Robert Galvin, Chief Technology Officer

The Port Authority of New York and New Jersey

Testimony for Joint Subcommittee Hearing “Enhancing Preparedness and Response Capabilities to Address Cyber Threats”, May 24, 2016

About the PA

The Port Authority of New York & New Jersey conceives, builds, operates and maintains infrastructure critical to the New York/New Jersey region's trade and transportation network. These facilities include America's busiest airport system, including: John F. Kennedy International, LaGuardia, and Newark Liberty International airports, marine terminals and ports, the PATH rail transit system, six tunnels and bridges between New York and New Jersey, the Port Authority Bus Terminal in Manhattan, and the World Trade Center. For more than ninety years, the Port Authority has worked to improve the quality of life for the more than 18 million people who live and work in New York and New Jersey metropolitan region.

I. It is important to keep the Authority up and running

The Authority operates a diverse groups of facilities that can have both logistic and economic impacts that can reach across the globe if the facilities were to be shut down by a cyber-attack. These facilities have implemented many different Internet based technologies to add efficiencies to how they operate. However, it is these technologies that make these facilities more vulnerable to cyber-attacks.

II. The Authority relies of its supply chain to operate

The Authority relies on its supply chain in two states (New York and New Jersey) in order to operate its facilities. Required resources are provided by multiple suppliers. If fuel cannot be provided, or if electricity is impacted in either state, the Authority cannot operate at full capacity. It is critical that these supply chains are resilient to cyber-attacks and have resilient business continuity plans.

III. The Port Authority takes Cybersecurity seriously and has an evolving program

The Port Authority takes Cybersecurity very seriously. In 2012, the Authority conducted an audit of its cybersecurity posture, and as a result, immediately started to build a Cybersecurity program. Working with a consultant to identify the requirements of our cybersecurity program, the authority decided to use the NIST SP 800-53 guidelines as a standard for organizing teams, and developing and implementing the program. Leveraging this existing standard created by a joint task for of NIST (National Institute of Standards and Technology), the Department of Defense, Department of Homeland Security, the Intelligence Community and the Committee on National Security systems saved The Port Authority time and effort we otherwise would have had to develop a framework implementing cybersecurity.

The first step the Authority took to advance the cyber security program was to implement services from MS-ISAC (Multi-State Information Sharing and Analysis Center). MS-ISAC analyzes all the logs generated by our perimeter security tools and provides the authority visibility into potential indicators of compromise.

The Authority built and staffs a 24x7 Cybersecurity Operations Center (CSOC) that responds to all of the alarms generated by our cybersecurity tools, and to alerts received from the agency partners and cybersecurity services.

We created and manage a mandatory cybersecurity awareness and training program for all staff who access the authority's computing resources.

Through this process, Port Authority developed and maintains strong partnerships with DHS, FBI, NYPD, NJSP, MS-ISAC (multi-state information sharing and analysis centers), US-CERT, and ICS-CERT. We continue to engage these agencies to perform vulnerability assessments and to assist with incident response. We also strengthened internal partnerships within the Port Authority between the Chief Security Office, Office of Emergency Management, Office of Inspector General and the Technology departments. Early on we recognized that no one team or group would have the total solution.

From these efforts, the Port Authority has seen positive results, but much work remains to protect critical assets. The technology we put in place provides visibility into emerging threats and have shown results, such as the ability to detect and automatically block 90% of critical incidents. We continue to make improvements in our cybersecurity operations. Last year, we reduced our critical incident response time by 1/3 over the previous year.

However, just as the technology sector continuously innovates, criminal organizations, nation-states, and hacktivists are also innovating their methods for exploiting vulnerabilities presented by new technologies, "apps", and new attack surfaces like the Internet of Things.

IV. The Port Authority's Biggest Cybersecurity Concerns

- Like many organizations, The Port Authority uses a large number of ICS (Industrial Control Systems) to operate its facilities, for example: tunnel ventilation systems, PATH Train Control Systems and Airport Airfield Lighting Systems. Some of these systems, if compromised, could cause loss of life. This year, the Authority initiated a program to better understand our vulnerabilities and properly patch and mitigate these systems. But, it is an enormous task.
- In order to properly respond to a massive cyber-attack or the breach of a partner organization, the PA must be in communication with partner organizations in real-time and have specific remediation actions or practices to follow. Today's ISACs while useful, do not provide such real-time breach notification. According to Verizon's 2015 Data Breach Investigations Report, 75% of attacks spread from the first victim to the second victim within 24 hours, and 40% spread from the first victim to the second in one hour.

- In order to operate all these diverse facilities and business functions, the Agency hires thousands of contractors. These individual have access to some of our most critical systems. The Authority has recognized that insider threat is potential attack vector.
- The Authority invests in resources and money to implement cybersecurity tools. We have learned from telecommunications carriers and cybersecurity service providers that it is possible for aggressive nation-states to obtain these tools through third parties and to reverse engineer them to determine how these detection and prevention tools may be circumvented.

V. How can the Federal Government help?

- **Education:** I think there is a clear role for the Federal government to play by launching a massive public education campaign to practice "Safe Computing". The weakest link in our cybersecurity chain is the end user. Phishing scams, e-mails with links to malevolent sites are often the first step toward a breach. Two-thirds of cybersecurity incidents that fit a pattern of cyber-espionage feature phishing scams. (DBIR, 2015). Raising our internal education & awareness level was a crucial step in improving the security posture at the Port Authority. I think PSAs (public service announcements) to inform the public about how technology works, responsible measures such as good passwords, "Think before your click" and other safe computing practices should be taught to the American public, beginning in school.
- **Communication**: Events such as today's, not built around an incident or a breach, but a conversation between technology and policy makers to reach understanding go a long way to help both technologists and our government make better decisions. Government and technology leaders need to work together to create safe forums to discuss prevention strategies and de-construct cybersecurity incidents. The Federal government can conduct in depth reviews following an organizational breach, similar to the investigations conducted following plane crashes or what hospitals do after a medical mistake. These non-punitive approaches have been very successful improving airline safety and in reducing medical mistakes in the hospitals and emergency rooms – I would think it could have a significant impact improving cybersecurity. The name of the breached organization could be withheld, and the Federal government can inform agencies of findings and recommendations after completing the review. Case studies provide more than technical remediation requirements; they inform industry how to prevent problems over the long term.
- **Simulations:** The Federal government can assist the PA and related agencies by coordinating an exercise or drill simulating a large scale Cybersecurity event. This drill would allow the agencies to understand where our deficiencies lie, and whether we have the right procedures and external relationships in place to respond correctly. For example, the operations of the Port Authority rely on several Federal Agencies: the CBP (Customs & Border Protection), TSA, FAA. If their systems were compromised, the impact on the Port Authority would be substantial. if the TSA cannot perform pre-screening, we cannot board passengers, if the CBP cannot review manifests, we cannot transport cargo, if the FAA air traffic controllers are

impacted, our regional airports can be shut down. The operational stability of these Federal entities has a direct impact on the Port Authority's ability to provide services to the region. Post-drill, the Fed can assist the agencies to ensure that their comprehensive cybersecurity programs and resilient business continuity plans are complete and coordinate with related agencies.

- Consider oversight of cybersecurity tool developers to ensure their intellectual property is not compromised. The Authority, like many public and private sector organizations, invests resources and money into their cybersecurity tools. If aggressive nation-states obtained these same tools through third parties and reverse engineered them to determine how they can be circumvented, the protection we seek from cybersecurity tools would be lost. The tech industry and federal government must work together to protect the intellectual capital that represents the vanguard of our security apparatus for it to operate effectively. The Federal government may be able to provide oversight of the developers of cybersecurity tools to ensure that they are not sold to malicious third parties.
- Consider stopping the Federal government's participation in "bug bounty" programs which encourage grey hat hackers to sell zero-day vulnerabilities to the highest bidder. The amount governments are willing to pay for some vulnerabilities inflates their value and creates a potentially lucrative secondary market for trading vulnerabilities and may even encourage programmers to 'build in' vulnerabilities they can later sell.

VI. Challenges related to planning for, and responding to, Cybersecurity

The first challenge of planning for Cybersecurity is the wide variety of threat scenarios an organization must plan for: viruses, ransomware, hacktivists, nation-states, simple human error, Point-of-Sale intrusion, payment card skimmers, web app attacks, denial-of-service attacks, and cyber-espionage.

The second challenge is the size, configuration and expanding nature of the attack surface: Internet presence (websites), internal network, desktops and servers, cloud based software systems & file storage, public WiFi infrastructure, portable storage devices, VOIP systems, and the looming Internet of Things. This list includes the traditional boundary of the organization. However, we are seeing a common entry point into an organization being the subcontractors and consultants who bring equipment onsite or connect their organization's networks to provide services. The computing networks and infrastructure of suppliers who provide critical support services to an organization should be considered part of any organization's 'attack surface' that could be exploited by a malevolent entity.

Another challenge is the speed with which threats evolve and time required to detect a breach before damage can be done. This is often referred to the "volume, velocity, and variation" of malware. At a high level, there are approximately 5 malware events globally every second (170 million in 2015). Most of this is filtered out by an organization's firewalls and other cybersecurity technology, but half of all organizations discover malware during 35 or fewer days per year. This seems to align with 'releases' of malware during specific periods, rather than all year long. As for variation, 70-90% of malware samples in 2015 were unique to the organizations in which they were found. This combination shows that adversaries are getting more sophisticated to overcome defenses and more targeted in their approaches.

Technology Glossary

Backdoor - is a method, often secret, of bypassing normal authentication in a product, computer system, cryptosystem or algorithm etc. Backdoors are often used for securing unauthorized remote access to a computer, or other systems.

Computer Viruses - are a malware that, when executed, replicates by reproducing itself or infecting other programs by modifying them. Infecting computer programs can include as well, data files, or the boot sector of the hard drive. When this replication succeeds, the affected areas are then said to be "infected".

C*omputer worm* - is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Cyber-attack - is any type of offensive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system.

Cyber-espionage - is the act or practice of obtaining secrets without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet, networks or individual computers through the use of cracking techniques and malicious software including Trojan horses and spyware. It may wholly be perpetrated online from computer desks of professionals on bases in faraway countries or may involve infiltration at home by computer trained conventional spies and moles or in other cases may be the criminal handiwork of amateur malicious hackers and software programmers.

Cybersecurity - is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide.

Denial-of-service (DoS) attack - is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

Distributed denial-of-service (DDoS) - is where the attack source is more than one, often thousands of, unique IP addresses. It is analogous to a group of people crowding the entry door or gate to a shop or business, and not letting legitimate parties enter into the shop or business, disrupting normal operations.

Dox - is the Internet-based practice of researching and broadcasting personally identifiable information about an individual. The methods employed to acquire this information include searching publicly available databases and social media websites (like Facebook), hacking, and social engineering. It is closely related to internet vigilantism and hacktivism.

Email spoofing - is the creation of email messages with a forged sender address. Because the core protocols do not have any mechanism for authentication. It can be accomplished from within a LAN (Local-Area Network) or from an external environment using Trojan horses.

Firewalls - is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted.

Grey Hat Hackers - describes a hacker who exploits a security weakness in a computer system or product in order to bring the weakness to the attention of the owners. Unlike a black hat, a gray hat acts without malicious intent.

Hacking - a hacker is someone who seeks and exploits weaknesses in a computer system or computer network. Hackers may be motivated by a multitude of reasons, such as profit, protest, challenge, enjoyment, or to evaluate those weaknesses to assist in removing them.

Hacktivism - (a portmanteau of *hack* and *activism*) is the subversive use of computers and computer networks to promote a political agenda. With roots in hacker culture and hacker ethics, its ends are often related to the free speech, human rights, or freedom of information movements.

Hashing – (cryptographic hash function) is a hash function which takes an input (or 'message') and returns a fixed-size alphanumeric string, which is called the hash value (sometimes called a message digest, a digital fingerprint, a digest or a checksum).

Information systems - is any organized system for the collection, organization, storage and communication of information. More specifically, it is the study of complementary networks that people and organizations use to collect, filter, process, create and distribute data.

Internet of Things - is the network of physical objects—devices, vehicles, buildings and other items—embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data.

Malware - is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software.

Phishing – emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

Ransomware - is a type of malware that can be covertly installed on a computer without knowledge or intention of the user that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction. Some forms of ransomware systematically encrypt files on the system's hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying.

Rainbow table - is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a plaintext password up to a certain length consisting of a limited set of characters. It is a practical example of a space/time trade-off, using less computer processing time and more storage than a brute-force attack which calculates a hash on every attempt, but more processing time and less storage than a simple lookup table with one entry per hash. Use of a key derivation function that employs a salt makes this attack infeasible

Salt - is random data that is used as an additional input to a one-way function that "hashes" a password or passphrase. The primary function of salts is to defend against dictionary attacks versus a list of password hashes and against pre-computed rainbow table attacks. A new salt is randomly generated for each password. In a typical setting, the salt and the password are concatenated and processed with a cryptographic hash function, and the resulting output (but not the original password) is stored with the salt in a database. Hashing allows for later authentication while protecting the plaintext password in the event that the authentication data store is compromised.

Spear phishing - is an email that appears to be from an individual or business that you know. But it isn't. It's from the same criminal hackers who want your credit card and bank account numbers, passwords, and the financial information on your PC.

Spyware - is software that aims to gather information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge

Trojan horse - is a program that seems to be doing one thing but is actually doing another. It can be used to set up a back door in a computer system, enabling the intruder to gain access later. (The name refers to the horse from the Trojan War, with the conceptually similar function of deceiving defenders into bringing an intruder into a protected area.)

VOIP systems - Voice over IP (VoIP) is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet.

Watering Hole - is a computer attack strategy, in which the victim is a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some member of the targeted group gets infected.

Zero-day vulnerability - refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it—this exploit is called a zero-day attack.

Reading List

Verizon Data Breach Investigations Report, 2016

http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

Verizon Data Breach Investigations Report, 2015

http://www.verizonenterprise.com/verizon-insights-lab/dbir/2015/

Target Breach Shows well-trained staff is best defense against Cyberattacks, Minneapolis Star-Tribune, 5/17/2016

http://www.startribune.com/reporter-who-wrote-about-target-breach-says-well-trained-staff-is-best-defense-against-cyberattacks/379831601/

Countdown to Zero Day, Kim Zetter, ISBN 987-0-7704-3619-3, 2014