CYBER FLORIDA
at the UNIVERSITY OF SOUTH FLORIDA

EDUCATION | RESEARCH | OUTREACH

THIRD-PARTY CYBER RISK MANAGEMENT

Overview

Scope: approximately 1.5-hour lecture with practical examples

Intended Audience: technical and non-technical personnel who have a role to play in how the organization mitigates third-party cybersecurity risk

Objective

Understand the essential components of Third-Party Cyber Risk Management and the factors going into creating and maintaining a program to mitigate this risk

House Keeping

Rest Rooms

Emergency Exits

Designated 911 caller

CYBER FLORIDA at the UNIVERSITY OF SOUTH FLORIDA

Foundational Concepts

Who are the ”bad guys” and what do they want?

Why is cyber “hard”?

Capability maturity models

CYBER FLORIDA at the UNIVERSITY OF SOUTH FLORIDA

Adversary	Examples	Capabilities	Motivation
Nation State	US Russia China North Korea Iran	The best: most talented most funding best infrastructure strict command & control	Geopolitical “rational actors”
Cybercriminals	ALPHV (Blackcat) Black Basta Hive FIN7	Good talent Good funding Good infrastructure Varied command & control	Financial
“Hactivists”	Anonymous Wikileaks	Variable talent Variable funding Variable infrastructure Varied command & control	Ideology: political, social, religious Potentially “irrational actors”
Lone Wolf / Insider	Edward Snowden	The least: Limited to individual skills	Financial Ideology Potentially “irrational”

Why is cybersecurity “hard”

- Deliberate malicious actors
  - Attackers usually only have to be right once to ”win”
- Defenders have to be perfect
  - Includes highly technical risk factors
    - Bits & bytes
  - The weakest link is the human
    - Social engineering
  - Constant technology change & many manual processes

Capability Maturity Models

- Capability Maturity Models (CMM)
  - Crawl, walk, run
- Typically presented as levels 1-5 where each level requires that the previous level is completed/functioning
  - 1 – Ad hoc
  - 2 – Repeatable
  - 3 – Defined
  - 4 – Capable
  - 5 – Efficient
- This workshop illustrates CMM Level 2-3

Third-Party Cyber Risk

CYBER FLORIDA at the UNIVERSITY OF SOUTH FLORIDA

Examples of Third-Parties

- Vendors
  - Products / Services
  - Personnel
- Contractors
- Consultants
- Contingent Workers
- Visitors/Guests
- Peer Organizations
- Government, Banks, Legal

Typical Stakeholders

- Information Technology (IT)
  - Assesses risk
  - Proposes, implements and maintains technical controls
  - Incident Response (IR)
- Procurement
  - Overall process
- Legal
  - Contracting
- Business relationship owner
  - Sign-off on risk / controls
- Third-party

Types of Third-Party Cyber Risk

- Products/Services Supply-chain
- Technical Access
- Personnel on-site
- Data off-site
- Freeware/Shareware
- Breach of the Third-party

Cyber Risk Examples

CYBER FLORIDA at the UNIVERSITY OF SOUTH FLORIDA

Products

- Hardware, software or a combination
  - Vulnerabilities
  - Trojan Horses
  - Back-doors
  - Time-bombs
- Remote support of the product
- Onsite support of the product

Services

- Onsite support
  - Vendor laptops
- Offsite data
- Remote support

Technical Access

- Remote access w/vendor account
- Business-to-business (B2B) connectivity
- Onsite access w/vendor account
- Remote control access

Personnel Onsite

- Vendor support, contractors, consultants, contingent workforce
- Local accounts & access
- Malicious Actor
- Passive Actor
- Cyber Florida Insider Threat Management workshop

Data Offsite

- Vendor breach
- Vendor privileged employees
- How is the data protected?
  - At rest, in transit, in memory
  - Encryption keys management

Freeware / Shareware

- Often no way to negotiate contract terms
- Often no support
- Often imbedded in other products/services

Third-party Breach

- How long do they have to notify?
- How do they notify?
  - Trigger for your IR Plan
- Cyber Florida Incident Response Planning workshop

Common Risk Mitigations

CYBER FLORIDA at the UNIVERSITY OF SOUTH FLORIDA

Pre-Contract Signing

Third-Party Cyber Risk Assessment

- Open source information
- SOC2 reports, penetration testing report results, mitigation plans
  - Probably requires a Non-Disclosure Agreement (NDA)
- Cybersecurity questionnaire
  - Standard Information Gathering Questionnaire (SIG) *fee
- Risk evaluation products/services *fees

Contract Items

- Breach response disclosure timing and procedure
- Agreement to follow YOUR cybersecurity standards & policies
- Agreement to implement agreed upon cybersecurity controls (if any)
- Right to audit
  - Remote
  - Onsite

- Cyber Florida Third-Party Cybersecurity Contract Terms Addendum Template – TO BE DEVELOPED

Post-Contract Signing

- Vendor monitoring (if feasible)
- Third-party breach IR Plan trigger
- Cyber Florida Incident Response Planning workshop

Keeping It Going

CYBER FLORIDA at the UNIVERSITY OF SOUTH FLORIDA

Third-Party Cyber Risk Management Maintenance

- Establish governance
  - Who is accountable for maintaining the program?
- Integrate continuous improvement
  - Stakeholder input
  - Changing risk environment

Common Obstacles to Success

- Master Service Agreements (MSAs) & Statements of Work (SOWs)
- Not going through the process
  - Non-PO purchases
  - non-procurement purchases
- The cloud/SaaS
- ”One-man bands”
- Vendors “too big to respond”

Advanced Capability/Maturity

CYBER FLORIDA at the UNIVERSITY OF SOUTH FLORIDA

Beyond Crawling

- Fully leverage right to audit
  - Perform periodically based upon risk
  - Can be done by a vendor
  - Trust, but verify
- Triggers for re-evaluation
  - change in scope/relationship/status
- Recertification
- Integrate into an overall risk management framework/program

- Cyber Florida Risk Framework Workshop

Resources

- Cyber Florida Third-Party Cybersecurity Contract Terms Addendum Template – TO BE DEVELOPED
- Third-Party Cybersecurity Questionnaire Template – BEING CONSIDERED
- NUMEROUS guides, plans, templates and checklists available from NIST, consulting vendors, etc.

Objective

Understand the essential components of Third-Party Cyber Risk Management and the factors going into creating and maintaining a program to mitigate this risk

Items of Note for Florida Local Government

- SS 282.3185 Local Government Cybersecurity
  - Cybersecurity Training
  - Cybersecurity Standards
    - Generally accepted best practice to have a *.gov domain
  - Incident Notification & After-Action Report
    - Generally accepted best practice is to have an incident response plan covering this and ransomware reporting requirements
- SS 282.3186 Ransomware Incident Compliance
  - a county, or a municipality experiencing a ransomware incident may not pay or otherwise comply with a ransom demand

- Each county with:
  - Population $\geq$ 75,000 – adopt by January 1, 2024
  - Population $<$ 75,000 – adopt by January 1, 2025
- Each municipality:
  - Population $\geq$ 25,000 – adopt by January 1, 2024
  - Population $<$ 25,000 – adopt by January 1, 2025

What Else Does Cyber Florida Offer?

CYBER FLORIDA at the UNIVERSITY OF SOUTH FLORIDA

Cybersecurity Awareness

- 2024 Workshops: Network Noise, Incident Response, Third-Party Risk Management, Insider Threat
- Newsletters
- Intelligence reporting

For Public-Sector Organizations:

- Customized In-person Training
- Live Virtual Training
- Online Classes

Workshop Feedback

10 Questions, ~ 5-minutes

CYBER FLORIDA
at the UNIVERSITY OF SOUTH FLORIDA

EDUCATION | RESEARCH | OUTREACH

THIRD-PARTY CYBER RISK MANAGEMENT