NEW CONTEXT
New Context Services, Inc
717 Market Street, Suite 200, San Francisco, CA 94103

Senate Committee on Energy and Natural Resources
Full Committee Hearing to Examine Cyber Technology and Energy Infrastructure
October 26, 2017

Chairperson Murkowski, ranking member Cantwell, and the other members of the committee, it's an honor and a privilege to testify before you today. My name is Daniel Riedel, and I'm the CEO and Founder of New Context Services. New Context was founded in 2013 with the vision of keeping the connected world safe. Our mission is to use Lean Security to automate the orchestration, governance, and protection of critical infrastructure.

For the past three years we have been working closely with Southern California Edison, Pacific Gas and Electric, and San Diego Gas and Electric, in partnership with Idaho National Lab and Lawrence Livermore National Lab, to assist in advanced cyber-security research for machine-to-machine threat detection and response within the energy industry. This project is referred to as California Energy Systems for the 21st Century. That work has resulted in our involvement in the STIX/TAXII and OpenC2 standards that are becoming the default for governmental agencies, enterprises, and information sharing communities (ISAOs & ISACs) to distribute cyber-threat intelligence rapidly.

Beyond working with utility companies, New Context offers secure engineering services to many industrial and financial service firms, to build and scale their infrastructures securely through our methodology, Lean Security.

There are five areas of advanced cyber-defense that I will be discussing in my testimony:

- Identity
    - Advancing authentication credentials by moving beyond static username and password, with just one other factor (commonly referred to as two-factor authentication) to multi-factor biometric and continuous authentication solutions.
- Trusted Data
    - Looking at advanced ways of using a cryptographic ledger to be able to secure and validate that data has not been manipulated. Additionally, cryptographic ledgers allow for the ability to assure data across multiple third party organizations and supply chains. This is popularly referred to as blockchain.
- Attributed Isolated Networks
    - Isolated networks have helped in protecting data, but they are still a hard outer shell, and many of the vulnerabilities that affect the public internet exist within those networks, from credential theft to malicious network activity. Advancing technologies and software to ensure that every actor is accounted for on that network creates a higher level of assurance that doesn't exist today.

- Threat Detection & Sharing
    - Machine speed threat detection and threat sharing, enables the ability to identify and respond to threats faster, and to share intelligence with other utilities, agencies, and organizations in near real time.
- Automated Response & Remediation
    - This is the ability for the grid to automatically take action to prevent potential devastating consequences to itself. Automated remediation is a key technology we are developing, it allows the grid to self heal in the event of well orchestrated cyber attack. If we are to continue to innovate and add new intelligent devices to the energy grid, we have to allow for automated response as the complexity will surpass the human ability to respond.

In the next few years, 20 billion IoT devices will be connected to the internet, and powered up to continue the support and grow of our economy and society. At the same time, Smart Grid technologies are being rolled out to utilities to modernize the energy grid. Organizations such as General Electric, ABB, Bosch and Siemens are building new ways of managing and responding to data, to create greater efficiencies as our nation's demand for power continues to grow dynamically.

Each of these technologies are going to add additional vectors of attack to an already complex environment. As the US modernizes its electrical infrastructure, we are also seeing an unprecedented number of cyber attacks that have been launched against organizations around the globe, including utilities. Those attacks have started to have physical consequences, as seen in the Black Energy attack on Ukraine's critical infrastructure.

Each of the five areas I will be discussing - Identity, Trusted Data, Attributed Isolated Networks, Threat Detection & Sharing, Automated Response & Remediation, all help build a stronger grid that allows for greater innovation and flexibility, while addressing more complex and sophisticated cyber attacks.

Identity

Over 80% of all cyber attacks are the result of stolen credentials. Credentials are one of the weakest links in cyber security today. We need to move to multi-factor, biometric, and continuous authentication for all individuals who interact within critical infrastructure. Current credentials and roles are still vulnerable to many types of phishing and spear fishing attacks, and two-factor authentication still has challenges. This level of authentication needs to extend beyond human authority to devices, applications, and systems.

For each human, device, or application that attaches to critical infrastructure, we will need to make sure to validate for identity, and authority to operate on that network. It is important to establish attribution early, by identifying the actors and devices, upon inception, to the network. Then we need to continually monitor those identities proactively, continually giving assurance. Based on early attribution we can establish identities before their actions, as opposed to discovering malicious activity, and then trying to establish attribution through forensics.

This is no easy feat to do and there are several factors to overcome. Rolling out a holistic process of attribution across the energy grid faces these challenges: current credential technology, current methodologies in IT, legacy applications, legacy devices, and the age of equipment.

Trusted Data

Within critical infrastructure networks, it is vital that we trust the data that is used in any decision making process. We protect that data today by running isolated networks, limiting interaction and control to devices. This is a good step, but we need to be looking at advanced threats that target the data, and manipulate its output, potentially causing devices and operators to make harmful decisions that have drastic consequences to the energy grid. These attacks could be made more powerful with automation, and the use of artificial intelligence to coordinate across many utilities at one time. To my knowledge no such attacks have taken place, but we should work to prepare against such a threat.

Building trusted data platforms means that we need to build in the ability to prove the data has not been altered at any point. Some research has pointed toward blockchain frameworks to prove this level of trust and certainty. This approach to building trusted data can be used for a variety of use cases within the energy grid. One such use case would be analytics used to make key decisions, or another use case such as supply chains where we need to guarantee there has been no altering of data between third parties.

Attributed Isolated Networks

Isolated networks are used relatively effectively today as a method of network separation, and security from threats on the open internet. However, insider threats and malware operate within the borders of the isolated network. This means we have to make sure that we build a chain of trust between all the devices and actions that happen on the network.

To build an attributed isolated network, we have to look at every device on that network and ensure that we know who is operating it, who is programming the software on it, and the entire history of the operation of that device. I would like to emphasize that we are always looking to get to the actual persons involved in the actions including the operators, and engineers. If we can move to world of whitelisting applications and devices based on our knowledge of it actions and history, including the applications residing on it, then we have assurance that we can find who is responsible for a given action. Once we have that actor we can then follow with legal recourse and evidence that allows us to prosecute malicious actors. We are a long way from having this level of transparency but this allows far greater assurance than we have today. It’s not impossible to do this, it’s just difficult but the outcome allows for a much more frictionless operational environment.

To build the history of operation trusted data technologies such as blockchain could allow us to be able to create cryptographic ledgers, that we can use to write the history of all the actions that are taken within a network, providing a much higher level of certainty for legal action against malicious behavior.

Threat Detection & Sharing

The ability to identify and share threat data at machine speed is another advanced strategy to respond within a time frame that prevents the spread and propagation of malicious attacks. Early in our work on CES-21, New Context identified Structured Threat Information Expression (or STIX, a structured language for describing cyber threat) to be the most applicable format for the energy industry. New Context has been working with the STIX open source group and the energy industry to make sure STIX is adaptable for the grids needs. STIX is backed by DHS and numerous commercial vendors.

STIX is just the first step; we now need to build the ability to rapidly share threats and remediations between organizations. Several information sharing organizations have taken initial steps to build out these capabilities, but most current practices still heavily rely on human analysts. If there were to be a coordinated attack on the grid, it is likely those analysts would not be able to respond to it in a timely fashion. To continue to advance threat intel we need to use new technologies such as artificial intelligence (AI) to help reduce the noise to human analysts and assist in making more rapid decisions.

Automated Response & Remediation

Discovering and sharing threats at machine speed is a huge step in the right direction, but the logical next step is to take automated actions against an overwhelming and rapid attack, we have to look at automated response. Automated response is a significant challenge for many reasons.

The first hurdle is how do we trust in the actions that are being recommended by a potential third party. We will need to ensure there is trust in the remediation about to be performed, which is why Identity, Trusted Data, and Trusted Networks are vital. Once we have been able to solve for trust, then our utilities, national labs, and agencies can distribute a remediation to the energy grid. These remediations can then be deployed within the utility networks, allowing them to be ready for anomalous behaviors and respond before potential instability in the network.

In summary, Identity, Trusted Data, Attributed Isolated Networks, Threat Detection & Sharing, and Automated Response & Remediation are technologies to focus on for advanced cyber defense. The battlefield continues to be changing, and we need to constantly look at new ways of protecting our infrastructure.

Our adversaries are formidable, and the challenge to most organizations is that the costs of defending their assets are high while the cost to attack is low. This is a hidden tax on our economy that will continue until we address the root cause instead of the symptoms.

Investing in these technologies will lower the cost to defend our infrastructure, and raise the cost to attack our infrastructure. In the end, it’s an economic game and any investment into better more effective solutions that address the core problems of cyber security instead of the symptoms, will significantly lower the cost of defense. This will allow more innovation in our industry and allow us to build the appropriate framework to welcome these 20 billion devices and applications to operate on the energy grid safely.

Thank you for the opportunity to testify. I look forward to the questions for today's hearing.