

The Broken: Assessing Corporate Security in 2012 to Make a Better 2013

by Paul Jaramillo, CISSP, EnCE

So as we are about to close out 2012, many of us in the IT Security community look around and try to assess where we were, what we have accomplished this year, and what is next. I've been working in IT since the late 90s with a focus on security for much of that time. Most of my work has been in large private-sector companies with a brief but very rewarding stint working for the government. To me while much has changed, many of the core issues remain today as they were back then. Our security condition has actually worsened in many cases. While that is up for debate, no one can argue the pace, sophistication, and impact of major cyber events related to nation-sponsored, organized crime. Hacktivism threats have increased exponentially in the last 4-5 years as well. This new normal has been applicable to the government and defense industrial base for a long time but really surfaced in the private sector around 2007. You would assume that with all that increased attention, dollars and executive support at the highest levels, it would be making things happen. To a certain extent they are, but we as an industry are still losing in the never-ending cat and mouse game with our adversaries. Why?

Over the years, I have sat through countless "you're doing it wrong" or "we're screwed" type of presentations. Some of them were very informative, and I absolutely respect anyone that publicly voices their opinions and ideas, knowing they will be criticized and nitpicked for things taken out of context. However, I often leaving conferences with a desire for a way to fix what we all know has been broken. So what is stopping us? That is where I would like to focus some energy. What are the key road blocks and stumbling points that are keeping the security industry from truly raising the bar as opposed to being stuck in a continual state of catch up?

The ideas that follow are not all my own, and I'm sure I have subconsciously absorbed them or unknowingly added them to my mantra. I have a set of wise men that I learn from constantly, however I won't list them out or directly associate them to this article out of respect. These ideas shouldn't be taken as a statement of fact either, as they are only my humble opinions. My goal is to start a real discussion and starting point for documenting and overcoming our greatest challenges to our broken system.

Discuss in Forums {mos_smf_discuss:Opinions}

Preamble

First off, any high level discussion that focuses on technical solutions is inherently flawed. That is the equivalent of trying to fix and improve the Maginot Line. To paraphrase the Matrix, "You've been down that road, you know that road, and you know exactly where it ends." We shouldn't be looking for point solutions, because just as you achieve them, the game changes. If we can all agree to "take the red pill," we can start addressing the behavioral issues and misconceptions that are keeping us in a reality distortion field.

In no particular order, here we go:

Obstacle 1: No Incentive or Penalty for Correctly Managing IT Security Risk

How many times have you had a business leader accept an enormous, unmitigated risk, despite the misgivings of their security department? I agree that security should not disrupt any business revenue generating activities; however, at a certain point the risk sometimes actually outweighs the profit. There are many factors that contribute to this behavior.

The most talked about issue is the fact that technical security people often don't correctly describe the risk in business terms. There absolutely is a need to have the right people who can translate the lack of encryption or the outsourcing of critical applications into what that may mean in business terms. So let's say, we are already doing that. That is a big if, I know.

The next challenge we have is a short-term fiscal quarter mentality that most c-levels have. They are incentivized to deliver results quarterly or annually to meet their bonus potential. By the time this risk they have accepted goes south; they have cashed the bonus check and may have been promoted into a different role or left the company all together. One thing is clear though, short term strategy rules the day. Hmm, just maybe the Chinese are right about one thing (See 5 year plan). I don't see an easy way to incentivize something that may take years to play out.

For me the most direct solution is available by modeling what you see implemented in the sports, legal and medical professions. Sometimes a pro athlete for a number of reasons creates a situation where they have violated the terms of their contract and their bonuses are subject to forfeiture. Imagine a world, where a senior leader that accepts a risk and then is found to have been negligent. That bonus achieved by cutting security corners should be returned even if they have left the company. I'm not sure if this was ever implemented, but I think this line of thought was discussed for SOX and FINRA regulation for CEOs that sign off on financial results. Similar to medical boards and the Bar association, that failure should be recorded and follow them throughout their career. For example, if you choose to put M&A or Intellectual Property data in a 3rd party cloud despite documented warnings, then all your future employers should know that. I'm not saying this would be easy to achieve or likely, but it would definitely modify behaviors. It's also right to consider, that this might swing the pendulum too far to where we become too risk adverse.

Obstacle 2 – Field Validated Results Uber Alles

At the business level, the ultimate driver is audit compliance and the potential for fines by a governing body. Due to the punitive nature of the compliance racket, it makes perfect sense that this always stays high on the radar. What clearly needs to change is the thought that IT Security compliance somehow equates to real world security. It doesn't and almost never has.

Some of the guidance provided by regulations and standards contain very reasonable controls. However, much of it (particularly FISMA) is creating a massive amount of overhead that actually detracts from improving security. Pro Tip: Stop funding auditing if you're not funding the actually fixing of the findings. I feel for the people placed in the horrible spot of having to write a single snapshot in time and create documentation to cover every possible deployment or IT environment imaginable. It's a losing proposition by any measure. You can't be all things to everyone all the time, unless your deity.

What is lacking is the concept of field validated results correlated with threats to drive your overall security strategy above all else. This has been discussed by many people and nobody with experience really disagrees with this. My suggestion is not to eliminate but rather lessen the importance of static, one-size fits all IT compliance. What should really be audited is the results of your incidents & pen tests and specifically whether or not you have closed the gap. Kevin Mandia used the term "Attack the Gap" recently. That couldn't be timelier. One of your primary jobs as an information security professional is ultimately reduce your attack surface. And to do that properly you have to have to know what the most exploitable points in your environment are to real threats, not outdated security guidelines.

Obstacle 3 – IT Security is a Competitive Advantage

Now that more stories are becoming public about companies literally getting hacked out of business, this strategy becomes easier to sell. I think its commonplace for leaders in non-tech industries to view IT as a cost center and not something that drives profits. I believe in the majority of cases this is not true. Nevertheless, a Fortune 100 company in my town actually told their IT workers that they don't value IT and to look for work elsewhere if you want to be valued. Wow! Well the guy who delivered that message is a straight shooter with upper-management written all over him.

If you're reading this right now, chances are you will agree that information and the speed with which you can analyze and act on it is a competitive advantage. Hence the availability, integrity, and confidentiality of that information are also an advantage. (CISSP credits ;-)). There is no leap in logic here. So what is lacking is getting c-level leadership to understand this. We have to sell this better. We have to speak in business terms. We have to make a well defined, quantitative, business plan as to how this makes the company better. Every day your company is either getting stronger or weaker in the marketplace. Each and every choice has a direct correlation to your bottom line. If you suffer brand damage, loss of intellectual property, or a complete business disruption and your competitor doesn't, guess who wins?

Obstacle 4 – Talent Gap from the Keyboard to the Boardroom

DHS needs 2000 Cyber Warriors in the next 5 years! The lack of IT security skills has been covered ad nauseum by the tech media. This is a real issue, but it's easier to fix than one would think. But I'm not going to discuss the key skills we need from DFIR people, which is another great discussion. Where I see this biggest deficit of talent is in the CISO/Director level security positions. I won't say that to be great at this role you have to have been a skilled technical person, because I don't believe that to be true. Certainly that is desired and helps, but it's hard to detail a prototypical background. I've definitely seen people come out of the DoD or other 3-letter agencies with the perfect resume and fall completely on their face.

To be honest, I'm not the best person to outline this problem, because I've spent more time at the keyboard than I have in meetings with c-levels. I just know a problem when I see it. It has impacted me personally on multiple occasions. My biggest issue is that you don't want someone in this role who is trying to climb the ladder or use it as a stepping stone. You have to be willing to put your career on the line and say ‘no’ to the people in power. If you can't do that, and you're more of a ‘yes’ man, then I beg of you… get into marketing, HR, finance, or some other part of the company. If you don't have a track record of rocking the boat and want to merely coast until your retirement, please step aside. You also at the same time need to be an astute politician, because having great success or striving for greatness often brings up a myriad of consequences.

Clearly for me though, the biggest required skill goes back to being able to show in understandable business terms the risks associated with not establishing or improving IT security. These people also need copious amounts of patience and a strong passion for security. If you can get one of these people, keep them happy. They are in very high demand and in short supply. People want to work for these types of leaders, and you will likely reap many rewards.

Obstacle 5 – IT Agility for Security

What is the number one reason that high performers leave for another job? Is it money? What about power? I can't say I have an answer for this, and everyone is different on their expectations for a job. I can say that the type of people with whom I like to work are problem solvers and enthusiastic about at least one aspect of IT or IT security. What I tend to see a lot is people leaving, because they are either pigeonholed into one area or have a sense of frustration because they can't accomplish what they want to.

It's very common for an IT organization to resist and delay changes that support security, because IT objectives are at odds with IT Security objectives (and in turn may be at odds with business objectives). That's not the only reason of course, but it's a reoccurring theme where people are fighting a slow moving process to make change

happen. This could be something as simple as instrumenting your network, collecting logs, or even product selection. At best it puts you further behind the curve, and at worst it halts progress altogether.

My proposal is to fast track all security related projects. Yes beat me with a stick now, as I know this is totally unrealistic. That doesn't stop me from selfishly wanting this. I firmly believe that turnover in your security department would come down, if we simply move quicker on security projects. I also believe that these delays often take so long that by the time a given changes is operationalized, it's no longer cutting-edge and attackers have already circumvented it. We need to become more agile and responsive as a whole, and I think there is consensus for that. How we get there is still an unanswered question.

Conclusion

So there you have it. My Top 5 suggestions to raise the bar in security and actually end the year being more secure than the year before. In case you're wondering, number 6 would have been Applied Threat Intelligence. I am hoping for some more maturity in this space and to make people understand that it's not simply paying for a 3rd party threat feed. I think if we can eject the vendors and the Gartners of the world from our strategy process, things will start to improve.

My message is stop following the crowd and start doing the hard work of building a security program that is right for your business, a program that is cognizant of the behaviors mentioned above; a program that not only enables the business, but is accountable to the business; a program that rewards and develops security talent. In short, organizations of all shapes and sizes need a program that its own employees can be proud of. Although it's broken, it's not hopeless. Let's do this.

Editor's Note: This opinion piece is meant to spark debate. Click on the cartoon bubble at the top of the article to join the conversation in the EH-Net Community Forums. Don't be shy... shy your experiences, show Paul where he went wrong, validate his thoughts, what do you plan to do in 2013... Participation on EH-Net pays. ;-)

Paul Jaramillo, aka DFIR_Janitor, has spent the last 15 years working in the IT industry, most recently focused on managing an incident response team for a Fortune 150 company. Paul has also spent time working various security roles in the telecommunications industry and for the Department of Energy. He currently spends most of his time finding evil and enjoys any day where he can eject an adversary from the network. Paul is a proud father, husband, movie buff, and sports fan. Paul is a graduate of the University of Oklahoma and holds CISSP and EnCE certifications.