APRIL 2004

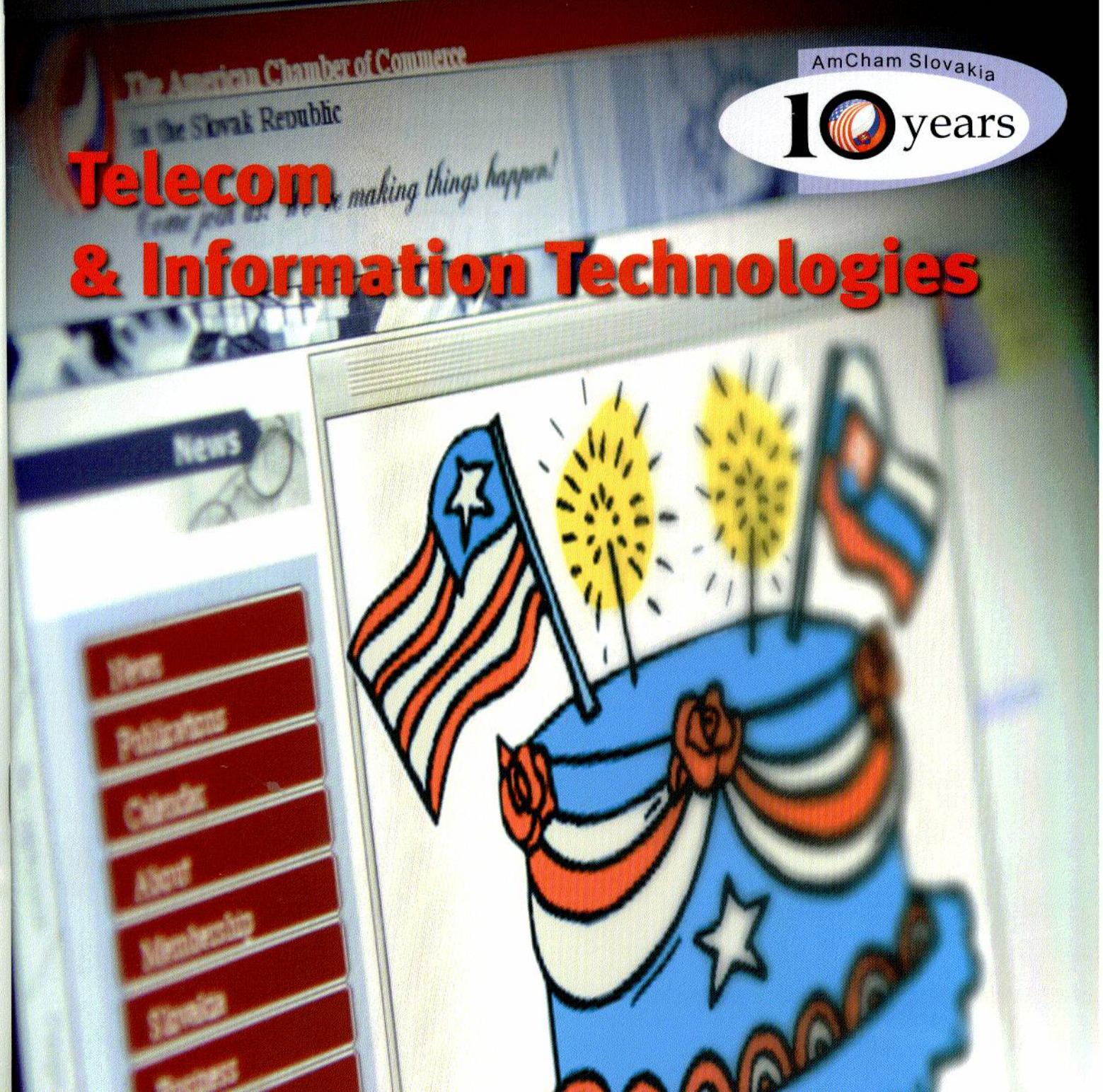
THE OFFICIAL MAGAZINE OF
THE AMERICAN CHAMBER OF COMMERCE IN SLOVAKIA

CONNECTION

WWW.AMCHAM.SK

AmCham Slovakia
10 years

Telecom & Information Technologies



An Executive Overview of Enterprise Security

Prepared by AmCham Member:

"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 be 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 and 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 pro-ject 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.

Dasha Pribylova
Stealth - International Intelligence Security Service Inc.

Internet for Business

EUROWEB

Communication is the life of business

Communication is the most characteristic phenomenon of the times we live in. To ensure optimal processes within a company it is necessary to pay attention to all aspects of communication. The success of a company depends on effective communication, especially in the dynamic and turbulent environment that business creates. Therefore, effective communication and the availability of relevant information has become a basic business value. Investment in this area is the most important factor to be successful and competitive.

Small business

Dynamic time management, a lot of different information, data and all requirements needing an immediate response – these are characteristic features of all small businesses. Your competitors and potential customers can be found in the virtual environment of the Internet. Access to information is a requisite for progress and every idea has market value. Communication through the Internet creates databases available for future decisions, analysis or monitoring. If you are part of this business, you can choose from options to make your communication and decision making process smoother and faster. To cover the communication needs for such a company size it is strongly re-commended that you use a high-speed broadband Internet connection with DSL technology, which enjoys the interest of the Internet community all over the world. This service, introduced to the Slovak market last year, allows unlimited access to the Internet at high speeds with economical prices.

Medium and enterprise business

For medium and enterprise businesses different technological solutions using various technologies such as FWA, MW or digital line can be provided. For businesses with international scope there are advanced solutions available to centralize administration. The Internet allows for Virtual Private Networks for interconnection to headquarters and all subsidiaries with appropriate data and information security. This solution supports the decision makers with appropriate and updated information about all internal processes such as stock management, accounting, etc. All subsidiaries are connected to one server and work with online, real-time information. The management of such a company is provided with flexibility and valid data to support their analysis and forecasts as well as with the cost savings achieved by effective logistics and excellent management. As a result, the customer gets impressive competitive advantages – effective communication, increased reaction time and competitive prices.

EuroWeb Slovakia, a.s. – a leading business Internet Service Provider

EuroWeb Slovakia, a.s. is the leading business Internet Service Provider in Slovakia, providing Internet connections, complex international Internet services, and business communication solutions. The establishment of EuroWeb Slovakia a.s. has resulted in the co-operation and joined forces of top professionals who were present at the emergence of the Internet in Slovakia. Extensive experience gained on the market since 1991 constitutes a firm basis for ongoing development and growth of the company. EuroWeb Slovakia is a subsidiary company of EuroWeb International, the leading regional business ISP in central Europe, whose majority shareholder is Royal Dutch KPN Telecom communication company. EuroWeb International manages operating companies in the Czech Republic, Slovakia, Hungary and Romania. EuroWeb Slovakia, a.s. is a member of ICANN, the organization which allocates domain names, and the national registrar of Top Level Domains (TLD) in Slovakia. The aim of the company is to provide the highest quality services and full coverage of Slovakia with a reliable network.