

Run information security like you run your business

A White Paper

Prepared by Danny Lieberman-Open Solutions

Feb 1, 2005

Abstract

Chances are, your firm is not running information security like a business unit with a tightly focused strategy on customers, market and competitors.

The sales people in your firm have sales quotas and are measured by gross profit margin and collections. The people who run manufacturing and distribution have quotas for throughput and inventory cycle times. Do *your* CSO, CIO, information security professionals and software developers have measurable quotas and compensation for meeting or exceeding their information security numbers? Without well-defined, standard, vendor-neutral threat models and performance metrics, there cannot be improvement; and improvement is what our customers want.

Today's business lives on digital assets. Whether you're a contractor digging ditches for a cable provider or if you're the cable provider CEO you live on information. Key company assets (such as customer records) are digital and live in a PC, a Windows server, a Linux server or mainframe; the paper is a "hard-copy" not the original. Your firm manages fixed assets and produces 10Q reports if publicly traded, **but** do you tag and value *digital* assets that are key to the operation? Can you calculate ROI for digital asset protection technology or prove compliance with Sarbanes Oxley 906 without measuring the *value* of your key *digital* assets?

Choose a business strategy for information security. Information security today works on a cycle of reaction and acquisition. Infosec needs to operate continuously and proactively within a well-defined, standards-based threat model that can be benchmarked against the best players in your industry just like companies benchmark earnings per share. In his classic article, "What is strategy?" Michael Porter writes how "the essence of strategy is what *not* to choose...a strong complete position requires clear tradeoffs and choices and a system of interlocking business activities that fit well and sustain the business". Security of your business information also requires a strategy.

Measure in order to manage, improve and comply There are widely accepted and practiced revenue models, costing models and performance metrics that work for all kinds of business units. To cost a product or service, we see that a distribution business uses mark up margins, a manufacturing unit uses bill of material costing and a professional services unit uses standard and activity costing. If you want to evaluate cash flow, just look at cash flow from operations or free cash flow (FCF) - simply cash from operations, minus capital expenditures. True, FCF omits the cost of debt but you have an objective indicator to go by that can be measured every week, every quarter, every month of the year. A major supermarket chain recently lost \$5M because an employee extruded their purchase prices of fresh produce to a competitor using instant messaging. The firm reacted with locked doors and cameras, but locked doors and cameras can't **audit** information flows and provide extrusion **performance metrics**.

Test your infosec business strategy IQ

1. Is your digital asset protection spending primarily driven by regulation?
2. Are Gartner Group white papers a key input for your purchasing decisions?
3. You still don't have security win/loss metrics?
4. Does your CSO meet at least 3 vendors each day?
5. Does your infosec purchasing cycle of a new product take at least 6 months?
6. Are you short on head count, and not implementing new security technologies?
7. You're a CTO and you never personally sold or installed your company's products?

If you answered YES to 4 out of 7 questions, you need a business strategy with operational metrics for your infosec operation.

Take action to protect your assets like you run your business

1. Setup indicators and publish them once a week on the company Intranet for everyone to see. Start with 3 indicators: the number of network anomalies your IDS found that week, your current patch cycle time and how much overtime your staff worked.
2. Do continuous security audits. Purchase a tool for network audit and run it once a week on a different part of the network. The guys over in the warehouse stopped doing full physical counts once a year 15 years ago, they count a little bit of inventory every day with hand-held barcode terminals. Get a consultant to help you set it up and run it yourself.
3. Run security awareness programs. Make the number of training hours one of your indicators
4. Build a threat model and maintain database of your key assets, threats and vulnerabilities and [start building a threat model today](#).
5. Define your competitive strategy for infosec operations. Is it low cost? Is it single vendor? Is it Linux desktops? Is it end-point security focus?
6. Implement a **consistent** set of activities, for example standardizing on diskless [thin clients](#), [remote desktops](#) and Windows Terminal services.
7. Think how activities can **reinforce** each other - for example by installing personal firewall software that reports on intrusion attempts to a central server so that you can plan your response to future attacks.
8. Identify sets of activities that **optimize** your efforts. Perhaps you have a totally flat network with a spaghetti plate of servers and workstations today. Segment the network into VLAN's, put the application servers on one segment, the data servers on another and client workstations on departmental segments and so forth. Performance and security will improve and you'll be able to monitor content effectively. You'll spend less time firefighting and more time thinking.
9. Install your company's products yourself. After you do that, follow a customer home and watch how they do the install and take notes. Update the threat model with your findings.

For perspective on competitive strategy see Michael Porter's article [What is Strategy](#) at the Harvard Business Review online. For more information visit us www.software.co.il/extrusion