



Huntsville Madison County Chamber

Cyber Insurance Issues for the Defense Industry

May 04, 2021

Heather Howell Wright & Andrew Tuggle

NotPetya

“The most destructive and costly cyber-attack in history.”

-- White House

“The weapon’s target was Ukraine. But its blast radius was the entire world.”

-- Andy Greenberg

“To put it plainly, this code was built to destroy, not extort.”

-- Iain Thomson

- In June 2017, malware crippled computer systems **around the world.**
- **\$10,000,000,000 (i.e., \$10 billion) damage**
- **Seven different countries blamed Russia.**

Current DoD Cybersecurity Requirements

NIST SP 800-171
Basic Assessment
Cyber Incident Reporting

CMMC Framework

Assessment and Certification
CMMC Marketplace & Ecosystem

Introduction to Cyber Insurance

Increasing Cyber Risks
Coverage under Standard Policies
Cyber-Specific Policies

War Exclusions

Mondelez v. Zurich
Evidentiary Problems

Protect Yourself.

Have good cyber hygiene.
Have good cyber insurance.

Current DoD Cybersecurity Requirements

Bradley



Adequate Security

“The Contractor shall provide **adequate security** on all covered contractor information systems.” – DFARS 252.204-7012(b).

Covered Defense Information (CDI)

- Unclassified controlled technical information
 - technical information with military/space application
 - usually Distribution Statements B – F
- Controlled Unclassified Information (CUI)
- Must be **marked** (or identified in the contract)
- Must be “in support of the performance of the contract”

Covered Defense Information (CDI)

- Unclassified controlled technical information
 - technical information with military/space application
 - usually Distribution Statements B – F

- Controlled Unclassified Information (CUI)

- Must be **marked** (or identified in the contract)

- Must be “in support of the performance of the contract”

This presentation focuses on CDI, **not** classified information or federal contract information (FCI).

DFARS Clauses for CDI

- DFARS 252.204-7008** *Compliance with Safeguarding CDI Controls*
- DFARS 252.204-7012** *Safeguarding CDI & Cyber Incident Reporting*
- DFARS 252.204-7019** *Notice of NIST SP 800-171 DoD Assessment Requirements*
- DFARS 252.204-7020** *NIST SP 800-171 DoD Assessment Requirements*
- DFARS 252.204-7021** *CMMC Requirements*

DFARS Clauses for CDI

- DFARS 252.204-7008** *Compliance with Safeguarding CDI Controls*
- DFARS 252.204-7012** *Safeguarding CDI & Cyber Incident Reporting*
- DFARS 252.204-7019** *Notice of NIST SP 800-171 DoD Assessment Requirements*
- DFARS 252.204-7020** *NIST SP 800-171 DoD Assessment Requirements*
- DFARS 252.204-7021** *CMMC Requirements*

Adequate Security

- For CDI, “adequate security” **means** NIST SP 800-171.
- As of November 2020, the Basic Assessment is now required.
- Cyber incident must be “rapidly reported” – *i.e.*, within **72 hours**.

NIST SP 800-171

- Protecting CUI in Nonfederal Systems and Organizations
- 110 security controls, categorized in 14 families
- Historically, compliance was largely aspirational.
- The option to self-certify + POA&M, led to endlessly delayed compliance.

*It was originally a subset of NIST SP 800-53, which controls contractors that manage IT systems for the government.

Basic Assessment

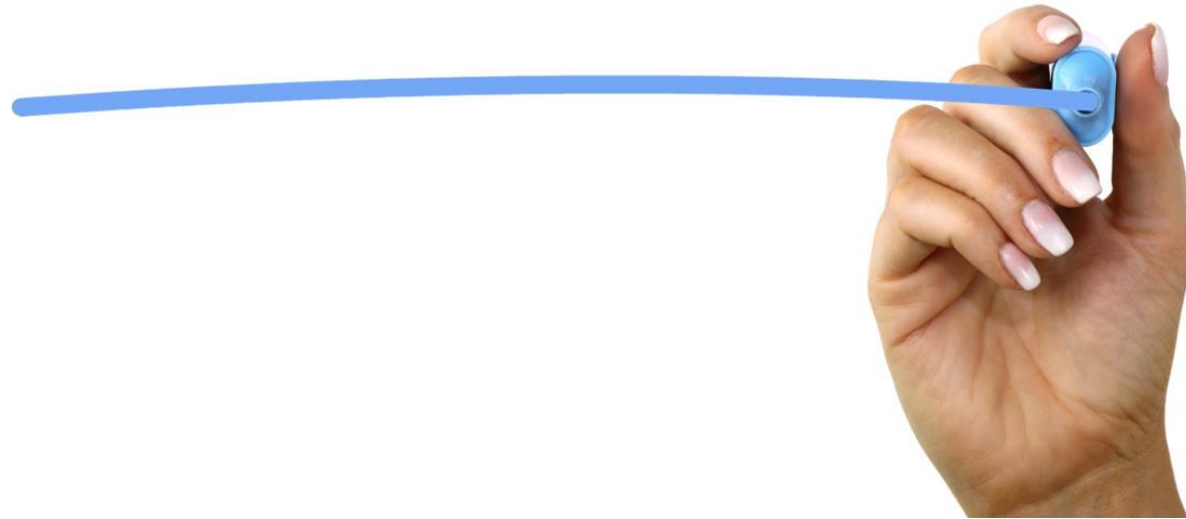


- Self-scored on a scale from -203 to +110
- Contractors must upload scores to SPRS ...
 - ... and have a date by which to score a *perfect 110*.
- We expect that the score will affect the government's procurement decisions.
 - A good score might also earn a lowered cyber insurance premium.
- Use this as a **bridge** from NIST SP 800-171 to CMMC.

CMMC Framework

Bradley

CERTIFIED



Cybersecurity Maturity Model Certification

“The Contractor shall have a current (*i.e.* not older than 3 years) CMMC certificate at the CMMC level required by this contract” – DFARS 252.204-7021(b).

CMMC Framework

- In many ways, CMMC builds on NIST SP8 800-171.
- Security requirements are arranged into 17 domains.
 - Substantially new domains are:
 - Asset management
 - Recovery
 - Risk management
 - Situational awareness
- But CMMC can be tailored up or down, and it has a more robust assessment ecosystem.

NIST SP 800-171 *versus* CMMC

NIST SP 800-171

- Self-certified
 - Scored under Basic Assessment
- One size fits all
- Only applies to CDI

CMMC

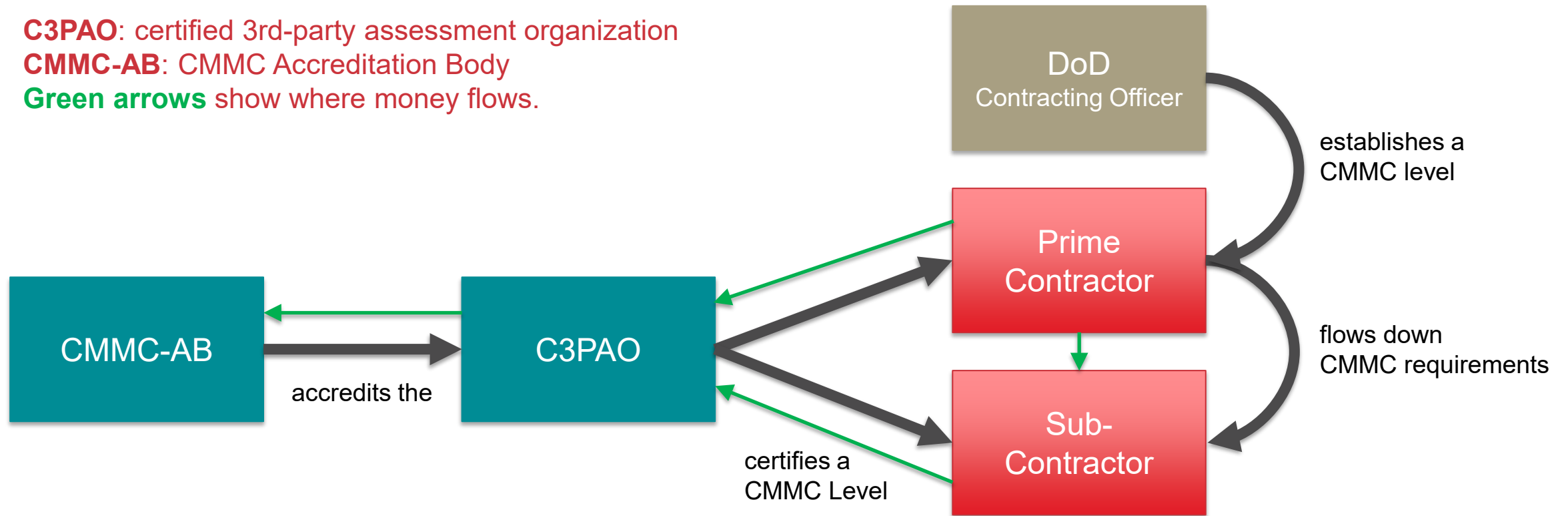
- Third-party certified by C3PAO
 - C3PAOs must be accredited
- Five CMMC levels
 - Level 3 corresponds most closely to NIST SP 800-171.
 - We expect Level 3 will be used with CDI
- Applies to all defense contractors
 - Level 1 will be used with FCI (*i.e.* FAR 52.204-21)

CMMC Framework

C3PAO: certified 3rd-party assessment organization

CMMC-AB: CMMC Accreditation Body

Green arrows show where money flows.



CMMC Framework

- CMMC Framework began rolling out last year.
- The plan was to completely supersede NIST 800-171 by October 2025.
- But the implementation has been delayed,
 - No C3PAOs have yet been accredited.
 - About 150 candidates are awaiting their Level 3 certification by DIBCAC.
- Like the Basic Assessment, a CMMC certificate would be good evidence that an insured is complying with an insurers requirements.

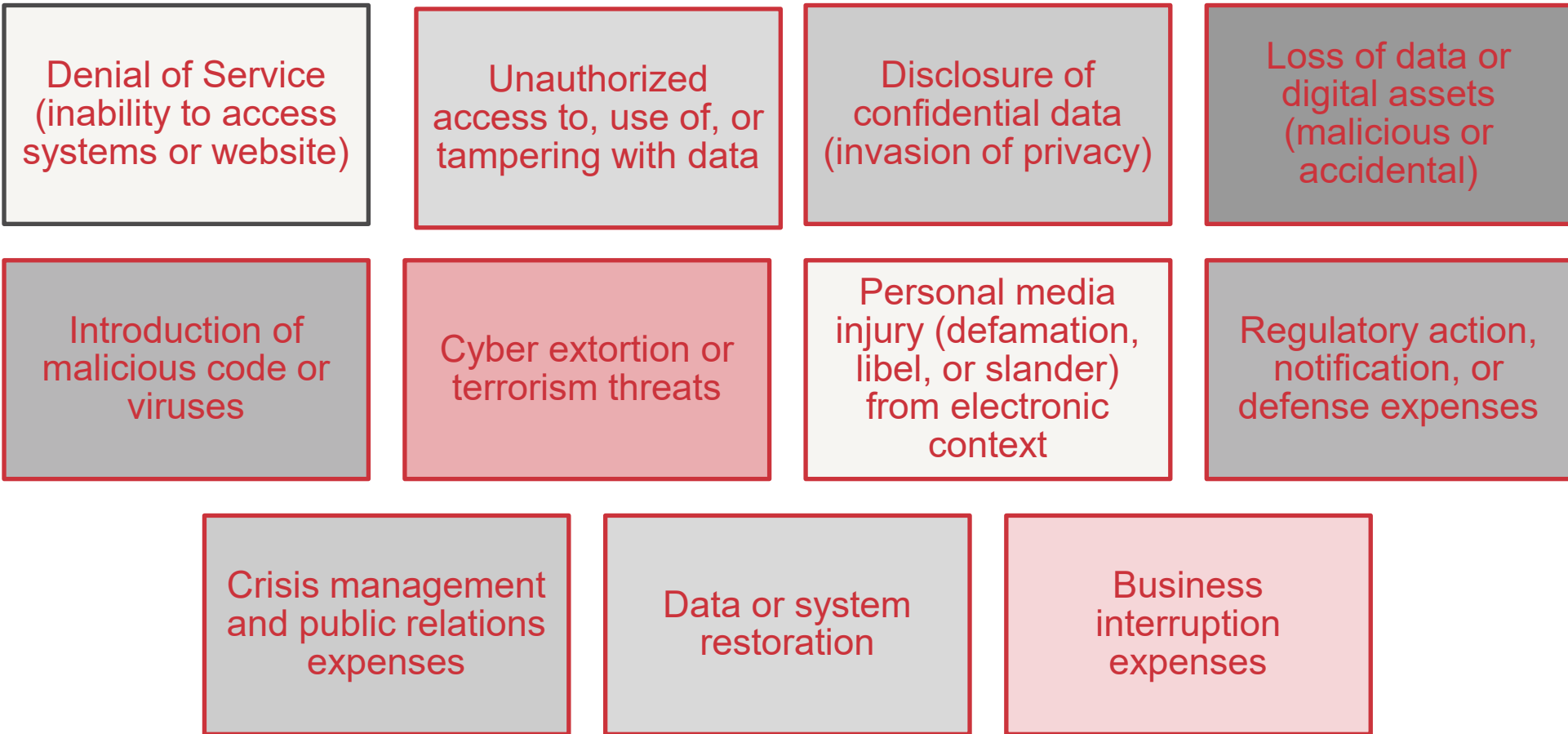
Introduction to Cyber Insurance

Bradley

Commercial Insurance 101



Cyber Insurance



Cyber Insurance 101

Property

Denial of Service/Access

Loss of Data

Business Interruption

Crisis Management

Extortion/Ransom

Liability

Disclosure of confidential data

Regulatory Action

Personal media injury

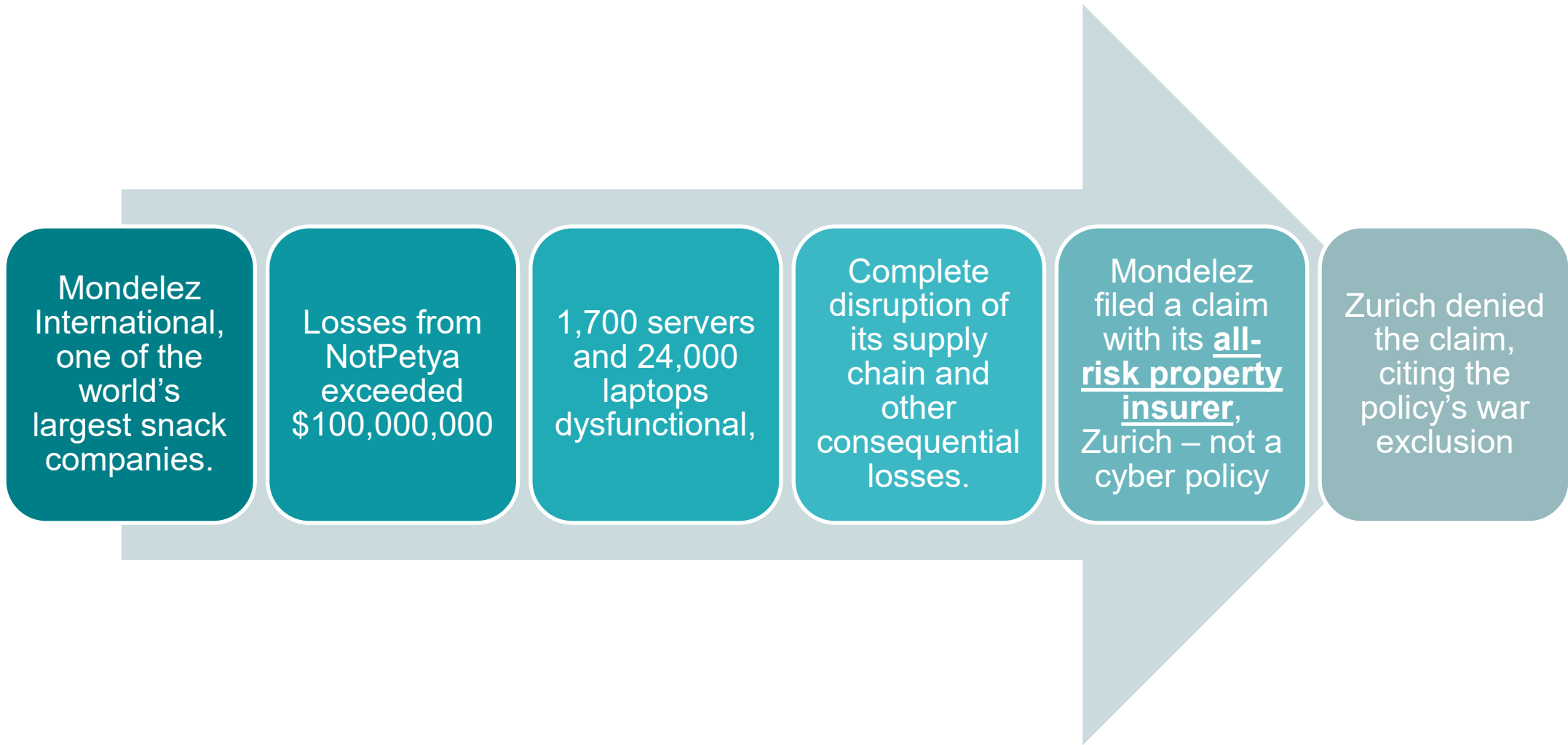
Introduction of Malware

Loss of Data/Data Corruption

War Exclusions

Bradley

Mondelez v. Zurich: War Exclusion Case Study



The Zurich Exclusion

This policy excludes loss or damage directly or indirectly caused by or resulting from . . . **hostile or warlike action** in time of peace or war, including action hindering, combating or defending against an actual, impending or expected attack by any:

- (i) government or sovereign power (de jure or de facto);
- (ii) military, naval, or air force; or
- (iii) agent or authority of any party specified in i or ii above

What is hostile and warlike?

Policy Interpretation

- Ambiguities in favor of insured
- Insurer must prove applicability of exclusion

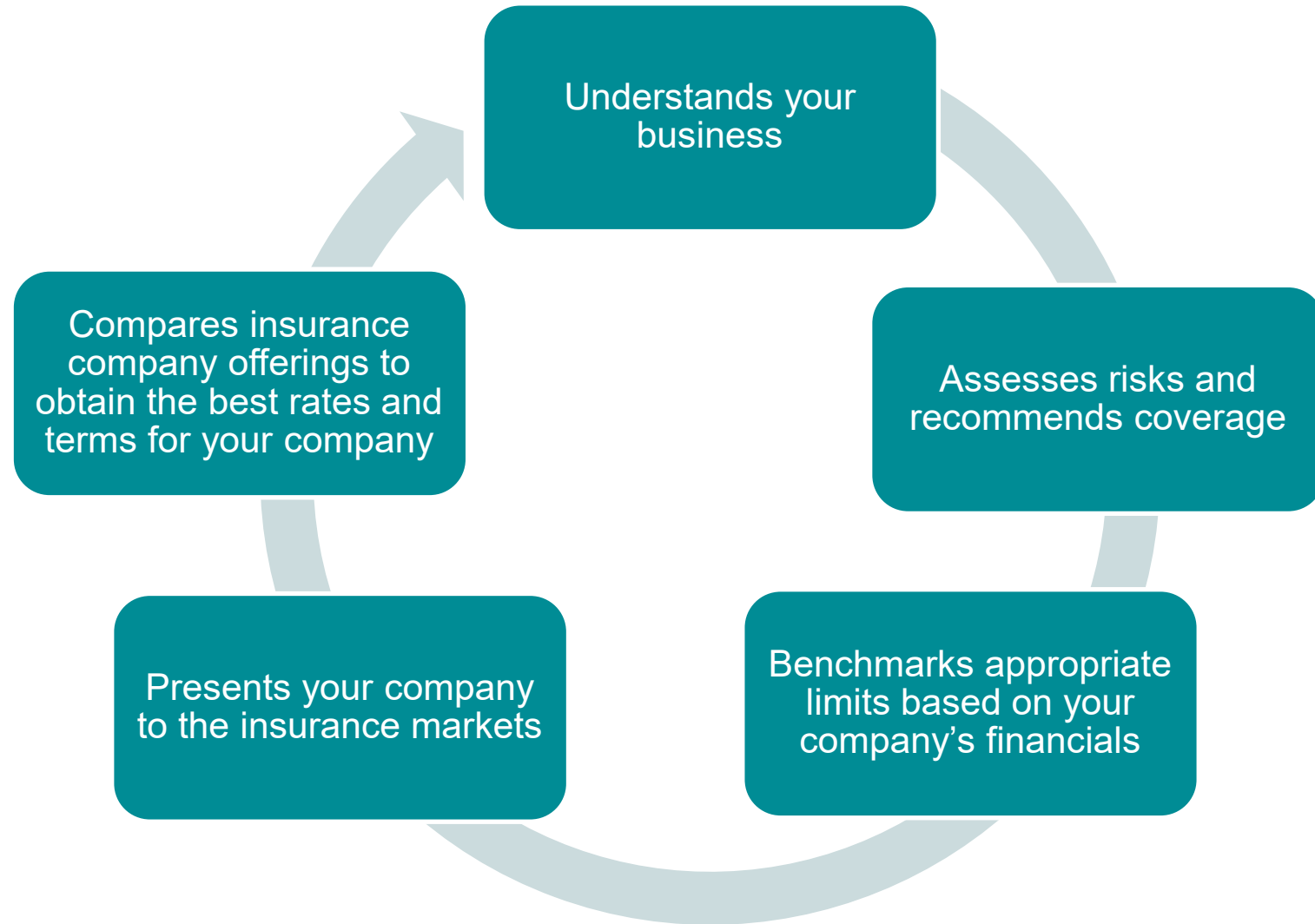
How to define

- What is hostile?
- What is warlike?


How to Prove

- Determination by State Department
- Terrorism Example

Ensuring Adequate Coverage: Working with a Broker



Questions?



Heather Howell Wright
Partner

Nashville, TN
hwright@Bradley.com
615.252.2342



Andrew Tuggle
Associate

Huntsville, AL
atuggle@Bradley.com
256.517.5107

These materials were developed by attorneys from Bradley Arant Boult Cummings LLP for informational purposes for members of the Huntsville Madison County Chamber. It is not possible to include discussion of every relevant issue. Thus, this information must be understood as a tool, rather than as an exhaustive statement of the law or as legal advice. Regulations change over time, so stay apprised of developments from official channels of communication.