CYBER FUNDAMENTALS FOR DFARS 252.204-7012 IMPLEMENTATION

Image source: readywisconsin.wi.gov

Marc N. Violante

Wisconsin Procurement Institute

August 16, 2017

What happens when ----

Ours

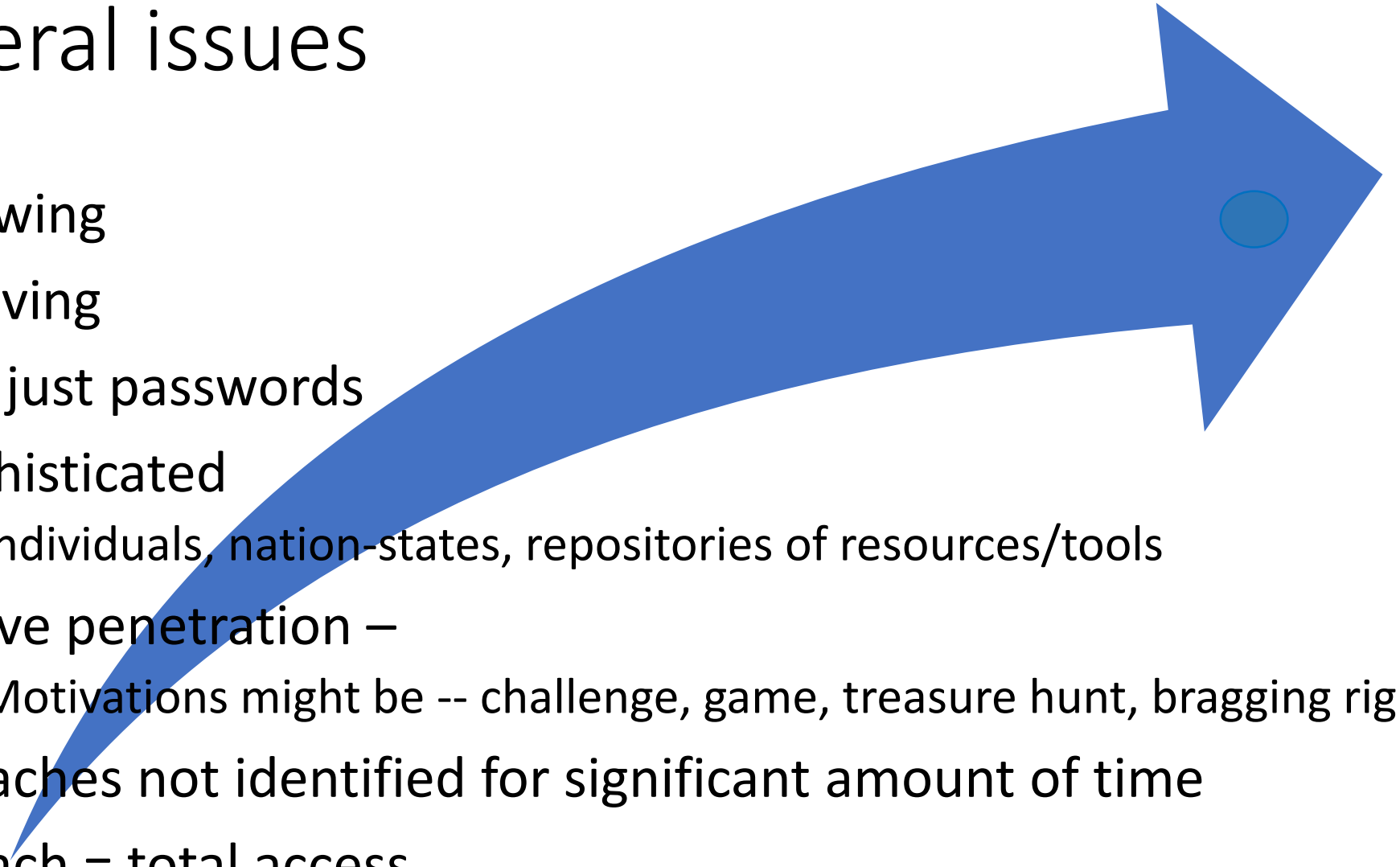
Theirs

Images copied from: eglin.af.mil

Webinar Overview

1. Background
2. Definitions
3. Threats
4. Actions
5. Resources
6. Moving forward

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

In the News – Summer of 2015

- Several of NY must prestigious trusted law firms
- Under cyberattack – trio of Chinese hackers
- Snuck in to law firm network via tricking partners into revealing email passwords
- Once in – snooped – highly sensitive document related to M&A's
- Then from ½ around the world, traded on that info – netting $4M
- "You are and will be the targets of cyberhacking, because you have information valuable to would-be criminals
- Aha moment – how vulnerable and defenseless

Jeff John Robers and Adam Lashinsky, Fortune, July 1, 2017, 52-59

In the News – Summer of 2015 – Hacker's view

- "Expensive data-security systems and high-priced information security consultants don't faze today's hackers."
- Hackers have – time and resources
- In the NY Law firm case, "attackers attempted to penetrate targeted servicers more than 100,000 times over seven months."
- "It has become abundantly clear that no network is completely safe. "

Jeff John Robers and Adam Lashinsky, Fortune, July 1, 2017, 52-59

In the News – Summer of 2015 – key point

"Where once companies thought that they could defend themselves against and onslaught, they're now realizing that resistance is, if not futile, certainly less important than have a plan in place to detect and neutralize intruders when they strike."

Jeff John Robers and Adam Lashinsky, Fortune, July 1, 2017, 52-59

DoD awareness of the issue

Secretary of Defense Jim Mattis visits Google Headquarters
Press Operations
Release No: NR-287-17
Aug. 11, 2017 Alpha 15
PRINT | E-MAIL
Chief Pentagon Spokesperson Dana W. White provided the following readout:

Today Secretary Jim Mattis visited Google headquarters and met with leadership to discuss innovative new technologies and methods to best leverage advancements in artificial intelligence, cloud computing and cyber-security for the Department of Defense.

The secretary emphasized that the DoD must continue to be a smart user of commercial technology and able to innovate at the speed of relevancy.

Official website of the Department of Homeland Security

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

5 Questions CEOs Should Ask About Cyber Risks

1) How Is Our Executive Leadership Informed About the Current Level and Business Impact of Cyber Risks to Our Company?
2) What Is the Current Level and Business Impact of Cyber Risks to Our Company? What Is Our Plan to Address Identified Risks?
3) How Does Our Cybersecurity Program Apply Industry Standards and Best Practices?
4) How Many and What Types of Cyber Incidents Do We Detect In a Normal Week? What is the Threshold for Notifying Our Executive Leadership?
5) How Comprehensive Is Our Cyber Incident Response Plan? How Often Is It Tested?

Who is visiting your site?

https://analytics.usa.gov/ visited 8/9/2017

Visits in the Past 90 Days

There were **2.28 billion** visits over the past 90 days.

Devices

Desktop	55.8%
Mobile	38.6%
Tablet	5.7%

Based on rough network segmentation data, we estimate that **less than 5%** of all traffic across all agencies comes from US federal government networks.

Much more detailed data is available in **downloadable CSV and JSON**. This includes data on combined browser and OS usage.

Browsers

Chrome	45%
Safari	27.1%
Internet Explorer	14.3%
11.0	12.7%
7.0	1%
10.0	0.3%
9.0	0.2%
8.0	0.1%
Other	< 0.1%
Firefox	6.4%
Edge	3.7%
Android Webview	1.1%
Safari (in-app)	1.1%
Other	1.3%

Operating Systems

Windows	46.9%
7	24.2%
10	18.4%
8.1	2.9%
XP	0.6%
8	0.5%
Other	0.4%
iOS	25%
Android	18.1%
Macintosh	8.5%
Other	1.4%

https://analytics.usa.gov/ visited 8/9/2017

Visitor Locations Right Now

Cities

New York	4%
Washington	3.1%
Chicago	1.7%
Los Angeles	1.6%
Plano	1.6%
Houston	1.3%
Dallas	1%
San Diego	1%
Seattle	0.9%
Kansas City	0.8%

Countries

United States	85.5%
International	14.5%
Mexico	1.6%
Canada	1.4%
India	1.1%
United Kingdom	0.9%
Colombia	0.6%
Spain	0.6%
Argentina	0.5%
Brazil	0.4%
Chile	0.4%
Germany	0.3%
Peru	0.3%
Puerto Rico	0.3%
Philippines	0.2%
Ecuador	0.2%
France	0.2%

https://analytics.usa.gov/ visited 8/9/2017

Visitor demographics for all participating agencies

Description	Download	Update frequency
Language	CSV JSON	Daily
Visitors per country	JSON	Every 5 minutes
Visitors per city	JSON	Every 5 minutes
Desktop/mobile/tablet	CSV	Daily
Web browsers	CSV JSON	Daily
• Versions of Internet Explorer	CSV JSON	Daily
Operating systems	CSV JSON	Daily
• Versions of Windows	CSV JSON	Daily
OS & browser (combined)	CSV JSON	Daily
Windows & browser (combined)	CSV JSON	Daily
Windows & IE (combined)	CSV JSON	Daily
Screen sizes	CSV JSON	Daily
Device model	CSV JSON	Daily

https://analytics.usa.gov/ visited 8/9/2017

What data/information is on your computer?
On your Network?

Risks - Identify and Prioritize Information Types

	Example: Customer Contact Information	Info type 1	Info type 2	Info type 3	…
Cost of revelation (Confidentiality)	*Med*				
Cost to verify information (Integrity)	*High*				
Cost of lost access (Availability)	*High.*				
Cost of lost work	*High*				
Fines, penalties, customer notification	*Med*				
Other legal costs	*Low*				
Reputation / public Relations costs	*High*				
Cost to identify and repair problem	*High*				
Overall Score:	*High*				

NIST Publication **NISTIR 7621 Revision 1, Small Business Information Security:** *The Fundamentals* Celia Paulsen Patricia Toth, Table 1, 10

Current Status – ongoing process

No issues

- Review complete, no issues identified

Unknown

- Reviews in progress
- Issues/questions require resolution

Issues present

- Unauthorized logins
- Questionable log activity
- External information – complaints, issues, other

Key Decision(s)

- Internal
  - Staff, full time, other duty as assign
  - Staff, part time, dedicated
- External – subcontract/consultant
- Staff
  - Awareness
  - Training
  - Refresher training
  - Updates to requirements

DFAR 252.204-7012

- Contractor systems with – Covered Defense Information
  - transiting | stored | transmitted from
- Required to provide Adequate Security
  - Implement NIST(SP) 800-171
- Monitor network/system
- Perform investigation when required – breach
- Report to dibnet.mil within 72 hours
  - IASE Medium Security Certificate required, 3 – 7 days
  - Account with dibnet.mil, requires certificate

Indications of CDI

- Review/inventory of computer/system files / storage
- DFAR clause – 252.204-7012
- DFAR clause – 252.204-7000 (“Mother may I”)
- Reference to the Joint Certification Program (JCP)
- Reference to Distribution Statements
- Language (sic) Controlling Unclassified Military Technology
- Item – listed on USML, ITAR
- Prime states or requires
- Defined: https://www.archives.gov/cui/registry

“Mother may I” 252.204-7000

- (a) The Contractor shall not release to anyone outside the Contractor's organization any unclassified information, regardless of medium (e.g., film, tape, document), pertaining to any part of this contract or any program related to this contract, unless—

  (1) The Contracting Officer has given prior written approval;

  (2) The information is otherwise in the public domain before the date of release; or

  (3) determined in writing by the contracting officer to be fundamental research in accordance with National Security Decision Directive 189 … and other requirements

Joint Certification Program - requirements

- TO MANUFACTURE THIS ITEM, NON-JCP CERTIFIED SUPPLIERS MUST SUBMIT A CURRENT MANUFACTURING LICENSE AGREEMENT, TECHNICAL ASSISTANCE AGREEMENT, DISTRIBUTION AGREEMENT OR OFF-SHORE PROCUREMENT AGREEMENT APPROVED BY THE DIRECTORATE OF DEFENSE TRADE CONTROLS WITH THE OFFER, UNLESS AN EXEMPTION UNDER THE PROVISIONS OF ITAR SECTION, 125.4 EXEMPTIONS OF GENERALAPPLICABILITY, AND/OR EAR PART 740 ARE APPLICABLE.

Further dissemination of JCP Technical Data

- NOTE: JCP CERTIFIED CONTRACTORS WHO RECEIVE TECHNICAL DATA PURSUANT TO THEIR DD FORM 2345 CERTIFICATION MAY NOT FURTHER DISSEMINATE SUCH DATA UNLESS FURTHER DISSEMINATION OF THE TECHNICAL DATA IS EXPRESSLY PERMITTEDBY DODD 5230.25.

NON-JCP certified suppliers

- NON-JCP CERTIFIED SUPPLIERS SEEKING EXPORT CONTROLLED TECHNICAL DATA ARE REQUIRED TO PROVIDE THE CONTRACTING OFFICER WITH AN APPLICABLE AGREEMENT OR IDENTIFY WHICH ITAR/EAR EXEMPTION APPLIES TO RECEIVE ACOPY OF THE EXPORT CONTROLLED TECHNICAL DATA.

Controlled Technical Information

- Technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.
- - is to be marked with one of the distribution statements B-through-F, in accordance with DoD Instruction 5230.24, Distribution Statements on Technical documents.
- The term does not include information that is lawfully publicly available without restrictions.

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

Distribution Statements

A. Approved for public release.

B. U.S. Government agencies only

C. U.S. Government agencies and their contractors

D. Department of Defense and U.S. DoD contractors only

E. DoD Components only

F. Further dissemination only as directed by

DoD Instruction 5230.24 August 23, 2012

Requirements for multiple individuals

- If multiple individuals in your company need access to the Technical Data Package (TDP) for a solicitation and an explicit
- access request is required, each individual MUST submit an explicit access request to be granted approval to view the TDP. Those
- same individuals MUST be registered in Federal Business Opportunities (FBO). Any individuals no longer with the company should be deleted. Questions related to registration in FBO should be directed to <deleted>
- Vendors are responsible for placing correct information in FBO.
- It is strongly suggested that you submit the explicit access request and provide the buyer with the completed Use and Non-Disclosure Agreement at the same time if the solicitation requires both to gain access to view the TDP.

Destruction notice

- Upon completion of the purposes for which Government Technical Data has been provided, the Contractor is

➢ required to destroy all documents, including all reproductions, duplications, or copies thereof as may have been further distributed by the Contractor.

➢ Destruction of this technical data shall be accomplished by: shredding, pulping, burning, or melting any physical copies of the TDP and/or deletion or removal of downloaded TDP files from computer drives and electronic devices, and any copies of those files.

Okay – now prove it!

Disposal

- 1/125” – that’s right! That’s the recommended size that a piece of a hard drive should be after destruction.
- Shredding (CD’s & DVD’s)
- Degaussing – hard drive
- Specialized services will disintegrate, burn, melt, or pulverize your HD
- Beware – do not
  - Use a microwave
  - Burn
  - Use chemicals
- Deleting
- Overwriting

U.S. DHS, US-CERT, Disposing of Devices Safely, 2012 Carnegie Mellon University. Produce for US-CERT

DFARS incorporated into contract

- THE FOLLOWING CLAUSES ARE HEREBY INCORPORATED INTO THE SOLICITATION:
- DFARS 252.204-7008-Compliance with Safeguarding Covered Defense Information Controls (DEVIATION 2016-O0001) (OCT 2015) and
- DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting (DEVIATION 2016- O0001) (OCT 2015) are incorporated by reference via the DPAP class deviation website (http://www.acq.osd.mil/dpap/dars/class_deviations.html).
  - Example only showing the incorporating language

Covered contractor information system

- Means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.
- Derived requirement – covered defense information must be handled with “adequate security” at all times.
- DOD’s IASE Certificate provides for
  - Digitally signing of documents
  - Encrypting documents
  - See: https://iase.disa.mil/Pages/index.aspx Information Assurance Support Environment

DFARS 252.204-7012 Definitions

Subcontracts – the contractor shall

- Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial items, without alteration, except to identify the parties.
- The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and
- Require subcontractors to—
  - Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and
  - Provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.

DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, (m)

Information Security – formal definition

"The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability" [44USC].

NIST Publication **NISTIR 7621 Revision 1, Small Business Information Security:** *The Fundamentals* Celia Paulsen Patricia Toth, 2

Information Security – key elements

- **Confidentiality** - protecting information from unauthorized access and disclosure.

  For example, what would happen to your company if customer information such as usernames, passwords, or credit card information was stolen?

- **Integrity** - protecting information from unauthorized modification.

  For example, what if your payroll information or a proposed product design was changed?

- **Availability** - preventing disruption in how you access information.

  For example, what if you couldn't log in to your bank account or access your customer's information, or your customers couldn't access you?

NIST Publication **NISTIR 7621 Revision 1, Small Business Information Security:** *The Fundamentals* Celia Paulsen Patricia Toth, 2

Cyber Security

- “Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation” [CNSSI4009][HSPD23].

NIST Publication **NISTIR 7621 Revision 1, Small Business Information Security:** *The Fundamentals* Celia Paulsen Patricia Toth, 2

What is a cyber incident?

- A cyber incident is defined as actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

https://dibnet.dod.mil/portal/intranet/Splashpage/ReportCyberIncident

Indications of a Cyber Incident

- Unusual/unaccounted for outbound traffic and between client networks.
- Privileged Account Anomalous usage
- User Account Activity from anomalous Ips
- Excessive failed logins
- Changes/large queries against web server pages
- Well known port vs. application usage
- Files – storage/transmission
- Other Web Browsing “spikes”

Don Murdoch, blue Team Handbook: Incident Response Edition, 2016, 60-65

Cyber Incident Record Retention/Availability

- Media preservation and protection. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.
- Access to additional information or equipment necessary for forensic analysis. Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, (e) & (f)

U.S. Steel is now claiming research on creating the next generation of high-strength steel was taken and reproduced in China. “

They couldn’t figure out how to move to the next level,” said Debbie Shon, an attorney representing U.S. Steel in the petition. “After the hack they were able to.”

http://www.engineering.com/AdvancedManufacturing/ArticleID/12050/Manufacturing-Sector-Identified-as-Leading-Target-of-Infrastructure-Cyber-Attacks.aspx

Manufacturing Sector Identified as Leading Target of Infrastructure Cyber-Attacks; visited May 9, 2016

Small Business risk – “it won’t happen to us”

- It’s not just Fortune 500 companies and nation states at risk of having IP stolen–even the local laundry service is a target.
- In one example, an organization of 35 employees was the victim of a cyber attack by a competitor.
- The competitor hid in their network for two years stealing customer and pricing information, giving them a significant advantage.

Hid for two years!

Internet Security Threat Report, Volume 21, April 2016, Symantec

The issue

Cybercrime cost businesses around $500 billion in 2015, and a new report from Juniper Research says it will quadruple to $2 trillion by 2019. There are 1 million cybersecurity jobs open in 2016... nearly 300,000 of them in the U.S., and the labor shortage is getting worse, not better. There will be $100 billion in spending on cybersecurity over the next four to five years, cybercrime is on the rise, and cybersecurity talent is hard to come by.

http://www.csoonline.com/article/3027383/security/top-five-u-s-defense-contractors-bungle-commercial-cybersecurity-market-opportunity.html

Threat Landscape

- Detection
- Cyber Issues
- Ransomware
- Spear fishing
- Insider Threats
- Social Engineering
- Spoofing
- Impersonation

"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."

Image copied from: fbi.gov

Prologue: @War the Rise of the Military Internet Complex

Id'ing the digital spy

"When businesses do eventually notice that they have a digital spy in their midst and that their vital information systems have been compromised, an appalling 92 percent of the time it is not the company's chief information officer, security team, or system administrator who discovers the breach."

- How do companies find out that they have been breached?
  - Law enforcement
  - Angry customer
  - Contractor

Marc Goodman, Future Crimes: everything is connected, everyone is vulnerable and what we can do about it, (New York: DOUBLEDAY, 2015), 16-17
Verizon's 2013 Data Breach Investigations Report is cited as the source

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

Ransomware

- Individuals
- Police Department
- Hollywood Hospital
- Bitcoin
  - Several days to install
  - Must have access to a machine – may need to be dedicated
- Evolving threats – sophistication
  - Network backup
  - Mirrored systems

Ransomware

May 5, Softpedia – (International) **Ransomware infections grew 14 percent in early 2016, April the worst month.** Kaspersky, Enigma Software Group, and the FBI issued a warning to companies about the increase in ransomware infections following reports of at least 2,900 new ransomware variants, representing a 14 percent increase in Quarter 1 of 2016. Researchers also found a significant increase in the number of attacks during April.

Source: http://news.softpedia.com/news/ransomware-infections-grew-14-percent-in-early-2016-april-the-worst-month-503743.shtml
May 9th; DHS Daily Open Source

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

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

Spyware

Class of malware that collect information from a computing system without the owner's consent – keystrokes, screenshots, credentials, personal email addresses, web form filed data, Internet usage habits and other

- Who would want to spy on me?
  - Marketers
  - Advertisers
  - Bad actors – data thieves
  - Employers
  - Trusted Insider
    - Employee – spyware to collect corporate information to sell
    - Spouse/family member/close relation
    - Cleaning crew/Contractor

U.S. DHS, US-CERT, Spyware, Aaron Hackworth, CERT Coordination Center, Copyright 2005 Carnegie Mello University

Phishing – Tackle Box

- Bots/Botnets
- Phishing Kits
- Technical Deceit
- Session Hijacking
- Abuse of Domain Name Service (DNS)
- Specialized Malware

Technical Trends in Phishing Attacks, Jason Milletary, US Cert

Situational Awareness – users - Phishing

- > eight million results of sanctioned phishing tests in 2015; multiple security awareness vendors
- 30% of phishing messages were opened by the target across all campaigns.
- About 12% went on to click the malicious attachment or link and thus enabled the attack to succeed. The median time for the first user of a phishing campaign to open the malicious email is 1 minute, 40 seconds.
- The median time to the first click on the attachment was 3 minutes, 45 seconds

2016 Verizon, Data Breach Investigation Report, 18

Insider threat

"Insiders who disclose sensitive US Government information without authorization will remain a significant threat in 2016. The sophistication and availability of information technology that can be used for nefarious purposes exacerbate this threat both in terms of speed and scope of impact."

STATEMENT FOR THE RECORD WORLDWIDE THREAT ASSESSMENT of the US INTELLIGENCE COMMUNITY February 9, 2016 – page 10

May 5, KUSA 9 Denver – (Colorado) **CDOT employee stole contractors' personal information.** A Colorado Department of Transportation (CDOT) spokesperson announced May 5 that the personal information of hundreds of CDOT contractors may have been compromised after a data breach involving a CDOT employee who had access to a database for Emerging Small Business (ESB) and Disadvantaged Business Enterprise (DBE) which contained confidential information. Authorities stated that the businesses potentially impacted by the breach submitted information to CDOT in order to qualify for ESB and DBE programs.

Source: http://www.9news.com/news/cdot-employee-stole-contractors-personal-information/175000302
May 9th DHS Daily Open Source

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. “
- “Energy companies do not think of themselves as big users of social media,” said Westby, “but their employees are, and they tend to have employees in some very sensitive areas of the world.”

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

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

CEO impersonation

"Glen, I have assigned you to manage file T521," the phony message to the accounting director **Glen Wurm** allegedly read. "This is a strictly confidential financial operation, to which takes priority over other tasks. Have you already been contacted by Steven Shapiro (attorney from KPMG)? This is very sensitive, so please only communicate with me through this email, in order for us not to infringe SEC regulations. Please do no speak with anyone by email or phone regarding this. Regards, Gean Stalcup."

Roughly 30 minutes later, Mr. Wurm said he was contacted via phone and email by Mr. Shapiro stating that due diligence fees associated with the China acquisition in the amount of $480,000 were needed. AFGlobal claims a Mr. Shapiro followed up via email with wiring instructions.

http://krebsonsecurity.com/tag/ceo-fraud/

General principles

- Enable auto-software updates
- Install, use, & keep updated antivirus software**
- Avoid unsafe behavior – websites, opening links/attachments
- Follow the principle of least privilege
  - Create secondary, non-admin/root account
  - Admin accountshave universal privileges – malicious software needs this access

**Beware of free AV Software

Routers (partial list)

- Turn ping feature off – harder to locate
- Turn off the Auto ID feature
- Turn the device off when not needed/ limit footprint
- Change default login username and password
- Change the default SSID (Service set identifier)
- Password protect – min 8 characters
- Configure WPA2-AES for data confidentiality
- Enable router firewall – most (home) include
- Monitor wireless traffic – routine log scan unauthorized users*

U.S. DHS, US-CERT, Small Office/Home Office Router Security, 2011

Free – well maybe sort of

- USB drives
  - Trade show – from who, what company
  - In the parking lot? – oh really
    - Let someone else be the good Samaritan!
- Software/Apps
  - It's free, but what access is required?
  - What do you know about the company?
  - Who have you trusted with your data/information?

U.S. DHS, US-CERT, Software License Agreements: Ignore at Your own Risk, Edward Desautels, Produced 2005 by US-CERT, Updated 2008

Questionable Host – Reputation Risk method

- Site names recently registered –
  - Time registered loosely relates to risk
- Listed in threat resources (Robtex, malwaredomain, etc)
- No reverse lookup value
- Short / low TTL (<1 day, for example)
- IP address changes frequently
- Site names – “gibberish” can’t be read

Don Murdoch, blue Team Handbook: Incident Response Edition, 2016, 113-114

Identifying a Suspicious host

- Contact the IP Address Owner
- Send Network Traffic to the IP Address
- Seek ISP Assistance
- Research the History of the IP Address
- Look for Clues in Application Content

NIST SP 800-86 **Guide to Integrating Forensic Techniques into Incident Response**, 6.4.4 Attacker Identification page 6-17-6-18

Reputation Risk – resource sites

- http://www.barracudacentral.org/lookups
- http://ipremoval.sms.Symantec.com/lookup/
- http://www.brightcloud.com/services/ip-reputation.php
- http://www.avgthreatlabs.com/website-safety-reports/
- http://www.malwaredomainlist.com/mdl.php
- Others ….

Don Murdoch, blue Team Handbook: Incident Response Edition, 2016, 114

Top 10 Ports – by Report

Port	Reports	Port	Targets	Port	Sources
22	106450	23	12254	23	39312
23	73916	1433	3822	22	4283
53	28051	22	3803	445	4105
80	27462	445	2765	5358	3738
1433	15769	3389	2244	2323	2834
445	12187	2323	1949	1433	2580
3884	6336	8080	1926	53	939
2323	4760	5358	1832	2222	679
5358	4475	80	1516	80	652
8080	3894	7547	1287	51413	639

www.dshield.org/top10.html; visited August 15, 2017

Top 10 Source IP Addresses; associated with attacks

IP Address	Reports	Target IPs	First Seen	Last Seen
047.044.013.106 ()	2,498	2,498	2017-08-14	2017-08-14
190.082.065.155 ()	1,266	1,266	2017-08-15	2017-08-15
095.037.160.073 ()	781	313	2017-08-14	2017-08-14
045.021.028.162 ()	460	269	2017-08-15	2017-08-15
073.205.092.142 ()	387	264	2017-08-15	2017-08-15
207.255.216.192 ()	405	260	2017-08-15	2017-08-15
051.015.042.034 ()	259	259	2017-08-14	2017-08-14
119.001.109.096 ()	258	258	2017-08-14	2017-08-14
072.019.038.249 ()	423	257	2017-08-15	2017-08-15
125.077.017.172 ()	513	257	2017-08-14	2017-08-14

Option: Apply the Top 10 blocklist automatically to your firewall via ThreatSTOP. Also can apply these IP's to a router.

www.dshield.org/top10.html; visited August 15, 2017

Threat Feeds

BOTS	OTHERS	PORT SCANNERS	RESEARCH
bebloh C&C server	CI Army List	Port 110 Scanner	Blindferret
Cryptowall C&C server	Emergingthreats	Port 143 Scanner	Erratasec Masscan
Dyreza Servers	Forum Spammers	Port 21 Scanner	Rapid7Sonar
Hesperbot C&C server	Malc0de Blacklist	Port 22 Scanner	Shadowserver
matsnu C&C server	TLD Name Servers	Port 25 Scanner	ShodanHQ
Palevo C&C IP	Tor Exit Node ✓	Port 443 Scanner	UMichigan scans.io
qakbot C&C server		Port 80 Scanner	
ramnit C&C server		Port 993 Scanner	
Ransomips		Apache Web Server Scanner	
Spyeye C&C server		Asterisk VoIP Scanner	
Symmi C&C server		Suspect Bots/Infected	
TinyBanker C&C server		Bruteforce	
Upatr Servers		courier imap attacker	
WebIron Bots		courier pop3 attacker	
Zeus C&C server		OpenBL FTP Scanners	
		OpenBL HTTP Scanners	
		OpenBL MAIL Scanners	
		OpenBL SMTP Scanners	
		OpenBL SSH Scanners	

www.dshield.org/top10.html; visited August 15, 2017

Forensics – planning considerations

- Applicable laws
  - Wiretap Act (18 U.S.C. 2510-22)
  - Pen Registers and Trap and Trace Devices Statute (18 U.S.C. 3121-27)
  - Stored Wired and Electronic Communication Act (18 U.S.C. 2701-120)
  - The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data. DFARS 252.204-7012
- May need to consult with an Attorney
- Plan
- Document
- Capture – save
- Reproducible

Computer Security Logs

- Generated by many sources; provide documentation of activity
  - including security software,
    - antivirus software
    - Firewalls
    - Networking equipment
      - Servers
      - Routers
      - Switches
    - Intrusion detection prevention systems
    - Operating systems
    - Workstations

Log management

- Log identification
- Log generation
- Log transmission
- Log analysis
  - Staff
  - Collection
  - Tools - software
  - Periodicity
- Log storage and disposal procedures/protocol

Log analysis

What to Look For in Logs

An administrator should look for all of the following things in log files:

- Probes to ports that have no application services running
- Unsuccessful logins to the firewall
- Suspicious outbound connections
- Source-routed packets
- Host operating system log messages
- Changes to network interfaces
- Changes to firewall policy
- Additions, deletions, and changes of administrative accounts
- Dropped and rejected connections
- Time, protocol, IP addresses, and usernames for allowed connections

Penetration Testing Security Analysis, EC-Council, Page 7-2

Log Protection

- logs contain records of system and network security
- they need to be protected from breaches of their confidentiality and integrity
- Improperly securing - intentional and unintentional alteration and destruction
  - May allow malicious activity to go on unnoticed
  - For example, many rootkits are specifically designed to alter logs
- Protect availability of logs – maximum size / overwriting

NIST SP 800-92 Computer Security and Log Management, 2.3.9 page 2-9

Maximizing Log value

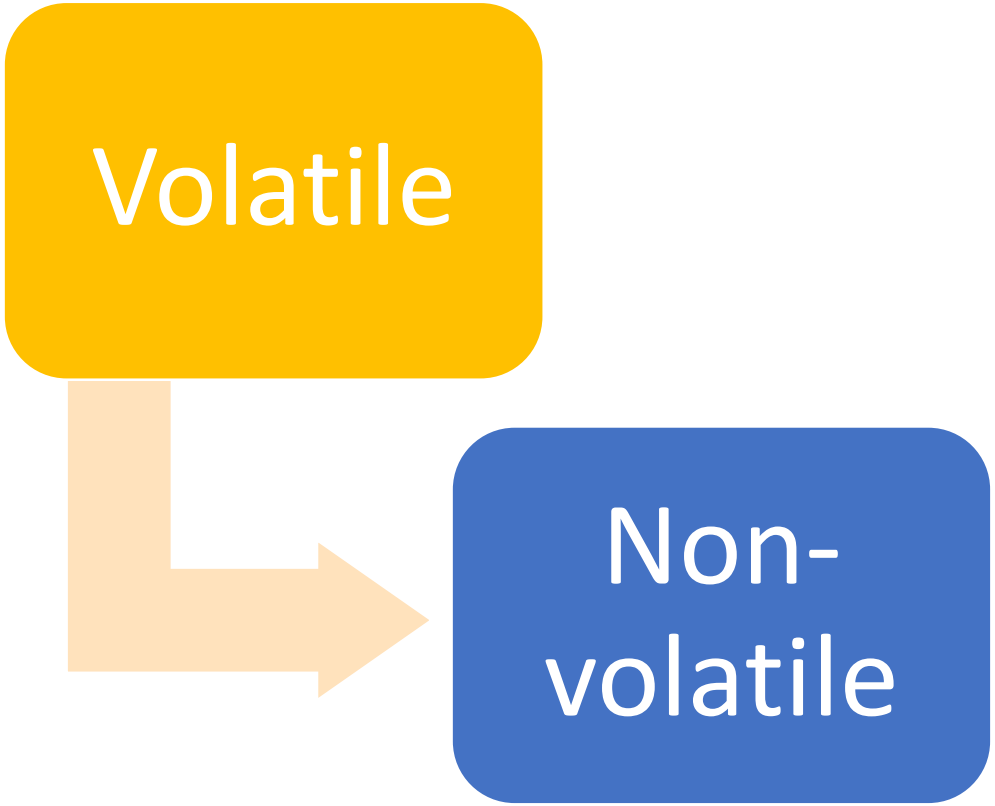
- Identify as high priority
  - Combat the notion of boring and of low benefit
- Provide sufficient tools
  - Assists with automation
  - Helps to identify patterns that a human will not see
- Provide training for efficient performance
- Reactive tool
  - After an event

NIST SP 800-92 Computer Security and Log Management, 2.3.3 page 2-10

Collecting & Prioritizing Data Collection

Volatile Data - prioritized

1. Network connections
2. Login sessions
3. Contents of memory
4. Running processes
5. Open files
6. Network configuration
7. Operating system time



NIST SP 800-86 **Guide to Integrating Forensic Techniques into Incident Response**, 5.2.1.3 page 5-8

Volatile Data collection – trusted tools

Netstat.exe –an	-	Lists active connects/open ports
Netstat.ext –m	-	Lists the local routine table
Pslist.exe	-	List running processes and associated data
Openports.ext	-	Lists active connects and open ports
Psloggedon.exe	-	Lists users logged on locally and via network share
Psfile.ext	-	Lists files opened remotely
Ipconfig.exe/all	-	Lists network adapter information
Now.exe	-	Displays system date and time – (Time/Date – DOS)

Examining and Analyzing Network Traffic

- Identification of an event of interest
  - Assess
  - Extract
  - Analyze
- Goal –
  - What happened
  - Affect to/on the systems and network
- Simple – reviewing few logs
- Complex – review and analyze multiple sources

NIST SP 800-86 **Guide to Integrating Forensic Techniques into Incident Response**, 6.4 page 6-11

Examining and Analyzing Network Traffic

- Identify an Event of Interest
  - Someone, received indication – alert, complaint, operational issue – crash
  - Information results from security log review
- Examine Data Sources
- Examination and Analysis Tools
- Draw Conclusions

Network Security - approaches

- CM – Continuous Monitoring (DHS & NIST approach)
  - Vulnerability centric
  - Focuses on configuration and software weaknesses
- NSM – Network Security Monitoring
  - Threat-centric
  - Adversaries are the focus
  - Visibility vice control
- Others – eg. Firewall, antivirus, whitelisting
  - Each of these
    - Blocking, filtering, denying mechanism
    - Recognize malicious activity and stop it

Richard Bejtlich, The Practice of network Security Monitoring (No Starch Press, Inc, San Francisco, CA 2013), 9

Threats

- Can be internal
  - Staff
  - Purchased equipment
- External
  - Hacker
- Blend
  - External threat
  - Internal, accidental initiation

Passive Information Gathering

- Key employees
- Dumpster diving
- Analyzing Web Page Code
- Exploiting Website Authentication Methods
- Mining Job Ads and Financial Data
- Using Google to Mine Sensitive Information
- Exploring Domain ownership
  - Whois | Domain Name System | Identifying web server Software & Location

Michael Gregg, The Network Security Test Lab; A step-by-Step Guide, (John Wiley & Sons, Inc, Indianapolis, IN 2015), XII

Security Software

- Antimalware Software
- Intrusion Detection and Intrusion Prevention Systems
- Remote Access Software
- Web Proxies
- Vulnerability Management Software
- Authentication Servers
- Routers
- Firewalls
- Network Quarantine Servers

NIST SP 800-92 Computer Security and Log Management, 2.1.1 page 2-2

Looking forward

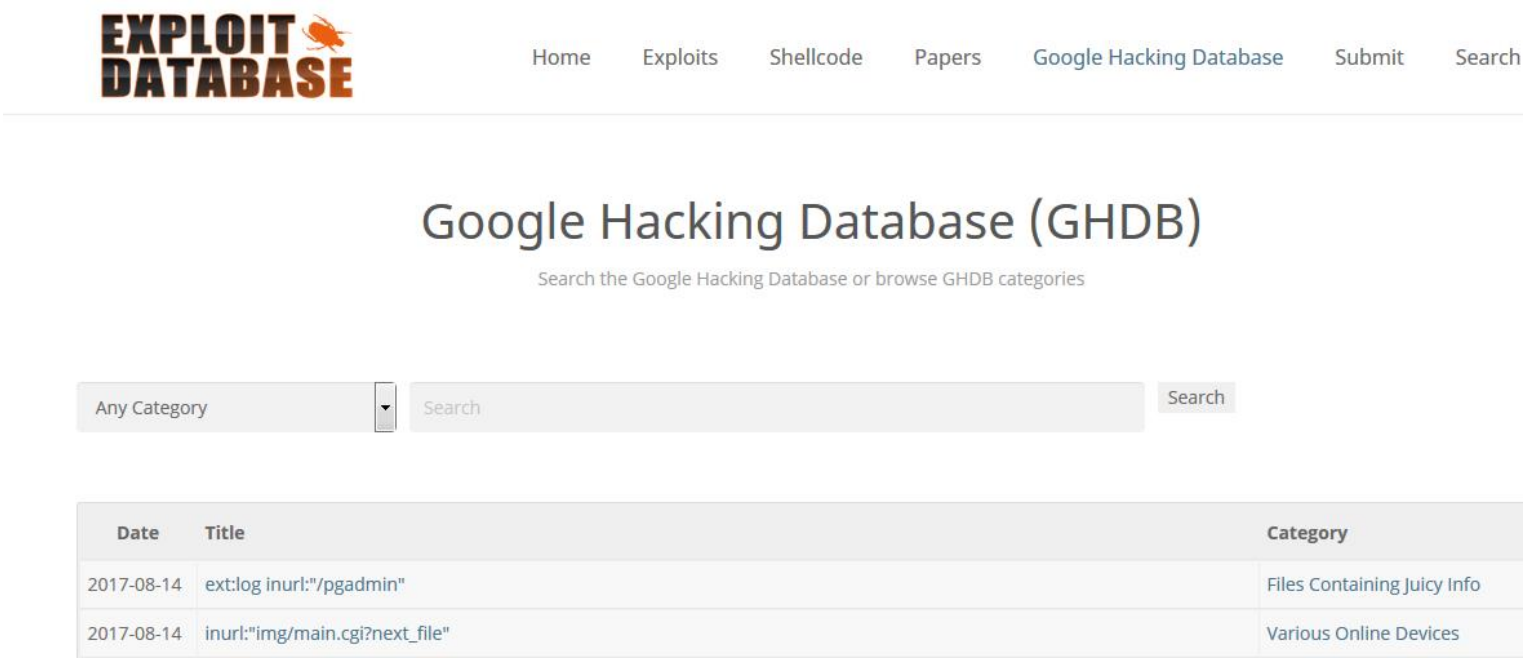
Scenario Questions

- 1. What are the potential sources of data?
- 2. Of the potential sources of data, which are the most likely to contain helpful information and why?
- 3. Which data source would be checked first and why?
- 4. Which forensic tools and techniques would most likely be used? Which other tools and techniques might also be used?
- 5. Which groups and individuals within the organization would probably be involved in the forensic activities?
- 6. What communications with external parties might occur, if any?
- 7. From a forensic standpoint, what would be done differently if the scenario had occurred on a different day or at a different time (regular hours versus off-hours)?
- 8. From a forensic standpoint, what would be done differently if the scenario had occurred at a different physical location (onsite versus offsite)?

NIST SP 800-86 **Guide to Integrating Forensic Techniques into Incident Response**, Appendix B - Scenariors page: Appendix B-1

What a difference a URL can make!

- www.exploit-db.com/google-dorks



Ports – loose analogy

- Discrete communication endpoint
  - Physical – socket, plug-in
  - Logical – application or process
  - Numbered - hundreds
- Ports in a business setting
  - Doors
  - Reception area
  - Telephones
  - Loading dock

Sleuthing with netstat -aon

```
TCP    192.168.5.216:49417    162.125.34.6:443       CLOSE_WAIT     4760
TCP    192.168.5.216:49421    52.201.32.182:443      CLOSE_WAIT     4760
TCP    192.168.5.216:49423    172.217.1.35:443       ESTABLISHED    6124
TCP    192.168.5.216:49424    216.58.216.206:443     ESTABLISHED    6124
TCP    192.168.5.216:49425    208.80.154.224:443     ESTABLISHED    6124
TCP    192.168.5.216:49427    208.80.154.240:443     ESTABLISHED    6124
TCP    192.168.5.216:49434    172.217.6.106:443      ESTABLISHED    4148
TCP    192.168.5.216:49435    172.217.9.37:443       ESTABLISHED    4148
TCP    192.168.5.216:49437    34.209.12.3:443        TIME_WAIT      0
TCP    192.168.5.216:49438    72.21.91.29:80         ESTABLISHED    6124
TCP    192.168.5.216:49439    72.21.91.29:80         ESTABLISHED    6124
TCP    192.168.5.216:49440    72.21.91.29:80         TIME_WAIT      0
TCP    192.168.5.216:49441    54.191.246.135:443     TIME_WAIT      0
TCP    192.168.5.216:49442    52.84.64.228:443       TIME_WAIT      0
TCP    192.168.5.216:49443    52.84.64.228:443       TIME_WAIT      0
TCP    192.168.5.216:49444    52.84.64.228:443       TIME_WAIT      0
TCP    192.168.5.216:49445    52.84.64.228:443       TIME_WAIT      0
TCP    192.168.5.216:49446    172.217.8.196:443      ESTABLISHED    4148
TCP    192.168.5.216:49447    172.217.6.106:443      ESTABLISHED    4148
TCP    192.168.5.216:49448    172.217.6.106:443      ESTABLISHED    4148
TCP    [::]:135               [::]:0                 LISTENING      884
TCP    [::]:445               [::]:0                 LISTENING      4
TCP    [::]:554               [::]:0                 LISTENING      5588
```

Google: Whois 192.168.5.216 – slide 1

192.168.5.216

City	Rome
Country	Italy
Country Code	IT
Longitude	0
Latitude	0

?

Based on several IP databases the most probable location for IP adresse 192.168.5.216 is Rome, Italy, IT.
Latitude and longitude: 0 and 0

Whois 192.168.5.216 – slide 2

Network information

ASN	137
IP starting by	192.167.0.0
IP ending by	192.167.255.255
Ip starting with	192.168.5
ASN Name	Consortium GARR
CDIR	192.167.0.0/16
Numerical IP	3232237016
Registry	ripencc
Last update	04/07/2017

Whois 172.217.6.106

Network information

ASN	15169
IP starting by	172.217.0.0
IP ending by	172.217.255.255
Ip starting with	172.217.6
ASN Name	Google Inc.
CDIR	172.217.0.0/16
Numerical IP	2899904106
Registry	arin
Last update	10/07/2017

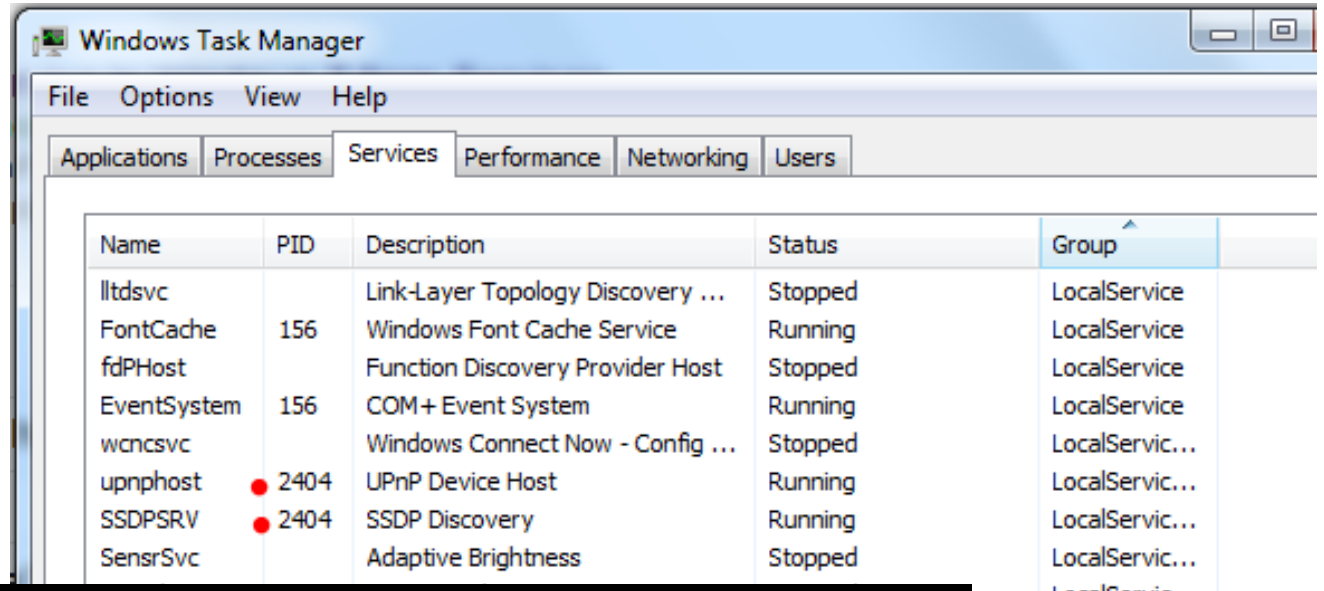
Local Address

The IP address 192.168.5.216 is provided by Consortium GARR, it's belong to the CDIR (Classless Inter-Domain Routing) 192.167.0.0/16 (range 192.167.0.0 to 192.167.255.255). The autonomous system number (ASN) is 137 and the numerical IP for 192.168.5.216 is 3232237016.

Foreign Address

The IP address 172.217.6.106 is provided by Google Inc., it's belong to the CDIR (Classless Inter-Domain Routing) 172.217.0.0/16 (range 172.217.0.0 to 172.217.255.255). The autonomous system number (ASN) is 15169 and the numerical IP for 172.217.6.106 is 2899904106.

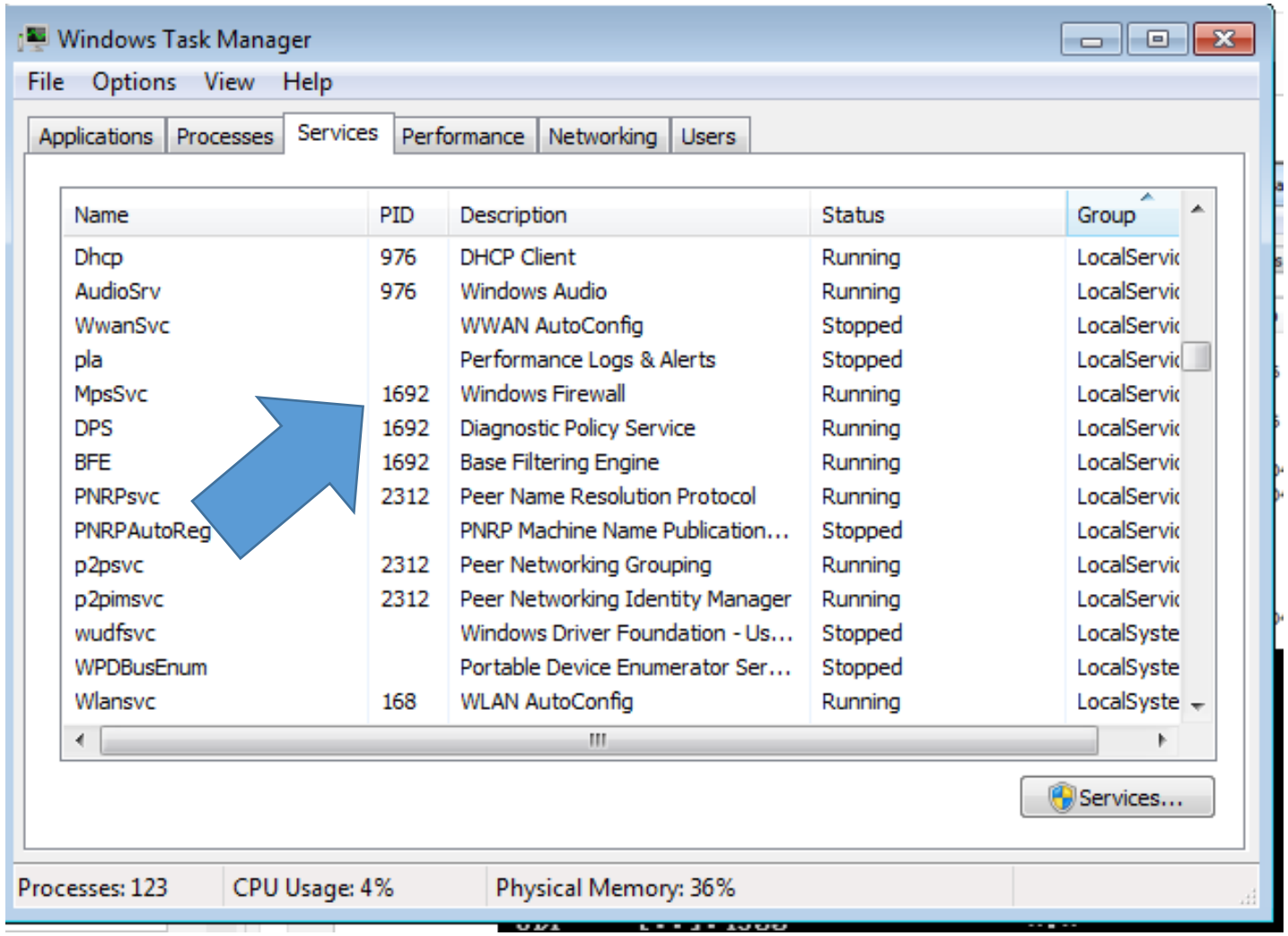
Information related to PID 2404




```
UDP    0.0.0.0:63566          *:*                                    1684
UDP    127.0.0.1:1900         *:*                                    2404
UDP    127.0.0.1:56842        *:*                                    2404
UDP    192.168.5.216:137      *:*                                    4
UDP    192.168.5.216:138      *:*                                    4
UDP    192.168.5.216:1900     *:*                                    2404
UDP    192.168.5.216:56841    *:*                                    2404
UDP    [::]:500               *:*                                    376
UDP    [::]:3702              *:*                                    2404
UDP    [::]:3702              *:*                                    2404
UDP    [::]:4500              *:*                                    376
```

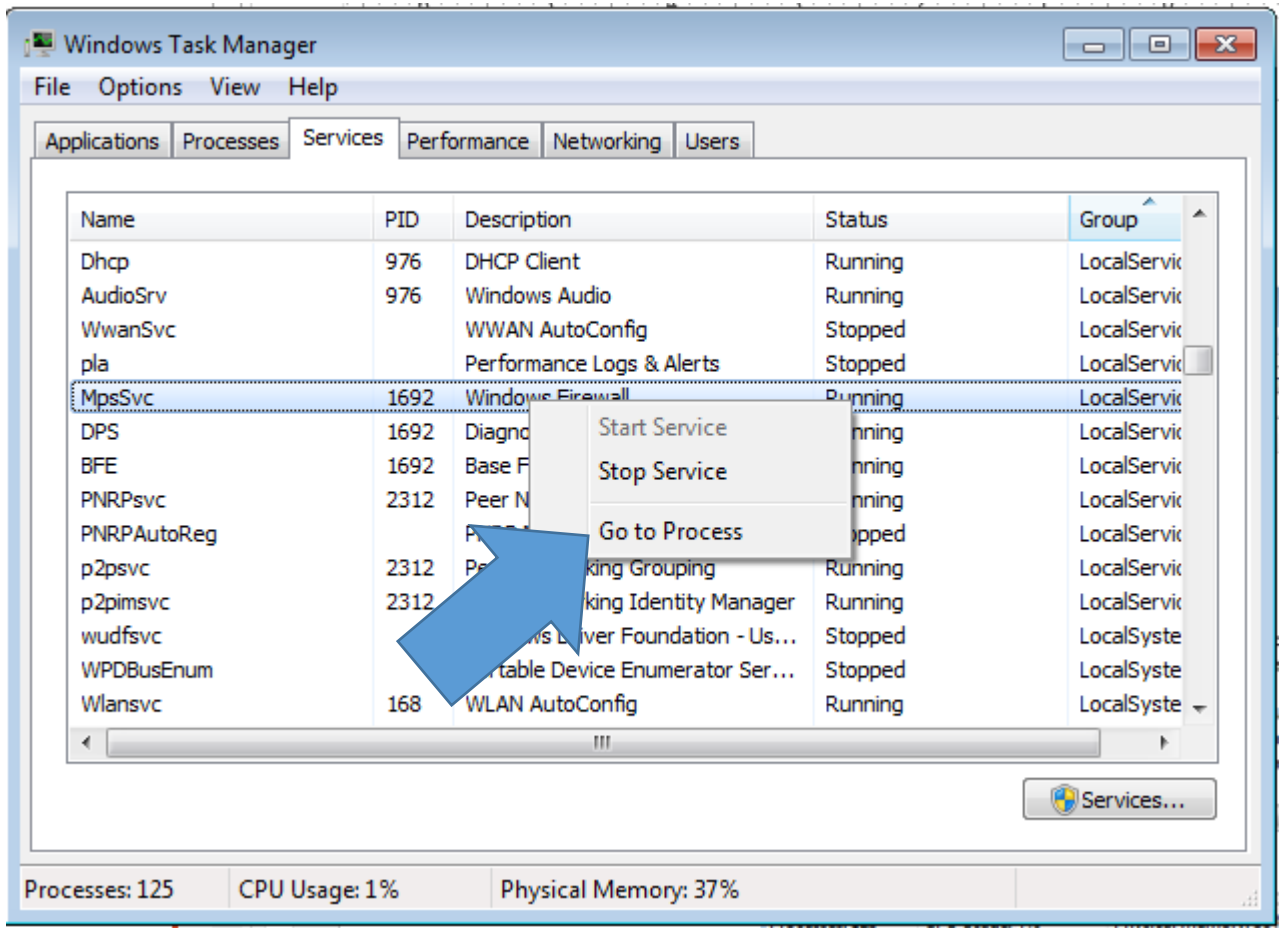
Grouping by PID

Hover over; right click

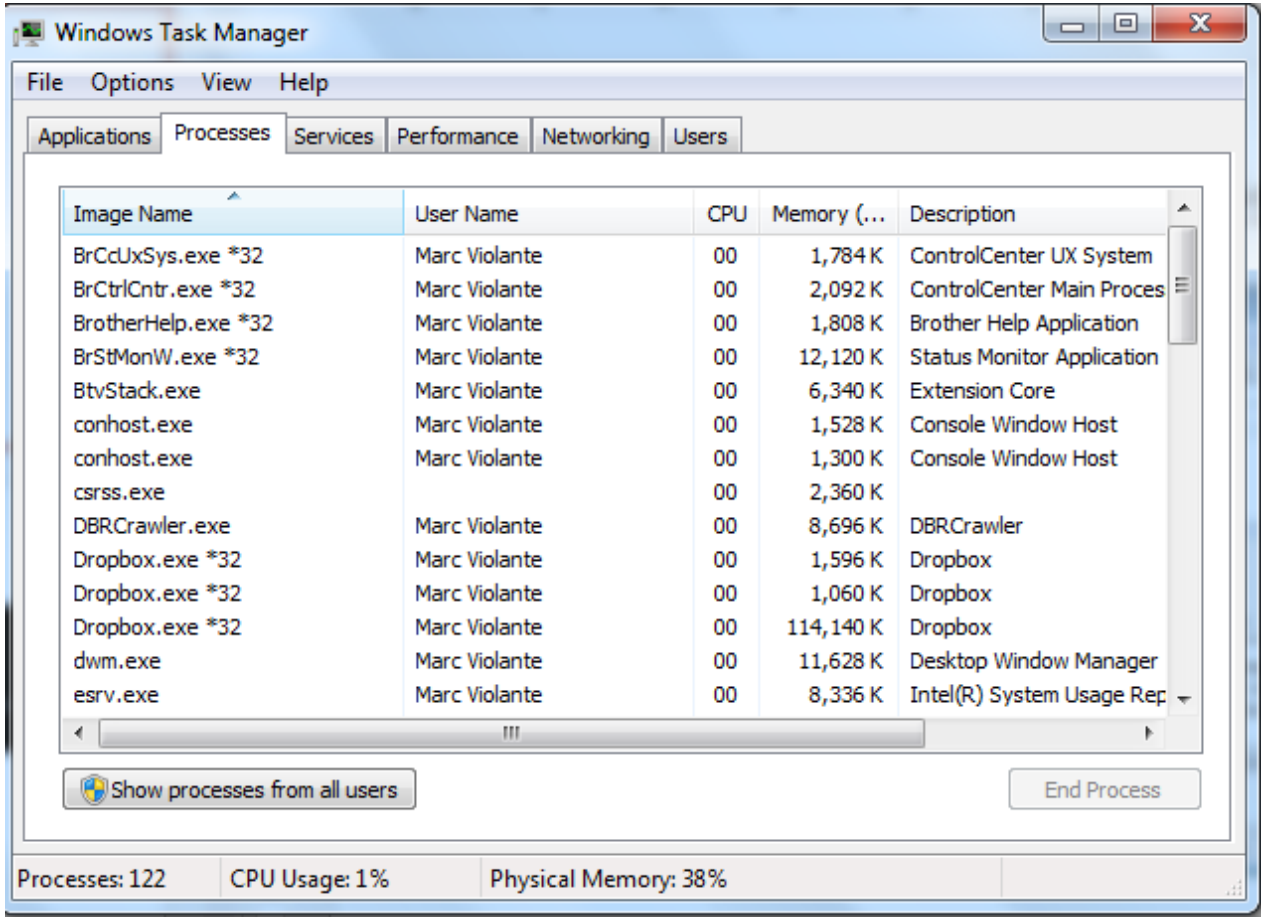


Show all PID related processes

Select Go to Process



Processes related to PID 1692



Cyber Incident – Reporting Requirements

- Actions required when
  - Cyber incident discovered
  - Cyber incident affects ability to perform
- Actions
  - Conduct a review for evidence to include
  - Rapidly report (within 72 hours) to https://dibnet.dod.mil
- Reporting required
  - Dibnet account
  - DoD Medium Assurance Certificate

DFARS 252.204-7012, SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (OCT 2016), (C)

Cyber incident report

- The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at http://dibnet.dod.mil.

DFARS 252.204-7012, SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (OCT 2016), (C) (2)

Cyber Incident Reporting -

DoD contractors shall report as much of the following information as can be obtained to DoD within 72 hours of discovery of any cyber incident

- Company name
- Company point of contact information (address, position, telephone, email)
- Data Universal Numbering System (DUNS) Number
- Contract number(s) or other type of agreement affected or potentially affected
- Contracting Officer or other type of agreement point of contact (address, position, telephone, email)
- USG Program Manager point of contact (address, position, telephone, email)
- Contract or other type of agreement clearance level (Unclassified, Confidential, Secret, Top Secret, Not applicable)
- Facility CAGE code
- Facility Clearance Level (Unclassified, Confidential, Secret, Top Secret, Not applicable)

https://dibnet.dod.mil/portal/intranet/Splashpage/ReportCyberIncident

- Impact to Covered Defense Information
- Ability to provide operationally critical support
- Date incident discovered
- Location(s) of compromise
- Incident location CAGE code
- DoD programs, platforms or systems involved
- Type of compromise (unauthorized access, unauthorized release (includes inadvertent release), unknown, not applicable)
- Description of technique or method used in cyber incident
- Incident outcome (successful compromise, failed attempt, unknown)
- Incident/Compromise narrative
- Any additional information

Other requirements

- *Other safeguarding or reporting requirements*. The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

252.204-7012 Safeguarding of Unclassified Controlled Technical Information. (l)

IP 192.168.0.8 – Identified using tracert

```
C:\>
C:\>tracert 192.168.0.8

Tracing route to MarcViolante-PC [192.168.0.8]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  MarcViolante-PC [192.168.0.8]

Trace complete.
```

- All good
- No system breach
- No report required

Resources

Image copied from: innovation.ed.gov

Frameworks

- SP 800-53
- SP 800-171
- NIST 32 – Establishing or Improving a Cyber Security Program
- NIST SP 800-86 Integrating Forensic techniques into Incident Response
- NIST SP 800-92 Computer Security and Logs
- NIST IR 7621 r1 Small Business Information Security Fundamentals
- Framework for Improving Critical Infrastructure Cybersecurity, NIST, February 12, 2014

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.

National Initiative for Cybersecurity Careers and Studies

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

HOME | ABOUT US | CAREERS | PUBLICATIONS | ALERTS AND TIPS | RELATED RESOURCES | C³ VP

Bulletin (SB16-095)

Vulnerability Summary for the Week of March 28, 2016

High Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
autodesk -- autodesk_backburner	Stack-based buffer overflow in manager.exe in Backburner Manager in Autodesk Backburner 2016 2016.0.0.2150 and earlier allows remote attackers to execute arbitrary code or cause a denial of service (daemon crash) via a crafted command. NOTE: this is only a vulnerability in environments in which the administrator has not followed documentation that outlines the security risks of operating Backburner on untrusted networks.	2016-03-28	7.8	CVE-2016-2344 CERT-VN
cisco -- ios	The IKEv2 implementation in Cisco IOS 15.0 through 15.6 and IOS XE 3.3 through 3.17 allows remote attackers to cause a denial of service (device reload) via fragmented packets, aka Bug ID CSCux38417.	2016-03-25	7.1	CVE-2016-1344 CISCO
cisco -- ios	Cisco IOS 15.0 through 15.5 and IOS XE 3.3 through 3.16 allow remote attackers to cause a denial of service (device reload) via a crafted DHCPv6 Relay message, aka Bug ID CSCus55821.	2016-03-25	7.8	CVE-2016-1348 CISCO

SANS

Login

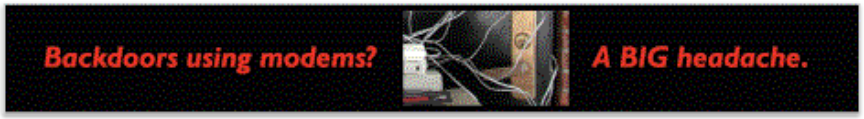
Find Training | Live Training | Online Training | Programs | Resources | Vendor | About

Reading Room

Take Cyber Insurance Survey for Chance to Win a $400 Amazon Gift Card!

SURVEY: Tell us how the healthcare industry is - OR should be - addressing infosec

More than **75,000 unique visitors** read papers in the Reading Room every month and it has become the starting point for exploration of topics ranging from SCADA to wireless security, from firewalls to intrusion detection. The SANS Reading Room features over 2,490 original computer security white papers in 96 different categories.



Latest 25 Papers Added to the Reading Room

SANS eNewsletters

Receive the latest security threats, vulnerabilities, and news with expert commentary

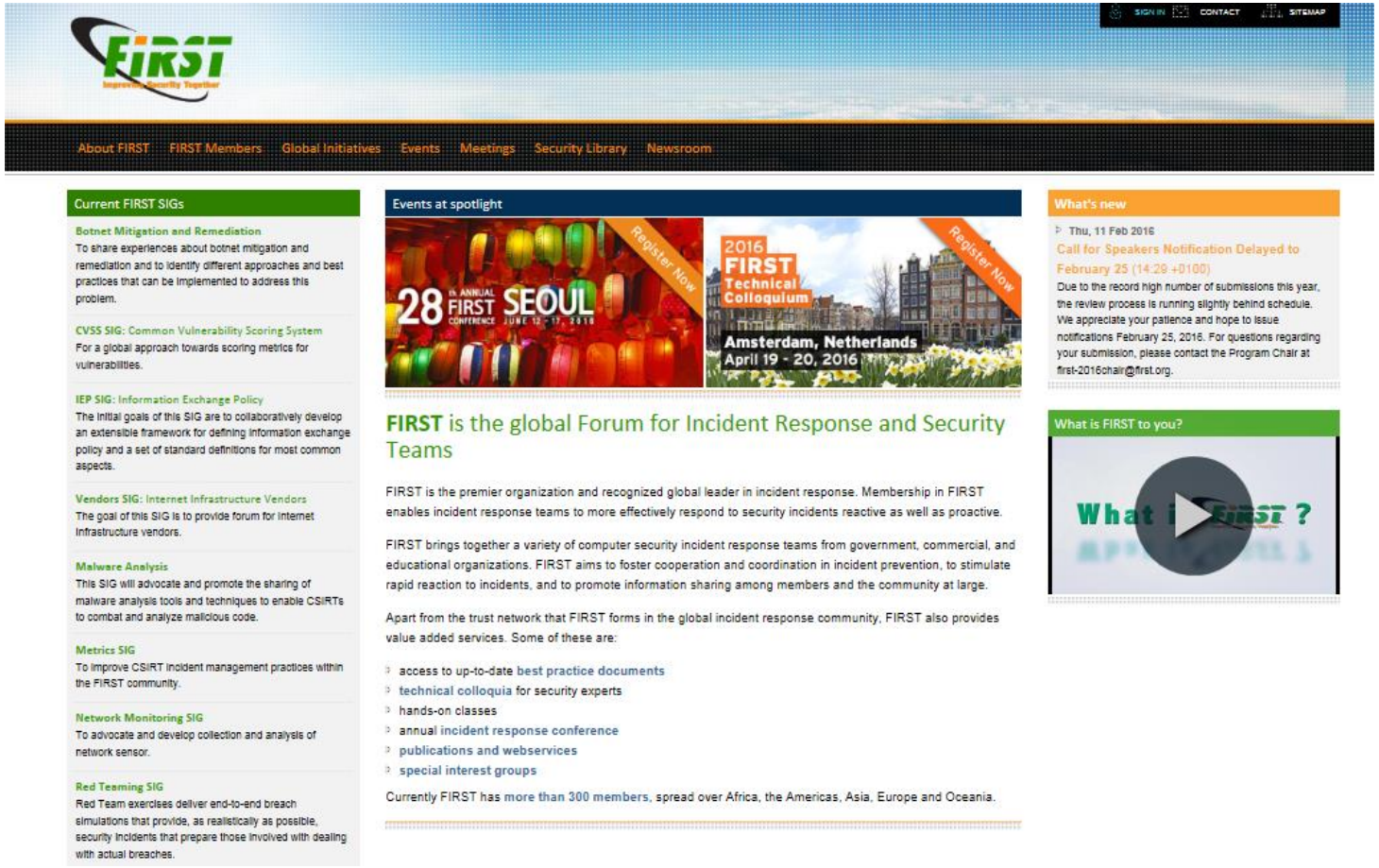
Get Newsletters

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



DIB ISAC

Take advantage of resources and tools

Resources

- NISTIR 7621 Revision 1 Small Business Information Security:
  - *The Fundamentals*
- 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 www.sans.org

Veterans have access to free training

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

A better pipeline for cyber talent

- Vets get free SANS training and certifications in cybersecurity
- Employers get highly qualified talent for critical jobs in cybersecurity

Introducing the SANS VetSuccess Immersion Academy, an intensive, accelerated program that provides the real-world training and certifications needed to fill critical jobs in cybersecurity.

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

Create a 30 day action plan

- Review DFAR 252.204-7012
- Review NIST SP 800-171
  - Group requirements by difficulty/technical requirement
    - Administrative – easy
    - Technical – will need outside assistance
- Inventory resources
- Inventory information – stored and other (commercial & DoD)
- Prioritize plans required and development schedule

Information handling requirements

- At what level – internally
- To what degree?
- Process for keeping current?
- How is information identified?
- How is it stored?
- Is there one level – two – more?
- How is information shared?
- Are the processes tested? – how often? – by whom? – results?

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 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

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. 3*

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*

It’s easy to sleep when your information is secure