

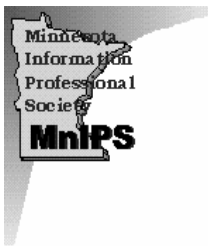
# Business Security

## How much is enough?

### Assess / Develop / Protect



8:30	<b>Introduction and Welcome</b> <b>Joe Perzel, Energi</b>
	<b>8:40</b> <b>Defense in Depth: Enterprise Information Security in Challenging Times</b> <b>Dr. William A. Estrem, University of St. Thomas</b> Dr. William A. Estrem is an Associate Professor in the College of Business at the University of St. Thomas. He holds the Honeywell Endowed Chair in Global Technology Management and is the director of the Information Technology Management concentration in the MBA program. Dr. Estrem is a senior member of the Society of Manufacturing Engineers and the IEEE Computer Society. He is also active in several industry standards organizations. His current interests relate to distributed computing architectures such as Web Services and Grid Computing.  This presentation will highlight key issues addressed in more detail throughout the conference. How can organizations manage their Information Technology assets to protect against a variety of threats? What guidelines, standards, and best practices exist to build coordinated multilevel security architecture? What are the key trends, opportunities, and threats that will affect organizations in the future?
	<b>9:25</b> <b>Security Assessments: Standards-Based and Measurable</b> <b>Jon-Louis Heimerl, Espiria</b> Jon-Louis Herimerl, CISSP, is the Principal Security Consultant at Espiria. A graduate of the University of Wisconsin, Eau Claire, he received his Certified Information System Security Professional designation in January 1997. Since 1985, Mr. Heimerl has designed security programs and program elements, and performed assessments or training for multiple Fortune 500 corporations, including international operations, as well as local and federal government. He has worked as a commercial consultant in the insurance, healthcare, financial, retail, e-commerce, educational, legal, manufacturing, communications and high tech industries.  This presentation will explore the “whys” and “wherefores” of assessing security. Mr. Heimerl will help us understand how to evaluate our security. He will explain existing security standards and measurements.
10:10	Break
	<b>10:25</b> <b>IT Security – Where’s the Value?</b> <b>Brett Nelson, Midwave</b> Brett Nelson has an extensive background in information security, e-commerce, firewalls, PKI, and smart cards. He is a Certified Information Systems Security Professional (CISSP). Before joining Midwave Corporation, Brett worked for Datakey as Director of Product Management. Prior to Datakey, Brett worked with Ernst & Young as manager of Information Systems Assurance and Advisory Services for e-commerce. Prior to Ernst & Young, BN was the director of marketing for Digital Privacy, Inc., a smart card software vendor creating smart card-based authentication and encryption products.  Effective security can provide you competitive advantage, but first you need to understand its value to your organization. An effective security program entails establishing metrics to align business, technology and financial objectives, while simultaneously providing protection commensurate with the associated risk tolerance, asset valuation and business impact. This session will address techniques to recognize the quantitative and qualitative value proposition surrounding your security program.



# Business Security

## How much is enough?

### Assess / Develop / Protect



11:10



#### **Practical Threat Management: Theory vs. Reality**

**Michael D. (Mick) Bauer, CISSP**

**Network Security Consultant, Upstream Solutions Inc.**

Mick Bauer is an information security consultant for Upstream Solutions, Inc. in Minneapolis, Minnesota. He is also Security Editor for Linux Journal Magazine, and lead author of its monthly "Paranoid Penguin" security column. O'Reilly & Associates has just published his first book, "Building Secure Servers With Linux."

Mick's areas of expertise include Linux security and general Unix security, network (TCP/IP) security, security auditing, and the development of security policies and awareness programs.

Effective risk management is essential if you wish to most effectively direct your information security efforts and budget.

Risk-management techniques used in more mature fields (e.g., civil engineering) don't necessarily translate well to information security; the ones that do aren't widely used or even understood by the people "in the trenches."

In this presentation, Mr. Bauer will describe and demonstrate some of these techniques, in plain English and with practical examples. He will also describe some new developments in information security risk assessment that may address some gaping holes in current methodologies.

12:00

LUNCH



#### **Home Security Today: Brief remarks with your questions answered.**

**CCTV Technology: The latest equipment and why it matters today.**

**Jon Barnett, EdinAlarm Inc.**

Jon Barnett, President & owner of EdinAlarm Inc. has 18 years experience in the design and installation of security equipment for business and residential applications. Providing protection for 1500 clients throughout the 10 county metro area Jon's expertise includes Bank security, UL 2050 defense contractor installations, data centers and various other special needs applications.

Jon will focus on home security as well as demonstrate the latest in CCTV for business applications. Please bring any questions you have regarding home or business security.

1:00

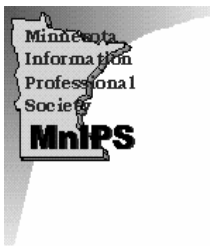


#### **Corporate Security Basics**

**Richard Bonneville, PC Solutions**

A 24-year veteran in the local data communications field, Richard Bonneville holds the CISSP Certification (Certified Information Systems Security Professional). Before taking the helm as the leader of the Network Services Group at PC Solutions, Richard held various positions including Corporate Security Officer and Senior Security Analyst. Beyond his day-to-day activities at PC Solutions, Richard now advises Minnesota companies, small and large, who recognize a need to protect their sensitive information and business processes.

Mr. Bonneville will be discussing the basic steps needed to secure a corporate environment, including both technical controls (firewall, intrusion detection, etc.) and administrative controls (corporate security policy, password construction, acceptable usage policy, etc).



# Business Security

## How much is enough?

### Assess / Develop / Protect



1:30



#### Organizational Security – When People are Involved

**Michael Ellsworth, StratVantage**

Mike Ellsworth is Managing Principal of StratVantage Consulting, LLC, where he helps companies make better technology decisions about emerging technologies like security, wireless, mobile computing, and eBusiness. He has helped senior company leaders from the Fortune 500 on down to startups create an effective information technology strategy and connect it with their business. In addition to starting StratVantage, Ellsworth founded CTOMentor, a subscription-based emerging technology advisory service targeted at small to medium size businesses that delivers personalized news, information and analysis to technology decision makers. An award-winning writer, he has contributed to two technical Internet books. He is a frequent speaker at technology industry events. He holds a B.A. in Psychology from Duke University.

One often-overlooked component of the security picture is organizational security, which encompasses what people do to ensure adequate network security. All the routers, firewalls, and security gurus in the world can't help if your people post passwords on their monitors or don't understand their role in ensuring security (the "human firewall" concept). This presentation describes an organizational security audit process that provides an organization with an understanding of how well equipped it is to prevent and deal with digital disruptions of key business processes from the perspective of policies, procedures/administration, and people. Hardware and software to aid in education and policy enforcement are briefly discussed.

2:00



#### Homeland Security – A Minnesota Perspective

**Jeff Luther, MN Homeland Security Coordinator**

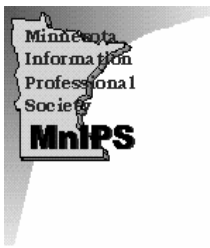
In 1983, after serving as an emergency paramedic, deputy sheriff and later as a patrol officer, Jeffrey Luther began his career with the Bureau of Criminal Apprehension, as a Special Agent. In 1990, Jeff was assigned to the Training and Development Section and promoted to Senior Special Agent in June 1998. In March 2001, Jeff was promoted to Special Agent in Charge and assigned to supervise the Special Operations Unit. The Special Operations Unit is responsible for the investigation of crime scenes, computer crime investigations, and technical and surveillance support. SAIC Luther served as the Emergency Response Team Commander.

In September 2002, Public Safety Commissioner and Homeland Security Director Charlie Weaver appointed Special Agent in Charge Luther to the position of Homeland Security Coordinator for Minnesota. Jeff is responsible for the coordination of state and federal efforts in Homeland Security.

Providing for security of our homeland is a complex challenge that demands significant investment and collaboration among local, state, and federal governments and integration with the private sector. This presentation will familiarize the attendees with the Minnesota Office of Homeland Security and our strategy to deal with the challenges that face our citizens during these difficult times.

2:30

Break





# Business Security

## How much is enough?

### Assess / Develop / Protect



<p>2:45</p> 	<p><b>How and When to Utilize Biometrics</b>  <b>John Nugent, Cybrix</b>          John Nugent, Senior Account Executive has over four decades of experience working for financial institutions and information technology consulting companies in technical, managerial and sales capacities. John’s IT security experience includes responsibility for establishing data security and disaster recovery plans for NORWEST Bank (now Wells Fargo), where he coordinated the entire data processing recovery during the 1982 Minneapolis bank fire. He has moderated seminars and made numerous speeches, nationally and internationally, on computer security and disaster recovery planning. John earned his BA degree from Metropolitan State University.</p> <p>Presentation will cover Biometric technologies and a brief history of device evolution. Industry use and a comparison of products, from Fingerprint to Smell Recognition will be discussed. Coverage of types of products with False Rejection Rates (FRR) and False Acceptance Rates (FAR) will likewise be reviewed. Wherever possible some cost(s) will be looked at.</p>
<p>3:15</p> 	<p><b>Security Tools and the Power of VPN</b>  <b>Michael Kelly, Norstan Communications, Inc.</b>          Michael Kelly has over 18 years experience in the Information Technology industry. He has a breadth of experience from software development, to application integration, from project management to systems and network management. Michael has built his own consulting firm focusing on enterprise management technologies and services and in particular, network and security management. Currently, Michael is responsible for the ongoing development of management services at Norstan, Inc. including security, network and systems management; focusing on the Converged Technologies industry – Voice Over IP and IP Telephony.</p> <p><b>Security Tools and the Power of the VPN</b> focuses on practical tools – applications, processes and procedures – that can be applied to any size corporation wrestling with mounting fears of digital security. As well, the Virtual Private Network (VPN) is defined and applied to real world situations to help the audience understand how this technology can enable a more nimble and flexible enterprise while saving precious IT funds.</p>
<p>3:45</p>	<p><b>Q &amp; A Panel</b>          Jeff Luther          Bruce Glasrud          Dr. William A. Estrem          Bob Burkhart</p>
<p>4:30</p>	<p>Dismissal</p>