10-20-2021

Third Party Risk Management and Cyber Supply Chain Risk Management

Jerald Garner
University of Arkansas, Fayetteville

Engineering and Operations Management Lunch & Learn Webinar Series

October 20, 2021

University of Arkansas

College of Engineering & Industrial Engineering Programs

- Master of Science
  - Operations Management
  - Engineering Management
  - Engineering
- Graduate Certificates
  - Project Management
  - Lean Six Sigma
  - Homeland Security

UNIVERSITY OF ARKANSAS

Today’s Presenter

Jerald L. Garner is currently a Global Business Services Expert Risk Analyst at Walmart, Inc. He is a team leader and assessor for providing innovative solutions for the determination of potential vendor risk on 3rd party risk assessments and the identification of internal market National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) Maturity model assessments. He was a National Field Supervisor (NFS) assigned to the Office of National Examinations and Supervision (ONES). Where he provided leadership and managerial direction in developing safe and sound operational examination processes over his ten-year tenure. He has worked in the Information Systems/Cyber Security field for over 35 years as a dedicated information/cyber security engineer and educator. Certifications: Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), Business Continuity Planner (BCP), ISO/IEC 27001:2013, Information Security Management System (ISMS) Lead Auditor, Certified in Risk and Information Systems Control (CRISC), Certified Information Security Manager (CISM), Certified Data Privacy Solutions Engineer (CDPSE) and Certification in Risk Management Assurance (CRMA).

UNIVERSITY OF ARKANSAS

College of Engineering
Master of Science in Operations Management

Third Party Risk Management

(Cyber Supply Chain Risk Management)

(C-SCRM)

Agenda

- Vendors - Why the Concern?
- Examples (Vendor Compromises)
- Potential Risks from Vendors to a Business
- Who Is Prepared?
- What is at Stake?
- Potential Challenge?
- Managing the Vendor Risk
- Validating Vendors
- References

Vendors - Why the Concern?

- **Rising Threat**
  - 51% of businesses have suffered a data breach caused by a third party
  - 44% suffering a breach within the previous 12 months
- Impact
  - Financial Losses
    - $3.92 million is the average cost of a data breach
    - $150 is the average cost of each lost record
    - $4.29 million is an adjusted average total cost of these data breaches

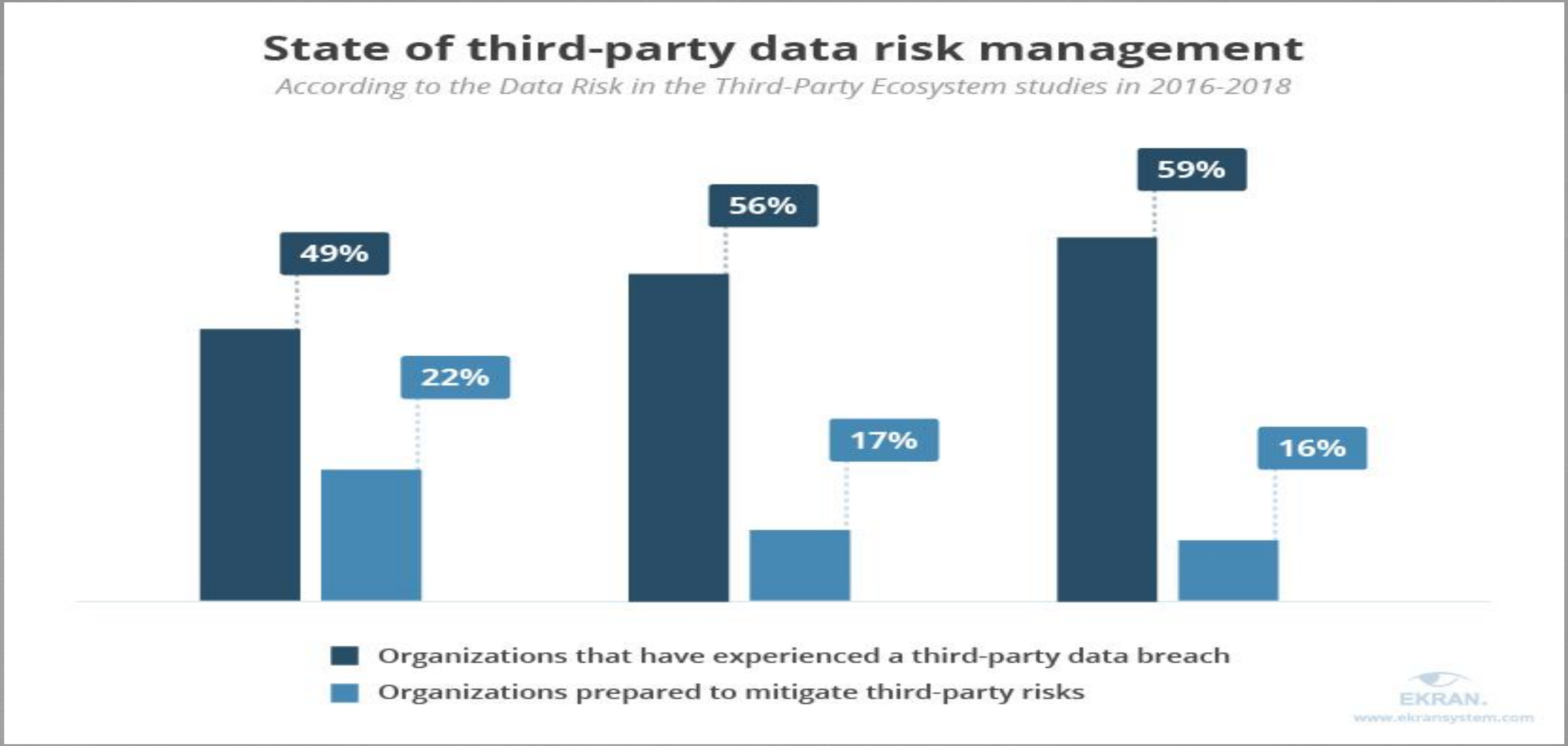
Examples (Vendor Compromises)

- Audi and Volkswagen (Notified in March)
  - Vendor left unsecure customer data on Internet (2019 – 2021)
  - 3.3 million records
- Kaseya VSA (July)
  - 1,500 companies affected worldwide
    - A Swedish grocery retailer co-op chain, which was forced to close more than 800 stores
  - REvil demanded a $70 million payment in bitcoin to decrypt
- Solarwinds Hack
  - Trojanized Software updates - Orion
- Cardinal Pipeline
  - Paid the cybergang known as DarkSide the ransom it demanded in return for a decryption key
  - $5 Million

Risk Exposure?

Potential Risks from Vendors to Business

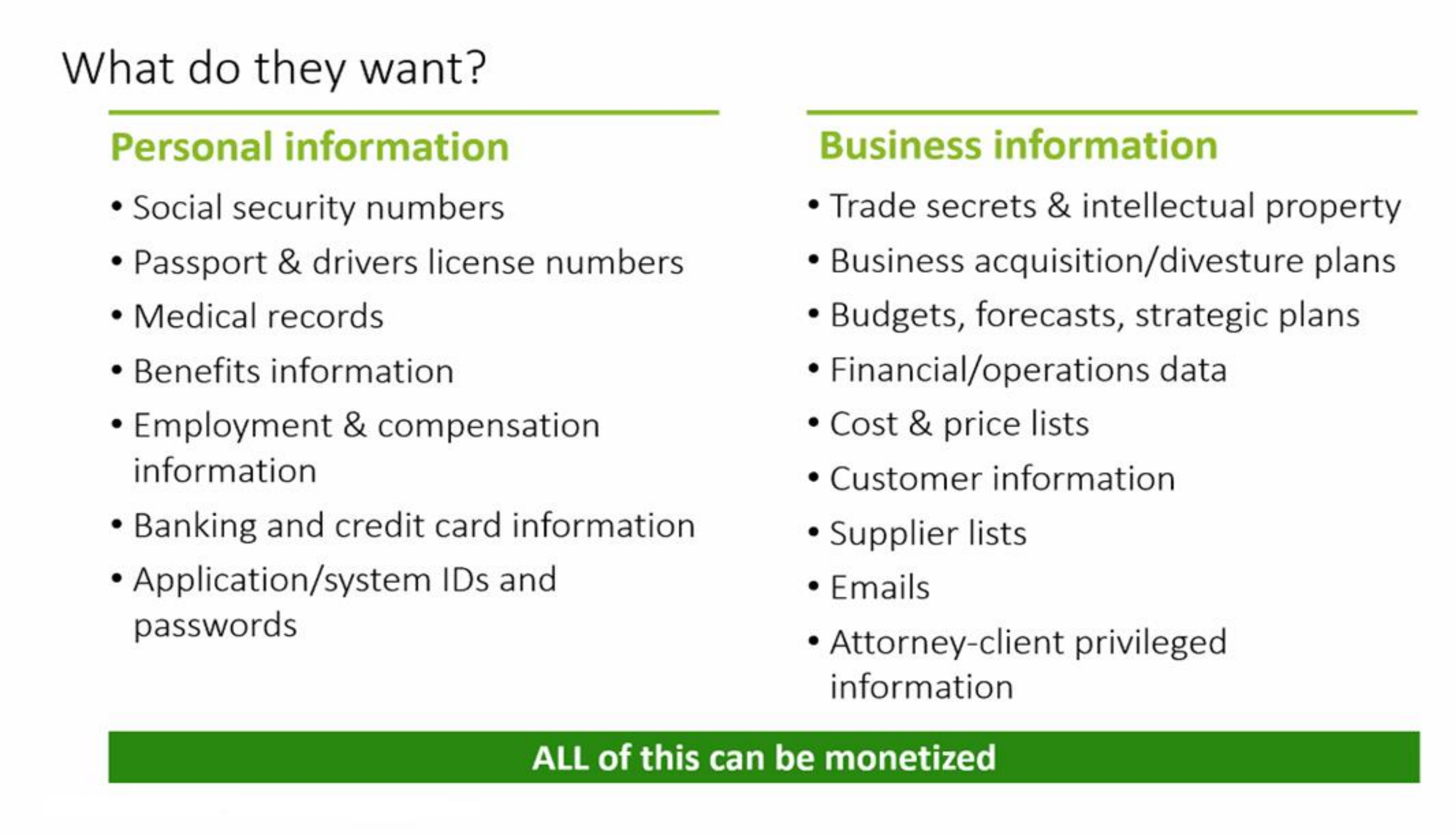
- Cybersecurity risk
  - Organization
    - Risk Threshold
    - Acceptable Risk Levels
  - Vendor Capabilities
- Compliance risk
  - Organization
    - Violations of laws, regulations, and internal processes
  - Vendor Meets
- Operational risk
  - Organizations
  - Vendor Capabilities



State of third-party data risk management

According to the Data Risk in the Third-Party Ecosystem studies in 2016-2018

What's at Stake?



What do they want?

Personal information

- Social security numbers
- Passport & drivers license numbers
- Medical records
- Benefits information
- Employment & compensation information
- Banking and credit card information
- Application/system IDs and passwords

Business information

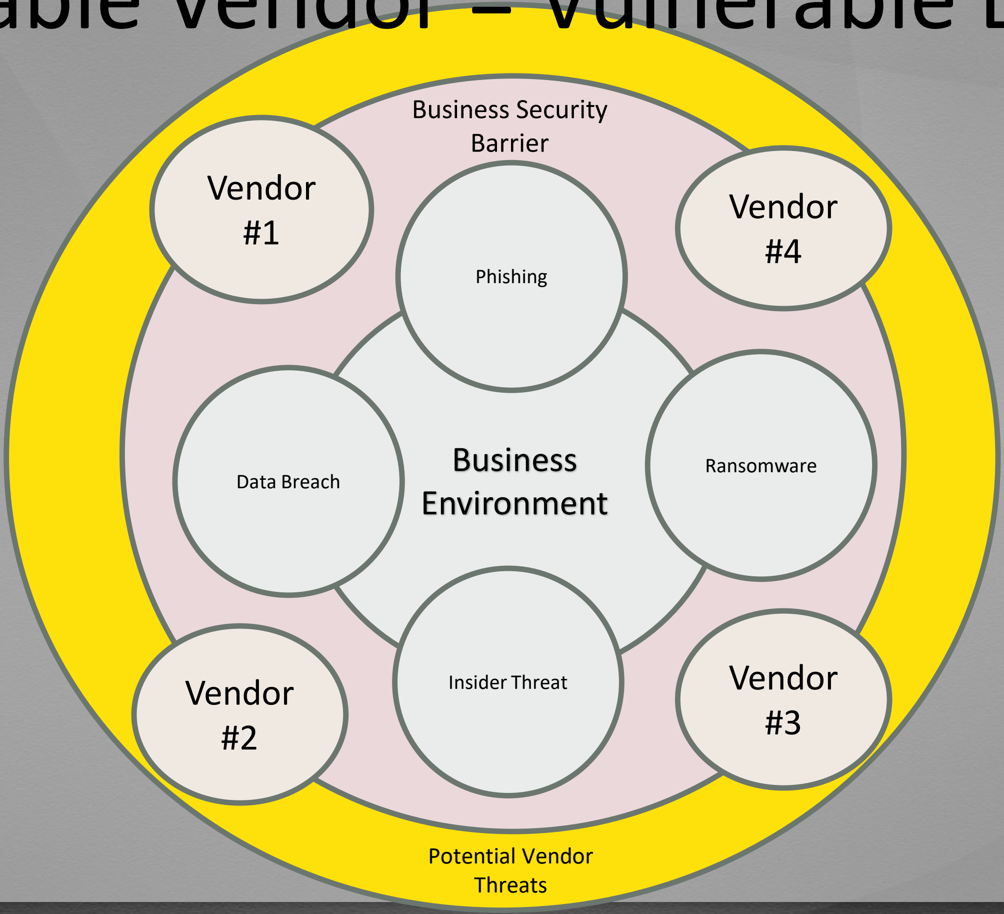
- Trade secrets & intellectual property
- Business acquisition/divesture plans
- Budgets, forecasts, strategic plans
- Financial/operations data
- Cost & price lists
- Customer information
- Supplier lists
- Emails
- Attorney-client privileged information

ALL of this can be monetized

Potential Challenges.

Deloitte Development, LLC

Vulnerable Vendor = Vulnerable Business



Business Security Barrier

Vendor #1

Vendor #4

Phishing

Data Breach

Business Environment

Ransomware

Insider Threat

Vendor #2

Vendor #3

Potential Vendor Threats

Managing the Vendor Risk

- **Vendor On-boarding**
  - Due Diligence Process
    - Structured and validated
  - Delineate Responsibilities
    - Contractual language
      - Use service-level agreements (SLAs)
        - » Outline who’s responsible for what in your cooperation with a third party
      - Master Service Agreement (MSA)
        - » Establishes what terms and conditions will govern all current and future activities and responsibilities

Managing Vendor Risk (Continued)

- Know Your Vendors
  - Maintain a vendor inventory
  - Classify the criticality of the vendor
    - High
    - Medium
    - Low
- Policies and Standards (Understanding)
  - Set clear cybersecurity rules
    - Educate/Inform Vendors
    - Develop policy that clarifies responsibilities of each party

Managing Vendor Risk (Continued)

- Limit Access
  - Privilege access management
    - Legitimate users can access your company's sensitive information
    - Apply secure access to critical assets
  - Enable continuous user activity monitoring
    - Monitor third-party vendor's activity within your working environment
- Plan for third-party incident response
  - Be Prepared!
- Perform regular audits
  - Include in MSA

Outcome!

Validating Vendors

- The Basic’s
  - Business must ensure and know:
    - Critical nature of data being shared with vendor
    - Vendors security systems and infrastructure
    - Continuous monitor vendor security activities or security gaps
    - Third-party risk assessments are completed
      - Vendor must meet the businesses risk thresholds
      - Reoccurring Assessments
    - Review of Service Level Agreement effectiveness
- Safe Cyber Working Environment!

References!

References

- National Institute of Standards and Technology (NIST)
  - CASE STUDIES IN CYBER SUPPLY CHAIN RISK MANAGEMENT
  - Information and Communications Technology Supply Chain Risk Management (ICT SCRM)
    - http://scrm.nist.gov
- Congressional Research Service
  - Cyber Supply Chain Risk Management Focus
- Bloomberg
  - Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom
- Ponemon Institute and IBM
- Deloitte Development, LLC
- EKRAN
  - https://www.ekransystem.com

Next Webinar:

Topic: Learning Through Service

Presented by: Phil Jones

Thanks for attending!

- For information about our flexible degree program options, email msom@uark.edu
- Visit **operations-management.uark.edu**
- *Registered* participants will receive an email with the video link to this webinar. We hope to see you online next month!