Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

ACQUISITION HOUR:

COMPLIANCE WITH NEW DOD REGULATIONS ON SAFEGUARDING COVERED DEFENSE INFORMATION – A LEGAL PERSPECTIVE

November 15, 2017

WEBINAR ETIQUETTE

- Please
  - When logging into go-to-meeting, enter the name that you have registered with
  - Put your phone or computer on mute
  - Use the Chat option to ask your question(s): We will read them and our guest speaker will provide an answer to the group
- Thank you!

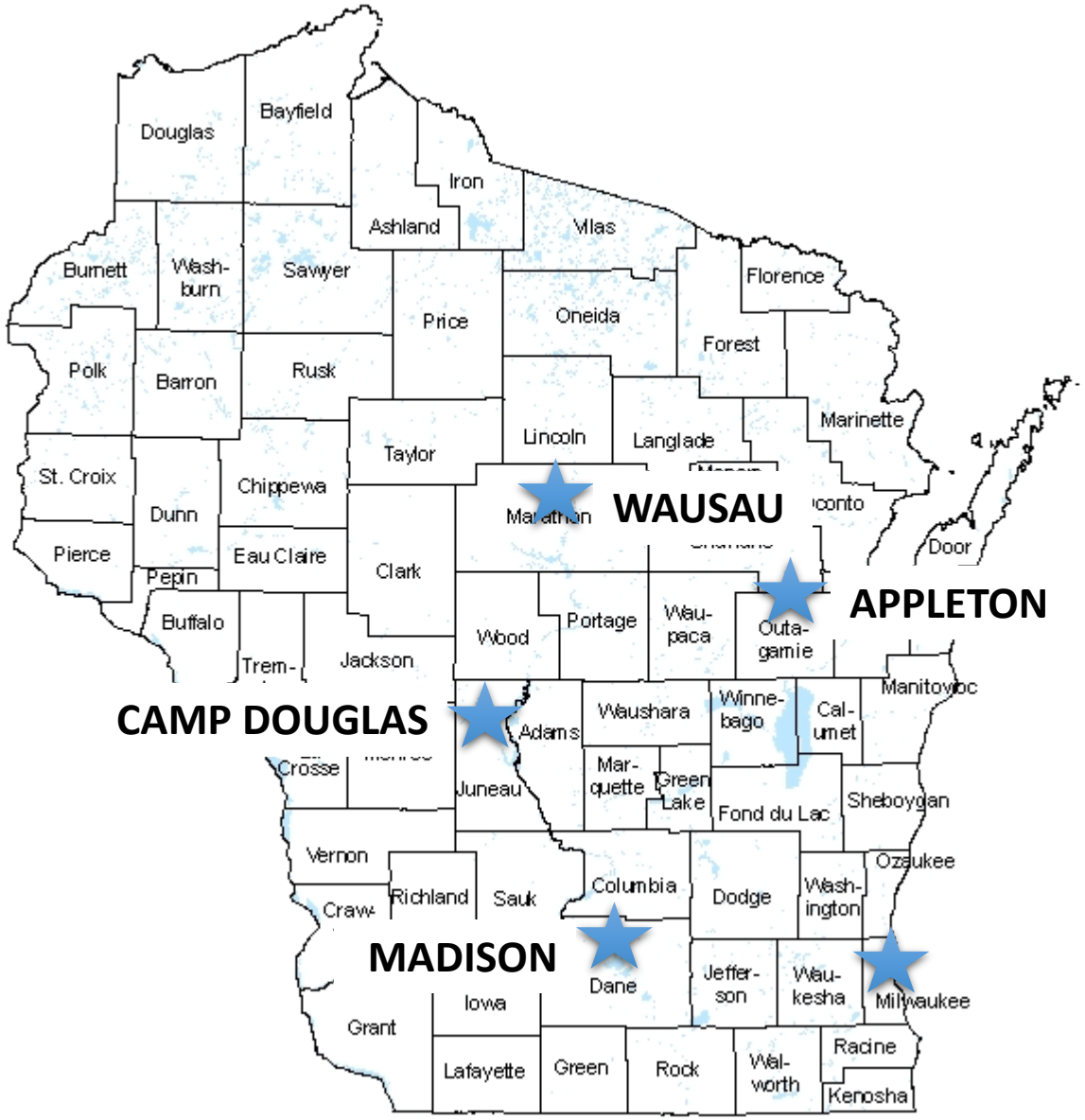
ABOUT WPI
SUPPORTING THE MISSION

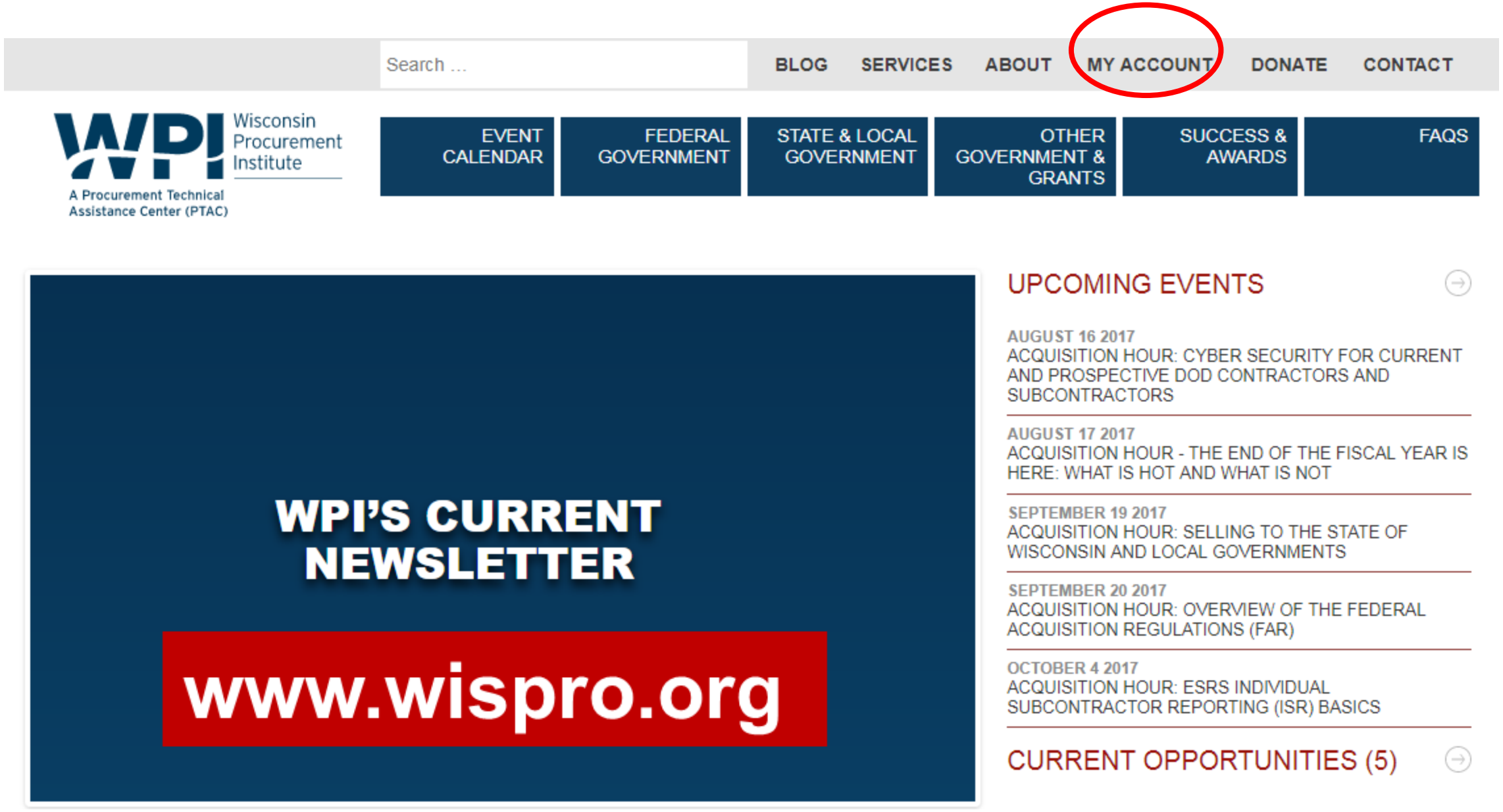
Assist businesses in creating, development and growing their sales, revenue and jobs through Federal, state and local government contracts.

Wisconsin Procurement Institute
A Procurement Technical Assistance Center

WPI OFFICE LOCATIONS

- MILWAUKEE – *Technology Innovation Center*
- MADISON –
  - *Madison Enterprise Center*
  - *FEED Kitchens*
- CAMP DOUGLAS– *Juneau County Economic Development Corporation (JCEDC)*
- WAUSAU – *Wausau Region Chamber of Commerce*
- APPLETON – *Fox Valley Technical College*




Search ...
BLOG
SERVICES
ABOUT
MY ACCOUNT
DONATE
CONTACT
Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
EVENT CALENDAR
FEDERAL GOVERNMENT
STATE & LOCAL GOVERNMENT
OTHER GOVERNMENT & GRANTS
SUCCESS & AWARDS
FAQS
WPI'S CURRENT NEWSLETTER
www.wispro.org
UPCOMING EVENTS
AUGUST 16 2017
ACQUISITION HOUR: CYBER SECURITY FOR CURRENT AND PROSPECTIVE DOD CONTRACTORS AND SUBCONTRACTORS
AUGUST 17 2017
ACQUISITION HOUR - THE END OF THE FISCAL YEAR IS HERE: WHAT IS HOT AND WHAT IS NOT
SEPTEMBER 19 2017
ACQUISITION HOUR: SELLING TO THE STATE OF WISCONSIN AND LOCAL GOVERNMENTS
SEPTEMBER 20 2017
ACQUISITION HOUR: OVERVIEW OF THE FEDERAL ACQUISITION REGULATIONS (FAR)
OCTOBER 4 2017
ACQUISITION HOUR: ESRS INDIVIDUAL SUBCONTRACTOR REPORTING (ISR) BASICS
CURRENT OPPORTUNITIES (5)

SERVICES OFFERED BY WPI

- FREE Bid Matching Services
- Individual Counseling and Assistance
- Locating Local, State and Federal Opportunities
- Government Market Strategy Development
- Training in use of Government websites and tools
- Assistance with System for Award Management (SAM) Registration
- Assisting in Market Research Process
- Development of Market Profile
- Small Business Subcontracting Plans Development, Outreach and Reporting
- Small Group Training
- Outreach and training with Local, State and Federal agencies
- Assist with Pre and Post Award Functions
- Assistance with Agency Specific Contracting Requirements
- Assistance with Contracting Regulations and Requirements, including FAR, DFAR, CFR
- Assistance with GSA Schedule Preparation and Administration
- Assistance with Local, State and Federal Certifications, including:
    - Service Disabled & Veteran Owned Small Business, HUBZone, Woman Owned Small Business, 8(a) Business Development Program
    - State
    - Local
    - DBE
- Bid review and Submission Assistance
- Proposal review and Submission Assistance
- Capabilities Statement and Related Government Marketing Material Development
- Assistance in Locating and Developing Teaming Partners and Subcontractors
- Updated Government Market Information

HUSCH BLACKWELL

Cybersecurity Readiness for Government Contractors

Mark Grider, Erik Dullea, and Sylvia Bartell

November 15, 2017

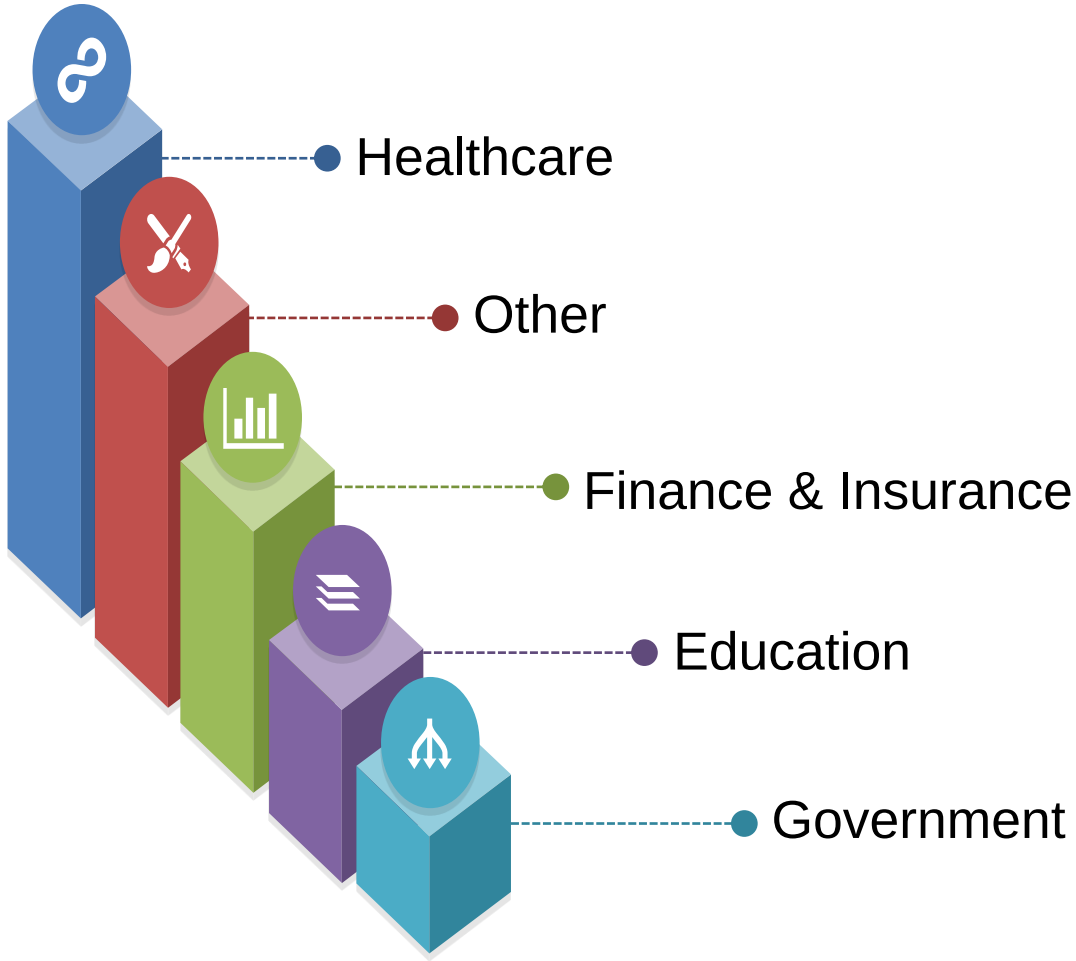
“There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again.”

– FBI Director Robert Mueller, 2012

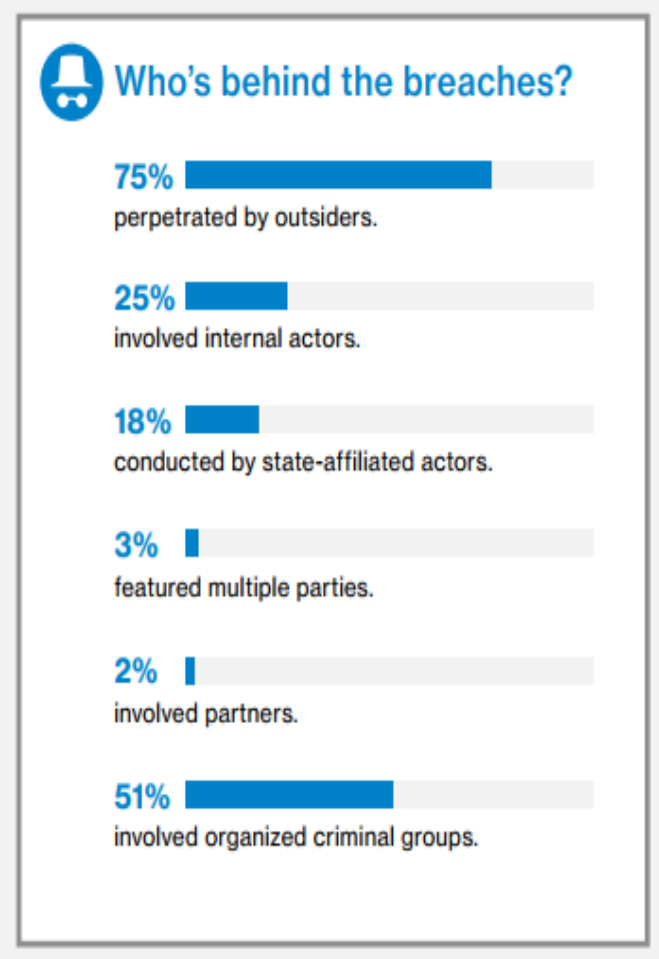
“An ounce of prevention is worth a pound of cure.”

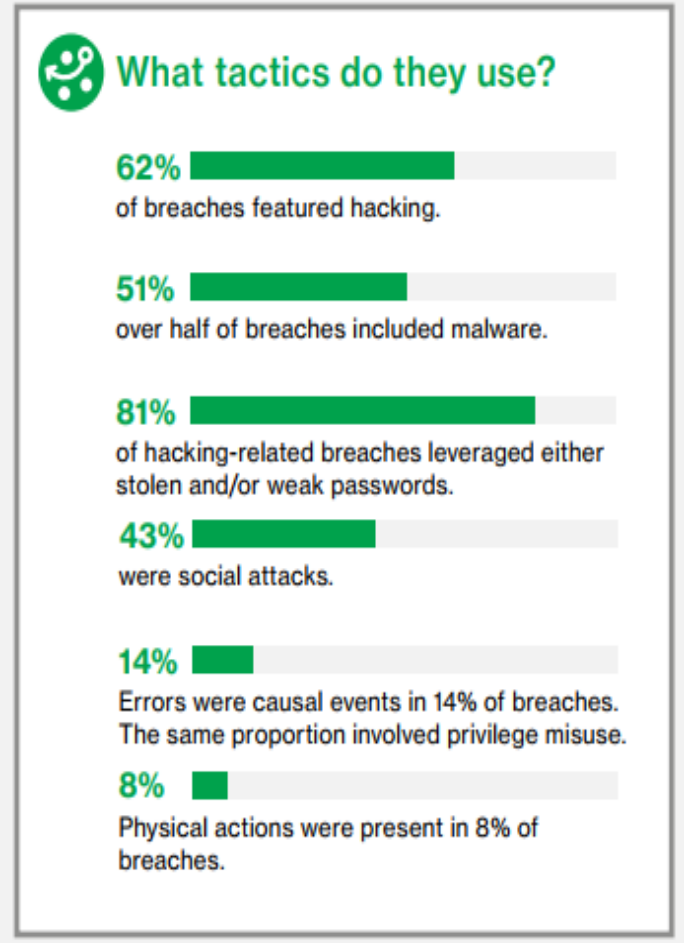
EQUIFAX

WHO DO HACKERS TARGET?



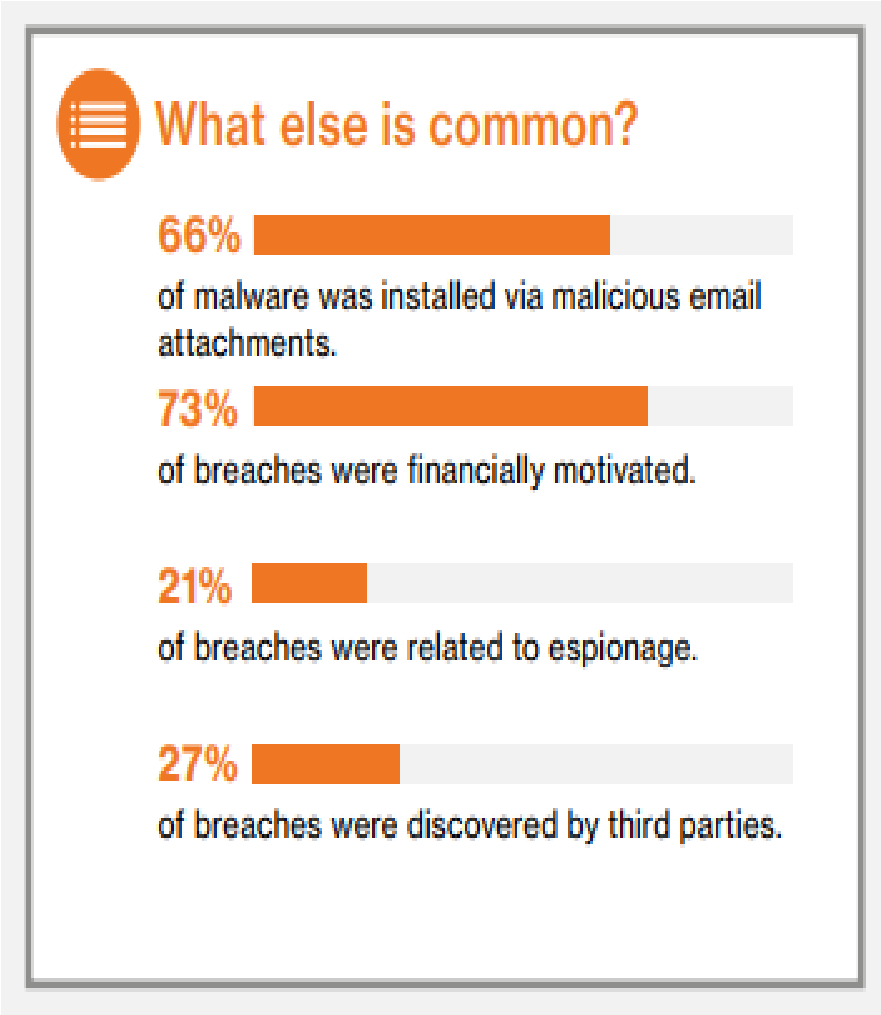
INCIDENT PATTERNS & TACTICS





Source: Verizon 2017 Data Breach Investigations

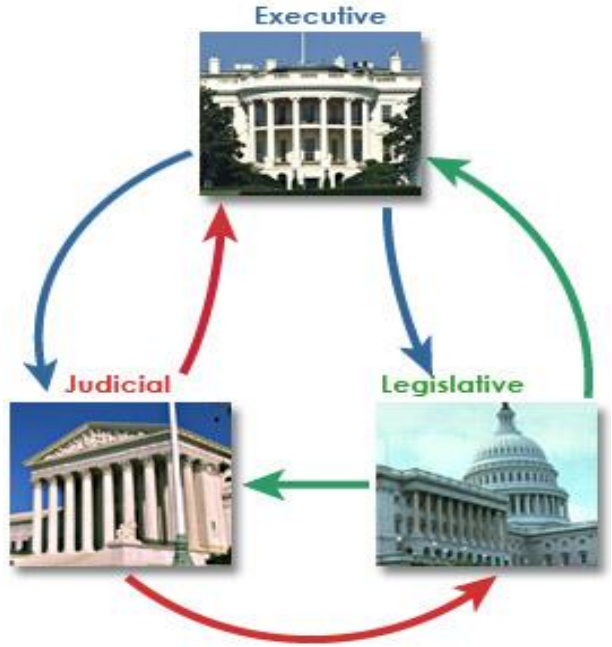
BREACH PATTERNS



Source: Verizon 2017 Data Breach Investigations

ROLE OF THE GOVERNMENT

- Legislation
- Executive (Regulatory) Action
- Judicial Involvement
- Private Sector Influence
- International Agreements



ENFORCEMENT & LAWSUIT POTENTIAL

Breaches may result in lawsuits:

- Government enforcement
  - Consumer Financial Protection Bureau
  - Fed. Trade Comm'n
  - Dept. of Justice (Civil Rights & HIPAA)
- Shareholder suits
  - BOD breach of fiduciary duties
- Breach of contract
  - NDA's, Reps & Warranties
- Class action suits
  - Consumer credit card owners
- State enforcement actions
  - Ex: California's "reasonable care" statute

LEGISLATIVE ACTIVITY

- Government (generally playing catch up)
  - Speed of Law lags the Speed of Technology
  - Ex: Facebook introduced in 2006; iPhone introduced in 2007

- How fast does Congress act?
  - Health Ins. Portability and Accountability Act (HIPAA) 1996
  - Financial Svcs. Modernization Act (Gramm-Leach-Bliley) 1999
  - Sarbanes-Oxley Act (SOX) 2002
  - Consumer Financial Protection Act (CFPA) 2010
  - Cybersecurity Information Sharing Act (CISA) 2015

EXECUTIVE ACTIVITY

- Executive Orders – President Obama signed two in 2016
  - Cybersecurity National Action Plan
  - Fed. Privacy Council – 24 agency stakeholders involved
- NIST Cybersecurity Framework for Critical Infrastructure (2/2014)
  - More of a process or practice than a standard
  - Request for Info published – 2015; Workshop – 2016; Draft Ver. 1.1 – 2017
- Contractors new requirements effective Dec. 2017

OVERLAPPING CRIMINAL AND NATIONAL SECURITY CONCERNS

- UK attributed global WannaCry ransomware attacks to North Korea
- North Korean hackers have stolen bitcoin, held data ransom, and robbed foreign banks
- North Korea may believe it can remotely attack and degrade the financial systems, telecom infrastructure, energy utilities, and media networks of US and its allies in response to conflict

Real Clear Defense – *Cyber Crime: NK's Billion Dollar Soft Spot,* Nov. 10, 2017

DOD GOVERNMENT CONTRACTING

- DOD Fed. Acq. Reg. Supplement (DFARS) Subpart 204.73
  - Safeguarding Covered Defense Information and Cyber Incident Reporting
    - Applies to contracts and all subcontracts
    - Must safeguard DOD info on its networks
    - Covers Unclassified Information
    - Must rapidly report cyber incidents
      - Rapidly Report is defined as 72 hours
    - Subcontractors report incidents to their higher tier contractor
- Contract clauses covering this topic are found at: 252.204-7008, 7009 and 7012

DOD GOVERNMENT CONTRACTING

- What Must Contractors Submit?
  - CO's refer to PGI 204.7303-4(c) for contractors' submissions of media and malicious software
- What Are the Repercussions for the Contractors?
  - Cyber incident shall not, *by itself*, mean the contractor failed to provide adequate security
  - By submitting an offer, contractors represent they will implement security requirements specified by National Institute of Standards and Technology (NIST)
  - If contractors discover and isolate malicious software, they must submit the malicious software to DoD Cyber Crime Center (DC3)

NON-DOD GOVERNMENT CONTRACTING

- FAR Subpart 4.19
  - Basic Safeguarding of Covered Information Systems
    - Applies to all acquisitions, including acquisitions of commercial items other than commercially available off-the-shelf items
  - FAR contract clause 52.204-21 inserted into all contracts
    - When the contractor may have contract information residing in or transiting through its network
    - Contractor shall apply the basic safeguarding requirements and procedures to protect covered contractor information systems
      - 15-item list of specifics
  - 52.204-21 flows down to all subcontractors
- Consider adding Cybersecurity to your Ethics & Compliance Program

10 Key Components of Breach Response

SECURITY

- Harden the system (*this is an ongoing process*)
- Be aware of hackers' typical first two moves:
  - Insert covert channel (Trojan Horse)
  - Delete all traces of insertion

LEGAL

- Maintain privileges
  - Attorney/client privilege
  - Work product doctrine
  - Privileges are NOT retroactive
- Determine whether there are reporting requirements under applicable law or contract. Comply promptly.

FORENSICS

- Separate skill set than IT
- Appearance of objectivity is important
- Third-party forensics make privileges easier to maintain

LAW ENFORCEMENT

- Is it a crime?
- Find the right law enforcement agent
- Maintain secrecy with friendly grand jury subpoena
- Whether and when to call
- Public relations implications

REGULATORS

- Federal Trade Commission (FTC)
- U.S. Department of Health & Human Services Office for Civil Rights (HHS-OCR)
- 48 Attorneys General (depending on impacted person's state of residence)

INSURANCE COVERAGE

- Coverage must be evaluated
- Cyber insurance policy
  - Panel providers
  - Losses covered
- Complying with policy requirements
- Timing of notifications

PUBLIC RELATIONS

- Communication plan, including leak plan
- Consistent message over time
- Prepare in advance:
  - Press release
  - FAQs

STAKEHOLDERS

- Customers
- Management
- External auditor
- Business associates and contractual partners

NOTIFICATIONS

- Protected Health Information (PHI)
- Personally Identifiable Information (PII)
- Payment Card Industry (PCI)

PERSONNEL MANAGEMENT

- Organization must determine what action is warranted:
  - Counseling
  - Discipline
  - Termination
- Determine
- Act
- Communicate

HUSCH BLACKWELL

Background and Reference Slides

DEFINITIONS

- **Administrator Access**: a level of access above that of a normal user
- **BotNet**: network of private computers infected with malware and controlled as a group without the owners' knowledge (used for sending spam or DDoS)
- **Denial of Service** (DoS): an attack to make a machine or network resource unavailable to its intended users.
  - A *distributed denial-of-service* (DDoS) features an attack source from more than one – and often thousands of – unique IP addresses.
- **Malware**: malicious software that damages, disables, takes control of, or steals information from a computer system.
  - Computer Virus: a type of malware designed to spread from one computer to another
- **Phishing**: e-mail user is duped into revealing personal or confidential info
  - Spear phishing: A targeted phishing attempt that seems more credible to its victims and thus has a higher probability of success
- **Ransomware:** encryption of the user's personal data, or lock-out of the entire PC, after which the owner is told to pay a "ransom" via an anonymous service in order to unlock the data or computer

SPECTRUM OF ATTACKERS BY RESOURCE LEVEL

- High School Hacker
- Disgruntled Employee
- Information Access Advocates, e.g. Anonymous
- Organized crime rings (comprise > 80% of hackers)
  - Ex: Russian and Jamaican criminal enterprises
  - “Ransomware is the black plague of the Internet” (Cisco Security)
    - Hollywood Presbyterian Med. Center ransomware attack $17K
- Corporate Espionage (some are state-sponsored)
- State sponsored terrorists / Non-State Actors
  - Ex: ISIS desires to conduct cyberattacks against US critical infrastructure
- Nation-State Forces
  - China, Russia, Iran, North Korea, United States, Israel

IMPACT OF CERTAIN TYPES OF ATTACKS

- Phishing
  - Data brokers capture > 50 trillion data transactions per year
  - Brokers increased use of social engineering with custom-made invites
- Data Theft
  - In 2014, an American was the victim of ID theft every 2 seconds
  - SSNs are not the primary target, username and passwords are
- Data Manipulation (are you aware it happens?)
  - Hackers are normally in your system 229 days before detected
  - DNI James Clapper: *"Decision making by senior government officials, corporate executives, investors, or others will be impaired if they cannot trust the information they are receiving"*
- Physical Damage to computer networks
  - Ex, entity ARAMCO experienced the indiscriminate deletion of data & hard drive damage. It did not result in an oil spill, explosion or other major fault in Aramco operations, but it affected the company's business processes

SCOPE OF THE PROBLEM

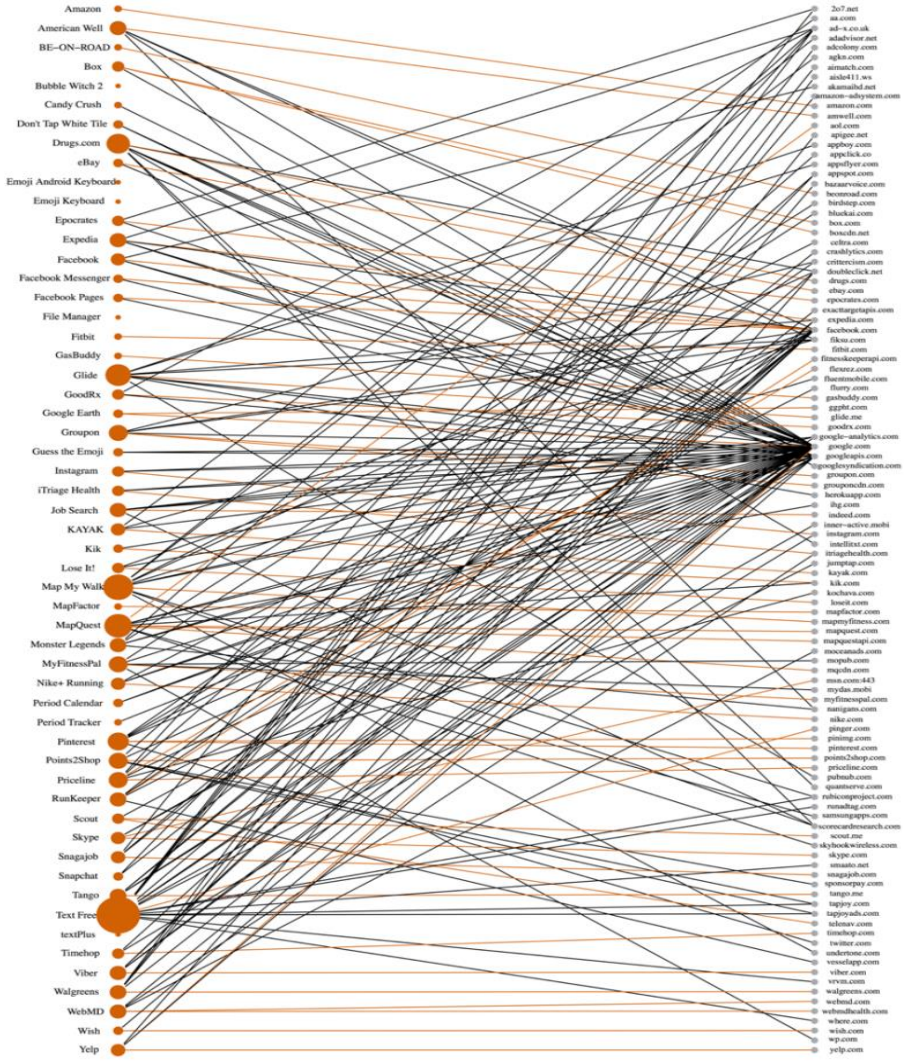
- The fundamental problem with computer security:
  - Legacy operating systems and applications we use today
    - Internet was designed to be a collaborative tool
    - Developed with little concern about potential for introduction of hostile or untrustworthy applications or data
- You're vulnerable because you're on the network
  - There is a reason malware was originally called a virus
    - Malware can be passed between your online acquaintances
    - Your subcontractors, partners, vendors may be the source of your data breach (renowned Government Contractors beware)
  - Transnational Commerce?
    - More risk of attacks and additional laws and regulations

SOFTWARE INTERACTION

Sharing of sensitive data: Android apps (left) with popular domains (right).

What can we do about it?

- IT Security
- Legislation
- Regulation
- Litigation



Source: http://www.thedatamap.org/

RESPONSE PLAN: WHAT YOU NEED

- Identify your team at the outset:
  - Internal team responsible for managing incident
  - Legal Team
  - Forensic Team
  - Law Enforcement
  - PR /Communications Team
  - Call Center Team
  - Credit Monitoring Service Team

RESPONSE PLAN: WHAT YOU NEED

- Prepare breach response checklist
- Identify sensitive information that could be compromised on your systems
- Compile key contracts and understand provisions
- Ensure you have appropriate insurance coverage
- Prepare draft press releases, notification letters and call center scripts
- Determine how and when employees and stakeholders will be notified

OTHER STEPS

- IT Review
  - Should be ongoing; there is no silver bullet that can prevent breach
  - Define Data Security Policies
  - Understand gaps and vulnerabilities
- Contract / Vendor Review
  - Ensure your contracts protect you
  - Ensure you are working with reputable vendors

JUDICIAL INVOLVEMENT

Litigation - legal theories are developing

- Choice of law & jurisdiction complicated by data roaming
- Attribution is complicated by anonymity (Cyberwarfare)
- Tendency to apply “old law” to new technology

OBLIGATIONS OF EMPLOYERS

- Corporate duties and obligations are expected from:
  - Executive Level - Board of Directors/Officers
  - Corporate Law Department
  - Outside Law Firms
- Sources of those duties and obligations?
  - Sarbanes Oxley Act
  - Duty of Care, Duty of Loyalty for corporate leaders
  - Model Rules of Professional Conduct for lawyers

DUTIES OF CORPORATE LEADERS

- Board of Directors' Role
  - Governance, Oversight, Strategic Direction, and Risk Management
    - *Does that include cyber security? YES, per the SEC*
  - SOX § 404: maintain control over financial reporting
- SEC Commissioner Luis Aguilar (June 10, 2014)
  - Boards of directors are responsible for overseeing the management of all types of risk … there can be little doubt that ***cyber-risk also must be considered as part of Board's overall risk oversight***
- California AG Kamala Harris (Feb. 2016)
  - Failure to implement the Center for Internet Security's Critical Security Controls is a lack of reasonable security
  - CA Code requires businesses that own, license, or maintain PII about CA residents implement and maintain reasonable security procedures and practices appropriate to the nature of the information

PUBLIC AND PRIVATE CORPORATIONS

- Private companies that only have Officers:
  - You are the new targets – assumption is you are less prepared
- SEC and SOX do not regulate privately-held companies, but the FTC authority applies to single-member and large privately-held entities
- Keep in mind:
  - Private companies are bought by public companies
  - Private companies contract & trade with public companies
  - What do your Reps & Warranties and NDA's say?
  - What if your data given to a public company is corrupted or manipulated?

CORPORATE OBLIGATIONS

- Corporate Responsibilities
  - Protect Employee Data (Office of Civil Rights case law)
  - Protect Customer Data (Payment Card Industry standards)
    - Regulatory Duties (Government Contractors)
    - Contractual Duties (Reps & Warranties, NDAs)
  - Protect financial data (SOX)
- Causes of Action – Federal and State
  - Agency Enforcement Actions (CFPB, FTC – unfair practices)
  - Derivative Lawsuits (duty of loyalty, duty of care)
  - Tort claims by business affiliates
  - Breach of Contract (reps & warranties and NDAs)
  - Government Enforcement (under applicable regulations)

CORPORATE OBLIGATIONS

- Role of a Corporation's Attorney (In House / Outside)
  - "Board oversight of cyber-risk management is critical to ensuring that companies are taking adequate steps to prevent, and prepare for, the harms that can result from such attacks."
  - ***"There is no substitution for proper preparation, deliberation, and engagement on cybersecurity issues***." SEC Comm. Aguilar
    - GC or outside counsel may have to tailor communication based on legal or business audience
- Determine if your company has or needs a Chief Information Security Officer (CISO)
- Determine who your "Network Security Expert" works for
  - The IT Department or the Legal Department?
  - This decision could be a factor in "preparation"

ATTORNEY OBLIGATIONS – RULES OF PROFESSIONAL CONDUCT

- Competence (Rule 1.1)
  - What level of cybersecurity understanding is expected?
  - What protections are in place (insurance)?
    - D&O Insurance generally covers the GC for advice on company's operation
    - Employed Lawyers Professional Liability insurance for in-house lawyers.
- Communication (Rule 1.4)
  - How do you notify your client?
  - How do you notify your client's customers?
- Confidentiality of Information (Rule 1.6)
  - Most important duty for attorneys (and arguably HR)
  - This duty permeates the legal team's activity
    - Not limited to legal advice

INSURANCE COVERAGE FOR CYBER

- Directors and Officers (D&O) insurance provides coverage to general counsel (GC) for advice given on company's operation
  - Typically no coverage for the GC's more traditional legal services
  - No coverage under D&O for legal services of other in-house attorneys
- Errors and omissions (E&O) policies likewise do not generally cover negligence by in-house counsel.
  - E&O coverage typically extends to mistakes made by a company in delivering its professional services.
  - In-house lawyer's malpractice is often excluded and argued to arise out of professional services delivered to an insured business, not to its customers.
- Employed Lawyers Professional Liability (ELPL) insurance better meets the needs of in-house lawyers.

CORPORATE LAWSUITS

- *FTC v. Wyndham Worldwide Corp.* (3d. Cir. August 2015)
  - Federal Trade Commission sued Wyndham and three subsidiaries for breaches of customer data by Russian hackers
    - Inadequate cybersecurity resources allocated by Wyndham
  - Third Circuit upheld FTC's use of § 5 of the FTC Act to challenge Wyndham's data security lapses
  - Case went back to the district court & settled Dec. 23, 2015
- *Dennis Palkon v. Stephen Holmes*, (D.C.N.J. 2014)
  - ***Unsuccessful shareholder suit***
  - Court applied the Business Judgment Rule
  - BOD had 13 meetings on Cybersecurity
  - General Counsel had briefed the Board on cybersecurity
  - Audit Committee analyzed the topic
  - **These details Mattered to the Court**

DATA BREACH LAWSUIT/SETTLEMENTS

- *In re The Home Depot, Inc., Customer Data Security Litigation,* No. 1:14-md-02583-TWT (N.D. Ga. Sept. 2015)
  - Class action suit on behalf of 55 million consumer cardholders
  - Class Action settled for $13MM in settlement funds and $6.5MM in identity and credit protection services
- *Bekken v. Home Depot* , No. 1:15-cv-2999-TWT (N.D. Ga Sep. 2015) (shareholder lawsuit alleging directors and officers failed to ensure customer data was protected)
  - Alleged company officials:
    - Were aware the company's systems were "desperately out of date"
    - Knew the company was vulnerable to a data breach.
    - Were "complacent" leaving vulnerabilities in place that "allowed hackers to enter the system undetected, and permitted them to continue siphoning customer cardholder and personal data for almost five months without detection."
    - Failed to implement and maintain an adequate fire wall
  - Alleged protective measures the company failed to put in place were required by the credit card industry.

PREPARE FOR THE RISK OF CYBER ATTACKS

- Not **If** but **When**
  - "Advanced targeted attacks are easily bypassing traditional firewalls and signature-based prevention mechanisms."
  - Human behavior still the weakest link:
    - Opening suspicious e-mails and links (ARAMCO in Saudi Arabia)
    - Obvious passwords
- Cyber defense is a continuous process and change in mindset
  - Cyber defense should become your new normal
    - Akin to teaching children to "buckle their seatbelt"
- Attackers use any entry point to access networks
  - To harm a company, attackers do not need to hack CEO
    - Any employee with network access is an entry point
    - Attackers move laterally within the network
    - After gaining access, hackers target individuals with System Administrator access rights

RESPONSE TO AN ACTUAL BREACH

- Plan ahead with best practices
- Immediate Actions (first 24 hours)
  - Initial Assessment
  - Minimize Continuing Damage
  - Record and Collect Information
  - Notify
- Post-Recovery Actions
  - Monitor for additional activity
  - Lessons Learned

ACQUISITION HOUR LIVE WEBINAR SERIES

- November 28, 2017 – **The HUBZone Program – Certification Benefits and New Regulations** – CLICK HERE for additional information – presented by Shane Mahaffy, Lead Business Opportunity Specialist, US.Small Business Administration (SBA)
- November 29, 2017 – **Overview of CPARS** – CLICK HERE for additional information – presented by Carol Murphy – Wisconsin Procurement Institute (WPI)
- November 29, 2017 – **Cyber Security and Technology** – CLICK HERE for additional information – presented by George Chavez, Chavez Consulting, LLC
- December 5, 2017 – **The SBA 8(a) Certification Program** – CLICK HERE for additional information – presented by Shane Mahaffy, Lead Business Opportunity Specialist, US.Small Business Administration (SBA)
- December 6, 2017 – **Cyber Security for Current and Prospective DOD Contractors and Subcontractors** – CLICK HERE for additional information – presented by Marc Violante – Wisconsin Procurement Institute (WPI)
- December 12, 2017 – **Intellectual Property for Government Contractors and Subcontractors** – CLICK HERE for additional information – presented by Laura J. Grebe, Attorney, Husch Blackwell LLP

UPCOMING EVENTS

National Contract Management Association, Wisconsin Chapter: **End of Year Federal Contractor Update**

January 17, 2018 - Milwaukee, WI

UPCOMING EVENTS

Pre-Marketplace Series: Money, Markets and Margins (M3) – Increasing Your Profitability, Networks and Net Worth

November 16, 2017 – Ashland, WI

November 30, 2017 – Wauwatosa, WI

December 6, 2017 – Green Bay, WI

UPCOMING EVENTS

MARKETPLACE 2017 – Governor's Conference on Minority Business Development **– December 13 – 14, 2017 – Milwaukee, WI**

QUESTIONS?

Mark Grider
Partner, Washington, D.C.
202.378.2353
mark.grider@huschblackwell.com

Erik Dullea
Senior Counsel, Denver, CO
303.749.7246
erik.dullea@huschblackwell.com

Sylvia Bartell
Associate, Washington, D.C.
202.378.2368
sylvia.bartell@huschblackwell.com

SURVEY

CONTINUING PROFESSIONAL EDUCATION

CPE Certificate available, please contact:

Benjamin Blanc

benjaminb@wispro.org

WPI CONTACT

Wisconsin Procurement Institute (WPI)
www.wispro.org

Benjamin Blanc, CFCM, CPPS | Government Contract Specialist
Benjaminb@wispro.org 414-270-3600

10437 Innovation Drive, Suite 320
Milwaukee, WI 53226