology baseline is derived from inventorying the elements of your technology environment. The problem is, changes are made in your environment daily. You add new technology, take some away, or change its configuration. New computers come on line everyday, while others drop out. You add new personnel, shift them around, and maybe fire some. You provide remote login capabilities to workers who are suddenly sick, on leave, or working at regional offices. You launch new custom projects, create isolated test environments, and tear them down when the project is done. And all the while you're deploying product patches, patches, and more patches. Your inventory is out of date the day after you start documenting it.

OK. Can't crack that nut. So instead you try to impose structure from the outside, defining policies that govern the parameters within which these tasks should be done. Procedures are written, distributed, and even sometimes followed. You launch security awareness programs, fund security training and follow a managed process for each and every one of these tasks. This is the best you think you can do. So why aren't things getting better.

It's because it's about the technology, stupid! Imposing structure from the outside won't solve the basic problem. The number of flaws in a program is essentially infinite. Look hard enough and you'll find more. When you think you've found them all, then tomorrow your environment changes or new external threats emerge exposing others. We can't win this game.

We can't win this game because in every case we are trying to address dynamic problems with static solutions. Today's secure software will be tomorrow's software problem. Today's secure code, becomes the basis for tomorrow's hacks. Today's policies and procedures will be insufficient for tomorrow's security environment. Our attempt to define static solutions to keep up with an infinite number of dynamic problems is draining our budgets, our businesses, and our convictions.

If, instead, we approach the problem as rational human being, we would conclude that yes, we cannot win this game. In a game you cannot win, you have only one recourse: change the rules.

Bruce Schneier is probably the brightest light in information security today. He gets it. There is nothing new under the sun. The problem of security is millennia old, and those related to technology share striking similarities with those of the ages. The objectives are the same, the mitigation approaches are the same, and the solutions are the same. He points out that probably the most debilitating aspect of technology security is not hackers, or criminals or terrorists. It is fear.

Fear paralyzes us from thinking rationally about our problems. Fear raises tensions, causes us to react without thinking, causes us to lash out and put blame anywhere else but on ourselves. Fear is what's killing us.

Knowledge is the best defense for fear. If you are grounded, have a complete understanding of your business objectives and technology environment, of your problems, what they affect, and how great their impact could be, then you can successfully overcome security fear.

So let's imagine we have that knowledge. Now, step back and look at the big picture. What is really the greatest threat to you business? Is it hackers? Uninformed users? Dishonest employees? Criminals? Terrorists? Regulatory mandates? Vendor updates? No. There is a constant threat we all grapple with every day, and it dwarfs all of these. It's called "change."

Like I said, if what is inside and outside our organizations never changed, we'd be able to achieve a secure state and sit back and relax, completely confident that we were optimally safe. The fact that things change is the greatest obstacle to security. By attacking every threat except that of change, we miss the greatest opportunity for securing our organizations. It's what will give us the biggest bang for the buck. We already know we can't beat the hackers. They will always find new ways to hit us. We also know our employees and customers won't always do the right thing, despite how much we spend on security awareness and training. Most companies, however, already have mechanisms in place to assess and manage business risk. Why can't such mechanisms be applied to technology risk as well? Is security really so mystifying a thing that it requires a whole new enterprise process? Is there really no relationship between security risk and that of quality assurance, business continuity and capacity planning? I don't think so.

Not recognizing security as a business risk, not treating it as one of a number of other risks that must be constantly re-evaluated, prioritized and addressed, is the reason most companies are failing at security. Sorry, to do so requires that you do actually "crack that nut" and have as good an idea as possible of what your environment looks like, what it contains and how it functions, and at what priority level these functions support the business for that brief slice of time during which security decisions must be made. Executives need to be handed a risk assessment that is assembled on the spot, giving

them a clear understanding what business functions are affected, how critical they are to productivity, of the costs and benefits of security solutions, and the potential risk impacts, quantified in estimated dollars and cents *at this exact point in time* in order to be able to make informed decisions about security, from the standpoint of control rather than fear..

To deliver this, we need a way to assemble an inventory list on the spot, isolating those systems affected by a security problem. Their business functions must be prioritized and their relationship to other interfaced systems must be clear. Their value to the business must be estimated, and the cost of potential disruptions must be represented. Armed with this knowledge, managers can make informed decisions as to whether to proceed with investment (which might be as little as authorizing a patch, or as high as buying a new security appliance). They can then decide, based on knowledge, to either accept the risk, or to go ahead with the solution.

When we finally shift from static to dynamic mode, from reactive to control mode and address technology change control in business context is when the fear will dissipate and we'll start living comfortably in the real world, instead of trying to stave it off.

Bar Biszick-Lockwood is CEO of QualityIT, an IT quality and security solutions organizations that solves business and security problems using proven quality assurance methods. She is a Certified Software Quality Analyst (CSQA), a Certified Information Systems Security Professional (CISSP), and a Certified Information Security Auditor (CISA). Ms. Biszick-Lockwood recently led an Information Security Assurance team that is recommending changes that would elevate the visibility and priority of security activities in IEEE's foundation P1074 *Standard for Developing Software Life Cycle Processes* standard. She is a member of IEEE, ISSA and ISACA, and is also on the curriculum writing staff of Logical Security, a security education company led by Shon Harris, author of McGraw-Hill's best selling CISSP *All-In-One-Guide*. She can be reached at barbis@qualityit.net. Or visit her website at www.qualityit.net