Popping Purple Pills: Who is the right gatekeeper for IT security?

A CIOview White Paper
by Scott McCready

Support links

CIOview

Table of Contents

Popping Purple Pills:
Who is the right gatekeeper for IT Security?

Lovegate, Kibuv and Bobax may sound like the unfortunate names for new generic drugs, but they are not. Instead they are among the most recent worms to be discovered, all three within only a few days. How do you respond to the latest threats, and what can you do about dealing with security issues in general? Clearly you can decide to pour more money into the problem and select from a dizzying array of new security technology, or just augment your Purple Pill regimen, both of which are less than appealing. The good news is that there is a better option.

Obviously there is no limit to what you can spend on security, just ask the US government. Certainly there is no shortage of available technology. However, unless a company has a robust risk/security model it will encounter costly problems. It may invest money in the wrong products, have unrealistic expectations of its IT staff, and spend far too much of its time and resources complying with regulatory requirements. Ultimately, security runs the risk of being the number one barrier to new business initiatives.

Right now, the idea of developing this type of risk management strategy is probably making you reach for the medicine cabinet. So, why not turn to your traditional accounting/consulting firm? Before answering that question you have to accept a number of security truisms, namely:

- Your security degrades on a daily basis
- Your security needs are dynamic and must change as your business priorities change
- Security risk strategies and loss minimization policies have to work hand-in-hand

Accounting/consulting firms do not work because security is a daily monitoring requirement. Using an accounting/consulting firm to perform a periodic audit is like driving a school bus down a major highway using the rear view mirror. An after-the-fact review of your security vulnerabilities is a wonderful blame-assigning strategy but does nothing for keeping customers happy and regulators satisfied.

Accounting/consulting firms do not work because their methodologies only change in response to their business needs, not yours. The result is either a security template that does not take into account your operational uniqueness or a very expensive consulting project that once again is only a snapshot in time. Regardless of what is in your security framework, the most important requirement is that you can easily alter it when new threats and vulnerabilities emerge. If you cannot alter your methodology, it becomes a straightjacket for new business initiatives.

Accounting/consulting firms do not work because they typically demand that you retrofit security requirements to existing operations. Instead of rigid “after the fact” audits, IT operational staff require an accessible framework that they can build into their project and policy planning. This will allow you to hit the sweet spot of attack prevention (cutting edge technology) and loss minimization (proper business practices and safeguards).

However, there is a better answer. What you need is a “state of the art” risk management methodology. So, what is a “state of the art” risk management methodology? There are six crucial tests that it must pass, namely, is it:

- Equally useful to both internal IT resources and outside security consultants?
- Capable of allowing IT staff to lower your regulatory compliance costs?
- Independent from your loss prevention policies but at the same time will allow for a unified financial view of security?
- Verifiable?
- Independent of the security technology vendors?
- Able to provide a quantitative risk assessment in two parts: justified risk (inherent risk of doing business), and actual risk (current vulnerability of your systems)?

In the end you have basically three choices:

- You can hand over responsibility to your accounting/consulting firm making security at best, a black box and at worst, a black hole for consultant expenditure
- You can keep popping the purple pills
- Or, you make sure your risk management methodology meets the six crucial tests for being “state of the art,” and therefore, ties your security spending directly to financial improvements

If you are wondering how to executive this within your own company, our next column will provide you with the necessary roadmap.

About CIOview

Established in 1997, CIOview has spent more than five years gathering data from IT customers, IT consultants, and the major hardware and software companies. The result is an industry standard method to measure the business value of IT products. CIOview's TCOnow! and ROInow! software combines customer data with a sophisticated system configuration engine, making it quick and easy for each customer to generate their own business case report.

CIOview has created 55 distinct products all of which use the same desktop player application and a product-specific content module. This provides customers access to a complete portfolio of business case analyzers for all of their IT purchase decisions.

Where Can You Go From Here?

- Any other questions? Contact CIOview at info@cioview.com
  CIOview Corp. • 4 Clock Tower Place • Maynard • MA 01754 USA • P +1.978.823.1600

Disclaimer

The information contained in the white paper scenarios is based on many variables and assumptions not stated herein. Results will vary, no results are guaranteed. Full terms and conditions can be seen at www.cioview.com/about_us/about_disclaimer.html

Copyrights