IT Security:
What shareholders should know about the exploding responsibility for data integrity

Commentary & opinion authored by: Milt Habeck
Founder & CEO, Unbeaten Path International Ltd.

Composed: May, 2004

Introduction

There's been an explosion in responsibility for IT security. The debris cloud is the product of three ingredients: the exponential growth of transactions, the increasing specificity of data, and the growing alphabet soup of IT security regulations and standards. The Sarbanes-Oxley Act (SOX) added further impetus to system security and data integrity demands placed upon IT management.

Based on almost three decades of manufacturing company observations as a manager and consultant, (in North America, Latin America, Japan, and Europe) I believe that these expectations for IT performance won't be fully achieved by a consequential number of enterprises. Why? Because, in my opinion ...

- The legacy of senior executive indifference to good business practice and internal controls can't be fully overcome despite the approaching SOX audits. It will be challenging to achieve prerequisite headway on the first step: attitude change.
- IT doesn't have authority to fix business process internal control problems; enthusiastic leadership/involvement from senior operational managers is required to accomplish that.
- Computer systems will continue to be populated with and, therefore, exponentially propagate inaccurate data until business process internal control problems are fixed. *(Bad data are typically the root cause of enterprise system performance accidents; now SOX auditors are poised to join the chorus of misinformed internal criticism endured for years by IT departments.)*
- IT resources are already stretched thin by other IT security requirements and the emergence of new transaction types with new mountains of more and more detailed data.

Consequently, shareholder confidence about the outcome of the first round of SOX audit reports may be misplaced. Shareholders must be confident about how senior managers are directing the practice of internal controls in their enterprises or otherwise they'd be moving from long positions to short positions. The balance of this essay will be a shareholder's primer on the challenges IT departments face with respect to data propagation, data accuracy, and system security.

Information technology used to be less complicated

I'm old enough to remember when UPC codes were introduced; I was in the Johnson Wax marketing department and recall figuring out how to squeeze the bar code block onto the back of the can. At the time it seemed like things were getting very organized ... but ... now we have the UCCnet Global registry with a Global Trade Identification Number (GTIN) for every conceivable packing configuration of a product. We've also got Global Location Numbers (GLNs) which will eventually define product delivery destinations right down to the vending machine level. Wow.

Resources are now pouring into RFID (Radio Frequency Identification) so that pallets and cartons of finished goods can be traced through the supply chain. Wal-Mart has set a January '05 compliance deadline for its top 100 suppliers. Benefits in the billions of dollars are expected from finding lost products, quantifying in-transit and trade inventories, and responding quickly to out-of-stocks.

UCCnet, RFID, and other business-to-business (B2B) technologies will be propagating mountains of fresh data for computer hard drives.

The propagation of data

The trend is clear: data is moving towards 'indivisibility.' That's the point where information can't be sub-divided anymore ... the point where the number of fields required for any given record will have reached the "we'll-never-have-to-add-another-field-again" limit. We haven't arrived there yet, but it seems as if the gas pedal is pushed all the way to the floorboard.

The trend isn't limited to commerce:

> It used to be that a social security number and a fingerprint record covered a great deal of ground. Now DNA information is stored in databases and culprits are being caught with it. Once an individual's DNA chain segments are on file, how do you further sub-divide that information?

When the trend towards data 'indivisibility' is multiplied by the enormous growth in transactions, any enterprise can quickly propagate mountains of data. That rate of growth warrants incisive questions from the floor at the annual stockholder's meeting:

- **Is the information in the corporate database accurate?**
- **Is the information categorized in a way that permits senior managers to really grasp what's going on?**

The not-yet-heard case for data accuracy

There were always outstanding reasons for good data accuracy ... even when we had much less data employed for much less ambitious reasons. Oliver Wight began preaching that in the 1970s. But, a quarter of a century later, it remains a rare exception to find an enterprise that has achieved and sustained the world class data accuracy levels needed to get the full ROI from an ERP system (which employs Oliver Wight's MRP II theory as a foundation).

> Speaking from my personal observations ...at this very moment, fork truck drivers are rolling up and down the warehouse aisles of multi-billion dollar enterprises looking for lost stuff ... cost accounting analysts are trying to explain variances that stem from bad engineering standards ...and ... buyers are fixing manufacturing material shortages with Federal Express shipments because bill of material scrap factors are inaccurate.
>
> The mathematics of reliability theory prove that if a computer program uses information that is only 90% accurate seven times, the probability that the calculated result will be useful is less than 50% (47.83%, to be exact ...the result of multiplying .90 by itself seven consecutive times).

It continues to mystify me why CEOs approve multi-million dollar budgets to change from ERP system brand X to ERP system brand Y without first investing to fix the data accuracy attitudes and internal control voids that are sabotaging the performance of brand X and will just as surely sabotage the performance of brand Y.

Unfortunately, shareholder concerns about data accuracy problems cannot be confined to just the warehouse and plant floor.

> Speaking again from personal observation ... at this very moment, order processing systems are applying the wrong promotional price to customer orders ... salesmen are compensating for the effect of a 1.5% list price increase by arbitrarily moving their customer accounts up one notch from the 18%-off-list discount bracket to the 20%-off-list discount bracket (more than offsetting the intended effect of the price increase) ... and ... available-to-promise systems are misquoting delivery lead times, accidents that will also end up lining the pockets of Federal Express.

So, unless you hold shares in an exceptional company, the honest response to the questions from the annual meeting audience would be:

"Some of the information is probably just fine ... but ...
the rest of the data has needed
considerable attention for a long time.

Quite candidly, we don't know how bad the problem is
and we don't have any plans in place to find out."

Raising the volume on data accuracy

If the CEO brushes off the data accuracy questions at the annual meeting, it might be because he/she hasn't yet grasped the escalating strategic significance of the subject. Shareholders can rejoin the issue with these two indisputable observations: 1) inaccurate data will preclude robust enjoyment of B2B commerce opportunities, and 2) the likely stock price consequence of an unfavorable audit is not acceptable. In a nutshell, third party "enforcement" is more likely to change executive management attitudes about data integrity than another Oliver Wight sermon.

Compelling reality #1: B2B has put a picture window in front of corporate databases

B2B commerce over the web has been exploding ... it's an accelerating chain reaction. If a company in your portfolio (e.g. Thinking On Purpose, Inc.) gets on board with B2B, here are the implications for TOP data accuracy:

> *TOP's customers and suppliers are going to be connected over the web making decisions in real time using data in the TOP database. TOP's supply-chain-pertinent information will be "visible" as if were behind a picture window. If TOP's data accuracy is unsatisfactory, TOP's supply chain partners will gradually move up the irritation scale from "annoyed" to "furious."*

The size of the picture window is going to get enormous as business-to-business commerce expands. That expansion will be substantial. Why? Two good reasons: it saves big money and it keeps enterprises competitive.

- **Saves big money**

  An ambitious MBA with several months of experience and a hall pass to the customer service department could whip together a decent ROI analysis for web-enabling customer service between 9:00AM Friday morning and 3:30PM Monday afternoon. That analysis would be off by a few percent points, but even six months of fine-tuning by a corporate task force won't move the ROI result out of the "this-is-really-compelling/we-should-do-this-right-away" range.

- **Keeps enterprises competitive**

  B2B is a type of chain reaction ... as soon as one player in a market adopts B2B, the other market participants have to get on board fast. And the risk of non-adoption isn't confined to a productivity disadvantage ... market share is on the line too.

  The UCCnet Global Registry is another competitive chain reaction in the making; UCCnet is intended to lay the groundwork for a much more efficient B2B connection between retailers and their suppliers. Suppliers that don't embrace their customers' imposed rush to UCCnet will end up frozen out of the big retail chains.

  Wal-Mart and other large retailers are leading the charge on UCCnet because they are supremely tired of having about 3.5% of their volume wasted on returns and allowances (wrong stuff, wrong price, wrong codes, wrong promotion on the label, you name it). By this time next year Wal-Mart and Home Depot and others of that ilk have threatened to start passing out fines and penalties to suppliers who are caught with bad data in the Global Registry.

So, here are the net B2B consequences for IT: new classes of transactions, substantially more specificity per transaction, much higher transaction volume, and supply chain partner "enforcement" of data accuracy. That all translates to burgeoning responsibility for achieving and sustaining IT security and data integrity.

Raising the volume on data accuracy, *continued …*

Compelling reality #2: **shareholders will have conniptions when they read audit reports reciting findings about bad data and sloppy internal controls**

The Public Company Accounting Oversight Board (PCAOB) interpretation of the Sarbanes-Oxley Act was published in March '04. PCAOB requires external auditors to search for and report material weaknesses in internal controls/data integrity together with their written opinion on the financial statements.

Given what I've observed as a consultant, my opinion is that auditors who diligently follow the PCAOB guidelines will shatter the myth of management competence at a not inconsequential number of companies.

When shareholders see an audit testifying to inaccurate data and associated internal control voids, they will have a strong incentive to i) unload their stock positions as soon as possible and then ii) be receptive to a class-action filing against management to recover their losses. If that potential outcome doesn't compel CEOs to take data accuracy seriously, nothing will.

Information Technology's exploding things-to-do list

Even before the PCAOB interpretation of SOX was published, **a veritable alphabet soup of standards and acts of Congress and professional guidelines** were already moving the bar up on internal controls, data accuracy, data integrity, and IT security. Heavy IT involvement had already been a fact of life in health care entities struggling to comply with HIPAA, in financial institutions working on GLBA compliance, in manufacturing and distribution companies touched by UCCnet, in FDA-regulated enterprises coping with 21 CFR Part 11, in companies under the jurisdiction of two California statues, and in federal government agencies under the auspices of NIST 800.

Now PCAOB's arrival has added another item to IT's crowded things-to-do list. PCAOB's interpretation gives external auditors carte blanch to examine nearly every corporate business process. IT will be a preeminent contributor for both the SOX practice audits and for the "real thing" because business processes and their related data mountains reside on the enterprise computer.

It is true that the information technology department can't fix things like engineering standards or bills of material scrap factors or available-to-promise accidents without leadership from operational managers. Nevertheless, external audit analyses of the data will end up being supported by IT and interrogations about the security and integrity of that data will be scheduled for the IT conference room.

The final PCAOB Auditing Standard No. 2 document does not have an umpteen point "IT checklist for SOX." Without such a checklist, the scope of IT involvement will be constrained only by the imagination of external auditors who will have every conceivable incentive to plan very aggressive Sarbanes-Oxley audit scopes. (Auditors have all heard about the Arthur Anderson implosion.)

SOX as interpreted by PCAOB will be a full employment program for IT security administrators.

Shareholder's primer:
Information Technology preparations for SOX

If the CEO permits you to hang on to the microphone at the annual meeting, you could ask him/her if these two IT security questions have been put on the CIO's things-to-do list:

- **Presuming for a moment that the information in the corporate database is accurate, how is data integrity sustained?**
- **Can IT prove that crucial information in the database hasn't changed without the proper authorization?**

Those questions go to the root of how IT management can competently prepare for SOX in the absence of an "IT checklist" from PCAOB. The questions remain pertinent even if the jury is still out on executive management's data accuracy attitude.

Shareholders can feel comfortable that IT is preparing well for SOX if the following steps have been authorized. These executional steps are well advised based upon i) PCAOB published standards, and ii) good practice as defined by **the alphabet soup of compliance regulations** for systems security and data integrity.

a) Acquisition of a risk assessment from a respected *external* source so as to i) identify vulnerabilities in OS/400 security procedures, and ii) recommend strategies to mitigate identified risks. If the objectivity of the source and the quality of the documentation is judged to be exceptionally high, then PCAOB authorizes external auditors to accept the results without further testing.

   Click **here** to see information about **Bill of Health**® software

b) Addressing and resolving the vulnerabilities identified in point a).

   Click **here** to see a sample **up a notch**™ vulnerability assessment and mitigation report

c) Re-execution of point a) after the vulnerabilities have been fixed. External auditors will be impressed if both the pre-fix and post-fix assessment documentation is available for review.

d) Implementation of data integrity software that monitors all changes to crucial iSeries data so as to i) establish individual accountability for each change, ii) enable reconstruction of events, and iii) provide the what/when/where/how information needed to identify and correct internal control problems. Stitch

   Click **here** to see information about **Stitch-in-Time**® software

e) Implementation of a formal software change management system that sustains the disciplines of software life cycle principles and gathers ample data to answer any auditor questions about the movement, change, testing, and redeployment of programming objects.

   Click **here** to see information about **Tight as a Drum**® software

f) Careful assignment and documentation of ERP system usage authority to employees so as to sustain separation of duty disciplines and guard the integrity of data.

   If your company uses BPCS, click **here** for information about **By Invitation Only**®

Shareholders beware: the case for unintended outcomes

Congress passed the Sarbanes-Oxley Act for the purpose of bolstering investor confidence. But is it conceivable that SOX could end up having the opposite effect? My advice to shareholders is to stay alert as SOX audit results begin to appear this December. Here's why.

External auditors are likely to have a very uncompromising attitude about their SOX conclusions. In years past, controllers and CFOs jawboned for weeks to get unfavorable comments removed from the final audit letter and that intense pressure typically had effect. Now that we've lived through the Arthur Anderson/Enron/Worldcom meltdowns and auditors have 216 SOX interpretation guidelines from PCAOB, the jawboning isn't likely to be as effective.

> Nevertheless, it is possible that a few SOX auditors will succumb to management pressure to erase audit findings. As incredible as it might seem after Arthur Anderson's implosion, Deloitte stands accused of that and more in the unfolding meltdown of the large Italian company, Parmalat.
>
> Furthermore, it is possible that a few SOX auditors will drop the ball by failing to discover internal control voids. A 38-page questionnaire does not transform battalions of recent MBA graduates into seasoned/savvy internal control evaluators.

Judging from the fact that many millions of investors are still buying/holding common stock, there must be peace of mind about corporate internal controls. Perhaps many investors believe the worst has blown over and that a small handful of other problems will be ironed out by SOX. That could be a pollyannaish assessment.

I'm more inclined to believe that a disturbingly high percentage of listed companies will end up with "material deficiency" findings (presuming that auditor ball-dropping does not reach epidemic proportions). The myth of management competence will be shattered at those companies. Could six bad December SOX audit surprises generate a wave of investor uncertainty about the next several thousand SOX reports? Would twenty bad audit results knock the legs out from under investor confidence in the market? How could institutional investors justify the risks associated with sustaining positions in stocks with discredited management?

Epilogue

If he were still alive, Oliver Wight's perspective on all this would capture my attention. I think the third party "enforcement" of the data integrity principles he championed would be a bittersweet affirmation for him. I believe he'd be lamenting the enormous opportunity cost caused by decades of executive management indifference.

Questions ?

It would be a privilege to answer any questions about this opinionated commentary. Please contact Milt Habeck. Here's Unbeaten Path International's contact information:

Toll free North America: (888) 874-8008
International: +(262) 681-3151
Send us an e-mail (click **here**)

Unbeaten Path®