Information Security for Small Business

Beyond the Alphabet Soup
February 1, 2018

Srinivas (Srini) Atluri, CISSP, CISM, GWAPT
VP Cyber Security Services. Anvaya Solutions, Inc.
About Us

Anvaya Solutions, Inc.
• Technology and Security Consulting since 2007
• 8(a), EDWOSB, SDB, Small, Woman-owned
• Compliance, Audit, Assessment, Advisory, Consulting, Risk Management
• Patents in Security – 3 issued, 4 pending

Srinivas (Srini) Atluri, CISSP, CISM, GWAPT
VP – Cyber Security Services, Anvaya Solutions, Inc.

18+ years in Information Security

Broad Spectrum Experience in multiple domains of Information Security

Email: Srinivas@anvayasolutions.com
Phone: (916) 673-9340
Attack Targets

- Large Biz
- Small & Medium
By the Numbers

28M

14M+

61%

Small & Medium Biz

84k to 148k

Your cost can be much more – Loss of business due to loss of customer trust and their information

DBIR:

82% of attackers compromised victims within minutes

UnHappy SIX Months

Credit: These Photos by Unknown Author is licensed under CC BY

These Photos by Unknown Author is licensed under CC BY-SA
Standards and Guides

NIST SP800-171 Protecting CUI
NIST SP800-53 Security & Privacy Controls
PCI-DSS
HIPAA
GLBA
SoX
DFARS 252.204-7012
CSF
RMF

NIST SP800-37 – Guide for Applying Risk Management Framework to Federal Information Systems
FIPS 199 – Standards for Categorization
FIPS 200 – Minimum Security Requirements for Federal Information and Information Systems

NIST SP 800-30 r1 – Guide for Conducting Risk Assessments
NIST SP800-39 – Managing Information Security Risk (Enterprise wide RM)
NIST SP800-18 – Security Planning
NIST SP800-63 - Authentication
Collective groan when this came out; WTF; %!@(#)@#!(%!!!

• I am not a tech company / I am small – Why should I comply?

DFARS Clause 252.204-7012
• DFARS 252.204-7012 requires NIST SP800-171 compliance for organizations handling Controlled Unclassified Information (CUI)
CUI Examples

- Email
- Blueprints, drawings
- Electronic files
- Physical records (printouts)
- Proprietary company/contractor information
<table>
<thead>
<tr>
<th>1. Access Control</th>
<th>8. Risk Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Awareness and Training</td>
<td>10. Security Assessment</td>
</tr>
<tr>
<td>5. Audit and Accountability</td>
<td>12. Systems and Communications Protection</td>
</tr>
<tr>
<td>7. Configuration Management</td>
<td>14. System and Information Integrity</td>
</tr>
</tbody>
</table>
• Work with an experienced knowledgeable security services provider

- Strategize
- Methodical Assessment
- POA&M
- Remediate
- Continuous Assessment
Risk Management Framework

Starting Point
FIPS 199 / SP 800-60

CATEGORIZE
Information System

FIPS 200 / SP 800-53r4

SELECT
Security Controls

Security Life Cycle
SP 800-39

IMPLEMENT
Security Controls

SP 800-53Ar4

ASSESS
Security Controls

SP 800-70

AUTHORIZE
Information Systems

SP 800-37

MONITOR
Security Controls

SP 800-37 / SP 800-53r4

SP 800-39

Compliant, But Secure?

- Take a holistic view of your environment and people
- Engage with a knowledgeable Security Services Provider
Holistic Security Approach

- Network
- Systems
- Apps
- Data
- IoT
- ICS
Help Fellow Businesses

MANAGE RISK

1. Monitor
2. Respond
3. Audit
4. Educate
5. Assess
6. Secure
Here to help SMB – B2B

Special Offers
Free Laptop Scan
Strategy Session
Questions?

My Contact Information

Srinivas Atluri
Srinivas@anvayasolutions.com
Ph: (916) 673-9340