Keynotes

Profitable Information Security Policies

Edward Humphreys[1]

When you go to Japan you hear businesses talking about implementing "ni nana zero zero ichi" and the benefits they have gained from their endeavors of implementing information security management systems. The same business excitement can be heard in other Asian, North American, European and Middle-eastern countries. So what is this buzz all about? Quite simply implementing information security policies that enable businesses to do well, to take business opportunities that are profitable. These companies are all talking about implementing ISO/IEC 27001 the international standard on information security management which has become the common language for securing their business operations and engaging in profitable business relationships with their clients, customers and business partners.

So what does it mean to have a profitable information security policy? Clearly a company is in the market to make profits, to have a viable business future, to be the best of its kind in the marketplace and to protect its current investments and invest in new business opportunities. As they say information is an important business commodity which can be bought and sold, and like a currency, helps your business to make its profits, to invest in future business opportunities and to protect itself in the marketplace. Having the right information, at the right time and appropriate use of this information can be driver for a company to become richer and more profitable, to better its market position and for self preservation. A company is in the business of taking risks, to make profits, to be a viable market player and to be 'best of its kind'. Every time it makes an investment, makes a management decision to offer a new range of products, offer new services, to back new opportunities the company is taking a risk. A profitable information security policy should be able to help the company to take the business risks it needs to take without worrying about the protection of its business information - that information it uses to run its business and the same information it uses to formulate its business strategy, make well-informed business decisions and to maximizing its business opportunities.

Therefore the lack of a viable information security policy or an information security policy ill suited to the business can be detrimental to the business, its hopes and vision, and its future business plans. A profitable information security policy should balance out the maximum protection it needs to protect against the risks to its business information, that is to minimize its security risks, and the minimum protection it needs for it to take the business risks it needs to take for the good of the company that is to maximize its investments

[1] Visiting Professor at Hagenberg University of Applied Sciences, Austria and BIT University Beijing, China, and Chair of the ISO/IEC JTC1/SC27 working responsible for the ISO information security management system standards.

B. De Decker and I. Schaumüller-Bichl (Eds.): CMS 2010, LNCS 6109, pp. 1–3, 2010.

and opportunities. So a profitable information security policy is a risk-based strategy and instrument that will ensure that profitable benefits will accrue if the policy is implemented by the company. Of course this policy be designed in a way that reflects the company's business vision and objectives.

This keynote talk goes through the past, present and future of ISO/IEC 27001 from its early beginnings as a British Standard to its rapid rise as the most successful, best selling international information security standard of all time to hit the international business community. It is a standard that companies around the global have used and continue to use to design their profitable information security policies.

The Impact of Cryptographic-Hardware-Research on Development of Next Generation Firewalls

Klaus Gheri[2]

The old network firewall paradigm has changed significantly. Today's next generation firewall no longer contents itself with making a traffic flow decision based on information readily available from packet and protocol header information. Additional computationally intense and latency critical traffic flow processing is required to determine the very nature of the application causing the traffic and to inspect the application data payload for data leakage, malware or exploit patterns. Since HTTP and its SSL encapsulated counterpart HTTPs have become the de-facto standard transport protocol for a huge number of applications these protocols need to be closely inspected. Especially for HTTPs the application protocol inspection involves a significant amount of CPU processing power. Furthermore a massive crypto load stemming from high bandwidth VPN tunnels and data compression must often be handled by the same device. With the market moving to full duplex wire speed performance requirements of 20 Gbps or more with all detection technologies switched on economically viable and future proof concepts for task acceleration are needed.

Network and Security Architectures - What Works, What Does Not, and What is Really Missing

Taher Elgamal[3]

Information security has grown from a few tools to protect enterprise networks to becoming an integral part of conducting commerce. This presentation provided the overall network and security architectures as they progressed over the last 15 years. The introduction of Internet connectivity in all our business interactions has required the industry to modify its thinking when it comes to securing the networks. This presentation also provided an overview of what worked, what did not work and what is really missing. Special attention was given to the new

[2] Chief Technical Officer, phion AG - a Barracuda Networks company.
[3] CEO of IdentityMind and CSO of Axway Inc.

waves of online fraud and intellectual property theft attacks. Some very well-known sites have been successfully exploited in the recent months, together with growing online fraud due to the exposure of private and confidential information. The presentation provided insight into why such attacks are possible and why are they successful in today's environment. A call for an improved security model with certain new controls can improve the situation and help organizations mitigate against these attacks. There are many existing technologies and commercial products that can help solve these issues, however, the deployment and implementations may be difficult or introduce unnecessary steps to hinder the use of these products. We discussed issues in authentication, access control, and network and application layer defense as well as various content protection and security ideas. There are still many open issues in solving the overall problem. We also discussed the how the use of the Internet to conduct commerce has opened many security issues. Areas for further research and development were discussed especially when it comes to securing content.

Statement from the Industrial Sector

"After a 10 year long research career as a theoretical physicist in quantum communication I was all set and on track for a life in academia. But I decided against the obvious and instead started up phion with a few colleagues. We grew the company in EMEA, went public and last year merged it with Barracuda Networks. This makes another 10 years of my life. In both these work lives I have been deeply involved in R&D both on the doing and management sides. Context and constraints of R&D were however widely different. Basic research as is done over years with great sophistication within academia is virtually impossible to conduct in a commercial environment. Economic constraints, much shorter timescales and a pushier socioeconomic environment require a very pragmatic approach in commercial product development. Therefore conferences such as CMS 2010 are immensely valuable to all of us in the industry because here we can learn firsthand about profound leading edge research, establish relationships on a personal level, and also get a chance to feed back our views and needs to the research community."

Klaus Gheri, Chief Technical Officer, phion AG - a Barracuda Networks company.