GWINNETT COUNTY
BOARD OF COMMISSIONERS

75 Langley Drive | Lawrenceville, GA 30046-6935
O: 770.822.7000 | F: 770.822.7097
GwinnettCounty.com

Nicole L. Hendrickson, Chairwoman
Kirkland Dion Carden, District 1
Ben Ku, District 2
Jasper Watkins III, District 3
Marlene M. Fosque, District 4

Official

Informal Presentation Minutes

Tuesday, March 15, 2022 – 3:00 PM

Present: Nicole L. Hendrickson, Kirkland D. Carden, Ben Ku, Jasper Watkins III, Marlene M. Fosque

1. **Information Technology Services**
   Cybersecurity Posture
   Information Technology Services Director Dorothy Parks and Deputy Director of Cyber Security Matthew Puckett provided information on the County's IT security framework, challenges, and future plans. The Board also discussed the County's equity plan and procurement process. No official action taken.

Gwinnett

BOC Security Briefing

March 15, 2022

Agenda

- Metrics
- Program history
- Current team
- Core responsibilities
- CIS Framework and Progress
- 2022 Plans
- Challenges
- Russia and Ukraine situation
- Final thoughts

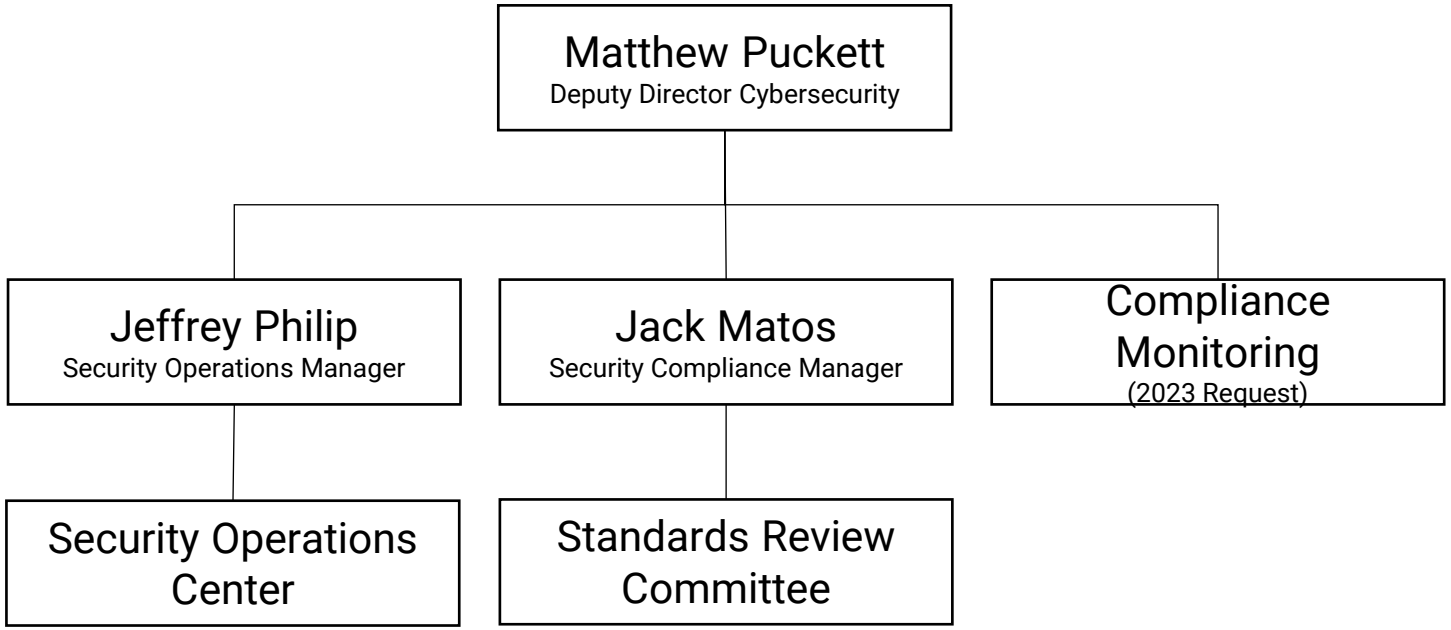
Metrics

- 4,000 emails a month are blocked because they are phishing or contain viruses.
- In the last 6 months Windows Defender has blocked 31 Medium or High threats, including 4 cases of suspected ransomware.
- Our security team and third-party monitoring service analyzes 1500 potential incidents per month.

Program History

- Started in March of 2018
- Currently consisting of 5 FTEs and 6 contractors
- 4 open positions as a result of 2022 decision packages
- Major projects
  - Monitoring
  - Vulnerability management
  - Multi-Factor Authentication (MFA)
  - Phishing simulations

Current Team



Core Responsibilities

- Security Operations Team
  - Identify and track system vulnerabilities
  - Conduct phishing training exercises
  - Internally or with third-party vendors try to break into our own systems
  - Provide technical input into systems designs and changes to mitigate risk
  - Security Operations Center
    - Currently handled by a third-party service, contract expires this month
    - Monitors the environment for potential attacks
    - Stays current on new attacks and how we can adapt our defenses

Core Responsibilities

- Compliance Team
  - Annual Payment Card Industry (PCI) compliance, which allows the County to accept credit cards
  - Criminal Justice Information Systems (CJIS) compliance, required by the GBI / FBI for the County to access criminal just information
  - Health Insurance Portability and Accountability Act (HIPAA) requires the County to reasonably protect health data
  - Review of purchases and vendor relationships for potential security risks
  - Development of internal standards
  - Conduct risk assessments and access reviews
  - Training and awareness

Security Framework

- Frameworks provide a reference point
  - What does complete security program look like?
  - How mature is our program?

- Two popular frameworks
  - National Institute of Science and Technology (NIST) created by the Federal Government
  - Center for Internet Security (CIS) Controls created by CIS which is a non-profit government and private industry partnership

Security Framework

- Gwinnett uses the CIS Framework
  - Easier to communicate
  - Free tools that assist us in tracking progress
  - Increasingly used by threat intelligence briefings

- Version 7 consists of 168 controls* grouped into 20 groups

- Controls are prioritized by recommended importance and then categorized by resources available

* “Control” refers to a specific action we take to reduce risk, such as requiring Multi-Factor Authentication

CIS Framework

1. Hardware inventory
2. Software inventory
3. Vulnerability Management
4. Administrative Privileges
5. Secure configuration of computers
6. Maintenance and logging
7. Email and Web protection
8. Malware defenses
9. Network port control
10. Backups
11. Secure configuration of network hardware
12. Firewalls
13. Data protection
14. Least privilege access
15. Wireless access control
16. Account monitoring and control
17. Security training
18. Application development security
19. Incident Response
20. Penetration testing

Security Framework Progress

Status	March 2018	March 2022
Not implemented or NA	96	52
Partially implemented	42	31
Implemented on most or all systems	30	85

CIS Framework – Strongest Areas

1. Hardware inventory
2. Software inventory
3. **Vulnerability Management**
4. Administrative Privileges
5. Secure configuration of computers
6. Maintenance and logging
7. Email and Web protection
8. **Malware defenses**
9. Network port control
10. **Data Recovery (Backups)**
11. Secure configuration of network hardware
12. Firewalls
13. Data protection
14. Least privilege access
15. Wireless access control
16. Account monitoring and control
17. Security training
18. Application development security
19. Incident Response
20. Penetration testing

CIS Framework – Weakest Areas

Gwinnett

1. Hardware inventory
2. Software inventory
3. Vulnerability Management
4. Administrative Privileges
5. Secure configuration of computers
6. Maintenance and logging
7. Email and Web protection
8. Malware defenses
9. Network port control
10. Backups
11. Secure configuration of network hardware
12. Firewalls
13. **Data protection**
14. Least privilege access
15. Wireless access control
16. Account monitoring and control
17. **Security training**
18. Application development security
19. Incident Response
20. **Penetration testing**

2022 Plans

- Heightened focus on awareness and training
  - Increased communication with department directors and elected officials
  - Annual training for employees

- Continued improvements of our Security Operations Center
  - Conduct tabletop exercises for responding to cyber incidents
  - More penetration testing via Homeland Security and American Rescue grant funding

- Deployment of Microsoft tools which will allow for increased management of user access and data protection

Challenges

- Extremely competitive job market for cybersecurity talent due to shortages
  - ISC² (a security certification organization) estimates that in 2021 there were 377,000 more cybersecurity positions than qualified individuals in the US
- Rapidly evolving threats against a constantly changing environment
- Navigating the autonomy of other elected offices
- Threat of nation state actors
  - Resources to “invent” new attacks and exploits
  - Patience, not always driven by financial motives

Russia and Ukraine

- Federal government has issued multiple advisories regarding potential Russian cyber attacks
- Guidance suggests carrying increased operational risk
- Past cyber attacks may have been preparation for situations like this
  - Solarwinds
- Focus will be on maximum disruption
- Disinformation campaigns are likely

Final Thoughts

- There has been a lot of progress, but there is still work to be done
- Request: Take advantage of opportunities to promote cybersecurity as a County priority
- Mistakes will happen
  - “The culture of organizations influences the willingness of personnel to communicate potential threat and vulnerability information, which ultimately affects the quality and quantity of the threats/vulnerabilities identified.” - (NIST SP800-39 Managing Information Security Risk)

Questions?