Breached!

Procurement In[cyber]security
Presenters

John Adler, CPPO, Dallas Area Rapid Transit
Dr. Rosemarie Pelletier, DPA, Norwich University
Jan Siderius, Negometrix
Task Force Members

John Adler, Rosemarie Pelletier, and Jan Siderius, are members of the Task Force that created the global best practice on Cybersecurity for Procurement. Task force members also include:

Abhijit Verekar    Tayler Hampton
Johnnie Terry      Robert Cato
Peter Miller
Objectives

1. How to Develop Contracts to Secure the Supply Chain
2. How to Protect Your University
3. How to Address Contact Tracing: Privacy, Cyber Security, and Health Care
Objective 1

Cybersecurity Risks in Contracts: How to Develop Contracts to Secure the Supply Chain
NASA Contractor Hacked

- DopplePaymer ransomware gang hacks Digital Management LLC.
- Digital Management LLC is a NASA Contractor.
- 20 archive files posted on dark web, including HR docs and project plans.
- NASA Spokesperson Sean Potter:
  - “NASA is aware of the report and coordinated appropriately with law enforcement and NASA’s procurement office.”
  - “As of April 2019, the company...is no longer performing any contractual services for NASA.”
Government Contractors Hacked

- 2020 – Netsential hacked exposing thousands of police records, and officer contact information
- 2019 – Miracle Systems hacked gaining access to 20 federal agencies, including Homeland Security
- 2019 – Perceptics hacked exposing Customs and Border Patrol data on dark web
- 2018 - PPI for 30,000 Pentagon employees exposed through Booz Allen subcontractor in 2018
- 2018 – Chinese hackers steal “massive amounts” of undersea warfare data through US Navy contractor
- 2007 - F-35 fighter plans stolen from Australian subcontractor
Contractors at Risk

- IT contractors
- Software applications
- Cloud services
- Staff augmentation
- HR and payroll services
- Background investigations
- Employee benefits
- CCTV systems and services
- Dash-cams and body-cams

- Environmental systems
- Railroad SCADA and PTC
- Building maintenance and security
- Consulting services
- Banking and payment services
- Backup data center
- Social services contractors
- Transportation services
- Call center and help desk
Risk Prevention and Mitigation

- Risk assessment
- Collaborate with IT and cybersecurity professionals
- Supplier onboarding
  - Minimum qualifications
  - Evaluation factors
- Performance standards and certification
- IT service policies and standards
- Cybersecurity insurance
- Onshore storage and transmission of data
- Key personnel background checks
- Audit rights
- Incident reporting requirement
- Application and source code security audit
- Prior approval and vetting of subcontractors
- Secure coding practices
- Encryption of cloud data
- PII protection
- HIPAA compliance
- Non-disclosure
Certifications and Standards

- NIST-800-122 - Personally Identifiable Information (PII)
- HIPAA – Health Insurance Portability Act of 1996
- ISO 27001 – Information Security Management System
- ISAE 3000/SAE2 – Independent Audit
- FISMA and FedRAMP – Federal security controls and risk assessment
- NIST SP 800-53 – DOD standards
- GDPR – Europe General Data Protection Regulation
“If you put a key under the mat for the cops, a burglar can find it too. Criminals are using every technology tool at their disposal to hack into people’s accounts. If they know there’s a key hidden somewhere, they won’t stop until they find it.”

Tim Cook
Apple CEO
Panel Discussion
Objective 2

How to Protect Your University
University of California San Francisco (UCSF) falls prey to supplier-imposter email scam followed payments to fraudster.
What happened?

1. Similar Internet domain name

2. Credibility: Use of names of senior staff, CFO

3. Similar email account:
   gary.smith@smith-construction.com
   garysmith@smithconstruction.com

4. Requested change to bank account information

5. Payment diverted
Panel Discussion

What could Procurement have done to avoid this fraud?
What actions did the UCSF take?

University leadership created a task force that has expertise in Audit, Supply Chain Management, Accounts Payable, Information Technology, and Finance. Reported to Chief Procurement Officer and the Controller.
Task force’s 3 objectives:

1. Strengthen key controls.

2. Improve business processes.

3. Identify a system for workflow approval to reduce the manual effort of supplier data entry Supplier Registration Software.
Recommendation from UCSF

• Act immediately, initial actions are vital.

• Obtain as much information as possible. Begins with transparency about incident.

• Fraud investigation must be conducted confidentially.

• Assign to senior, trusted individual who works directly with the appropriate authorities. Details may contain essential clues that help in the fraud investigation.

• File initial report (and updates) with the police department.

• Contact bank immediately to request a recall of funds.

• Insurance Claim Submission; A well-organized packet can result in faster claims processing.

• Raise awareness; Fraud prevention training is offered to all employees at UCSF.
Thanks to: Vanessa Wong serves as the Executive Director of Procurement and Solutions in Supply Chain Management at the University of California San Francisco (UCSF), providing strategic leadership programs in e-Commerce, procurement card.
Discussion
Objective 3

Contact Tracing Apps: How to Address Contact Tracing: Privacy, Cyber Security, and Health Care
“The lure of automating the painstaking process of contact tracing is apparent. But to date, no one has demonstrated that it’s possible to do so reliably despite numerous concurrent attempts. Apps that notify participants of disclosure could, on the margins and in the right conditions, help direct testing resources to those at higher risk. Anything else strikes us as implausible at best, and dangerous at worst.”

Bruce Schneier
BuzzFeed News
https://www.buzzfeednews.com/article/carolinehaskins1/coronavirus-contact-tracing-google-apple
“My problem with contact tracing apps is that they have absolutely no value. I’m not even talking about the privacy concerns, I mean the efficacy. Does anybody think this will do something useful? … This is just something governments want to do for the hell of it. To me, it’s just techies doing techie things because they don’t know what else to do.”

Bruce Schneier
BuzzFeed News
https://www.buzzfeednews.com/article/carolinehaskins1/coronavirus-contact-tracing-google-apple
Contact Tracing App will have issues
False Positives: A precise definition of a contact, while defined in software, does not take into account environmental circumstances, such as walls. The location capabilities of the devices is not accurate enough.

Bruce Schneier
Schneier on Security
https://www.schneier.com/blog/archives/2020/05/me_on_covid-19_.html
Malicious Use of Apps

“Imagine an unscrupulous political operative who wanted to dampen voting participation in a given district, or a desperate business owner who wanted to stifle competition. Either could falsely report incidences of coronavirus without much fear of repercussion. Trolls could sow chaos for the malicious pleasure of it. Protesters could trigger panic as a form of civil disobedience. A foreign intelligence operation could shut down an entire city by falsely reporting COVID-19 infections in every neighborhood. There are a great many vulnerabilities underlying this platform that have still yet to be explored.”

Contact-tracing apps are not a solution to the COVID-19 crisis
Soltani, Calo, & Bergstrom
Privacy & Security

“I am concerned about the privacy and security of apps used for contact tracing. The Apple-Google contact tracing framework exists that promotes privacy, but few apps are approved to use it. Other apps may exist that claim to do this, but we should be concerned about what is being done with our data, where it goes, who has access, and where it ‘lives’. Any app can claim to do one thing, but what else is it doing behind the scenes?”

George J. Silowash
Chief Information Security Officer, Norwich University
Panel Discussion
Thank you!

John Adler jadler@dart.org
Jan Siderius jan.siderius@negometrix.com
Rosemarie A. Pelletier r pellet2@norwich.edu