

Published on *Infoworld* (<http://www.infoworld.com>)

[Home](#) > [News](#) > [Security](#) > The 7 dirty secrets of the security industry > The 7 dirty secrets of the security industry

The 7 dirty secrets of the security industry

By Joshua Corman

Created 28 Jan 2009 - 6:22am

Do you ever get the feeling your security providers are failing to tell you the whole truth? We entrust the industry to protect us from unacceptable risk. But we must confront the underlying truth: The goal of the security market is to make money.

Here are the seven dirty secrets of the security industry and practical ways to command honesty from your trusted security providers.

[Discover the top-rated IT products as rated by InfoWorld's 2009 Technology of the Year Awards ^[1]. | And keep up on the latest tech news headlines at InfoWorld News ^[2], or subscribe to the Today's Headlines newsletter ^[3].]



1. Antivirus certification omissions. The dirtiest secret in the industry is that, while antivirus tools detect replicating malicious code like worms, they do not identify malcode such as nonreplicating Trojans. So, even though Trojans have been around since the beginning of malicious code, there is no accountability in antivirus certification tests. Today Trojans and other forms of nonreplicating malcode constitute 80% or more of the threats businesses are likely to face. Antivirus accountability metrics are simply no longer reflective of the true state of threat.

2. There is no perimeter. If you still believe in the perimeter, you may as well believe in Santa Claus. That isn't to say there is no perimeter. But we need to define what the perimeter is. The endpoint is the perimeter, the user is the perimeter. It's more likely that the business process is the perimeter, or the information itself is the perimeter too. If you design your security controls with no base assumption of a perimeter, when you have one you are more secure. The mistake we tend to make is, if we put the controls at the perimeter, then we will be fine. For many threats, we couldn't be more wrong.

3. Risk management threatens vendors. Risk management really helps an organization understand its business and its highest level of risk. However, your priorities don't always

map to what the vendors are selling. Vendors focus on individual issues so you will continue to buy their individual products. If you don't have a clear picture of your risk priorities, vendors are more than happy to set them for you. Trusted security partners will provide options for assessing your risk posture and help you develop plans to make the most security impact for the least cost and complexity. Security needs to conform to and support your business priorities. Too often, vendors want your business to conform to their portfolio.

4. There is more to risk than weak software. The lion's share of the security market is focused on software vulnerabilities. But software represents only one of the three ways to be compromised, the other two being weak configurations and people. The latter is the largest uncovered area of risk. This is malicious code that doesn't leverage a vulnerability but rather leverages the person. For example, downloading a dancing skeleton for 'a spooky good time' (this was a trick employed by Storm), social engineering, spear phishing, etc. While we still need to find vulnerabilities and patch them, we must understand that an organization is only as strong as its weakest link. And more attention needs to be paid in mitigating the other two ways beyond software.

5. Compliance threatens security. Compliance in and of itself is not a bad thing. But, compliance in and of itself does not equal security. At the very least it's a resource and budget conflict, and it splits our focus. Compliance is supposed to raise the minimum standard of security, but it just gets us to do what we are required to do and nothing else.

What's more, that which is easy to measure is not necessarily that which is most valuable. So if there were 15 software vulnerabilities last month, we can measure that 12 of them have been patched. It is much harder to measure how effective end user training was to make administrators immune to social engineering attacks. The lesson is you need to be compliant, but your entire risk strategy cannot be based on it.

6. Vendor blind spots allowed for Storm. Storm is being copied and improved. The Storm era of botnets is alive and well, nearly two years from when it first appeared. How is this possible? 1. Botnets thrive in the consumer world where there is little money for innovation, a fact Storm and its controllers know. They are making money off of everything from spam to pump-and-dump stock scams. 2. They eat antivirus for breakfast. A lot of the techniques and innovations used by Storm are not new; they are just being leveraged artfully against the blind spots of antivirus certifications and antivirus vendors. 3. Malcode does not need vulnerabilities. Most of the Storm recruitment drives have leveraged social engineering and play off of a holiday or sporting event.

7. Security has grown well past "do it yourself." Technology without strategy is chaos. The security market is often far too focused on the latest hot box or technology. The sheer volume of security products and the rate of change has super-saturated most organizations and exceeded their ability to keep up. Organizations realize only a fraction of the capabilities of their existing investments. Furthermore, the cost of the product is often a fraction of the cost of ownership. There was a time when you could "do it yourself." But the simple days of Virus meets Antivirus are long gone. Highly effective organizations are embracing professional and managed security services to extend and augment their in-house expertise. By focusing your in-house expertise on what you know best -- your

business -- scale comes from teaming with third-party expertise. This will be increasingly necessary in these tough economic times.

The primary goals for executives over the next few years is to cut cost and reduce complexity. Today we are seeing a massive convergence in the security market. There are only going to be a few large players left and a bunch of smaller players. Will consolidation lead to better efficiency, or will it lead to vendor lock-in?

As executives simplify, they will face many choices. Simply reducing vendors may fail to balance cost, complexity and risk. Vendors have a responsibility in this equation and must rise to the challenge. True risk management can show where to prune solutions, but the key is risk driven, responsible simplification.

Corman is principal security strategist for IBM Internet Security Systems. [Network World](#) [4] is an InfoWorld affiliate

[Networking and management](#) [Security Central](#) [Anti-virus](#) [Business](#) [Malware](#) [Network monitoring](#)
[Networking](#) [Regulatory compliance](#) [Risk management](#)
[Security](#)

Source URL (retrieved on 26 Apr 2009 - 6:20pm): <http://www.infoworld.com/d/security-central/7-dirty-secrets-security-industry-622>

Links:

[1] http://www.infoworld.com/article/09/01/13/02TC-toy-2009_1.html?source=fssr

[2] <http://www.infoworld.com/news/?source=fssr>

[3] <http://www.infoworld.com/newsletter/subscribe.html?source=fssr>

[4] <http://www.networkworld.com>