Building in the Safe Zone: Deconstructing Cyber Risks

Addressing Cyber Security in the Construction Industry

CONSTRUCTION SUPERCONFERENCE 2016

BRG Berkeley Research Group

Charles V. Choyce, Jr., MRICS, PSP, CM-LEAN, PMP, CFCC
Managing Director
Amit Garg, CISSP, PMP, MBCI
Director

JONES DAY

Fernand Lavallee, Esq.,
Partner

YATES CONSTRUCTION

Dodds Dehmer, Esq.
VP and General Counsel

ROGERS JOSEPH O'DONNELL, PC

Aaron Silberman, Esq.
Shareholder

Panelists

- **Charles V. Choyce, Jr., MRICS, PSP, CM-LEAN, PMP, CFCC**
  Managing Director, Berkeley Research Group, LLC

- **Amit Garg, CISSP, PMP, MBCI**
  Director, Berkeley Research Group, LLC

- **Dodds Dehmer, Esq., Vice President and General Counsel**
  The Yates Companies

- **Fernand Lavallee, Esq.**
  Partner, Jones Day

- **Aaron P. Silberman, Esq.**
  Shareholder, Rogers Joseph O'Donnell, P.C.

WHAT ARE THE CURRENT CYBER SECURITY RISKS IN THE CONSTRUCTION INDUSTRY?

Top 5 Cyber Issues Facing the Construction Industry

- Phishing attacks
  - Malware
  - Ransomware / extortion
- Corporate / industrial espionage
- Unauthorized access to client or employee information (PII) and lost or stolen intellectual property including
  - Project/bid data
  - Architectural design data
  - Privileged contracts
  - 3rd party data
  - Laptops and mobile devices
- Internet of Things (IOT) – smart thermostats, connected devices, water heaters, sensors, smart light bulbs, and power systems, etc.
- Lack of encryption for valuable data

WHAT ARE THE CURRENT CYBER SECURITY REQUIREMENTS FOR GOVERNMENT CONTRACTS?

Controlled Unclassified Information (CUI) Program Implementation

- Virtually all information developed, created, ***used in the performance*** of, a federal construction contract or subcontract (at any tier) can be CUI
- NIST Standards
  - NIST SP 800-53: *Security and Privacy Controls for Federal Information Systems*
  - NIST SP 800-171: *Protecting CUI in Nonfederal Information Systems and Organizations*
- No Overarching Federal Acquisition Regulation (FAR) CUI Clause – Yet
  - Some agencies, particularly DoD, established interim rules to protect certain information
- National Archives & Records Administration (NARA) Final Rule [32 C.F.R. part 2002], effective Nov. 14, 2016, establishes policy for designating, safeguarding, marking, decontrolling, and disposing of CUI

Federal Contract Clauses

- FAR Clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems (Jun 2016)
- DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

Cyber-Incident Reporting and Response

- Contractors and subcontractors must "rapidly report" incident reports to DOD
  - Rapidly report: 72 hours
    - https://dibnet.dod.mil
    - Medium assurance certificate from ECA
- Conduct review for evidence of compromise, ID affected servers, data, accounts, etc.
  - Image/Preserve contractor network for at least 90 days
  - Contractor "shall" provide Government with access to information or equipment

FAR Clause 52.204-21 Basic Safeguarding of Covered Contractor Information Systems (June 2016)

- Outlines minimum controls for protecting contractor information systems that process, store, or transmit federal contract information
  - *Information, not intended for release, provided by or generated for the government under a contract to develop or deliver a product or service to the government*
  - *Includes e-mail*
- 15 discrete control requirements identified in the clause

DFARS Clause 242.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting

- Effective October 21, 2016
  - Replaces Interim Rules implemented in 2015
- Finalizes DFARS cybersecurity provisions and cyber-incident reporting requirements
- Expands definition of Covered Defense Information ("CDI")
  - Unclassified Controlled Technical Information ("UCTI")
  - Other CUI that is (1) marked or otherwise identified in the contract or (2) collected, developed, etc. in support of the contract

HOW SHOULD CYBER SECURITY RISKS BE ADDRESSED IN CONSTRUCTION CONTRACTS?

WHAT BEST PRACTICES SHOULD BE FOLLOWED TO ADDRESS CYBER SECURITY RISKS IN CONSTRUCTION?

Risk Management & Compliance Best Practices

- Take a risk based approach to security and privacy
- Engage all stakeholders – IT, legal, vendors, compliance, users, business development, CIO/CISO level support
- Go for the low hanging fruit / the “basics”
  - Change default passwords
  - Patch and update where possible
  - Enable encryption
  - Limit administrative accounts and remove unneeded accounts
- Have an incident response plan in place
- Develop a third party vendor risk management program

5 Things You Can Do Today to Combat the Cyber Threat

- Develop an enterprise risk management program
  - Draft and implement security policies and procedures
  - Develop remediation plan
- Conduct a baseline risk assessment and periodically thereafter
- Develop an incident response plan and test it at least annually
- Apply industry best practices – NIST, ISACA, ISO standards, ISACs
- Create a culture of security awareness and training

QUESTIONS?

Charles V. Choyce, Jr., MRICS, PSP, CM-LEAN, PMP, CFCC
Managing Director, Berkeley Research Group, LLC
1800 M Street, NW, 2nd Floor
Washington, DC 20036
(202) 480-2732
cchoyce@thinkbrg.com

Amit Garg, Director
Berkeley Research Group, LLC
1800 M Street, NW, 2nd Floor
Washington, DC 20036
(202) 747-3483
agarg@thinkbrg.com

Dodds Dehmer, Vice President and General Counsel
The Yates Companies
500 Greymont Avenue, Suite A
Jackson, MS 39202
(601) 351-2015
dodds@wgyates.com

Fernand Lavallee, Esq.
Jones Day
51 Louisiana Avenue, NW
Washington, DC 20001
(202) 879-3486
flavallee@jonesday.com

Aaron Silberman, Esq.
Rogers Joseph O'Donnell, PC
311 California Street, 10th Floor
San Francisco, CA 94104
(415) 365-5339
Asilberman@rjo.com