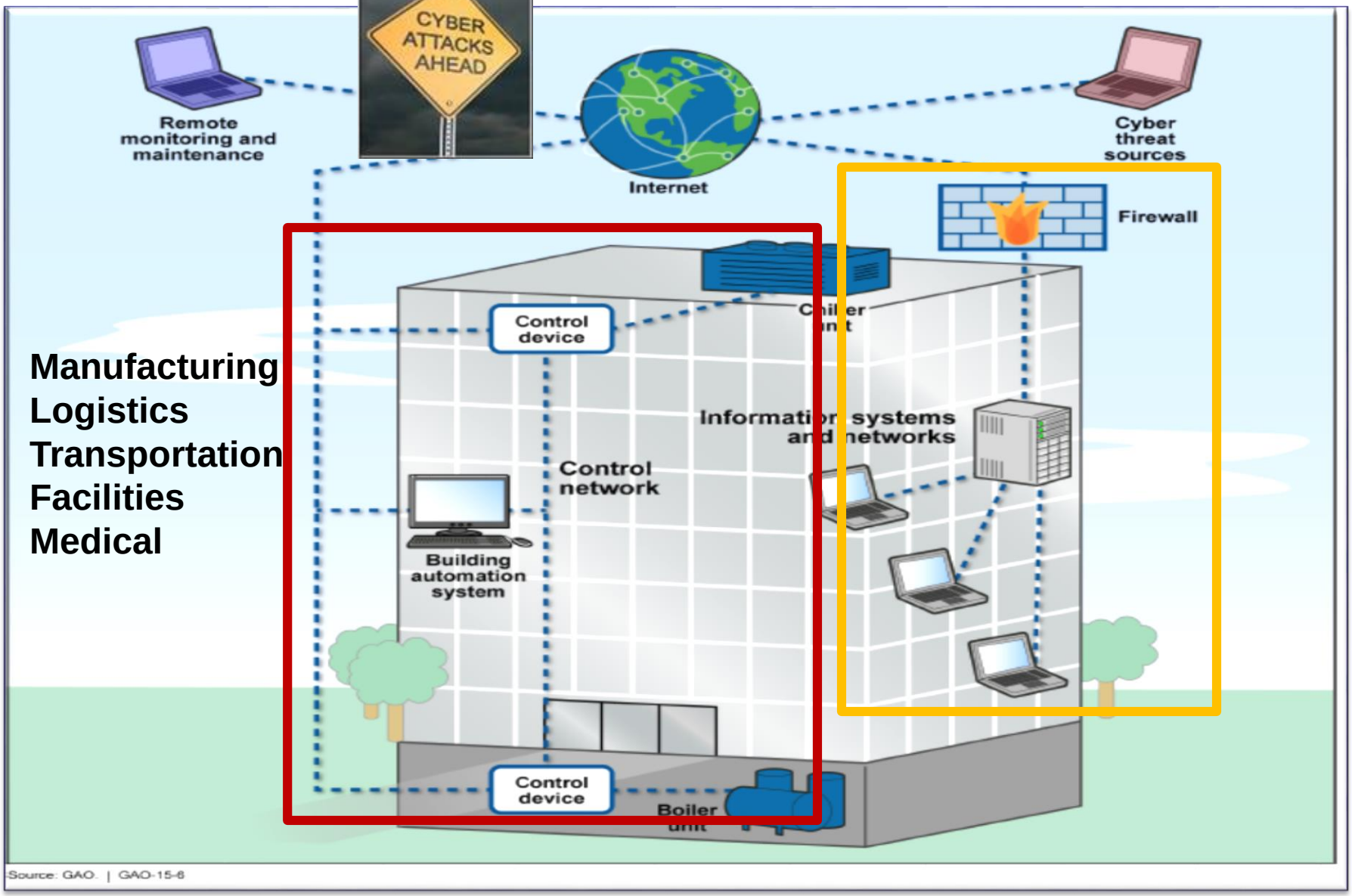
DoD: GSA/DoD Control Systems Cyber Policy and Strategy

Presented by **Daryl Haegley,** Program Manager, Office of the Assistant Secretary of Defense for Energy, Installations, and Environment

What's in Your Network?

- Manufacturing
- Logistics
- Transportation
- Facilities
- Medical

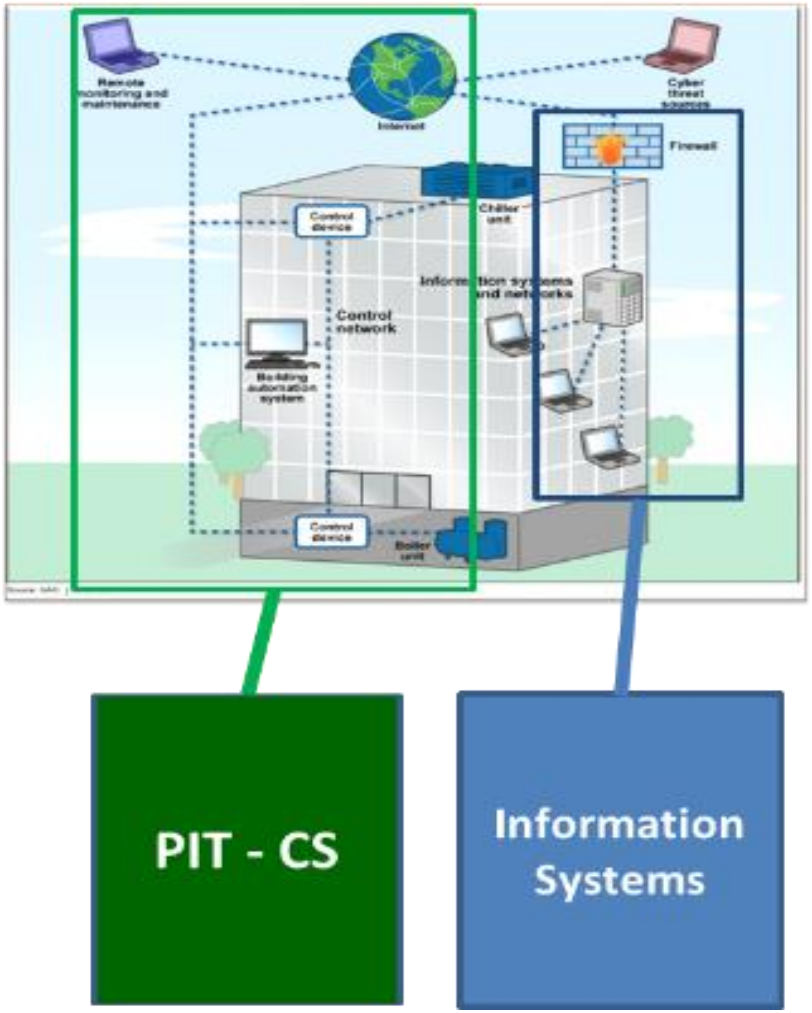


245 = Avg # Days Undiscovered Adversary

DHS ICS CERT

Same Meaning but Different:
PIT, CS, PIT-CS, ICS,OT, SCADA, CPS

- **PIT = Platform Information Technology**
- **CS = Control Systems**
- **PIT-CS = PIT Control Systems**
- **ICS = Industrial Control Systems**
- **OT = Operational Technology**
- **SCADA = Supervisory Control And Data Acquisition**
- **CPS = Cyber Physical Systems**
- **IoT = Internet of Things**



DoD = PIT; DHS & NIST = ICS, SCADA, CPS; Commercial = OT, IoT

UNCLASSIFIED

>500 Installations
>250K Buildings
>200K Structures

Buildings



Weapon Platforms







Operational Energy




Electrical and HVAC



Pumps and Motors



Nuclear



Typical Controller

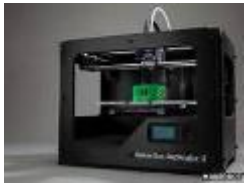
Vehicles/Charging



Medical

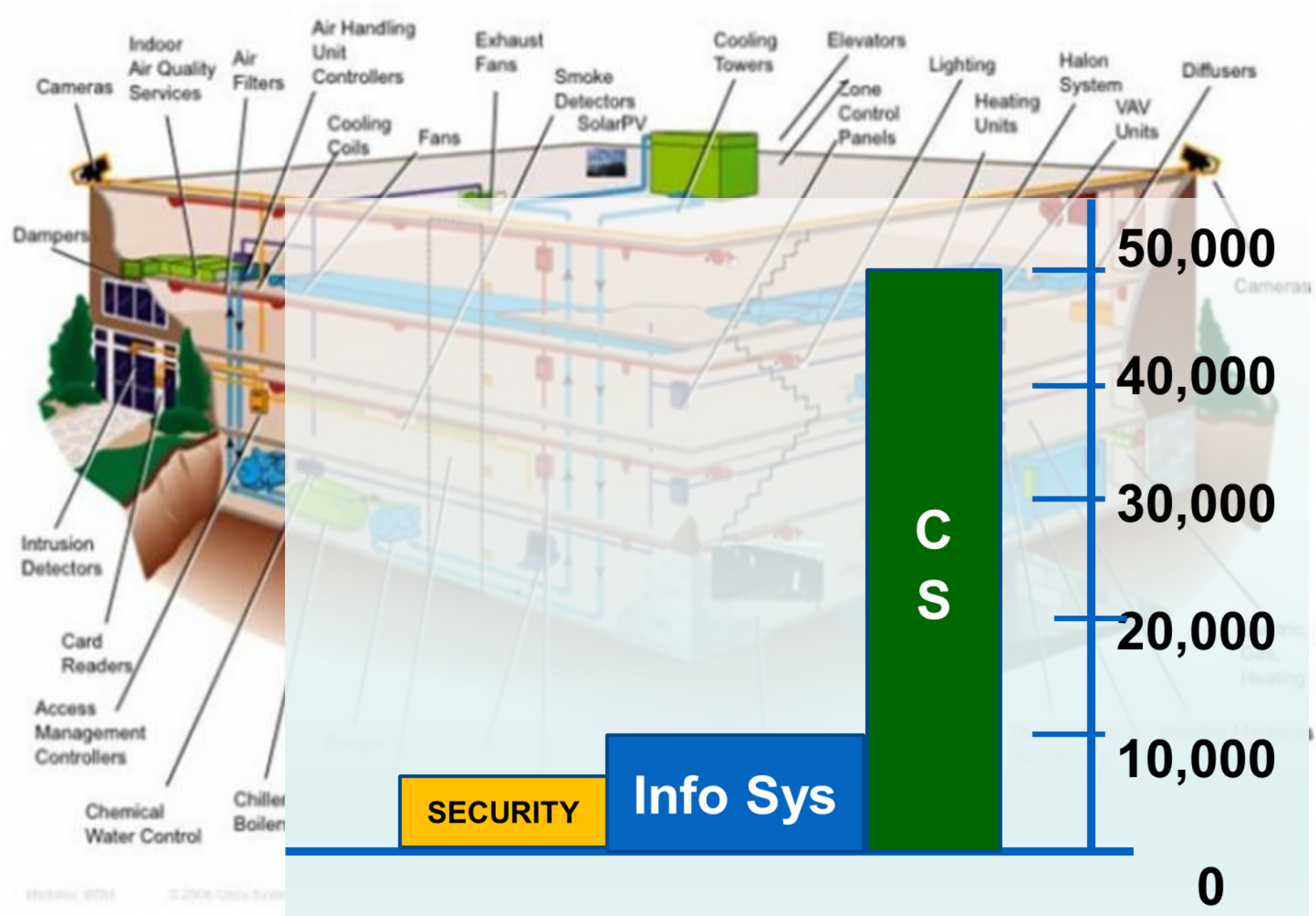


Manufacturing

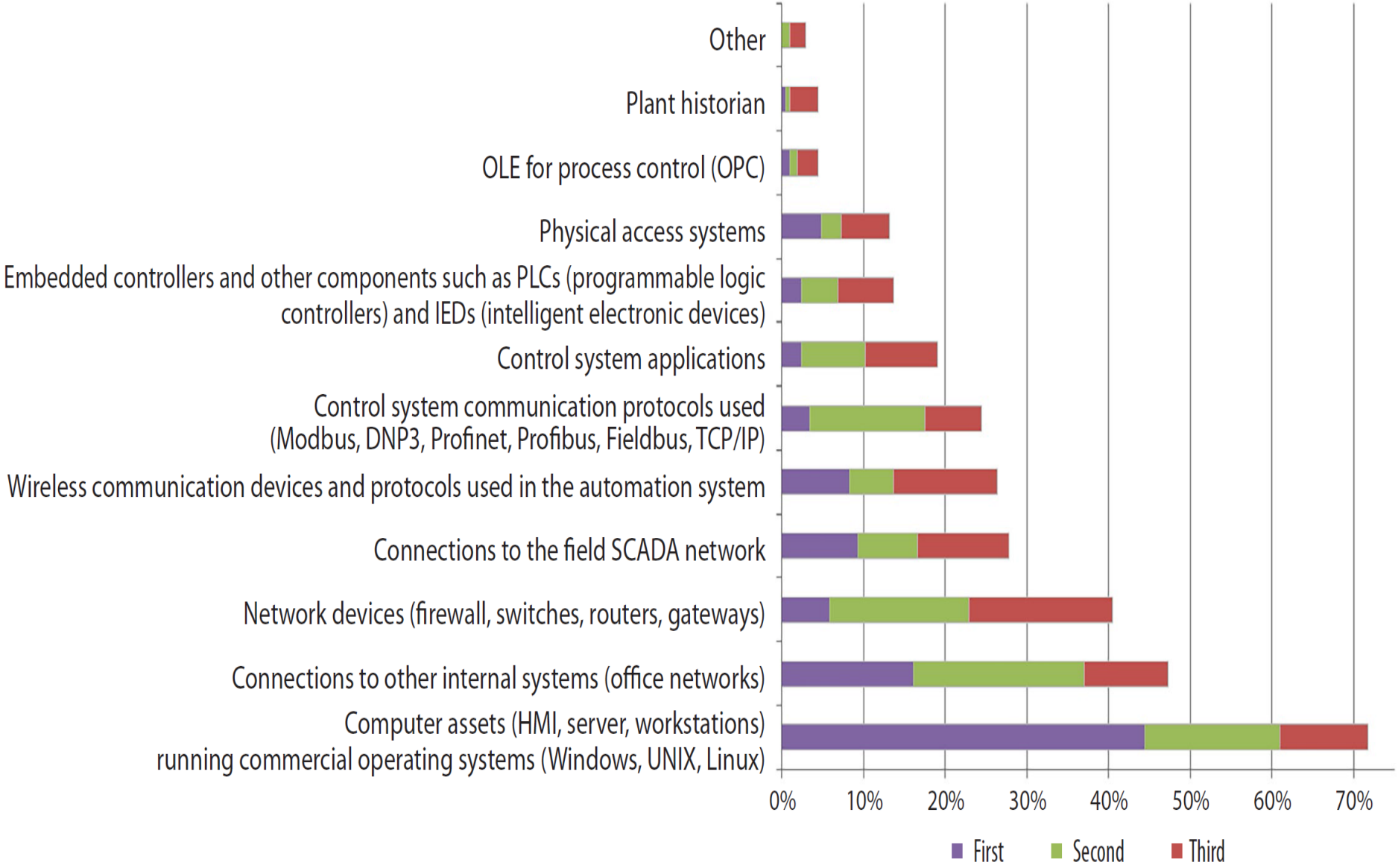



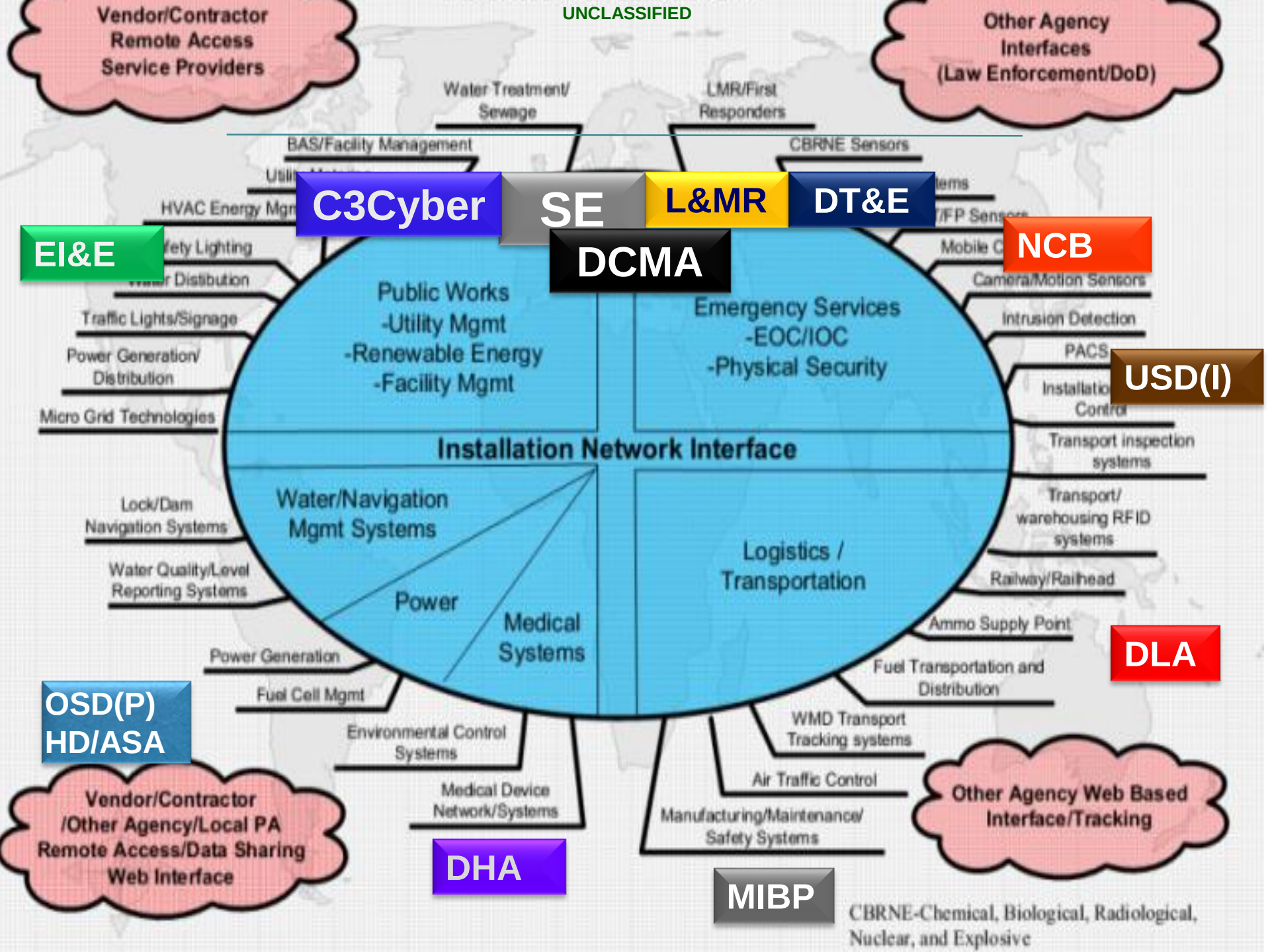

Same Commercial Device Installed Across DoD Enterprise

What's in Your Building?



SANS ‘16 Survey - 235 Companies “Greatest Risk for Compromise”





CBRNE-Chemical, Biological, Radiological, Nuclear, and Explosive

Vendors & Integrators

Acuity Brands Roam Advantage Controls ALC Alerton AIE Alerton BACtalk Alerton BCM-WEB American Auto-Matrix Auto Pilot American Auto-Matrix Andover Controls Continuum Asi controls Auto Matrix Sage Automated Logic WebCTRL Automated Logic Barber Coleman Network 8000 Bristol Babcock CAPRON Carrier Carrier Comfort Network Carrier Com-Trol Control Microsystems SCADAPack Cylon Unitron UC32 Daikin Data Aire Dell Vostro Delta Controls ORCA Distech Echelon i.Lon Emerson-Liebert EXHAUSTO Flygt ITT Industries APP 700 General Electric WESDAC General Electric Honeywell Excel 5000 Honeywell WEBs-AX HSQ Technology Invensys I/A Series Invensys Micronet Invensys Network 8000 Johnson Controls Facility Explorer Johnson Controls Metasys Johnson Controls M-Series KMC LANDIS Landis & Staefa Integral MS2000 Landis & Staefa Liebert SiteGate LOYTEC Electronics L-VIS Lynxspring JENEsys Merlin Gerin PowerLogic Microwave Data Systems Mitsubishi Motorola SCADA Systems Odessa Engineering OmniaPRO Orion Controls Paragon EC7000 Series Raco Reliable Controls MACH-ProWebSys Richards-Zeta Robert Shaw DMS RUGID Schneider Electric I/A Series Schneider Electric PowerLogic Siebe Network 8000 Siemens ACCESS Siemens Apogee Siemens Desigo PX Siemens Synco 700 Staefa Staefa/Siemens STULZ Air Technologies TAC I/A Series TAC Network 8000 TAC Xenta TAC Vista Telvent Smart Grid Solution Trane Tracer Trane Tracer Summit Trane Varitrac TREND Trend Control Systems IQ2 Tridium Vykon

Operating Software Options

•Axon CAT SARL Desigo Insight KNX STANDARD ABB Symphony Plus OptimaxRev 4 ABB Symphony Plus 800xA SV 5.1 ABB Symphony Plus Composer 6.0 ABB Symphony Plus S+ Operations 1.1 Alerton BACTalk Envision 2.0 Alerton BACTalk Envision 2.6 Alerton VisualLogic Allen-Bradley RSLogix 500 Allen-Bradley RSLogix 500, RSView32 Automated Logic ExecB 6.0 Automated Logic SuperVision WebCTRL 5.5 Automated Logic WebCTRL WebCTRL 3 Automated Logic WebCTRL WebCTRL 3.0 Automated Logic WebCTRL WebCTRL 5 Automated Logic WebCTRL WebCTRL 5.2 Automated Logic WebCTRL WebCTRL 4.1 SP1 Automated Logic WebCTRL WebCTRL Automated Logic ExecB 4.1 SP1 Automated Logic ExecB drv_lge_4-02-175 Automated Logic ExecB drv_melgr_vanilla_4-02-175 Automated Logic ExecB Automated Logic Supervision 2.6b Automated Logic WebCTRL 4 SP1B Automated Logic WebCTRL 4.1 SP1 Automated Logic WebCTRL 4.1 SP1b Automated Logic WebCTRL SVR 5.5 Calsense Command Center 4.15.11.20 Carrier Comfort Network Comfort Network 3.0 Control Microsystems ClearSCADA 2009 Ed. R2.2 Data flow Systems HyperTAC 2 Data flow Systems HyperTAC HT3 Delta Controls ORCA ORCAview 3.30 Delta Controls ORCA ORCAview 3.40 Delta Controls Orcaview 3.22 Delta Controls Orcaview 3.30 Delta Controls OrcaView 3.3 Delta Controls Orcaview 3.33 Delta Controls Orcaview Delta Controls, TAC ORCA, I/NET ORCAview, Seven Rel 2.15 EFACAC Prism ERI Siemens Insight 3.6 GE, Intellution Proficy, iFIX, FIX Desktop _, _,4.0, _ General Electric Cimplicity Plant Edition 6.1 General Electric Multilin Config Pro 5.03 General Electric Proficy Cimplicity 7.0 General Electric Proficy iFIX 4.0 Honeywell Symmetre Station 3.5 Symmetre 3.5 Honeywell Webstation-AX Niagara Niagara 3.5.40.1 HSQ Miser 6.06 HSQ Miser HSQ, Sun Microsystems Miser, Xview 6.06 Iconics Genesis32 Genesis32 8.3 Iconics Genesis32 Genesis32 9.13 Iconics HMI SCADA Solutions Genesis 32 3.12.005 InduSoft Web Studio Intellution 7 Intellution FIX32 3.5 Intellution FIX32 Intellution iFIX 3.5 Intellution IFIX Intellution iFIX Reporter ITT Flygt AquaView AquaView 1.50 Johnson Controls Metasys 6.0.0.9000 Johnson Controls Metasys GX9100 7.05A Johnson Controls Metasys Metasys 5 Johnson Controls Metasys Metasys 5.1 Johnson Controls Metasys Project Builder 5:1 Johnson Controls Metasys Project Builder 3 Johnson Controls Metasys 5 Johnson Controls Metasys 12.04 Johnson Controls Metasys 2.0.0.70.0 Johnson Controls Metasys 5.2.0.5400 Johnson Controls Metasys Johnson Controls M-Graphics 5.3 Microsoft Explorer N/A N/A N/A N/A Pneu-Logic Pneu-Logic RACO RACO 3.14 Rainbird MAXICOM2 Central Control 4.3 ReLab Software ClearView-SCADA 7.2.8 Reliable Controls MACH ProWebSys RC-Studio 2.0 Robert Shaw Digital Management System Operator Interface 11.0 Rockwell FactoryTalk Service Platform 2.30 Rockwell FactoryTalk View, Rsview Site Editiion, Supervisory 6.0, 6.0 Rockwell Factory Talk 6.0 Rockwell Automation FactoryTalk View Machine Edition 5.1 Rockwell Automation FactoryTalk View Site Edition 4.0 Rockwell Automation FactoryTalk View Site Edition 5.1 Rockwell Automation FactoryTalk View Site Edition Rockwell Automation RSView Supervisory Edition 4.0 Rockwell Automation RSView Supervisory Edition Rockwell Automation RSView32 7.600.00 ScadaTEC SCADASIS 5.8.14.213 Schneider Electric PowerLogic ION Enterprise 5.6 Schneider Electric PowerLogic ION Enterprise Siebe Network 8000 Signal 4.4.1 Siemens S7 300 STEP 7 Siemens Apogee Insight Siemens Desigo Insight Siemens Insight Desigo Insight 2.31 Siemens Insight Desigo Insight 2.35.021 Siemens WinPM.Net 3.2 SP3 SUBNET Solutions SubSTATION Explorer 1.3.0 SUBNET Solutions SubSTATION Explorer 1.5.7 Sun Microsystems Xview 3.2 Symantec Backup Exec 2011? TAC 1/A Series WorkPlace Tech 5.7 TAC I/A Series Workbench TAC I/A Series WorkPlace Tech 5.7.2 TAC 4.1 TAC Signal, XPSI & ZPSIPC Teletrol eBuilding Telvent OaSys DNA 7.4.* Trane Tracer SC Tracer 3.5 Trane Tracer Summit Tracer 11 Trane Tracer Summit Tracer 16 Trane Tracer Summit Tracer 17 Trane Tracer Summit V14 Tracer 14 Trane Tracer Summit V16 Tracer 16 Trane Tracer Summit V17 Tracer 17 Tridium Vykon Niagara 2.301.428 Tridium Vykon Niagara 2.301.430.v1 Tridium Vykon Niagara 2.301.431.v1 Tridium Vykon Niagara 2.301.514 Tridium Vykon Niagara 2.301.514.v1 Tridium Vykon Niagara 2.301.522 Tridium Vykon Niagara 2.301.522.v1 Tridium Vykon Niagara 2.301.522.v2 Tridium Vykon Niagara 2.301.522V1 Tridium Vykon Niagara 2.301.527.v1 Tridium Vykon Niagara 2.301.529 Tridium

Device Level Controllers

AAEON Electronics AAON SS1016 ABB ACH550-UH-045A-4 ABB ACH550-UH-04A1-4 ABB ACH550-UH-246A-4 Acuity Brands Roam Gateway ADDER ADDERLink INFINITY ALIF 1000R-US ADDER ADDERLink INFINITY ALIF 1000T-US Advantech Touch Panel Computer TCP-1770H-C2BE Advantech Touch Panel Computer TPC-1780H Advantech Touch Panel Computer TPC-650H AEG BLR-CX 04R AEG Schneider Automation Modicon Micro 612 Alerton VLC-1188 Alerton VLC-444 Alerton VLC-550 Alerton VLC-853 Alerton BACtalk BCM-PWS Alerton BACtalk VAV-SD Alerton BACtalk VLC-1180 Alerton BACtalk VLC-1188 Alerton BACtalk VLC-444 Alerton BACtalk VLC-550 Alerton BACtalk VLC-651R Alerton BACtalk VLC-660R Alerton BACtalk VLC-853 Allen-Bradley Allen-Bradley CompactLogix L23E Allen-Bradley CompactLogix L32E Allen-Bradley ControlLogix 1756-A10 Allen-Bradley ControlLogix 1756-L61 Allen-Bradley ControlLogix OEM Allen-Bradley FlexLogix 1794-L34 Allen-Bradley FlexLogix 5433 Allen-Bradley FlexLogix FLEX I/O Allen-Bradley Integrated Display Computers 6181P Allen-Bradley MicroLogix 1000 1761 Allen-Bradley MicroLogix 1000 1761-L16BWB Allen-Bradley MicroLogix 1100 1763 Allen-Bradley MicroLogix 1100 1763-L16AWA Allen-Bradley MicroLogix 1100 1763-L16BWA Allen-Bradley MicroLogix 1400 Allen-Bradley Micrologix 1400 1766-L32AWAA 8/10.00 Allen-Bradley MicroLogix 1500 1764-24AWA Allen-Bradley MicroLogix 1761-NET-ENI Allen-Bradley PanelView Plus 1000 Allen-Bradley PanelView Plus 2711P-KM420D Allen-Bradley PanelView Plus 600 Allen-Bradley PanelView Plus 700 Allen-Bradley PowerMonitor 3000 Allen-Bradley PowerMonitor 3000 1404-DM A Allen-Bradley PowerMonitor 3000 1404-M405A-ENT B Allen-Bradley SLC 500 DH-485 Allen-Bradley SLC 500 SLC 5/00 Allen-Bradley SLC 500 SLC 5/02 Allen-Bradley SLC 500 SLC 5/03 Allen-Bradley SLC 500 SLC 5/04 Allen-Bradley SLC 500 SLC 5/05 Allen-Bradley VersaView 1500P Andover Controls Continuum Infinet II i2810 Andover Controls Infinity SCX 920 APC AP7960 APC PNET 1 APC Back-UPS BE350R APC Back-UPS BE750G APC Back-UPS BX900R APC Back-UPS ES550 APC Back-UPS Pro 1000 APC Back-UPS RS800 APC Back-UPS XS1500 APC Smart-UPS 1000XL APC Smart-UPS 2200 APC Smart-UPS 2200XL APC Smart-UPS 750 APC Smart-UPS AP5719 APC Smart-UPS SMT3000RM2U APC Smart-UPS SU2200NET APC Smart-UPS SU220RMXL APC Smart-UPS SU3000RMXL APC Smart-UPS SU3000XLM APC Smart-UPS SUA1000RM1U APC Smart-UPS SUA1500 APC Symettra APC Symmetra AP9617 / Symmetra 40K Arena EX III Arista ARP-2217AP Armstrong SteamEye Gateway 3000M Autoflame DTI MK6DTI Automated Logic LGR1000 Automated Logic LGR25 Automated Logic M line M0100 Automated Logic M line M220nx Automated Logic M line M4106 Automated Logic M line M8102 Automated Logic M line M8102nx Automated Logic M line Mcpu Automated Logic ME812u line ME812u Automated Logic S line S6104 Automated Logic U line UNI/32 AutomationDirect DL06 AutomationDirect DL205 AutomationDirect EA7-T10C AutomationDirect EA-T10C AutomationDirect C-More EA7-T6CL AVG EZ-T10C-F AVG EZ-T15C-FSU Axiomtek DIN-rail Embedded System rBOX201-4COM-FL Axis 214 PTZ Axis 2400PTZ Axis 241Q Axis P5512 B&B Electronics MES1B Badger Meter Disc Series 120 Badger Meter Disc Series 170 Badger Meter Disc Series 35 Badger Meter Disc Series 70 Badger Meter M Series 4000 Badger Meter Turbo Series 2000 Badger Meter Turbo Series 450 Barber Coleman Network 8000 MZ2A Basler Electric BE1-25 Basler Electric BE1-700V Basler Electric BE1-CDS220 Basler Electric BE1-GPS100 E3N2R0U Bay Controls BayNet Belkin F6C1100-AVR Belkin F6C750-AVR Bitronics PowerPlex MTWIN3 Black Box ME838A-R2 Black Box ME838A-R3 BOCA Bristol Babcock DPC 3335 Brother HL-2270DW Brother HL-4040CDN Brother HLYOC Buffalo TS-H0.0TGL\RG Buffalo TeraStation Pro TS-H03TGL-R5 CalAmp VIPER SC Campbell Scientific CR1000 Carel pCO3 Carrier 30RRB06052_00__3 Carrier 30XAB50062-03X93 Carrier Comfort Network Comfort Controller 6400 Cohen OEM Computrol 32X Control Microsystems 5000 Series 5302 Control Microsystems SCADAPack 100 Control Microsystems SCADAPack 334 Cooper Power Systems CL-6A Cooper Power Systems CL-6A WA366B67G6AR Cooper Power Systems CL-6A WE383F44K6XR CyberPower 1500ADR CyberPower CPS1500AVR Cylon Unitron UC32 Daikin McQuay MicroTech II WMC Danfoss OEM Danfoss BACLink VLT DEC LA400-A2 Dell 3000CN Dell 71PXP Dell UPS1000W Dell Color Laser Printer 1320C Dell Laser Printer 1110 Dell Laser Printer 2330dn Dell Laser Printer 3100CN Dell PowerValut MD3000i Dell PowerValut TL2000 Delta Controls ORCA DSC-1212E Delta Controls ORCA DSC-1616E Delta Controls ORCA DSC-633E Deltak OEM Digi AccelePort C/X (1P) 50000598-01 Digital Loggers Web Power Switch III Dolch ORCA-19 Dolch ORCA-19PM DROBO 902-00001-001 Eason Technology 950 Eaton RO LIC-100 HMI Eaton Power Xpert PX4000 Eaton Powerware 3105 Eaton Powerware 5125 Eaton Powerware 9125 Eaton Powerware FE2.1KVA Eaton Powerware PW9130L1500T-XL Electro Industries Nexus 1262 Electro Industries Nexus 1270-S-SWB2-20-60-4IPO-SE Electro Industries Nexus 1272 Electro Industries Shark 100S elo Touch Solutions Touch systems Elo Touch Solutions Touchmonitor ET1739L Elo TouchSystems Elster American Meter 3.5M Elster American Meter AL-425 Elster American Meter AL-800 Elster American Meter GT-3 Elster American Meter RPM Series 1.5M Elster American Meter RPM Series 2M Elster American Meter RPM Series 3.5M EMC CLARiiON CX4-120 Emerson M-Series MD Plus Encorp KWS GDU Encorp KWS2222501 Encorp UPC GDU Endress+Hausser Promass 80 Endress+Hausser Prowirl 72W EPSON FX 2190 Fireye Nexus NX6100 Flygt ITT Industries APP 700 APP700F Fuji HDC 500 Fuji Micrex-F F120S F120S Fuji Micrex-SX SPH3000MM Gamewell 1033502501VD General Electric 16SB1BB339SSS2V General Electric 16SB1CB201SDM2Y General Electric 510-0183-01A General Electric 526-2006 General Electric IC695ETM001 General Electric Fanuc 90-30 IC693CPU311 General Electric Fanuc 90-30 IC693CPU311-AD General Electric Fanuc 90-30 IC693CPU311-AE General Electric Fanuc 90-30 IC693CPU311-BE General Electric Fanuc 90-30 IC693CPU311N General Electric Fanuc 90-30 IC693CPU311T General Electric Fanuc 90-30 IC693CPU311W General Electric Fanuc 90-30 IC693CPU311-XX General Electric Fanuc 90-30 IC693CPU311Y General Electric Fanuc 90-30 IC693CPU350 General Electric Fanuc 90-30 IC693CPU352 General Electric Fanuc 90-30 IC693CPU360 General Electric Fanuc 90-30 IC693CPU363 General Electric Multilin 469 General Electric Multilin 750P5G5S5HIA20R General Electric Multilin SR489-P5-HI-A20 General Electric Multilin SR74555HI485 General Electric PACSystems RX3i General Electric PQMII PQMII General Electric RRTD RRTD General Electric Rx3i PacSystem IC694MDL240 General Electric Rx3i PacSystem IC694MDL940 General Electric Rx3i PacSystem IC695ALG112 General Electric Smart Meter kV2c General Electric SR 745 General Electric SR 750 General Electric Versamax IC200CPUE05 Genicom 3850 Hach SC100 Hadax Series 6000 Heliodyne Delta-T Pro Honeywell HC900 Honeywell XL50-MMI Honeywell Excel 5000 Q7055A BNA- Honeywell Excel 5000 Q7750A-2003 Honeywell Excel 5000 XC5010 Honeywell Excel 5000 XCL5010 Honeywell Excel 5000 XL100 Honeywell Excel 5000 XL100C Honeywell Excel 5000 XL20 Honeywell Excel 5000 XL50 Honeywell Excel 5000 XL5010 Honeywell Excel 5000 XL5010C Honeywell Excel 5000 XL50-MMI Honeywell Excel 5000 XL80 Honeywell Excel 5000 XLC50 Honeywell Excel 5000 XLC5010 Honeywell Excel 5000 XLC50-MMI Honeywell Excel 5000 XLC8010 Honeywell Excel 5000 XLC8010A HP HP 700/43 HP 8100 ELITE HP Color LaserJet 4500 HP Color LaserJet CP2025 HP Deskjet 6122 HP InkJet BC354A HP Jetdirect 170x J3258B HP LaserJet HP LaserJet 02461A HP LaserJet 4 HP LaserJet 4600n HP LaserJet 4MV HP LaserJet 5 C3916A HP LaserJet 5200tn HP LaserJet C3980A HP LaserJet CB94A HP LaserJet CP2025 HP LaserJet CP2025DN HP LaserJet CP5225DN HP LaserJet P1102W HP LaserJet P2015 HP LaserJet P4014dn HP OfficeJet 7000 E809a HP Officejet CM755A/8500A HP StorageWorks Tape Array 5300 HSQ Technology HSQ Technology 22501 HSQ Technology 86004862 HSQ Technology 8600-4862 HSQ Technology 8600-6135L HSQ Technology 8602 HSQ Technology 8602-080 HSQ Technology 8602-080A Rev E HSQ Technology 8602-RTU-080-A Rev E HSQ Technology HSQ9588T HSQ Technology V86VR-R030 iEi Technology AFOLUX LX AFL-12A Infinias Intelli-M eIDC Invensys Invensys I/A Series FCM 10E Invensys I/A Series UNC-520-2 ITRON IX100X Johnson Controls Johnson Controls Facility Explorer FX-PCG2611 Johnson Controls M Series MS-N30 Supervisory Controller Kiltech Embedded Field Controllers SX-CPU/RS-485 190715 Koyo DL205 Koyo DL206 Koyo DL207 Koyo DL250 CPU Landis & Staefa Integral MS2000 NRK16-NICO Landis & Staefa Integral RSA NRK16/A Lantronix Lantronix Universal Device Server UDS100 Lexmark Optra E312L LG V-NET PQNFB17B0 Liebert StieLink 12 Liebert StieLink 4 LOYTEC Electronics LINX LINX-101 LOYTEC Electronics L-VIS LVIS-3E100 LOYTEC Electronics L-VIS ME215 Maple Systems OIT3175 Maple Systems OIT3250-B00 Maple Systems PC217B Mcquay H62PY McQuay Maverick I OM 1077 MCS MCS-R010 MechoShade Systems SunDialer I-Con Meidensha ADC5000 Meidensha T01E-E01A Meidensha T01E-E01A-A Meidensha Uniseque RC500 MGE UPS SYS UPS 1500 MGE UPS SYS UPS 800 Mitsubishi Mitsubishi AG-150A Mitsubishi MP-22-AF Mitsubishi MP-22-AR Mitsubishi MP-22-CB Mitsubishi CITY MULTI BAC-HD150 Mitsubishi CITY MULTI GB-50ADA Mitsubishi MELSEC Q63P Mitsubishi Q Series FX2N Modicon Micro Modicon Momentum 170ADM39030 Modicon Quantum Automation Series 140CPU113 MODICON TSX Quantum Modicon TSX Series TSX3705028 Modicon TSX TSX3705028 Motion Control Engineering Motion Control Engineering 24-10-0012 Motorola MOSCAD-L Motorola SCADA Systems ACE3600 Moxa MGate IMC-101-M-SC Nalco Switch 2226 3D Trasar NETGEAR ReadyNAS 3200 NETGEAR ReadyNAS Pro NOVAR NL INC B541200039 NovaTech Orion5r Obvius Holdings AcquiSuite A8812 Odessa Engineering DiaLog Plug Okidata MicroLine 321 Turbo Okidata MICROLINE ML420 OMNTEC OEL8000II OEL8000IIP Opto 22 Opto Brian Panasonic BB-HCM531 Panasonic GN 15 Panasonic i-Pro WV-NP244 Panasonic i-Pro WV-NS202A Panasonic i-Pro WV-NW964 Patton Copper Link 2156 Perle IOLAN SCS PML ION7350 PML PowerLogic ION7300 PML PowerLogic ION7330 PML PowerLogic ION7350 PML PowerLogic ION7500 PML PowerLogic ION7550 PML PowerLogic ION7600 PML PowerLogic ION7650 PML PowerLogic ION7700 PML PowerLogic ION8600 Pneu-Logic 10A22646 Pneu-Logic PL4000 DCM Powerlynx OEM Preferred Instruments PCC-III Preferred Instruments PCC-III-0000 Preferred Instruments PCC-III-F000 Preferred Instruments PCC-III-FZ00 Pro-Face GP577R-TC11-OY ProSoft MVI46-MNET Qualitrol ITM 509 ITM RACO VERBATIM DFP RACO VERBATIM SFP Raritan CompuSwitch CS4R Raritan Dominion KX II 216 Raritan Dominion KX II DKX2-216 Raritan Dominion KX II DKX2-432 Red Lion G308 Red Lion G310C Ricoh Aficio MP C2050 RUGID RUG6D RUGID RUG7D RUGID RUG9 RUGID RUG9B RUGID RUG9D Sanyo Denki SANUPS A11H Schneider Electric 170INT11000 Schneider Electric 171CCS76000 Schneider Electric HMIPSCIDE03 Schneider Electric Modicon M340 Schneider Electric I/A Series MNB-1000 Schneider Electric Magelis XBT GT 2330 Schneider Electric Momentum Processor 171CCC96020 Schneider Electric Momentum Processor 171CCS78000 Schneider Electric Powerlogic CM2000 Schneider Electric Powerlogic CM3000 Schneider Electric Powerlogic CM4000 Schneider Electric Powerlogic ECC Schneider Electric Powerlogic EGX 100 Schneider Electric Powerlogic EGX 200 Schneider Electric Powerlogic EGX 400 Schneider Electric Powerlogic enercept Meter Schneider Electric Powerlogic Energy Meter Schneider Electric PowerLogic ION7330 Schneider Electric PowerLogic ION7350 Schneider Electric PowerLogic ION7500 Schneider Electric PowerLogic ION7600 Schneider Electric PowerLogic ION7650 Schneider Electric PowerLogic ION8300 Schneider Electric PowerLogic PM710 Schneider Electric PowerLogic PM850 Schneider Electric Powerlogic Power Meter Schneider Electric TSX Momentum Schneider Electric TSX Momentum 171CCC9803 Schneider Electric TSX Quantum 170-ENT-110-00 Schneider Electric Xenta 280 282 Schneider Electric Xenta 300 301 Schweitzer Engineering Laboratories SEL-2020 Schweitzer Engineering Laboratories SEL-2032 Schweitzer Engineering Laboratories SEL-2407 Schweitzer Engineering Laboratories SEL-2411 Schweitzer Engineering Laboratories SEL-2440 Schweitzer Engineering Laboratories SEL-3332 Schweitzer Engineering Laboratories SEL-351S-7 Schweitzer Engineering Laboratories SEL-3530 Schweitzer Engineering Laboratories SEL-451 Schweitzer Engineering Laboratories SEL-487E Schweitzer Engineering Laboratories SEL-587Z Schweitzer Engineering Laboratories SEL-700G Schweitzer Engineering Laboratories SEL-751A Schweitzer Engineering Laboratories smart-UPS SEL-3332 Seiko TS-2540 Siebe Siebe CP-8161-333-3 Siebe DMS-3501 Siebe MSC-P1502 Siebe MSC-P1504-D Siemens MP277 10 TOUCH Siemens PXC36 Siemens ACCESS 9510 Siemens Apogee Series 200 MEC Siemens Apogee 545-793 Siemens Apogee AEM200 Siemens Apogee Power MEC Siemens Apogee Power MEC 1200 Siemens Apogee Power MEC 1210 Siemens Apogee Power Mec 1210E Siemens Apogee Power MEC 40 Siemens Apogee Power MEC 40 System 600 Siemens Apogee Power Mec Series 200 Siemens Apogee Power Mec System 600 Siemens Apogee PXC100 Siemens Apogee PXC24 Siemens Desigo PX PXC36 Siemens Desigo PX PXC52 Siemens Desigo RCX PXR11 Siemens Desigo RCX PXR12 Siemens HydroRanger 200 7ML50342AA01 Siemens SIMATIC S7-1200 Silex SX-3000GB Solar OEM STULZ Air Technologies Fieldserver DCC828 Symmetricom bc635PCI Symmetricom TrueTime 820-202 Symmetricom TrueTime XL-DC TAC Xenta 302/N/P Teletrol eBuilding Concentrator Telvent Smart Grid Solution SAGE 2300 Telvent Smart Grid Solution SAGE 2400 Terminator T1H-EBC100 Terminator T1H-EBC101 Toshiba OIS-DS52 Total Control Products QuickPanel Trane EMTF000AAC02100 Trane OEM Trane TNS1 Trane UC800 Trane Tracer CH530 Trane Tracer EX2 Trane Tracer MP503 Trane Tracer MP580/581 Trane Tracer MP581 Trane Tracer SC Trane Tracer Summit BCU Transformative Wave Technologies eIQ nSITE 600 Trend Control Systems IQ250 Trend Control Systems NXNI Trend Control Systems XCITE Trend Control Systems IQ2 IQ204 Trend Control Systems IQ21x IQ210 Trend Control Systems IQ21x IQ233 Trend Control Systems IQ21x IQL-SDK Trend Control Systems IQ22x IQ220 Trend Control Systems IQ24X IQ241 Trend Control Systems IQ25 Woodward 505 DC100-21-11-1M

Difference Between DoD & Commercial Products = None!

"8 Star Memo"

Cybersecurity of DoD Critical Infrastructure ICS

COMMANDER, U.S. PACIFIC COMMAND
(USPACOM)
CAMP H.M. SMITH, HAWAII 96861-4028

February 11, 2016

The Honorable Ash Carter
Secretary of Defense
The Pentagon, Washington D.C.

Mr. Secretary,

We respectfully request your assistance in providing focus and visibility on an emerging threat that we believe will have serious consequences on our ability to execute assigned missions if not addressed – cybersecurity of DOD critical infrastructure Industrial Control Systems (ICS). We believe this issue is important enough to eventually include in your cyber scorecard. We must establish clear ownership policies at all levels of the Department, and invest in detection tools and processes to baseline normal network behavior from abnormal behavior. Once we've established this accountability, we should be able to track progress for establishing acceptable cybersecurity for our infrastructure ICS.

The Department of Homeland Security reported a seven-fold increase in cyber incidents between 2010 and 2015 on critical infrastructure (e.g., Platform Information Technology (PIT) systems, ICS, and Supervisory Control and Data Acquisition (SCADA) systems) that control the flow of electricity, water, fuel, etc. Many nefarious cyber payloads (e.g., Shamoon, Shodan, Havex and BlackEnergy) and emerging ones have the potential to debilitate our installations' mission critical infrastructure.

As Geographic Combatant Commanders with homeland defense responsibilities and much at stake in this new cyber-connected world, we request your support.

Sincerely and Very Respectfully,

WILLIAM E. GORTNEY
Admiral, U.S. Navy
Commander, U.S. Northern Command

Sincerely and Very Respectfully,

HARRY B. HARRIS
Admiral, U.S. Navy
Commander, U.S. Pacific Command

- **Establish Clear Ownership**
- **Include in Scorecard**
- **Invest in Detection Tools**
- **7x cyber incidents**

What's the Real Cyber Risk?

"The threat is real and the risks are high, but our exposure is low…the control systems don't connect to the internet."

The risk of a damaging cyberattack is "greater than zero … the real threat is Mother Nature and humans doing stupid stuff."

Marcus Sachs, CSO of the North American Electric Reliability Corporation (NERC)

NERC SME: Utility Cyber Attack "Very Unlikely"

What's the Real Cyber Risk?

- Project SHINE (SHodan INtelligence Extraction) scanned the internet looking for SCADA and ICS devices. "Found more than 2 million (control) system devices directly connected to the Internet"
- Targeted ICS attacks in the US have caused, "loss of electric and water SCADA, damage to manufacturing lines, shutdown of HVAC systems, and damage to facility equipment including critical motors"

Control Systems Cybersecurity Expert, Joseph M. Weiss, recognized international authority on cybersecurity, control systems and system security

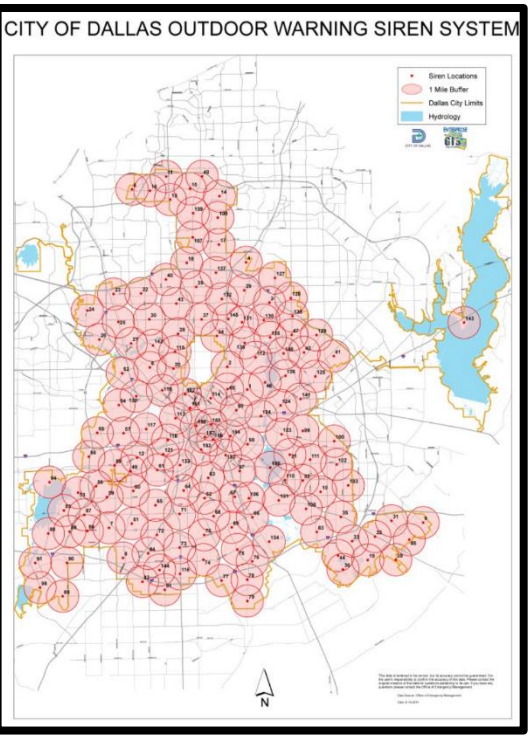
30yr SME: Utility Cyber Attack "Very Likely"

Mission Assurance Dependency

- Mar'16: RPA mission based in U.S. was flying a targeting mission overseas
- Routine maintenance power outage stateside, the RPA feed temporarily lost power
- Target was able to get "away and is able to continue plotting against the U.S. and our allies"

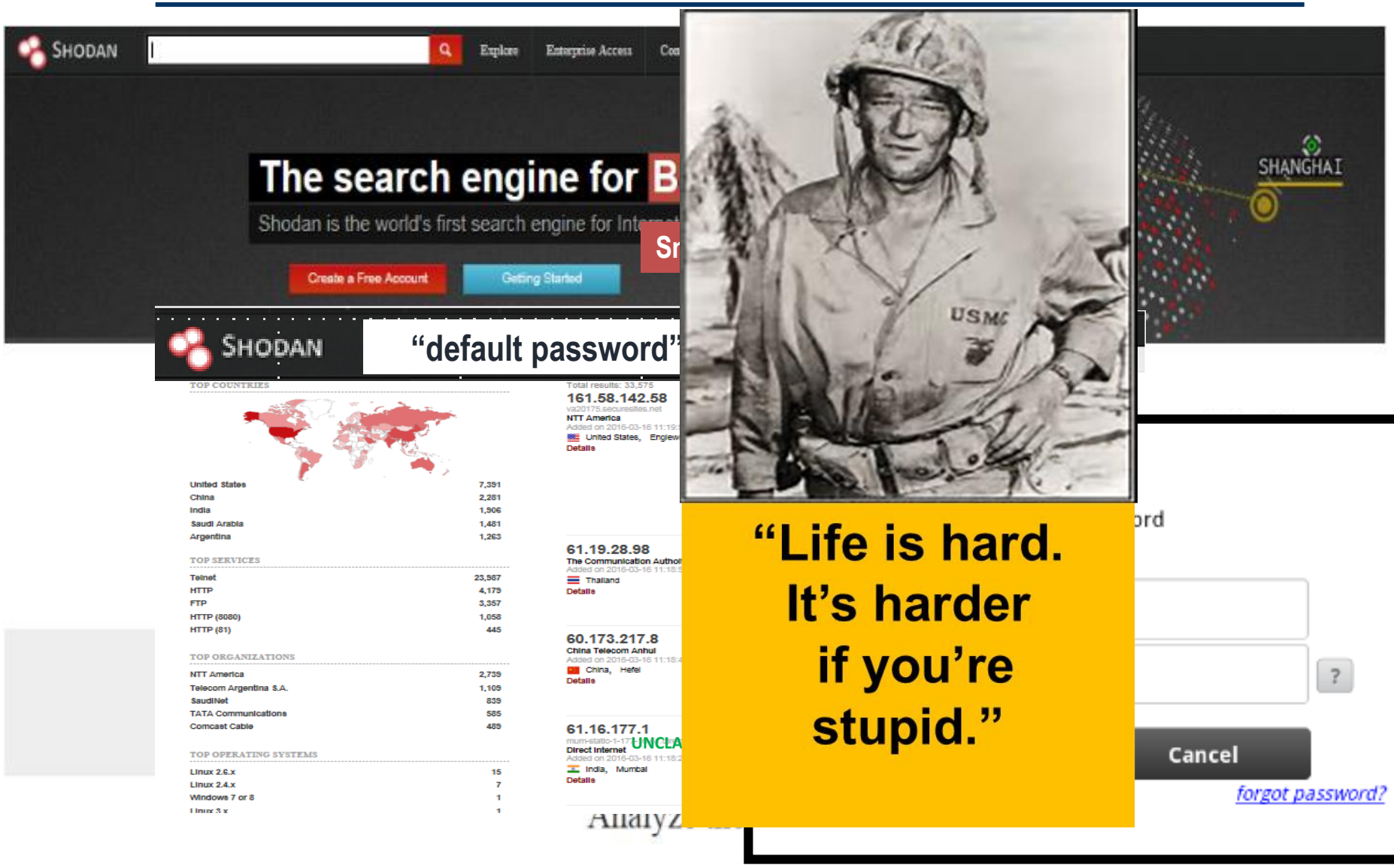
Was it Maintenance or Cyber? How Can You Tell?

Tornado Sirens Hacked in Dallas Texas



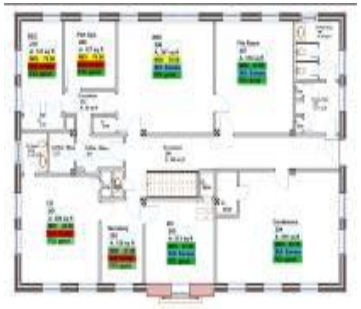
- 11:42 pm 156 emergency weather sirens blared
- 90 min to 1.3 million residents
- 1,000s of calls flooded Dallas 911 system
  - Real emergency responses delayed
- 1:20 a.m. officials: “unplug radio systems & repeater, turn siren system completely off.”
- Mayor Mike Rawlings called hack “an attack on our emergency notification system.” Urged upgrades to Dallas’s chronically and sometimes dangerously wonky electronic infrastructure and promised the city would “identify and prosecute those responsible.”

Locating Connected Devices



What's the Risk of Exposing Energy Consumption Data?

Facility Level



- Generators for individual critical loads

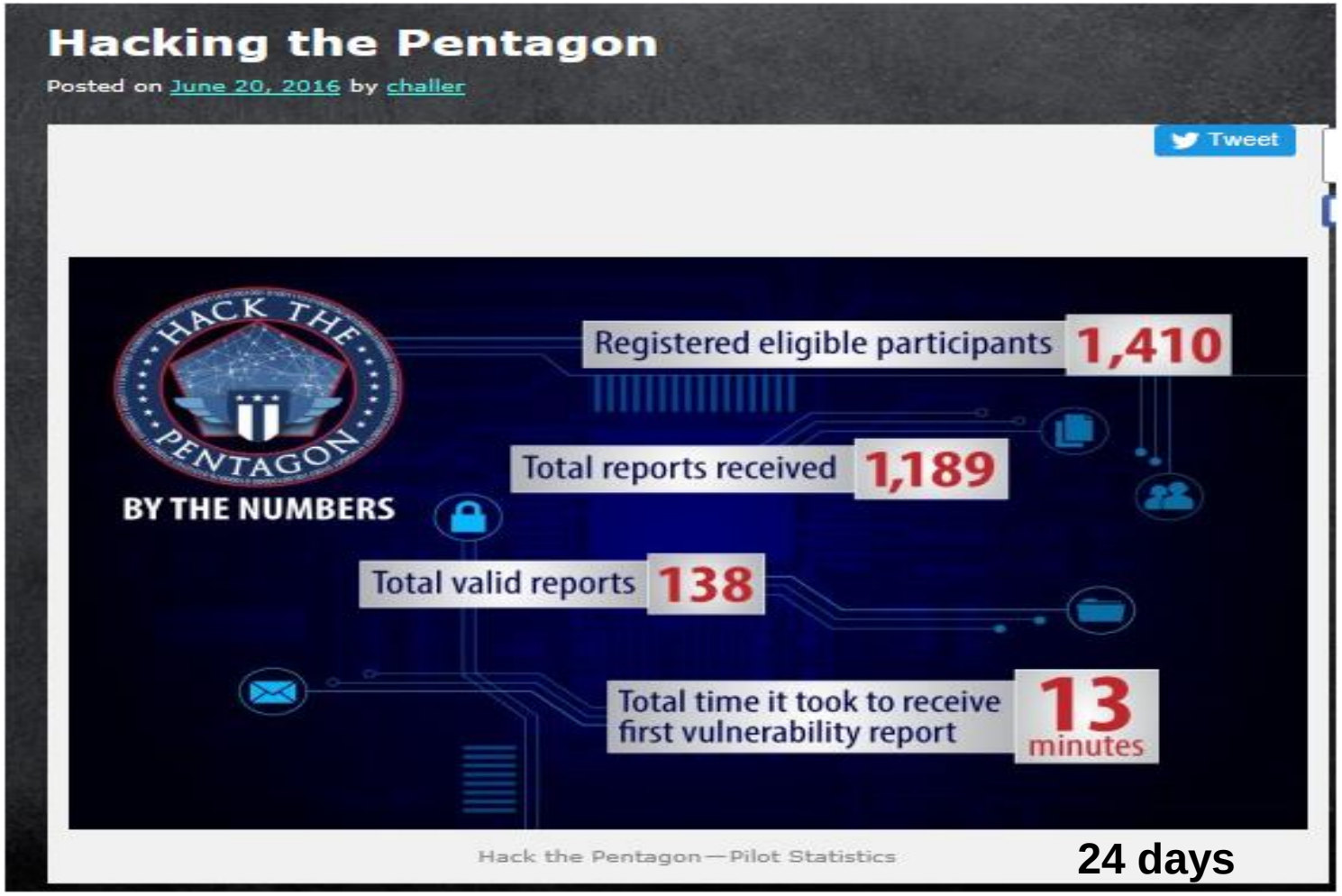
Site / Campus Level

Regional / Enterprise Level

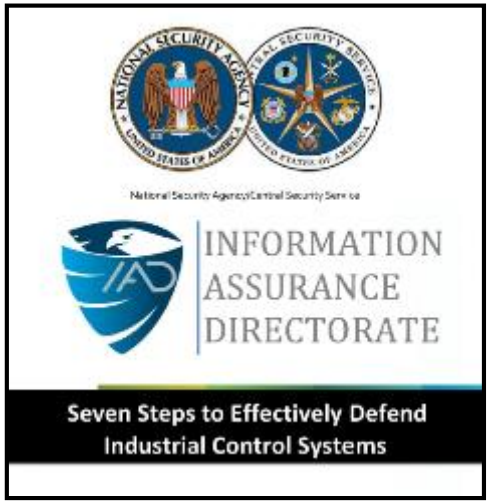
Usage or Criticality?

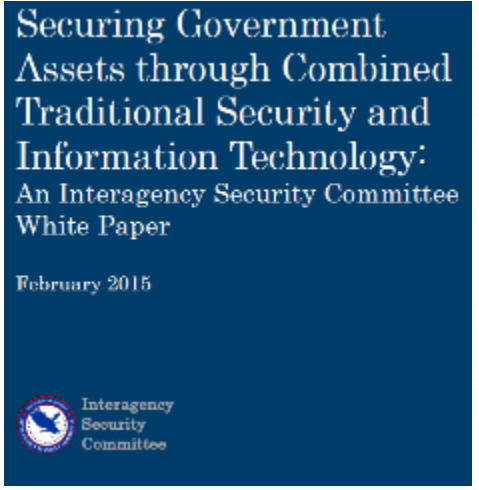
"All Energy Data is UNCLASSIFIED"…True?

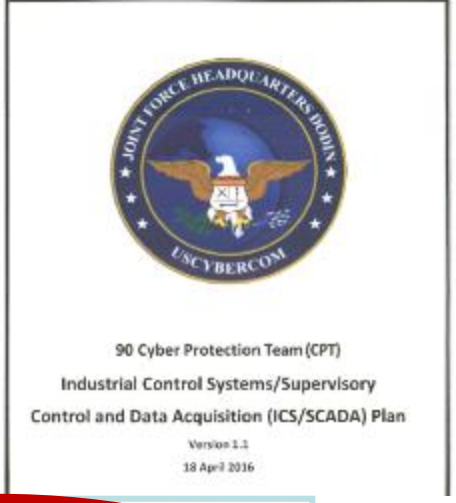
Embracing Silicon Valley Crowdsourcing: "Bug Bountys" *Will Utilities & ICS be Next?*

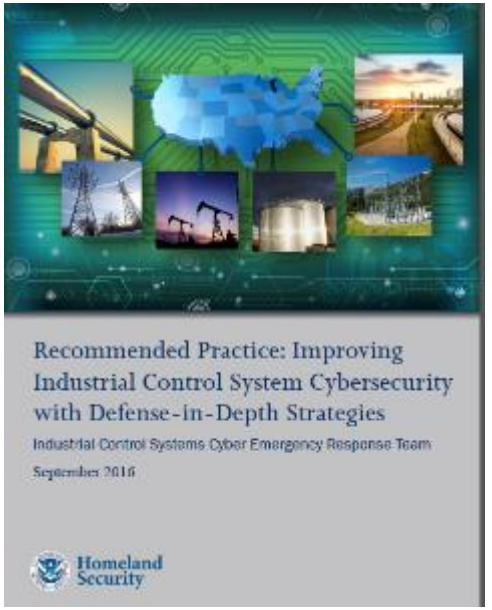


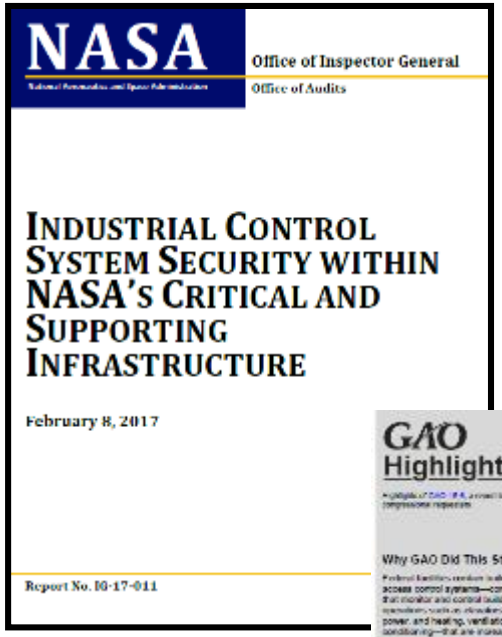
Cost: $175K vs. Typical Contractor $1M

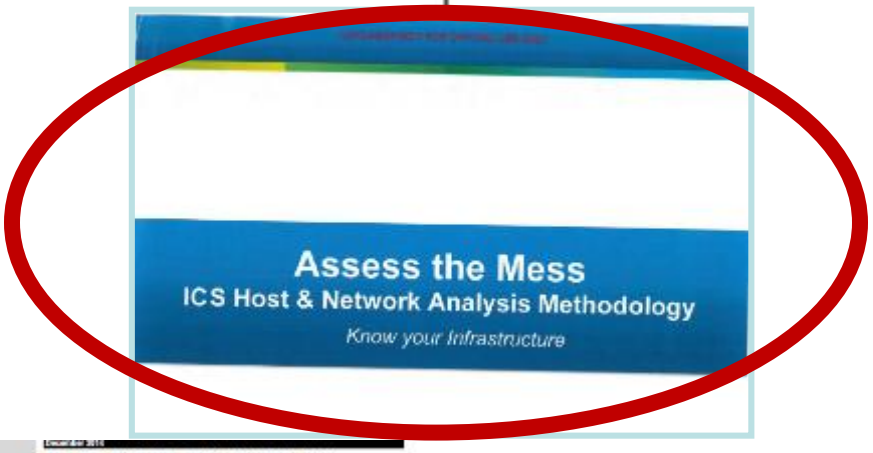


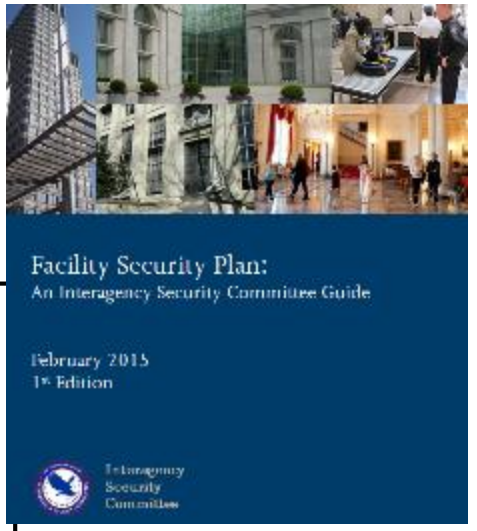


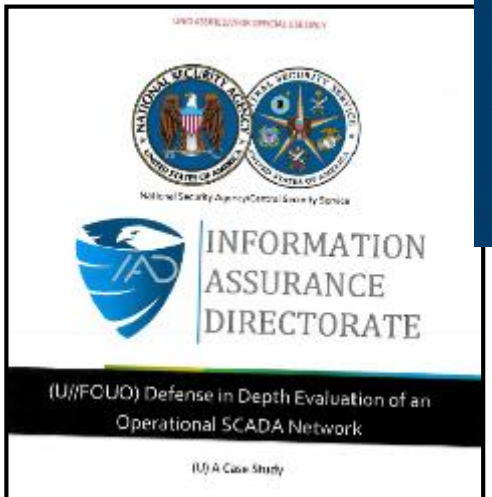












UNCLASSIFIED

What's in Your Cloud?

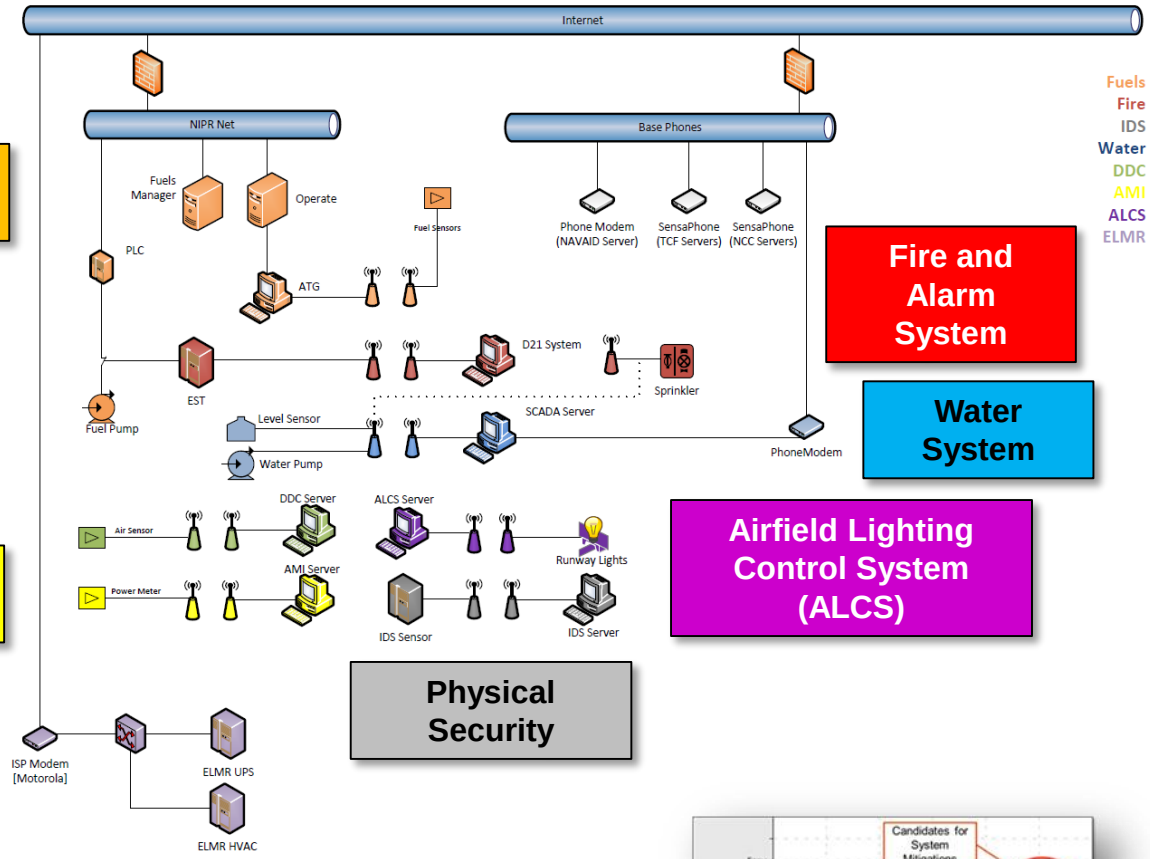
- **Infrastructure as a Service (IaaS)**
  - provide pay-per-utility pricing, dynamic scaling, security control, faster provisioning and guaranteed performance levels
- **Platform as a Service (PaaS)**
  - deliver lower operational cost, faster development, and seamless integration
- **Software as a Service (SaaS)**
  - improves upgrade cycle times, automated backups, and location independence

MindSphere, Siemens PaaS

IBM Bluemix

Better & More Secure to Outsource? $ vs Security

Example – Topology & Mission Heat Map



Fuel System

HVAC

Automatic Metering

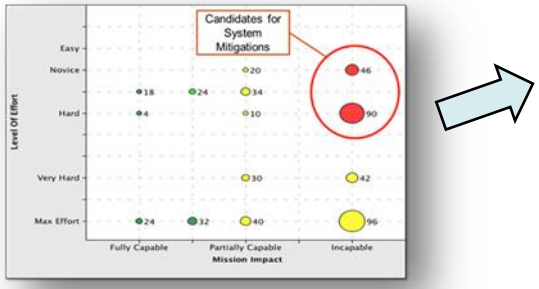
ELMR

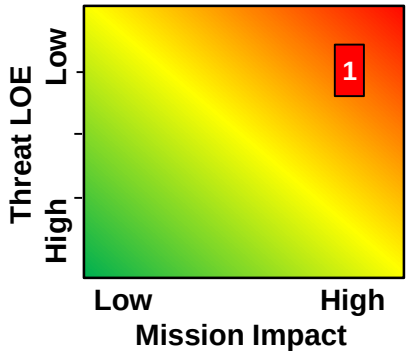
Fire and Alarm System

Water System

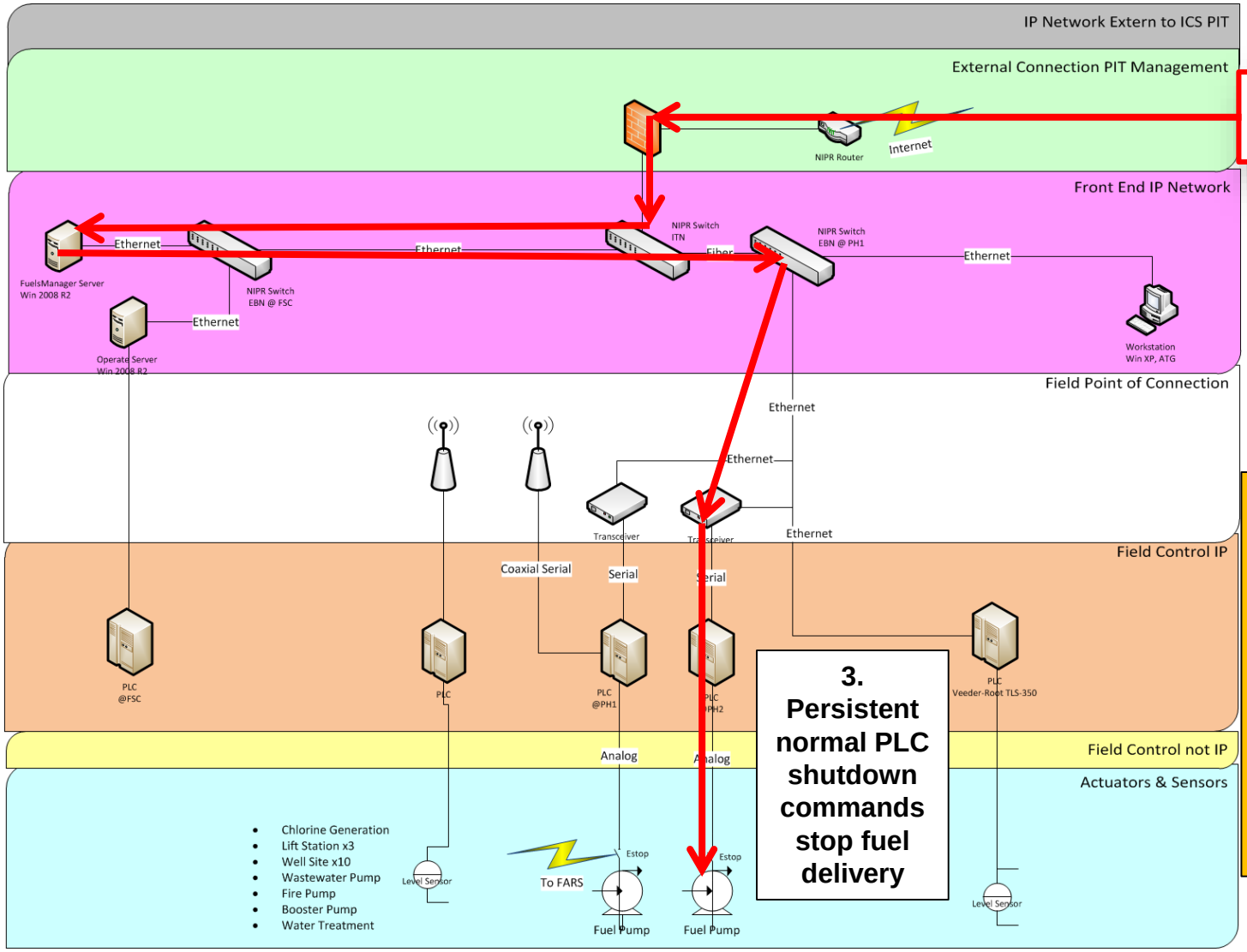
Airfield Lighting Control System (ALCS)

Physical Security





Example: Disruption of Fuel System



1. Phishing attack via the Internet

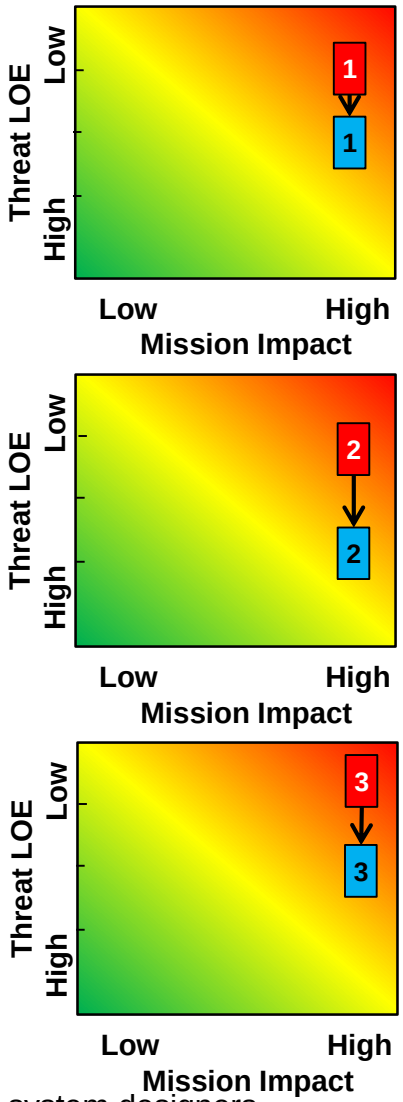
2. Reconnaissance on NIPRNet to identify PLC controller of pump

3. Persistent normal PLC shutdown commands stop fuel delivery

- Specific Attack: Internet phishing attack targets unpatched system
- Level of Effort: Script Kiddies to access CS systems
- Impact: Lack of ability to execute OPLAN

Mitigations & Results

#	NIST CSF Phase	Finding	Mitigation	Blue Skill Level	Estimated Cost	System	System Owner
1	Protect	Extensive connect-ivity	Isolate networks	I - Patch (IAT / IAM)	$	NIPRNET	Comms squad
2	Identify	No CS monit at system level	Establish CS monitoring	III - Active Defense	$$	Network Defense	Comms squad
3	Protect	Lack of patch mgt system	Perform config mgt	I - Patch (IAT / IAM)	$$$	Fuels Mgr	DLA

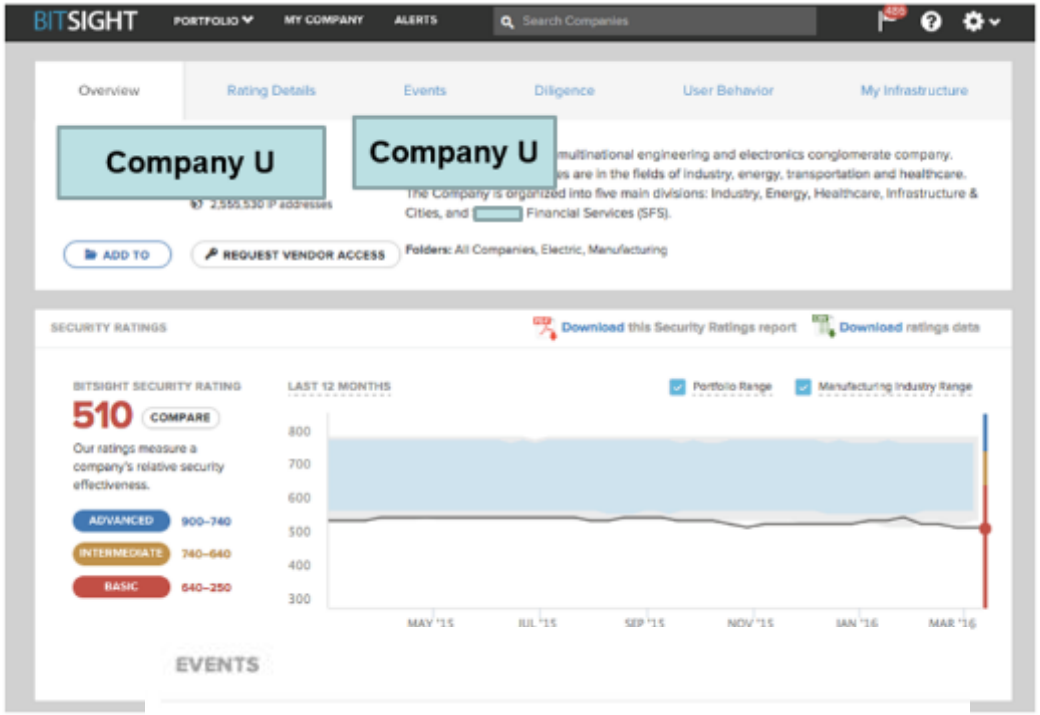


Before mitigation → After mitigation

Blue skill level: I – patching, II – investigating, III – active defense, IV – integrators, V – architects, system designers
$: 10Ks, $$: 100Ks, $$$: 1 Ms, $$$$: 10Ms, $$$$$: 100Ms; Mitigation effect levels based on DSB Tiers 1-6

“Cyber Trust” Rating…What’s Yours?

- Rating # Correlates to Breach Potential
- Detailed Event and Configuration Information via External Parties



EVENTS

Botnet Infections	F
Spam Propagation	B
Malware Servers	A
Unsolicited Communication	B
Potentially Exploited	C

DILIGENCE

SPF Domains	C
DKIM Records	F
TLS/SSL Certificates	C
TLS/SSL Configurations	B
Open Ports	C
DNSSEC Records beta	C
Application Security beta	C

USER BEHAVIOR

File Sharing	D

OTHER

Data Breaches	A

Events are observed incidents of compromise on a company's network. These include risk vectors such as botnet infections and malware servers. Industry averages are calculated from similarly sized companies.

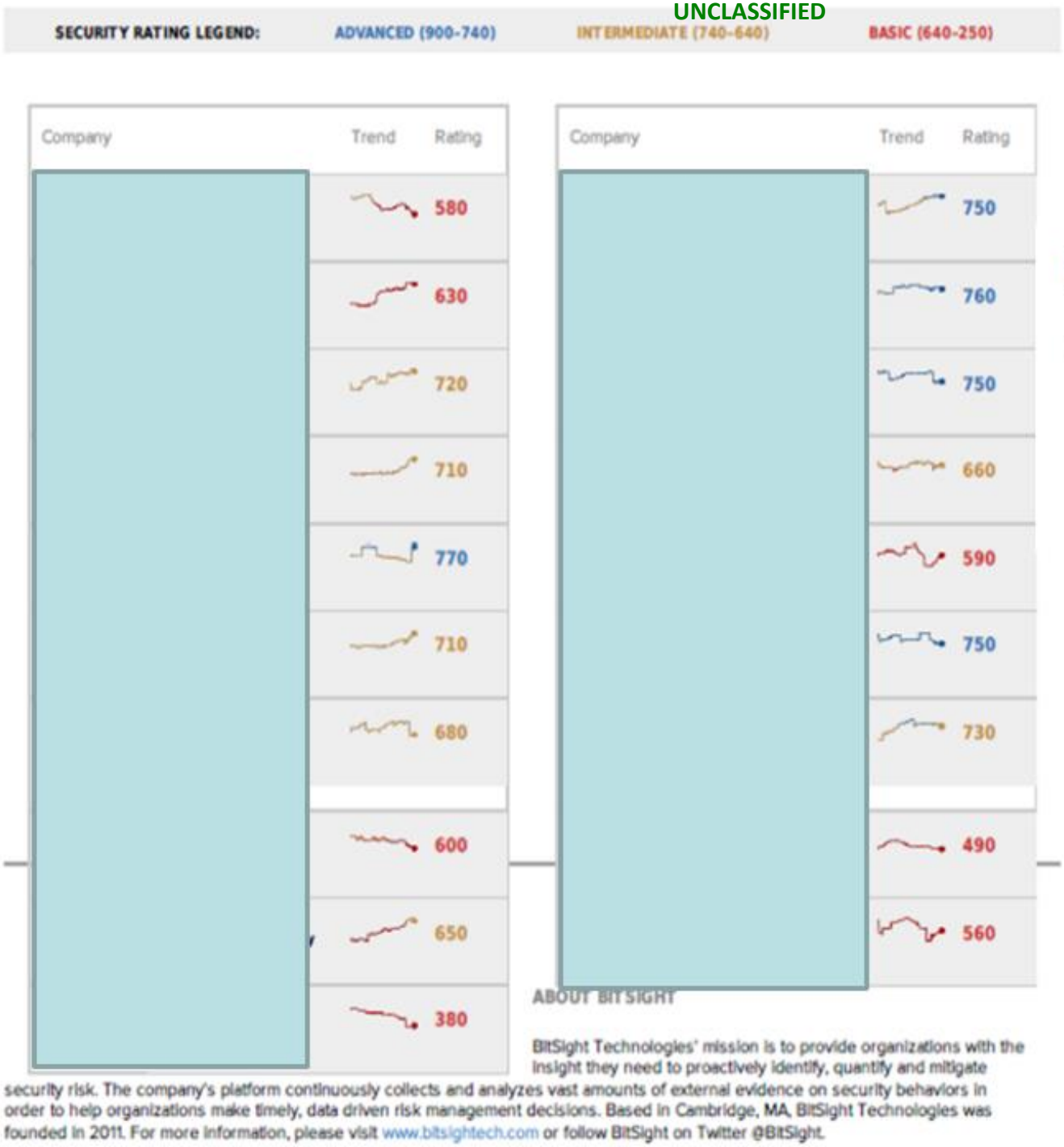
THIS WEEK	PAST YEAR	AVERAGE EVENT DURATION
10	1,416	2.8 days

3.4% faster to resolve events than the Manufacturing industry average.

2.8 days Company U

2.1 days Portfolio average

2.9 days Manufacturing industry average



BITSIGHT
Security Rating Report

PORTFOLIO STATISTICS

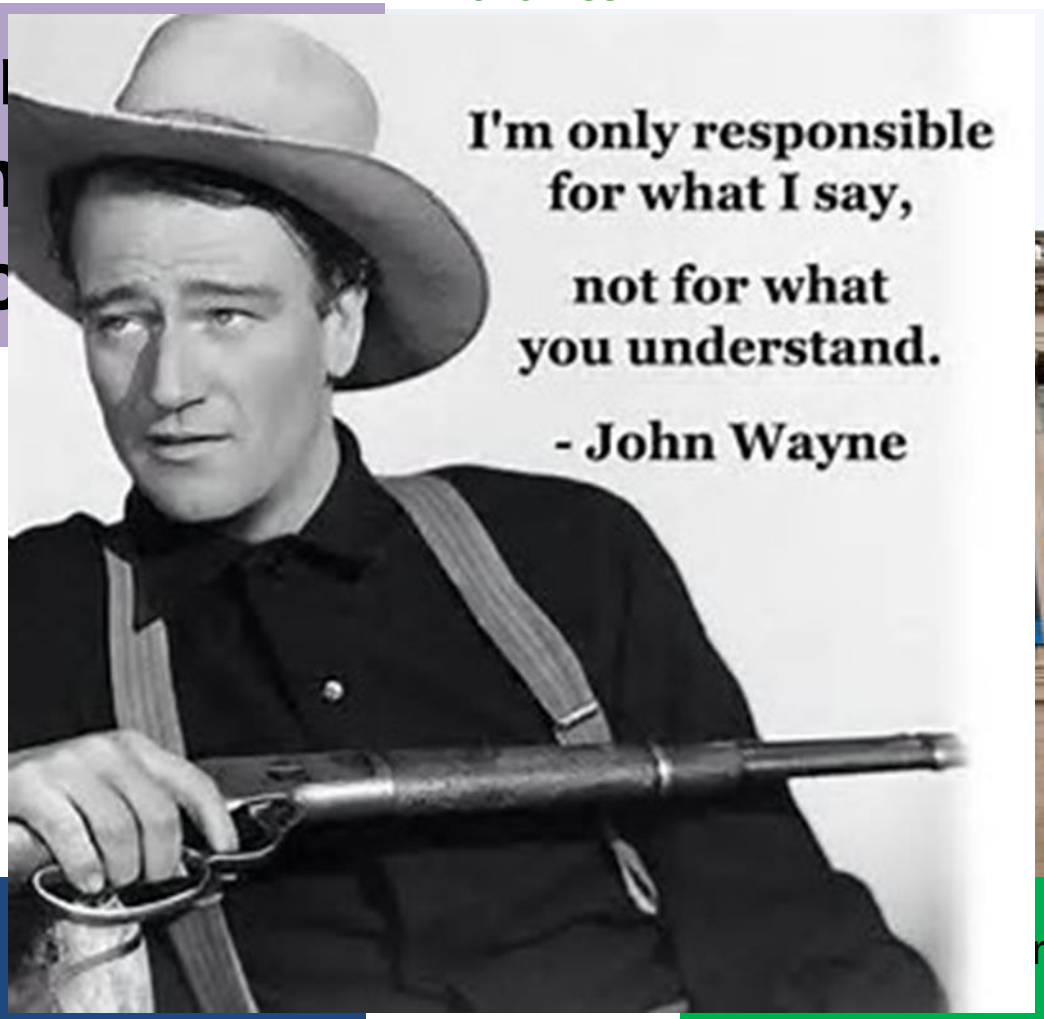
COMPANIES	IP ADDRESSES	INDUSTRIES
19	9,868,600	5

MEDIAN SECURITY RATING	RANGE OF SECURITY RATINGS
660	380-770

Analysis of 27,458 companies reveals companies with ratings >400 are

5X *more likely* to have experienced a publicly disclosed breach.

US Cha
Comm
Dec



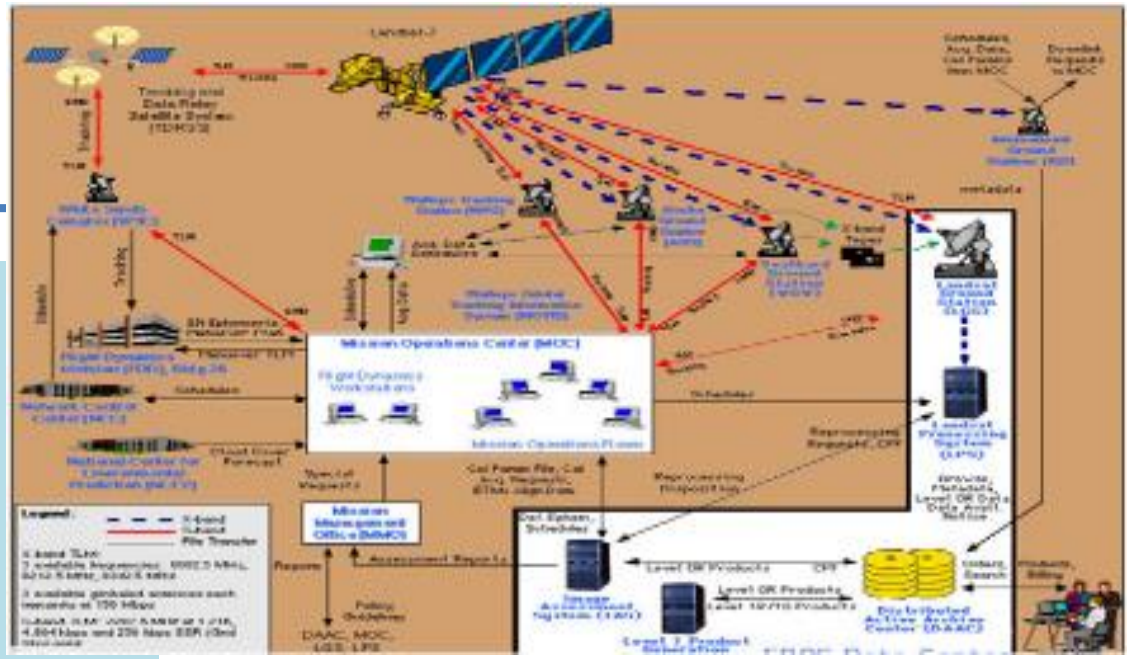
- Not mine
- Not funded

ng

- Not Mine
- Not funded

http://abcnews.go.com/International/chinese-hack-us-chamber-commerce-authorities/story?id=15207642

Discussion



Information Systems

Control Systems

Who's Role? Detect, Mitigate & Recover from Cyber Exploit

WHAT'S NEXT?

….Your organization failed to consider impact of exploiting control systems….

Target Retail Stores - 2013

BACKDOOR ATTACK

The attackers backed their way into network by compromising a 3rd-party vendor to steal data.

Kemuri Water Company - 2016

PLC ATTACK

Hack accessed hundreds of PLCs used to manipulate control applications altering chemicals.

Saudi Aramco & RasGas

ENTERPRISE ATTACK

Networks infected with the Shamoon virus erased information causing enterprise network outages.

Ukraine Utilities - 2015

SCADA ATTACK

Left 225,000 customers in the dark. 1st successful cyber attack to knock a power grid offline.

.

Project Basecamp - 2012

PLC ATTACK

A team used a penetration test on PLCs to realize how badly vulnerable their SCADA/ICS were .

Unnamed" Steel Mill, Germany - 2014

INSIDER ATTACK

Hackers disrupted networks to access automation equipment resulted in massive damage.

"Unnamed" Steel Mill - 2011

ENTERPRISE INFECTION

The Conficker worm infected the control network causing an instability in the communications.

New York Dam - 2013

BACKDOOR ATTACK

Iranian hackers tried to open flood gates. Was this a dress rehearsal for something bigger?

Natanz Nuclear Facility - 2010

SCADA MALWARE

Stuxnet infected the air-gapped control network bypassing causing damage to centrifuge.

Google HQ, Wharf - 2013

MISS-CONFIGURE

SHODAN discovered over 21,000 miss-configured building automation systems.

Maroochy Water System - 2010

INSIDER ATTACK

Disgruntled ex-employee hacks into the water system and floods the community of sewage.

New Malware Deliberately Destroys IoT Devices

April 7, 201

- Uses known default user credentials to attack unsecured IoT devices & destroy them
- Discovered by Radware - BrickerBot.1 / BrickerBot.2 – targets Linux BusyBox-based device open Telnet ports
- Renders devices inoperable w/in seconds via PDoS (*Permanent Denial of Service*) or "phlashing" attacks
  - BrickerBot.1 via worldwide IPs likely assigned to Ubiquiti network devices, BrickerBot.2 attacks are hidden behind Tor exit nodes and difficult to trace
- Motive uncertain; it destroys w/o benefiting destroyer
- Could be vigilante alerting users to unsecured devices.

ENERGY, INSTALLATIONS AND ENVIRONMENT

DoD & Commercial Resources

DoD CIO Knowledge Service (requires CAC) https://rmfks.osd.mil/login.htm

Department of Defense Advanced Control System Tactics, Techniques, and Procedures (TTPs) 2017:
http://www.wbdg.org/pdfs/aci_ttp_rev1_2017.pdf

UFC 4-010-06 CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS Sept 2016
https://wbdg.org/ffc/dod/unified-facilities-criteria-ufc/ufc-4-010-06

Strategic Environmental Research and Development Program (SERDP) and Environmental Security Technology Certification Program (ESTCP) [info & funding solicitations]
https://serdp-estcp.org/Investigator-Resources/ESTCP-Resources/Demonstration-Plans/Cybersecurity-Guidelines

DoD OASD(EI&E) and Federal Facilities Council (FFC), under the National Research Council (NRC) sponsored a 3-day Building Control System Cyber Resilience Forum in Nov '15.
http://sites.nationalacademies.org/DEPS/FFC/DEPS_166792

DoDI 5000.02 Cybersecurity in the Defense Acquisition System Jan 2017
http://www.dtic.mil/whs/directives/corres/pdf/500002_dodi_2015.pdf

Whole Building Design Guide website cyber references
http://www.wbdg.org/resources/cybersecurity

Tools
https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A
https://ics-cert.us-cert.gov/tips/ICS-TIP-12-146-01B

Workshops / Building Control Systems Cyber Security Training
http://hpac.com/training/workshop-what-do-when-building-control-systems-get-hacked-set

Industrial Control Systems Joint Working Group (ICSJWG_
https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG

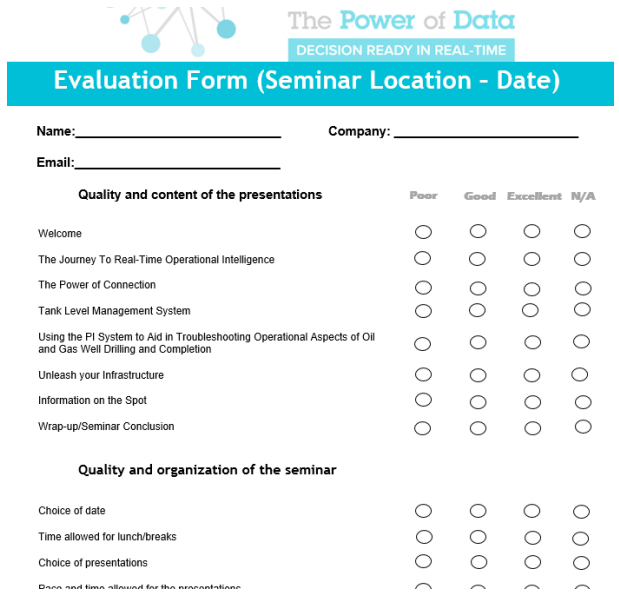
Questions

Please wait for the **microphone** before asking your questions

State your
name & organization

Please don't forget to…

Complete the Survey
for this session



© Copyright 2017 OSIsoft, LLC