



CYBER SECURITY  
SUMMIT 2017

# DIY RISK ASSESSMENTS

OCTOBER 2017



**Yan Kravchenko**

(CISSP, CSSLP, CISA, CISM)

**Chief Information Security Officer**



[ykravchenko@atomicdata.com](mailto:ykravchenko@atomicdata.com)



#yanfosec



[linkedin.com/in/yankravchenko](https://linkedin.com/in/yankravchenko)

**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**



## 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 an expert to confirm you are right
- ▶ Security is expensive and you want to make sure you need it
- ▶ Requested by the Board of Directors

## 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

## THE DIY APPROACH

- ▶ **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

## IMPROVING IT

- ▶ **Document your network**
- ▶ **Clean up your Active Directory (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**

## **BASIC SECURITY CONSIDERATIONS**

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

## 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**

## ADVANCED CONSIDERATIONS, CONTINUED

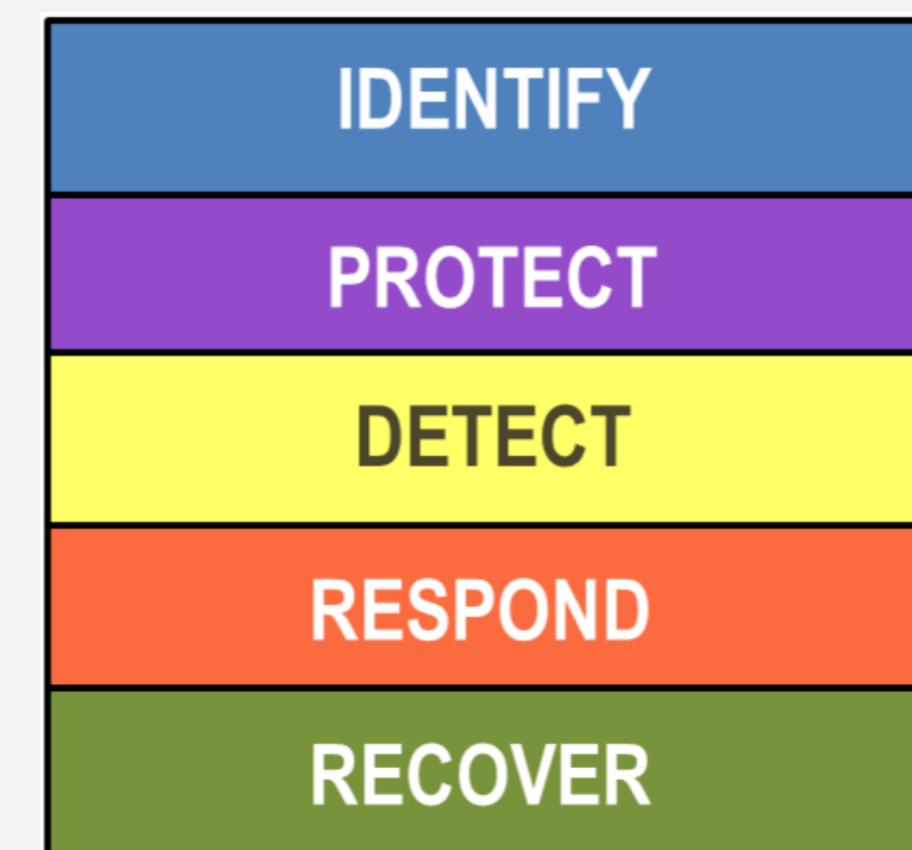
### ► Framework for Improving Critical Infrastructure

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**

**[www.atomicdata.com/css](http://www.atomicdata.com/css)**

- ▶ **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**



**QUESTIONS?**



THANK YOU!