NEW YORK
STATE OF
OPPORTUNITY.

NY Power
Authority

MINUTES OF THE REGULAR JOINT MEETING
OF THE
CYBER & PHYSICAL SECURITY COMMITTEE
January 30, 2019

Table of Contents

January 30, 2019

Minutes of the regular joint meeting of the New York Power Authority and Canal Corporation's Cyber and Physical Security Committee held at the Authority's offices at 123 Main Street, White Plains, New York at approximately 9:15 a.m.

Members of the Cyber & Physical Security Committee present were:

Michael Balboni - Chairman
John R. Koelmel
Eugene L. Nicandri
Tracy B. McKibben
Dennis G. Trainor

Also in attendance were:

Gil Quiniones	President and Chief Executive Officer
Justin Driscoll	Executive Vice President and General Counsel
Joseph Kessler	Executive Vice President and Chief Operating Officer
Angela Gonzalez	Senior Vice President Internal Audit
Robert Piascik	Senior Vice President & Chief Information Officer
Karen Delince	Vice President and Corporate Secretary
Kenneth Carnes	Vice President – Critical Secure Services and Chief Information Security Officer
Daniella Piper	Vice President – Digital Transformation/Chief of Staff
Saul Rojas	Vice President – Technical Compliance
Victor Costanza	Senior Director – Configuration Control and Deputy CISO
Lawrence Mallory	Senior Director – Physical Security & Crisis Management
Thomas Spencer	Senior Director of Enterprise Risk and Corporate Insurance
Lorna Johnson	Senior Associate Corporate Secretary
Sheila Quatrocci	Associate Corporate Secretary

Chairman Balboni presided over the meeting. Corporate Secretary Delince kept the Minutes.

Introduction

Committee Chair, Michael Balboni, welcomed the committee members, Eugene Nicandri, Tracy McKibben and Dennis Trainor and the Authority's senior staff to the meeting. He said that the meeting had been duly noticed as required by the Open Meetings Law and called the meeting to order pursuant to Section B(4) of the Cyber and Physical Security Committee Charter.

1. Adoption of the January 30, 2019 Proposed Meeting Agenda

Upon motion made by member John Koelmel and seconded by member Dennis Trainor, the agenda for the meeting was adopted.

2. Motion to Conduct an Executive Session

I move that the Committee conduct an executive session pursuant to the Public Officers Law of the State of New York §105 to discuss matters regarding public safety and security. Upon motion made by member Tracy McKibben and seconded by member John Koelmel, an Executive Session was held.

3. Motion to Resume Meeting in Open Session

I move to resume the meeting in Open Session. Upon motion made by member John Koelmel and seconded by member Tracy McKibben, the meeting resumed in Open Session.

Chairman Balboni said no votes were taken during the Executive Session.

4. CONSENT AGENDA

Upon motion made by member Eugene Nicandri and seconded by member John Koelmel, the Consent Agenda was adopted.

a. Adoption of the Meeting Minutes of August 7, 2018

Upon motion made and seconded, the Minutes of the joint NYPA/Canal Corporation meeting held on August 7, 2018 were unanimously adopted.

5. DISCUSSION AGENDA

a. 2019 Q1 Security Briefing

Mr. Kenneth Carnes, Vice President of Critical Secure Services and Chief Information Security Officer and Mr. Lawrence Mallory, Senior Director of Physical Security & Crisis Management provided an overview of the security posture for NYPA (Exhibit "5a-A").

Mr. Carnes discussed some of the threats targeting the utility industry and the Authority's 2019 plan for investments to improve cyber security and continue to stay proactive and ahead of the curve in 2019 and beyond. He said an article titled the "*Chief Information Security Officer Priorities for 2019*" was released by Forbes in January, and highlighted the following points from that article as it relates to NYPA:

1. *Gain threat visibility across all platforms*

NYPA have been investing significantly in visibility since 2017, making sure that it has the capability to see risks throughout its environment.

2. *Understanding the new perimeter*
   - NYPA understands that its identity is the new perimeter.
   - As NYPA goes digital, it is going to have more end-points.
   - NYPA does not have the historical single-edge entry point that it had to deal with in the past.

3. *Nurture a culture of security*

NYPA has revamped its entire security awareness program and is pushing a program of NYPA secure.

4. *Align security operations with IT operations*

In October, NYPA made some IT organizational changes. NYPA combined the IT operations with the Network Operations, Security Operations and iSOC groups. In addition, NYPA incorporated all of the IT operation functions and compute servers with cyber security.

5. *Addressing risks from inside the firewall*

NYPA manages security in the cloud and plans to continue to monitor and leverage the risks.

Mr. Carnes then highlighted the four main areas and the partnerships that NYPA leverages:

1. Monitoring – Internal and External
   - Threat Vulnerability Management Program
   - Continuous External Scanning – NYPA leverages external scanning, automated indicators of compromise, and its partners.
   - Continuous Logging & Monitoring – NYPA leverage threats, both internal and external, to make sure it is looking threats from all directions.

2. Partnerships – state, local, federal, and industry
   - State Partnerships – NYPA partnered with the State Homeland Security, and is also working on some efforts with the State National Guard for cyber mutual aid. In addition, NYPA is working with the State Security Working Group and completed a drill with the NYISO late last year.

   - Information sharing – Information sharing is continuous. This enables NYPA to know what others are seeing and how to make sure its environment is seeing any targeting that is pointed towards it.

- Industry Focused Partnerships – Partnerships with sector specific industries such as the Electric Subsector Coordinating Council; the Electric Power Research Institute; and NERC, the regulator for NYPA's bulk electric system.

3. Exercises – Internal and External
   - Response – NYPA partners with Emergency Management, Physical Security, IT and OT for cross-functional hazard drills to make sure that it has a response in place for any scenario whether generated from a cyber attack or a weather event.

   - Training – Annual Staff Technical Training / NERC CIP Site Drills and Manual Control Exercises in order to get IT staff trained and making sure that they are up-to-date on what is targeting industrial control systems.

   - Black Start – NYPA partnered with the Department of Energy for the Liberty Eclipse drill.

     NYPA is also a part of the planning group to support Grid X, a bi-annual drill that is completed by the electric sector information sharing analysis center, a subset of NERC. NYPA plans to participate in the next drill in November.

4. Assessments – Internal and External
   - Continual Improvement – assessment exercises are conducted to verify the environment and security posture throughout NYPA.
   - Frequent External Penetration Testing – Red Team Exercises

Cyber Security – 2019 Look Ahead

2019 Predictions and things to watch:

- New Zero Trust Models – Zero Trust model came out in 2010. However, technology has not caught up to it to be able to build it into NYPA's environment. Staff is working on implementing this model with segmentation and micro segmentation.

- Managed Service Provider Attacks – the Department of Homeland Security indicted some attackers towards Managed Service Providers earlier this year. NYPA will have to leverage more cloud services.

- Supply Chain Attacks – Staff is making sure that it is adequately managing vendor partnerships through its supply chain process. This will include increasing NYPA's vendor risk management, vendor controls, and also its cyber risk assessment processes for everything that is bought and implemented at the Authority.

- AI based Attacks will continue to grow as machines get more capable to carry out attacks and take what they have learned from feedback and adjust and continue to modify.

- Nation/State Actions – Staff will focus on making sure that the Authority have the machine capabilities along with the human interaction to support and guide the Intel that is collected in the Authority's environment. Moreover, these actions have been in the press repeatedly from adversaries of the US.

2019 Investments

- IT/OT Visibility – Staff is working on some innovative pilots to increase visibility in the Authority's environment to make sure that they are aware of any attack or intrusion of any type within the Authority's environment.
- Segmentation – Staff is building on the Zero Trust model, creating risk-based micro segments.
- Access Anywhere – Enhancing the Authority's digital worker, making sure that we are pushing the capabilities of technology in our digital vision, and making sure it is delivering what people are looking for, and providing the security as a basis in all of that work.

Security – What is changing?

The SANS Sliding Scale of Cybersecurity created by Rob Lee, a past NSA analyst, shows a scale of where capability is in an environment or a defensive posture in cyber security.

- Architecture – Planning, establishing and upkeep of systems, putting controls in place to prevent access; and putting security like firewalls and other defenses in place for cyber security.
- Passive defense – Architecture to provide reliable defense of insight without human interaction.
- Active Defense – Analyst monitoring for responding to, and learning from information. NYPA sees a value in greater investment into cyber security. To that end, last year, NYPA invested in developing capabilities, skills and training of staff focusing on defense.
- Intelligence – NYPA will continue to push its capabilities, skills and training to become more intelligent in how it operate and gather intelligence in the future – Collecting data, exploiting it into information and producing intelligence to make sure the Authority's environment stays secure and resilient.
- Offence – Legal countermeasures and self-defense actions against an adversary.

Staff is leveraging a model designed by MITRE that focuses on the techniques and procedures of an adversary including their tradecraft of cyber entry and mitigation.

Staff is designing a security control implementation strategy around the MITRE model, building it into the Authority's environment, daily posture, and processes to ensure that the Authority have visibility no matter what the threats might be or how they change.

NYPA will maintain focus on its standard security architecture and security controls leveraging the MITRE ATT&CK Model in order to increase its cyber detection capabilities.

6. Next Meeting

Chairman Balboni said that the next regular meeting of the Cyber and Physical Security Committee is to be determined.

Closing

Upon motion made by member Tracy McKibben and seconded by member John Koelmel, the meeting was adjourned by Chairman Balboni at approximately 9:57 a.m.

Karen Delince

Karen Delince
Corporate Secretary

CYBER & PHYSICAL SECURITY COMMITTEE

EXHIBITS

For

January 30, 2019

Meeting Minutes

NEW YORK
STATE OF
OPPORTUNITY™

NY Power
Authority

2019 Q1 Security Briefing

Cyber Security | Physical Security | Compliance | Emergency Management

Kenneth Carnes - VP Critical Secure Services & Chief Information Security Officer

Readiness – Preparedness / Information Sharing / Assessments

Monitoring

Internal | External | Both

- Threat Vulnerability Management Program
- Continuous External scanning | Automated Indicators of Compromise
- Continuous Logging & Monitoring 24x7 Security monitoring and response

Partnerships

State & Local | Federal | Industry

- State Partnerships –Homeland Security | National Guard | Security Working Group
- Information Sharing - Federal Partners | Information Sharing & Analysis Centers | State Fusion Center
- Industry Focused Partnerships – Sector specific Agencies like Electric Subsector Coordinating Council| EPRI | NERC

Exercises

Internal | External

- Response – Cross functional All Hazards drills | Quarterly Cyber Incident Response Drills
- Training - Annual Staff technical training | NERC CIP site drills | Manual Control Exercises | Purple Team Exercises
- Black Start / Significant Impact - GRID Ex | Liberty Eclipse | NY State Exercise

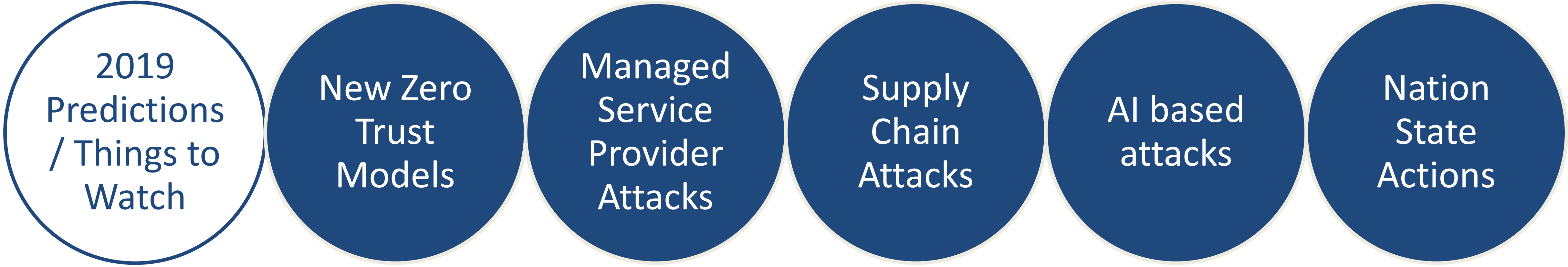
Assessments

Internal | External | Both

- Assessment tools – NIST CSF | NREL C2M2 Assessment | LPPC Cyber Principles | NPCC Internal Controls
- Continual Improvement - Internal Audit | Cyber Hygiene | LPPC Cyber Principles | CIP Assessments
- Frequent External Penetration Testing | Red Team Exercises

NEW YORK STATE OF OPPORTUNITY. | NY Power Authority

Cyber Security – 2019 Look Ahead



2019 Predictions / Things to Watch

New Zero Trust Models

Managed Service Provider Attacks

Supply Chain Attacks

AI based attacks

Nation State Actions

2019 Investments

IT/OT Visibility

- Innovative Pilots
- Strengthen Security and Compliance
- Further iSOC integration

Segmentation

- Build on zero trust
- Create risk based microsegments
- Explore new methods to separate

Access Anywhere

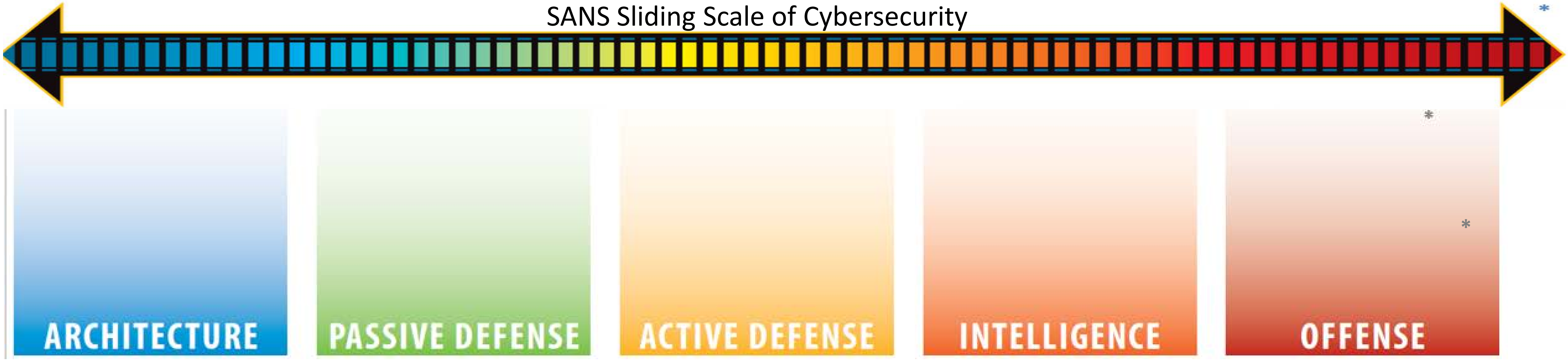
- Enhanced Multi-Factor
- Cloud Security
- Data Loss and Data Protection

Resiliency

- Continued Exercises
- Coordinated Response
- Standardized processes
- New Partnerships

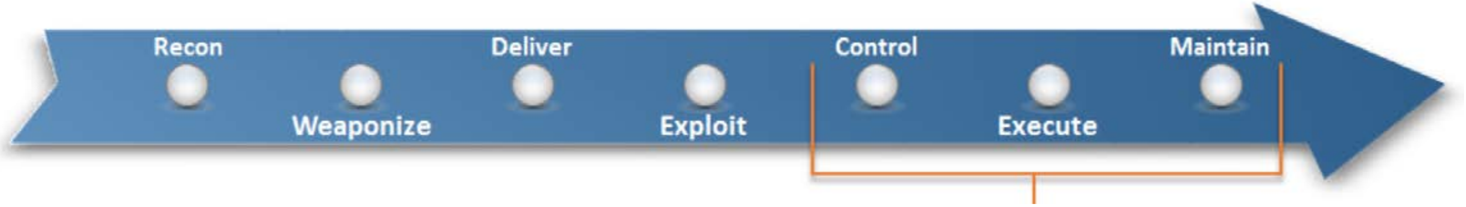
Security – What is really changing?

SANS Sliding Scale of Cybersecurity



ARCHITECTURE	PASSIVE DEFENSE	ACTIVE DEFENSE	INTELLIGENCE	OFFENSE
The planning, establishing, and upkeep of systems with security in mind	Architecture to provide reliable defense of insight without human interaction	Analysts monitoring for, responding to, and learning from information	Collecting data, exploiting it into information, and producing intelligence	Legal countermeasures and self-defense actions against an adversary

Continual improvement : NYPA's will maintain focus on our standard security architecture and security controls but leveraging the MITRE ATT&CK Model in order to increase our cyber detection capabilities



NEW YORK STATE OF OPPORTUNITY. NY Power Authority

* Sliding Scale Image referenced from SANS (text summarized for clarity)

*Image referenced from MITRE