

To Tell the Truth: Why Vendor Hype Benefits No One

By Diana Kelley

Introduction

Software and technology vendors, especially those in the United States, have gotten into the habit of overselling the capabilities of their products in an effort to close deals. While this is an annoying practice for non-security related products, it can be downright dangerous when it's applied to the products that enterprises rely on to protect their assets. The issue is so serious that the government has stepped in. On August 8, 2002 the FTC ruled that Microsoft had misstated the security of their Passport product. Timothy Muris, FTC Chairman said, "Privacy and security promises must be kept. It's good business. It's the law, and we'll take action against companies that do not keep their promises."¹

Security vendors that overstate the ability of their solutions can lead to enterprises installing inferior systems that don't work as advertised. And the use of inferior products can translate into security vulnerabilities and costly exploits and attacks. How bad can it get? Well, in an extreme case, let's take a security vendor that sells an IDS (Intrusion Detection System) that is purported to warn of any serious attack to the enterprise. What if the 'enterprise' was the United States Government's defense network? What if it were the network used to direct air traffic? And what if the product failed to work as promised? As you can imagine, the consequences of technology that doesn't work as advertised can be great indeed.

While many vendors may indulge in hype hoping to increase sales, this is a shortsighted approach that's doomed to failure. Buyers aren't foolish. They know that no product can provide "bullet proof" protection. Yet vendors persist in perpetuating the hype.

Why do they do it?

The reasons that vendors overstate are as numerous as the vendors themselves, but there are a few recurring themes.

1. People Unclear on the Concept of What the Product Really Does

The marketing team gets a lot of grief and often the lion's share of the blame for product hyperbole. I was on the phone the other day being briefed by a security company touting a new, proactive security solution. The CTO of this company had been quite high up at another security vendor. The CTO explained why the new company was providing a previously undelivered innovative solution. After listening to the message for a while, I asked: "didn't your last company claim to do exactly this almost three years ago?"

The CTO responded that yes it had, but that it was only a marketing claim; the technical group didn't have any say over what the marketing people released. In other words, the marketing team had claimed something that the technical group didn't stand by.

Diana Kelley leads the Security practice at Baroudi Group. She has been working professionally for over 12 years creating secure network architectures and secure online business solutions for large corporations. Prior to joining Baroudi Group, she was the Vice President of SecurityTechnology for Safewww, Inc. She served as the General Manager of a development group at Symantec Corp and was Vice President of Corporate Development for LockStar. Kelley was the Senior Security Analyst for Hurwitz Group, and served as a Manager in KPMG's Financial Services Consulting practice, where her clients included Bank of America, General Electric, Merrill Lynch, MetLife and The Travelers.

Baroudi Group is an exclusive group of top-tier industry experts providing research, analysis, as well as strategic and tactical advisory services related to transforming and emerging technologies.

While it's convenient for vendors to blame marketing for the hype, it's a gross abandonment of responsibility. Everyone on the C-team is responsible for the messages going out about a product and it's technical capability. Marketing and sales folks need the technical and product management personnel to help them craft reasonable and truthfully realistic collateral. Anything less is inexcusable.

2. Confusing "Total" Security with Realistic Risk Management

Security implies that something, such as a network or an application or a server, is secure. While that's a great goal the reality is that companies need to employ risk management techniques to bring their risk down to an acceptable level. In the real world, and especially on the Internet, there is no such thing as "Total" Security.

Companies that want a single product or a product suite to give them total protection need to get over their illusions. And vendors that feed into this illusion may sell a few products but will be soon placed on the shelf and viewed as failures.

3. Rushing to Market

These are difficult times for many vendors and the market wants solutions that are released quickly. Unfortunately this can translate to the release of products, with known operational deficiencies, such as bugs and design flaws. While any and all products should come with a set of release notes and known vulnerabilities this is critical for security vendors because it allows the customer for be "forewarned" and "forearmed". It also saves the vendor from a potentially embarrassing situation where a vulnerability that was known is released to the general public. The bad publicity and lack of customer trust that can result from such an incident can be extremely damaging to a vendor.

Also common is when a previously known vulnerability in another product is overlooked in an existing piece of software. Just recently a flaw was discovered in Symantec firewalls that leaves companies vulnerable due to predictable Initial Sequence Numbers (ISNs)². Because of the flaw, it is possible for attackers to predict what the next number in the sequence will be and hijack the session to gain entry to the internal network protected by the firewall. While this is a newly reported vulnerability in the Symantec firewall line it is not a new vulnerability. Microsoft's NT 4.0 was found to have the same flaw in 1999 for that it declared publicly and issued a Service Pack patch for.³

4. Wishful Thinking

A corollary to the 'unclear on the concept' issue is the incoherence of thought that results from wishful thinking. In this case a vendor has become

so intoxicated by the possibilities of their solution that they come to believe that it is indeed the answer to all (or almost all) of the world's computer security ills. A terrific example of this syndrome was seen when PKI first hit the commercial market in the mid-90s. PKI vendors like Entrust claimed it would be the one thing needed to make the Internet secure. These vendors felt that there was no security problem that could not be solved with PKI.

Nothing could have been further from the truth. PKI was at best an expensive solution to a limited problem and at worst, in certain implementations, even less secure than plain old usernames and passwords. Failure to present the real business value (and cost) of these products arguably ruined companies that were not able to expand their solution offerings fast enough. When Baltimore failed to morph beyond PKI they saw their stock delisted, and VeriSign and Entrust had to abandon their PKI-centric business models in order to survive.

5. Willful Deceit

While the previous two hype holes are often results of 'honest mistakes', this one sure isn't. There are some vendors who are simply slimy and have no compunction whatsoever about overselling their product. This kind of trickery is often referred to as selling snake oil. Blatant deception only works in the very short term. As soon as reality rears its ugly head, buyers and investors will run, and fast – just think about how quickly Enron sunk. A sobering example of this in the security industry happened to TriStrata, who made a big splash in 1998 with a purported one-time pad encryption system. The deceit was quickly outed by Bruce Schneier,⁴ and the company went out of business soon after.

6. The Market Wants It

And, let's not forget that wishful thinking can go both ways. Buyers need to continue to educate themselves and their staff about what can reasonably be expected of a security product. As long as there are buyers out there who continue to believe that there is a 'magic silver bullet' for security products, there will be vendors who attempt to sell magic.

Here's a, sadly, too typical scenario in the industry:

Vendor "A" subscribes to the school of deceitful, "snake oil", marketing. The vendor supplies partially honest case studies and claims that the software is invulnerable to attack. This vendor does not supply any information about potential drawbacks or existing deficiencies on the software. Because the vendor has not done extensive operational testing or QA they are offering the product for a very low price.

Vendor "B" operates with a much more realistic and honest approach. They provide a list of "known issues" (some of which are security related), and a realistic risk assessment of the product. They also provide a road map for managing the vulnerabilities and mitigating the risks in production environments. Because the cost of testing the product and providing risk mitigation tactics can be high, the product is more expensive than the one from Vendor "A."

The client reviews the documents from both vendors and decides to go with "A" because it is cheaper and appears to be 'more secure.' "A" is able to book the sale and put the client on their customer list. Subsequently the purchasing company's network is attacked via a vulnerability in A's product but the attacked company does not want to advertise the attack so the vulnerability is not published. A, for now, continues to sell their vulnerable software. But the client cancels the maintenance contract with A and discontinues use of the product. The client tells other buyers in the industry about their concerns about A's product and A fails to sell through to new clients at the same pace they had in the past.

It's Time for Clarity

Now we have an idea of why and how some product-vendors oversell and the consequences they face from such behaviors, but what sorts of remedies are available to consumers?

There's a trend in the industry calling for enhanced vendor liability. The concept of liability has had quite a bit of pushback because it's tricky to enforce when connected to the performance of the product. Software and hardware vendors have no control over their products once they are in the hands of consumers. And unlike other regulated industries there aren't really any controls over how the consumer uses the product. Think about what would happen in the automobile industry were the liability spread between the manufacturer and the user. The user is required to have a valid driver's license in order to operate the car and must keep the car in proper repair. Firewall managers, on the other hand, can be completely untrained and configure the firewall in a way that would be like removing the brakes in a car. Who is liable for a poorly configured firewall: The vendor that shipped it in an insecure default configuration or the administrator who put it into production that way?

Liability as it relates directly to marketing claims, however, is easier to regulate. Companies should be responsible for the claims they make regarding their product. If the marketing team doesn't understand the product well enough to put out representative material, the company heads should be held liable for any misinformation.

For the wishful thinkers out there, a dose of cold, hard reality is in order.

Nothing is more deadly for a company than misinformation and an overly rosy outlook. John Ryan believed that PKI was going to save the world, right up to the moment in February of 2001 when he and the Entrust board decided it was "was an opportune time for the company to seek new leadership." If people inside a company are too close to the situation to view it clearly, get an objective Board and a seasoned Board of Advisors and other knowledgeable but objective observers to validate and sanity check corporate claims.

Finally, for the truly deceitful companies, it would be wonderful to see regulation enacted that required vendors to undergo audits that ensured that products work as advertised. For example, a review to ensure that anti-virus and IDS signatures are valid or that a data inspection firewall is actually inspecting data. This would be an adjunct to the liability for correct marketing claims. Unfortunately, industry regulation is not here today and may not be for a long time. In the meanwhile, the best way to keep vendors from presenting false hype is to stop rewarding it. Nothing speaks more loudly than a closed wallet.

Diligent buyers can demand reference customers and if a company can't show their products functioning well in an established environment, hold out for someone who can. And executives that may not have all of the technical knowledge necessary to evaluate products need to engage security professionals, either from in house resources or reputable third party advisory firms and systems integrators, to help them make informed choices. Preferably, look for an expert that knows how to ask very specific questions about how the product works in the intended installation environment. This means someone who has not only installed, configured, and managed the systems in question, but also one that understands the kind of business your company is in. Security requirements for a financial services institution are different from those of a University. An authentication system that is secure enough for something relatively low risk, like campus email, may not be strong enough for a FedWire transfer.

Summary

It's high time for security vendors to come to grips with reality and stop overselling their products. This common practice is ineffective and damaging and now that the FTC is getting involved it could also be quite costly. Microsoft has agreed to pay for future security violations and the fine is fairly steep, \$11,000 per day. Misinformation confuses buyers and leads to very unsatisfied customers. Even more concerning are the products that simply do not work as advertised and leave enterprises open to attack. Vendors need to understand that, in the end, these deceptive practices only hurt themselves. If a vendor isn't straight with you, if their product doesn't work correctly, return it. And don't buy from them again. If a product

doesn't work as advertised, eventually, people will stop buying it. It's a simple lesson, but one that vendors seem to keep ignoring. Buyers aren't stupid, while oversold promises of a security technology may result in short term sales, in the long run they backfire. It's much better for everyone involved to be realistic about what the product can really deliver.

The dot coms should be a lesson to everyone: be skeptical and demand that the product match the picture. It's up to us as an industry to insist on it.

The author would like to thank Ed Moyle, of CSC, for his editorial comments and technical insights.

¹ Microsoft Settles Passport Privacy Case,
<http://www.cnn.com/2002/TECH/internet/08/08/microsoft.ftc/index.html>

² Security Flaw Found in Symantec Firewalls, Paul Desmond,
http://www.esecurityplanet.com/trends/article/0,,10751_1441461,00.html.

³ MS99-046: How to Prevent Predictable TCP/IP Initial Sequence Numbers,
<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q243835>

⁴ "Review of TriStrata Public Information," Counterpane Systems, October 5, 1998, <http://www.counterpane.com/tristrata.html>