Whiz Bang 2000

Facts: Cyberattacks are a known threat to the information systems of organizations around the world. There are many products on the market that purport to detect and/or prevent cyberattacks. Cyberattacks are happening anyway.

Why is this so?
• Maybe the companies that make cybersecurity products do not have good salespeople? No, that is not the reason.
• Maybe chief information security officers (CISOs) are not interested in products that detect and/or prevent cyberattacks? No, that is not the reason either.
• Maybe the products are not very good? That is a possibility, but there is no comprehensive evidence to that effect.
• Maybe cyberattacks are not a problem that lends itself to packaged solutions? Hmm...

CYBERSECURITY PRODUCT FEATURES
There are many cybersecurity software products on the market. They come from large companies better known for computer hardware, small firms that have gained a reputation for after-the-fact repair of cyberattack-related damage and start-ups about which little is known beyond their web sites. Some of these products promise to stop advanced persistent threats (APTs) used by cybercriminals. Others merely say they will detect zero-day attacks, malicious communications, and anomalous attacker indicators. Rather than pick on any one vendor, or even several at a time, I have invented a totally fictitious product that I call Whiz Bang 2000 (WB2K) (trademark, copyright, patent pending, marca registrada, etc., etc.). WB2K is intended to be a compendium of the features claimed by many, if not all, of the products I have seen in the marketplace. It will:

• Maintain awareness of all changes to an organization's infrastructure configuration
• Enforce access control and change management policies to monitor, detect, contain and prevent malicious activities across end points, including servers, laptops and desktops
• Aggregate risk factors to automatically elevate alerts and containment controls including the trigger of forensic actions
• Monitor and block known bad applications and unknown applications, preventing the rapid spread of cyberattacks
• Detect, prevent and contain malicious software effectively on and off the network
• Use a signature-less approach to detect new or unknown malware with automated behavioral analysis of code in physical memory
• Manage scans based on schedule or policy violation and facilitate the retrieval of memory forensics to support incident response
• Determine the characteristics of an attack and which resources—software and data—have been affected
• Monitor all software coming through the Internet gateway for viruses and other malware

So, aside from the fact that the product does not exist, why is my phone not ringing off the hook with orders for WB2K?

OTHER TOOLS
Many of the features of WB2K are available in products that already are in use in many data centers. For example, configuration management databases (CMDBs), and their related software, generally have knowledge of configuration changes. These are often fairly expensive tools. While they are often found in large enterprises, they may be beyond the budgets of small to medium-sized businesses.

For those that do have a CMDB and the aligned ITIL-supported change and configuration management processes that go with it, a cybersecurity product may, in many cases, be redundant.

Intrusion detection and prevention systems (IDPSs) are aware of malicious activities on
networks and information systems (IS) infrastructures. They can trigger alerts and prevent the spread of malicious software across an organization’s systems. In my opinion, no organization that is serious about cybersecurity should operate without an IDPS, and, in my experience, few do. But they do not always apply them everywhere and on every endpoint, so there may be gaps in many organizations’ defenses. There is no reason to believe, however, that the detective properties of a cybersecurity product, such as the mighty Whiz Bang 2000, would be any more effective than long-used IDPS tools.

MARKET DOMINANCE
Across the IT field, there are certain products that have achieved such dominance that they are the de facto standards, attracting the vast bulk of customers and antitrust lawsuits. No product has attained that status in the area of cybersecurity. Considering how long information security products have been in the marketplace, it is a bit surprising that no company has captured the imagination, if not the money, of those who buy such products for large organizations.

It may well be that buyers are waiting for the market to shake out the lesser products and let a clear winner (or at least a few) emerge. If this is just a matter of an immature marketplace, it is time for it to grow up quickly; the threats are getting worse, not slackening. But there is a circularity to this argument: Buyers are not buying because vendors are not selling. In the bazaar that is software sales, we should expect the imprimatur of purchases of certain leading organizations to spur further deals with similar companies. I do not see that happening, at least not yet.

PURCHASE INHIBITORS
I think there is a psychological inhibitor working against the large-scale acquisition of cybersecurity products. The New York Times pointed out recently that CISOs have thankless jobs. Their positions are only as secure as the next successful cyberattack. Andrew Casperson, a former CISO, is quoted as saying “In the old days, there was a saying, ‘Nobody ever got fired for buying IBM,’ because you could trust IBM. But security firms have never been able to establish that level of credibility.”

To go to management with a request for budget for a cybersecurity product is an implicit endorsement not only of a specific vendor’s product, but of the concept that any product is capable of solving the problem of cyberattacks, without any clarity as to what a solution might be. The community of information security professionals has labored for decades to protect information systems from abusers, misusers, fraudsters and thieves. And, the professionals have not always succeeded. In most cases, their strategy has been to make the difficulty and cost of undermining security so high that attempts, much less successful attacks, were rendered unlikely. The world is now contending with highly skilled, well-financed attackers with sufficient resources and incentives to undermine or overwhelm the barriers that have been erected in the past.

For many CISOs, buying and implementing a cybersecurity product is taking a gamble with their careers. Unless and until there is a demonstrably superior product, I suspect that products in this area of IT will be slow to take command in data centers around the world. And, until the information systems that live in those data centers are demonstrably securable, it may make no sense to buy protective products that do not, cannot, protect.

But if anyone is interested, I would be glad to offer the next release of Whiz Bang 2000.

ENDNOTES
1 Software advertising tends to be of the “leaps over tall buildings” school of panegyrics. Throughout this article, I use paraphrases of vendor text, but do not identify them.