IBTTA

TOLLING. MOVING SMARTER.

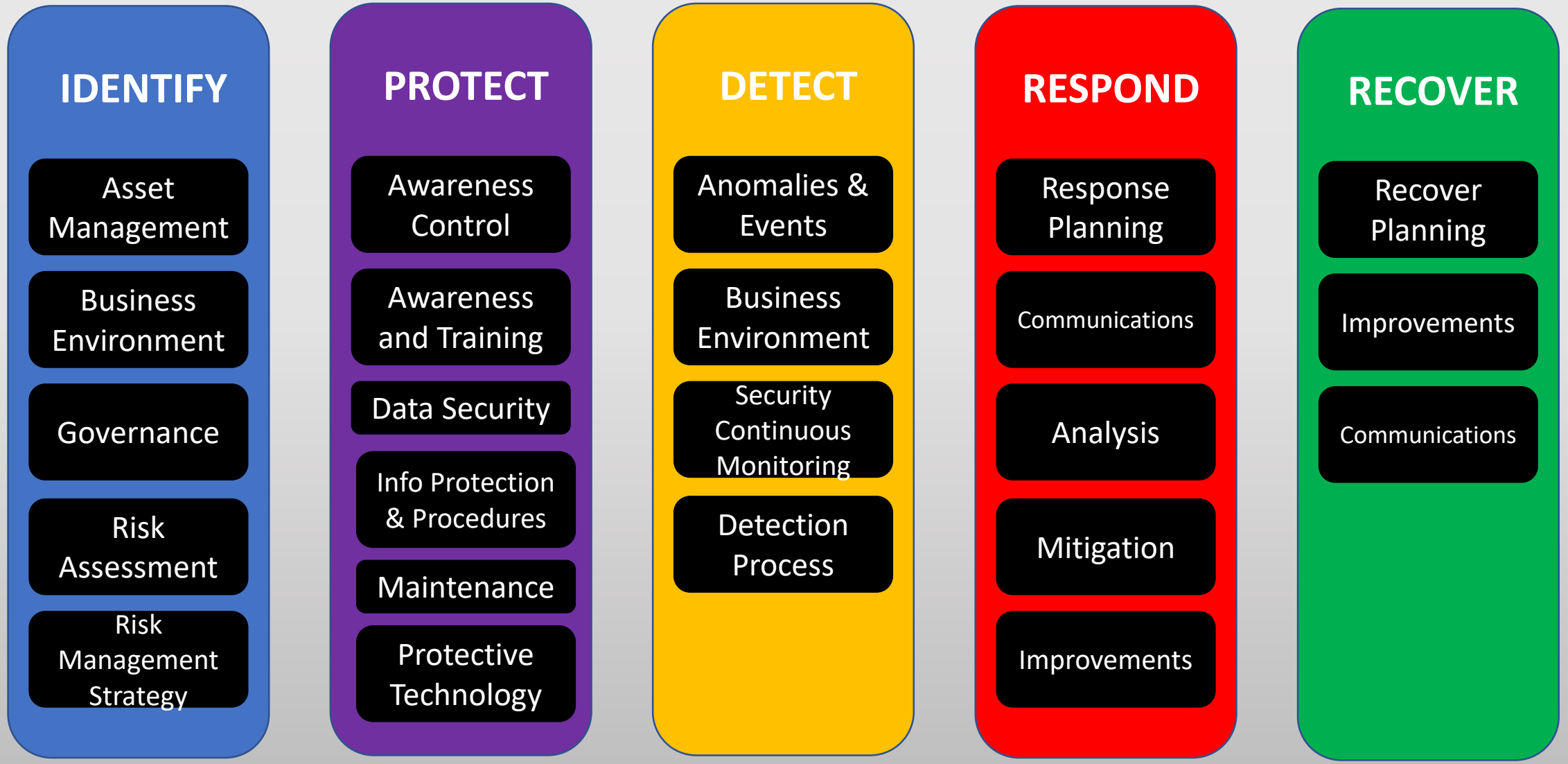
ANNUAL TECHNOLOGY SUMMIT | ORLANDO, FL | MARCH 31-APRIL 2, 2019

William Crosbie

Critical Infrastructure - Global Business Development Director

PARSONS

NIST Cybersecurity Framework



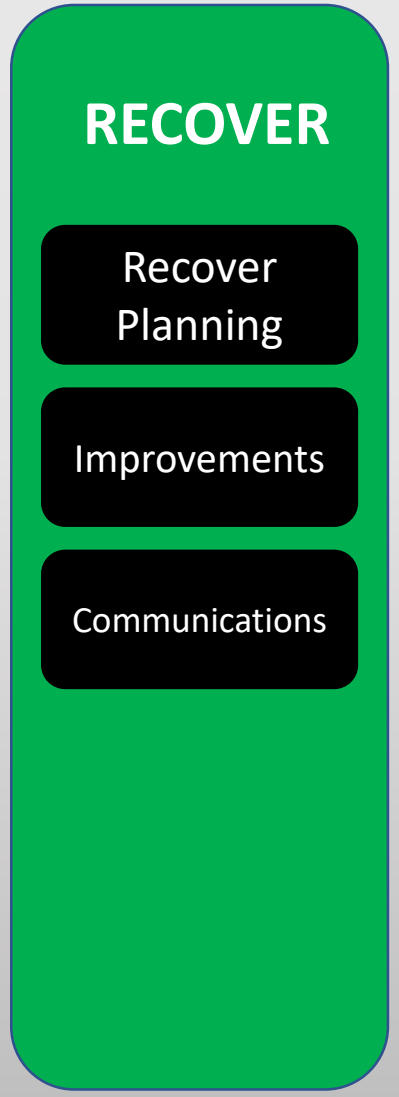
The Most Devasting Cyberattack in History

- *THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBERATTACK IN HISTORY* by Andy Greenberg, Wired Magazine
- https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
- Maersk – global integrated container logistics company
- Eight business units ranging from ports to logistics to oil drilling, in 574 offices in 130 countries around the globe
- Within two hours of the attack – 4,000 servers, 150 domain controllers and 45,000 PCs were infected
- 76 ports on all sides of the earth and nearly 800 seafaring vessels, including container ships carrying tens of millions of tons of cargo, representing close to a fifth of the entire world's shipping capacity, was dead in the water
- Financial impact is estimated at $250M to $300M

RESPOND

- Business Continuity, Emergency and Communication Plans
  - Must contemplate a cyber event
  - Independent facilities and systems
  - Cyber Insurance
- Forensic Analysis On-call Experts
  - Identify attack surfaces
  - Identify threat sources
  - Assess impact to customers, shareholders, and employees (the stakeholders) quickly
  - Access secondary threats and vulnerabilities
  - Minutes not hours or days
- Mitigation actions
- Communicate findings and mitigation actions to stakeholders including the board of directors. insurance company, politicians, and the public
- Communicate updates at regular intervals

RECOVER



- Communicate latest findings and mitigation actions to stakeholders
- Assess impact
  - Lost revenue
  - Expenses
  - Consequential damages
  - Liquidated damages
- Document everything
- Open an insurance claim
- Independent re-certification of the network, IoT devices and associated hardware
- Leave it stronger

Certification Case Study

- **Team was formed in response to Bloomberg articles alleging hack on OEM's mother boards**
- **Parsons was brought as a result of expertise with hardware manufacturing for National Security customers**
- **OEM's primary motivation was loss of stock value**
  - Roughly 50% hit to valuation…so they were very motivated to address the issue
- **Our role was to determine if any of the hardware was compromised**
- **We were provided complete design documentation**
- **We verified assemblies against the design docs**
  - All parts in bill of material
  - No additional parts
- **We X-rayed key areas and components**
  - Connectors, major Integrated Circuits
- **We also X-rayed depopulated boards to verify no malicious embedded components**

Questions

William Crosbie
Global BD Director
Critical Infrastructure
Telephone: 202-868-9017
Email: William.Crosbie@parsons.com

PARSONS