



COVID-19: Insights and Guidance

An ABC webinar series featuring industry experts to answer your questions about the legal, safety, technology and economic impacts of COVID-19.



Brought to you by ABC's Strategic Partners



Presenters



David Pugh

- Partner at Bradley, represents owners, general contractors, subcontractors, engineers, architects, insurers and sureties throughout the United States, advising his clients at every stage of a construction project.
- He also serves as ABC's 2020 Southeast region vice chair. He has been an active member of the ABC Alabama Chapter since 1998 and served as its chair in 2017.



David Vance Lucas

- Partner and Lead of the International and Cross Border Practice at Bradley
- Provides legal strategy for technology and business on intellectual property, international, governmental and complex litigation



Mike Manley

- President Gray Analytics
- Provides strategic direction and leadership for the business portfolio at Gray Analytics. Over 30 years' experience in the IT and Cybersecurity fields



Scott Gray

- Vice President Gray Analytics
- Provides Operational and Business Development leadership for Gray Analytics. Over 30 years' experience working with government customers and systems integrators.



Bradley | 150 YEARS **Gray**
Analytics

Cybersecurity

Health and Compliance

Associated Builders and Contractors



Cybersecurity Training

Agenda

- ✓ Protecting Critical Data and Assets
- ✓ Basic Cybersecurity Hygiene
- ✓ Email Security
- ✓ Patching/Updating
- ✓ Password Best Practices
- ✓ Social Media Best Practices
- ✓ Insider Threat
- ✓ Remote Workers
- ✓ Cybersecurity Maturity Model Certification
- ✓ Cybersecurity Compliance

Cybersecurity Ventures predicts cybercrime damages

will cost the world \$6 trillion annually by 2021,
up from \$3 trillion in 2015.



Protecting Critical Data and Assets

What is critical data?
What is a critical asset?

Bradley

Protecting Critical Data and Assets

General Rule of Thumb:

Determining a critical data or asset involves deciding if the information can be shared outside of the organization.

Only you and your company can define the organization's "crown jewels."

A partial list:

- ✓ Key Intellectual Property
- ✓ Customer Information
- ✓ Employee Records
- ✓ Company Financial Information
- ✓ In-Development Product Offerings
- ✓ Patent Information
- ✓ Passwords



Basic Cybersecurity Hygiene

What. Why. How.

Basic Cybersecurity Hygiene

What is it?

“The practice and steps that users of computers and other devices take to maintain system health and improve online security.”

~Digital Guardian

Cybersecurity Hygiene Practices should be based on the Cyber “CIA” Triad.



Basic Cybersecurity Hygiene

Why should I maintain it?

To avoid these high risks:

- ⚠️ Lack of availability to critical information
- ⚠️ Corruption of valuable company data
- ⚠️ Loss of proprietary company data
- ⚠️ Company reputation damages
- ⚠️ Network security breaches
- ⚠️ Identity theft

What are common practices for strong Cybersecurity Hygiene?

USE CAUTION

If you aren't sure, ASK!



Be suspicious! You are a target!

Recognize your and your client's information is at risk.



Physical security for cyber assets.

Keep your devices locked. Be careful what you attach to your devices.



Follow password rules.

(More about this later.)



Work with Client Services.

Keep all software, virus protection, and endpoint protection current.



Back it up.

Securely back up critical information and data.



Be careful what you click and what you download.

Don't know the source? Assume it is dangerous.

Email Security

Phishing
Spear Phishing
Whaling
Business Email Compromise

LEARNING THE DIFFERENCES



Phishing

What is it?

Phishing is the practice of sending fraudulent emails, purporting to be from legitimate sources in order to induce divulging personal or company information.

This attack type is usually executed using a “payload” file or web link.

Recipients click the link, giving the attacker a foothold into recipient’s computer or causes user to divulge desired information (SSN, Bank Account, Password, etc.).

These attacks are usually sent to masses of people.

Spear Phishing and Whaling are very similar to phishing but are more targeted to specific individuals - often executive or administrative level employees.

Intelligence is gathered and individuals are targeted based on their standing or ability to provide protected information.

Most often used in an attempt to gain access or information from corporate entities.

Whaling targets the individuals in the company at the highest levels

The assumption is that highest level individuals would have complete access to the crown jewels or most critical information of the company.

”

It is a consistent finding during our cyber incident investigations that email is the top vector for compromising individuals and organizations

Gray Analytics



Phishing, Spear Phishing, and **WHALING** attacks are meant to steal something or gain a foothold for further malicious actions:

- ⚠ Personal or company information
- ⚠ Credentials
- ⚠ System and network information
- ⚠ Access to other personal or company systems ... including customers and partners!



What is Business-Email Compromise ?

Business Email Compromise is e-mail fraud

that typically targets employees with access to financial systems, bank accounts, or customer systems and accounts.

The attack is orchestrated by

- gaining access to corporate email systems or spoofing addresses and
- sending requests for funds transfers, payments, or even gift cards,

... purportedly from a high-ranking official.

*The FBI estimates over \$5.3 Billion in losses between
10/2013 -12/2016 .*

<https://www.ic3.gov/media/2017/170504.aspx>

How to Avoid Email Compromise

Tips from
FBI Tech Tuesday Newsletter

#1

Look at sender's email header.

Watch for email addresses appearing similar to, but not identical to those used by work supervisors or peers.

Example:

"abc_company.com"

vs.

"abgcompany.com"

#3

Watch for grammatical errors or odd phrasing.

#2

Be wary of requests to:

- wire funds,
- make payments,
- or buy multiple gift cards,

even if request seems ordinary!

#4

Notice language that tries to pressure you to purchase the cards quickly.

How to Avoid E-mail Compromise

Tips from
FBI Tech Tuesday Newsletter



#5

Be extremely wary if the sender asks you to transmit a gift **card number** and the **PIN** back to them.

#6

Don't rely on e-mail alone!

Speak directly to
The sender, a supervisor
or their supervisor.

Use 2 party verification!

Initiate the action!

#7

Train, Train, Train your employees.

Run or have someone run Phish testing simulations regularly

A person's hands are shown typing on a laptop keyboard. The image is overlaid with a blue-tinted digital security theme, including a large shield icon with a keyhole, binary code, and network diagrams. The word "Passwords" is written in large white letters across the center.

Passwords

Password Best Practices

Create passwords with at least 14 characters.

Use upper & lowercase.

Use passphrases like:

- *Thequ!ckBr0wnfoxjumpedoverthe1@zydog*
- *\$howMetheMon3y!*

Change your password often.

Avoid using your username within passwords.

Avoid using one password for multiple accounts.

Avoid simple keyboard combinations.

Avoid storing passwords
in a plain text file or
writing them on a sticky note!



Use Multi-Factor Authentication!

Store passwords in an electronic
password “vault,” like:

- LastPass
- PasswordSafe
- KeepPass

A person's hands are shown typing on a laptop keyboard. The background is a dark blue digital theme with a network of white lines and nodes. A large, semi-transparent shield icon with a white keyhole is positioned on the right side of the image. The shield is surrounded by a circular pattern of white lines. The overall aesthetic is futuristic and tech-oriented.

Patching/Updating

Patching/Updating Systems



Image from ITarian

Create a patch management policy, define systems, responsible parties, what is to be patched and how frequently

Use automation, employ automated patch management where possible through multiple vendors or through a holistic patch management system

Have a well-defined and robust testing plan, regularly test patches and updates before deploying to your IT systems to reduce unnecessary downtime

Review efficacy of patch management, don't just trust that systems are being updated. Verify THEN trust

Plan for Technology Refresh, Old systems become more vulnerable through time. Have a plan and budget to keep systems current

Social Media



Social Media Best Practices

Don't post or tweet:

- Personal or confidential information
- Specific travel details
- Threatening statements
- Illegal activities

Avoid publishing posts that create a negative impression of:

- Yourself
- Your family
- Your company

Good practice: Annual Google Checkup!

*Everything on social media is searchable****

Everything on social media creates a permanent record!

[Insider Threat]

EMAIL SECURITY



Insider Threat

Insider Threat is potentially malicious and damaging, intended or unintended,

and can come from anyone with access to / knowledge of organizational information, data, computers, and security practices.

Current & Former Employees
Business Partners
Contractors & Vendors

Watch for suspicious behavior:

- Failure to follow security processes & processes
- Sudden change in financial situation
- Working outside normal hours
- Disgruntled employee
- Absenteeism
- Constant Tardiness

What motivates insider threats?

- Money
- Job Dissatisfaction
- Political Beliefs
- Coercion


Timely reporting to management is the best defense to insider threats!

Insider threat may be the **#1 risk** to organizations.

IS Decisions estimated **666,000** internal security breaches within the U.S. in 12 months.

(2,560 per day)

IBM found **60% of all attacks** were carried out by insiders.



Remote Workers



Bradley

GrayAnalytics

Remote Worker Threats

Command and Control through Phishing

- Attackers Use Email Links to Deliver Payload
- Gain Elevated Access to Home Machines
- Can Use Key Loggers
- Steal Personal or Company Information

Negligence

- Remote Workers Can Access and Process Company Information
- Home Machines May Not be Protected with the Same Rigor as Work Machines
- Remote Workers May Leave Sensitive Files Open to Unauthorized Access
- Remote Workers May Use Risky File Sharing Mechanisms

What Can We Do?

- Have a Policy for Remote Workers– Set clear expectations
- Educate Users!
- Run Phish Testing Campaigns Against Remote Workers
- Reinforce a Verify, then Trust Approach

Cybersecurity Maturity Model Certification (CMMC)

DoD's Next Evolution in Cyber Compliance:

- What is CMMC?
- Why is there a need for CMMC?
- How Does it Affect Me?
- How Should We Prepare for CMMC?

What is CMMC?



- Cybersecurity Maturity Model Certification or CMMC is the DoD's Framework for Cybersecurity Preparedness for Cleared Defense Contractors
- Applies to ALL Government Contractors Doing Business with DoD
- Will Include Levels One Through Five (Basic Cyber Hygiene to Advanced Controls)
- Will be Based on Multiple Current Cyber Control Standards
- NIST SP 800171, NIST SP 80053, ISO 270001, AIA NAS9933, Others
- Government will Prescribe the Appropriate Tier Level Based on Contract Requirements
- Sections L & M of RFPs

Why is There a Need for CMMC?

- Loss of Controlled but Unclassified Information (CUI) from Cleared Defense Contractors Threatens National Security
- Council of Economic Advisers Estimated U.S. Economic Losses From Cyber Attacks of Between \$57B and \$109B for 2016
- It has Been Estimated that Almost 1% (\$600B) of GDP May be Lost Annually Due to Cybercrime
- 2018 Report from MITRE Corporation Determined Majority of CDCs Did Not Meet Current Federal Acquisition Standards for Cyber Protection
- DoD Must be Able to Assess and Improve Cyber Posture for the Defense Industrial Base (DIB)
- CMMC Serves as the Verification Mechanism for Assurance of proper Cyber Process and Practices for DIB Companies
- Will effectively replace NIST 800-171 Compliance Self Certification



How Does CMMC Affect Me and My Company?

- ALL Government Contractors Who Do Business with DoD Must Be Certified by Certified 3rd Party Assessing Organization (C3PAO)
- For Most Organizations, Preparation for Certification Will Take Some Time and Effort
- Certifications Will be Valid for 3 Years
- Forces Strategic Decisions to be Made Related to Which Level of Certification to Pursue and When
 - Could be a Business Differentiator
- If You are a Subcontractor, Will Still Need to be Certified



How Should We Prepare for CMMC?



- Ensure Leadership Buys In Immediately
 - CMMC Will Happen and Cannot be Ignored
- Begin Now With Internal Policy and Practice Reviews
 - Be Proactive – Pursue Level One Now
- Review NIST SP800-53 and SP800-171 Controls for Current Compliance
 - Compliance to SP800-171 was Mandatory for all Government Contractors by December 31, 2017
- Enlist Help from a Professional, 3rd Party Organization Now
 - An Independent Viewpoint of Current State Can Help You Prepare Better for Future Needs
 - Registered Provider Organization (RPO) program being set up



Cybersecurity Compliance **US Department of Defense Contracting**

David Vance Lucas

US DoD Cybersecurity Requirements

Executive Cyber Order 13556

- Protect national security data and networks from cybersecurity threats
- Eliminate inconsistent agency-specific policies
- Establish a uniform program for safeguarding information
 - Government contractors and subcontractors that handle Controlled but Unclassified Information (CUI)
 - Defense information on systems that support the performance of DoD contracts



Bradley

Cybersecurity Regulations

Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7000 et. seq.

- DFARS regulations adopted October 2016
- Compliance deadline December 31, 2017

Defense Security Services “Insider Threat Program” (ITP)

- May 2016 “Insider Threat Program” (ITP)
- NISPOM Change 2 required the implementation, certification and maintenance of an ITP

DFARS Key Points

Subcontractors

- Prime Contractors must "flow down" 7012 requirements to subcontractors
- Subcontractors must notify the Prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from NIST SP 800-171 to the Contracting Officer

DFARs / ITP Cybersecurity Requirements

- Access control, authentication, media protection, physical protection, monitoring, and malware defense as specified in NIST SP 800-171
- Robust policies and procedures
- Procedures for incident response, document retention, audits, awareness and training
- Rapid response capability to data and network threats and breaches

DFARS Key Points

Adequate Security



- Compliant with NIST SP 800-171 by 12/31/2017
- Cloud services must
 - comply with DFARS 252.239-7010 if operated on behalf of government
 - meet Federal Risk and Authorization Program (FedRAMP) Moderate baseline requirements if not operated on behalf of government

DFARS Key Operational Considerations

- Medium Assurance Certificate
 - Obtain a DoD-approved medium assurance certificate
 - <http://iase.disa.mil/pki/eca/Pages/index.aspx>
- Malicious Software
 - Notify your Contracting Officer
 - Submit malicious code to DoD Cyber Crime Center (DC3)
- Media Preservation and Protection
 - Preserve and Protect images of affected information systems
 - Maintain for at least 90 days after submitting the cyber incident to the DoD

What is DCSA / NISPOM ?

- Defense Counterintelligence Security Agency (DCSA)
 - Responsible for security of US classified information and cleared facilities
- National Industrial Security Program Operations Manual (NISPOM)
 - Specifies requirements for US cleared facilities and handling of classified materials
- NISPOM Change 2 "Insider Threat Program" (ITP) – requires
 - Certification and maintenance of an ITP
 - Appointment of Insider Threat Program Senior Official (ITPSO)
 - Awareness training of all cleared personnel by May 31, 2017.

Who is Covered?

- Any contractor that stores **CUI** on its servers, in support or performance of a DoD contract
- Any contractor who has **access/connectivity** to DoD networks or systems

DFARS 252.204-7012

What is Controlled Unclassified Information (CUI)?

- Information which would be export controlled or restricted under US export control laws or regulations
- U.S. Army Medical Research Institute for Infectious Diseases
 - Technical enhancements for responding to biological threats, including the world's deadliest pathogens



What is Covered Defense Information?

- CUI that is either identified by DoD, or collected, developed, received, transmitted, and stored by or on behalf of the contractor
- Information which has certain controlled distribution markings
 - Certain Federal military architecture specifications, for example



Barracks



Military Facilities, Afghanistan

Third-Party Intrusion / Disclosure

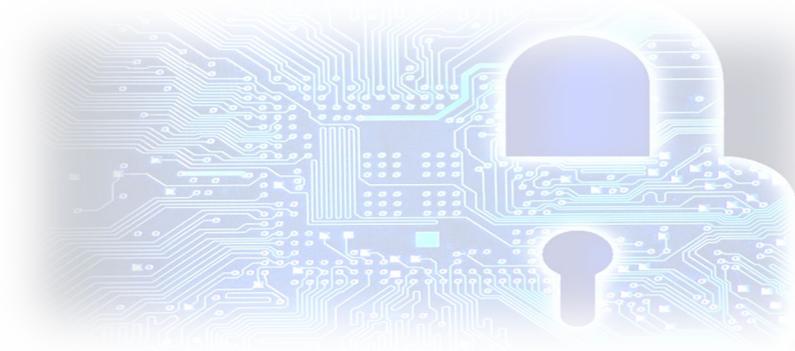
Network / Systems Breach

- **Economic espionage**
 - Malicious Software
 - Cloud-based attack
 - Market disruption
- **Political Espionage**
 - Cyberwar
 - Virtual trade disputes
 - Geopolitical targets



Physical Intrusion

- **Unauthorized Persons**
 - Access to facilities
 - Access to documents
 - Access to computers
- **Criminal Break- In**
 - Theft of equipment



Internal Intrusion / Disclosure

Rogue employees

- Co-workers leave around same time
- Customer receives substantially similar technical materials
- Rogue employees had access to confidential technical, customer and CUI
 - Rogue employee leaves with “personal effects”
 - Actual personal effects left in employee’s office
 - Search reveals email to competitor and access to CUI bid files before departing
 - Call to competitor confirms new employment



Key DFARS Cyber Incident Requirements

- Cyber incident must be reported within 72 hours of discovery (DFARS 252.204-7012)
- Malicious software must be provided to DOD Cyber Crime Center (DFARS 252.204-7012 subsection (d))
- Must preserve copy of system and monitoring data for 90 days from incident report, and allow DOD access for forensic analysis (DFARS 252.204-7012 subsections (e)-(f))

Cyber Incident Reporting

DoD cyber submissions at <https://dibnet.dod.mil>

DIB Cyber Incident Collection Form - Dcise Survey Portal Page 1 of 3

Unclassified for Official Use Only (When Filled Out)
Defense Industrial Base (DIB) Cyber Incident Reporting
Incident Collection Format

Mandatory Incident Report
*Questions marked with * are required.*

General Information	I. Company Identification	II. Company POC Information	III. Contract or Other Agreement	IV. Incident Information	V. Ancillary Information	Preview
---------------------	---------------------------	-----------------------------	----------------------------------	--------------------------	--------------------------	---------

USG Contracting POC

USG Contracting Officer or Other Agreement Point of Contact 1

* Last Name * First Name

* Position/Title

* Address

* City/Town * State/Province * Postal Code * Country

* Telephone * Email Address * Time Zone

* Is there a USG Administrative Contracting Officer Point of Contact?
 Yes No

USG Administrative Contracting Officer Point of Contact 1

* Last Name * First Name

* Position/Title

* Telephone * Email Address * Time Zone

USG Program Manager Point of Contact 1

* Last Name * First Name

* Position/Title

* Address

* City/Town * State/Province * Postal Code * Country

* Telephone * Email Address * Time Zone

https://dcise.cert.org/dib-cyber-incident-collection-form?p_auth=9kUIGM1a&p_p_id=Surv... 2/9/2018

Information Subparts for On-line Reporting

- General Information
- Company Information
- Company POC Information
- Contract or Other Agreement
- Incident Information
- Ancillary Information



Proliferation of Laws, Standards and Regulations

- Federal and state laws
- Federal and state privacy statutes of general applicability
- Sector-specific laws: Health, Financial, Workplace, Student
- Industry and regulatory guidance
- Non-U.S. laws with extraterritorial reach
- Contracts

Cybersecurity Advanced Preparation

General preparations

- Evaluate need for CUI / Personal Data
- Identification of CUI / Personal Data, uses and locations – “Data Map”
- Assessment physical, cyber and data weaknesses
- Understanding of business, operations, customers and employees
- Determine need for DPO and ITPSO

Rapid response

- Analysis of possible response strategies
- Identification of programs which could be involved
- Analysis of probable intrusions and mitigation plans
- Pre-determination of resources for rapid response

Cyber/Privacy Operational Strategies

- CUI / Personal Data Provisions
 - Employment Agreements
 - Employee Proprietary Rights Agreements
 - Employee Handbook and Code of Conduct
 - Non-disclosure and Confidentiality Agreements
 - Customer Agreements
 - Teaming, Secondment and Joint Development Agreements
- Procedures for tracking CUI / Personal Data
- Physical and cyber security of CUI / Personal Data

Questions?



Michael.manley@grayanalytics.com
256.424.6786



Scott.gray@grayanalytics.com
256.929.2630



dpugh@bradley.com
205.521.8314



dllucas@bradley.com
256.517.5131

Gray Analytics

Gray Analytics:

<https://www.grayanalytics.com>

Thank You!!

Bradley

Bradley Arant

<https://www.bradley.com>



Brought to you by ABC's Strategic Partners

