Cyber to SWOT

Marc N. Violante

WISPRO

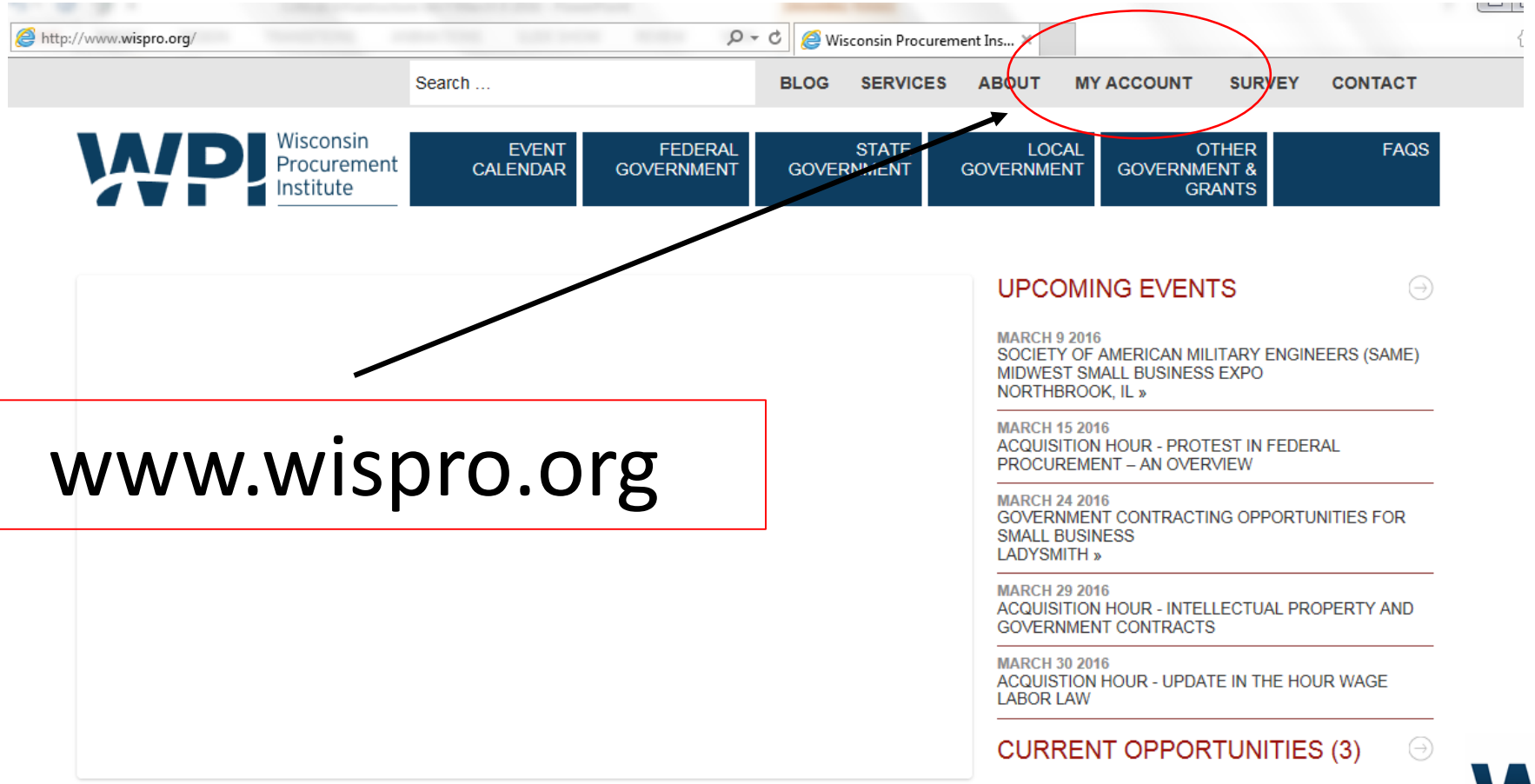
Wisconsin Procurement Institute

Today’s topics

- Accessing the presentation
- Cyber issues
- Frameworks and questions
- How to stay current
- Resources
- Tools

Wisconsin Procurement Institute

Access this presentation & others



www.wispro.org

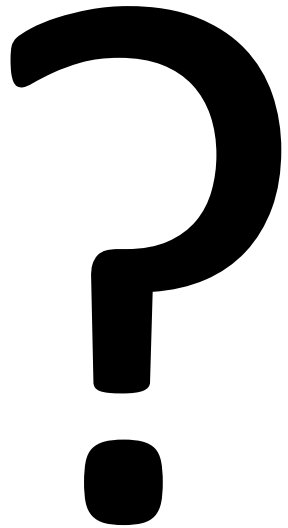
WPI Wisconsin Procurement Institute

Probably not the intended approach

Wisconsin Procurement Institute

Cyber – Key question

- Is anti-virus enough and changing passwords good enough?



Wisconsin Procurement Institute

General issues

- Growing
- Evolving
- Not just passwords
- Sophisticated
  - Individuals, nation-states, repositories of resources/tools
- Active penetration –
  - Motivations might be -- challenge, game, treasure hunt, bragging rights
- Breaches not identified for significant amount of time
- Breach = total access

“The Spies had come without warning. They plied their craft silently, stealing secrets from the world’s most powerful military. They were at work for months before anyone noticed their presence. And when American officials finally detected the thieves, they saw that it was too late. The damage done.”

Prologue: @War the Rise of the Military Internet Complex

Wisconsin Procurement Institute

Cyber – breach detection

"February 25, SecurityWeek – (International) **Breach detection time improves, destructive attacks rise: FireEye.** FireEye-owned Mandiant released a report titled, M-Trends which stated that current organizations were improving their breach detection rates after an investigation on real-life incidences revealed that the median detection rate improved from 205 days in 2014 to 146 days in 2015. The report also stated that disruptive attacks were a legitimate threat and gave insight into how organizations can prepare for and deal with such attacks.

Source: http://www.securityweek.com/breach-detection-time-improves-destructive-attacks-rise-fireeye "

Copied from: DHS Open Source Daily Infrastructure Report, Item 18, February 29, 2016

WPI Wisconsin Procurement Institute

semper vigilans – Latin for always vigilant

Source:https://en.wikipedia.org/wiki/List_of_Latin_phrases_(S)ce:

Wisconsin Procurement Institute

Shift in Thinking

- Not
  - Computers
  - Networks
  - Devices
- Intellectual property
- Company
- National

Wisconsin Procurement Institute

Frameworks

- SP 800-53
- SP 800-171
- NIST 32 – Establishing or Improving a Cyber Security Program
- Referenced in DFARS (252.204-7008/7012)
- 252.204-7000 “Mother may I”

- Framework for Improving Critical Infrastructure Cybersecurity, NIST, February 12, 2014

Wisconsin Procurement Institute

Personnel

- Are employees provided any IT training?
- Are employees screened prior to granting access to the IT system?
- Are third party vendors who have access to the IT system screened?
- Do you travel with your business laptop?

Office procedures

- Who has access to your network?
- Does each employee have their own computer?
- Are computers shared?
- Do all employees have access to all information?
- Are passwords used to protect folders and files?
- Are employees required to change their passwords?
- Does each computer have anti-virus software loaded and enabled?
- Are IT functions accomplished in-house or by a third party?
- Do you monitor your network?

Business Relationships

- Do you openly share information/files with suppliers?
- Do you verify that your suppliers can have access to information that you plan to share?
- Are you aware of the different regulations governing protection of data?
- Have you read and researched the regulations that apply to governing data and unclassified information?
- Do you pass down these requirements to your subcontractors/suppliers?

WPI Wisconsin Procurement Institute

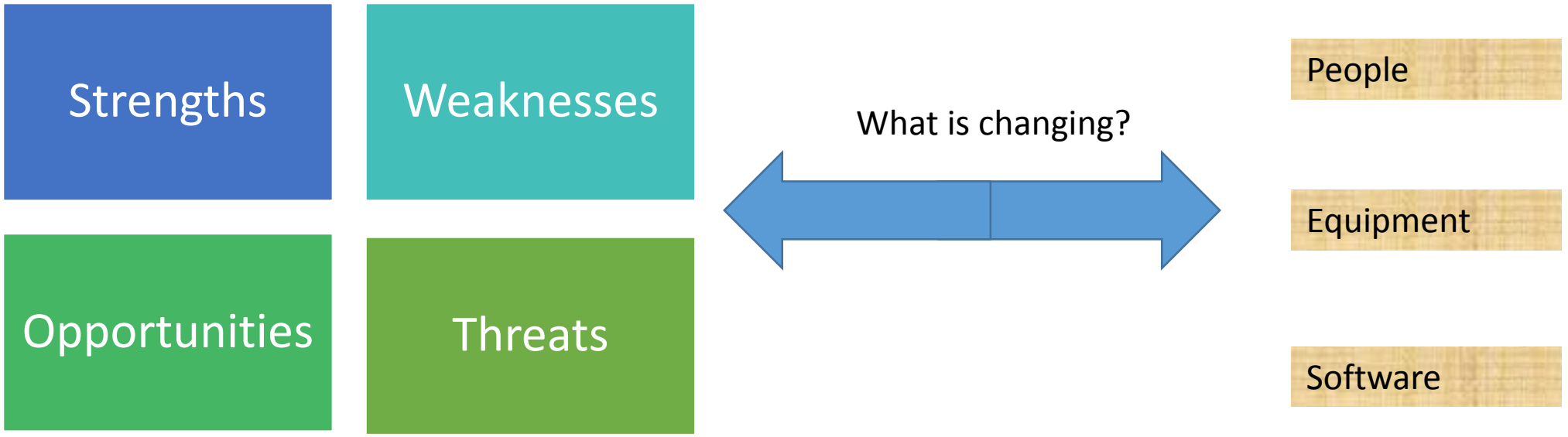
Hypotheticals

- Do you manage the contents (files) on USBs that you share?
  - With subcontractors
  - Vendors
  - At events – public use terminals
- Can you be sure that the contents of the drive were not copied?
- Do you pick up and use “Thumb Drives” from trade shows?
- Other sources?
- What are your policies?

Business Continuity Plan

- Identify critical functions
  - Redundancy
  - Training
  - Current information
  - Appropriate/acceptable authorization in place
- Evaluate (S, W, O, T)
- Identify critical vendors
- Succession planning
- Continuing if there is not access to computes/internet
- Bitcoin account – separate computer

WPI Wisconsin Procurement Institute



New CSO, New Network, New service provider, New third party vendor

Wisconsin Procurement Institute

Cyber Math

- (S, W, O, T) + Cyber =
  - Positive
  - Negative
  - Multiplier

Wisconsin Procurement Institute

Seagate Technology – phishing email

- Seagate Technology reported that its employees' personal information was compromised after a phishing email disguised as a legitimate internal company request **prompted an employee to disclose employee data** to an unauthorized third party. – *CNBC*

Copied from: DHS Open Source Daily Infrastructure Report, Top Stories, March 8, 2016

Wisconsin Procurement Institute

Cyber – phishing, spoofing, impersonation

"February 29, ZDNet – (International) **Snapchat falls foul of CEO impersonation, hands over employee pay data.** The video messaging application, Snapchat reported that many of its current and former employees' payroll information was compromised after a cyber-attacker impersonated the firm's chief executive officer (CEO) via a phishing campaign and collected employee payroll information from staff at the firm. Snapchat stated that the incident was contained and reported the scheme to the FBI.

Source: http://www.zdnet.com/article/snapchat-falls-foul-of-ceo-impersonation-hands-over-employee-pay-data/ "

Copied from: DHS Open Source Daily Infrastructure Report, Item 14, March 1, 2016

Wisconsin Procurement Institute

Cyber - ooooppppps

Social Media Risk

- “The threats and exposures are many and varied. They range from a single rogue employee to organized crime to terrorists to spying by other nations. The threats can be theft of confidential personal data or proprietary competitive information, to malicious acts causing loss of data or actual disruption of operations.
- For the energy industry, which handles hazardous materials, a hacking event that leads to a spill becomes more than just a bad day at the office. “

Copied from: http://www.riskandinsurance.com/fueling-cybersecurity/ visited, March 5, 2016

Wisconsin Procurement Institute

Cyber – other

"February 24, SecurityWeek – (International) **API flaw exposes Nissan LEAF cars to remote attacks.** A security researcher discovered that the application program interface (API) used by Nissan Motor Corporation to allow LEAF model owners to manage their vehicles from a mobile device was vulnerable to remote control hacks that can send requests to enable and disable the climate control, obtain information on the vehicle's status, and collect driving history using the Nissan LEAF's Vehicle Identification Number (VIN). The company is working to release a patch and has decided to disable its NissanConnect EV app until the vulnerability was addressed.

Source: http://www.securityweek.com/api-flaw-exposes-nissan-leaf-cars-remote-attacks "

Copied from: DHS Open Source Daily Infrastructure Report, Item 2, February 26, 2016

WPI Wisconsin Procurement Institute

Cyber – just the tip of the iceberg?

"I have one energy client that conducted an online search as part of an exposure assessment and found critical plans for some of its facilities out there on the Internet."

Copied from: http://www.riskandinsurance.com/fueling-cybersecurity/ visited, March 5, 2016

Wisconsin Procurement Institute

Uncharted waters - Bitcoin

March 6, Softpedia – (International) **First fully functional Mac ransomware spread via transmission BitTorrent client.** Researchers from Palo Alto reported that the official Transmission BitTorrent Web site used by Mac customers was allegedly hacked after researchers found that the Transmission Web site was replaced for Mac version 2.90, which came embedded with the KeRanger ransomware. The ransomware targets over 300 file extension types, uses Advanced Encryption Standard (AES) encryption to lock files, and demands a 1 **Bitcoin** payment fee.

Source: http://news.softpedia.com/news/first-fully-functional-mac-ransomware-spread-via-transmission-bittorrent-client-501411.shtml

Copied from: DHS Open Source Daily Infrastructure Report, Item 22, March 8, 2016

Cyber Insurance – Top Considerations

1. Establish the correct level of coverage you might need. While quantifying cyber risk in financial terms may still be more art than science, one starting point is through an internal audit to determine the total value of your company's data as well as the aggregate cost of a possible breach.
2. Carefully check definitions of terms such as "hackers," "attacks" or "incidents," and "breach"
3. Make sure that policies (and situations) meet your needs.
Keep in mind that your business might also need specific coverages such as extortion, intellectual property infringement and advertising injury.
4. Consider that many cyber insurance policies do not cover nontechnical attacks, such as an authorized person stealing confidential data.

Copied from SANS Reading Room: Quantifying Risk: Closing the Chasm Between Cybersecurity and Cyber Insurance, *Barbara Filkins, Marc 2016 pg.*

Wisconsin Procurement Institute

Cyber Insurance – Considerations

5. Know which business insurance policy covers that contingency.
6. Make sure that one policy does not negate another.
7. Ensure that policies cover more than just the immediate damage and any possible losses from litigation following a breach.
    - The ideal level of cyber insurance protection should cover a business for all costs associated with an
    - incident—discovery, investigation and remediation, as well as any court costs, judgments or penalties.
8. When you're talking to underwriters, find out how much weight they put on the security controls you already have in place. Judgments about the degree to which those controls reduce your company's risk, and therefore its cyber insurance premiums, can be made based on your company's history or the underwriter's own data and calculations.
9. Work closely with a broker you trust,

Copied from SANS Reading Room: Quantifying Risk: Closing the Chasm Between Cybersecurity and Cyber Insurance, *Barbara Filkins, Marc 2016 pg. 3*

Wisconsin Procurement Institute

Understanding Cyber

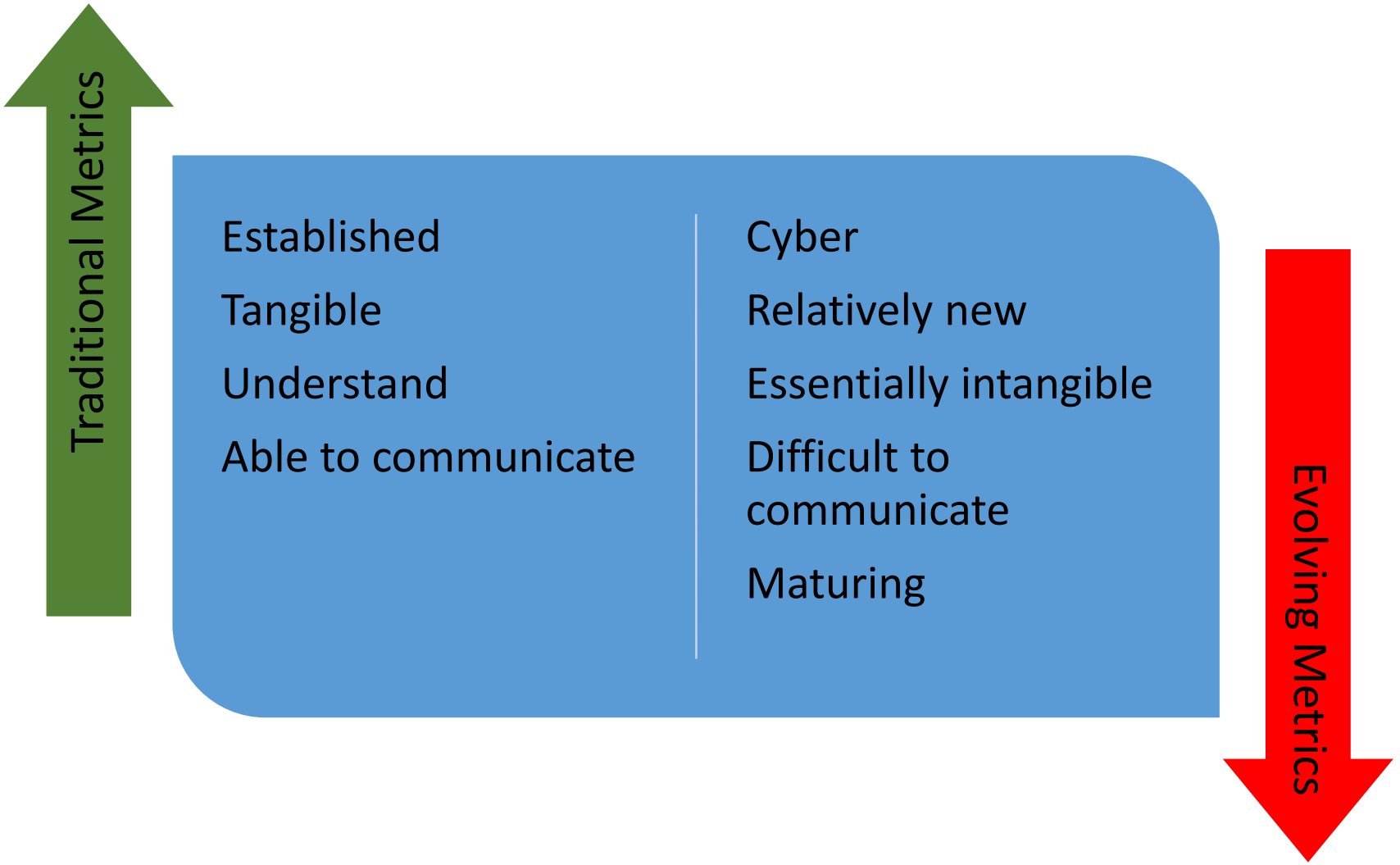
- At what level – internally
- To what degree?
- Process for keeping current?
- How is information shared?

Wisconsin Procurement Institute

Cyber v. Other considerations

- Financial Statements
- Plant visits
- Third party attestations – ISO, DCMA
- Public acceptance – brand recognition
- Longevity

Wisconsin Procurement Institute



Wisconsin Procurement Institute

Ransomware

- Individuals
- Police Department
- Hollywood Hospital
- Bitcoin
  - Several days to install
  - Must have access to a machine – may need to be dedicated

DoD's Defense Industrial Base (DIB) Cybersecurity and Information Assurance (CS/IA) Program

- Part 236, "Department of Defense (DoD)-Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities" of title 32, Code of Federal Regulations (CFR),
- DoD shares
  - unclassified and classified cyber threat information
  - IA best practices and related information, with participating DIB companies.
- In addition, relationships are established with company senior officials (e.g., Chief Information Officer (CIO), Chief Information Security Officer (CISO), etc) and their respective staffs. Your company's Chief/Facility Security Officer(s) also will be involved since DoD shares classified under the program.
- Eligibility

  Have or acquire DoD-approved medium assurance External Certificate Authority (ECA) certificates.

  Have an existing active Facility Security Clearance (FCL) granted under the National Industrial Security Program Operating Manual (NISPOM) (see DoD 5220.22-M) with approved safeguarding for at least Secret information

  Have or acquire a Communication Security (COMSEC) account in accordance with the NISPOM, Chapter 9, Section 4.

  Obtain access to DoD's secure voice and data transmission system supporting the DIB CS/IA program.

  Own or operate an unclassified information system that processes, stores, or transmits DoD information.

  Execute the standardized Framework Agreement (FA), which implements the requirements set forth in part 236, title 32 CFR, sections 236.4 through 236.6.

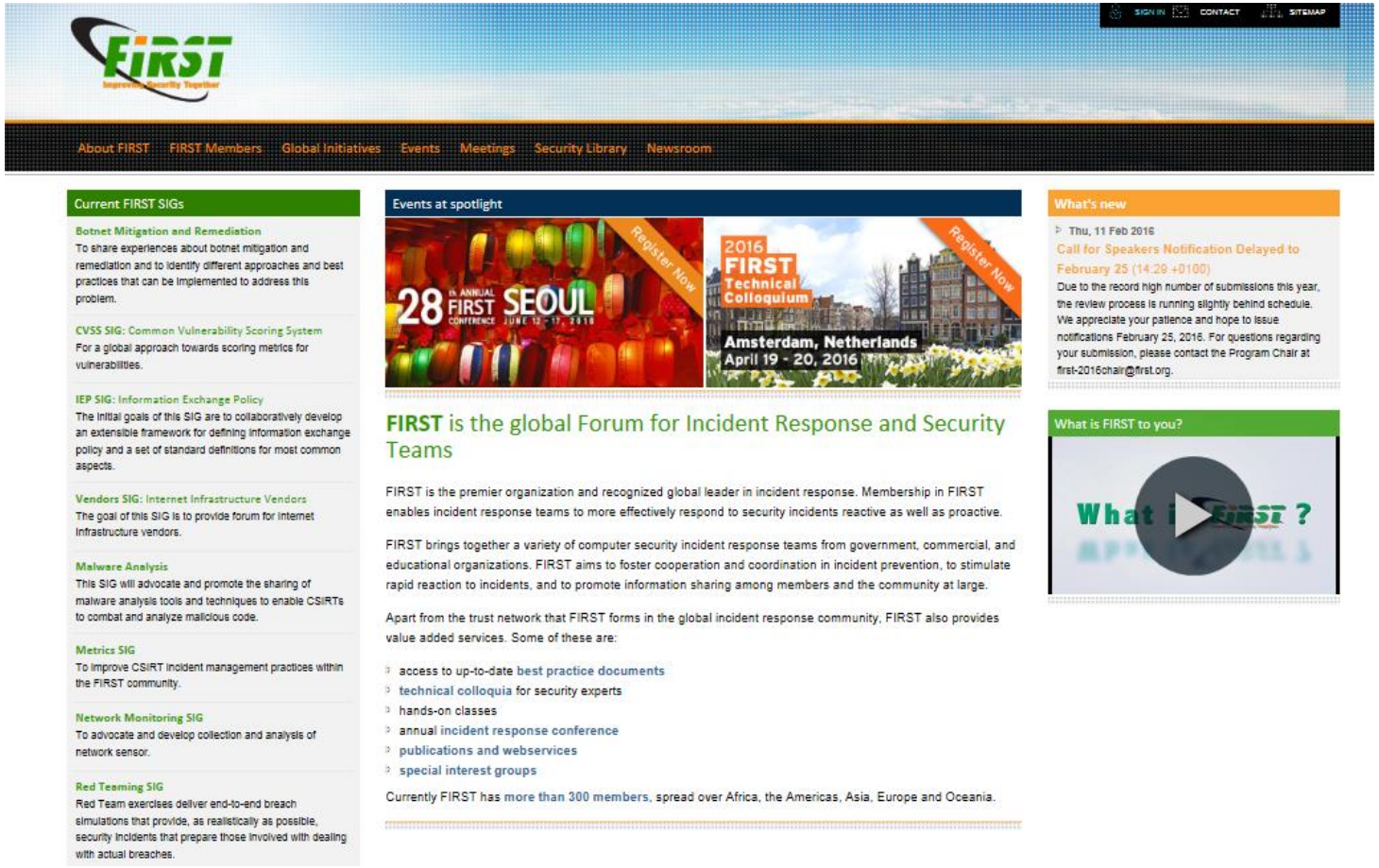
WPI Wisconsin Procurement Institute

InfraGard

InfraGard is a partnership between the FBI and the private sector. It is an association of persons who represent businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the U.S.

Source: www.infragard.gov

First.org



Wisconsin Procurement Institute

Take advantage of resources and tools

WPI Wisconsin Procurement Institute

Resources

- Cybersecurity Workforce Planning Diagnostic
  - https://niccs.us-cert.gov/careers/cybersecurity-workforce-planning-diagnostic
- NICCS: https://niccs.us-cert.gov/training/tc/search - Training Catalog
  - 2,000 courses
- SANS institute
- Veterans have access to FREE cybersecurity training!
  - SANS

WPI Wisconsin Procurement Institute

Veterans have access to free training

https://niccs.us-cert.gov/training/fedvte

https://www.sans.org/cybertalent/vetsuccess-pilot?msc=sctslider

WPI Wisconsin Procurement Institute

Interesting books

- Lights Out – Ted Koppel
- Future Crimes –Mark Goodman
- Social Engineering: The Art of Human Hacking, Christopher Hadnagy and Paul Wilson
- Hacked Again - Scott N. Schober
- Black Code Surveillance, Privacy, and the Dark Side of the Internet, Ronald J. Deibert
- @War: The Rise of the Military-Internet Complex Shane Harris
- Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet, Joseph Menn
- Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground, Keven Poulsen

WPI Wisconsin Procurement Institute