Special Report

A Summary of the Seminar Conducted at the Ewing Marion Kauffman Foundation, Nov. 15, 2012

Greater Kansas City
Cyber Security Seminar

November 15, 2012
Kauffman Foundation Conference Center
Kansas City, Mo.

Command and General Staff College Foundation, Inc.

Arthur D. Simons Center
for Interagency Cooperation

Dear Readers:

In a recent issue of the Wall Street Journal, Tam Harbert noted that "market research firm IDC estimates that the amount of digital information created and replicated has been more than doubling every two years. In 2011 it exceeded 1.8 zettabytes and will reach almost 8 zettabytes by 2015. What's a zettabyte? It equals a trillion gigabytes which is equivalent to the amount of information on 250 million DVDs." This level of digital activity creates an amazing web of interdependency and a corresponding amount of vulnerability.

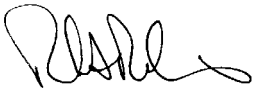
In addition to the malware, viruses, and intentional hacking many of us experience in our personal lives, there are serious threats to commercial and governmental computer systems. For example, every day, Department of Defense information networks receive over 100,000 attacks. The energy industry and grid experience 80 million cyber-attacks each month. The FBI reports an estimated $400 billion in cyber-crime occurred in 2011 alone. Director of National Intelligence, James Clapper, in testimony before the Senate Intelligence Committee stated that computer activities of foreign adversaries, criminals, terrorist groups, and other non-state actors are "a profound threat to this country, to its future, to its economy, to its very being."

In this report, you will read about the discussion that took place during the Greater Kansas City Cyber Security Seminar organized by the CGSC Foundation's Simons Center for Interagency Cooperation in partnership with Business Executives for National Security and the Kansas City Division of the FBI. The seminar convened at the Kauffman Foundation Conference Center on November 15, 2012, and was attended by over 140 business and government leaders. Participants represented all business sectors along with local, state, and federal government organizations from Kansas City, Topeka, Wichita, Columbia, and Jefferson City.

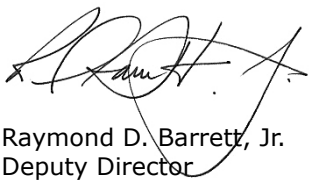
Keynote speakers included Joseph Demarest, Assistant Director of the FBI Cyber Division and William Hagestad, cyber security strategist and author of *21st Century Chinese Cyberwarfare*. Panelists included national and local cyber security experts representing banking, finance, public utilities, national defense, law enforcement, investment, infrastructure, and telecommunications.

Many believe that the first shots in the new age of warfare have already been fired and that cyber as well as kinetic weapons are currently in use by national and transnational actors. Our defense establishment is keenly aware of the threat. Likewise, individual, commercial, and state actors are aggressively seeking to penetrate and steal our personal, financial and intellectual property.

The Greater Kansas City Cyber Security Seminar explored the threat and discussed the challenges. It is our hope that we all continue to engage in an active dialog about the challenges that affect our lives—to seek knowledge and understanding and to discuss solutions and capabilities that will enable us to protect our way of life.



Robert R. Ulin
Chief Executive Officer
CGSC Foundation, Inc.



Raymond D. Barrett, Jr.
Deputy Director
The Simons Center

Foreword

The recently concluded Greater Kansas City Cyber Security Seminar was a great success and a tribute to the event partnership efforts of the Command and General Staff College Foundation and the Simons Center for Interagency Cooperation.

In October 2012, Secretary of Defense Leon Panetta speaking to members of Business Executives for National Security (BENS), stated that there is a new domain that we must secure to have peace and prosperity in the world of tomorrow. The current cyberspace technology has fundamentally transformed the global economy and our way of life, providing two billion people across the world with instant access to information, to communications, and to new economic opportunities. When people think about cyber security today, they worry about criminals who prowl the Internet and steal people's identities, sensitive business information, trade secrets, and various kinds of money fraud. Our greatest fear, however, is a cyber attack perpetrated by nation states or violent extremist groups that could be as destructive as the terrorist attack of 9/11; an attack that could dismantle the nation's power grid, transportation systems, financial networks and government facilities; an attack that would cause physical destruction and loss of life, paralyze and shock the Nation, and create a profound new sense of vulnerability.

To mitigate these threats will take an interagency approach in conjunction with federal, state, local, and the private sector to cooperate, collaborate, and communicate solutions across the broad spectrum of possibilities. Secretary Panetta said, "we must work with the business community and develop baseline standards for our most critical infrastructure - including power plants, water treatment facilities, and gas pipelines." The business community must be able to take commonsense steps against basic threats, but also take proactive measures to secure themselves against sophisticated threats. He acknowledged that although awareness is growing, the reality is that too few companies have invested in even basic cyber security. He urged business leaders to shore up their corporate cyber defenses, and become part of the solution rather than part of the problem.

The recent Greater Kansas City Cyber Security Seminar built upon Secretary Panetta's challenge to improve business cyber security awareness and encourage development of corporate defensive strategies. This seminar was just a start, and we intend to continue cyber security awareness within the business community through a series of future Cyber Security Executive Roundtables for senior business leaders in the Kansas City metropolitan area.

We hope you will be able to participate.

Landon H. Rowland
Chairman, Kansas City BENS

Business Executives for National Security

Agenda

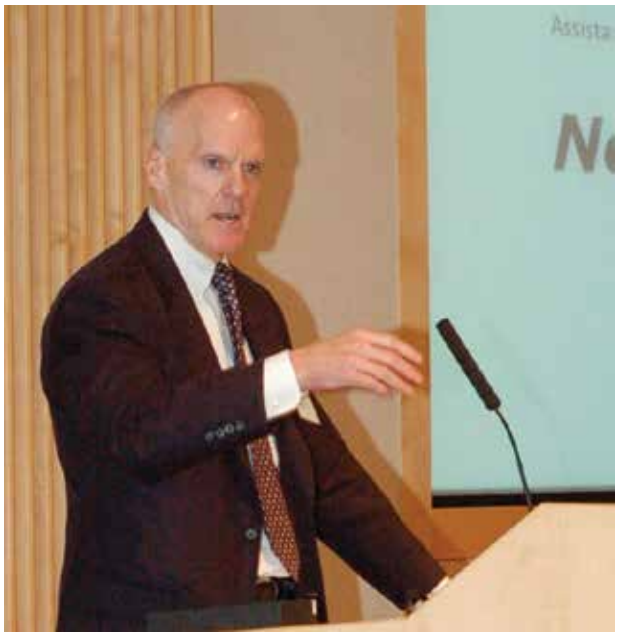
9:00 – 9:05 a.m.	**Welcome**
9:05 – 9:45 a.m.	**Keynote Speaker: *Next Generation Cyber*** – Joseph Demarest, Assistant Director, Cyber Division, FBI Headquarters
9:45 – 10:00 a.m.	**Break**
10:00 – 11:00 a.m.	**Panel – *The Cyber Threat Environment***
	Hackers, Criminals, Non-State and State sponsored Threats Special Agent in Charge Michael Kaste, FBI Kansas City Division
	Threats to the Grid and other Sensitive Infrastructure Amit Khosla, National Cybersecurity & Communications Integration Center, Department of Homeland Security
	Threat to Financial and Economic Systems John Mallery, Mallery Technical Training and Consulting
	Threats to the Department of Defense Col. Patrick Kerr, Operations Officer, U.S. Army Cyber Command
11:00 – 11:45 a.m.	**Panel Question and Answer**
11:45 – 12:00 a.m.	**Break**
12:00 – 1:00 p.m.	**Lunch and Keynote Speaker:** ***21st Century Chinese Cyberwarfare*** William T. Hagestad, II, Cyber Security Strategist
1:00 – 1:15 p.m.	**Break**
1:15 – 2:15 p.m.	**Panel – *Cyber Security: What Are We Doing About It?***
	Regional Cyber Crime Threats and Response Special Agent Robert Schuett, FBI KC Division Cyber Crime Task Force
	Protecting Banking Systems Tim Raines, Information Security Officer, UMB Bank
	Protecting the Investment System Aaron Weissenfluh, Information Security Officer, BATS Exchange
	Protecting Telecommunications Systems Perry Siplon, VP/Corporate Security, Sprint Nextel
	Protecting Energy and the Grid Scott Harris, Information Security and Compliance, KCP&L
2:15 – 3:00 p.m.	**Panel Question and Answer**
3:00 – 3:05 p.m.	**Closing**

Next Generation Cyber

Joseph Demarest

Summary of opening remarks by Assistant Director Joseph Demarest, Federal Bureau of Investigation, Cyber Division, Washington, D.C.

Cyber is certainly the next big challenge. Director Mueller believes that in five years, cyber will overtake terrorism as our greatest concern; it is that broad and pervasive. We prepare for what we see happening each day, both the advanced persistent threat and other threat actors. We have seen distributed denial of service activities in New York, as well as attacks on a large, energy giant from the Middle East by the same threat actors. These malware attacks caused significant damage to internal systems and rendered 30,000 desktop computers at Saudi Aramco useless. So, we need to engage not only domestically, but also abroad.



FBI Assistant Director Joseph Demarest provides the opening address to attendees at the Greater Kansas City Cyber Security Seminar.

Last year, the FBI's Internet Crime Complaint Center saw over 300,000 complaints, up four or five percent from the previous year. Self-reporting, as far as dollar loss, was about a half billion dollars. Self-reporting ranges from mom and pop reporting—such as Internet fraud— to major corporations reporting embezzlement. Symantec blocked a total of 5.5 billion malware attacks in 2010, an 81 percent increase over the year prior. The Russian cyber security firm Kaspersky claims that the number of reported browser-based attacks in 2011 increased from 580 million to over 946 million. One company subjected to an intrusion attack lost about ten years of intellectual property development overnight. Some of these firms don't even know it's happened. And if they do, they don't believe it, or they don't know what to do next. The lifeblood of the U.S. is being stolen, and the U.S. government must protect all of us. Some will argue that the government should pay more attention to a certain sector or a certain level of corporation or firm. But what about the mom and pop company that's creating some new technology for the military or the U.S. intelligence community that doesn't have the same resources? I think we should be protecting everyone.

The threat has changed. In 2000, we worked with the Royal Canadian Mounted Police to track down a Canadian teenager by the name of "Mafia Boy." He was responsible for the largest denial of service attack at the time. We finally caught up with him at a sleepover, watching *Goodfellas*. Once confronted, he didn't realize the consequences of what he was doing. Today, the cyber threat is, obviously, much advanced. Twelve years later we're looking at threat actors on the terrorism side, such as Al Qaeda in the Arabian Peninsula, who are waging cyber jihad. We have a whole unit in the Cyber Division to look just at terrorism or terrorist hackers.

General Alexander from the National Security Agency (NSA) has noted a 17-fold increase in computer attacks against our infrastructure. We look at, monitor, and observe targeting of certain systems throughout critical infrastructure, and it leaves us very concerned. Of the 18 critical infrastructure sectors, we're focused on telecoms, finance, and energy. Resources being what they are, we are trying to develop close working relationship with key components or firms within each of those industries.

In New York City, the attackers were good enough to post their intended targets, so they gave us advance notice. We were able to invite the private sector in before something happened and brief them completely on what the threat was. When it comes to preventing or defending the country, we are all involved. You're going to see the U.S. government effort here, and it's united. Defense mainly falls to the Department of Homeland Security for certain systems, and then NSA. But we're all involved on the prevention piece, collecting intelligence to provide to the defenders to better protect the country.

But when it comes to investigations, the FBI is on point. We work very closely with the Secret Service at Headquarters now. We see great opportunities to leverage one another in addressing the intrusion threat. Intrusions range from terrorism hackers or terrorist actors to nation/state criminals. What we want to have and don't have as yet, is a national picture of all intrusions.

Our number one concern is cyber *jihad*. Extremists have or they could develop the skill to actually impact the nation's Industrial Control Systems or Supervisory Control and Data Acquisition systems. Another concern is nation-state actors. The FBI continues to work within the intelligence community on focusing on those actors. The FBI is the lead agency for national security matters, and we share responsibility on the criminal side with Secret Service. As laid out by the Director, advanced persistent threats are the gravest. If you are hooked up to the Internet, and you have something they want, it's only a matter of time before they get it. There are certain law enforcement tools we like to bring into this. We want to make sure that if you've committed crimes against the U.S. and you've taken from us, you someday pay for it. We want to know everything about actors overseas: who are their associates, who are their friends, where do they travel, where do they bank?

Cyber Division is now focused just on intrusions, malware, and botnets. The FBI has also established cyber task forces at home and abroad. Each field office is staffed with agents, analysts, and computer scientists. We'll hire 70 computer scientists by 2014 and place them in each of our 56 field offices. We probably have some of the best agents in the world working this issue.

Presidential Directive 54 established the FBI as the executive agent of the National Cyber Investigative Joint Task Force. So it's an interagency platform. There are 19 agencies that play in it now; the four required agencies include the FBI, Secret Service, CIA, and NSA. The National Cyber Investigative Joint Task Force not only looks at national security issues, but criminal as well. We have included overseas partners because the cyber issue is a global sport, and what impacts us is surely impacting them. So right now we are working very closely with the Brits and Aussies, among others.

We have 16 regional computer forensic laboratories, and we're looking to bring on more state and local officers through our task forces in the field and then back at Headquarters. We just kicked off a Fellowship program. We pay for a six-month-tour at Headquarters, and participants get the full range of training. We hope to start building the capacity within state and local departments, tribal, and territorial, because we think this is a beginning threat.

We can't do it without you. This is a big team approach. We are only as strong as the weakest link. So if you are planning operations, and security is not really there, I encourage you to build a relationship with the intelligence or law enforcement services. Engaging these services early allows you to address and work through legal and other concerns in advance.

The Cyber Threat Environment

Special Agent in Charge Michael Kaste, Federal Bureau of Investigation, Kansas City Division, discusses criminal activity during the first panel. From left to right: Kaste, Amit Khosla, John Mallery, and Colonel Patrick Kerr.

The first panel discussion focused on identifying the current cyber threats and their targets from a national perspective. Panel members included experts from the main federal agencies tasked with monitoring and addressing these threats: Special Agent in Charge Michael Kaste, Federal Bureau of Investigation, Kansas City Division; Amit Khosla, National Cybersecurity and Communications Integration Center, Department of Homeland Security; John Mallery, Mallery Technical Training and Consulting; and Colonel Patrick Kerr, Operations Officer, U.S. Army Cyber Command.

Panelists agree that cyber security threats continue to evolve; however, current threats include "script kiddies," recreational hackers, cyber "hacktivists", organized crime, terrorist organizations, nation-states, and insiders. "Script kiddies" are hackers whose skills are limited to using commonly available hacking tools from the Internet. They have no ability to modify the tools or create new exploits, and they usually work alone or in a small group. A recreational hacker can possess a wide range of skill levels, but are typically motivated by bragging rights or curiosity. They also usually work alone or in a small group. Cyber hactivists can also possess a wide range of skill levels, but to date, their observed activities have been limited to defacements and Department of State attacks. Organized crime hackers are motivated by profit. Their skill levels range from moderate to extremely skilled. Hackers working for large, organized crime efforts also receive significant support and protection. Terrorist groups employ individual hackers or groups to work on their behalf, either directly or in sympathetic support. Their skill levels can range from "script kiddie" to extremely proficient. Nation-states employ well-organized and supported hacker groups. Their skill levels are usually very high, but they often only operate at a level sufficient to accomplish the mission. Arguably, the most dangerous threats are insiders who have physical access to the network.

Panelists identified three likely targets of cyber warfare: grid and sensitive infrastructure, financial institutions, and the Department of Defense (DoD). The grid and sensitive infrastructure contain old systems once completely isolated, but today are interconnected providing easy targets for cyber attacks. Unfortunately, security patches are not routinely applied, and security audits are too rare. Industrial Control Systems (ICS) are a constant target because they provide proprietary technical data, a future foothold for a cyber attacker, and can cripple the economy. ICS is the cyber-physical nexus where electronic systems control physical activity and "things go boom." ICS are targeted by external

and insider threats, spear phishing, and control-engine targeting. The progression and successive iterations of malware add to the problem. Cyber attacks on banks are unprecedented, and the largest banks are under constant attack. Thirty-four percent of phishing is financial. Cyber attacks on the DoD are persistent and growing. The military is increasing the size of its cyber force to better understand the threat, and working toward integrating cyber training at every echelon.

DHS is working to educate companies on potential vulnerabilities. DHS protects the .gov domain and works to educate companies on potential vulnerabilities while sharing information with the public. DHS National Coordination Centers located around the country communicate with infrastructure owners so they stay current and protect themselves through information sharing (actionable intelligence), technology (blocking websites), and building operational contacts. Attackers are creative, highly skilled, and competent, and often their targets do not expend enough resources to protect themselves. Sharing information on attacks and cooperating with law enforcement are key to slowing the attacks and protecting critical infrastructure.

Questions and Answers

What occurs when the FBI is contacted about a cyber crime? If you are hacked, do not consider it a failure. Instead, share your information so the FBI can help others mitigate their vulnerabilities and avoid an attack. Involving the FBI does not typically result in media attention. Cyber crime cost business over $400 billion in 2011, so it is important to create a local partnership with the FBI.

What watchdogs monitor banking? The Treasury Department, the Federal Deposit Insurance Company, and Cyber Standard Law Enforcement (FBI and Secret Service) monitor the banking industry.

What are we doing nationally to train cyber analysts? DHS is developing the next cyber-threat workforce through online and hands-on training. The Army is developing a cyber internship program.

How are mobile networks and social media creating complexity for the military? "Bring your own device" and differing tactics, techniques, and procedures mean there are times Soldiers can be mobile and times they cannot. The Army may need to provide an alternative to social media to allow Soldiers to connect with their families.

Should we seek to reduce student visas for students from rogue states? Granting student visas is a national security issue, and granting access to systems should be on a "need to know" basis.

Advance hacking techniques are taught in California colleges. Is this a proper role for educational institutions? Not all hacking is bad. "White" hackers can identify vulnerabilities for businesses and government. However, the educational environment is the most difficult to secure based on the culture of academic freedom. The FBI conducts outreach programs for major educational institutions and maintains some visibility through these programs.

Who is conveying cyber security issues to management? Both the FBI and DHS conduct outreach programs aimed at management. But the message needs to be conveyed by the IT experts within those companies and those experts need to present their information in the financial terms management is comfortable operating with.

21st Century Chinese Cyberwarfare

William T. Hagestad, II

Retired Marine Lieutenant Colonel William T. Hagestad, II, author of *21st Century Chinese Cyberwarfare,* speaks to seminar attendees about Chinese cyber warfare capabilities and intentions.

Lieutenant Colonel (Retired) William T. Hagestad, II, served more than 27 years in the United States Marines Corps. An internationally recognized expert on the Chinese People's Liberation Army (PLA) and government information warfare, he advises international intelligence organizations, defense experts, and multinational commercial enterprises on the linguistic, historical, cultural, economic, and military aspects of Chinese cyber warfare.

Cyber attacks from the People's Republic of China (PRC) threaten corporations, research institutes, militaries, international organizations, and governments. The Chinese use calculated, precise hacking methodologies, such as brute force attacks and distributed denial of service (DDoS), to gain unauthorized access to a network. They also employ Trojans, viruses, and malware or a combination of methods known as advanced persistent threats (APT).

The Chinese government is motivated by three primary factors: fear of foreigners, self-preservation, and hegemony. The power of the Chinese state subordinates every element of modern Chinese society, including threats of religion. Other motivations include the frenzied Chinese economy; strategic advantage over regional and international affairs; the Communist Party of China (CPC) mandate of 2010, and the PLA mission statement.

The rise of a digital China began in 1987 with educational Internet connectivity, and China built on this connectivity to develop its cyber warfare doctrine. The basis of China's net-centric asymmetric warfare doctrine is Sun Tzu's *Art of War* and Sun Ping's *Military Methods*. Hacktivists were originally supported by CPC and PLA, and served to reinforce the PRC nationalism via the web.

The CPC codified cyber warfare in 2010 in response to the U.S. DoD standing up Cyber Command six months earlier. President Hu Jintao vowed to "protect national infrastructure from external cyber threats" and his recently appointed successor, Xi Jin Ping, believes that CPC + PLA x IT superiority = China's worldwide dominance.

Even though there is no evidence pointing to the Chinese government—such as IP attribution—the CPC, the PLA, state-owned enterprises, and hacktivists are behind these threats. We know this because the Chinese military slipped up and recently broadcast its cyber-war campaign against U.S. targets. Some of these state-owned enterprises include:

- China Telecom, which is owned by the CPC and operated by the PLA.
- Huawei, which is owned by a former PLA officer and has direct links to the PLA.
- China Petroleum & Chemical Corporation.
- SinoChem.
- China National Petroleum Corp.
- China National Pharmaceutical Group.

Retired Marine Lieutenant Colonel William T. Hagestad, II, says the world can not stop Chinese information warfare, but could learn to more effective slow it down, learn to detect it better and plan more effective responses.

President Hu Jintao ordered subordinates to strengthen the nation's cyber-infrastructure. Notable PLA information warfare and electronic warfare leaders include General Zhang Qinsheng, General Chen Bingde, General Ma Xiaotian, Vice Admiral Sun Jianguo, and Major General Hou Shu Sen.

Conclusions

Cyber warfare is a central component of China's future. Its ability to modernize, catch up with the developed world, expand its economy, defend its interests, and achieve its strategic goal of hegemony depends on exploiting and dominating cyber-space. Cyber warfare is state sponsored, deliberate, and encouraged in multiple segments of Chinese society, economy, military, and politics. The PLA has created organizations focused on offensive and defensive cyber warfare, including a "Blue Army" charged with probing the PRC's cyber infrastructure in search of vulnerabilities that need strengthening. The CPC has long advocated citizen hacking and has expanded in scale and sophistication to the point that it can no longer be centrally controlled by the party apparatus.

The nuance of Mandarin Chinese is an exceptional form of cryptography rendering malware, random access Trojans, and botnets undiscoverable. Commercial IPs are ineffective against attack rendering enterprises worldwide permeable to Chinese cyber hacking in all its forms and methods. Businesses, governments, and the Department of Defense cannot adequately defend themselves from alleged Chinese information warfare threats. But they can slow them down, learn to detect them when they occur, and plan an effective rapid response.

The United States' future position in the world—economically, militarily, politically, and informational—depends on protecting our innovation, intellectual property, and our information networks. To compete in the cyber-domain we must develop multi-layer detection and defense, evolve rapidly, make the proper public and private investments, share information, work collaboratively, and develop offensive capabilities. Diplomatic initiatives need to be employed in tandem with military initiatives across the globe, but particularly in the Asia/Pacific region.

Cyber Security: What are We Doing About It?

Special Agent Robert Schuett, left, Kansas City FBI, Cyber Crime Task Force, comments on the FBI's reponse to cyber crimes during the second panel of the seminar. From left to right: Schuett; Tim Raines, Information Security Officer, UMB Bank; Aaron Weissenfluh, Information Security Officer, BATS; Perry Siplon, VP Corporate Security, Sprint Nextel; and Scott Harris, Information Security and Compliance, Kansas City Power and Light (KCP&L).

The second panel discussion focused on regional cyber-crime threats and how local corporations are responding. Panel members included subject matter experts from the Federal Bureau of Investigation (FBI) and the financial, telecommunications, and energy sectors. Members of the panel included Special Agent Robert Schuett, Kansas City FBI, Cyber Crime Task Force; Tim Raines, Information Security Officer, UMB Bank; Aaron Weissenfluh, Information Security Officer, BATS; Perry Siplon, VP Corporate Security, Sprint Nextel; and Scott Harris, Information Security and Compliance, Kansas City Power and Light (KCP&L).

Hackers have evolved from "script kiddies" to state-sponsored intelligence operatives. They are persistent and will eventually get inside the network. Panel members agreed that to protect themselves from cyber attacks, corporations must prepare and practice a response plan. When attacked, corporations must willingly share lessons learned to assist other partners who may face the same problem in the future. Other protective measures include hiring an intrusion team to test cyber security; identifying and take off the Internet where proprietary information is stored, and using legitimate credential locking.

Cyber attacks on banks include distributed denial of service (DDoS), customer email takeover, spear phishing, and advanced persistent threats (APT). Corporations can mitigate DDoS by employing anti-DDoS services, segmenting services, tuning load balancers, installing web application firewalls and intrusion protection systems, applying regular security patches, and using external methods of intrusion testing.

Corporations can lessen or eliminate email takeover with enhanced employee training and coaching, customer identification, and automated fraud detection. Like email takeover, spear phishing can be lessened or eliminated with enhanced employee training. In addition corporations can install SPAM filters, anti-virus software, and web filtering. Increasing intelligence gathering, segmenting the network, and practicing the basics of cyber security can go a long way in mitigating APTs.

Keeping systems safe involves knowing what is normal, the attacker, how to slow the attack, and when to react. Custom controls include latency management anomaly detection, open protocols, and education. The Financial Services Information Sharing and Analysis Center, the Financial Services Sector Coordination Council for Critical Infrastructure, the FBI liaison, and the Security and Exchange Commission can facilitate information sharing.

Aaron Weissenfluh, BATS Information Security Officer, third from left, successfully uses humor to make a point to seminar attendees.

Protecting the telecommunications system should begin with continuous and regular security reviews by multiple third parties combined with monitoring, vulnerability testing, and patch management. Protection plans and incident response processes must be multi-layered, evolve with the threat, and correlate physical and technical events. In addition, corporations must proactively manage third-party business partners and hold them to the same security standards they use to run their business.

There are an estimated 80 million cyber attacks on the grid and energy industry per month. Breaching critical systems, such as the Energy Management System, could result in a widespread disaster for customers and the utility industry requiring intervention by government agencies. Since local power plants are connected to regional utilities, attacks on weakly protected sites could become a major incident affecting millions of individuals and losing credibility with customers, stakeholders, and state commissions.

Industry must deter, defend, detect, and respond. Businesses can deter cyber attacks by implementing policies, providing information security training, conducting background checks, managing vulnerabilities, segmenting the network, and implementing configuration management and change control. In addition, strong authentication, a separation of duties, and physical security all act as deterrents to cyber attacks. Next generation threat protection includes application control/identity awareness, HTTPS inspection, and FireEye/Dambala. Intrusion prevention systems, anti-virus controls, malware kiosks, and encryption can also help industries defend against APTs.

Industries can respond to cyber attacks by establishing an incident response plan and conducting regular drills that include executive management.

Members of the second panel field questions from attendees.

Questions and Answers

How do you see speed effecting security? Speed will result in more redactions and more security questioning.

What courses should academia focus on to prepare IT professionals? Developers (C++, Linux, etc.), software coding, and courses for translating "geek speak" into "corporate speak."

What do first-line managers need to know about security? They must recognize common threats and train personnel to respond correctly. Social engineering/spear phishing feeds off social sites. They must be aware.

How about degrees focused on cyber security? A wide breadth of knowledge is more important than a specific degree.

What should a company do first when an intrusion occurs?

- Begin your response.
- Determine how severe the attack is.
- Alert management.
- Convey information to the FBI about how you want them to approach the situation.
- Provide log files.
- Identify machines affected.
- Maintain chain of custody and any forensic evidence.

Special Thanks to Our Sponsors

~ *Platinum Sponsors* ~

KAUFFMAN
The Foundation of Entrepreneurship

Based in Kansas City, Missouri, the Ewing Marion Kauffman Foundation was established by the late entrepreneur and philanthropist Ewing Marion Kauffman. The Kauffman Foundation's vision is to foster "a society of economically independent individuals who are engaged citizens, contributing to the improvement of their communities." In service of this vision, and in keeping with the founder's wishes, the foundation focuses grant making and operations on two areas: advancing entrepreneurship and improving the education of children and youth.

LOCKHEED MARTIN

Headquartered in Bethesda, Maryland, Lockheed Martin is a global security and aerospace company that employs about 120,000 people worldwide and is principally engaged in the research, design, development, manufacture, integration and sustainment of advanced technology systems, products and services. The corporation's net sales for 2011 were $46.5 billion.

Sprint

Sprint Nextel offers a comprehensive range of wireless and wireline communications services bringing the freedom of mobility to consumers, businesses and government users. Sprint Nextel served nearly 56 million customers at the end of the third quarter of 2012 and is widely recognized for developing, engineering and deploying innovative technologies, including the first wireless 4G service from a national carrier in the United States; offering industry-leading mobile data services, leading prepaid brands including Virgin Mobile USA, Boost Mobile, and Assurance Wireless; instant national and international push-to-talk capabilities; and a global Tier 1 Internet backbone. The American Customer Satisfaction Index rated Sprint No. 1 among all national carriers in customer satisfaction and most improved, across all 47 industries, during the last four years. Newsweek ranked Sprint No. 3 in its 2012 Green Rankings, listing it as one of the nation's greenest companies, the highest of any telecommunications company. You can learn more and visit Sprint at www.sprint.com or www.facebook.com/sprint and www.twitter.com/sprint.

~ *Silver Sponsors* ~

DuraComm Corporation

Mariner Capital

Metropolitan Community College

Pioneer Services, a Division of MidCountry Bank

Grantham University

Park University

UMB Bank

University of Kansas

Organizers

Command and General Staff College Foundation, Inc.

The Command and General Staff College Foundation, Inc., a 501(c)(3) tax-exempt non-profit educational foundation, provides resources and support to the U.S. Army Command and General Staff College in those areas where appropriated funding is either not available or not authorized.

The mission of the CGSC Foundation is to:

- Enrich the College's academic environment
- Foster a strong relationship between the military and the private sector
- Enhance the institution's research activities
- Promote leader development
- Encourage excellence in the faculty and student body
- Maintain contact with alumni

www.cgscfoundation.org

Visit the Foundation on:

facebook

facebook.com/CGSCFoundation

LinkedIn

linkedin.com >> CGSC Foundation, Inc.

Arthur D. Simons Center *for Interagency Cooperation*

The CGSC Foundation's Simons Center focuses on the practice and understanding of interagency coordination at the operational and tactical levels of effort. Its programs support and promote scholarship at the U.S. Army Command and General Staff College, and embrace the involvement of all participants in the interagency community.

www.TheSimonsCenter.org

For more information visit the CGSC Foundation or Simons Center websites at www.cgscfoundation.org or www.thesimonscenter.org

Command and General Staff College Foundation, Inc.

CGSC Foundation, Inc.
100 Stimson Avenue, Suite 1149
Fort Leavenworth, Kansas 66027
phone: 913-651-0624
fax: 913-651-4519
email: office@cgscf.org
www.cgscfoundation.org

Arthur D. Simons Center *for Interagency Cooperation*

Arthur D. Simons Center
P.O. Box 3429
Fort Leavenworth, Kansas 66027
phone: 913-682-7244
fax: 913-682-7247
email: office@TheSimonsCenter.org
www.TheSimonsCenter.org