AWARENESS, PREPAREDNESS, RESILIENCE AND OUTREACH + GA CYBER CENTER

RealTalk 2019

Agenda

- Intro and Overview
- Cyber Security v. Cybersecurity???
- Layered Architecture/Defense-in-Depth
- Cyber Kill Chain
- Left of Bang!
- Awareness, Preparedness and Resilience
- Georgia Cyber Center

BEGIN:

Cyber-Security or Cybersecurity or ???

Cyber-security is one of the most misused terms in technology today and the misunderstanding that it causes can create problems.

Security and risk management leaders must agree on what cybersecurity means to address the risks and threats of digital transformation.

- UNKNOWN

OPENING

- Cyber-Security is:
  - Protecting information and information system in whatever form and wherever…
  - Protecting the user, the app, the data, the system, the cloud and the network.

THINK IN ABSTRACT!

LAYERED ARCHITECTURE OR DEFENSE-IN-DEPTH

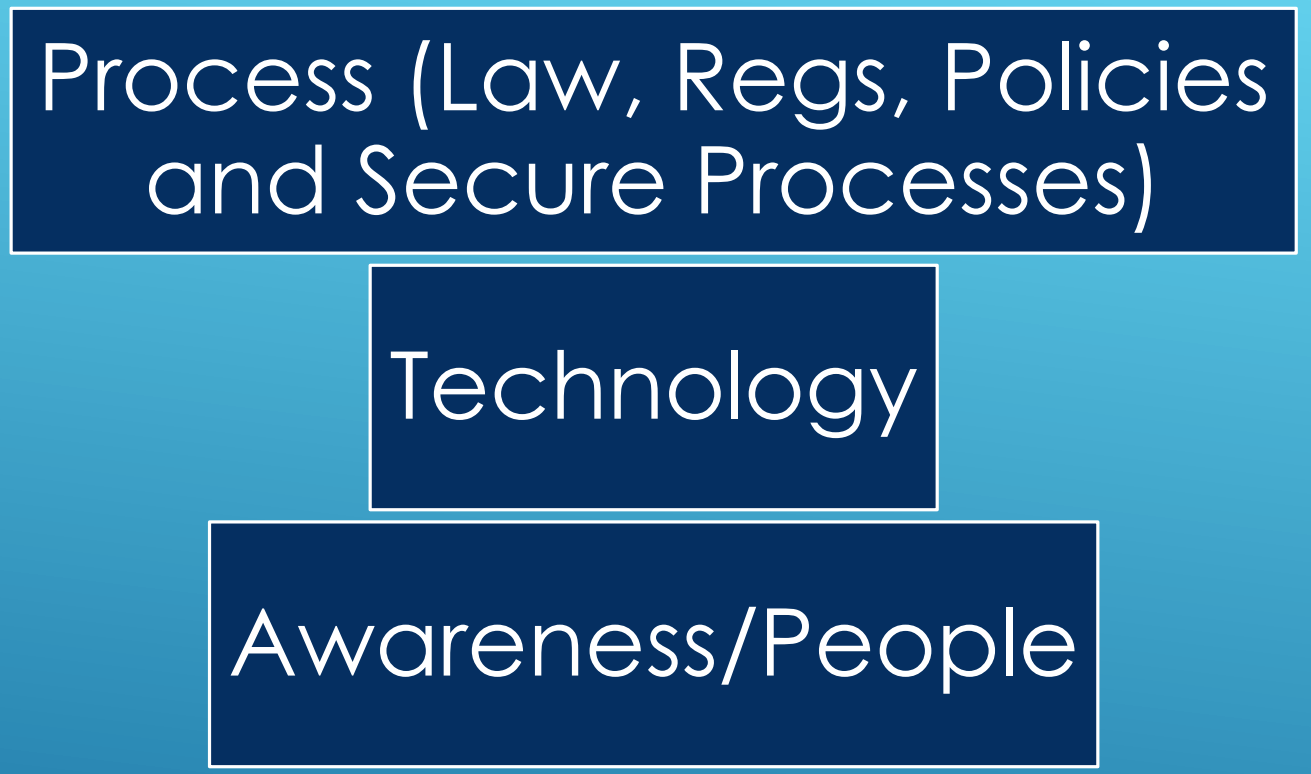
For 25+/- Years

CYBER-SECURITY MUST EVOLVE, AND MATURE

Layered Architecture + Defense-in-Depth

Process, Technology and People

Maturing Cyber Protection Methods



TYPICAL DEFENSE-IN-DEPTH AND LAYERED ARCHITECTURE

- And, we have gotten very/very good at reacting to attacks and breaches…

AND STILL, THERE IS NO SUCH THING AS 100% SECURE…

HOW ARE THEY GETTING IN?

Remember: security is a process; not a product…

THE "CYBER KILL CHAIN"

CYBER KILL CHAIN

Military Term - It's part of an intelligence model for the identification and prevention of cyber intrusions activity.

How does it work - A 7-Step process which identifies what the adversaries must complete in order to achieve their objective.

(developed by Lockheed Martin)

LEFT OF BANG: CYBER SECURITY

1. **Reconnaissance**
    1. Port scanning, gathering and recon to obtain info…
2. **Weaponization**
    1. Develop weapon(s) specific to target
3. **Delivery**
    1. Delivery, involves transmitting the APT code from the attacker to the target information system for exploitation.
4. **Exploitation**
    1. Execute APT on the target
5. **Installation**
    1. APT installs itself on target and proceeds to download additional SW
6. **Command & Control (C2)**
    1. APT + system + North, South, East and West
7. **Action on Objective**

STAGES 1-7

IF YOU UNKNOWINGLY ALLOW AN APPLICATION TO BE INSTALLED ON YOUR YOUR SYSTEM

It's not your system anymore…

MODIFY DEFENSE-IN-DEPTH MODEL

Add More Awareness, Preparedness and Resilience

LEFT OF BANG! CYBER BANG THAT IS…

- It is recommended, strongly recommended that an organization implement a modified defense-in-depth strategy that will serve to protect the organization's people, process, and technology in a holistic and layered fashion.

DEFENSE IN DEPTH RECOMMENDATIONS

Proactive

Reactive

SOC, SIEM, Continuous Monitoring, Logging, Correlation, Threat Intel, CIS 20, Constant ATE, Testing/Exercising

Backups & Recovery Process, Cyber Incident Management, DRP, BCP and Business Resumption

LEFT OF BANG: CYBER SECURITY

- Situational Awareness
  - Originally a military term referring to a pilot's operational status and knowledge of immediate threats, today the term has broad applications in any environment, including "cyber-space". At its essence, situational awareness refers to real-time information about what's happening in and around a given physical, logical and human-element environment.
    - Awareness of your environment
  - Thinking in abstract
  - What is *NORMAL*?
  - Proactive v. reactive
- User Awareness: building knowledge, skills and abilities and is a continuum

AWARENESS

PREPAREDNESS

- **Cyber preparedness** in general is the process of ensuring that an agency, or organization has developed, tested, and validated its own capabilities to protect against, prevent, mitigate, respond to, and facilitate recovery from a significant **cyber** incident.
- Protection: People, Process and Technology

"Bad things happen to good people…"

- People, Process and Technology
  - Backups and Recovery
  - Cyber Incident Management Plan/Process
  - Disaster Recovery Plan
  - Business Continuity Plan
  - Business Resumption Plan

RESILIENCE

THE GEORGIA CYBER CENTER

Augusta Cyber Center

CYBER CENTER

- The Cyber Center is located on the Nathan Deal Campus for Innovation.
- Broke ground June 19, 2017, on the Georgia Cyber Center in Augusta
- $100 million and boasting 332,000 square feet in two adjacent buildings, the center is the single largest investment in a cybersecurity facility in the nation to date.
- Unique public/private partnership that includes Augusta University, Augusta Technical College, the University System of Georgia's research institutions, the City of Augusta, the Georgia Bureau of Investigation, the Georgia Department of Defense, and other state, federal, and private-sector partners working together to meet **workforce** demand.

- The center is helping fill the current and growing shortage of cybersecurity talent in the state and nation. The global cybersecurity labor shortage is predicted to hit 3.5 million unfilled jobs by 2021, up from one million openings in 2016. The U.S. alone is on pace to hit a half-million or more unfilled cybersecurity positions by 2021. (Source: Cybersecurity Ventures report, June 2017)

- 21st Century Workforce Training
- The Georgia Cyber Range
- GBI Cyber Crime Unit
- Partner Space
- Incubator/Accelerator
- Georgia's Research Universities Demonstration Space

RESOURCES

THE HULL MCKNIGHT BUILDING, FOREGROUND; THE SHAFFER MACCARTNEY BUILDING, BACKGROUND.

CONCLUSION

Q&A

- Left of Bang: Book by Jason A. Riley and Patrick Van Horne
- People, Process and Technology: **Bruce Schneier**
- Unknown; Unknowns: Donald Rumsfeld, US Secretary of Defense
- Center for Internet Security – CIS Controls: https://www.cisecurity.org/

CREDIT, AND READING SUGGESTIONS…

MORE AVAILABLE AT:

Georgia Cyber Security Workforce Academy

- **Learn, Hear, Discover and Get tips & techniques**