An Executive Overview of Enterprise Security

"We live in an age that is driven by information. Technological breakthroughs... are changing the face of war and how we prepare for war."

-,former U.S. Secretary of Defense, William Perry

The cold war was political. It's over. World War III is an economic war. It's here - it's now. Information is where the money is and theft is easy, safe, and lucrative. Eavesdropping and other high tech related crimes are difficult to enforce and prove. Advancements in electronics and optical electronics have made communications interception easy and cheap. Business ethics don't have the same value as they did in the good old days of the "deck of punch cards" computing.

IT and business security is becoming more and more critical in today's commercial environment. Every day we are faced with new computer risks, viruses and new "ideas" from hackers on how to gain access to our network or other systems or physical locations. Fortunately, there are even more sophisticated business solutions out there that can be implemented to secure us from these dangers. These can be anything from simple firewalls up to very expensive encryption and biometric authentication solutions or remote communication modules. These new business realities affect you as much as it does your competitor - no matter what your line of business. The question is how can you protect your organization, no matter how large or small, from the known and unknown security dangers and risks to remain as competitive, and therefore profitable as possible?

What about all the other business risks that are also getting more sophisticated? Have you considered all the risks that cannot he covered by technology? What about the human side of business? No business can function without the human touch. Yet how do you know when that necessary "human touch" is about to reach out and touch you in the form of an "insider" attack? Have you thought about your employees behind the technology? How about social re-engineering forces or disgruntled employees? When did you have your last corporate risk assessment completed or even considered if ever?

As a person you are prepared for the unexpected: you face the unexpected several times a day without giving it a second thought. You follow the rules of the road when you drive because you know it is the right thing to do. You purchase insurance for yourself and your car, carry health insurance and life insurance because you know it is the right thing to do for your family. Unfortunately, with many of the business risks of today there is no "red light, green light" to tell us when to stop arid when to go. But how can you say you are sorry enough to your customers, when you have to tell them some hacker has posted their credit card number on the hackers web site? When it comes to your organization or business, have you put the same level of consideration into how

your employees and customers will continue to rely on you should the unexpected happen?

If you're like the Senior Executive or owner of most companies, the answer may be a frightening "No, we have never had any comprehensive business risk assessment completed." Or worse yet, perhaps you have a false sense of security in a plan that was developed several years ago. With all we hear about how high the price of security can be these days you may find yourself saying, "Investing in a security and privacy solution is expensive; too expensive for our organization or business right now." But can you afford to risk spending more than 15, times the cost of preventing a security breach or a communications breakdown when the unforeseen does in fact happen?

Proactively preparing your business with a comprehensive security assessment and plan is far less expensive. According to David Bauer, first vice president, chief information security and privacy officer at Merrill Lynch, a key component of any strategy is a dynamic risk assessment. By using tools such as scanners, log analysis, risk metrics and asset inventory that produce a biweekly security report you can more quickly analyze and prioritize current or potential threats. This approach allows organizations to move from a circle-the-wagons approach to intelligent risk management.

With an intelligent risk management solution the percentage of the IT budget that needs to be spent on effective risk protection is actually far less than what your competitors will be forced to spend. The answer is not about how much you spend but how well you spend it. This way about half the spending is advisory, helping build secure systems, while the rest goes toward risk management, prevention and response. For instance it is easy to get somebody's password, so the damage that can be done by an individual has to be as small as possible. William Farrow, CIO at the Chicago Board of Trade, told how a woman cleaning a conference room became suspicious of a laptop left running overnight. She reported it to security, and it was later discovered that someone had left the laptop running port scanning software aimed at penetrating the corporate computer network. In this case even an employee at the lowest level of the corporate structure was made aware of the potential damage that can be done to the organization with a security breach. In corporate or IT security, emotional reactions, panic and legislation are counterproductive. But intelligent approaches can safeguard your organization or business from an uncertain future and substantial financial losses.

If you ask CEO's of large corporations, who have gotten even low-level employees to be savvy about security, you get advice on employee education: "Make it a part of daily conversation in every project meeting. Make it clear that every project has responsibility for security. You have to make it part of day-to-day operations." Adherence to clearly defined security principles should be a part of each employees contract. It is also important to publicize employee caused security incidents internally, not necessarily naming the employee who made a mistake, but doing it in a way that others learn from the error. Those organizations or businesses that have evolved a system of process improvement as a natural consequence of their business

demands are those organizations or businesses that will excel and win the security wars.

The main key between companies that have implemented a dynamic security plan and those who have not is: preparation. Preparation requires a focus on risk management, intelligence-driven identification, prevention and response. A good organizational or business security strategy is built around these principals: threat management, including intelligence, planning and instant response; comprehensive security services; attention to public policy, including active attempts to educate legislators; and an agile response to the changing risk environment. After all, as we have learned, an intelligent security response needs to be everyone's responsibility and it is not always limited to technology and IT security that matters the most.

By Dasha Deckwerth
Stealth - International Intelligence Security Service Inc.
www.stealth-iss.com

About Stealth - ISS® Inc.
Stealth - ISS®, headquartered in Tampa, FL., is a privately owned Information Technology security consulting company with main focus on regulatory compliance, security integration, security consulting and managed security services for both government and commercial customers.
Founded in 2002, the company has earned an outstanding reputation for professional security services including vulnerability assessments and regulatory compliance such as Sarbanes-Oxley, HIPAA, NIST and ISO standards. Stealth – ISS® also recently expanded its data center services providing faster and secure hosting and colocation solutions for customers worldwide.
Stealth - ISS® has partnerships with several leading manufacturers of various security applications and products and was awarded the NATO BOA agreement in 2003.

About the Author
Dasha Deckwerth is the CEO at Stealth - ISS, with extensive experience in international business and computer security. Prior to her position as CEO, Dasha had gained extensive international business experience in various European, Asian and Central American countries and later became the VP of Marketing and Business Development at Stealth - ISS® in Berlin, Germany. She also worked on several projects as security and regulatory compliance consultant in the commercial sector as well as for various NATO countries and government agencies. Dasha's current focus includes managed data center services, knowledge management, regulatory compliance applications and services and security implementations and consulting. Mrs. Deckwerth holds a B.A. in International Relations and Foreign Affairs from Eckerd College, is currently pursuing an MBA in IT Management from Touro University and speaks six languages.