HOW SECURITY MATTERS TO YOU

Alex Wood

ELEVATION
Security Consulting

Who Am I?

- CISO, Pulte Financial Services
- Principal Consultant, Elevation Security
- Director, ISSA International
- Speaker

ELEVATION
Security Consulting

How Did I Get Here?

CURRENT CYBERSECURITY THREATS

Trends

- Ransomware
- Business Email Compromise
- Credential Theft
- Internet of Things
- Nation State Activity

ELEVATION Security Consulting

Ransomware

- What is it?
  - Software used by Cybercriminals that encrypts data or prevents usage of a system until a ransom is paid
  - Theft of data that is held and threatened to be released until a ransom is paid
- Disrupts business with potential financial loss

Ransomware

- Nearly 50% of business surveyed had been hit with ransomware at least once in the last 12 months
- 56,000 documented infections in March alone
- $209M paid in Q1 2016

ELEVATION Security Consulting

Business Email Compromise

- What is it?
  - “a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.”
  - Could also include theft of confidential data

ELEVATION Security Consulting

Business Email Compromise

- Over $3.1B in losses worldwide
- 1300% increase in losses since January 2015
- 14,000+ US victims with losses over $950M

ELEVATION Security Consulting

Credential Theft

- What is it?
  - Data breach involving usernames and password of users of a particular website or service

Credential Theft

- Yahoo: 500M credentials
- LinkedIn: 160M+ credentials
- MySpace: 360M+ credentials

Internet of Things (IoT) Security

- What is it?
  - The ever growing number of “things” connected to the Internet, such as thermostats, refrigerators, security cameras, and a host of other devices
  - IoT devices are made for functionality not security and are very vulnerable to compromise
- 6.4B IoT devices expected to be used in

Internet of Things (IoT) Security

- Mirai Botnet made up of ~400,000 infected security cameras and other devices
- Carried out record sized Distributed Denial of Service attacks of 600+ Gb/s

Nation State Activity

- Cyberespionage
  - Conducting espionage via the Internet
  - Happening now
- Cyberwarfare
  - Acts of war carried out via the Internet
  - Not yet but when?
  - Still a murky area in policy

Nation State Activity

- OPM Breach
  - 4 million records stolen by the Chinese
- DNCC/Election Interference
  - Russian intelligence services conducting activities to interfere with US elections

Data Breaches?

- Where are all the data breaches of Credit Card numbers and personal information?
- No “headline” breaches of PII or credit cards
- Over 500 breaches in 2016 affecting over 12M records

ELEVATION Security Consulting

OK, SO HOW DOES THIS AFFECT ME?

All Businesses are Information Businesses

- Southwest and Delta grounded planes because of IT
- Hollywood Presbyterian patient care affected due to ransomware
- Issues affecting the confidentiality, integrity, or availability of IT systems cost your business

ELEVATION Security Consulting

Data Confidentiality

- Average cost of a data breach in 2016 is $158 per record lost

- Businesses experiencing breaches could experience an abnormal customer churn rate of up to 6.2%

ELEVATION
Security Consulting

Availability

- How much $ could your business lose without Internet connectivity?
- What if your website or customer facing website or applications were unavailable?
- 83% increase in DDoS activity in Q2 2016

ELEVATION Security Consulting

Compliance

- OCR has issues fines of over $39M for HIPAA violations
- Target $39.4M settlement with credit card issuers
- FTC vs Wyndham
  - Required to implement a comprehensive security program
  - 20 year monitoring period

ELEVATION Security Consulting

SO WHAT CAN WE DO ABOUT IT?

You Need a Plan

- FTC Start with Security
  - 10 steps to start with
- NIST Cybersecurity Framework
  - A more robust but flexible framework

ELEVATION Security Consulting

FTC Start with Security

- Start With Security!
  - Think about security on all business decisions you make. Do we need to collect that data?
- Control access to data sensibly.
  - Give access to sensitive data to those who need it for their jobs, and nobody else.
- Require secure passwords and authentication.
  - “121212” is not a good password. Good passwords are complex and changed regularly.

ELEVATION Security Consulting

FTC Start with Security

- Store sensitive personal information securely and protect it during transmission.
  - Not only should be sent in a secure way, it shouldn't be left sitting around on servers unprotected.
- Segment your network and monitor who's trying to get in and out.
  - Like a bank, getting in the front door shouldn't mean you have access to everything.
- Secure remote access to your network.
  - Getting in from outside the office needs to be properly controlled. Bad guys love remote access too!

ELEVATION Security Consulting

FTC Start with Security

- Apply sound security practices when developing new products.
- Make sure service providers implement reasonable security measures.
  - They are an extension of your company. Make sure they're protecting your interests.
- Put procedures in place to stay current.
  - New vulnerabilities appear continuously. You need to keep up with them.
- Secure paper, physical media and devices.
  - These are ripe for theft of loss

ELEVATION Security Consulting

NIST Cybersecurity Framework

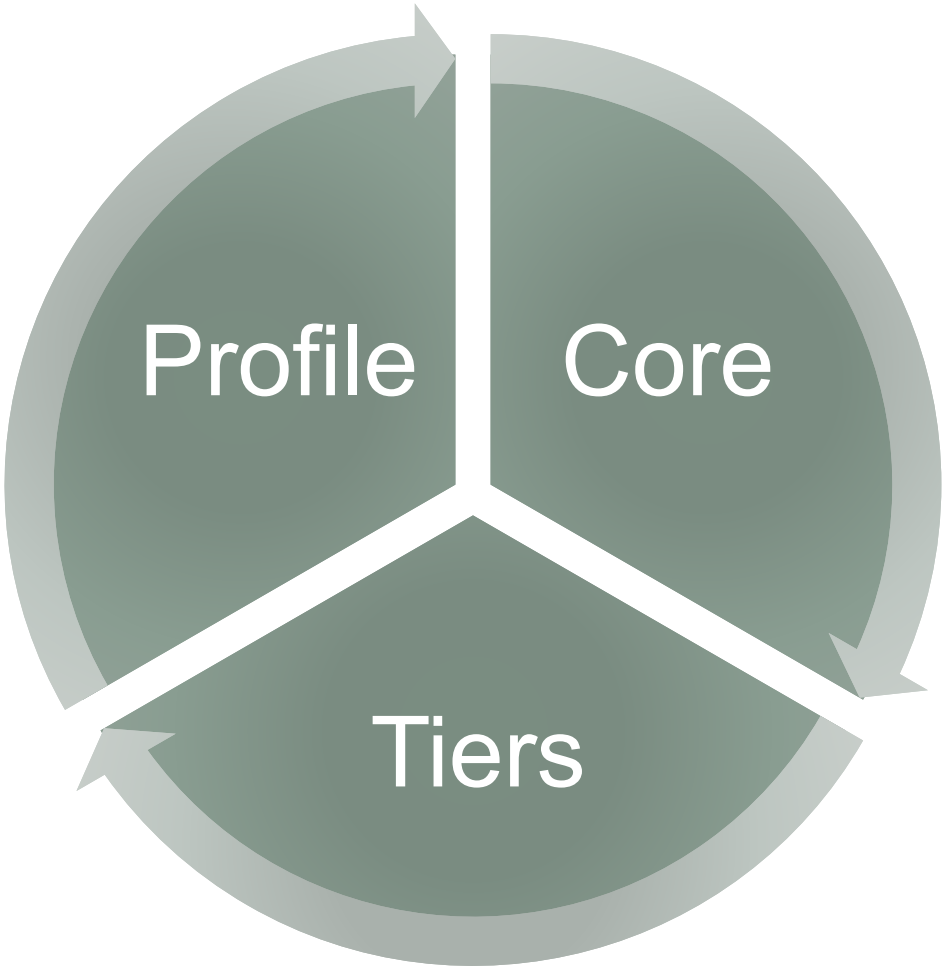
- Developed based on Presidential Executive Order
- Designed for the private sector to help secure critical infrastructure
- Robust but flexible enough for any organization

ELEVATION Security Consulting

Goals of the Framework

- Current state
- Future state
- Gaps
- Assess progress
- Communicate risks and progress
  - Internally
  - Externally

Framework Overview



ELEVATION Security Consulting

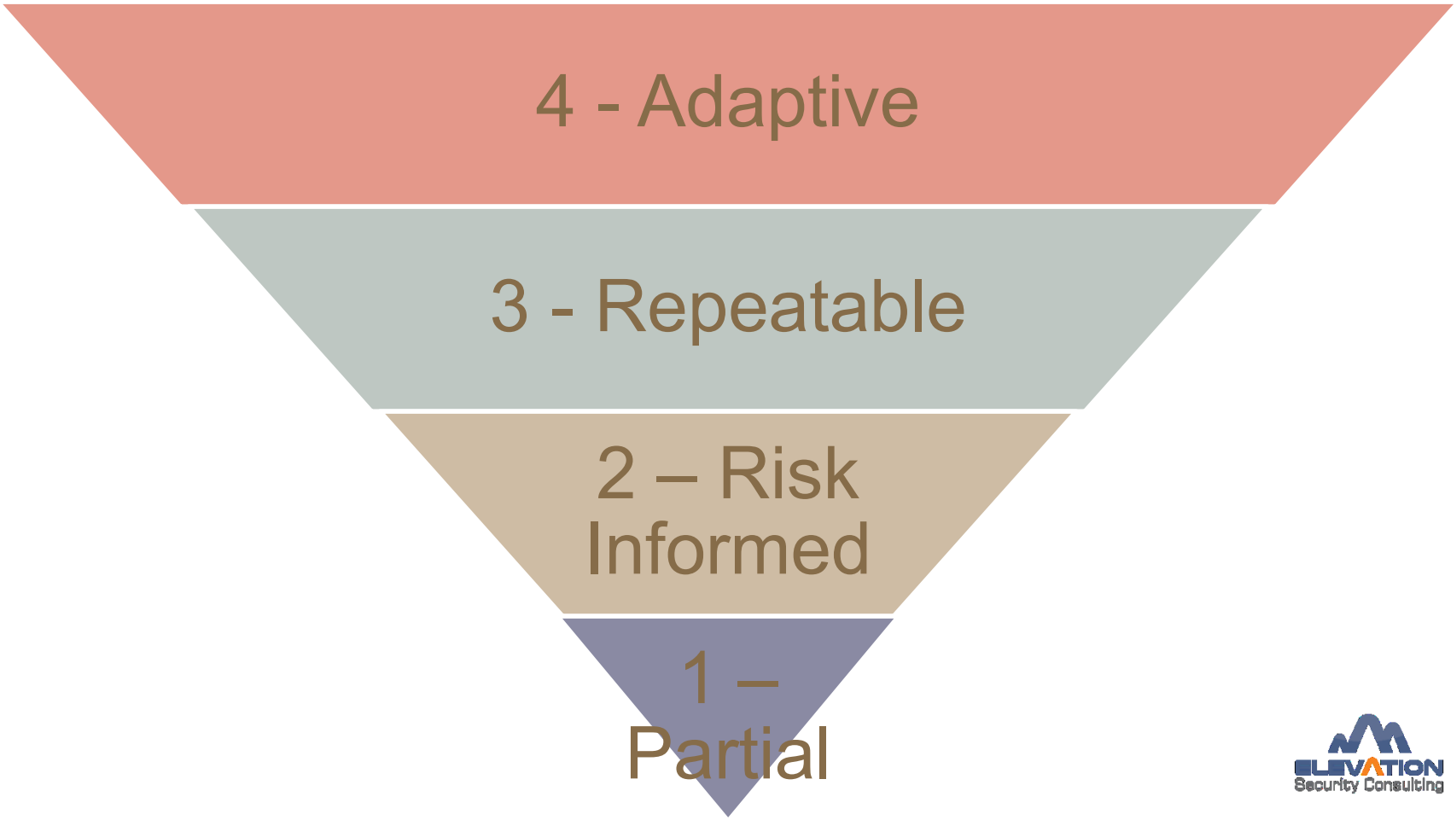
Framework Core

- Identify – ***Know yourself***
- Protect - ***Stop the bad guys!***
- Detect – ***Know when something bad happens***
- Respond – ***React to events nimbly***
- Recover – ***Get back up and running***

ELEVATION Security Consulting

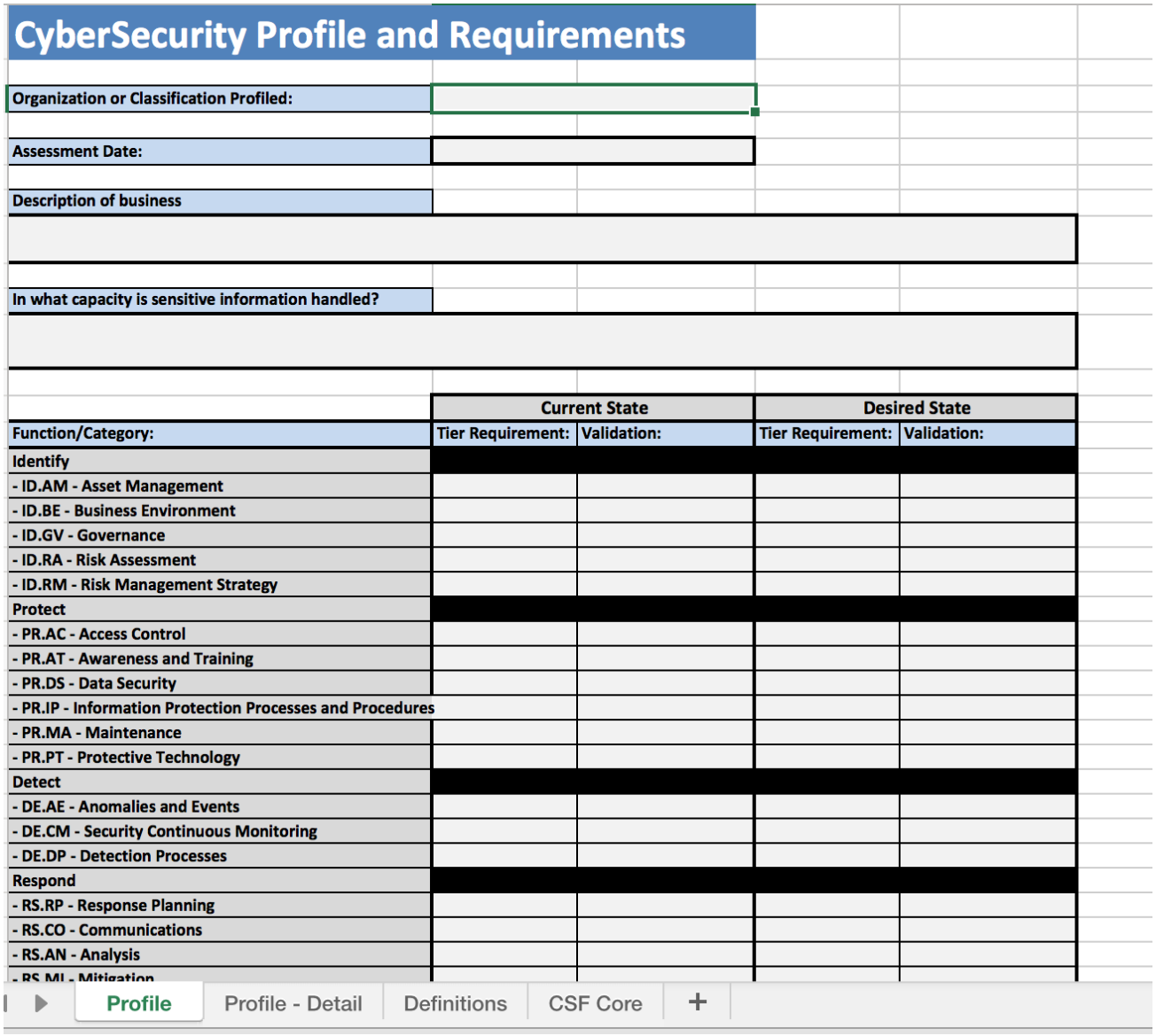
Framework Tiers

The tiers go from reactive to proactive



ELEVATION Security Consulting

Framework Profiles



CyberSecurity Profile and Requirements

Organization or Classification Profiled:				
Assessment Date:				
Description of business				
In what capacity is sensitive information handled?				
	Current State		Desired State	
Function/Category:	Tier Requirement:	Validation:	Tier Requirement:	Validation:
Identify				
- ID.AM - Asset Management				
- ID.BE - Business Environment				
- ID.GV - Governance				
- ID.RA - Risk Assessment				
- ID.RM - Risk Management Strategy				
Protect				
- PR.AC - Access Control				
- PR.AT - Awareness and Training				
- PR.DS - Data Security				
- PR.IP - Information Protection Processes and Procedures				
- PR.MA - Maintenance				
- PR.PT - Protective Technology				
Detect				
- DE.AE - Anomalies and Events				
- DE.CM - Security Continuous Monitoring				
- DE.DP - Detection Processes				
Respond				
- RS.RP - Response Planning				
- RS.CO - Communications				
- RS.AN - Analysis				
- RS.MI - Mitigation				

Profile | Profile - Detail | Definitions | CSF Core | +

ELEVATION Security Consulting

Implementation Guidelines

Provided by NIST – High Level

1. Prioritize and Scope
2. Orient
3. Create a Current Profile
4. Conduct a Risk Assessment
5. Create a Target Profile
6. Determine, Analyze, and Prioritize Gaps
7. Implement Action Plan

ELEVATION Security Consulting

How Do I Start?

- Assess your current state. Use a 3rd party.
- Make your cybersecurity plan and begin to implement
- Ensure you have an incident response plan and test it
- Lather, rinse, and repeat

ELEVATION Security Consulting

And We're Secure Now Right?

The End

ELEVATION
Security Consulting

Questions

Contact Alex:

alex@elevationsec.com

@abwoodrow

ELEVATION Security Consulting