Security still underfunded

Kelly Martin,

Blackhat is one of my favorite places to do some casual online banking over an insecure WiFi connection. Where's the risk, right? All joking aside, Blackhat is in fact a great place to do some deep thought on the current state of the security industry.

Yes, the industry has grown a great deal and many things are now big. There's big money and big players, but most of all there are still big vulnerabilities and exploits -- some of which easily dwarf the immense amount of time and effort that is being used to combat them. Are we making any progress at all? I'm not so sure.

It's money that matters

Many of the Blackhat presenters work as researchers for small, independent security companies. As more and more money pours into the industry, smaller companies get bought by larger players. During any buyout, individuals are enticed to remain with the company using financial incentives -- which works to some extent. Despite all this, research into new vulnerabilities and attack vectors continue, individuals leave organizations and move on.

Sometimes, the more profound research presented at Blackhat has quite the opposite effect than it should have. Case in point: Michael Lynn and his now-famous Cisco IOS presentation, given to an eager audience in a Blackhat presentation room that was barely half-full. I enjoyed his demonstration. But let's see... what is the best approach to thwart the work of a security researcher: threaten him with lawsuits to keep him quiet, or offer him a job and large sums of money to have him on your side and improve your company's product offering and security?

Big risks

Companies and governments secure their networks because they have massive financial resources, intellectual property and assets that need protection. Security for most companies, particularly the Fortune 100, does not exist in a vacuum -- most do something other than make hardware or software for their customers. Spending on security is up dramatically over where it was five years ago, but it's still much lower than it needs to be. Why? Because we're losing the battle.

I have always enjoyed the analogy of the guy who owns an expensive car like a Porsche, yet keeps it secure in a garage with a door lock that's barely worth $100. If the threat of the lock being broken so the car gets towed away in the middle of the night is high enough, how much should he spend on a lock? A thousand dollars? Ten thousand?

With so much money pouring into the security industry, I think the major players need to focus much more on hiring brainpower, and pay people who are in the know some exorbitant sums of money to think of new ways of doing things. The reason? If an unemployed security researcher already has the ability to gain the keys to your kingdom anyway, it's little more than his ethics and morals that keep him or her from going through the door illegally, and slipping inside.

Michael Lynn quit his job and risked two personal lawsuits, one from his former employer and one from Cisco, because he believed what he discovered was that important. And it is. He seemed to believe there was no choice in the matter; what he

discovered had to be made public. What is the value of this discovery to Cisco, a highly respected company with oodles of cash, a near monopoly in the Internet's core infrastructure, and a market cap of $125 Billion?

It's all about ethics

Most discussions of ethics tend to result in glassy eyes and yawns from those involved, so I'll keep this brief. The fact is there's little else preventing many researchers from going to the dark side, and slicing off tiny bits of the fortunes of the Fortune 100, bit-by-bit.

Michael Lynn could have taken the easy road and kept quiet, or even used what he found to own the edge routers of some of the largest companies in the world. It's an excellent way to slip inside. He has stated very times tht he disassembled Cisco's software, apparently under ISS' direction, which undoubtedly violates Cisco's license agreement. That's probably wrong. But the Cisco source code has been stolen two times now, and those criminals who have it now very much have an upper hand. That is much worse. Lynn did nothing more than any other security researcher or academic with strong ethics would do: he published his findings and presented them to the world.

Hire someone complex

Complexity is all around us, more than ever before -- and yet some very smart people can still slip in and out of the world's most secure servers and workstations with ease. Other smart people know about this, and plead with their managers to do something about it. People most in the know too often have the least amount of power to do anything. In fact, the tables should be turned.

The largest computer companies like Cisco, Oracle, Google, Symantec and Microsoft should try a little harder to proactively hire smart, independent security people, protect themselves, and then use the assimilated brainpower to develop products and services that earn enormous sums of money for their organization. Google and Microsoft are already well-known for doing this, but there's still room for much more. Particularly those people who can demonstrate that they have strong ethics and morals should be on that list. Still don't see the threat?

The Cisco routers that hold up your company's infrastructure may already be under someone else's control. A generation four Windows rootkit could lead to a pot of gold -- and might remain undetected for years. Rest assured that all those unpatched Oracle hacks could lead to another ten pots of gold, among the jewels of your enterprise's database. A Symantec security gateway turned into its evil twin could really hurt detection efforts, and give you a false sense of security to boot. Even after a stealthy intrusion is one day discovered, and the FBI or Interpol are brought in, the very forensic tools they use can be turned against them, with an electronic time bomb that explodes when specific forensic tools are used. There is no safe haven in the security world, only risk mitigation and one's hope for the best.

The brain-drain

I enjoy reading people complain about brain-drain, as if we all work for some altruistic reason that is completely absent from any financial gain. Get with it, this is business. Double my salary and offer me a position higher up in your organization, and I'd be the first one to leave. It's not brain-drain, it's common sense.

Of course, this is all oversimplified, and no one in the security industry wants to focus

on the simple things. We all enjoy the fact that security is growing evermore complex; it drives us to do what we do, and it pays the bills. But the financial incentives on both sides of the fence is growing, and the payouts are increasingly great. Companies need to spend more money on security, protecting those billions in profits using the greatest resource that is available: hiring smart people. Without them, all those expensive security products will go to waste.