SECURE360

The DIY Approach to Risk Assessments

Presented by:

Yan Kravchenko

Atomic Data, LLC

About Me

Yan Kravchenko, CISSP, CSSLP, CISA, CISM
CISO at Atomic Data
ykravchenko@atomicdata.com

#yanfosec
github.com/yanfosec

12+ years of performing 3rd party Risk Assessments

Agenda

- Common reasons for outsourcing
- Common Failures
- The DIY Approach
  - Talking about security
  - Improving IT
  - Covering basics
  - Advanced security considerations
- "Selling" your Risk Assessment
- QA / DIY Kit

SECURE360

Common Reasons to Outsource

- Risk Assessments are complicated
- Not sure how to do it
- Don’t have time to do it
- Need help passing an audit
- Want and expert to confirm you are right
- Security is expensive and you want to make sure you need it
- Requested by the Board of Directors

SECURE360

Why So Many Fail…

- Scope vs. cost
  - Good and bad risk assessments look identical
  - You only get what you pay for (or less)
- Unreasonable expectations
  - How long does it take a new CISO to get up to speed?
  - 1 week = repeating what I am told
- Rarely worth the expense
  - Starting around $30,000
  - Money spent on security would actually help…

DIY Risk Assessment

- Talking about security
- Improving IT
- Basic security considerations
- More advanced security considerations

Talking About Security

- Regular Governance Meetings = Ongoing Risk Management
- Policies - All you need is:
  - AUP / Code of Conduct
  - Non Disclosure / Confidentiality
  - Access Management / Passwords
  - Data Classification
  - Incident Response
  - {Check Compliance Requirements}
- Awareness Training
  - Talk about your company, policies, and why people should care

SECURE360

Improving IT

- Document your network
- Clean up your AD
- Improve Password Management
  - Change passwords
  - Increase length / complexity
  - Consider a Password vault
- Patch your servers
- Identify where sensitive data lives
- Configuration Hardening Standards / Benchmarks

SECURE360

Basic Security Considerations

- Vulnerability Scanning
- 2FA Authentication for Remote Access
- Disk / Backup Tape Encryption
- Malware Protection
- Network Security / Guest segregation
- Email Filtering (Spam / Malware)
- Vendor Management
- Incident Response Plan

SECURE360

Advanced Considerations

- Penetration Testing / Code Review
- IDS / IPS
- AD Membership Monitoring
- Centralized Logging / SIEM
- Network Segmentation
- Network Authentication
- GRC Tools (there is still hope)
- NIST CSF Framework ← CSF Reference Tool

NIST CSF

- Framework for Improving Critical Infrastructure Cybersecurity was published by NIST on 2/12/2014
- Based on many standards, best practices, and guidelines
- Mapped to:
  - ISO 27001
  - NIST SP 800-53
  - COBIT 5
  - CCS CSC 4
  - ANSI/ISA-62443-2-1 and -3-3

"Selling" Your Risk Assessment

- Ongoing Risk Management
- Governance Meeting Notes:
  - Current security issues
  - Emerging threats
  - 0-day vulnerabilities
  - Risk remediation / tracking
  - Decisions
- Risk Register
  - Risk acceptance is never permanent

DIY RA Toolkit Includes

- AD Analysis Power Shell Scripts – audit.ps1
- Sample Governance Meeting Agenda
- Sample Risk Register
- NIST CSF Resources
- DIY Risk Assessment Checklist
- Sample Vendor Assessment Checklists

https://github.com/yanfosec/diy_ra_toolkit

ATOMICdata®

SAFE. SIMPLE. SMART.

- IT ASSET INVENTORY & ANALYSIS
- SOC 3 CERTIFIED PRIVATE CLOUD
- SOC 3 CERTIFIED COLOCATION FACILITIES
- ENTERPRISE NETWORK ARCHITECTURE
- INTRUSION PREVENTION & MULTI-FACTOR AUTHENTICATION

ATOMICdata®

SAFE. SIMPLE. SMART.

Does your security group need a meeting venue? We can help!

Contact events@atomicdata.com for details.

STOP BY **BOOTH #305** TO

LEARN MORE ABOUT ATOMIC DATA

SECURE360

Questions?