WEBINAR SERIES

Good Practices to Keep Your Information Secure

Presented by:
American Technology Services
Association Technology Solutions

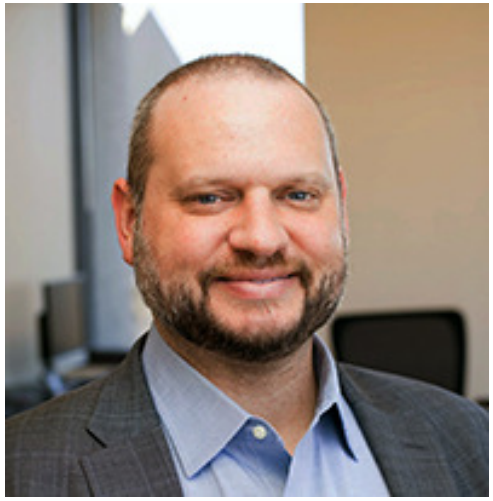
ABOUT ATS

- Serving iMIS community since 1995
- Full-service Authorized iMIS Solutions Provider (AiSP)
- Application development to extend the functionality of iMIS
- 2015 & 2016 Authorized iMIS Solution Provider (AiSP) of the Year

ABOUT AMERICAN TECHNOLOGY SERVICES

- Established in 1994
- Deep expertise and experience helping associations with their IT needs
- Security-first focus with a 24/7 Security Operations Center

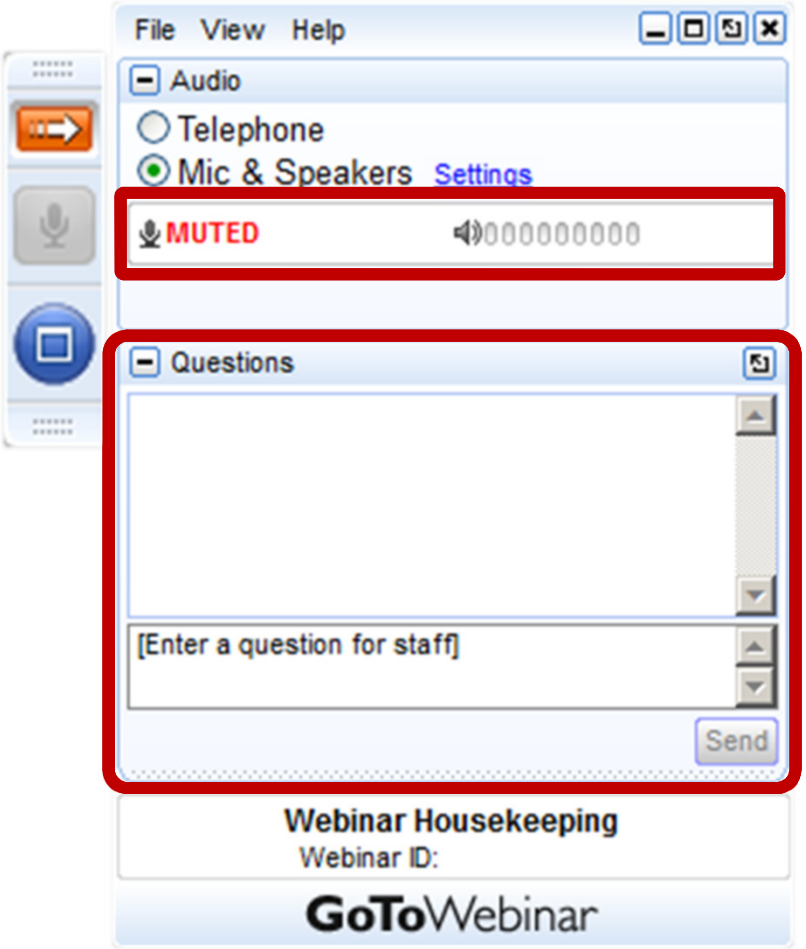
PRESENTERS



Bill Rankin
Manager, Compliance and Security Services
American Technology Services
Direct: (571) 405-5378
Email: wrankin@networkats.com

Tom Valadez
Senior Security Architect
American Technology Services
Direct: (571) 405-5391
Email: tvaladez@networkats.com

USING GOTOWEBINAR



- Attendees are muted to reduce background noise
- Remember to ask questions via the **Questions** panel
- Questions will be answered during Q&A after presentation is complete

AM I A TARGET?

- Yes
- Targets are easy to find
- Looking for vulnerabilities not organizations
- Size does not matter
- Ransomware
- Exfiltrate credit card or sensitive information

A SUCCESSFUL SECURITY PROGRAM

- Buy-in from the Top
- Balance between security and business

DON'T GO AT IT ALONE

- Risk Management Frameworks – e.g., NIST RMF
- Security Control Frameworks – e.g., CIS Controls
- Security Management Program Frameworks – e.g., NIST CSF
- IT Governance Frameworks – e.g., ITIL
- Be a part of the community

INDEPENDENT ASSESSMENT

- Vulnerability Assessment and Penetration Test
- Framework or Compliance Assessment
- Unbiased
- Turn unknowns into knowns

BUILD A FOUNDATION – CYBER HYGIENE

- Know what is in your environment
- Passwords/Multi-Factor Authentication
- Standard configurations
- Limit administrative privileges
- Endpoint and server protection
- Patch
- Document processes
- Training and awareness
- Setup routines

THE NEXT LEVEL

- Continuous Security Monitoring
- File Integrity Monitoring
- Encryption
- Spam Protection
- Email Forgery Protection
- DNS Filtering
- Certificate-based Wireless Access

SECURITY RELATED TO IMIS

- **Keep up to date on patches**
  - Patches include security fixes, performance improvement, and enhancements
- Make all connections to iMIS as https
- Passwords
  - Passwords are minimum of 7 characters (1 letter and 1 number)
  - Have a policy in place when staff members leave the organization
- Best practice, install iMIS with a non-SA password
  - Consider password changes for SA or SA <equivalent>
  - Changing SQL password used in iMIS, normally requires reinstallation of iMIS
- Do not lose or delete your kek file – is tied to the database and if lost you cannot access your iMIS database
- Be careful about saving passwords on websites, cell phones, tables, etc., to speed up login.

SECURITY FEATURES

- **Multi-factor authentication**
  Multi-factor authentication is being introduced to provide PCI-compliant sign-in security. Each time a system administrator logs in to iMIS, they are prompted to enter a security code. Without a valid security code, authenticated access to iMIS is prohibited. For authenticated access to the Advanced Accounting Console, system administrators must enable this feature in the Staff site. System administrators must perform the initial multi-factor setup through the **I don't have a security code** link in the Contact Sign In content item.

SECURITY FEATURES

- **Passwords** – System administrators can enforce password expiration, password reuse, and session timeout requirements to all administrator and non-administrator users separately. These enhanced password security options comply with PCI 3.2 guidelines.
- **Encryption** - The key-encrypting key can now be reset through the iMIS Scheduler site. From the Scheduler page, iMIS SysAdmins can reset the encryption keys and re-encrypt cardholder data, as well as change the key-encrypting key file. (took 2.5 hours on a recent client)
- **Credit card retention and storage** Outdated credit card data can be removed from databases with the PCI Data Retention Cleanup task, and users are able to configure the number of days this data is retained.

QUESTIONS & ANSWERS

MORE FROM ATS

Looking for more from the experts at ATS?

Upcoming Webinars

http://atsol.org/Webinars
schedule of upcoming webinars

Past Webinars

http://atsol.org/PastWebinars
video recordings and downloadable presentation slides

Other Questions?

Email: info@atsol.org

Online: http://www.atsol.org

Phone: (720) 945-7252