PILIERO MAZZA PLLC
ATTORNEYS AT LAW

e-end
Secure Data Destruction & Electronics Recycling
www.eendusa.com

CYBERSECURITY RESOLUTIONS FOR THE NEW YEAR

A Joint Webinar | PilieroMazza and e-End
January 14, 2015

PRESENTED BY

Jon Williams, Partner
PilieroMazza PLLC
Government Contracts Group
jwilliams@pilieromazza.com
(202) 857-1000

Steve Chafitz, President
e-End USA
steve@eendusa.com
(240) 529-1010

OVERVIEW

- Why cybersecurity matters
- Recently-implemented cybersecurity rules and laws
- Rapid reporting of cyber incidents and additional cybersecurity measures coming soon
- Handling end of life equipment and data taken out of service
- New Year's resolutions for your cybersecurity practices
- Q&A

WHY CYBERSECURITY MATTERS

- Most small business owners are not focusing on cybersecurity, and do not believe they are vulnerable
- But we are small, we are not a target like Sony Pictures . . .
  - Think again! Small businesses are subject to nearly half of all cyber attacks
- And it is not just rogue nations and organized Russian crime – disgruntled employees and former employees can do significant damage
- Easier for cyber criminals and government agencies to go after small businesses as the "weak link" in our information systems

WHY CYBERSECURITY MATTERS (CONT'D)

- Inadequate cybersecurity or a "cyber incident" can have many adverse consequences, including:
  - Loss of data
  - Harm to reputation/loss of business opportunities
  - Termination of or exclusion from government contracts
  - Negative past performance rating or responsibility determination
  - False Claims Act liability and suspension/debarment
  - Fines and other civil liability
    - *Emily Byrne v. Avery Center for Obstetrics and Gynecology*
- Not to mention the time and money to fix the problem

SAFEGUARDING UNCLASSIFIED CONTROLLED TECHNICAL INFORMATION (UCTI)

- DFARS 252.204-7012
  - Effective November 13, 2013
  - Required for all new DoD contracts and subcontracts
    - Could be added to existing contracts via modification
    - No exception for small businesses or commercial items
    - Must be flowed down to subcontractors
  - Primary requirements:
    - Provide adequate security to safeguard UCTI on your unclassified information systems
    - Report certain cyber incidents that affect UCTI within 72 hours, and preserve information to aid government investigation
  - Noncompliance could result in breach of contract, which could have several adverse consequences including default and damages

SAFEGUARDING UCTI (CONT'D)

- What is UCTI?
  - Technical data or computer software with military or space application that is subject to controls – generally relates to sensitive information subject to marking and release restrictions the government will identify
- What is adequate security?
  - Vaguely defined; you must provide protective measures commensurate with consequences and probability of loss
  - Must adhere to 51 security controls from NIST Special Publication 800-53, or explain why they are not applicable or necessary
  - No approval of your system, so use good faith effort to comply
- What is a cyber incident?
  - Not entirely clear – appears to cover intentional use of a computer network to obtain information (hacking), even if unsuccessful
  - Also appears to cover inadvertent releases of UCTI

SUPPLY CHAIN SECURITY FOR DEFENSE CONTRACTORS

- DFARS 252.239-73
  - Interim rule effective November 2013
  - Created a pilot program through September 2018 to allow DoD to assess impact of IT supply chain risk in certain types of procurements involving "covered systems"
    - Covered system = national security system, which are systems involved in intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapon system, or that is otherwise critical to fulfillment of military/intelligence missions
    - Not just government systems – could include a contractor's system and telecommunications providers
  - Clause must be included in all IT procurements subject to DFARS
  - Must be flowed down to subcontractors

SUPPLY CHAIN SECURITY FOR DEFENSE CONTRACTORS (CONT'D)

- DoD can exclude a contractor from a procurement if the contractor presents a supply chain risk
  - Could happen if you fail to meet certain qualification standards, or if you do not get an acceptable rating for a supply chain risk evaluation factor
  - DoD can also direct a prime contractor to exclude a subcontractor
  - Authorized official must first obtain a joint recommendation based on a risk assessment, jump through other hoops, before exclusion
  - Limited disclosure of exclusion decisions
  - Unreviewable in bid protests
- Will exclusion be publicized or reported to other agencies?
  - Could result in *defacto* debarment

RAPID REPORTING OF CYBER ATTACKS

- 2013 NDAA
  - Implementing rules first expected in early 2013, but have been delayed several times
  - Rules expected to require cleared contractors to rapidly report successful cyber attacks and assist government investigation of the attack
  - Contractors will likely be required to provide DoD information about the method of attack, a sample of malware used, and summary of compromised data
  - Many unknowns, such as:
    - How much access will government have to your system?
    - What constitutes a penetration that must be reported?
    - How long will you have to report?
    - Will this extend to unclassified networks as well?

RAPID REPORTING OF CYBER ATTACKS (CONT'D)

- 2014 Intelligence Authorization Act (passed July 2014)
  - Applies to:
    - Future contracts and contract renewals after enactment
    - Intelligence community (IC) contractors: contractors granted clearance to access, receive, and store classified information for the purpose of bidding a contract or conducting activities in support of the IC
    - "Covered networks": any network or information system of a cleared IC contractor that contains or processes information created by or for an element of the IC with respect to which such contractor is required to apply enhanced protection
  - Aimed at developing procedures for how IC contractors must report penetration of IC networks
  - Will also require network security plan for all IC contracts
  - Successful penetration not defined in the law; most of the work is yet to be done to flesh out how this will work through rulemaking

RAPID REPORTING OF CYBER ATTACKS (CONT'D)

- 2015 NDAA
  - Requires DoD to establish, within 90 days, procedures for rapid reporting of cyber incidents experienced by "operationally critical contractors"
    - Cyber incident = actions taken through the use of computer networks that result in an actual or potential adverse effect on any information system or the information residing therein
    - Operationally critical contractor = critical source of supply for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation
  - New procedures to address how DoD will identify operationally critical contractors, how DoD will notify such contractors of their designation, and provide mechanisms for DoD to assist such contractors, if requested, to detect and mitigate cyber incursions
  - Act does not define "rapid"

COMING SOON TO A FAR NEAR YOU?

- NIST Special Publication 800-171
  - Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
  - Draft released for comment in November 2014
  - Signals focus on protecting sensitive unclassified federal information residing on nonfederal information systems – i.e., contractor information systems
  - Relies on NIST 800-53 for required basic security controls
- Expected to yield a FAR clause broadly applying cybersecurity requirements to all acquisitions

OTHER POTENTIAL DEVELOPMENTS

- Will Congress revive the Cyber Intelligence Sharing and Protection Act (CISPA)?
  - Recent cyber attacks may push us closer to "Big Brother"-style requirements
- President Obama pushing new cybersecurity legislation
  - Unveiled January 13th in wake of Sony Pictures hack
  - Similar measures have stalled over the last few years due to privacy concerns
  - Promotes cybersecurity information sharing between private sector and government, first to DHS
  - DHS to then share with NSA, FBI, Secret Service, and other agencies, raising privacy concerns
  - Law would shield companies from liability for sharing cyber threat data, as long as they remove personal information first
  - DHS must develop guidelines for the government's use and retention of the data

INCREASING FOCUS ON END OF LIFE EQUIPMENT TO PREVENT A DATA BREACH

- Improper handling of equipment taken out of service creates risk of data breach
  - Proper recycling of old equipment is becoming mandatory
  - Putting electronics in the dumpster for landfilling is not an option
  - Equipment removed from service must be isolated and secured
  - Most businesses create the potential for theft by leaving old equipment in an unsecured storage area
  - A majority of business equipment and devices store and retain data

IDENTIFYING AND SECURING DATA-CONTAINING MEDIA BEFORE RECYCLING

- Start with the assumption that all your equipment and devices contain data that must be protected
  - The 2014 Bitglass Healthcare Breach Report found 68% of breaches are a result of lost or stolen devices – only 23% are from hackers
  - Assign responsibility to inspect all material for data, either with your own personnel or a third party
  - Remove and secure data containing media and hold for proper data sanitization and destruction

REQUIRED CYBERSECURITY PRACTICES FOR ALL BUSINESSES

- Your business collects and stores Personal Identifiable Information (PII) and Electronic Protected Health Information (EPHI) in addition to your businesses confidential information
- There are scores of federal regulations related to safeguarding a wide range of data, including:
  - **HIPAA** – Health Information Portability and Accountability Act
  - **SOX** – Sarbanes Oxley
  - **GLB** – Graham Leach Bliley
  - **FACTA** – Fair and Accurate Credit Act
  - **FISMA** – Federal Information Security Management Act
  - **COPA** – Child Online Protection Act

LET'S TALK ABOUT HIPAA

- HIPAA has very specific requirements for safeguarding data and can be applied to any entity to safeguard data
- Specific safeguards must be implemented
  - **DISPOSAL (R) - § 164.310 (d)(2)(i)**
    - This disposal implementation specification states that covered entities[1] must:

"Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored."

[1] A covered entity includes healthcare providers, companies with health plans, any person or organization who furnishes, bills, or is paid for health care in the normal course of business and who electronically transmits any health information in connection with transactions.

HIPAA DATA BREACHES ARE COSTLY

- Fine limits have increased from $25,000 per incident to $1,500,000 per incident and up to five years in prison
- State Attorney Generals can enforce the HIPAA Data Security Provision
- According to the latest study by the Ponemon Group, the average cost of a data breach to a company was $3.5 million in US dollars in 2014 – 15% more than in 2013
- The average cost per record compromised in a data breach for US companies is $201, not including the cost to reputation, brand, and goodwill
- Credit card records go for $1, while medical records go for $50

RESOLUTIONS FOR HIPAA COMPLIANCE

- Create written policies and procedures and ensure they are followed
- Designate someone responsible for inspecting all equipment for data
- Remove data containing media and have it properly sanitized following NIST 800-88 or NSA guidelines
- Use a vendor who specializes in data sanitization and will provide a Certificate of Data Sanitation, since your IT department cannot "self certify"
- Use a vendor for the recycling of the equipment that can certify 100% recycling and that nothing was illegally exported or landfilled (Look for R2:2013 or eStewards Certifications)
- Perform very detailed due diligence in selecting vendor – You generated the data and are still responsible for safeguarding it, plus a vendor cannot indemnify you
- You must enter into a Business Associate Agreement (BAA)
- Consider "Data Breach Insurance" (Cyber Liability Insurance)

MORE CYBERSECURITY RESOLUTIONS

- Be more introspective
  - Conduct a "data inventory" so you know what type of data you have, and what data transitions over your network
  - What are you currently doing to protect your data?
  - Who can access your systems and data?
  - What are your internal policies and procedures regarding safekeeping of your data and systems, incident response and reporting, employee training, etc.?
  - What do your contracts with customers and up/downstream partners require of you in terms of data security?
  - Do not think of cybersecurity simply in terms of ROI – your reputation and business development are potentially at stake

MORE CYBERSECURITY RESOLUTIONS (CONT'D)

- Make a Plan
  - You should have a company policy and procedures for protecting your sensitive data
  - Your plan should at least address:
    - How different types of data you have will be handled and protected
    - NIST 800-53 controls, as appropriate
    - Who has access to your data
    - Password and encryption protocols
    - Data backup procedures
    - Incident reporting procedures and timeline
    - Responsible company officials and chain of escalation
    - Control physical access to your computers and networks
    - Regular updates for anti-virus software, software security patches, firewalls, etc.
    - Employees: training; social media policy; access restrictions; and consequences for noncompliance with the policies and procedures

MORE CYBERSECURITY RESOLUTIONS (CONT'D)

- Do unto others
  - You should have the same expectation of adequate security from your contracting partners and vendors as the government and other contractors will have of you
  - Critical to tighten up your subcontracts, joint venture agreements, and other arrangements with customers, partners, and vendors
    - Make sure to flow down prime contract cybersecurity requirements to subcontractors
    - Require proof of adequate security measures
    - Include indemnification and other recourses for noncompliance

Questions?

Thank you for joining us today.

If you would like to speak with Jon or Steve about cybersecurity issues, please contact them at:

Jon Williams
jwilliams@pilieromazza.com
(202) 857-1000

Steve Chafitz
steve@eendusa.com
(240) 529-1010

WANT TO LEARN MORE?

Sign up for our newsletters and blog at
www.pilieromazza.com

PM Legal Minute - Our blog, written by all of PilieroMazza's attorneys, provides trending insight to small and mid-sized businesses.

Legal Advisor Newsletter - Our publication which addresses current issues that are of concern to federal government contractors and commercial businesses nationwide. The *Legal Advisor* articles focus on recent legal trends, court decisions, legislative and regulatory rule-making as well as other newsworthy events.

Weekly Update - An e-mail sent every Friday that provides an up-to-the minute recap of legislative and regulatory issues affecting small businesses.

You can also follow us on:

@pilieromazza

Find past webinar recordings on the PilieroMazza YouTube Channel