

# The War on Security Can(not) Be Won

A CIOview White Paper  
by Scott McCready

**Support links**

## Table of Contents

Table of Contents .....	2
The War on Security Can(not) Be Won.....	3
10% and Growing .....	3
Not Just Technology.....	3
A Business Obstruction.....	4
No Standard Method .....	4
Black Box .....	5
The Answer.....	5
About CIOview.....	7
Where Can You Go From Here? .....	7

## The War on Security Can(not) Be Won

---

The threat of viruses, hacking, denial-of-service attacks, terrorism and all kinds of other worldly evils has propelled spending on computer security to the number one spot on the IT budget for many companies. However, there are early signs that the security checkbook may be about to get snapped shut and unless security professionals and the industry at large adjusts quickly, the era of big spending may come to a rapid close. There are several reasons to believe that the security industry has reached a point of inflection in its growth, namely:

- Security spending now exceeds 10% of many IT budgets
- Security is increasingly viewed as not just a technology issue
- Security is beginning to hamper business
- Companies have no standard method to determine how much they should spend on security or how they should best direct the financial resources they have
- Security remains a “black box”

### 10% and Growing

Spending on IT security currently exceeds 10% of many IT budgets. Like any rapidly growing category of expenditure, senior management scrutiny is becoming more an issue. Frankly, fear and the imminent threat of new legislation have driven many IT security budgets to their present state, but as the cost of security continues to expand the pendulum is already beginning to swing back to greed. Once that happens security will come under the same financial scrutiny as any other IT expenditure. Unless the security industry is ready to show the financial implications of not investing in security there will be a sharp drop in security spending.

### Not Just Technology

There is a dazzling array of security technology out there and the industry at large does an excellent job showcasing their wares from a technology perspective. However, as security becomes an increasingly pervasive portion of every IT initiative and business process the operational aspects of security become much more visible. This is good for the security industry overall because it helps set realistic customer expectations. It is bad in the sense that it is a wake-up call for those companies that thought they could simply spend their way to winning the war.

The challenge for the security industry is to do a much better job of explaining the financial implications of loss controls and the role they play in conjunction with security technology to limit a customer's risk.

## A Business Obstruction

---

The good news for the security industry is that new business processes are increasingly designed with security issues taken into account. The result is fewer problem areas compared to those cases where security is retrofitted into a less than optimal solution. The bad news is a pending precipitous drop in the purchase of security from “reactive customers” and a dramatic increase in the number of “proactive” security buyers. On its own this simple but undeniable change in consumer behavior should be enough to rock the security industry back on its heels. If you are not a great believer on the impact of consumer behavior changes then just look at the shocks the US auto market has gone through or the growth of the iPod.

The proactive security customer comes with a good side and a bad side. Security solutions will ultimately be more elegant because they will become intrinsic to almost any new business initiative. Better yet, the dollars spent on services that were previously required for retrofitting will now be largely released to the product vendors. The downside is that as a pervasive element of any new business initiative, security will become increasingly seen as the enemy for timely deployment. Time to market is a key financial metric in most companies and one which is easy to quantify from a financial perspective. Security vendors will have to respond with either products that are easier to implement or a time to market model that allows their customers to trade off time to market vis a vis increased operational risk.

Time to market is only one of many business hurdles that many new security initiatives need to get over. Take the example of EDS and its desktop contract with the US Navy: certainly EDS is making Navy desktops more secure but in the process they are taking away the ability of the individual to personalize their work environment and usurping the local administrator’s authority to grant use and access privileges. No question this will benefit the Navy’s security but EDS is losing \$146,000,000 a year in customer satisfaction bonuses because they have failed to prove the business value benefit of security to the masses.

Clearly, companies need to find the optimal level of security that balances business process operation with potential security risks. Too much security can be as much of a hindrance and danger to businesses as too little. Technology must be balanced with systems of loss controls that anticipate security breaches and minimize the potential damage.

### No Standard Method

There is no standard method for companies to evaluate the financial implications of the risk their current security posture exposes them too. Why bother with something quantifiable when, driven by fear, people are clamoring to buy now. Financial analysis in this case is simply a hindrance in the purchase cycle. However, for the security vendors this may prove to be the ultimate challenge. Avoiding the whole question of risk and financial implications means that a key sector of the IT industry has no experience using a rational business-spending model.

Not having a standard model for assessing overall risk, the technology vendors have in a way short-changed themselves because even though 10% of an IT budget may seem like a lot, some companies should probably be spending more. Also, since there is no standard model to assess financial impact, there is no way for a customer to know what security products offer the best financial return. As a result, security spending is not necessarily flowing to those products or vendors that have the biggest impact. In effect the product folks, service providers and customers are all effectively “Dancing in the Dark” which appropriately brings us to the next issue of a black box.

### Black Box

Security is arguably one of the most complex IT subjects because it covers such a broad set of issues and permeates every aspect of technology. For technology neophytes security is simply an overwhelming issue. In the short term the natural reaction to this Pandora's box is to abdicate responsibility to the experts. However, once spending reaches some critical level, management is going to suddenly want to catch up and the educational learning curve is going to be very steep indeed. Historically, as technologies go through the education phase spending declines.

#### Clearly there needs to be a way to make:

- The whole issue of investing in security transparent to the financial folks
- Security accessible to a broader audience so that security professionals can more easily communicate what needs to be done

### The Answer

Organizations need a free software package that lets them complete a security self-assessment in 30 minutes or less. This analysis needs to:

- Rapidly identify key security vulnerabilities and assign a financial cost to each
- Forecast how the security environment will change over time
- Evaluate various loss control policies and their effectiveness at reducing risk
- Calculate the Return On Security Investment for 100's of possible strategies

Part and parcel of the assessment needs to be a standards-based methodology. CIOview's SecurityNOW! SX quantifies risk using a commonly accepted framework, Risk Assessment Value (RAV). RAV allows organizations to compare their security between departments and over time. In fact, RAV is increasingly the most common security measure that regulatory bodies are demanding. SecurityNOW! SX has the Institute for Security and Open Methodologies (ISECOM) seal of approval and embodies the six capabilities key to making security transparent in 30 minutes or less:

- Accelerated
- Accessible
- Objective
- Customized
- Forward-looking
- Graphical

## The War on Security Can(not) Be Won

The result is that the security industry now has a free, standard method for risk assessment and financial analysis. Suddenly the security industry will derive a number of key benefits, namely:

- At last the risk and financial nuances of security will be readily understandable to a broad audience ensuring that the proverbial educational “monkey” will not hamper the short-term growth of the industry
- Security spending will now be driven by financial priorities and the technology vendors that provide business value will prosper
- Services providers will have a more educated audience and spend less time providing basic education and collecting data
- Security spending should accelerate as companies realize that their security naturally degrades daily
- Companies have a standard framework to collect data and respond to existing and new legislation. The costs for security compliance will go down dramatically

Perhaps the best news ultimately is that security will be better understood and customers will have more realistic expectations. Meanwhile security professionals and auditors will benefit from the Professional Edition of SecurityNOW! which provides a variety of automation features that reduce the time to deliver a set of audit results from 30 to 3 days, namely:

- Validated data can be imported from a number of network port and vulnerability detection scans;
- Verified data from OSSTMM or similar security audits can be directly entered;
- A financial and business case for security spending as well as a certified audit report can be published with one mouse click.

SecurityNOW! Professional Edition for the first time offers financial transparency for IT security and increases auditor productivity by 90%. Perhaps the only un-answered question at this point is when companies will see a corresponding drop in the audit fees big accounting firms have got used to charging!

## 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](mailto: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](http://www.cioview.com/about_us/about_disclaimer.html)

### Copyrights

CIOview® and ROInow® are registered trademarks of CIOview Corp.  
TCONow™, Real-Time Business Value™ and Simplifying IT Purchasing™ are trademarks of CIOview Corp.

All other trademarks used are the properties of their respective owners.