SOLARPLAZA webinar

SOLAR ASSET MANAGEMENT – NORTH AMERICA

Understanding and mitigating Cybersecurity risks in the solar industry

31 January 2018 - 10:30am PST - 1:30pm EST - 7:30pm CET

Moderator

Kostis Tzanakakis /// Project Manager - Solarplaza

Speakers

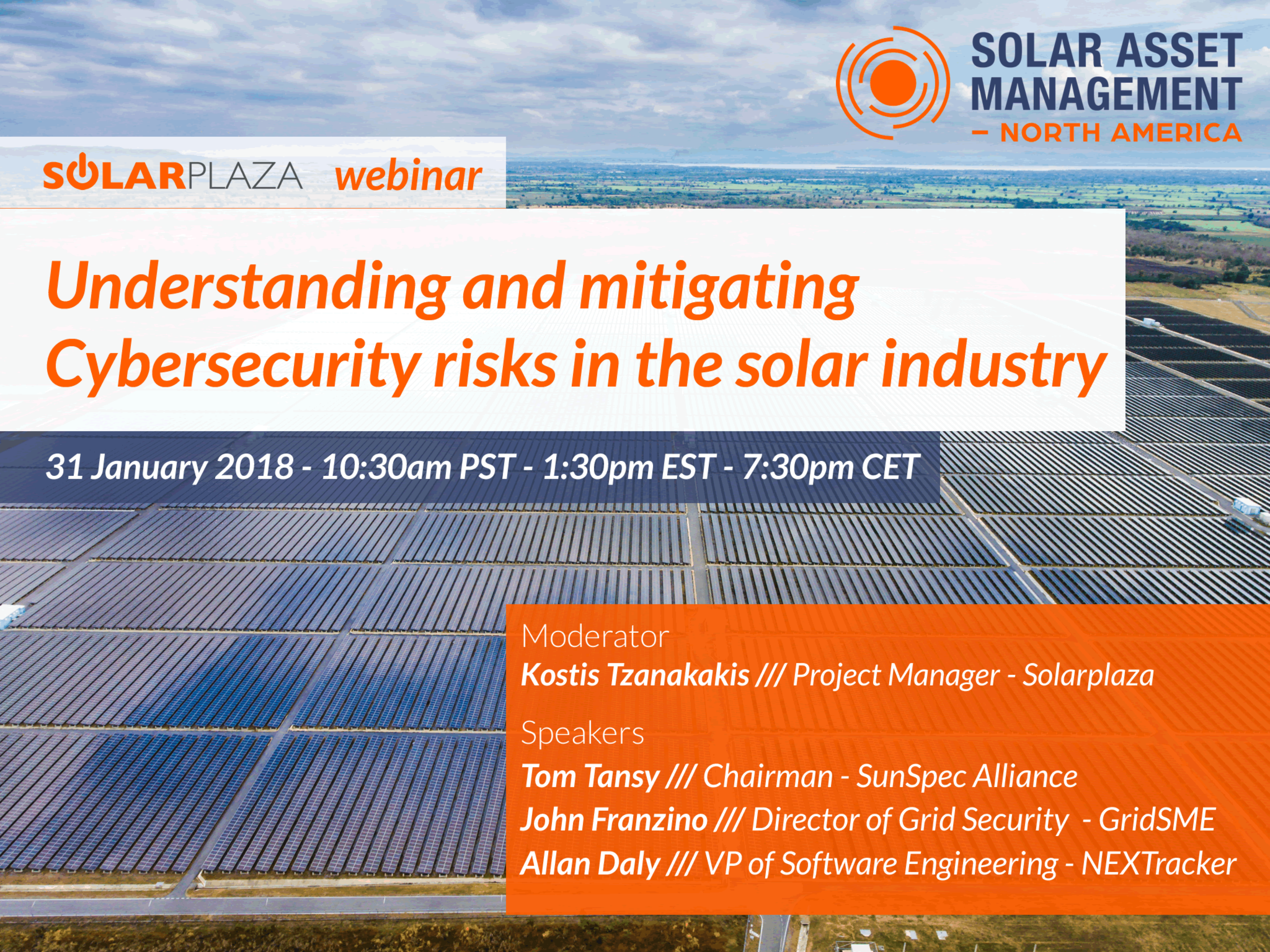
Tom Tansy /// Chairman - SunSpec Alliance

John Franzino /// Director of Grid Security - GridSME

Allan Daly /// VP of Software Engineering - NEXTracker

Welcome to the webinar!

We will start within a few minutes



SOLAR ASSET MANAGEMENT – NORTH AMERICA

SOLARPLAZA *webinar*

Understanding and mitigating Cybersecurity risks in the solar industry

31 January 2018 - 10:30am PST - 1:30pm EST - 7:30pm CET

Moderator

Kostis Tzanakakis */// Project Manager - Solarplaza*

Speakers

Tom Tansy */// Chairman - SunSpec Alliance*

John Franzino */// Director of Grid Security - GridSME*

Allan Daly */// VP of Software Engineering - NEXTracker*

Agenda

- Introduction Solarplaza
- Presentations

❖ Threat assessment - Tom Tansy | SunSpec Alliance

❖ Cyber Security & Solar – A consultant’s view - John Franzino | GridSME

❖ Building Security into Product Design - Allan Daly | NEXTracker

- Q&A
- End of the webinar

SOLAR ASSET MANAGEMENT – NORTH AMERICA

Q&A time

Kostis Tzanakakis

- *Email / skype:* kostis@solarplaza.com
- *Phone:* +31 10 302 7903

Website: **www.solarassetmanagement.us**

SOLAR ASSET MANAGEMENT – NORTH AMERICA

About Solarplaza

"To positively impact the world by accelerating the sustainable energy transition"

- Established in 2004
- 100+ events organized
- In 30+ countries worldwide
- Network of 60.000+ solar PV professionals

Solar Asset Management North America

13-14 March 2018 /// San Francisco

The leading conference focused on the operational phase of solar plants and portfolios

- THE must-attend event fully dedicated to the **operational phase** of PV assets
- **500+ attendees**, representing the value chain **from service provider to asset manager and investor**
- **90+ leading experts** on stage sharing their vision, expertise and experience
- **40+ sponsors and exhibitors** profiling themselves and their leading products/services

SOLAR ASSET MANAGEMENT – NORTH AMERICA

Attendees 2018

- 8minutenergy renewables
- AES Distributed Energy
- aep Affordable Equity Partners, Inc.
- ALECTRIS Solar asset care innovation
- Amicus O&M Cooperative
- arbox
- Borrego Solar
- c2
- CalCom Solar Solar for Agriculture & Water
- CALSEIA California Solar Energy Industries Association
- CERTREC Your regulatory experts
- Churchill Stateside Group
- Clēnera
- cmi
- Coronal Energy powered by Panasonic
- Cypress Creek Renewables
- DSM Bright science. Brighter living.
- ecos energy
- eDF renewable services
- ENERG-TECH
- ENERPARC
- ENVISION
- e.on
- First Solar.
- FMI
- GREENBACKER Renewable energy company
- GreenPowerMonitor Global solar asset management partner
- GridSME Subject matter experts
- Heliolytics
- IMCORP Power Cable Reliability
- inaccess Global solar asset management partner
- infiswift
- Ingeteam
- kWh analytics
- Locus Energy
- longroad Energy
- MEASURE The Drone as a Service Company
- Munich RE
- North American Development Bank
- namasté solar
- NautilusSolar
- New Energy Solar
- NEXTracker a flex company
- Nor-Cal Controls ES, Inc.
- North American Development Bank Banco de Desarrollo de América del Norte
- NREL National Renewable Energy Laboratory
- nrg
- obvius
- PG&E Pacific Gas and Electric Company
- PLEXUS Strategic insurance solutions
- Power Factors Drive
- POWERHUB Global solar asset management partner
- QOS Energy
- Shizen Energy Group
- SMA Global solar asset management partner
- Solar-Log
- SOLICHAMBA consulting · market intelligence
- Soltage Renewable energy provider
- solv
- SOS Reliability Matters
- S·Power Sustainable power group
- Stäubli
- Strata Solar
- SunSpec Alliance
- TESLA
- TRAVELERS
- UKC
- vivint.Solar
- Wells Fargo

SEE THE FULL OVERVIEW ON THE WEBSITE

Sponsors

Diamond Sponsors

POWERHUB
GLOBAL SOLAR ASSET MANAGEMENT PARTNER

SMA
GLOBAL SOLAR ASSET MANAGEMENT PARTNER

Gold Sponsors

GreenPowerMonitor
GLOBAL SOLAR ASSET MANAGEMENT PARTNER

UKC

namasté SOLAR

solv
The complete solar management solution

EDF renewable energy

infiswift

Locus ENERGY
A GENSCAPE COMPANY

QOS ENERGY

ENVISION

First Solar.

Heliolytics

POWER FACTORS
DRIVE

Networking Sponsors

TRAVELERS

DSM
BRIGHT SCIENCE. BRIGHTER LIVING.

STÄUBLI

inaccess
GLOBAL SOLAR ASSET MANAGEMENT PARTNER

NautilusSolar

MEASURE
The Drone as a Service® Company

NEXTracker
A Flex Company

Solar-Log®

Exhibition Sponsors

obvius

CERTREC
YOUR REGULATORY EXPERTS

GridSME
SUBJECT MATTER EXPERTS

Branding Sponsor

Ingeteam

Solar Asset Management North America

Special Webinar Promotional Discount

First 10 registrants to use the code **WEBINAR20** are eligible for a 10% discount on the registration fee.

https://solarassetmanagement.us/register-now/

Practical notes

- **Technical issues**? → Use chatbox
- The **presentation slides** will be available afterwards

Tom Tansy

- CHAIRMAN - SUNSPEC ALLIANCE

- In SunSpec Alliance he leads the distributed energy industry's efforts to establish data and communication standards that enable seamless integration of solar PV and storage into the Smart Grid.
- The SunSpec Alliance has more than 100 stakeholders across the globe, including leading fleet operators, component suppliers, software developers, and utilities.

John Franzino

- DIRECTOR OF GRID SECURITY – GRIDSME

- John and the cyber security team assist clients with all aspects of Critical Infrastructure Protection (CIP), as well as general cybersecurity support outside the scope of CIP.
- John manages both day-to-day operations and long-term projects, while simultaneously building out the supporting business processes and strategic goals.
- He has hands-on experience implementing security controls in the field, conducting vulnerability assessments in production SCADA environments, network monitoring, and incident response.

GridSME SUBJECT MATTER EXPERTS

Allan Daly

- VP SOFTWARE ENGINEERING – NEXTRACKER
- Allan Daly leads the software team and is lead product manager for the Company's TrueCapture smart software control system.
- In this capacity, he leads a team of 10 software engineers to design and develop intelligent, connected industrial software to enhance the NEXTracker customer experience.
- He has always been an ‘energy guy’, with a life-long interest in energy and buildings. He brings together his broad experience from policy-work, research, teaching, and consulting to inform the design and operation of innovative and sustainable mechanical systems.

NEXTracker A Flex Company

Threat assessment: what should asset managers be thinking about?

Tom Tansy

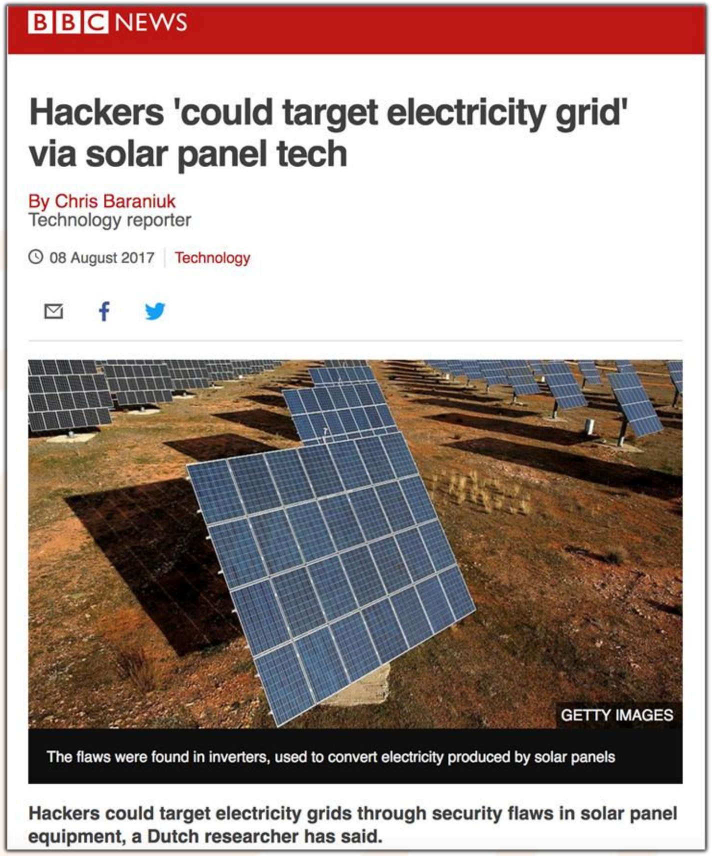
SunSpec Alliance

www.sunspec.org

Security required for all PV systems

- State-level mandates specify secure networks for all systems
  - C&I and Residential
  - California (Rule 21) and Hawaii (Rule 14H) effective now
- National mandate to securely network ALL DER systems
  - Specified in IEEE 1547-2018
- Considerations are different
  - Scale: 720 total utility-scale vs. 300K small systems per year in CA
  - Operations: local vs. remote
  - Regulations: NERC CIP vs. state interconnection rules

Why worry about small systems?



BBC NEWS

Hackers 'could target electricity grid' via solar panel tech

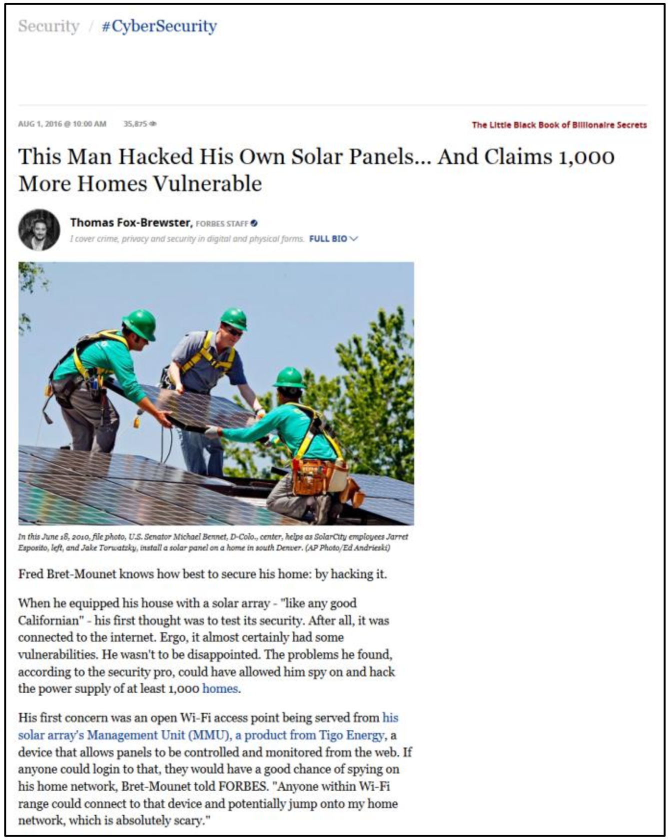
By Chris Baraniuk
Technology reporter

08 August 2017 | Technology

The flaws were found in inverters, used to convert electricity produced by solar panels

Hackers could target electricity grids through security flaws in solar panel equipment, a Dutch researcher has said.

http://www.bbc.com/news/amp/technology-40861976



Security / #CyberSecurity

AUG 1, 2016 @ 10:00 AM 35,875

The Little Black Book of Billionaire Secrets

This Man Hacked His Own Solar Panels... And Claims 1,000 More Homes Vulnerable

Thomas Fox-Brewster, FORBES STAFF
I cover crime, privacy and security in digital and physical forms. FULL BIO

In this June 18, 2010, file photo, U.S. Senator Michael Bennet, D-Colo., center, helps as SolarCity employees Jarret Esposito, left, and Jake Torwatzky, install a solar panel on a home in south Denver. (AP Photo/Ed Andrieski)

Fred Bret-Mounet knows how best to secure his home: by hacking it.

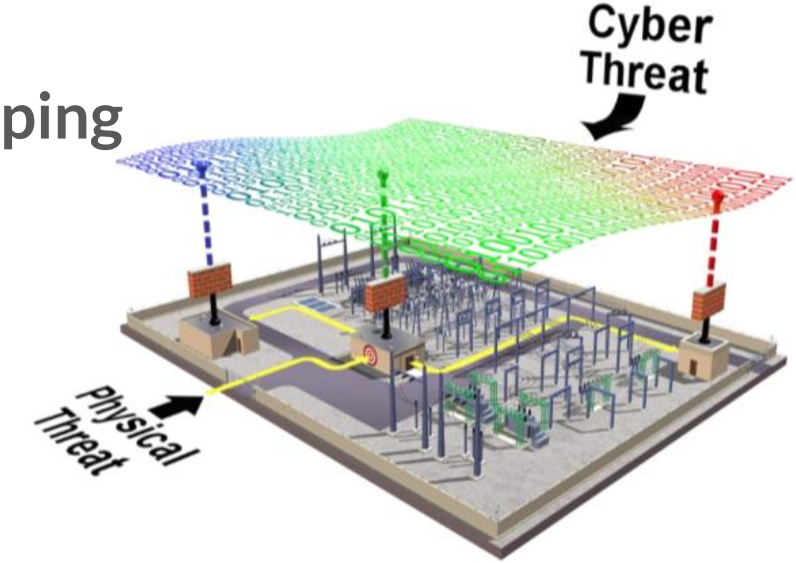
When he equipped his house with a solar array - "like any good Californian" - his first thought was to test its security. After all, it was connected to the internet. Ergo, it almost certainly had some vulnerabilities. He wasn't to be disappointed. The problems he found, according to the security pro, could have allowed him spy on and hack the power supply of at least 1,000 homes.

His first concern was an open Wi-Fi access point being served from his solar array's Management Unit (MMU), a product from Tigo Energy, a device that allows panels to be controlled and monitored from the web. If anyone could login to that, they would have a good chance of spying on his home network, Bret-Mounet told FORBES. "Anyone within Wi-Fi range could connect to that device and potentially jump onto my home network, which is absolutely scary."

http://www.forbes.com/sites/thomasbrewster/2016/08/01/1000-solar-panels-tigo-vulnerable-hackers

Considerations for asset managers

- Risk management: proportional responses
- Regulatory: rules that apply differ by system size
- Equipment: products that work
- Finance: budgets that scale
- Personnel: training & record keeping



Discussion

SUNSPEC ALLIANCE

GridSME SUBJECT MATTER EXPERTS

NEXTracker A Flex Company

Upcoming Events

Solar Asset Management North America

13-14 March 2018

San Francisco

www.solarassetmanagement.us

Solar Asset Management Asia

24-25 May 2018

Tokyo, Japan

www.solarassetmanagement.asia

SOLAR ASSET MANAGEMENT – NORTH AMERICA

Cyber Security and Solar PV

Solar Asset Management – North America

January 31, 2018

John Franzino

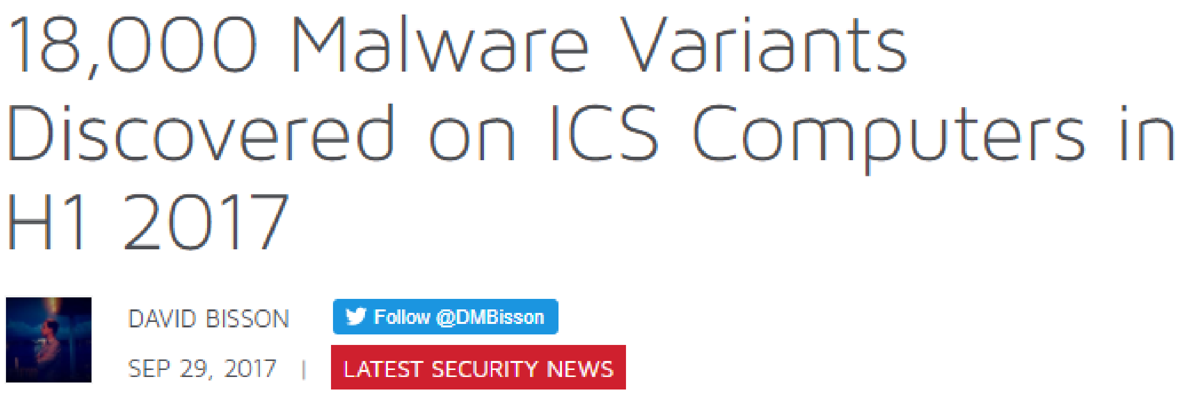
Director of GridSecurity

GridSME

SUBJECT MATTER EXPERTS

SOLAR ASSET MANAGEMENT – NORTH AMERICA

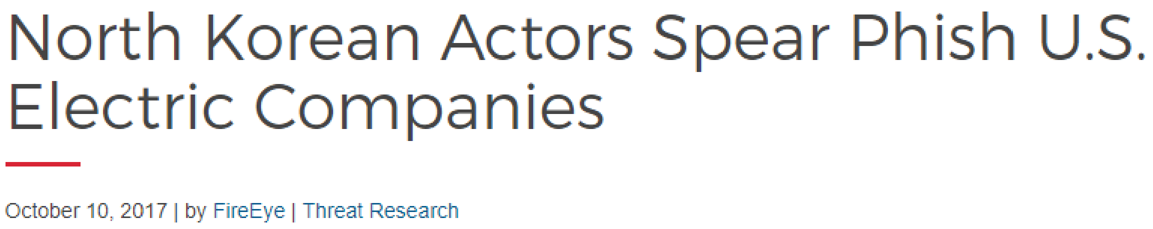
Observing the Fact of the Matter



18,000 Malware Variants Discovered on ICS Computers in H1 2017

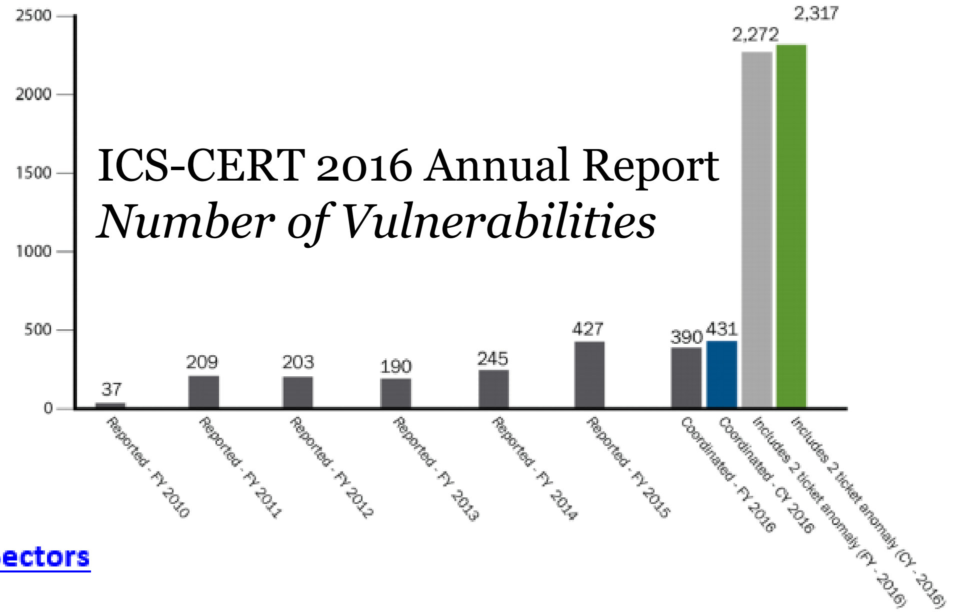
DAVID BISSON

SEP 29, 2017 | LATEST SECURITY NEWS



North Korean Actors Spear Phish U.S. Electric Companies

October 10, 2017 | by FireEye | Threat Research



ICS-CERT 2016 Annual Report

Number of Vulnerabilities

Homeland Security

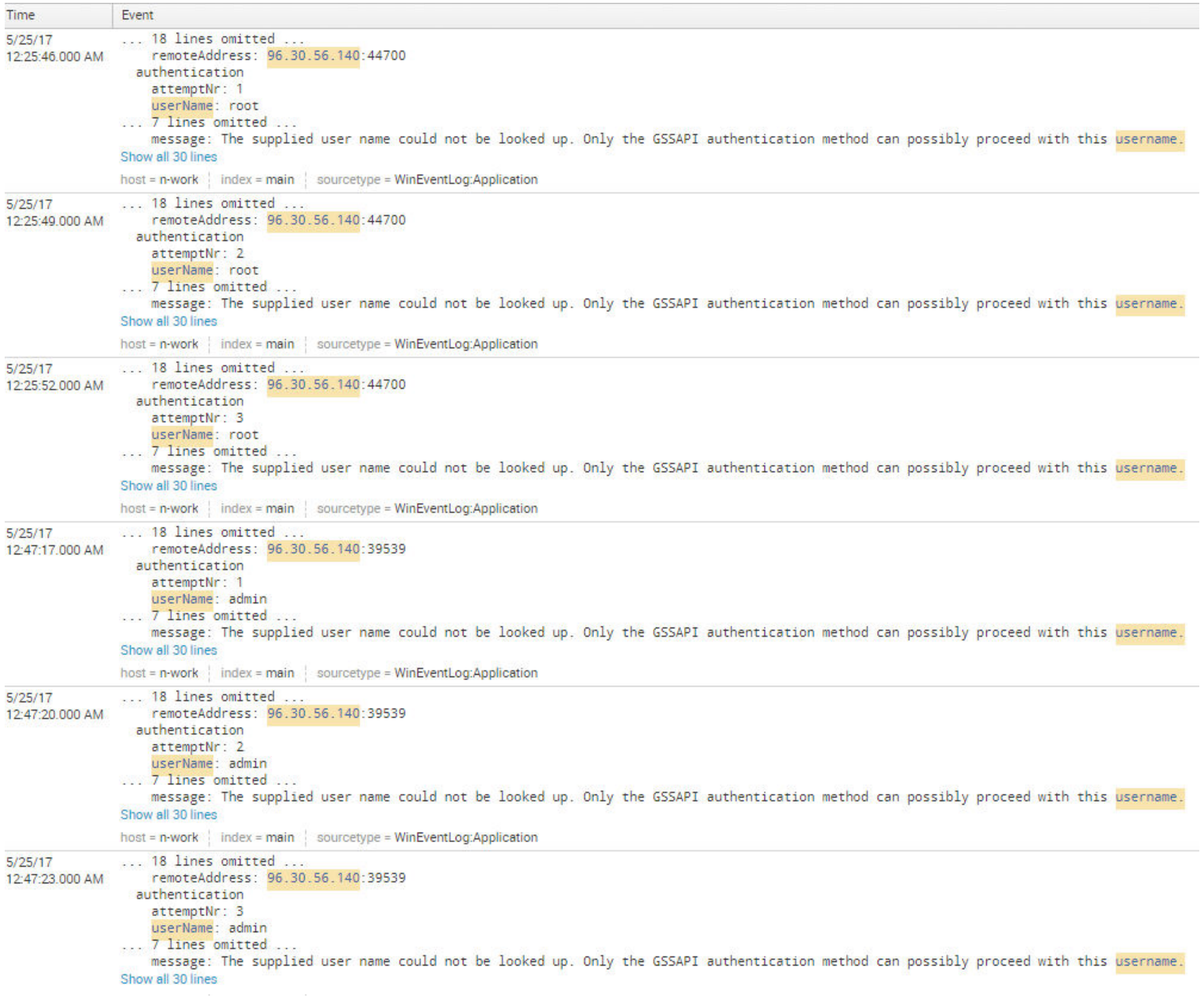
US-CERT United States Computer Emergency Readiness Team

National Cyber Awareness System:

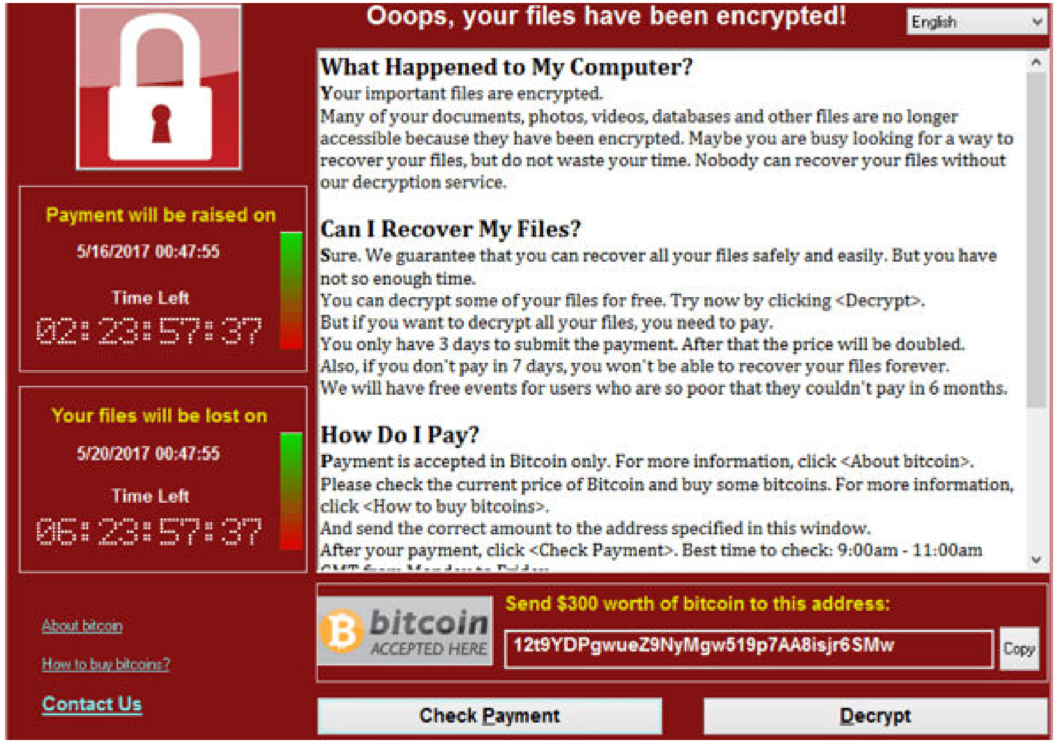
TA17-293A: Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors

10/20/2017 06:50 PM EDT

Observing You’re Not Too Small



```
Time                   Event
5/25/17                ... 18 lines omitted ...
12:25:46.000 AM            remoteAddress: 96.30.56.140:44700
                         authentication
                           attemptNr: 1
                           userName: root
                       ... 7 lines omitted ...
                           message: The supplied user name could not be looked up. Only the GSSAPI authentication method can possibly proceed with this username.
                       Show all 30 lines
                       host = n-work | index = main | sourcetype = WinEventLog:Application
5/25/17                ... 18 lines omitted ...
12:25:49.000 AM            remoteAddress: 96.30.56.140:44700
                         authentication
                           attemptNr: 2
                           userName: root
                       ... 7 lines omitted ...
                           message: The supplied user name could not be looked up. Only the GSSAPI authentication method can possibly proceed with this username.
                       Show all 30 lines
                       host = n-work | index = main | sourcetype = WinEventLog:Application
5/25/17                ... 18 lines omitted ...
12:25:52.000 AM            remoteAddress: 96.30.56.140:44700
                         authentication
                           attemptNr: 3
                           userName: root
                       ... 7 lines omitted ...
                           message: The supplied user name could not be looked up. Only the GSSAPI authentication method can possibly proceed with this username.
                       Show all 30 lines
                       host = n-work | index = main | sourcetype = WinEventLog:Application
5/25/17                ... 18 lines omitted ...
12:47:17.000 AM            remoteAddress: 96.30.56.140:39539
                         authentication
                           attemptNr: 1
                           userName: admin
                       ... 7 lines omitted ...
                           message: The supplied user name could not be looked up. Only the GSSAPI authentication method can possibly proceed with this username.
                       Show all 30 lines
                       host = n-work | index = main | sourcetype = WinEventLog:Application
5/25/17                ... 18 lines omitted ...
12:47:20.000 AM            remoteAddress: 96.30.56.140:39539
                         authentication
                           attemptNr: 2
                           userName: admin
                       ... 7 lines omitted ...
                           message: The supplied user name could not be looked up. Only the GSSAPI authentication method can possibly proceed with this username.
                       Show all 30 lines
                       host = n-work | index = main | sourcetype = WinEventLog:Application
5/25/17                ... 18 lines omitted ...
12:47:23.000 AM            remoteAddress: 96.30.56.140:39539
                         authentication
                           attemptNr: 3
                           userName: admin
                       ... 7 lines omitted ...
                           message: The supplied user name could not be looked up. Only the GSSAPI authentication method can possibly proceed with this username.
                       Show all 30 lines
```



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

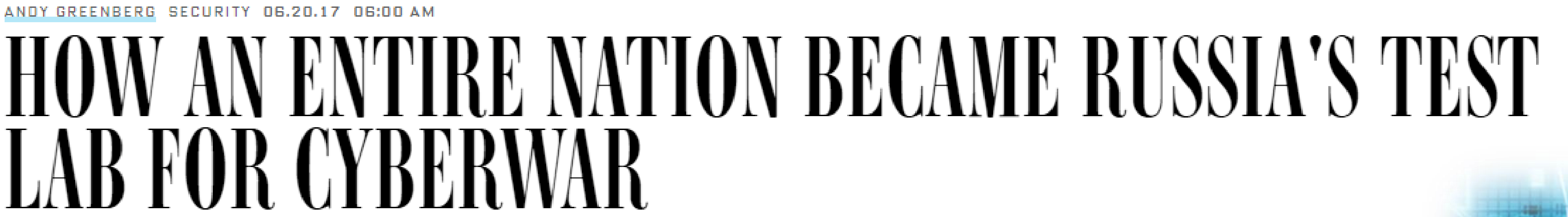
And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

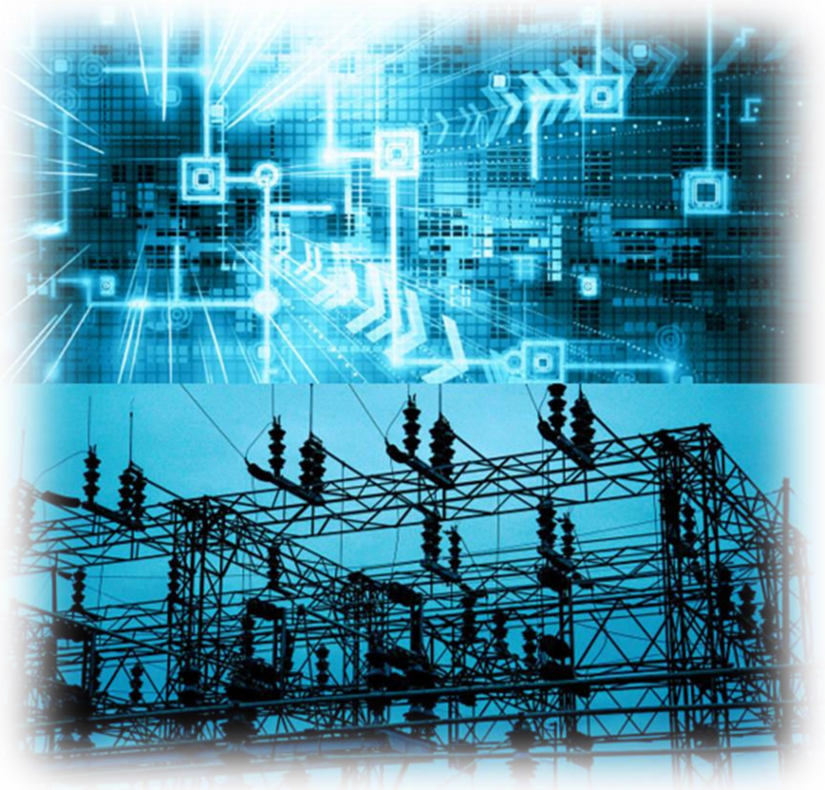
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Observing You’re Not Too Small



ANDY GREENBERG SECURITY 06.20.17 06:00 AM

HOW AN ENTIRE NATION BECAME RUSSIA'S TEST LAB FOR CYBERWAR



Homeland Security

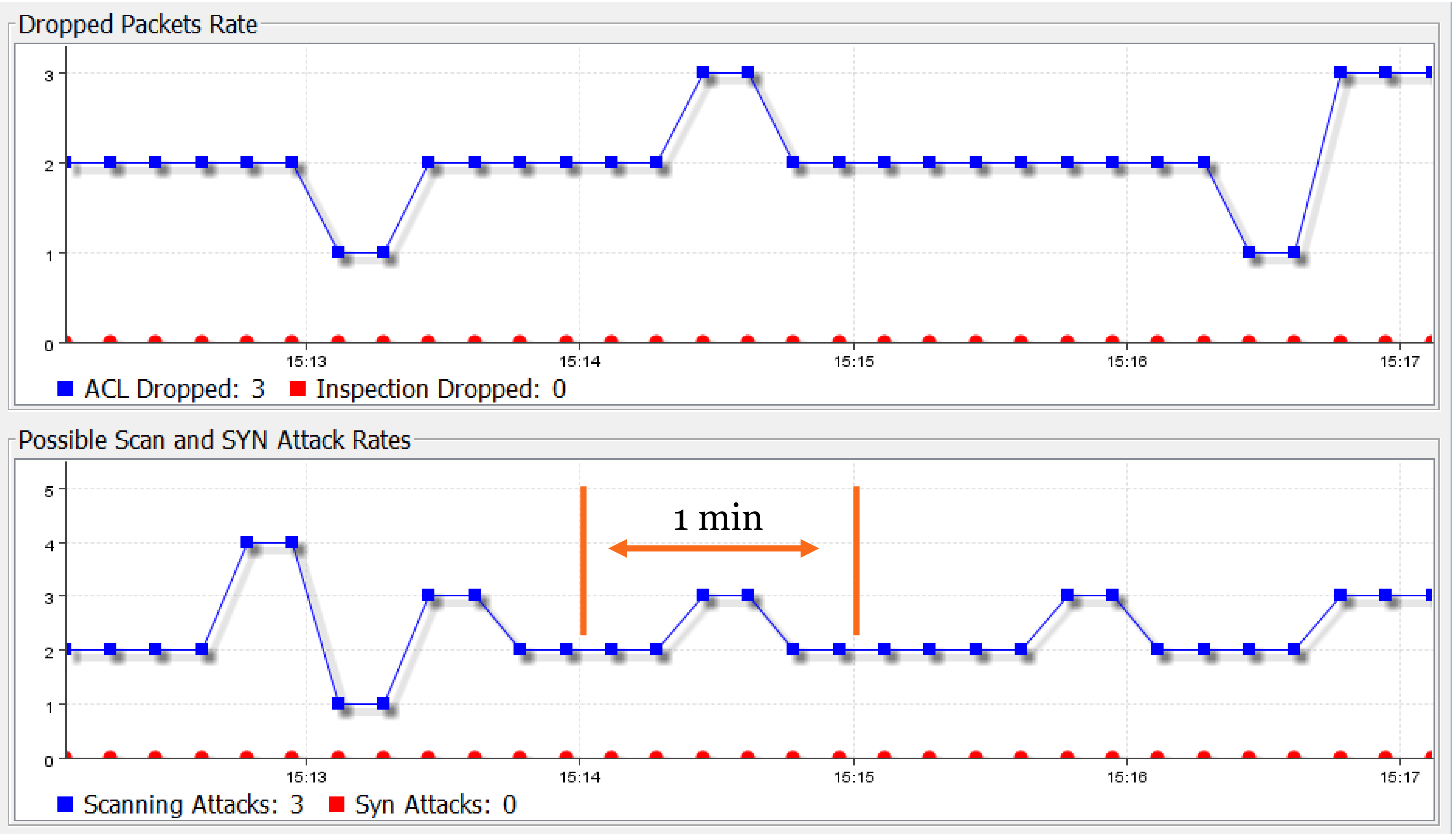
US-CERT United States Computer Emergency Readiness Team

National Cyber Awareness System:

[TA17-293A: Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors]()

10/20/2017 06:50 PM EDT

Observing Threats in Real-Time



Dropped Packets Rate

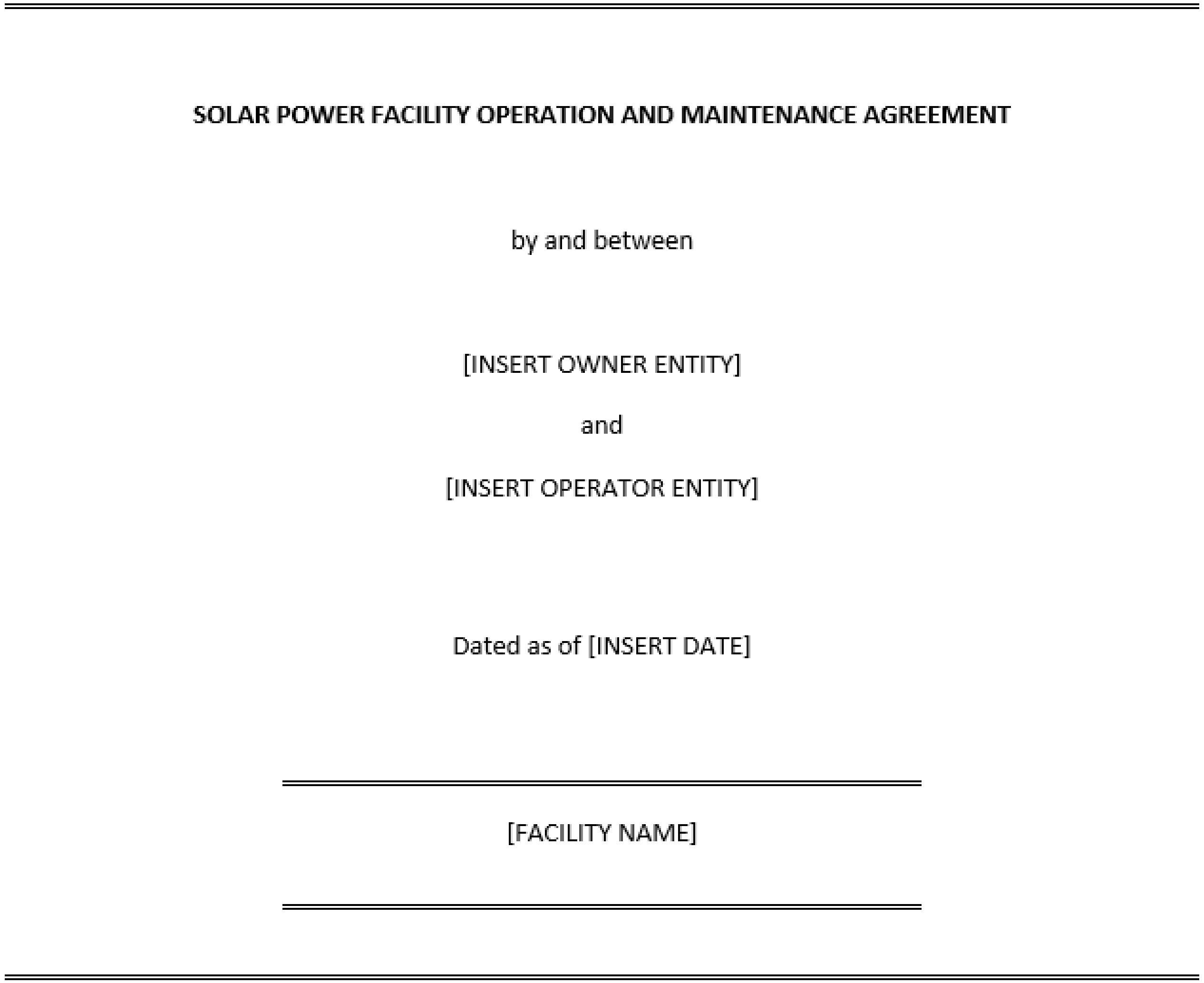
🟦 ACL Dropped: 3 🟥 Inspection Dropped: 0

Possible Scan and SYN Attack Rates

1 min

🟦 Scanning Attacks: 3 🟥 Syn Attacks: 0

Orienting Business Constraints & Opportunities



SOLAR POWER FACILITY OPERATION AND MAINTENANCE AGREEMENT

by and between

[INSERT OWNER ENTITY]

and

[INSERT OPERATOR ENTITY]

Dated as of [INSERT DATE]

[FACILITY NAME]

CYBER

INSURANCE

CLAIM FORM

sonal Information

e (Last)

(First)

(Middle Initial)

Home Telep

Other Tel

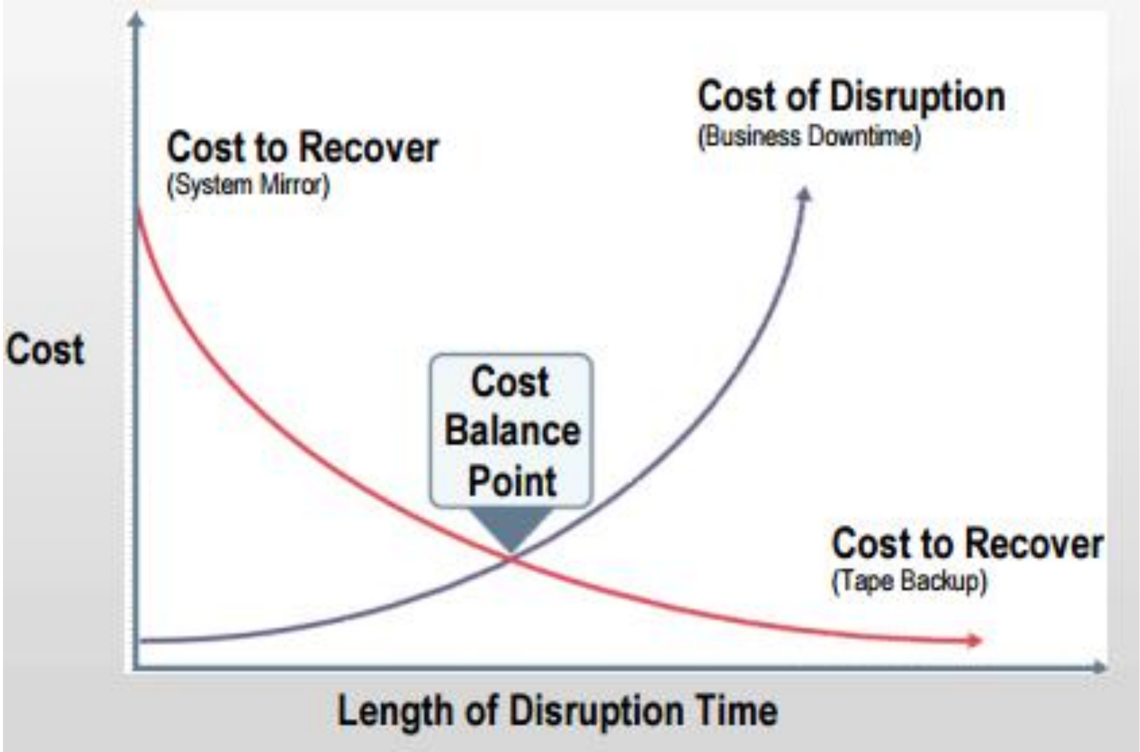
dress (Mailing Address)

(City)

(State)

(Zip)

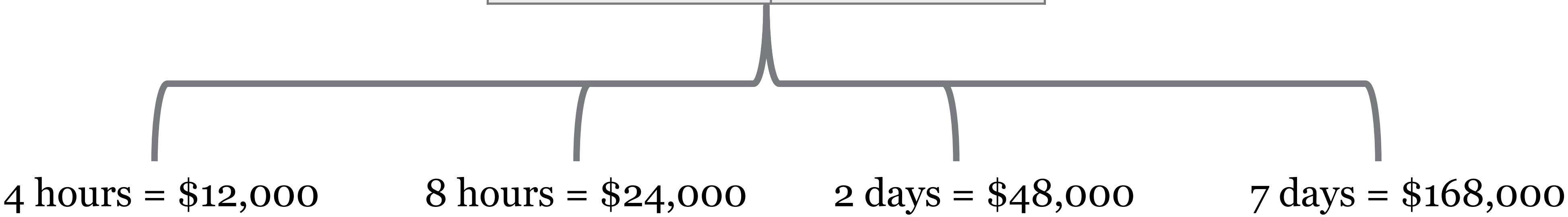
Deciding Impacts



***Annual Loss Expectancy** = [Likelihood, expressed as "# of incidents per year"] * [Impact, expressed as "$ loss per incident"]*

Deciding Budgets

PPA	$40/MWh
Nameplate	100 MW
Capacity Factor	25%



4 hours = $12,000

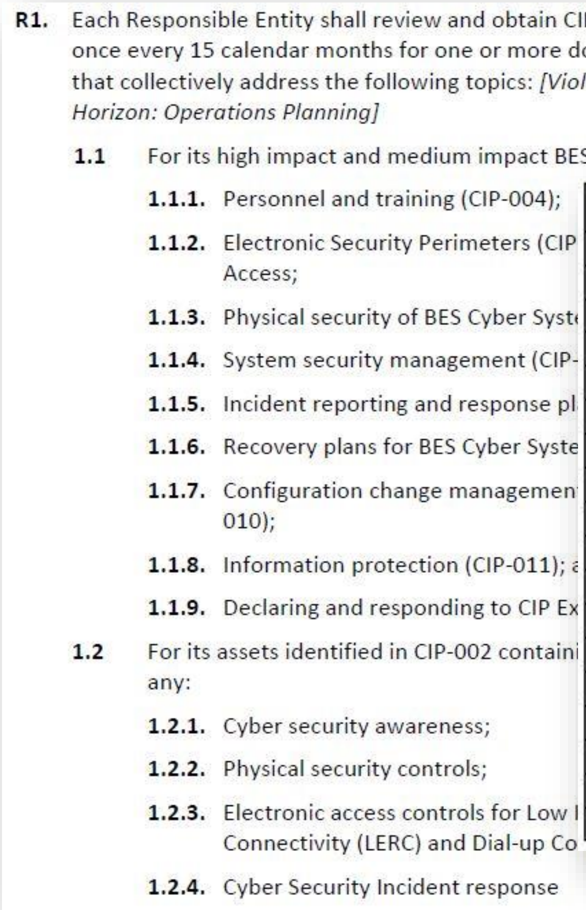
8 hours = $24,000

2 days = $48,000

7 days = $168,000

Guiding Decisions

NERC CIP



R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP Access;

1.1.3. Physical security of BES Cyber Syst

1.1.4. System security management (CIP-

1.1.5. Incident reporting and response pl

1.1.6. Recovery plans for BES Cyber Syste

1.1.7. Configuration change managemen 010);

1.1.8. Information protection (CIP-011); a

1.1.9. Declaring and responding to CIP Ex

1.2 For its assets identified in CIP-002 containi any:

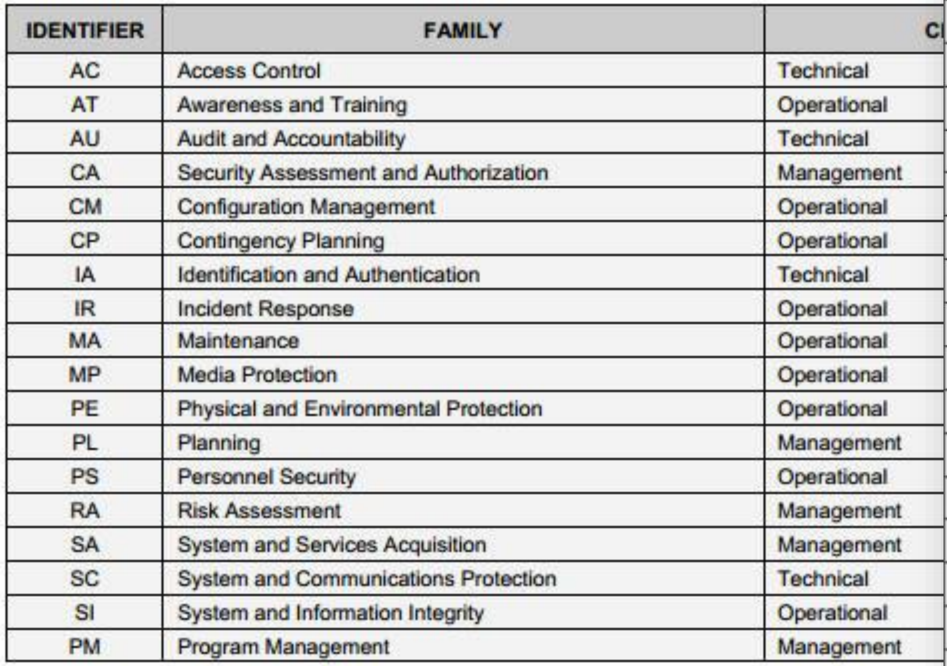
1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls for Low I Connectivity (LERC) and Dial-up Co

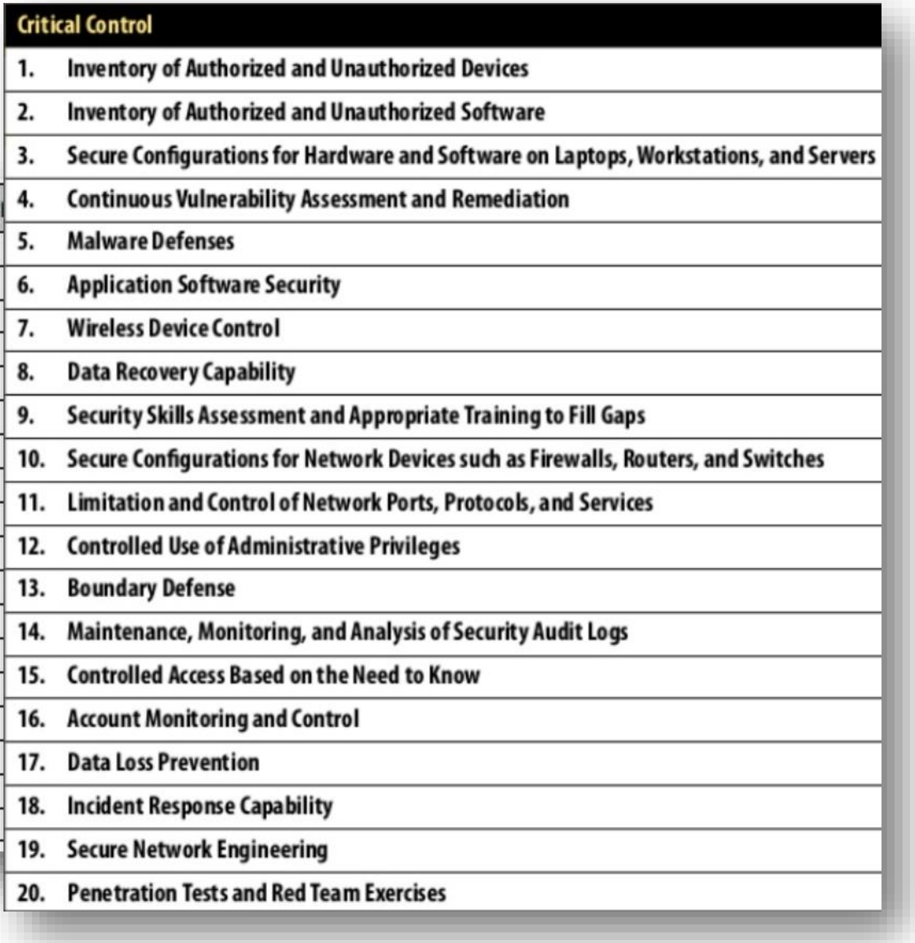
1.2.4. Cyber Security Incident response

NIST SP 800-53



IDENTIFIER	FAMILY	Cl
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

CIS Top 20 CSC



Critical Control
1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Malware Defenses
6. Application Software Security
7. Wireless Device Control
8. Data Recovery Capability
9. Security Skills Assessment and Appropriate Training to Fill Gaps
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11. Limitation and Control of Network Ports, Protocols, and Services
12. Controlled Use of Administrative Privileges
13. Boundary Defense
14. Maintenance, Monitoring, and Analysis of Security Audit Logs
15. Controlled Access Based on the Need to Know
16. Account Monitoring and Control
17. Data Loss Prevention
18. Incident Response Capability
19. Secure Network Engineering
20. Penetration Tests and Red Team Exercises

Compliance Pause

NERC CIP is meant to be the floor not the ceiling

NEXTracker
A Flex Company

Cyber Security Framework & Solutions for Utility-Scale and Commercial/Industrial Systems

Allan Daly, VP Software, January 31, 2018

CYBER SECURITY

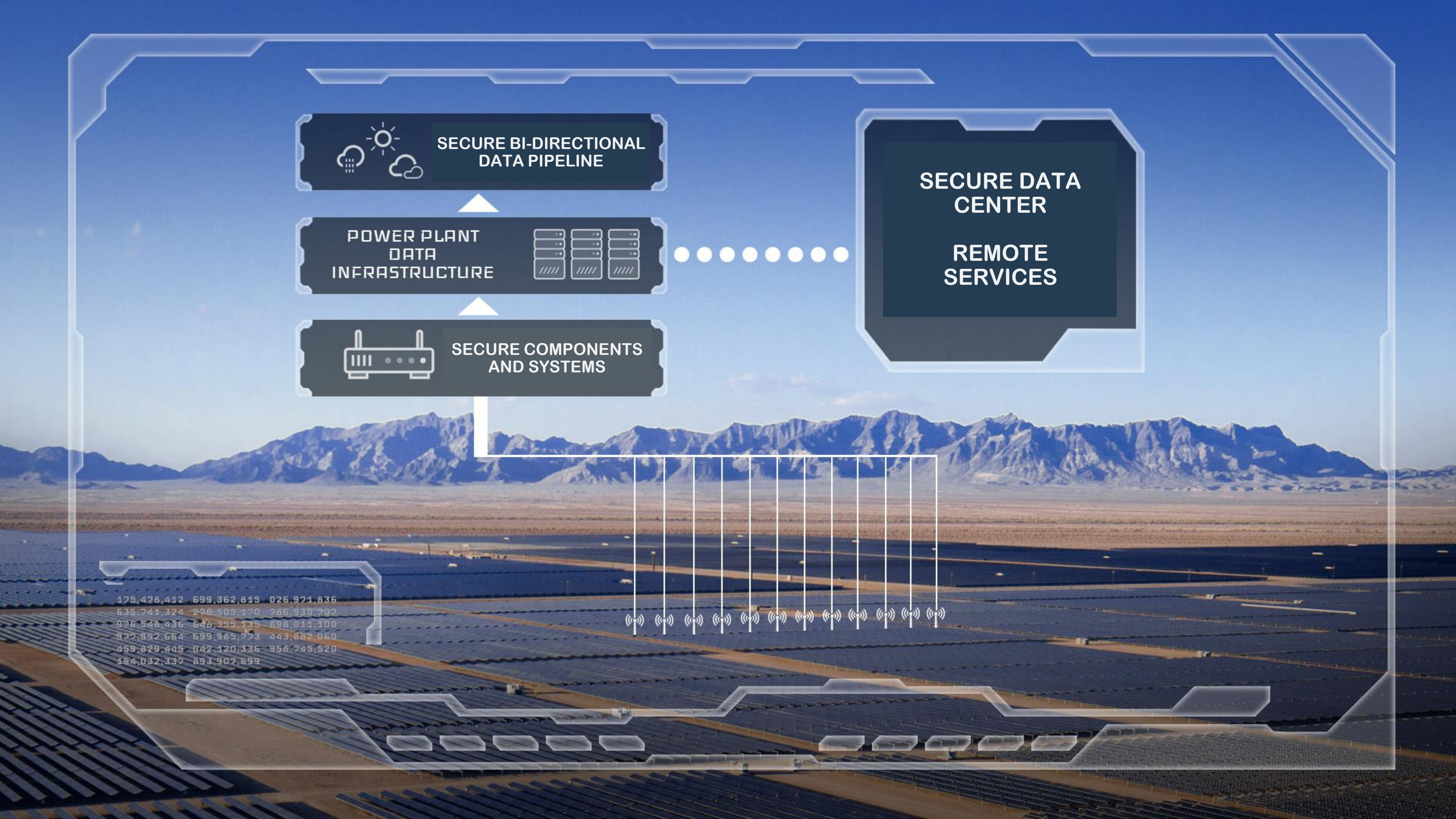
Careful planning and implementation of many "little things" make Secure Connectivity at Scale possible and achievable.

"It's the little details that are vital. Little things make big things happen."

— John Wooden

"It has long been an axiom of mine that the little things are infinitely the most important."

— Arthur Conan Doyle



SECURE BI-DIRECTIONAL DATA PIPELINE

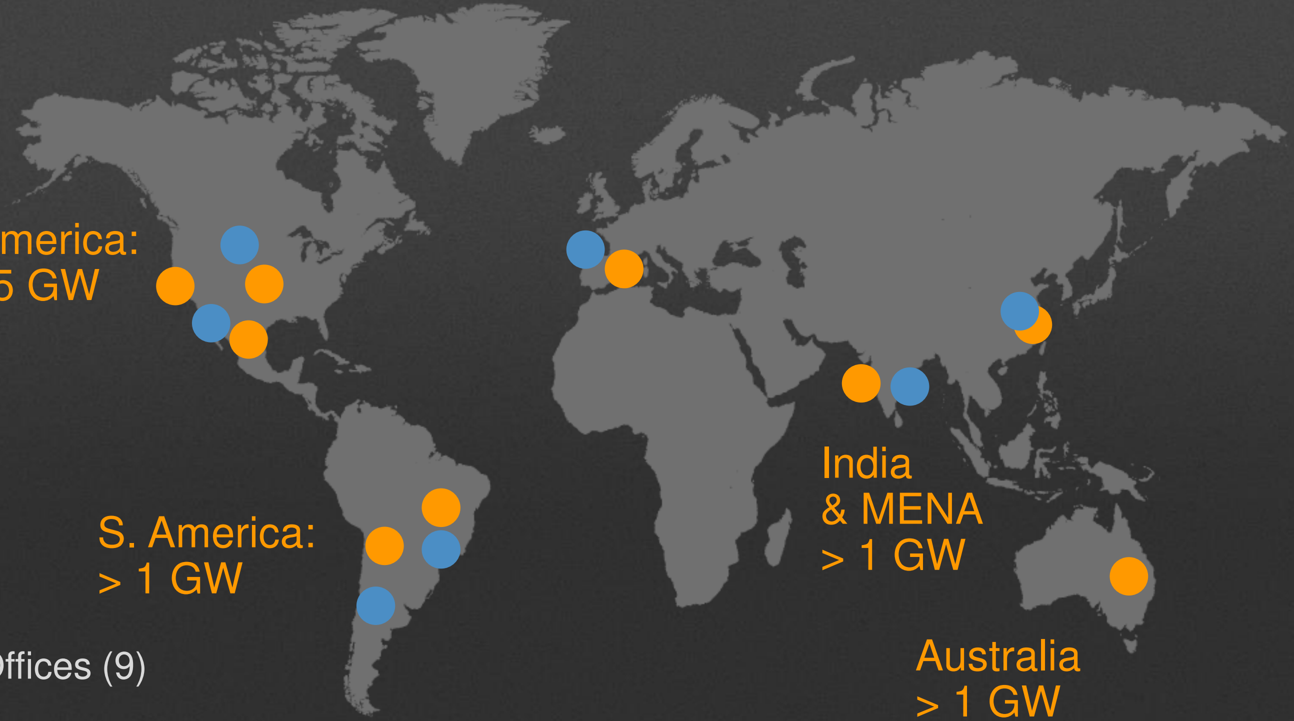
POWER PLANT DATA INFRASTRUCTURE

SECURE COMPONENTS AND SYSTEMS

SECURE DATA CENTER

REMOTE SERVICES

OUR WORLD @ NEXTRACKER



● Offices (9)

● Manufacturing (7)

KEY METRICS & GOALS

- 11 GW trackers delivered & in fulfillment
- 175 MW weekly manufacturing capacity
- #1 market share, 2 years
- Parent company Flex, $24Bn revenue
- Connect to, and acquire data from, every component and every system every 5 minutes across the world
- Create meaningful value with this data and connectivity

TOP 7 QUESTIONS OWNER/OPERATORS ASK:

1 How do you handle security with your Zigbee wireless network?

2 How do you protect power plants from hackers if there is remote access?

3 What protocols do your equipment use and what protections does your equipment have?

4 What data do you use?

5 What platforms are your SCADA systems and your web dashboard built on?

6 What's your patch management scheme and how often do update your systems?

7 Are your technicians vetted? Do they have a background check and training? What customer data policies do you have?

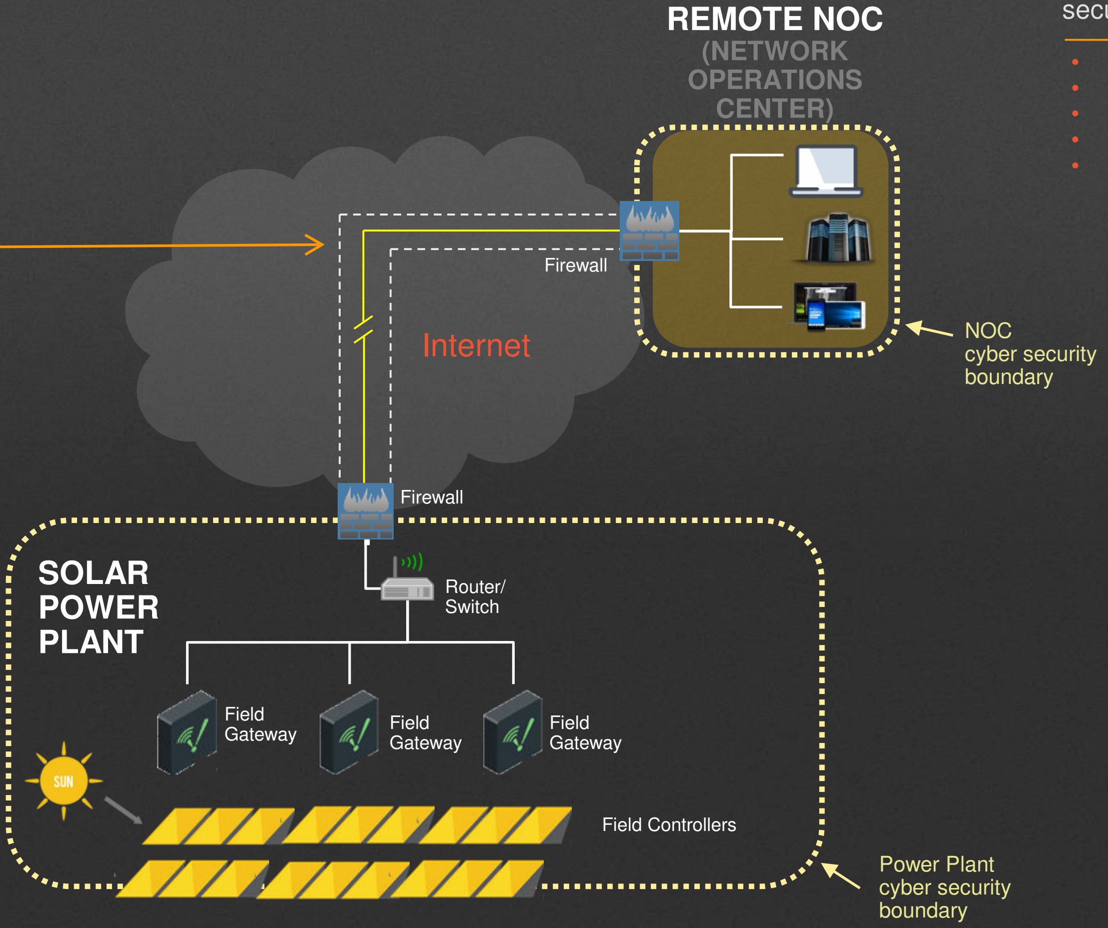
CASE STUDY: C&I (DG) CYBER SECURITY

Bi-Directional Data Connector security measures

- encryption
- Authentication
- authorization

Remote NOC security measures

- access control
- incident response
- patch management
- virus management
- access logging



Solar Power Plant security measures

- encrypted communication
- configuration management

CASE STUDY: UTILITY-SCALE CYBER SECURITY

Data Center security measures

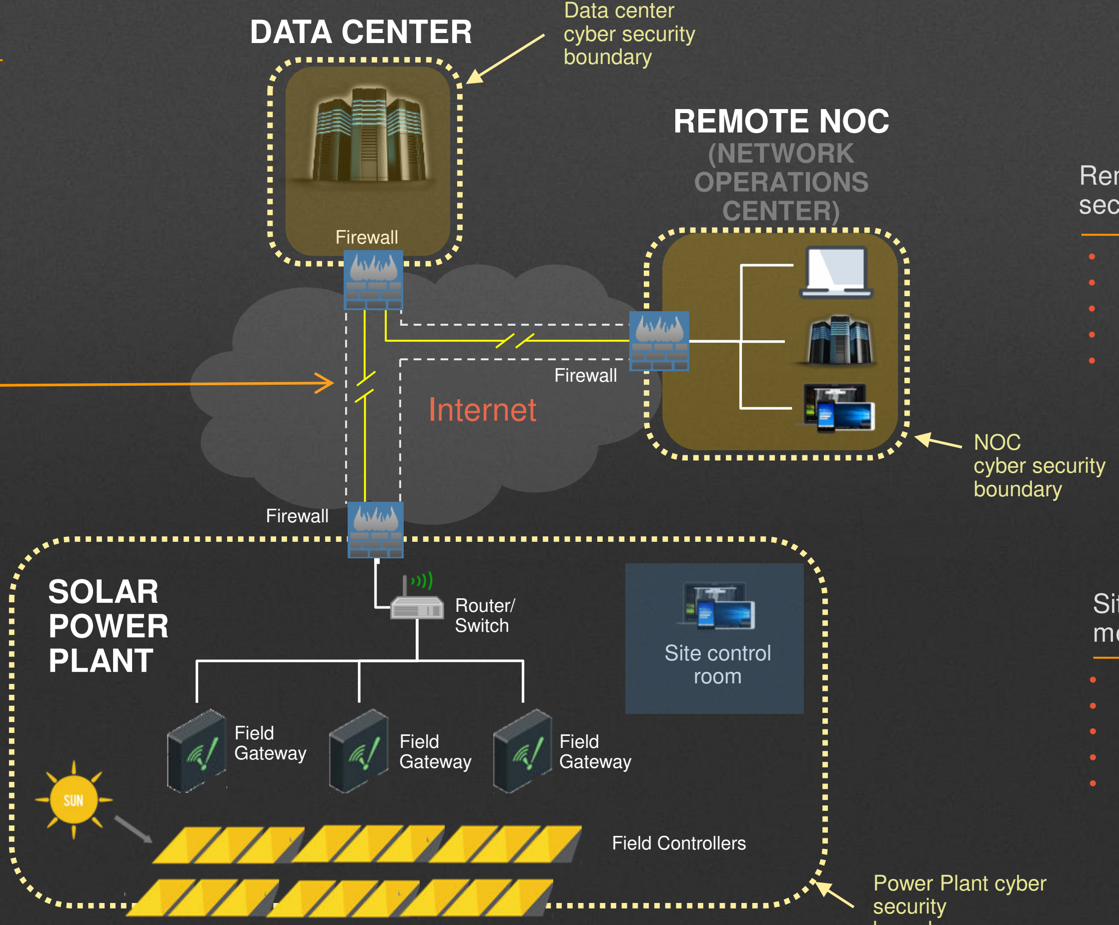
- access control
- incident response plan
- data management
- virus management
- access logging

Bi-Directional Data Connector security measures

- encryption
- Authentication
- authorization

Solar Power Plant security measures

- encrypted communication
- configuration management



Remote NOC security measures

- access control
- incident response
- patch management
- virus management
- access logging

Site Control Room security measures

- access control
- incident response
- patch management
- virus management
- access logging

TYPICAL SECURITY PLATFORM RECURRING TASKS

Activity	Frequency
Physical Security Plan Audit	Annually
Cyber Awareness Training	Annually
Electronic Security Perimeter (ESP) Plan Audit	Annually
System Access Plan Audit	Annually
Threat Deterrence & Detection Plan Audit	Annually
Event Monitoring & Notification Plan Audit	Annually
System Access Plan Audit	Annually
Incident Response Plan Audit	Annually
System Recovery Plan Test	Annually

Activity	Frequency
System Recovery Plan Audit	Annually
Change Management Plan Audit	Annually
Configuration Monitoring Plan Audit	Annually
Configuration Change Report	Monthly
Vulnerability Plan Audit	Annually
Paper Vulnerability Assessment	Annually
Operational Health Check	Monthly
Security Patch Evaluation & Application Report	Monthly
Backup and Recovery Performance	Monthly

NEXTracker
A Flex Company

CONTACT:

Allan Daly
VP Software Engineering
Email: adaly@nextracker.com

THANK YOU