



Speaker Topics & Speaker Bios

On the following pages, please find a list of topics that Perimeter can present followed by our Speakers Biographies.

NOTE:

Perimeter can present each topic in any of the following formats:

- Educational Online Webinar
- Live Presentation at a Scheduled Event
- Live Full Day Seminar Scheduled Upon Request

Topics & Descriptions

Is Your Institution At Risk?.... New Online Risk Modeling Tool Helps Institutions Profile Their Business Processes and Areas of Risk

The Risk Profiler allows Financial Institutions to evaluate their business risk for the purpose of examinations, audits, board reviews, best security practices, technology reviews and budgeting. This tool helps the Financial Institution to create a business profile of each of the business processes, and evaluate their risk (high, medium, or low) within each of the following areas: financial, compliance and reputation. Then the Financial Institution answers a few questions regarding accessibility and selects which technologies are currently employed to mitigate the business risk. A full report including an executive summary and technical detail is generated on the fly. The report details areas of best practices, high, medium, and low risk, as well as a breakdown by business process of what technologies could be employed to increase security, network availability, and compliance. The Risk Profiler is valued at \$750/year BUT you get UNLIMITED access FREE just by attending the webinar.

So You Think You Are Secure: Information Security Risks and Financial Institutions

Protecting your institution's network infrastructure is critical, but how do you know if your network is secure?

During the presentation, Susan Orr explains the numerous information security risks and threats, what examiners expect, and what you should do to protect your institution. She will cover current headlines, risks facing institutions, regulation, and the needed controls.



WiFi – Is Your Institution At Risk?

With over 50 million people having Wi-Fi access (according to the Privacy Rights Clearinghouse (PRC) in San Diego), a new form of cyber theft is born creating new security risks and challenges for financial institutions. ChoicePoint Inc., a company that stores consumers' financial records, revealed that thieves had accessed information on some 145,000 people. The announcement began a round of similar revelations and sparked interest in the security of commercial, government, and other databases.

So how do you know if someone is accessing your network via their WiFi? Is there such a thing as a Secure WiFi? Susan Orr will answer those questions and explain the potential risks of WiFi and best practices to secure your institution.

Policy Enforcement and the Next Frontier of Network Security

With faster exploits, the growth in external applications and the increase of mobile and remote users, your institution's security is becoming less and less effective over time. Does your institution have the visibility, analysis and control capability to effectively enforce security policies? Andy Greenawalt, CTO at Perimeter Internetworking™ will help the audience understand how to enforce policy and patch policies with tools that help to identify security gaps to ensure your institution does not have "back door" vulnerabilities. Andy will also share with you some of services and tools Perimeter Internetworking™ can provide your institution to enforce policy and match management.

Decrypting Security Reports

The lack of an appropriate security documentation process, including developing summary reports for Senior Management and the Board, is one the most common deficiencies cited in examination and audit reports. In many cases, organizations will use a firewall or IDS log as their periodic summary and update. What do your current security documentation reports look like? Are they geared towards the appropriate audience? What are your examiners and auditors looking for? How does implementing appropriate security incident documentation tie in with other regulations and regulatory guidance?

In this session we will review best practices for documenting security incidences for your Credit Union. We will also take a close look at appropriate reporting frameworks for:

- Security Alerts/Events
- Vulnerability Assessments
- Executive Summaries/Briefings

Email And GLBA Compliance

Learn how to Protect your Email with Encryption, Content Filtering, Archiving & Spam Control. We will focus on the regulatory importance of securing your email. You will learn how to protect your institutions outgoing email with encryption and content filtering tools. You'll also learn the importance of email archiving and how to battle spam. In addition we will outline the importance of establishing and enforcing your institutions email security policy and discuss the inherent security problems of email and the need to establish and enforce policy. Perimeter Internetworking will then focus on best solutions to ensure that sending secure emails are policy driven and consistent with the privacy requirements of the Gramm Leach Bliley Act.

Taking Security to the Desktop

Malicious code, such as worms and viruses, are assaulting your network. Security flaws are uncovered seemingly hourly, thus patches and updates are created before you're even aware of the latest attack. Are your desktops kept secured? Join Jerry Piatkiewicz, Senior Security Consultant at Perimeter Internetworking™ and find out if your desktops are secured. Jerry will also share with you some of services and tools Perimeter Internetworking™ can provide your institution to protect your desktops and your network.

- ***Viruses, Trojans, Worms - Why Isn't My Desktop Anti-Virus Enough?***

While the world is a better place because of the increasing speed of computers and networks, it is this same speed that makes computer viruses so effective and dangerous. Given this reality, the time to react to new viruses is becoming more and more critical. Jerry, will provide the audience with a better understanding of how malicious code spreads and how an institution can close the window of exposure and better protect against the spread of viruses. Jerry will also share with you some of services and tools Perimeter Internetworking™ can provide your institution to better protect your network from viruses, Trojans and worms.

- ***Hacking Demonstration: Why Your Firewall & Intrusion Detection Aren't Enough***

Jerry will describe some of the new developments in hacking trends. He will use these developments to demonstrate some of the techniques of modern hackers and help the audience better understand how to effectively protect against such hacking methods.

Developing a Proactive Security Program To Meet Regulatory Compliance and Best Practices

The lack of an appropriate security program including the implementation of appropriate controls and monitoring to protect information assets is the most common deficiency cited in examination and audit reports. What are your examiners and auditors looking for? How does implementing an appropriate security program tie in with other regulations and regulatory guidance? What are the risks of not having an appropriate security program? What are the critical security measures to have in place?

Not On My Watch...Bringing True Security to Web-Based Systems

Protection of an institution's most important asset – its customer information – is necessary to establish and to maintain trust and confidence between the institution and its customers. Daily possible exposures and vulnerabilities threaten web security and these assets. Is there a single security control to adequately to protect information assets? Does reliance on insufficient controls create a false sense of security? Are systems compliant with new Web security regulations? This presentation will focus on best practices to implement for web security and will provide recommendations on how to achieve the appropriate layers of control and monitoring. Don't be caught off guard on your watch.

Getting the Most Out Of Your Firewall?

The latest in firewall technology, what it can do, can't do, and is your firewall doing it? What are the common limitations in firewalls and how to mitigate those issues. Also a few things you can do on most firewalls to improve your security today without spending any money.

Intrusion Detection and Prevention

The void and limitations of firewalls drive the need for IDS/IPS protection. But with so many different providers, technologies, etc. how do you know what to pick? Learn the basics of IDS/IPS. Do you need it? Where you should put it? Do I need it managed and monitored, or can I do it myself? What technology should I use?

Virtual Private Networks

Learn how you can both save money and increase your security posture with the use of VPN's. Many providers and partners are requiring VPN connections, including the Fed's. Learn how to deploy these VPN's in a secure way, that will stay within regulation compliance. Also learn how you can use this technology to telecommute, or work while traveling.

The Latest Internet Security Threats & How to Protect Your Network / Hacker Attack Methods

Learn some common hacking methods. See a step-by-step approach of what a hacker can learn about your network and users that will assist them in an attack. See freely available Internet resources and tools they use to scope and probe your network. Then learn what you can do to protect yourself from these threats.

Unified Threat Management, the Latest in Internet Security Protection

Learn about the latest in Internet security protection, Unified Threat Management (UTM). This technology allows a customer to build multiple layers of security within a single physical device. This consolidation of technology creates a faster, more reliable network while stopping the latest security threats from both inbound and outbound from your network.

Phishing and Pharming

Learn about Phishing and Pharming attacks. Understand the realities behind Phishing and current statistics. See information regarding real Phishing attacks and the step-by-step approach used by attackers. Then learn what can be done to protect your member information.

Vulnerability Assessments

Learn the difference between a penetration test, vulnerability assessment, and full risk assessment. Find out what examiners are looking for specifically. What should you expect from these tests and reports.

OTHER TOPICS PERIMETER CAN PRESENT:

- Best practices for defending your network against cyber intrusions
- IP Telephony – Ready for Prime Time?
- Wireless network security
- Email content filtering, spam control, encryption
- External auditing



- Internal auditing
- Anatomy of an Internet attack
- Components of a successful Internet security framework/Intrusion prevention
- Internet security and firewall systems
- Managing e-business risk
- Firewalls are not enough
- Disaster proofing your disaster recovery
- Cyber Security Risks and Solutions
- Information Security Risks, Financial Institutions, and Regulators
- Overview of FFIEC IT Handbooks
- What Examiners Will Look For: Management, Audit, Business Continuity

Perimeter's Speakers

- *Andrew Greenawalt, Founder & Chief Technology Officer*
- *Susan Orr, Former FDIC Bank Examiner & Security/Regulatory Compliance Advisor*
- *Kevin Prince, Chief Security Officer*
- *Brian Otte, Vice President, Corporate Development*
- *Sebastian Fazzino, Senior Vice President, Technical Sales Engineering*
- *Maureen Kaplan, Director, Technical Sales Engineering*
- *Jerry Piatkiewicz, Senior Security Consultant*

Andrew Greenawalt ~ BIO Founder & Chief Technology Officer

As the founder and CTO of Perimeter Internetworking, Andrew Greenawalt's vision and energy has lead the market to address the needs of the middle market with a new paradigm of computing. Andrews's technology experience spans the last two-decades, in which he has been an early adopter of every major computing development since the Apple II. From there, he has been at the forefront of technology with the PC, Macintosh, DEC VAX, Unix, Internet, networked databases, Novell, fiber optics, LAN switching, Frame Relay, VPN, Enterprise Integration, data warehousing, Windows NT, among others.



Susan Orr ~ BIO

**Former FDIC Bank Examiner & Security/Regulatory Compliance Advisor
CISA, CISM, CRP**

Susan Orr is a leading financial services expert with vast regulatory, risk management, and security best practice knowledge and expertise . During her 14 year tenure as a bank examiner, Susan held numerous lead positions including Regional IT Examination Specialist, Special Assistant to the Regional Director, Special Assistant to the Director of DSC, and Special Assistant to the Vice Chairman of the FDIC. Susan was also a lead instructor for the FDIC's technology school and was instrumental in key industry initiatives such as the FDIC E-Risk Strategic Initiatives Risk Monitoring Committee, the Chicago Region Interagency Technology Group, and the Federal Financial Institutions Examination Council (FFIEC) IT Handbook rewrites. Prior to launching her consulting practice, Susan was Vice President of Regulatory Compliance at for an Internet security company where she advised staff, customers, and partners on regulation, security, and risk management. Susan retains close relationships within the FFIEC agencies as well as industry trade groups to stay abreast on new technologies, best practices, and regulatory issues.

Susan currently consults for several security providers and vendors as well as performs IT security and regulatory reviews for financial institutions. She also speaks regularly at risk management and security educational seminars and has authored numerous white papers on emerging information technology and security risk management topics. Susan is a Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM) and Certified Risk Professional (CRP).

Kevin Prince ~BIO Chief Security Officer

Kevin Prince, Chief Security Officer, Perimeter eSecurity

As Chief Security Officer (CSO) at Perimeter eSecurity™, Kevin Prince assists with the company's strategic plan and is responsible for many of its strategic relationships. Perimeter Internetworking is the leading provider of multi-threat, managed "Security in the Cloud" services to financial institutions and other firms with high data security and regulatory requirements.

A well known expert in the security industry, Kevin regularly trains organizations regularly on topics such as firewall security, remote access, virtual private networks, vulnerability defense, intrusion detection and prevention systems, and on what examiners look for when they examine a financial institution.

Prior to joining Perimeter eSecurity Kevin was CEO of Red Cliff Solutions, which he founded five years earlier with no start-up funding and grew into the leading provider of managed security services to Credit Unions. While at Red Cliff Solutions, Kevin developed the industry leading CounterPhish product, the first anti-phishing incident response program specifically designed for Credit Unions. In January of 2006, Perimeter eSecurity acquired Red Cliff Solutions making Perimeter the largest provider of On Demand managed security services to financial institutions in the nation.



Prior to founding Red Cliff Solutions Kevin was a Senior Network Engineer and Senior Sales Engineer at Intellispan which was later bought by McCloud USA. Before this he was a Network Project leader for National Computer systems responsible for computer security. For over 16 years, he has worked in the Information Technology industry, focusing exclusively in the last 9 years on Internet security. Kevin has developed and managed several Internet security products designed for financial institutions in the areas of vulnerability assessments, firewalls, virtual private networks, and intrusion detection and intrusion prevention systems. He has helped hundreds of financial institutions understand the risks and threats of Internet security and conducted thousands of vulnerability assessments for financial institutions. Kevin is a frequent speaker at industry leading conferences and trade shows including the National Credit Union League (NCUA) and others.

Brian M. Otte ~ BIO
Vice President, Corporate Development

Brian Otte is responsible for Perimeter Internetworking's Business Development initiatives. He comes to Perimeter through the merger with Guarded Networks, Inc. ("GNI"). As one of the co-founders of GNI, Brian assumed the role of leading the Business Development practices, in 2000, where his responsibilities included forming strategic partnerships within the financial sector. He has spoken at over 20 financial based events since the formalization of the Gramm-Leach-Bliley Act and has written numerous articles published in financial institution magazines.

Prior to his career in Perimeter, Brian served as a network security auditor at a Big Six firm. Brian helped establish a network security competence team, and helped formalize the review process for the financial institutions that they audited. He has a great deal of experience in using industry security tools such as Axent's ESM and ISS (Internet Scanner, Database Scanner) as well as other cutting edge security tools to evaluate large scale network environments and to assist clients in designing corrective actions. Brian's primary industry focus as an auditor was within the financial industry.

In addition, to his professional achievements, Brian has a BS in both Accounting and Management of Information Systems ("MIS"). He is also a Microsoft Certified Systems Engineer ("MCSE") and holds various other security certifications and is an active member of several security organizations including the Information System Audit and Control Association ("ISACA") and Information System Security Association ("ISSA").

Sebastian Fazzino ~ BIO
Senior Vice President, Technical Sales Engineering
CISSP, CISM, CCSE

Sebastian has been with Perimeter since 1999. His responsibilities include managing a team of Sales Engineers who work with our clients, partners, sales, and operations, assisting with the exchange of technical information and services. Prior to working with Perimeter, Sebastian held the position of Vice President, Chief Technology Officer for one of the largest Marketing and Integrated Business Strategy companies in North America, Servicing Fortune 1000 clients. Mr.



Fazzino has experience in managing enterprise financial systems, data centers, complex WAN & LAN's, network operations and technical support services in complex, multi-platform environments for the past 15 years. Sebastian is an active member of the following security associations: ISSA, InfraGard, ISACA

Maureen Kaplan ~ BIO
Director, Technical Sales Engineering
CISSP

Primary responsibilities include assisting the sales team, strategic partners and existing clients with the exchange of technical information on all of the services offered by Perimeter. Ms. Kaplan also conducts monthly customer seminars on a variety of information security topics. Prior to this position Ms. Kaplan was a Senior Software Engineer at Digital Equipment Corporation's manufacturing automation division. In that role she provided project management, strategic planning, software development and technical sales support to the national sales team. Ms. Kaplan holds a Bachelors Degree in Hydraulic Engineering and brings 12 years of experience to Perimeter.

Jerry Piatkiewicz ~ BIO
Senior Security Consultant
CISSP, MCSE, CCNA

Jerry Piatkiewicz has over 9 years of experience as a professional computer engineer and joined Perimeter through the acquisition of ITM Technology as Manager, Security Engineering. Jerry has been the architect for numerous corporate security plans, and has coordinated, implemented, and supported changes to network infrastructures, and performed extensive network monitoring analysis and forensics. Jerry has conducted security audits, security training, and security consulting for companies such as Alticor, Borland, and FEMA.

Contact:
Debbie Bergenske, Product Manager
CUNA Strategic Services
dbergenske@cuna.com
800-356-9655 ext. 4340