# Introduction to: Cyber Security

## Schneider Electric's Approach

Presented by: Hugh Lindsay



Life Is On Schneider Electric

# Banks and Cyber Security

## A Persistent and Destructive Global Threat

MARKETS

**New York Bank Regulator Details Cybersecurity Regulations**

By CHRISTOPHER M. MATTHEWS
Nov. 10, 2015 12:42 p.m. ET

**Cyber Attacks Are The Root Cause in 30 Percent of Data Center Outages: Study**

**Banks With Weak Cybersecurity Could Be Downgraded: S&P**

Given banks' function as key nodes in the global financial system
"natural targets facing a high threat of cyber-risk."

Katie Kuehne

September 29, 2015

November 02, 2015

**Bank of England to test banks' security in operation Resilient Shield**

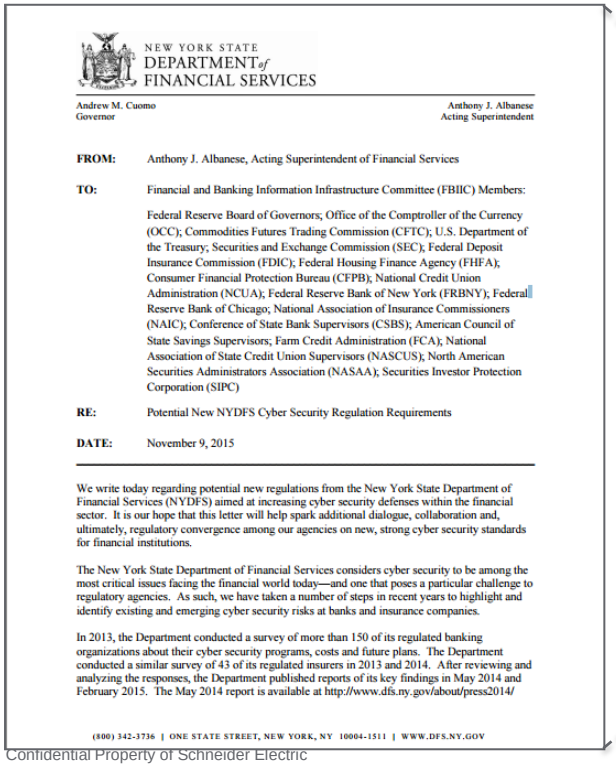
Apr 5, 2013 SECURITY

**Cyber Attackers Target Building Management Systems**

Banks and their Building Control Systems are significant targets

# Regulator Responses

## NY State Regulator



NEW YORK STATE
DEPARTMENT of
FINANCIAL SERVICES

Andrew M. Cuomo
Governor

Anthony J. Albanese
Acting Superintendent

**FROM:** Anthony J. Albanese, Acting Superintendent of Financial Services

**TO:** Financial and Banking Information Infrastructure Committee (FBIIC) Members:

Federal Reserve Board of Governors; Office of the Comptroller of the Currency (OCC); Commodities Futures Trading Commission (CFTC); U.S. Department of the Treasury; Securities and Exchange Commission (SEC); Federal Deposit Insurance Commission (FDIC); Federal Housing Finance Agency (FHFA); Consumer Financial Protection Bureau (CFPB); National Credit Union Administration (NCUA); Federal Reserve Bank of New York (FRBNY); Federal Reserve Bank of Chicago; National Association of Insurance Commissioners (NAIC); Conference of State Bank Supervisors (CSBS); American Council of State Savings Supervisors; Farm Credit Administration (FCA); National Association of State Credit Union Supervisors (NASCUS); North American Securities Administrators Association (NASAA); Securities Investor Protection Corporation (SIPC)

**RE:** Potential New NYDFS Cyber Security Regulation Requirements

**DATE:** November 9, 2015

We write today regarding potential new regulations from the New York State Department of Financial Services (NYDFS) aimed at increasing cyber security defenses within the financial sector. It is our hope that this letter will help spark additional dialogue, collaboration and, ultimately, regulatory convergence among our agencies on new, strong cyber security standards for financial institutions.

The New York State Department of Financial Services considers cyber security to be among the most critical issues facing the financial world today—and one that poses a particular challenge to regulatory agencies. As such, we have taken a number of steps in recent years to highlight and identify existing and emerging cyber security risks at banks and insurance companies.

In 2013, the Department conducted a survey of more than 150 of its regulated banking organizations about their cyber security programs, costs and future plans. The Department conducted a similar survey of 43 of its regulated insurers in 2013 and 2014. After reviewing and analyzing the responses, the Department published reports of its key findings in May 2014 and February 2015. The May 2014 report is available at http://www.dfs.ny.gov/about/press2014/

(800) 342-3736 | ONE STATE STREET, NEW YORK, NY 10004-1511 | WWW.DFS.NY.GOV

### Recommendations

**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.

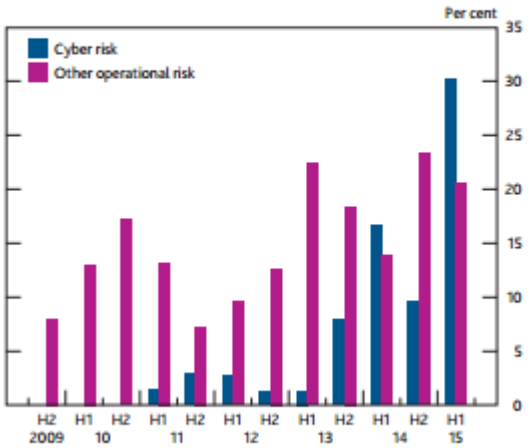
# Regulator Responses

## Bank of England

### Studies

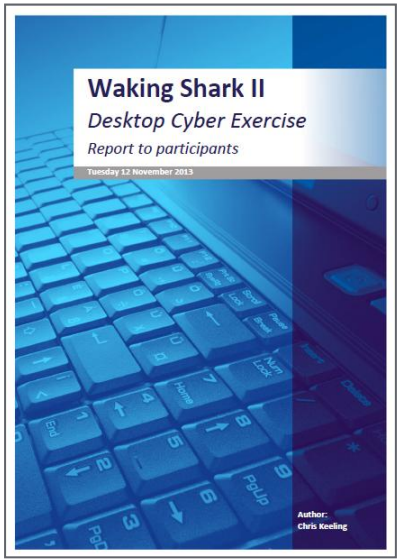
**Chart A.31** Concern about cyber risk has grown

*Systemic Risk Survey*: proportion of respondents highlighting operational/cyber risk as a key concern




Sources: Bank of England *Systemic Risk Surveys* and Bank calculations.

### Systemic Exercises




**OPERATION RESILIENT SHIELD**

In response to a growing threat to the UK's economic security, the Bank of England readies itself to put the UK's financial institutions through their paces in a new wargame.

# The Cyber Security Challenge

**Concerns, pressures and regulations are increasing:**

- US, UK and China are demanding response to cyber threats for Critical Infrastructure
- Regulatory (NERC-CIP) and Standards (ISO/IEC) activity increasing
- Customers expecting improved and timely response to vulnerability disclosures and fixes

**Control systems (BMS, EPMS and others) are increasingly targeted by attackers:**

- Even systems not directly connected to the corporate network are vulnerable

**Schneider needs to take a proactive role in the protection of customers and our systems:**

- Invest and develop the right security capabilities; market specific and application focused
- Cyber secure development processes and validation
- Ensure we “securely” accomplish the digitization  and Internet of Things (IoT) journey

# Our Cyber Security Vision

"To live in a world where all Schneider offerings are secure, customers are satisfied with our security and we can leverage our security as a competitive advantage…"

# Global Cyber Security Trends

***Terrorism***

***Extortion***

***Espionage***


650% increase in cyber threats during the last year


Successfully attacking best guarded organizations



Regulatory compliance is in a constant state of flux

Increasing budgetary pressures & fewer resources

Rapid pace of technology evolution – IT/OT convergence



IT – Information Technology
OT – Operations Technology

# Cyber Security Principles

- **What is Cyber Security:**
  - Threats attack vulnerabilities and can include:
    - Internal threats
    - External threats
  - Potential risks:
    - Safety of personnel (injury, fatality)
    - Operational disruptions and direct financial loss
    - Loss of sensitive data
    - Reputation
- **Key Security Principles: CIA Triad**
  - **C**onfidentiality – Prevent disclosure of private information.
  - **I**ntegrity – Data cannot be modified without authorization.
  - **A**vailability – The information must be available when it is needed.

# Where Does Schneider Fit?

**Schneider faces risks to reputation, revenue and regulatory impact**

> Protecting assets against computer or network threats: the C-I-A triad (Confidentiality, Integrity, Availability)
> Cyber Security covers all domains of activity (Human, Process, Technology)
> Cyber attacks have “jumped the gap” from virtual to physical world resulting in real physical damage to critical assets
> Cyber attacks can put people at risk, cause operational downtime, create financial loss, destroy reputations, and can exfiltrate sensitive data.

**Why now?**

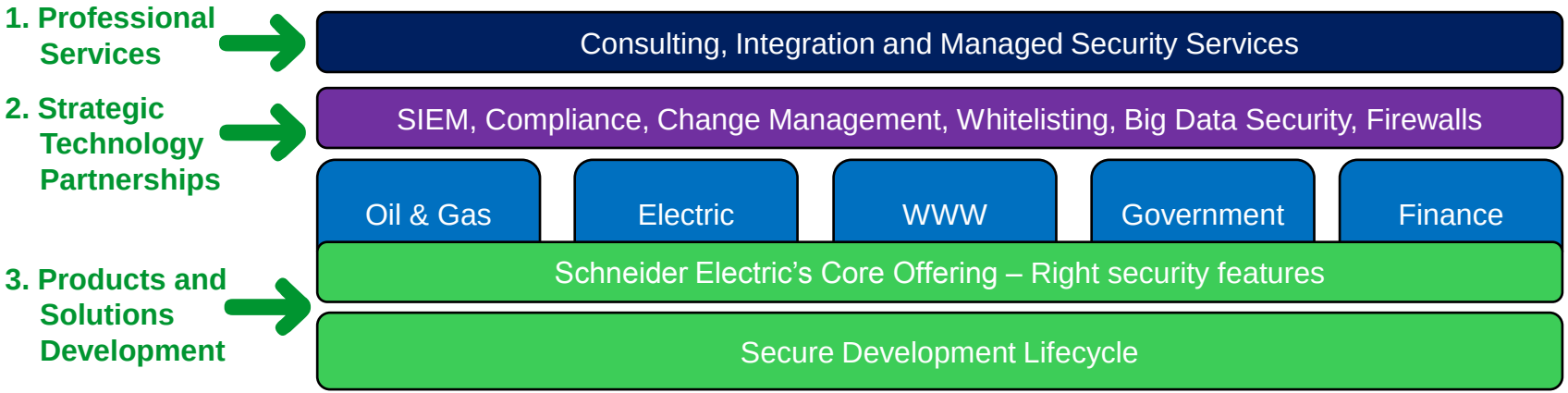
> Focus of attacks has shifted toward infrastructure
> Schneider’s systems may be the target of groups looking to harm infrastructure, engage in cyber warfare, send a political message, or build street “cred” in the hacker community.
> As a premier provider of products and services to critical infrastructure customers, we must act.

# Schneider's Comprehensive Approach

Guiding Principles

Schneider Electric stands by our safe, reliable and secure core control system and intelligent devices
- Our cyber security products & services needed to increase prevention, detection & response
- We need to develop a portfolio of services through recognized Schneider Electric's consulting arm & local players
- We need to bring the best third party solutions through partnership ecosystem & 'vendor agnostic' mindset

Comprehensive Approach



# 1. Professional Services

## Cyber Secure Control System Consulting

### Assessments

- Cyber Security
- Compliance
- FEED Studies
- Policy
- Security Baseline
- Risk
- Site
- Vulnerability

1

### Workshops

- Technology Roadmap
- Active Directory
- Planning Workshop
- Security Compliance
- Compliance Evaluation

2

### Remediation

- Network Design
- Hardening
- Firewalls
- Patch Management
- Remote Access
- Intrusion Detection
- Back Up Recovery

3

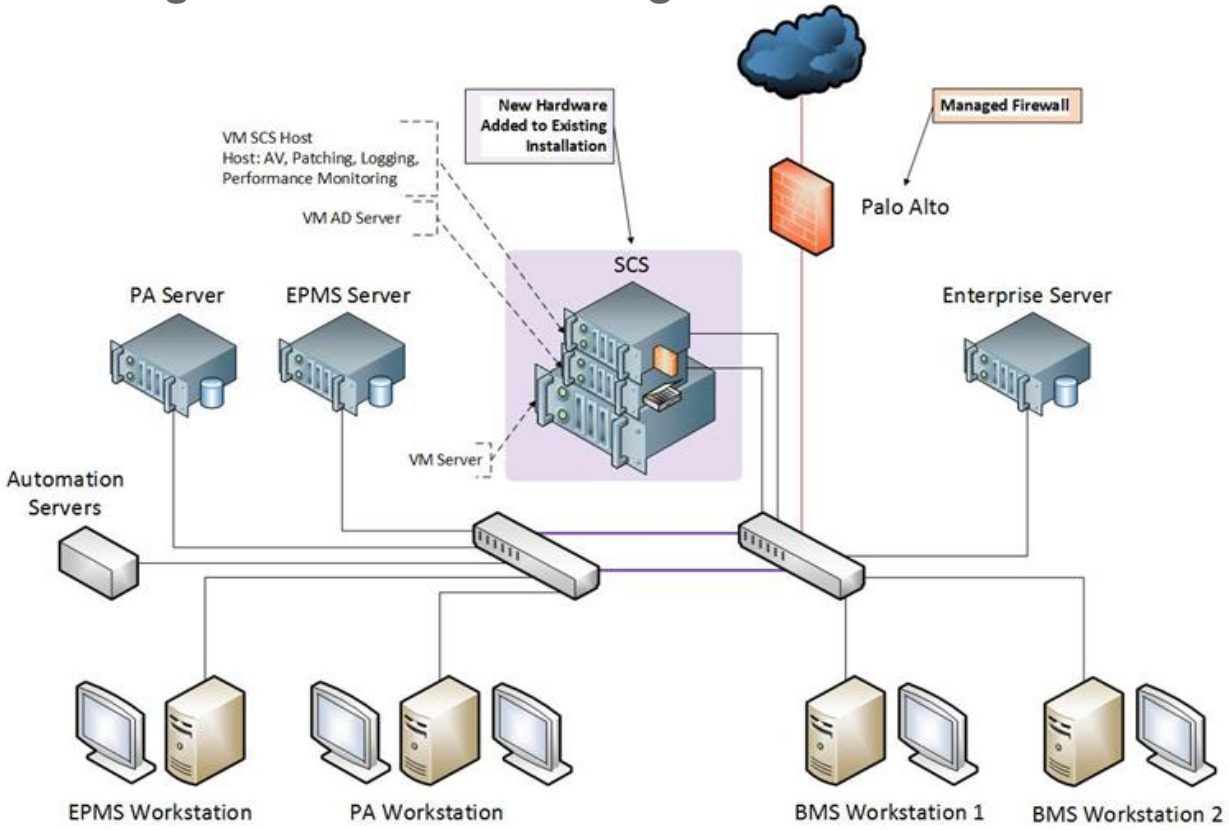
### Management

- Managed Security Services
- Contracted Incident Response
- Network Management

4

# 2. Strategic Technology Partnerships

## Leverage the Best Technologies in the Market




## Partner Examples:

GFI LanGuard™
Network security scanner and patch management

McAfee®

Symantec™

Symantec Backup Exec™

# 3. Products and Solutions

## Cyber Secure Development Lifecycle


| Deliver Security Training | Security Requirements | Secure Design Reviews | Secure Code Practices | Security Testing | Secure Release Management | Secure Deployment | Incident Response |
|---|---|---|---|---|---|---|---|
| On-demand training for each role | Security requirements based on regulations | Conduct Threat Modeling and Architecture Review | Scan all code related to product | Secure white box and black box testing | Documentation and process details to securely deploy the offering | Full security lifecycle services for customers | Respond to incidents and vulnerabilities reported |

### Stage Deliverables

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| On demand training delivered through our global learning platform | Completed security requirements checklist per project based on regulatory requirements | Threat model workshop and final threat model report with next steps | Security test report from code security quality tool | Security test results report with categorized findings by severity | Security documentation that details security features and deployment best practices | Deliverables will vary by customer engagement and project scope | Disclosure report posted to web and external sites such as ICS-CERT where applicable |