Cooley

"OK, So GDPR Is Out Of The Way…Now What?"

Kristin Grimes, Leidos
Michael Miller, FBI
Randy V. Sabett, Cooley LLP

Presented at the
ACC National Capital Region
Cybersecurity & Privacy Year-In-Review
for 2018

leidos

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

January 9, 2019

Prelim stuff

Our lawyers made us do this…

Cooley

Disclaimer

- The views expressed during today's session are those of the speakers and do not necessarily reflect the positions of any current or former clients or customers of the respective speakers…and nothing we discuss today constitutes legal advice. For any specific questions, seek the independent advice of your attorney, query the cloud, check the "Interwebs", or ask your social network. Furthermore, Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet…

Obligatory Agenda (though we love questions and have two hours, so may deviate…significantly)

- Privacy highlights 2018
- Law enforcement update
- Cybersecurity highlights 2018
- Notable legislative and case law developments

PRIVACY HIGHLIGHTS 2018

Cooley

Privacy highlights 2018

- General Data Protection Regulation (GDPR)
- Privacy Shield
- California Consumer Protection Act (CCPA)
- Privacy and security by design – case studies

“OK, so it’s not REALLY out of the way…”

G-Day….May 25, 2018

Cooley

What is GDPR? (just a quick level set)

- EU law governing collection, use, disclosure, and security of “Personal Data:”
  - Employee Data
  - Consumer Data
  - Patient Data
  - Business Partner Data
- Personal Data – any information that can identify an individual
  - Know who the individual is
  - Track an individual
  - Allow someone to display an ad to or communicate with the individual
  - Identify or track a connected device an individual uses
- Applicability/Jurisdiction
  - Companies in the EU/EEA
  - Companies offering goods/services to EU
  - Companies that track/monitor EU residents
- Consequences
  - Harmonized, robust enforcement of data protection law in Europe
  - Authority to impose fines of up to 4% of global turnover or €20M
- Opportunity
  - Companies that comply can secure right to leverage data (consumer, analytics, etc.)
  - B2B players can use compliance as a marketing advantage (SaaS providers, HR tech providers, fintech, telemedicine, etc.)

Key Corporate GDPR Issues in 2018

- General corporate issues:
  - GDPR compliance critical to successful M&A/IPO; due diligence
  - Noncompliance may compromise business; compliance could mean starting over
  - In B2B, compliance can be a sales advantage
  - Becoming a significant issue for boards of directors

…and let's not forget Privacy Shield

- **Data Handling**
  - ✓ Must be technically and operationally compliant
  - ✓ Fairly and lawfully
  - ✓ For the specified, explicit and legitimate purposes
- **Data Collection**
  - ✓ Adequate, relevant and not excessive
  - ✓ Accurate and kept up to date
  - ✓ Not kept for longer than necessary

- **Privacy Policy**
  - ✓ Privacy Shield Principles
  - ✓ State Privacy Shield-compliant
  - ✓ Clearly explain how personal data is used
  - ✓ Link to the Privacy Shield website
  - ✓ Link to dispute resolution provider
- **Verification and P.O.C**
  - ✓ Verify compliance Internally OR Externally
  - ✓ Must designate a point of contact for questions, complaints, access requests etc.
  - ✓ Can be the officer certifying compliance or another official –e.g. Privacy Officer

Privacy Shield Update – 2018

- **Summer 2018**: EU Parliament recommended (non-binding) suspension of Privacy Shield pending GDPR compliance updates and other efforts in U.S. to ensure adequate protections
- FTC made renewal of Privacy Shield a main priority and increased enforcement actions, including settling claims against four companies for misrepresenting their compliance
- **December 19, 2018**: results of the second annual review released
  - U.S. continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the EU to participating companies in the U.S.
  - Steps taken by the U.S. authorities to implement the recommendations made by the Commission in last year's report have improved the functioning of the framework.
  - Requires "permanent Ombudsperson by 28 Feb 2019 to replace the one that is currently acting"
  - Concerns expressed re (a) "Facebook/Cambridge Analytica case and other revelations," (b) various limitations of the US legal framework leading to plans by the Commission plans to "closely monitor" or "closely follow" several points to see if future action is required

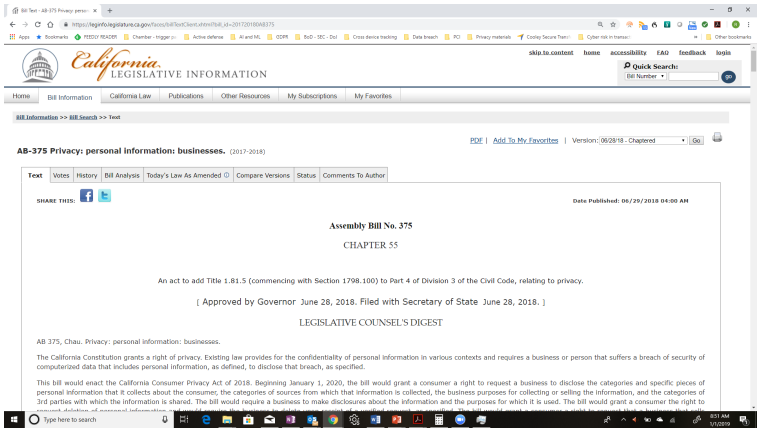
“If you build it, they will come…”

The California Consumer Privacy Act (CCPA)

Cooley

California Consumer Privacy Act (CCPA)

- Unanimously approved by CA legislature and signed into law on June 27, 2018
- Rushed through legislative process to avoid a more stringent privacy law planned for California's November 2018 ballot
- "Technical amendments" (SB 1121) enacted on September 23, 2018 and more amendments possible
- ~10,000 words with drafting errors
- CA AG to issue regulations



How will CCPA affect businesses?

- Global impact
- Estimated 500,000 U.S. businesses affected per IAPP
- Threat to ad-supported free services and data brokerage?
- California-specific websites/products may emerge
- Increased compliance costs (especially processing access/deletion/opt out requests)
- Increased potential liability and class action litigation
- Spurring push for preemptive federal legislation

- Key dates:
  - **January 1, 2020**
    - CCPA takes effect
    - Private right of action for security breaches
  - **July 1, 2020**
    - Deadline for CA AG to adopt regulations
  - **Earlier of 6 months after final regulations or July 1, 2020**
    - CA AG may bring enforcement action

Who must comply with CCPA?

- For-profit “businesses” that collect Personal Information (“**PI**”) of California residents and households, and
  - Have annual gross revenues more than $25 million;
  - Obtain PI of 50,000 or more California residents, households or devices; or
  - Derive 50% or more annual revenue from “selling”California residents’ PI.
- A covered business’s affiliates that use the same branding, even if those affiliates don’t surpass these thresholds themselves
- Possible exceptions for businesses that do not do business in California and whose commercial conduct takes place “wholly outside of California”

- Service Providers
  - For-profit legal entity that processes information on behalf of a business pursuant to a written contract
  - Contract must prohibit personal information use for any purpose other than for the specific purpose of performing the services specified in the contract
- Third Parties
  - Any party to which a “business” discloses PI other than a “service provider”

What data does the CCPA cover?

- *"Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or* ***household****.*

- CCPA "personal information" is broader than GDPR "personal data"
- Includes a long, non-exhaustive list of examples of PI that include everything you expect, plus some things you might not, including information about a "household" (i.e., more than one person)
- IP addresses, device IDs, cookie IDs
- Inferences drawn from personal information to create profiles
- Any other information that could reasonably be linked, directly or indirectly, with a particular consumer or household

What Must Businesses Do To Comply?

Notice & Transparency

Update privacy policy to provide required disclosures (covering prior 12 months' activity)

On homepage put Do Not Sell My Personal Information link to instructions on opting out of sale of PI

Establish a toll-free phone # that individuals can call to opt out of the sale of PI without an account

Individual Rights

Verify identities of individuals requesting to exercise rights

Honor requests to exercise rights within 45 days (+45 day extension when reasonably necessary)

Train relevant employees to assist individuals with privacy-related questions and requests

Consent

Avoid asking for opt-in consent to sell PI for 12 months after opt out

Obtain affirmative consent to sell PI of minors 13-16

Obtain parental consent to sell PI of minors under 13

What Should You Be Doing Now?

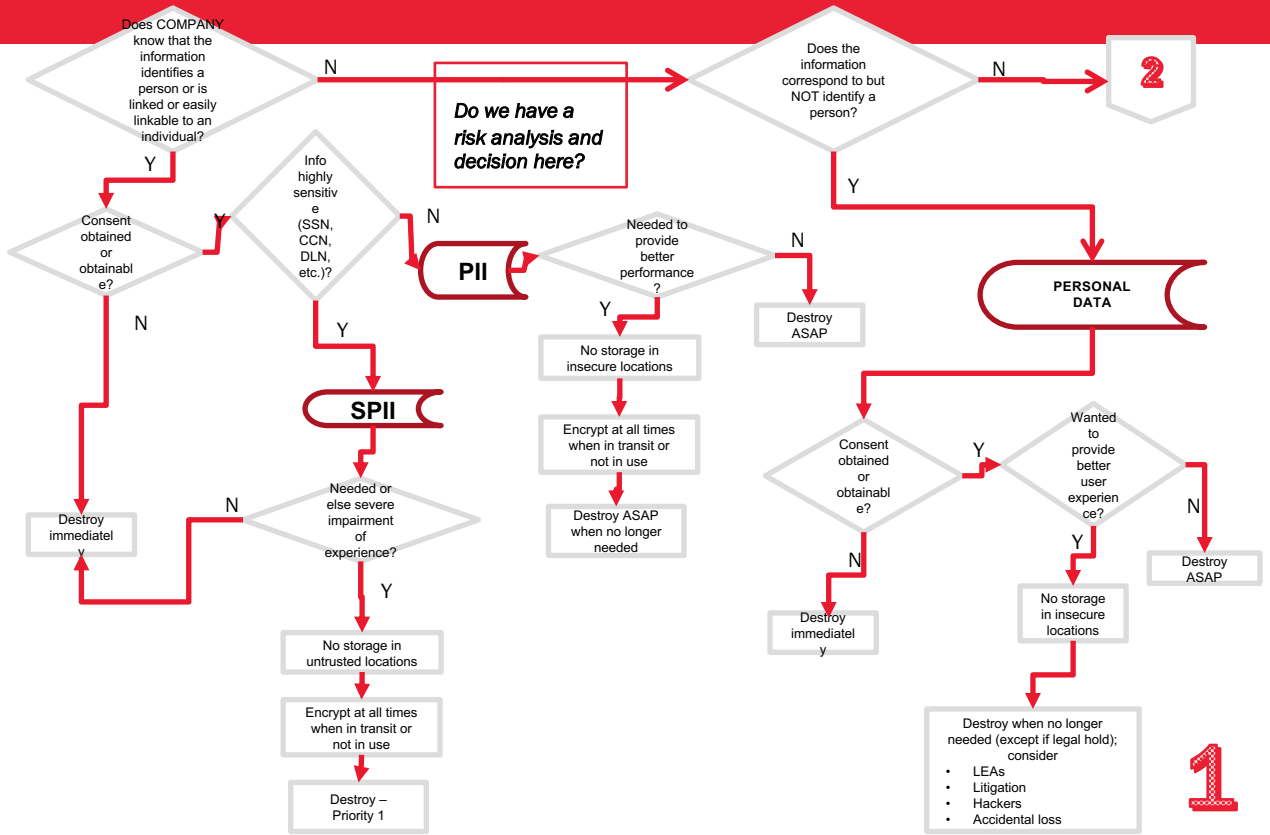
Year	Actions
2018	• Get started – deadline will come fast • Understand requirements • Consider CCPA in risk factor disclosures (e.g., in public filings) • Consider CCPA risk/issues in strategic transactions (e.g., M&A, financings) • Identify CCPA compliance resources and kick-off CCPA compliance projects
2019	• Gap assess, prioritize efforts and execute remediation plan • Monitor amendment activity and AG rulemaking; consider rulemaking participation • Build technical capabilities to honor access, deletion, opt out and other rights • Prepare privacy policy and other externally-facing updates for New Year's release
2020	• **January 1, 2020:** CCPA takes effect • **July 1, 2020:** Deadline for final regulations • **July 1, 2020** (or 6 months after final regs if earlier): AG may bring enforcement action >>Ongoing remediation<<

“It’s all about the data, Marty…”

Privacy and Security by Design

Cooley

Privacy and Security By Design



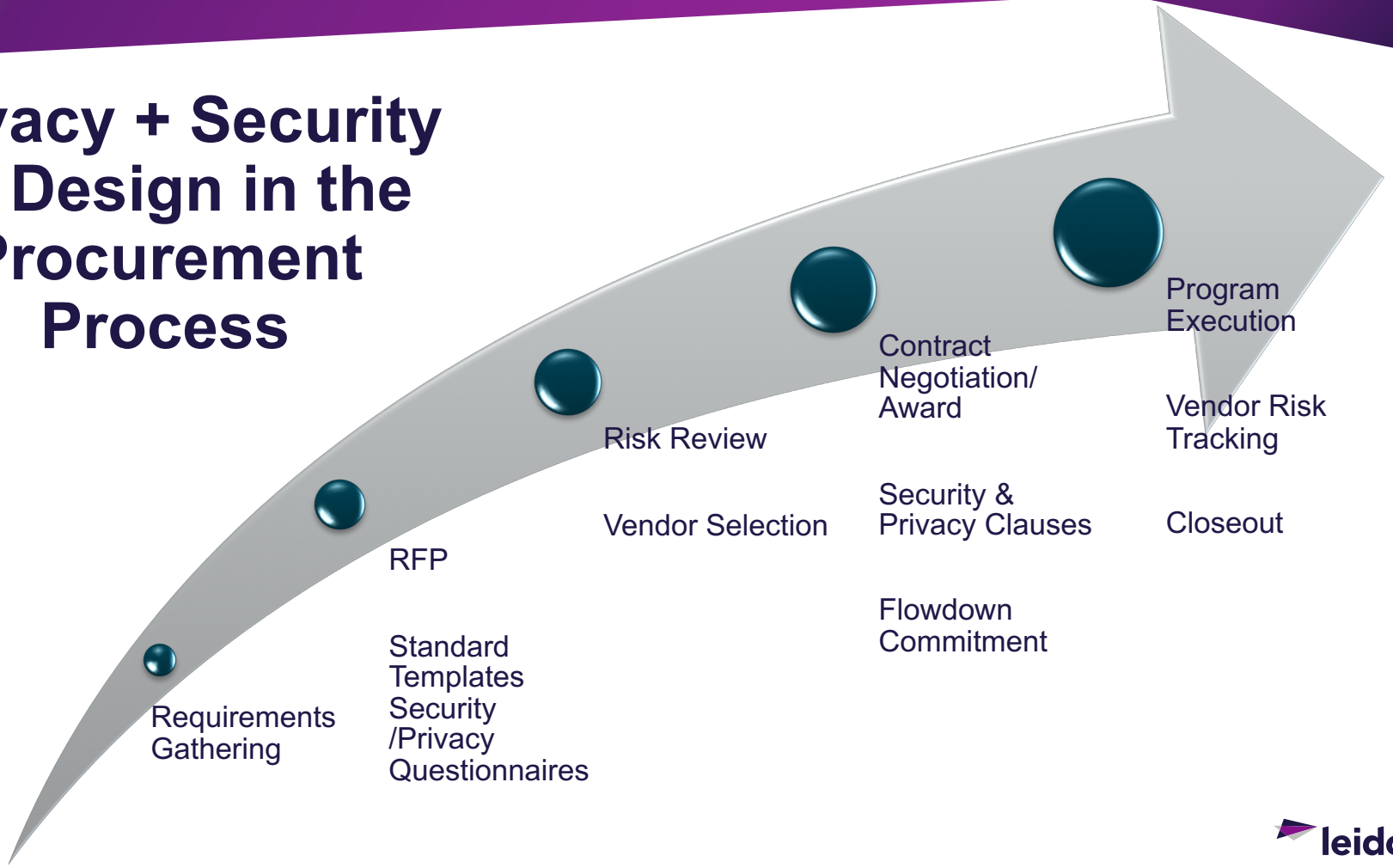
- Example of a simplified privacy by design decision tree
- Two other pages of similar content
- Collaboration between attorneys and design engineers

Defense Contracting

Requires risk-based assessments and diligence at multiple levels

leidos

Privacy + Security by Design in the Procurement Process



leidos

Tracking the Data

- Need to know where the data is
  - Data mapping key for timely incident response
- Need to know where data flows
  - Within organization
  - To subs/suppliers/vendors
  - To the cloud
- Contractual terms in place with business partners for minimum security and reporting requirements
- If compartmentalizing crown jewels, better air gap!

LAW ENFORCEMENT UPDATE
2018

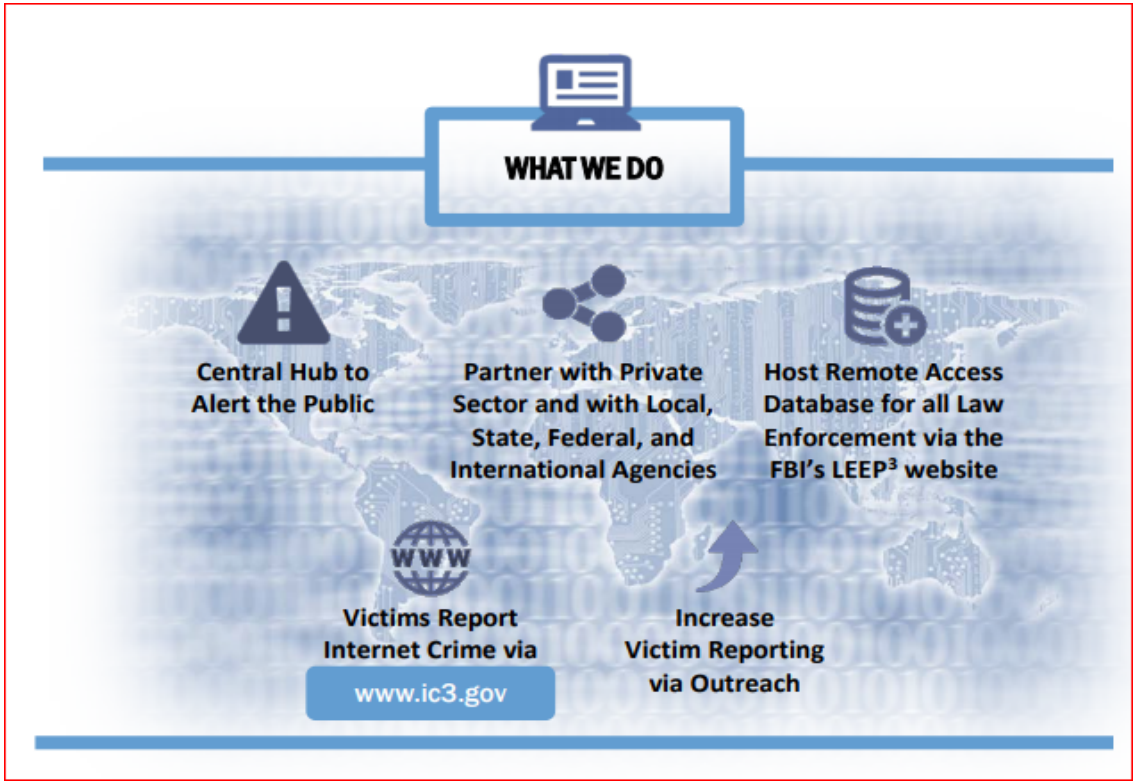
Cooley

Business E-mail Compromise (BEC)

- Sophisticated scam targeting businesses that often work with foreign suppliers and/or businesses that regularly perform wire transfer payments
- Criminals will often impersonate C-suite executives and contact the company's finance department to request immediate wire transfers
- Often carried out through spear-phishing campaign and execution of malware
- If undetected, an intruder may remain in the system for weeks or months studying organization's vendors, billing mechanisms, and the executive's style of communication
- In 2017, the FBI received 15,690 BEC complaints with losses in excess of $675 million

Internet Crime Complaint Center (IC3)

- Established by the FBI in May 2000
- Centralized point for businesses and consumers to submit complaints pertaining to internet-related crime
- Since inception, more than 4 million complaints submitted with losses in excess of $5.52 billion



Internet Crime Complaint Center (IC3)

www.ic3.gov

Interacting with Law Enforcement

- The FBI maintains 56 field offices throughout the United States and more than 75 offices in strategic locations throughout the globe
- Contact local FBI field office and/or IC3 (www.ic3.gov)
- Law enforcement requests for information, what will you provide?
- Who will be law enforcement's point of contact?
- Who will handle notifications to stakeholders, if necessary?

“There is no such thing as perfect security, only varying levels of insecurity.”

- Salman Rushdie

Cybersecurity highlights 2018

- Governance and tone from the top
- Hardware vulnerabilities
- Supply chain issues
- The breaches continue…
- Increasing attention to offensive cyber

Some stats from 2018

- U.S. is #1 target of targeted attacks at 38% (India is #2 at 17% and Japan is #3 at 11%) [Symantec]
- 65% of malicious attacks target small and medium sized businesses according to a recent survey [Kesler]
- Over past 5 years, an average of 3.8M records per day have been stolen in breaches [Cyber Ventures]
- 200B connected devices by 2020 [Symantec]
- Three stats from the 2018 Ponemon Institute/IBM breach study:
  - **Cost of the average data breach to companies worldwide**: $3.86 million (U.S. dollars)
  - **Cost of the average data breach to a U.S. company**: $7.91 million (U.S. dollars)
  - **Average time it takes to identify a data breach**: 196 days

Tone From The Top

What does privacy and security governance and maturity look like in 2018?

Cooley

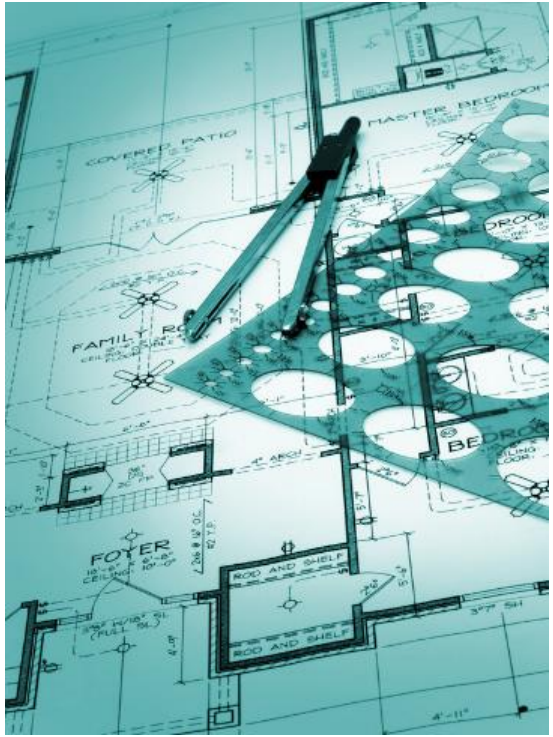
Importance of a Governance Model in 2018

- Establish a Governance Framework
  - "Board"-like oversight
  - CIO/CISO/CPO/CCO/IT involvement
  - Certifications (corporate and individual)
- Information Sharing/Threat Intelligence/External Involvement
- Board Participation
- Tools (for exercising governance model)

> "[A] leadership-driven, business-focused approach to cyber governance is essential to creating robust, sustainable, cyber security."
>
> - Forbes, February 2018

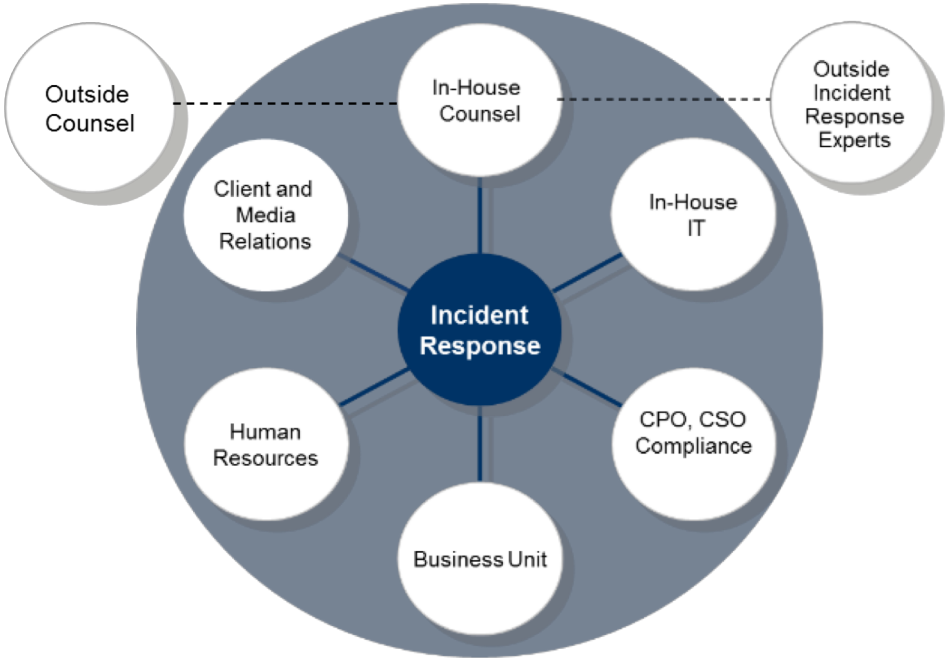
Tool - Incident Response Plan

- Management endorsement
- Cross-disciplinary team
- Contact lists
- Legal analysis and timeline
- Categories of adverse events
- Escalation process
- Communications plan



Tool - Information Security Tiger Team

- OK, so it's not an original name…but the idea makes sense
- Distinctly identified, cross functional team of professionals
- Responsible for recommending and implementing reasonable security practices



Tool – Table Top Exercise (TTX)

- Goal: Identify issues to be resolved and best practices to incorporate into response plans.
- Example TTX:
  - Consider existing response plans, policies and procedures for:
    - a cyber attack incident;
    - supporting and identifying actions required to meet immediate needs during a cyber attack incident;
    - prioritizing the repair or replacement of CI; and
    - supporting recovery operations
  - Evaluate coordination efforts (SOPs, communications and decision support mechanisms) and incident response; and

Governance Structure Implementation

- Create a privacy and security governance structure, then use that governance structure to:
  - Research Threats
  - Prioritize Information Assets
  - Perform a Privacy Impact Assessment
  - Perform a Risk Analysis and Cyber Assessment
  - Create a Security Protection Plan Tied to a Technology Acquisition Strategy
  - Engage Third Parties Appropriately (legal, technical, procedural)
  - Request Regular Updates and Adjust Accordingly
  - Test the Response Plan
  - Maintain Appropriate Insurance Coverage
  - Provide Regular Privacy and Security Training for Employees, Vendors, and Other Third Parties

Happy New Year!!

Spectre/Meltdown (1/2/2018), Rice Kernals, and a variety of other assorted vulnerabilities and breaches…

Cooley

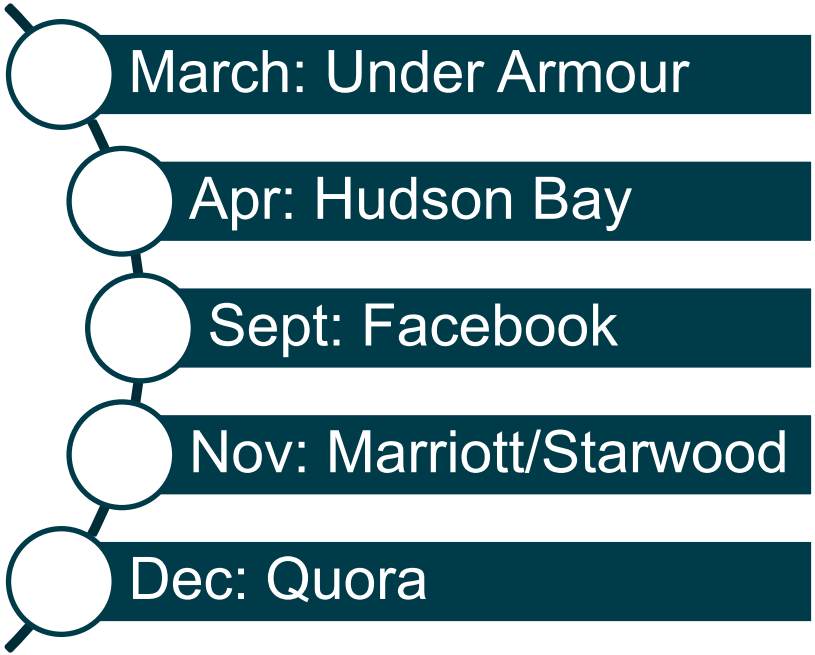
Spectre and Meltdown

- **Spectre** and **Meltdown** exploit what is known as the “speculative execution feature” that exists in most processors today, allowing user-level programs to access sensitive memory using processor caches as covert side channels
- Possible results of exploitation:
  - Could allow random access to the entire processor memory-space
  - Works across VMs
  - Attacks from one user to another user possible
  - Leaking code module addresses in user space is possible (which could lead to remote code execution on the affected machine)
  - Disclosure of sensitive information and privilege escalation attacks, because accessed memory may contain password hashes, private keys, etc.

Supply Chain Issues

- For years, some nation states accused of supply chain compromise
- On October 4, Bloomberg story appeared re rogue chips on boards
  - Apple, Amazon, and other issued strong denials
  - Stock of board supplier Supermicro dropped over 40%
- Investigation ensued
- On December 11, Supermicro issued letter saying third party investigation had concluded no rogue chips on boards
- DoD-commissioned “Deliver Uncompromised” report

A Year of Breaches



Underlines the need for:

IT Security + Physical Security + Privacy + Legal + HR + Comms

One, coordinated incident response plan

Practice breach response!

leidos

Defining “Breach”

- Depending on the law or regulation, reporting duties vary widely
- Data breach vs. personal data breach
- Defense contractors are subject to very strict reporting requirements under DFARS
- Proposed NY SHIELD law – breach shall mean unauthorized access to OR acquisition of (do not need both)
- Many states require both, so arguably a ransomware attack would not be reportable if no acquisition

Reporting Required under the DFARS when:

Compromise

of an information system and/or the information residing therein

OR

Actual or Potentially Adverse Effect

on an information system and/or the information residing therein

AND

IMPLICATES

Covered Contractor Information System

OR

Covered Defense Information

leidos

"It is unfortunate when men…are restrained in the means which are necessary to avert [danger at a distance]. Not less difficult is it to make them believe, that offensive operations, often times, is the surest, if not the only (in some cases) means of defence."

- George Washington, 1799

Active defense, offensive cyber operations, etc.

Cooley

Offensive Cyber / Active Defense / ~~"Hack Back"~~

- Offensive cyber developments by governments and what it means for public and private sector entities
  - NATO: "NATO is clear that we will not perform offensive cyberspace operations. However, we will integrate sovereign cyberspace effects from the allies who are willing to volunteer."

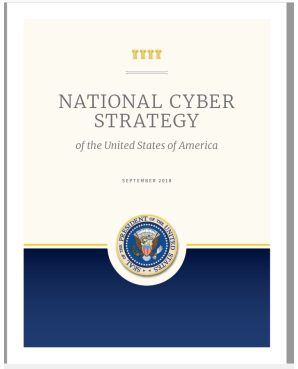
    - Maj. Gen. Renner, head of the NATO Cyber Operations Center, at a conference in November 2018

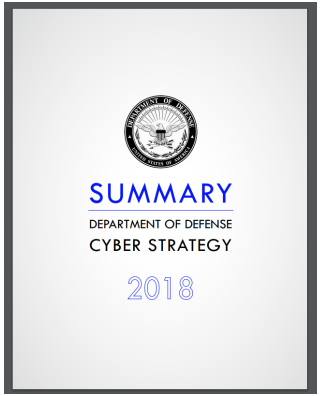
  - The Netherlands MoD will invest (more) in offensive capabilities, among others for the purpose of attribution
  - U.S. made a number of policy changes in 2018

U.S. National Cyber Strategy

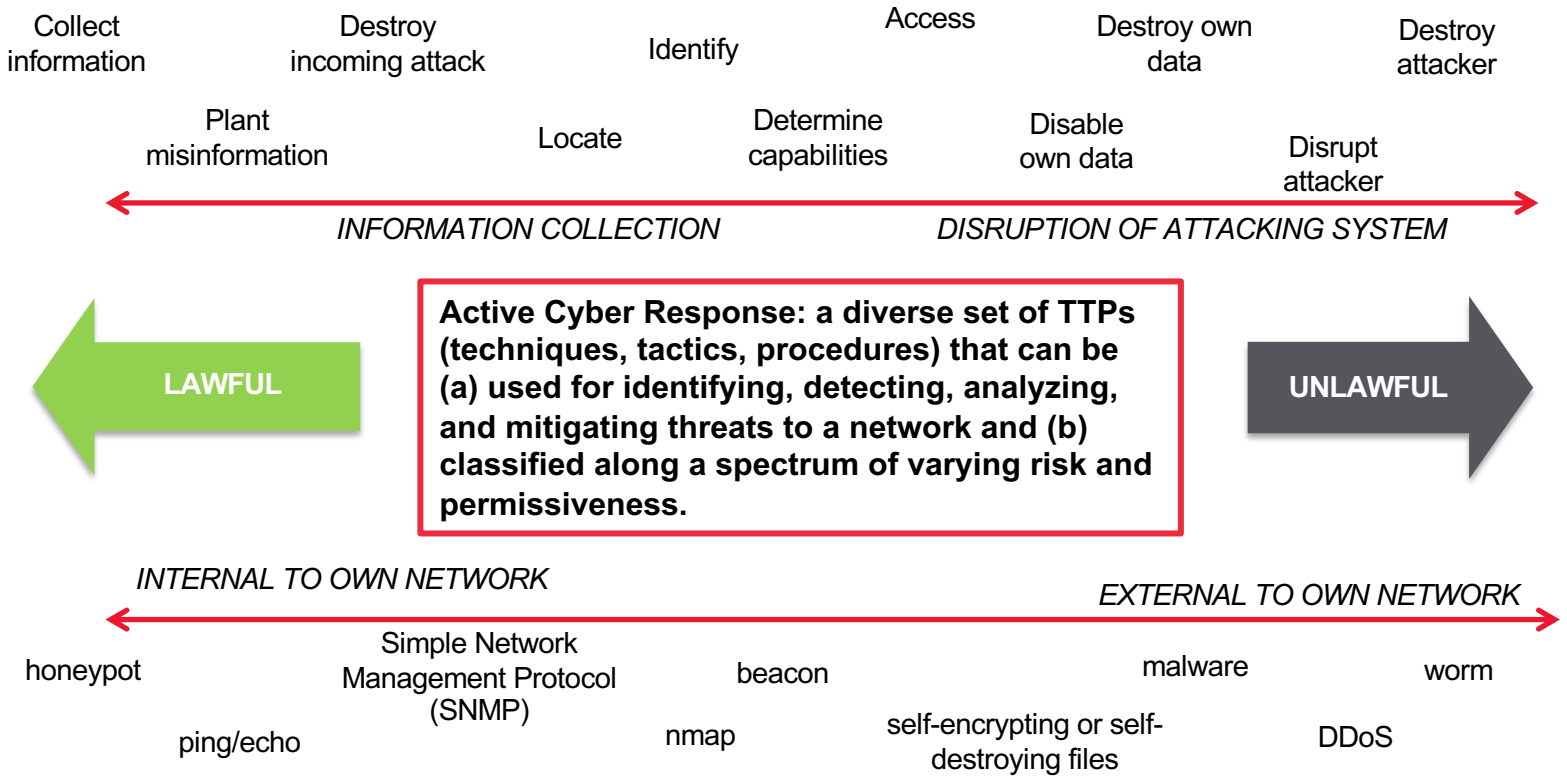
- September 2018: DoD releases public version and summary of a classified cyber strategy
- First update since 2015
- Significant policy shift by the U.S. Government
  - "[W]e must also work to ensure that there are consequences for irresponsible behavior that harms the United States and our partners. **All instruments of national power are available** to prevent, respond to, and deter malicious cyber activity against the United States."
  - "We will defend forward to disrupt or halt malicious cyber activity at its source, **including activity that falls below the level of armed conflict**."
- "Failing to articulate a clear set of expectations about when and where we will respond to cyber attacks is not just bad policy, it's downright dangerous."

  - Sen. Mark Warner (December 2018)





An Active Cyber Defense Spectrum



Observations entering 2019

- Fundamentally, active defense is NOT a bad thing…but a broad policy dialog is definitely needed
- Significant amount of hyperbole and overgeneralization about active defense; be careful!
- It's NOT hacking back
- Reasonable steps may be possible without "attacking" the other party
- Very careful consideration is needed (including discussions between the tech/cyber and legal teams and, potentially, discussions with law enforcement) before undertaking any kinds of activities like these

"Security against defeat implies defensive tactics; ability to defeat the enemy means taking the offensive."

- Sun Tzu, The Art of War [4:5]

“The United States is a nation of laws; badly written and randomly enforced.”

- Frank Zappa

Notable legislative and case law developments

Cooley

Legislative Update

- Clarifying Lawful Overseas Use of Data (CLOUD) Act
  - Enacted on March 23, 2018
  - Orders by U.S. law enforcement officers under the Stored Communications Act can be used to acquire data in other countries
  - New bilateral agreements with certain foreign countries
  - Service providers must plan accordingly since data stored outside the U.S. may now be subject to requests under the SCA
- EU Directive on Security of Network and Information Systems (NIS)
  - Entered into force in July 2016 and was to be transposed by May 2018
  - Intended to improve overall EU cybersecurity
  - Includes a CSIRT, cooperation group, NIS toolkit, and cyber incident reporting
  - Related effort by U.S. Chamber of Commerce

Healthcare Voluntary Guidance (but could influence legislation…)

- HHS released voluntary healthcare cyber practice guide on December 28, 2018
  - Cybersecurity Act of 2015 contained a mandate to develop healthcare cybersecurity standards
  - HHS worked with over 150 experts to develop the guidelines which set forth "common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes"
  - Covers:
    - Threats to healthcare industry
    - Current weaknesses that create vulnerabilities
    - Techniques to be used by healthcare stakeholders to defend against threats
  - Contains five threats and ten practices for mitigation

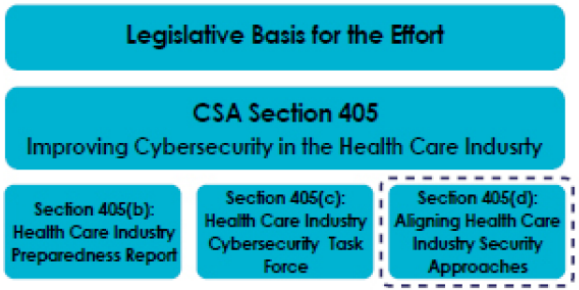


Figure 1. Section 405(d) is Part of CSA Section 405, Which Focuses on the U.S. Health Care Industry

Legislative/Regulatory Landscape

- H.R.4036 - Active Cyber Defense Certainty Act
- Ohio Data Protection Act
- EU Cybersecurity Act
- CISA Act (November 2018)
- Foreign Investment Risk Review Modernization Act of 2018

Federal data breach legislation

leidos

Legislative/Regulatory Landscape (cont'd)

- Colorado: "Protections for Consumer Data Privacy" law
  - became effective Sep. 1, 2018
  - requires companies to develop and have plans in place for securing and disposing of personal data on Colorado residents
- Vermont: new data privacy law focuses on data brokers
  - ***Transparency.*** During annual registration must disclose whether consumers may opt-out of data collection, retention, or sale (effective 1/1/19)
  - ***Duty to secure data***. Must adopt data security programs with administrative, technical, and physical safeguards (effective 1/1/19)
  - ***No fraudulent collection***. No collection of personal information by fraudulent means, or for purposes of harassment or discrimination.
  - ***Free credit freezes***. Bars credit agencies from charging consumers fees for credit freezes.

Cyber Insurance Issues in Case Law

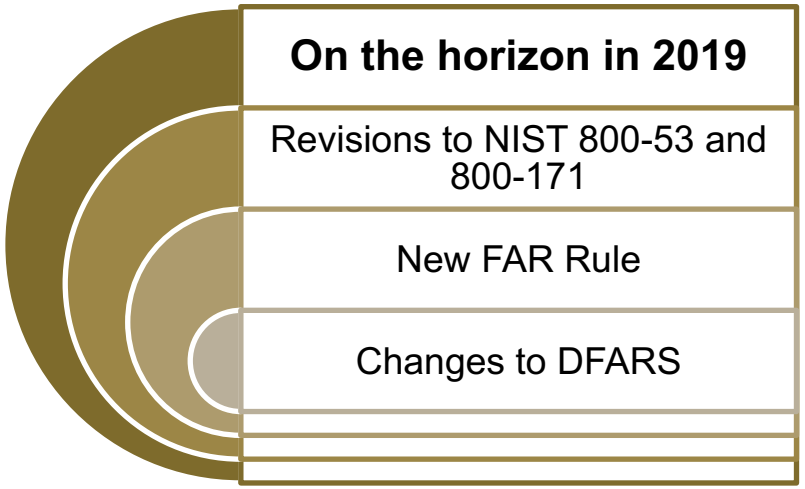
- Exclusion for “hostile or war like act” by any “government or sovereign power”
  - Mondelez claim to Zurich in aftermath of NotPetya attack, which was widely attributed to Russia
  - Zurich asserting the exclusion; Mondelez suing Zurich
  - Highlights the importance of understanding cyber coverage, especially where state-sponsored actors could be the source of an attack
- Cyberinsurance computer fraud policies
  - Most cover indirect or direct loss of property due to the fraudulent transfer of property by a third party
  - Some circuits have ruled that these policies do not cover situations where an authorized employee is tricked via phishing to transfer funds to a malicious or criminal actor
  - May want to consider additional specific insurance policy addressing phishing scams

Biometrics in Case Law

- Illinois' Biometric Information Privacy Act (2008) first state law to regulate the collection of biometric information
  - Only law that allows private individuals to sue for damages
- *Rivera, et al. v. Google, Inc.* – Plaintiffs alleged Google unlawfully collected, stored, and exploited their face-geometry scans via cloud-based Google Photos
- U.S. District Court judge ruled that plaintiffs "have not suffered an injury sufficient to establish Article III standing" and dismissed claims
  - Retention of an individual's private information, on its own, is not a concrete injury sufficient to establish standing
  - No unauthorized access to accounts or data associated with face templates
  - Hackers had not obtained their data
- Many employers use biometric data – keep an eye on this space to see how laws play out for individual action concerning misuse of such data

DFARS 252.204-7012: One Year Later, Many Challenges

- Lack of marking
- Overlapping authorities
- Overlapping audits
- Constantly evolving guidance
- Enhanced standards & new CDRLs
- Difficulties in flowing down



leidos

Insider Threat

Malicious & Unintentional

Insider threats often both enabled and detected by cyber means

Top Deterrence Methods:

- Data Loss Prevention (DLP) (60%)
- Encryption of Data (60%)
- Identity & Access Management (56%)
- Endpoint & Mobile Security (50%)

Top Detection Methods:

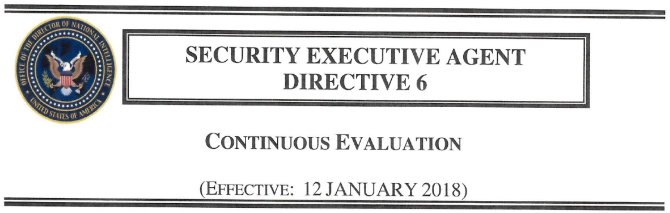
- Intrusion Detection & Prevention (63%)
- Log Management (62%)
- Security Information & Event Management (SIEM) (51%)

[Cybersecurity Insiders 2018 study]

leidos

Insider Threat: Government Actions

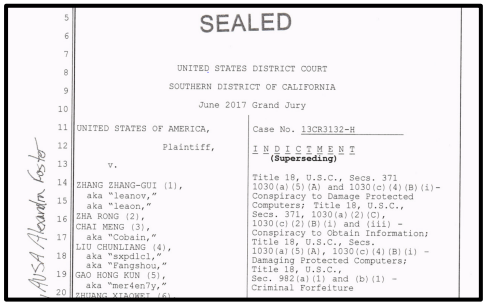
- Jan. 2018 ODNI issued Security Executive Agent Directive (SEAD) 6, which strengthened requirements for Continuous Evaluation of cleared personnel
- DoD already implemented its CE program to include DoD contractors
- DOJ indictments for insider- and cyber-enabled economic espionage
- Creation of “China Initiative”



SECURITY EXECUTIVE AGENT DIRECTIVE 6

CONTINUOUS EVALUATION

(EFFECTIVE: 12 JANUARY 2018)



SEALED

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

June 2017 Grand Jury

UNITED STATES OF AMERICA, Plaintiff, v.

ZHANG ZHANG-GUI (1), aka "leanov," aka "leaon," ZHA RONG (2), CHAI MENG (3), aka "Cobain," LIU CHUNLIANG (4), aka "expdlcl," aka "Fangshou," GAO HONG KUN (5), aka "meraen7y," ZHUANG XIAOWEI (6),

Case No. 13CR3132-H

INDICTMENT (Superseding)

Title 18, U.S.C., Secs. 371 1030(a)(5)(A) and 1030(c)(4)(B)(i)- Conspiracy to Damage Protected Computers; Title 18, U.S.C., Secs. 371, 1030(a)(2)(C), 1030(c)(2)(B)(i) and (iii) - Conspiracy to Obtain Information; Title 18, U.S.C., Secs. 1030(a)(5)(A), 1030(c)(4)(B)(i) - Damaging Protected Computers; Title 18, U.S.C., Sec. 982(a)(1) and (b)(1) - Criminal Forfeiture

leidos

WRAP UP

Cooley

Predictions for 2019

- Federal Cyber and Privacy Law
- Expanding 5G deployment and vulnerabilities
- More IoT-enabled attacks
- Compliance no longer equals security; more will be required
- Increased industry association involvement to coordinate cyber activities
- Intersection of AI and privacy/cyber will continue to grow

Other questions?

- Let us know if you have any questions or reach out to us afterwards if you want to discuss things further
- Thank you for your attention and best wishes for 2019!

Bios

Contact info on your speakers

Cooley

About the Speakers

Kristin M. Grimes * kristin.m.grimes@leidos.com * 571.526.6326

Ms. Grimes is corporate counsel at Leidos, specializing in cyber issues from the program to enterprise level and throughout the Leidos supply chain. She advises stakeholders on data protection best practices, incident response, and all aspects of cyber regulatory compliance. Ms. Grimes is also responsible for industrial security, insider threat mitigation, and domestic and international investigations, including privacy implications. Prior to joining the legal department, Ms. Grimes spent ten years with SAIC/Leidos working operational and strategic counterintelligence, counterterrorism, and cyber issues for the U.S. Intelligence Community. Ms. Grimes is the founder of the Leidos Pro Bono Program and is a Vice Chair for the American Bar Association Public Contract Law Cybersecurity, Privacy, and Data Protection Committee.

Michael Miller * mbmiller@fbi.gov

Mr. Miller is a special agent at the Federal Bureau of Investigation (FBI) and is currently assigned to investigate cyber intrusion incidents. He has more than 10 years of investigative law enforcement experience and has primarily investigated cyber-related incidents throughout his career. Prior to his FBI career, Mr. Miller served as a state special agent investigating criminal cyber matters and conducting mobile device forensic examinations. He also instructs law enforcement investigators regarding cyber investigations and often presents on cyber incident response procedures for public and private sector entities. He holds a Master of Science degree in Cybersecurity and a Master of Public Administration degree.

Randy V. Sabett, J.D., CISSP * rsabett@cooley.com * 202.728.7090

Mr. Sabett is a former NSA crypto engineer, who focuses at Cooley LLP on cybersecurity, privacy, licensing, and IP. Mr. Sabett has managed numerous data breach responses, involving major retailers, financial and health care organizations, and on-line service providers. He served on the Commission on Cybersecurity for the 44th Presidency and the NSTAC Cyber Moonshot project. Mr. Sabett is a member of the Boards of Directors for the Georgetown Cybersecurity Law Institute, a frequent lecturer and author, and has appeared on or been quoted in a variety of national media sources.

Cooley

"OK, So GDPR Is Out Of The Way…Now What?"

Kristin Grimes, Leidos
Michael Miller, FBI
Randy V. Sabett, Cooley LLP

Presented at the
ACC National Capital Region
Cybersecurity & Privacy Year-In-Review
for 2018

leidos

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

January 9, 2019