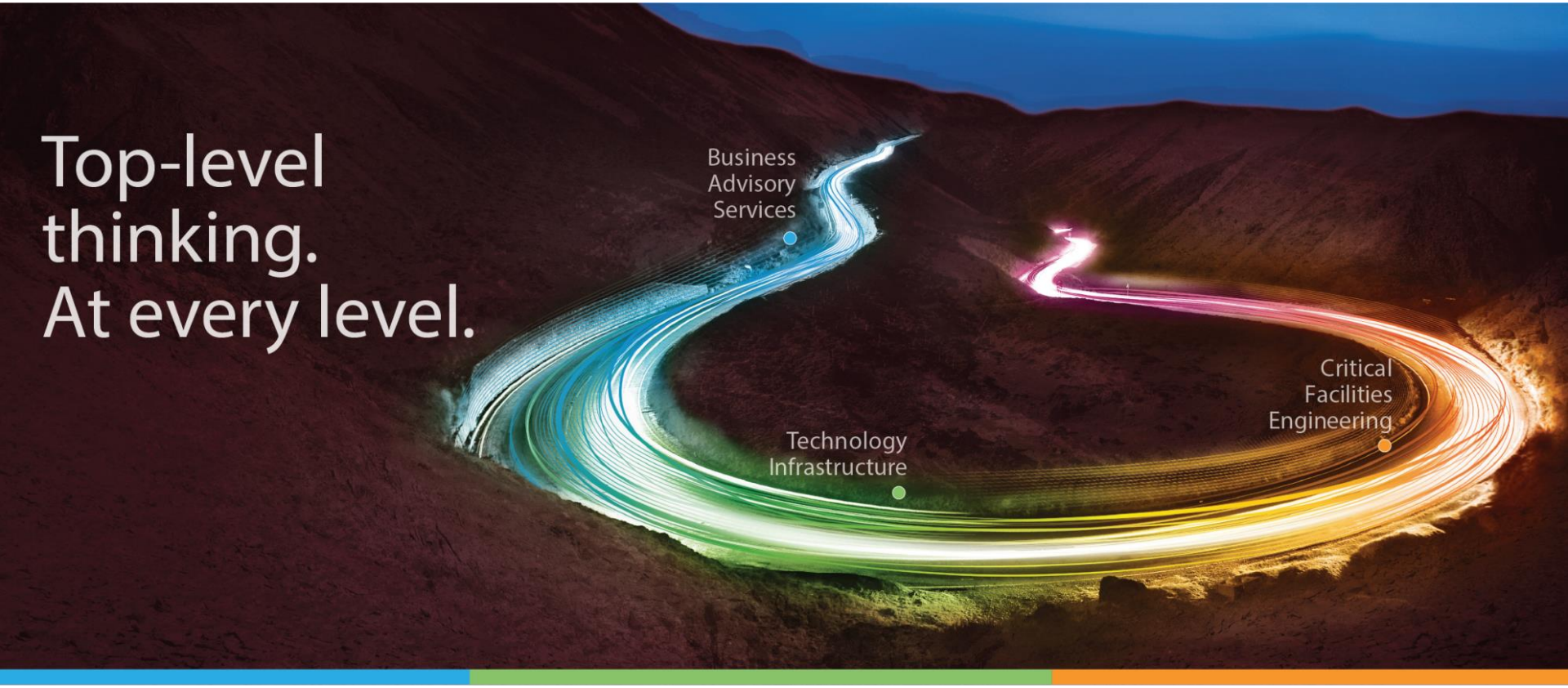
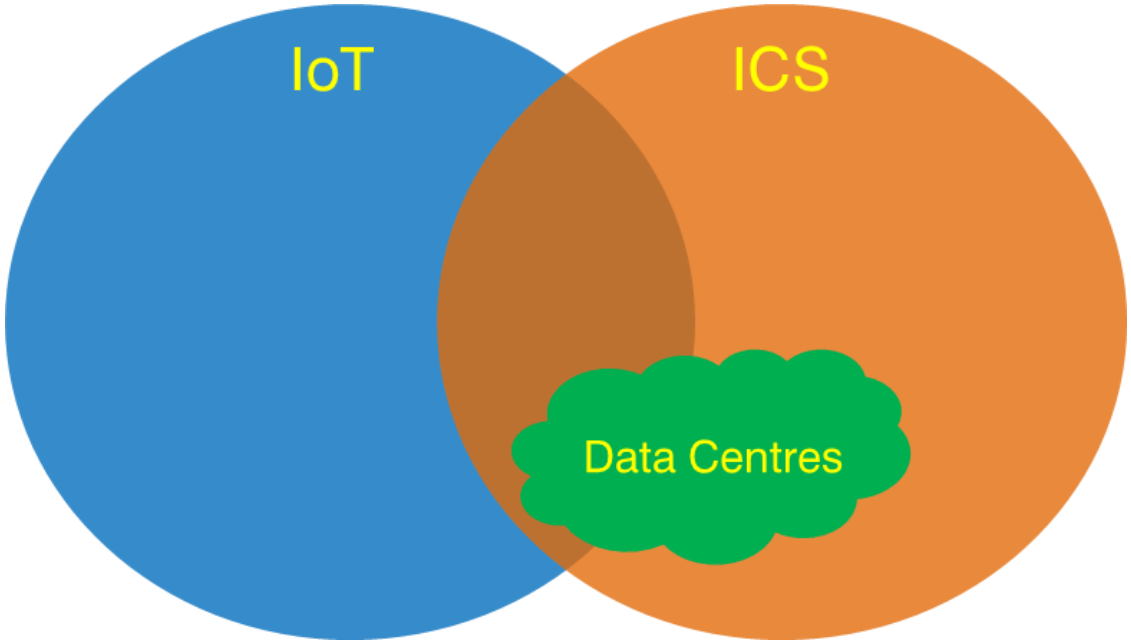
i3 solutions



The Evolving M&E Cybersecurity Threats

IoT, ICS and Data Centres

- Data Centres are a subset of Industrial Control Systems
- They are subject to similar attacks as ICS
- Most Data Centres have connections to the Internet



The Open Back Door

- The back door open is open for the following reasons:
  - Lack of awareness regarding M&E data centre vulnerabilities despite the ICS experience
  - Naïve belief that the data centre M&E systems are air-gapped
  - Vendor back doors
  - Weak perimeter patching and authentication
  - No checks carried out on third party M&E firmware upgrades / patches
- The issues exist because it concerns **M&E Software.** It therefore falls neatly between IT Security and M&E Engineering

Power Systems

- High Voltage Switchgear (HV)
- Low Voltage Switchgear (LV)
- Emergency Generators
- Static Uninterruptable Power Supply (UPS)
- Dynamic Rotary Uninterruptable Power Supply (DRUPS)
- Power Distribution Unit (PDU)
- Static Transfer Switch (STS)

Specific M&E Security Risks

- Internet Connectivity. Networked devices are connected to the public Internet (for service, support, monitoring etc.)
- General purpose machines are connected to the M&E network and devices: PCs, laptops, mobile devices
- Long life cycle of M&E components, usually > 4 times longer than other technology elements.
- Bad patching policies; external vendor
- Inability to efficiently test changes (e.g. patches, configuration, firmware).
- 24/7 operations: Read / Write access to M&E controls.
- Lack of non-IT, M&E-specific, cyber-engineering knowledge, in order to identify risks and possible mitigation steps.

Cooling Systems

- Water Storage
- Chillers
- Cooling Towers
- Water Pumps
- Cooling Fans
- Control Valves

Control & Monitoring Devices

- **SCADA** High / Low Voltage Switchgear & Generators
- **PLCs** High / Low Voltage Switchgear & Generators
- **BMS** Mechanical Systems (Primarily Monitoring)
- **DCIM** Mechanical & Electrical Systems (Primarily Monitoring)

Control & Monitoring Devices

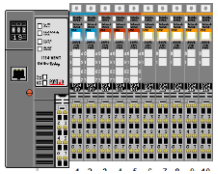
- VSDs
- Wireless
- Gateways
- Generic IEDs
- RTUs

M&E Network Characteristics

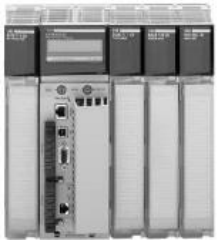
- Complex and Multi layered network.
- Multi Protocol: IP, SCADA and much more.
- Wired and Wireless traffic (+ public Internet access).
- Various types of elements, some of them with very long “life span”.
- General purpose machines (e.g. PCs) mixed with specific elements (PLCs, I/O, RTUs and more).
- “Language barrier” between the “M&E” people and the IT people.

RTU

I/O



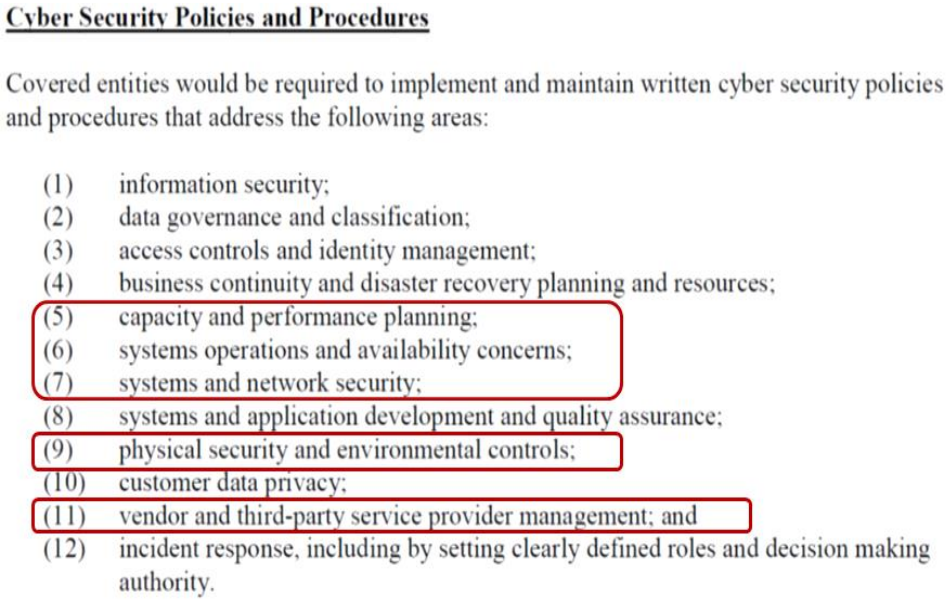
PLC



NY State Department of Financial Services
(9th Nov 2015)

- The regulators on are the case. Pending cybersecurity regulations by the New York State Department of Financial Services requires financial services organizations to address the threat. Everyone will be affected.

- Steps to address the issue will need to cover attacks from within the logically secure perimeter and external access from the internet and other connected networks



Cyber Security Policies and Procedures

Covered entities would be required to implement and maintain written cyber security policies and procedures that address the following areas:

(1) information security;
(2) data governance and classification;
(3) access controls and identity management;
(4) business continuity and disaster recovery planning and resources;
(5) capacity and performance planning;
(6) systems operations and availability concerns;
(7) systems and network security;
(8) systems and application development and quality assurance;
(9) physical security and environmental controls;
(10) customer data privacy;
(11) vendor and third-party service provider management; and
(12) incident response, including by setting clearly defined roles and decision making authority.

It Isn't Difficult to Halt a Business

- Practically every Data Centre uses one or more of the following protocols

Protocol	Cybersecurity Threat
Modbus	No security and no encryption
BACnet	Minimal security and weak encryption
SNMP v1 & v2	Minimal security, no encryption
SNMP v3	Minimal security and weak encryption

- These protocols are used by critical power and cooling systems such as:

Protocol	Cybersecurity Threat
Power	Emergency Generators, UPS, PDUs, Switchgear, Power Meters
Cooling	Chillers, Cooling Fans, Pumps

Modbus Security Issues

Modbus TCP Frame

Start	Address	Function	Data	CRC	End
Silent T1-T4	8 Bits	8 Bits	n x 8 contiguous stream	16 Bits	Silent T1-T4

- Lack of Authentication. Modbus sessions only require a valid Modbus address and Function code. Addresses are easily guessed or spoofed. Function codes are easily obtained
- Lack of Encryption. Commands and addresses transmitted in clear text therefore easily captured or spoofed

M&E Attack Example #1
BMS Server

SURVEY	• Anonymous search engine and Metadata search • Obtain M&E System Drawings
RUN	• Port Scan • Vulnerability Scan
SELECT	• Vulnerable port(s)
RUN	• Default Username/Password • Password Decoder
POLL	• Devices UPS, PDU, Chiller
ALTER	• Program Device Malfunction Shutdown • DoS Attack

Ports

500 4500

Services

500 udp ike

```
VPN (IKE)

Initiator SPI: e5f858a0876af576
Responder SPI: 54105ac94ca3ed30
Next Payload: Security Association (SA)
Version: 1.0
Exchange Type: Identity Protection
Flags:
    Encryption:     False
    Commit:         False
    Authentication: False
Message ID: 00000000
Length: 108
```

4500 udp ike-nat-t

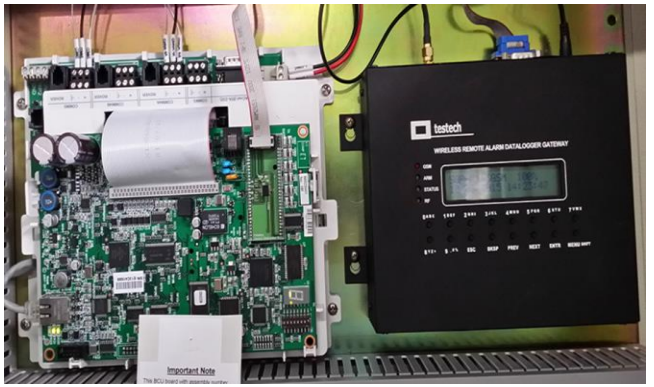
```
VPN (IKE NAT-T)

Initiator SPI: e5f858a0876af576
Responder SPI: ad0adecfdcc1095f
Next Payload: Security Association (SA)
Version: 1.0
Exchange Type: Identity Protection
Flags:
    Encryption:     False
    Commit:         False
    Authentication: False
Message ID: 00000000
```

M&E Attack Example #2
Cooling Controller Wireless Gateway

SURVEY
- Obtain Chiller standard control system drawings
- Connect from outside the data centre perimeter

RUN
- Default Username/Password
- Password Decoder

PROGRAM
- Modify Chiller program e.g. unplanned shutdowns



Reducing the Risk to Your Organization

- Approach
  - NIST Framework for Improving Critical Infrastructure Cybersecurity
- Methodology
  - Inventory vulnerability assessment
  - Perimeterization and Policy
  - Internal segregation
  - Test and verify

Areas to be Addressed in M&E Cybersecurity

- Security Policy
- Design Specifications
- Patch Management
- Secure Default Settings & Hardening
- Access & Account Management
- Plant Network Topology
- Secure Remote Access
- System Connectivity
- Security Monitoring & Diagnostics

Thank you