NYSTEC

YOUR INDEPENDENT TECHNOLOGY ADVISOR

Advice
Strategy
Solutions
Consulting

Cyber Protections: First Step, Risk Assessment

Presentation to:

NYSAC
NEW YORK STATE ASSOCIATION OF COUNTIES

Presented to:
Mark LaVigne, Deputy Director
NYSAC
November 21, 2017

500 Avery Lane
Rome, NY
13441
315.338.5818
www.nystec.com

In this presentation

Cyber Protection Business Strategy

- The importance of cyber protection
- Cyber protection strategy
- Products of NYSTEC risk assessment
- Leveraging NYSTEC Cyber Protection Services

Importance of Cyber Protection

- Data breach at an upstate New York hospital
- Hackers gain access to NYS county's 911 system

Typical outcomes from a security incident

Financial loss $154-$158 per Record*	Regulatory penalties / contract issues	Credit monitoring ~$40/person per year	Cost of litigation and mitigation

Productivity loss	Reputation Damage	Executive loses job

* 2016 Ponemon Institute https://securityintelligence.com/media/2016-cost-data-breach-study/

Cyber Protection Strategy

- Begins with a comprehensive assessment of risk
- No quick-fix
- Must be baked in and not bolted on
- Full leadership commitment
- Holistic and multi-faceted approach
- Continuous process

Value of a Risk Assessment

Helps to identify:

- Threats to Systems
- Gaps in Defenses
- Likelihood of system compromise
- Business Impact

Benefits:

- Optimize Investment in Security
- Plan Implementation of Safeguards
- Justification for County and State Sponsors

NYSTEC Risk Assessment

Results of the Risk Assessment:

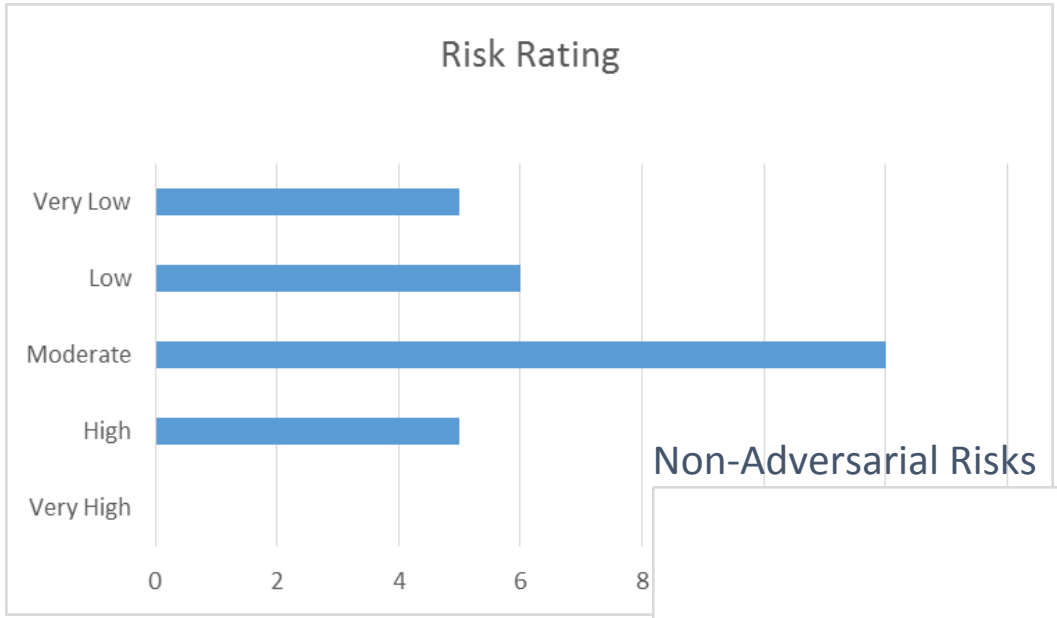
- Detailed explanation of review
- CIS Top-20 Heat Map
- Prioritized mitigation plan
- Business Impact

Value of the Risk Mitigation Plan:

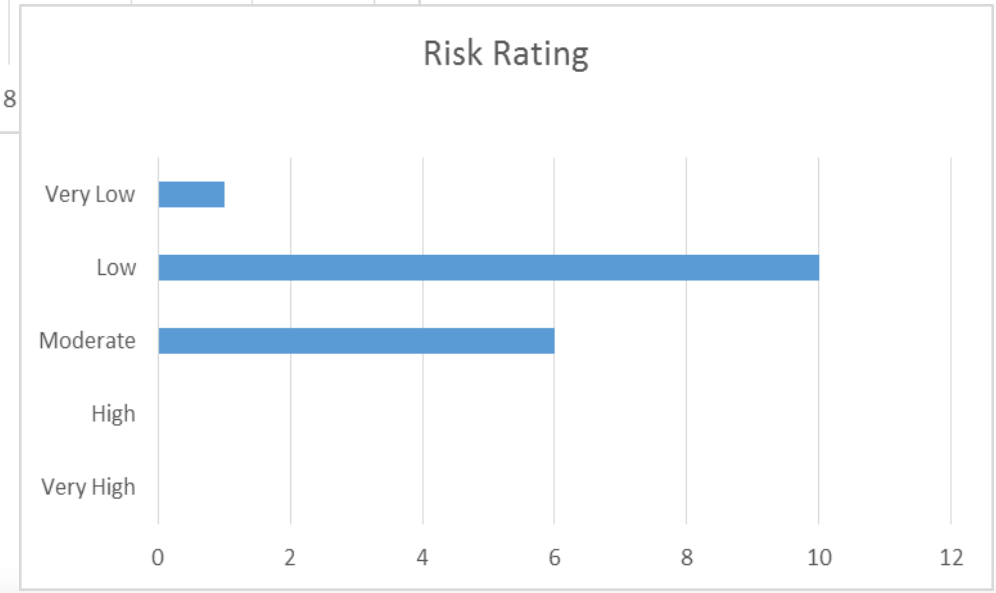
- Use to justify funding requests
- Identify where limited funds should be invested
- Maximize return on investment

NYSTEC Risk Assessment Product

Adversarial Risks



Non-Adversarial Risks



NYSTEC Compliance Heat Map

Control	Control Description	Explanation %	Artifacts %
CSC 1	Inventory of Authorized and Unauthorized Devices	80	75
CSC 2	Inventory of Authorized and Unauthorized Software	73	67
CSC 3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	69	57
CSC 4	Continuous Vulnerability Assessment and Remediation	87	83
CSC 5	Controlled Use of Administrative Privileges	60	25
CSC 6	Maintenance, Monitoring, and Analysis of Audit Logs	63	55
CSC 7	Email and Web Browser Protections	69	57
CSC 8	Malware Defenses	60	40
CSC 9	Limitation and Control of Network Ports, Protocols, and Services	20	0
CSC 10	Data Recovery Capability	100	60
CSC 11	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	66	38
CSC 12	Boundary Defense	73	48
CSC 13	Data Protection	76	48
CSC 14	Controlled Access Based on the Need to Know	80	40
CSC 15	Wireless Access Control	92	60
CSC 16	Account Monitoring and Control	57	30
CSC 17	Security Skills Assessment and Appropriate Training to Fill Gaps	20	0
CSC 18	Application Software Security	4	0
CSC 19	Incident Response and Management	31	14
CSC 20	Penetration Tests and Red Team Exercises	63	43

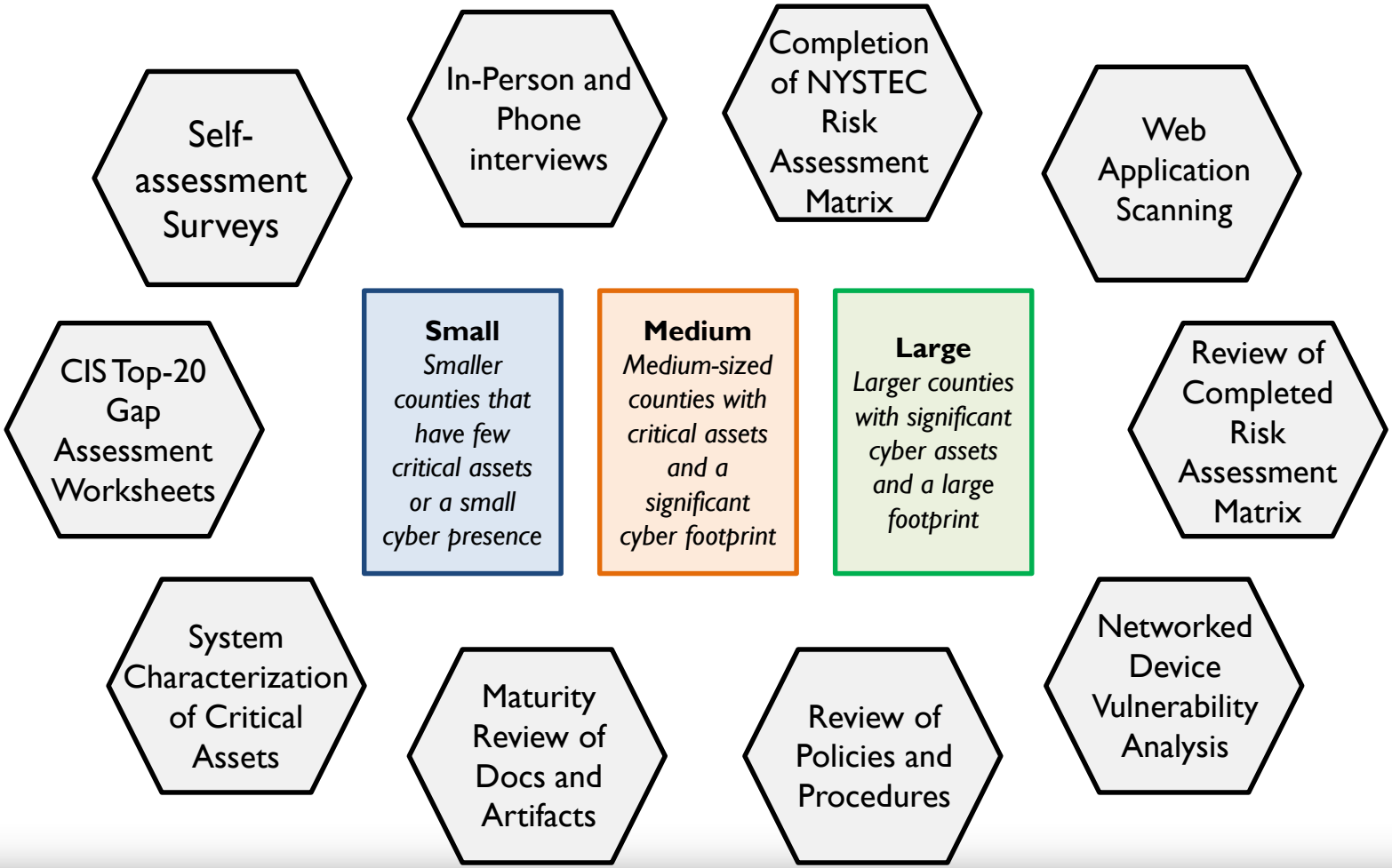
Interpreting the Heat Map

Control	Control Description	Explanation %	Artifacts %
CSC 1	Inventory of Authorized and Unauthorized Devices	80	75
CSC 2	Inventory of Authorized and Unauthorized Software	73	67
CSC 3	Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	69	57
CSC 4	Continuous Vulnerability Assessment and Remediation	87	83
CSC 5	Controlled Use of Administrative Privileges	60	25
CSC 6	Maintenance, Monitoring, and Analysis of Audit Logs	63	55
CSC 7	Email and Web Browser Protections	69	57
CSC 8	Malware Defenses	60	40
CSC 9	Limitation and Control of Network Ports, Protocols, and Services	20	0

Risk Assessment will provide:

- Detailed explanation of scoring and business risks
- Recommended mitigation steps
- Recommended priority for implementing changes

NYSTEC Cyber Protections Services Menu



Thank you

Questions?