



“Providing Services for Your Success”

Centerville Rotary – August 15, 2013

<http://www.km-groupllc.com>

Agenda

- Speaker Profile
- Part 1 Security Overview
- Part 2 KM Group, LLC Overview
- Summary
- Q&A

The logo for KM Group, LLC is displayed in a light blue, semi-transparent font. It consists of the letters "KM" in a large, bold, sans-serif font, with "GROUP, LLC" in a smaller, all-caps, sans-serif font directly below it. The entire logo is contained within a thin, light blue rectangular border.

KM
GROUP, LLC

Speaker Profile

Mark A. Metzner

- Partner, General Manager and Senior Consultant for KM Group, LLC
- “44” Years of Experience in Information Technology
- “42” Years of Security Focused Work
 - Both Public and Private Sectors
- Retired Federal Employee and US Marine Veteran



Part 1 Security Overview

What is Security?

Ask and you will get many different descriptions

- Security is the degree of protection against risks from danger/harm, damage, loss and crime
- Applied structures and processes that provide or improve security as a condition to mitigate or eliminate risks
- Encompasses more than physical controls



Summary – A continuous process to monitor, measure all risks to mitigate to acceptable level for Administrative, Technical and Physical areas

Security Categories

- **Physical**
 - Home, Schools, Infrastructure, Entertainment, Shopping, Restaurants, Facilities of all shapes and sizes
- **Technical**
 - Computing, Applications, Network, *Data, Information*
- **Administrative**
 - Organization, HR, Financial



Physical, Administrative, Technical

Physical examples

- CATV, Visitor Controls for access to areas



Administrative

- Policies, Procedures, Processes, Training and Controls



Technical

- Patches out of date, Antivirus, spam, phishing, firewalls, policy enforcement, data loss prevention



Current Events

- Since January 2005 608, 278,176 records containing personal information involved in breaches
- Natural Disasters
 - Hurricane Sandy
 - Wildfires destroying homes, businesses
- Violent crimes
 - Shootings at schools, shopping malls, entertainment centers
 - Boston Marathon bombings
- Classified Information leaks
 - Wiki Leaks (Bradley Manning)
 - NSA information leaks (Edward Snowden)
 - Retired Marine General under investigation Stuxnet leaks



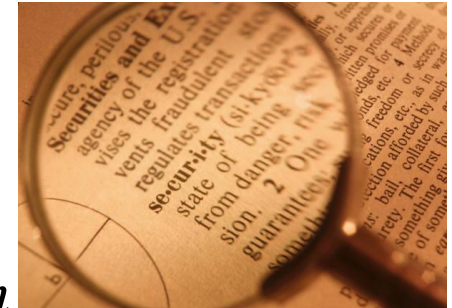
Current Events

- Personal Information Breach
 - Facebook breach due to bug in June affecting 6,000,000 users – allowing unauthorized users view of personal contact information
 - Florida Department of Education 47,000 teacher records publically accessible for two weeks after a data transfer with Florida State University
- Local
 - Skimmers found at local gas station pumps Moraine OH
 - Key loggers found on public systems in local schools and hotels
 - Phishing and Social Engineering on the rise
- General
 - Mobile Computing Risks (BYOD in workplace)
 - Move to Cloud Computing without analysis of security risks



Security Management

- Holistic and Continuous Risk Management approach
- Industry Standards (ISO 27000, PCI)
- Regulations and Laws
 - **HIPAA, GLBA, SOX, State and Local**
- Professional organizations
 - *(ISC²) International Security Consortium*
 - *(ISSA) Information Systems Security Association*
 - *(ISACA) Information Systems Audit and Control*
 - *(SANS) Institute – research and education organization*
 - *(NIST) National Institute Standards and Technology*
 - *(SEI/CMU) Software Engineering Institute/Carnegie Mellon University*
 - *(CIS) Center for Internet Security*



Common Problems

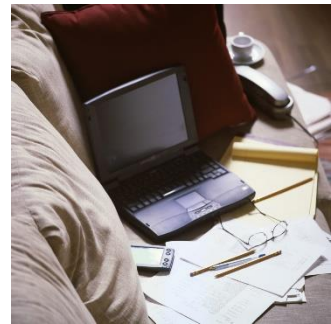
- Awareness of the risks involved
- Misconception that all information is private and no one else can access or view
- Acceptance of bad habits
- Not following procedures and processes when performing tasks
- Connecting to unsecure access points (Wi-Fi hotspots)
- Encryption not being used for sensitive information
- Not keeping malware software or system patches up to date
- Not thinking before clicking/connecting



What Can You Do

Business

- Business Impact Analysis
- Develop Security Management Plan and Policy
- Develop Disaster Contingency Plan and Policy
- Develop Incident Handling Plan Policy
- Develop Security Awareness and Training Plan and Policy
- Documented/Communicated Governance policies, procedures, processes
 - Ethical behavior and Rules of Access
- Review & test plans, processes and procedures
 - Annually or with each significant change
- BYOD management and controls
- Inventory of Assets (Physical and Information)



What Can You Do

Home and personal

- Secure your home broadband/DSL connection and wireless
 - Do not broadcast SSID and always use WPA
 - Change default name and password of your home router
 - Use personal firewalls if available
- Update and Patch all software and hardware
- Use parental controls available

Always be aware of your surrounding and connections

Think before you act, if in doubt DON'T



Sources of Information

<http://csrc.nist.gov> National Institute of Standards and Technology

<https://www.issa.org> Information Systems Security Association

<https://www.isaca.org> Information Systems Audit and Control Association

<http://iase.disa.mil> Information Assurance Support Environment

<http://cisecurity.org> Center for Internet Security

<http://www.dhs.gov/index.shtm> Department of Homeland Security



Part 2 KM Group, LLC Overview

- **KM Group, LLC is a WOSB/EDWOSB and is an LLC partnership**
- **In operation since March 2011**
- **Providing Services**
 - **Business Intelligence**
 - **Information Assurance**
 - **Infrastructure**
- **Four Tenets for services provided:**
 - **Highest Availability and Survivability**
 - **Security inherent in all areas and aspects**
 - **Maximization of existing resources**
 - **Monitored, measured and managed**



KM Group, LLC Overview

- **Budgets are a high priority consideration with our customers we do not employ sales personnel on commission for scoping and pricing. Scoping and pricing accomplished by communication with the people who deliver the service(s) and the customer**
- **All services are available via Subscription**



KM
GROUP, LLC

Contact Information

- **Website:** www.km-groupllc.com
- **Email:** contact@km-groupllc.com
- **Telephone:** (937) 619-0137
- **Office Location -**
6234 Far Hills Avenue
Dayton, OH 45459



KM
GROUP, LLC

Question and Answer

- **Questions**

KM
GROUP, LLC