

## *Integrating health risk - group health or workers' compensation - into the corporate risk profile*

# The time has come

*Part 2 of a 2 part article*

By Ted Connolly, Robert E. Bossert and Andrew R. Reese

In part 1 of this 2 part series, the authors presented the case that there are no real procedural, methodological or technological barriers to the elevation of health risk, both group health and workers' compensation, to equal status with any other element of risk contained in a corporation's risk profile. The remaining myth we will confront in part 2 is the lack of availability and affordability of the sophisticated technology and security demanded by health care data. Quite simply, it's available now. The traditional defense against this reality is and has always been the "we're different" argument. We know of one large multi-risk insurance company that housed its' health and workers' compensation staff and

equipment in a separate facility jokingly referred to as "The Leper Colony." It is time to put an end to both that attitude and the traditional bias it represents.

It is often claimed that there are a combination of elements somewhat unique to the health care industry - the fact that medicine is primarily a cottage industry, that cost constraints are real (but so are the personal wealth statistics depending on specialty and business acumen,) or that operating margins can be narrow if you don't count pre tax profit or "foundation funding" (unless you are an insurance company complaining about cost escalation, anticipated risk escalation, and quietly banking substantial profits.) However, these characteristics are far from unique to health care. We face the same issues as many other indus-

tries. The same range of solutions is available. The technology and expertise is available, and innovations are evolving to make the transition into at least state-of-the-market if not state-of-the-art data and security management with manageable financial investment.

We are now seeing major credit card providers such as MasterCard and Visa, viewing Information Technology security for operational processes as well as product data bases as equally critical components to their very survival. Most are convinced that if they do not bring IT security technical services in to help "clean-up" and support their cyber security controls, they will not only suffer public embarrassment and financial loss but will likely be faced with restrictive and costly government regulations as well. As

(See page 12)

identity theft becomes a primary concern of most people who use a personal computer to do everything from paying their power bill and managing their bank account to communicating with their friends all over the country or even globally, the ability and extent of their providers to insure strong privacy and security is unquestionably their number one concern. We need to learn that lesson in health care and workers' compensation. It is an integrated problem with equal elements - all aspects of corporate risk and corporate information are at stake.

Our industry preoccupation with HIPAA has gotten in the way of recognizing the broader problem. We must recognize that risk data can be among the most sensitive information any corporation maintains, but it is far from unique. Security and privacy issues quickly go to a higher level when one addresses the vulnerabilities and risks organizations face with their financial and intellectual /knowledge assets (by most cyber predators, these are seen as "low hanging fruit")! Then there are the MOST IMPORTANT issues of National Defense and Homeland Security. We all saw what happened when a simple automated switch "miss-communication" took place in Ohio last year. The north-east USA went BLACK! We need to secure our risk data, our operating information and our computer systems. Security is no longer an "add-on-thought" we are all trying to bring into play — it IS the PLAY!

The field is growing more complex because the attackers are becoming more sophisticated and are using blended threat technology in their attacks. Blended threats represent the worst risks to computer security since the origin of computer viruses more than 20 years ago. Everyone has seen news reports about the recent Blaster and Slammer worms. Blended threats combine the most harmful characteristics of worms, viruses, Trojan horses and malicious code to exploit existing computer and Internet vulnerabilities. Many blended threats require no human interaction to spread, which accounts for their almost unbelievably fast infection rate. In addition,

blended threats are typically very malicious once they infiltrate and infect a computer. The Slammer worm, for example, created a denial of service that caused servers to become inaccessible.

Businesses today must use a layered approach to their technology security; this is referred to as security in-depth. From the client to the servers to the Internet gateway, security products need to be implemented at all levels of the network. But too many companies have already learned from experience that security technology alone cannot completely secure a network. In addition, the workforce should be trained regularly on how to identify and avoid today's sophisticated Internet threats.

Ever tightening budgets have thinned out organizational structures. Companies are doing more with less, but the requirements for properly organizing and implementing these technologies are expanding at a rapid rate. Making the wrong choice in technology and the proper management of it can be costly. In addition, laws and regulations are forcing organizations to formally document and demonstrate their full compliance or be fined.

Finding the right people with the management and technical skills to move the organization in the right direction is difficult - these are scarce resources. Major corporations are able to attract the necessary talent in most instances. The rest of us have a problem. If we are able to find that one special resource, today's organizational budgets often prevent us from hiring. The fact is, however, that there are solutions in place now that meet the need. It can be done today, and it is. We can no longer use the "we're different" defense to justify obsolete technology, obsolete software, and obsolete skills.

Grass roots efforts are currently underway with private and public companies, universities, law enforcement, and governments, all working together to provide the security and privacy necessary to make available talent and technology for companies on an efficient and cost effective

basis. One such effort is being led by Dr. J. Hanson, Vice President of Security Services for DynTek together with Florida Gulf Coast University.

Dean Richard Peggnetter, Dean of the College of Business at Florida Gulf Coast University (FGCU) had this to offer, "Universities have traditionally stimulated regional growth in technology and business development. The College of Business at FGCU, through its facility and our Center for Leadership and Innovation, has partnered with the DynTek Corporation over the past three years to bring forward a Center of Information Technology Security named the DynTek Security Research Lab. Through this important cooperation between university and industry partner, much needed knowledge and IT Security leadership will benefit our region as well as the entire worldwide computer industry." DynTek, Medical Technologies Group, and Case-Manager.net, Inc. are part of this effort.

## The Virtual CxO - a contemporary solution\*

"The Virtual CxO" is a service that can be tailored to meet any specific business needs at a reasonable and affordable cost. Let's take a deeper look into business requirements and what can be gained. Organizational structures expand and contract as enterprises strive to meet budgetary constraints. There is a defined structure of roles and responsibilities that all organizations follow depending on their size and stage of development, inclusive of the functions of Chief Executive Officer (CEO), Chief Operations Officer (COO), Chief Financial Officer (CFO), Chief Technology Officer (CTO), Chief Information Officer (CIO), Chief Security Officer (CSO), and Chief Privacy Officer (CPO). In the virtual model, we can refer to all of these positions with one acronym, CxO. When an organization is small, one person may perform several of these defined responsibilities. Some organizations might not

(see page 14)

■ **The Time Has Come** (continued from page 12)

even be able to address some of these roles and responsibilities. And yet they are vital.

Skill sets are a problem because often the people who possess the skills to perform one type of technical job may not have the skills to replace a technically competent person in another assignment. The result is often a mismatching of skill sets and abilities, placing technically-oriented people in management-oriented positions. The problem is further complicated when people with the necessary technical skills simply are not available and time constraints prohibit training anyone. The mismatch is perpetuated and organizations continue to struggle.

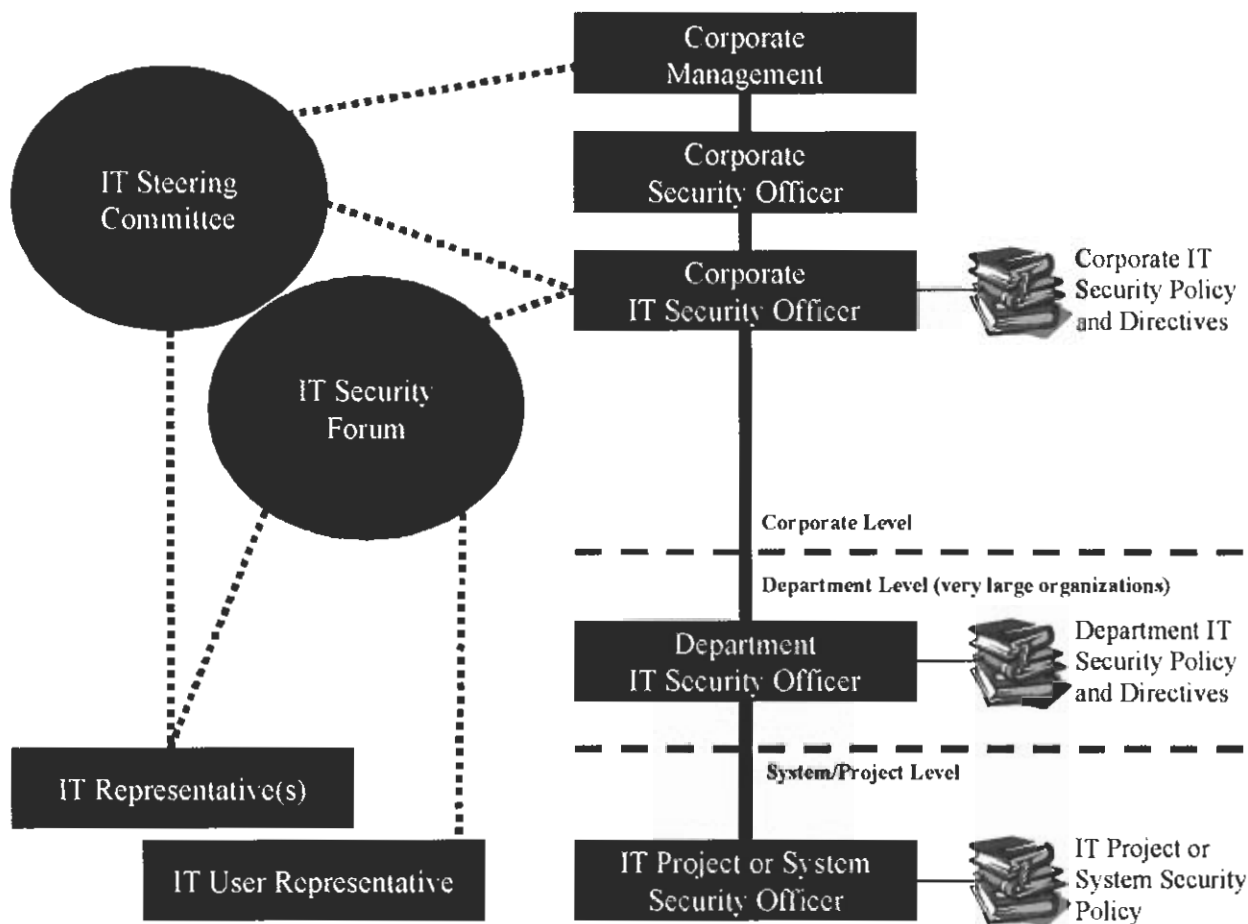
Experience is another basic problem. If we are talking about a straight forward technical responsibility such as managing a firewall or running a help desk for a

given application, finding and/or developing a qualified (certified) individual to assume a position isn't easy. Recruiting and/or developing a qualified (certified and experienced) individual to assume a position such as the Chief Security Officer (CSO) is a different challenge all together. The key word here is "Experienced". The job requirements and responsibilities of a CxO demand skill sets and experience not readily found. Yet according to most industry executives and together with a cursory review of new regulations across, are absolutely necessary for the security and privacy of today's technology based information systems.

The result is often a "piece meal" arrangement, with a few people wearing quite a few hats at the same time, struggling to stretch their limited skill sets and experience across the many and varied

responsibilities. All too frequently people with conflicting interests, limited skill sets and experience are tasked with nothing more than trying to accomplish regulatory compliance.

With all of today's new laws and regulations, from HIPAA to the Gram-Leach-Bliley Act (GLB) and the Sarbanes-Oxley Act (S-OX), it is critical for organizations to quickly bring their business operations into compliance. There are several industry standards that provide guidance regarding industry best practices, such as Generally Accepted System Security Principles (GASSP), International Standards ISO-17799 and ISO-13335; however, building a technology and security program to address the many laws, regulations, and industry best practices takes knowledge, experience, and process planning. It can't be done overnight, but it can be done quickly by



## Structure Defined by ISO-13335

using a small comprehensive team of experienced professionals who become the Virtual CxO.

The Virtual CxO service allows any combination of organizations to obtain highly skilled and experienced resources. The costs are spread across the participating organizations. The Virtual CxO service team essentially becomes each company's Chief Security Officer (CSO), working with each management and respective technical teams to continuously improve the participant's security posture, bringing the right technical and managerial resources to bear when and how they are needed.

The Virtual CxO Team fits into the organizational structure by filling one or several roles and responsibilities, such as: Corporate Security Officer (CSO), Corporate IT Security Officer (CISO), Department IT Security Officer, IT Project or System Security Officer.

The Virtual CxO Team can work with Executive Management, an IT Steering Committee or executive, and the corporate Security structure to develop methods and procedures based on industry best practices and standards.

The Virtual CxO Team provides participating companies with a multitude of technology and security services that in an IT marketplace that otherwise doesn't allow smaller and medium sized companies the ability to quickly implement a balanced technology security program that meets compliance requirements in a cost effect manner.

Times have changed - there will be no going back. Post 9-11 represents a totally new "category of challenges" to our technological world! If we are to survive this time of challenges to our business, let alone our lifestyle and still draw on all the advantages information technology has to offer, we must focus our attention not only on speed, application, and cost but also on privacy and security. The time has come to bring security and privacy to the forefront of Information Technology design standards and incor-

porate the contributions of industry, governments, and universities to add security and privacy to the availability, flexibility, and economic attractiveness of computer technology and the Internet. It can be done - it must be done. In the risk information business as well as virtually every other aspect of management information, nobody's "different" anymore.

\*The "Virtual CxO" is a concept developed by DynTek currently in use by authors.

*Observations From The Field is a commentary on items and issues followed by Case-Manager.net, edited by Gerald E. Connally, Chief Operating Officer. It is published periodically and distributed to a select list of clients and friends with whom members of our staff routinely exchange information and points of view. Comments, reactions, and even criticisms are welcomed. Feel free to call or write to discuss anything of interest or to obtain further information.*

*Gerald E. Connally is Chief Operating Officer of Case-Manager.net, Inc., a national network of superbly qualified and credentialed Nurse Case Managers who take a hands-on approach to meeting the needs of employees and families covered by group health plans.*

*He has over thirty-five years of management and consulting experience with considerable expertise in Health Care deliv-*



*ery. He maintains a continuous consulting relationship to small number of self-funded health plans, directing major case management, in addition to his operating responsibilities for the Company. He can be reached at (tel) 239-560-5527, (fax) 239-332-5571, or via e-mail at [tconnally@casemanagement.com](mailto:tconnally@casemanagement.com).*

*Robert E. Bossert: Chief Executive Officer*



*Mr. Bossert launched Medical Technology Group*

*(MTG) in May of 2003, after spending months developing the operating plan for MTG. Prior to joining MTG, Mr. Bossert was Chief Information Officer and Chief Technology Officer for Protocol Communications, a leading provider of marketing services, call center and material logistics. His responsibilities included business strategy, product development, consulting, marketing, sales, operations and general management. He can be reached at Medical Technology Group, 9040 Town Center Parkway, Suite 209 Bradenton, FL 34202 Phone: (941) 227-4200*

*Fax: (603) 849-3080*

*Email: [rbossert@medicaltechnologygroup.com](mailto:rbossert@medicaltechnologygroup.com)*

*Andrew R. Reese, <http://www.ReeseWeb.com>, is National Director of Security Consulting, DynTek, Inc. He is the Symantec Regional Partner Council Member representing the United States as well as the Symantec Global Partner Advisory Council Member representing North America.*



*Mr. Reese is a Certified Information Security Manager, nationally recognized security expert, having performed numerous detailed security assessments and audits and authored and developed structured corporate information security policies that adhere to industry best practice, laws, and regulations, such as: HIPAA, GLB, S-OX, GASSP, ISO-17799, and ISO-13335. Has chaired technical advisory committees for Raptor Systems and Axent Technologies*