Building a Resilient Cybersecurity Program

North Carolina Cybersecurity Awareness Symposium

October 7, 2021

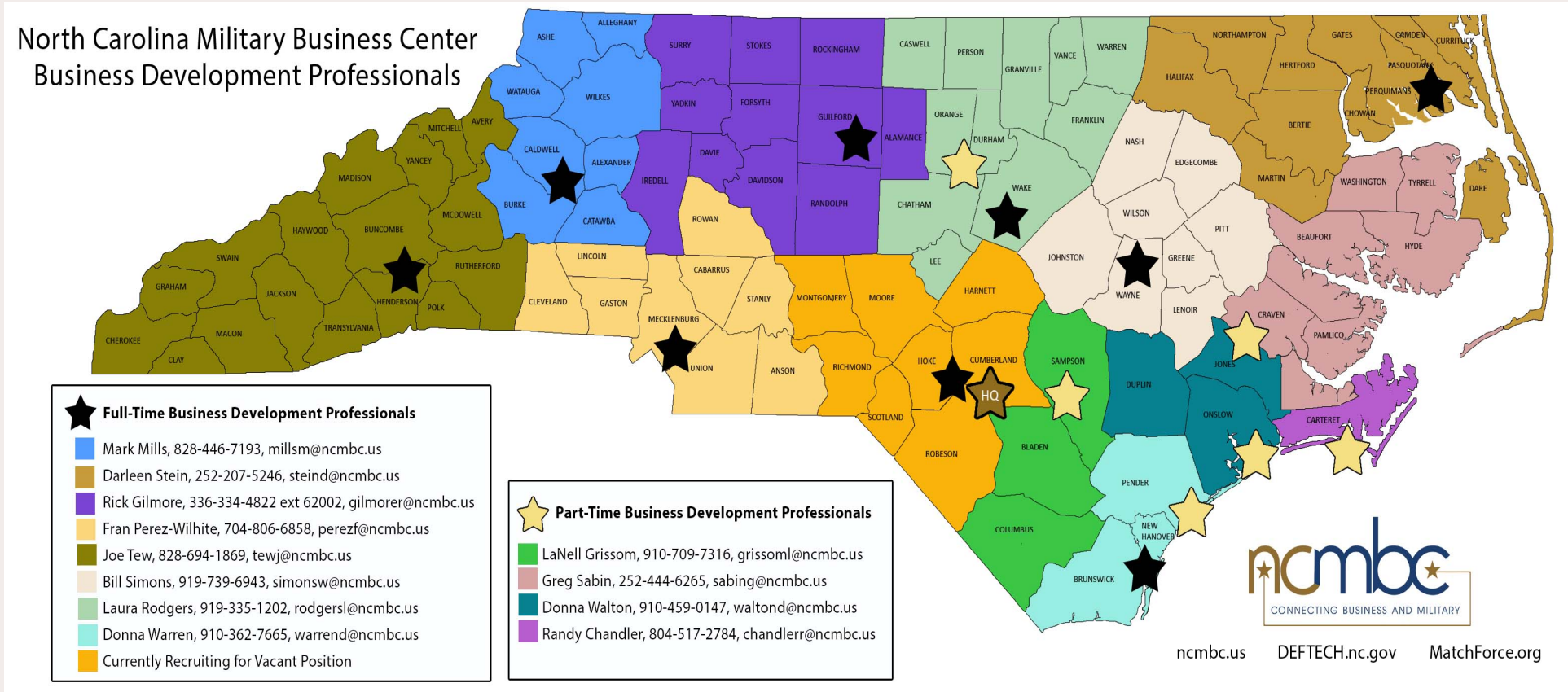
Laura Rodgers, North Carolina Military Business Center
www.ncmbc.us/www.cyberNC.us

North Carolina Military Business Center

Who We Are

- The NCMBC is a statewide, business development and technology transition asset of the NC Community College System, headquartered at Fayetteville Tech
- Totally State-funded, the NCMBC is the only statewide, military-focused economic development entity in the US, and the only NC agency solely focused on growing the defense economy through existing industry

North Carolina Military Business Center



North Carolina Military Business Center

MatchForce is a free tool that:

- Matches businesses to federal opportunities
- Matches contracting staff to NC businesses
- Matches prime contractors to NC subcontractors
- Matches businesses to future opportunities (forecast data)
- Businesses won >$5.51 billion, 2006-2021 contracts

Matchforce.org

North Carolina Military Business Center

Laura Rodgers
Cybersecurity Compliance
rodgersl@ncmbc.us
919-314-7317
Wake Tech Community College
RTP Campus in Morrisville

www.ncmbc.us
www.cyberNC.us

Building a Resilient Cybersecurity Program

We live a time of unprecedented change and change is occurring at an unprecedented rate – the “Exponential Age”. It is almost impossible to keep up – to stay ahead of evolving threats and new technologies.

Building a Resilient Cybersecurity Program

Resilience: the ability to prepare for, withstand, adapt to, respond to, and rapidly recover from changing conditions and acute disruptions. Requires competence, flexibility, responsibility, communication, teamwork, and problem-solving.

Resilience = Business Continuity

Building a Resilient Cybersecurity Program

Prepare

- *Tone at the Top* – leaders must understand the need for a resilient cybersecurity program, communicate that need effectively, and provide the resources to develop, maintain, evaluate and evolve the program.

Developing a cybersecurity program is a business decision

Building a Resilient Cybersecurity Program

Prepare

- ✓ *Asset Inventories – to protect assets you must know what assets you have, where they are located and who is responsible for them; AND if the assets must be protected per government regulations.*

Building a Resilient Cybersecurity Program

Prepare

- *Asset Inventories*
  - Data (the new currency)
    - ✓ Types of data – sensitive, IP, legal documents, regulated, intangible (brand), etc.
  - IT – software/hardware
  - Any asset(s) that could be harmed by a cybersecurity incident

Building a Resilient Cybersecurity Program

Prepare

- Know your risks and vulnerabilities – perform a thorough *risk analysis*. Be sure to include supply chain risks.

Building a Resilient Cybersecurity Program

Withstand –
Risk Treatments

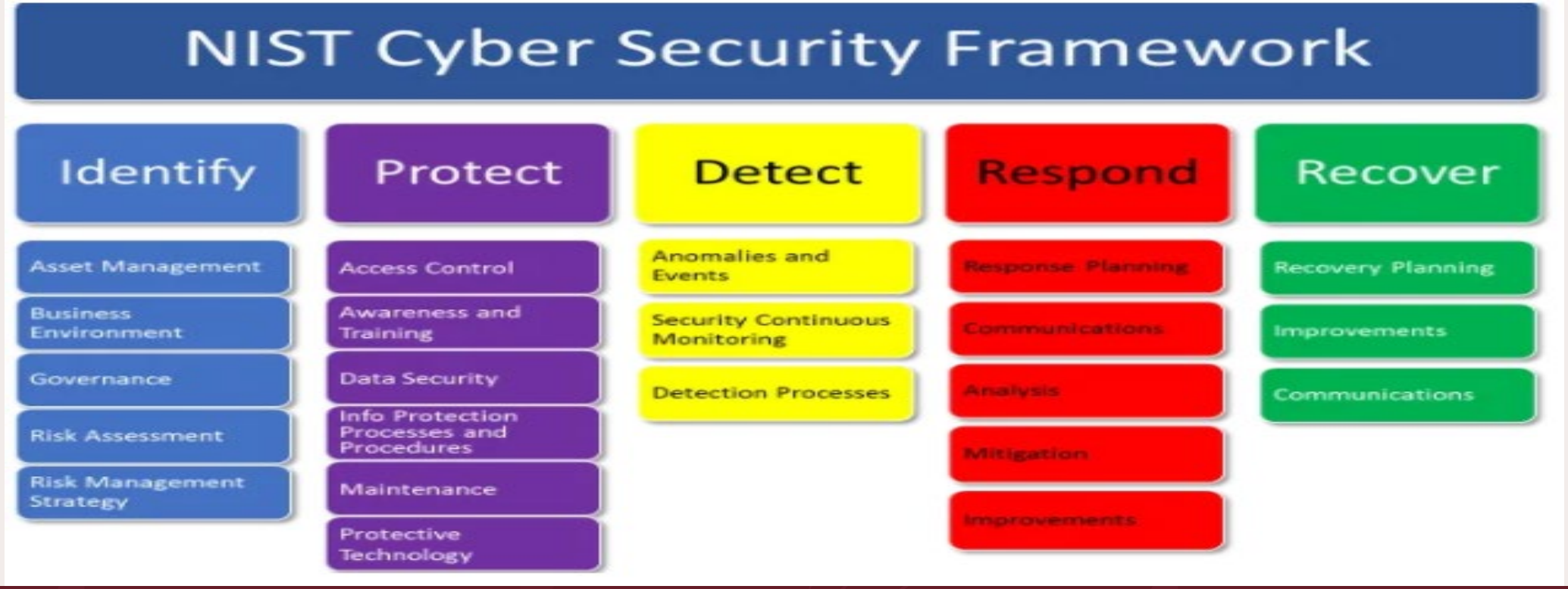
Building a Resilient Cybersecurity Program

Withstand

- *Transfer Risk*
  - Cloud service provider - handle complex cybersecurity controls
  - Purchase cybersecurity insurance
- *Avoid Risk*
  - Dispose of unnecessary assets (such as old data)
  - Minimize the transfer of sensitive data

Building a Resilient Cybersecurity Program

Withstand **–** *Reduce Risk* **–** Select a Framework/Controls



Building a Resilient Cybersecurity Program

Withstand

Reduce Risk - Example

- Training – for most organizations, the biggest cybersecurity risk is people risk. Invest in awareness and task-specific training. A well-trained workforce is your first line of defense.
    - Recommend Wizer's free training: https://www.wizer-training.com/

Building a Resilient Cybersecurity Program

Withstand

- *Residual Risk* - risk can't be 100% eliminated. Decide how much risk you are willing to accept based on your organization's risk appetite.

Building a Resilient Cybersecurity Program

Withstand

Policies/Procedures – comprehensive cybersecurity policies and procedures keep everyone in the same boat and paddling in the same direction. You will get repeatable, quality results with a good policy/procedure framework. Ad hoc frameworks create confusion and chaos – and increase risk.

The SANS Institute has good – and free – templates:
https://www.sans.org/information-security-policy/

Building a Resilient Cybersecurity Program

Withstand - *Respond*

- Need event/incident detection – can't respond if you don't know an incident has occurred
- Incident analysis – to respond effectively you need to understand the incident/impact
- Know how to report cyber incidents – NCDIT Incident Reporting
- Develop processes/procedures to handle a variety of incidents
- Practice incident response

Building a Resilient Cybersecurity Program

Adapt

- In this Exponential Age, *situational awareness* is critical – and it must be intentional. You can't adapt if you don't know what is changing.
  - ✓ Cybersecurity & Infrastructure Security Agency (CISA) – website shows recent vulnerabilities, threat analysis reports, and an alert system that sends the latest information to you via email. https://us-cert.cisa.gov/
  - ✓ Federal cyber regulations, Executive Orders, CyberSpace Solarium Commission Report, MITRE ATT&CK framework, etc.

Building a Resilient Cybersecurity Program

Adapt

- Implicit in adaptation is *continuous improvement* – understanding how the new information/technology impacts your organization then determining how to incorporate it into your current system – AND learning from cyber incidents.

Building a Resilient Cybersecurity Program

Rapidly Recover

- Easier to recover if you have good policies/procedures in place to provide direction
- Need to know what assets were lost/impacted (asset inventory)
- Have multiple back-ups with one being offsite
- Test back-up and restore process to make sure it works
- Perform a root cause analysis of the incident
- Lessons Learned meeting
- Incorporate information from root cause/lessons learned

Building a Resilient Cybersecurity Program

Key takeaways:

- Takes time – no quick fixes
- Team effort – not an IT task
- Should be “foundational” – just as important as cost, schedule and performance
- Should be approached holistically – not a checklist of controls
- Requires a change in culture – focus on continuous improvement
- ***May save your organization***

Building a Resilient Cybersecurity Program