Fighting Cyber Security FUD and Hype

securityweek.com/fighting-cyber-security-fud-and-hype

By Kevin Townsend on March 08, 2017

Dr. Ian Levy is technical director at the UK's National Cyber Security Center (NCSC), which is part of GCHQ. It is fair to say that the NCSC will play a major part in defining and delivering the UK government's cyber security policy over the next few years.

In October 2016, Ian Levy reportedly made an unusual comment at the Wired Security conference in London. He said,

> *"If you're told that cyber security attacks are purported by winged ninja cyber monkeys who sit in a foreign country who can compromise your machine just by thinking about it you're going to have a fear response. And that's where we are today. The security companies are incentivized to make it sound as scary as possible because they want you to buy their magic amulets."*

This was not a one-off sentiment voiced on-the-fly. He repeated it in February 2017:

> *"We are allowing massively incentivized companies to define the public perception of the problem. If you call it an advanced persistent threat, you end up with a narrative that basically says 'you lot are too stupid to understand this and only I can possibly help you – buy my magic amulet and you'll be fine.' It's medieval witchcraft, it's genuinely medieval witchcraft."*

The security industry stands accused by the UK's leading cyber security agency of over-hyping the cyber security threat to sell under-achieving products. It does this in two stages: firstly by defining the threat (by manipulating the media); and secondly by positioning its own product as the sole effective cure (by manipulating the buyer).

Manipulating the Media

The vendor/media relationship is a complex symbiosis. In the age of free news, each needs the other — but there are well-known, if unspecified, rules. The primary rule is that the media must appear to be entirely independent of vendor influence, even when largely funded by vendor advertising.

The vendor industry is forced to manipulate the media subliminally — and different parts of the media accept this subliminal manipulation to differing degrees.

Historically, the vendor's primary tool has been the 'press release'; but this is now supplemented by the vendor blog. The former is used to frame the company and its product; while the latter is used to frame the threat. The ultimate aim is to define the vendor as the sole cure for a dire threat; and to get the media to describe both in the vendor's terms.

The serious media will genuinely seek the underlying truth in all it receives. But journalists have their own pressures: the need to write compelling copy that will attract the largest possible readership, and to do so repeatedly to very tight deadlines.

The first requirement (compelling copy) leads to the simple acceptance of new buzz words framed by the vendor to define a major new threat that it discovered, and by implication is best positioned to counter. It only takes a few major publications to use the term for it to rapidly become part of the security lexicon. Examples include kill chain, cyberwar, cyber pearl harbor, 'perfect storm threatening Europe', cyber 9/11 and many more.

Ian Levy singles out the use/misuse of 'advanced persistent threat' to describe everything. "He pointed out that a UK telco [TalkTalk] had recently been taken offline using a SQL injection flaw that was older than the hacker alleged to have used it. That's not advanced by any stretch of the imagination, he said." (TalkTalk originally described the attack as a 'significant and sustained' cyber assault.)

The second requirement (tight deadlines) is probably the primary cause of what is now known as 'fake news'. For the most part, this is not a conspiracy to spread false rumors, but a failure to take sufficient time to check facts rather than simply trust sources.

Fake news is not new — it has existed for as long as there have been reporters. Examples include CNN's 1999 report that Kevin Mitnick "hacked into the North American Defense Command (NORAD), a feat that inspired the 1983 film 'War Games'." He didn't do that. And the late 2016 Washington Post headline, "Russian hackers penetrated U.S. electricity grid through a utility in Vermont, U.S. officials say." That didn't happen.

If Levy is correct, security vendors have been remarkably successful in subtly manipulating the media to frame the security threat in its own terms: that is, "*cyber security attacks are purported by winged ninja cyber monkeys who sit in a foreign country who can compromise your machine just by thinking about it…"* But he goes on to imply that the purpose of this manipulation is to make it easier to sell *"magic amulets"*. This last part requires manipulating the buyers into believing in the amulets.

Manipulating the Buyer

It is easy to forget that vendors are businesses, and their primary purpose is to make a profit. "I used to work selling security software," comments Drew Koenig, now security solutions architect with Magenic. "The primary goal is not to solve the security problems, but sell you a product that you *think* can solve your security problems."

Sales methods

It is the methods used to sell the product regardless of effectiveness that worry some buyers; and the ability to see through these methods only comes with experience. Martin Zinaich, information security officer with the City of Tampa, has found salesmen will not necessarily take his 'no' for an answer. "I actually find vendors, when I express my appreciation of their product but do not see a true business fit, will start calling my younger staff. They know the shiny stuff can win a sale."

One vendor told him to use FUD (fear, uncertainty and doubt) to get budget to buy product. It didn't work: "I never have and never will. The reality is the business relies on its professionals to act as such. If there is a real risk, we need to attack it. If there is perceived risk, we need to evaluate it."

A second problem is that salesmen do not necessarily understand either the technicalities of the product they must sell, or the specific demands of the security market — and resort to their own version of FUD or fibs to make a sale.

Malware researcher Rob Slade gave an example. At a vendor presentation, he was told this great new product will automatically make your products more secure. He asked if there was any assurance requirement that would mandate every developer use the product in a secure fashion. "The salesman gave a long-winded response," said Slade, "that said you could use the product in a secure way, but, actually, it didn't require you to. In other words, he gave a verbose answer that boiled down to 'no'. I strongly suspect that the presenter didn't know he was lying to me. He probably didn't even know what an assurance requirement was."

Marketing budgets

Surprisingly, the size of security product marketing budgets is also seen as an issue. "Vendor marketing budgets are a massive problem," says security author Raef Meeuwisse; "especially as the largest budgets are often backing the most out of date and ineffective security technologies. It often feels like the larger the ads, the less the vendor has to sell." He believes that this has a direct effect on the size of the security market, because it "helps us buy security brands that have been around for a while rather than security solutions that often work considerably better." The whole issue, he suggests, is then made worse by "commercial research companies whose business model requires that they only actively promote the companies paying in the most research money."

Ilia Kolochenko, CEO of High Tech Bridge, points out that it isn't just the budgets of the big firms that causes problems. "We should keep in mind that numerous VCs that appeared on the bubbling market of venture capital during the last few years are also responsible for hype and FUD in cyber security."

Venture capital makes its money by buying low and selling high. It gambles that a new small company will become a big powerful company through increased sales before it cashes in on its investment. In short, venture capital is motivated by increasing sales rather than improving product. "Many of them," explains Kolochenko, "put pressure on the company to increase sales by any means, selling to everyone, without really thinking if the client will get any benefit from their technology. This is why today many startups are trapped by easy-cash distributed by VCs, and now must spend all their time and other resources on aggressive sales rather than on technology. Entrepreneurs should remember that there is

no free cash."

But it's not a new problem, and it doesn't just apply to cyber security. "There's a degree of sensationalism that product marketers have always applied, not just now," comments Bill Burns, chief trust officer and cloud business transformation at Informatica. "They're always looking for 'an edge' to capture the market's attention."

Fighting the F.U.D.

"It is the business, guided by our experience and input, which needs to make the final decision," says Zinaich. "The fact is, more squirrels have taken out power around the globe than any hacker has to date. It is not even close. Yet, the fragile 'House of Internet Things' we are rapidly building is full of risk. That risk has to be managed in the light of reality, not by carnival barkers."

There is an acceptance among security leaders that security vendors will hype the products and FUD the threat; and that it is down to the professionals' own knowledge and experience to get to the right product for the right price for their own environment. "I've found the best approach is to leverage proof-of-concepts on every solution we are considering," comments John Masserini, CISO at MIAX Options. "Not only does it vet the hype from the reality, but it also gives you a deep understanding of the operational impact the solution will have on your specific infrastructure. This is an often-overlooked aspect of many security solution providers and could be far more challenging than the risk you're trying to mitigate. Make them prove their functionality in your specific environment before ever signing a check."

Meeuwisse takes a similar view. "My main advice is this: security technology is moving so fast, don't buy anything on an uncancellable multi-year deal. You never know when it will start to become an inferior or outdated product or service."

Steve Lentz, chief security officer at Samsung Research America goes further — he almost makes it personal. He doesn't want a product that does what it says, he wants one that does more. "When I can get a vendor where I can trust that they will always do more, that is a big plus. This also includes that their support is top notch; and they better give me their best price the first time. If I have to keep haggling for a lower/best price they are out. If I have to send an email to their VP of Support and Sales, saying 'your support sucks!', they are out. If the vendor does what he says and more, and we prove that by first POCing and then purchasing, they usually stay in our security environment. I will renew as long as they keep this up."

The best way to combat vendor hype and FUD, says Koenig, "is to know what your security problems are before you look at vendors to solve them. Only a business knows what problems you have — a guy in a booth or cold calling you shouldn't tell you what problems they think you have."

When you fully understand the problems you have, he continues, “then go research the vendors yourself, hit the forums, ask your peers before you pick up the phone, talk to everyone but the vendor before you talk to the vendor. When it comes time to bring the vendor in always have the vendor prove it. Make them show the tools solving your problems, not a vendor made canned demo that will work 100% of the time showing you the buzzwords in action. Whatever you decide you will have to deal with it long after the sales team moves on. If you bring something in that doesn’t solve your problems, the vendor won’t be held accountable.”

‘Try before you buy’ is the repeated recommendation. Bill Burns thinks this is a new and growing option that may eventually solve the hype and FUD problem. “With the advent of mobile, SaaS and cloud computing, companies can now offer ‘trial versions’ of their software on the same infrastructure and offer the same user experience as the ‘real product’. Vendors can now show off their products — warts and all — directly to their target customers with the obligation to prove value in their product. The time between ‘awareness of an unmet need’ and ‘testing a solution’ is growing smaller quickly; good marketers know that relying on ‘hype’ will generate a negative reaction even faster than before.”

The Ultimate Solution

There is no ultimate solution. Salesmen will continue to sell the products they represent rather than the correct solutions. Publications will continue to seek readers by making their news stories as ‘interesting’ as possible. The combination will always drift towards Ian Levy’s *winged ninja cyber monkeys*; but if Bill Burns is correct, the new Information Age may make it a self-correcting issue through the democratization of information. The new element is the citizen journalist — the independent blogger who does not hesitate to correct the professional journalist who makes a mistake, nor criticize a product that is over-hyped or inadequate. Independent blogs will keep both publications and vendors honest.

David Harley is both a security researcher and a prolific blogger. “There's no doubt that emotive language relating to warfare and/or epidemiology has long been a staple of security-related marketing (and journalism!). I can't say I like it – much of my career in security has been devoted to damping down the fires of hyperbole and advocating less drama and more precision,” he says.

“But I'm most concerned by the misuse of language in ways that are actually deceptive rather than everyday sloppiness. It annoys me (quite disproportionately) when a system is described as 'infected' when 'compromised [by some form of Trojan]' would be more accurate; or when people use 'virus' as a synonym for 'malware'. However, I regard it as frankly deceptive when people evade the distinction between 'successful attacks' and

'attempted attacks' because saying 'ten million systems were attacked' is more dramatic and makes a marketing point more effectively than adding that '0.001% of attacks were actually successful'...

Over time, bloggers like Harley could disarm, if not remove, the winged cyber ninja monkeys by keeping journalists honest and vendors truthful.

Kevin Townsend is a Senior Contributor at SecurityWeek. He has been writing about high tech issues since before the birth of Microsoft. For the last 15 years he has specialized in information security; and has had many thousands of articles published in dozens of different magazines – from The Times and the Financial Times to current and long-gone computer magazines.

Tags: