RSA Conference 2018

San Francisco | April 16 – 20 | Moscone Center

NOW MATTERS

SESSION ID: TECH-W04

STOP TRANSLATING, START DEFENDING: COMMON LANGUAGE FOR MANAGING CYBER-RISK

Dawn Cappelli

VP, Global Security and CISO
Rockwell Automation
@dawncappelli

Umair Masud

Portfolio Manager, Cybersecurity Services
Rockwell Automation
@utmasud

$6.3B
FISCAL 2017 SALES

22,000 EMPLOYEES

80+ COUNTRIES

WORLD'S LARGEST COMPANY DEDICATED TO INDUSTRIAL AUTOMATION AND INFORMATION

AUTOMATION SOLUTIONS for a *broad range of industries*

SERVING CUSTOMERS FOR 114 YRS

A·B QUALITY

- Innovation
- Domain expertise
- Culture of integrity & corporate responsibility

ABOVE-MARKET GROWTH | PRODUCTIVITY | INTELLECTUAL CAPITAL VALUE CREATION

Rockwell Automation

RSAConference2018

Industries We Support

Automotive · Chemical · Entertainment · Fiber and Textiles · Food and Beverage

Household and Personal Care · Infrastructure · Life Sciences · Marine · Mining, Metals, and Cement

Oil and Gas · Power Generation · Print and Publishing · Pulp and Paper · Semiconductor

Tire and Rubber · Water Wastewater

Rockwell Automation

RSA Conference2018

UNCLASSIFIED

Mokusatsu: One Word, Two Lessons

BY (b)(3)-P.L. 86-36

Unclassified

Source: National Security Agency

RSAConference2018

THE CORPORATE **SECURITY ECOSYSTEM**

IT → OT

Information Technology

Third Parties

Product Security

Customers

Connected Services

Supply Chain

Rockwell Automation

RSAConference2018

The Beginning of our Journey: A New CISO

CISO 1.0

CISO 2.0

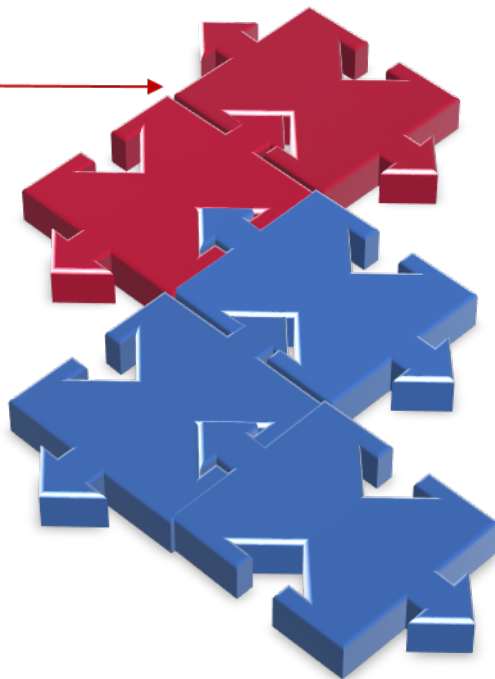## Extended Security Team

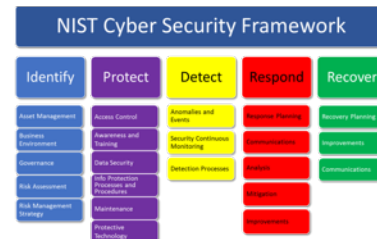Business and functional liaison network

Partnership with IT

Foundational Programs

Secure Development Environment

Insider Risk Program

Third-Party Risk Program

Risk-Based Approach to Developing a Strategy

NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Rockwell Automation

RSAConference2018

Transformation to Rockwell Automation's Culture

NIST CSF: (5) Functions, (22) Categories, (98) Sub-Categories
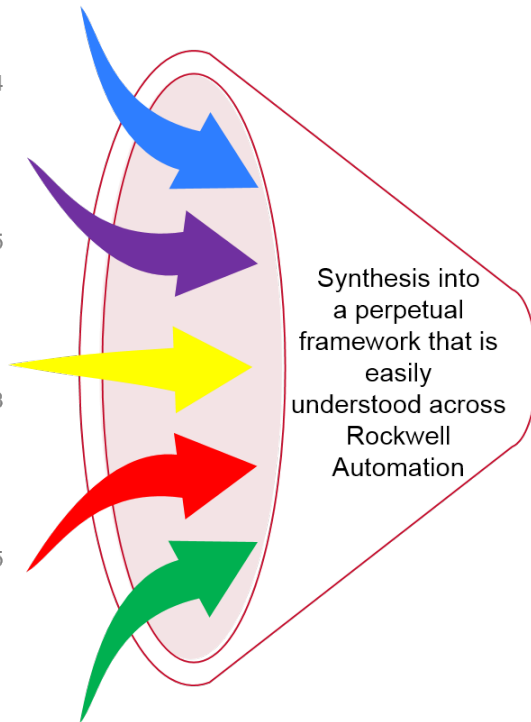
Identify
Category : 5
Sub-Category: 24

Protect
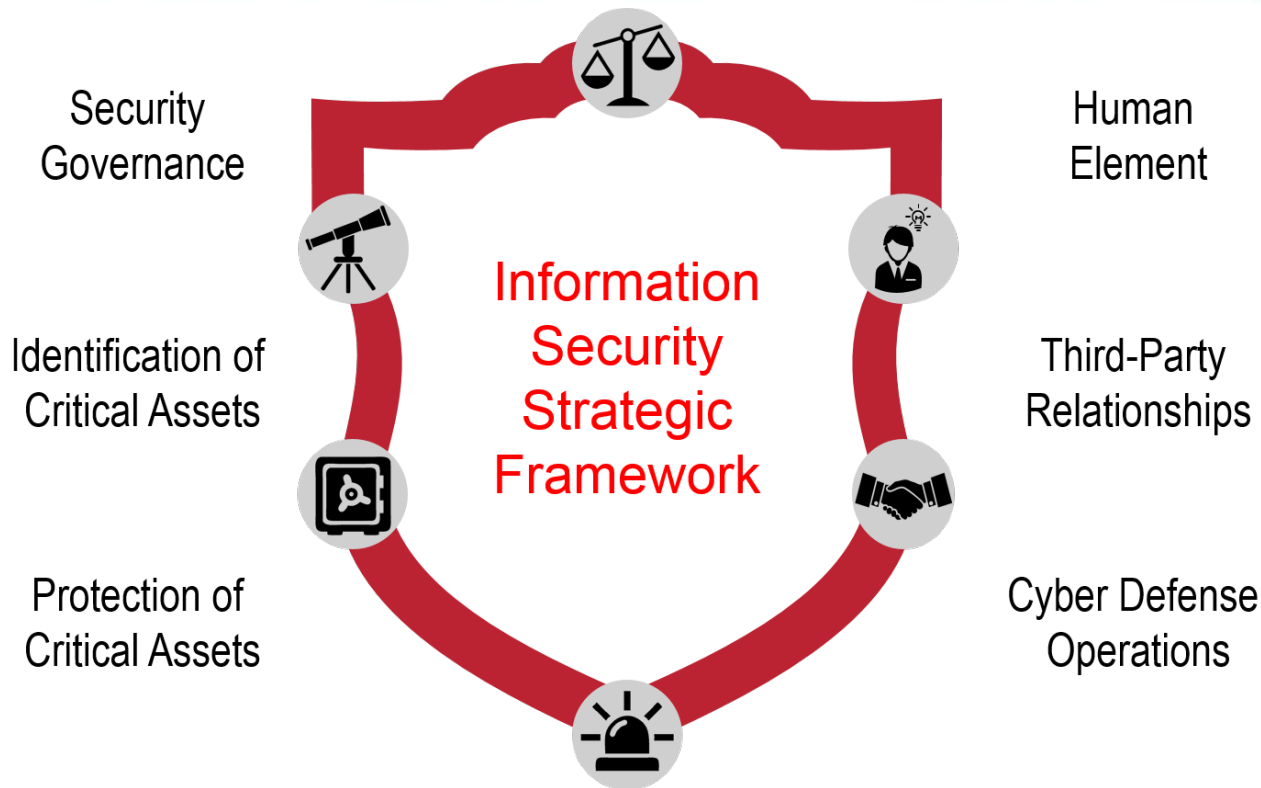Category : 6
Sub-Category: 35

Detect
Category : 3
Sub-Category: 18

Respond
Category : 5
Sub-Category: 15

Recover
Category : 3
Sub-Category: 6
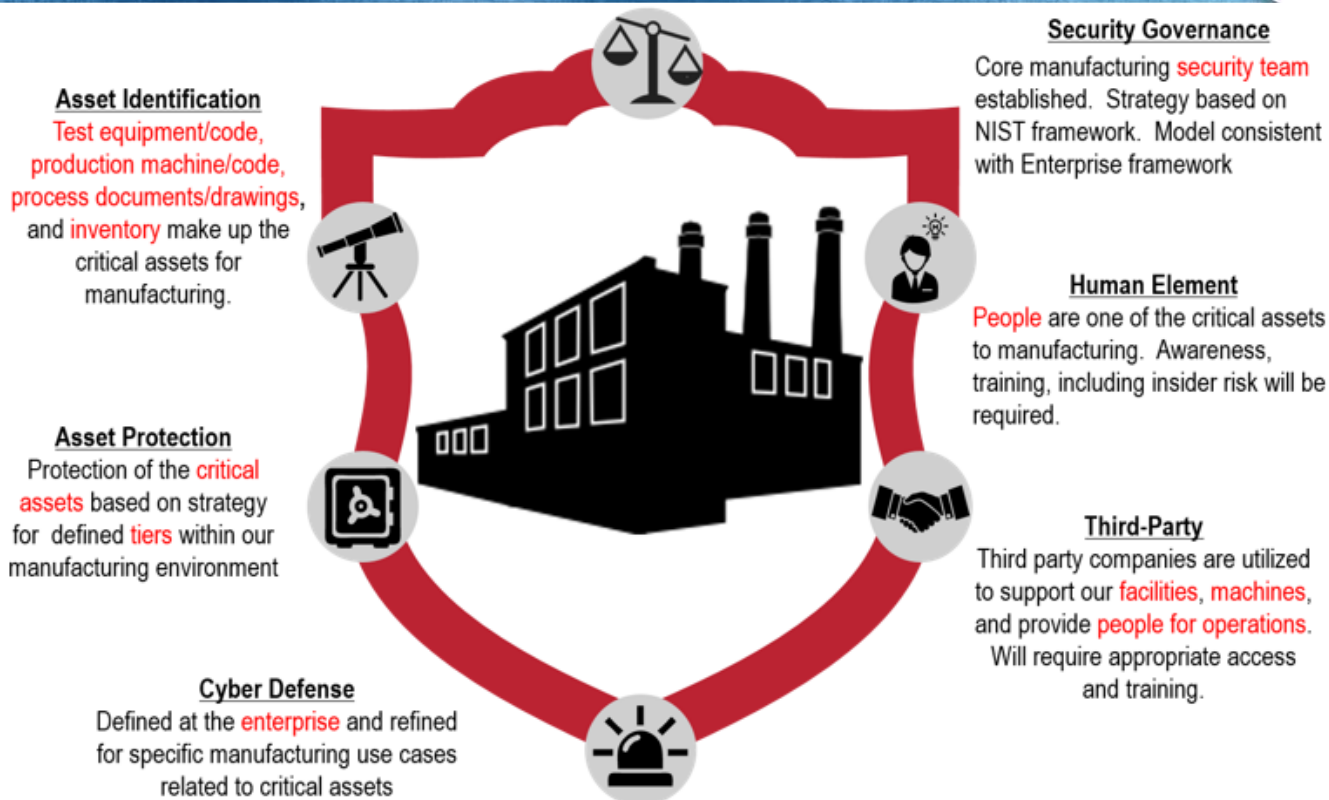
Synthesis into a perpetual framework that is easily understood across Rockwell Automation

RA Information Security Strategic Framework

Security Governance

Asset Identification

Asset Protection

Human Element

Third-Party

Cyber Defense

The Rockwell Automation Information Security Framework

Information Security Strategic Framework

Security Governance

Identification of Critical Assets

Protection of Critical Assets

Human Element

Third-Party Relationships

Cyber Defense Operations

Security Governance
Core manufacturing security team established. Strategy based on NIST framework. Model consistent with Enterprise framework

Asset Identification
Test equipment/code, production machine/code, process documents/drawings, and inventory make up the critical assets for manufacturing.

Human Element
People are one of the critical assets to manufacturing. Awareness, training, including insider risk will be required.

Asset Protection
Protection of the critical assets based on strategy for defined tiers within our manufacturing environment

Third-Party
Third party companies are utilized to support our facilities, machines, and provide people for operations. Will require appropriate access and training.

Cyber Defense
Defined at the enterprise and refined for specific manufacturing use cases related to critical assets

Attack Continuum

BEFORE	DURING	AFTER
Identify & Protect	Detect	Respond & Recover

WannaCry
Ransomware

Petya/NotPetya
Ransomware

Tales from the Crypt

Ooops, your important files are encrypted!

Now what?

RSAConference2018

NIST CSF Helps us to Adapt to the Changing Threat Environment

Increasing Risk

5 New vulnerabilities could expose global eco-systems

2017 – 2018

MELTDOWN   SPECTRE

3 Global nation state attacks use cyber weapons   **4** Regional regulations

2016 – 2017

WannaCry

Petya/NotPetya Ransomware

me doc
МІЙ ЕЛЕКТРОННИЙ ДОКУМЕНТ

EU General Data Protection Regulation

2 Limited nation state cyber sabotage attacks targeted at individual companies

2007 – 2014

STUXnet

أرامكو السعودية
saudi aramco

SONY PICTURES

1 Hackers, cyber-criminals, and nation states target PII and financial data at specific firms

2011 – 2017

PlayStation   TARGET   YAHOO!   THE HOME DEPOT   BlueCross BlueShield   EQUIFAX   UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Rockwell Automation

RSA Conference 2018

A Common Language with the Board
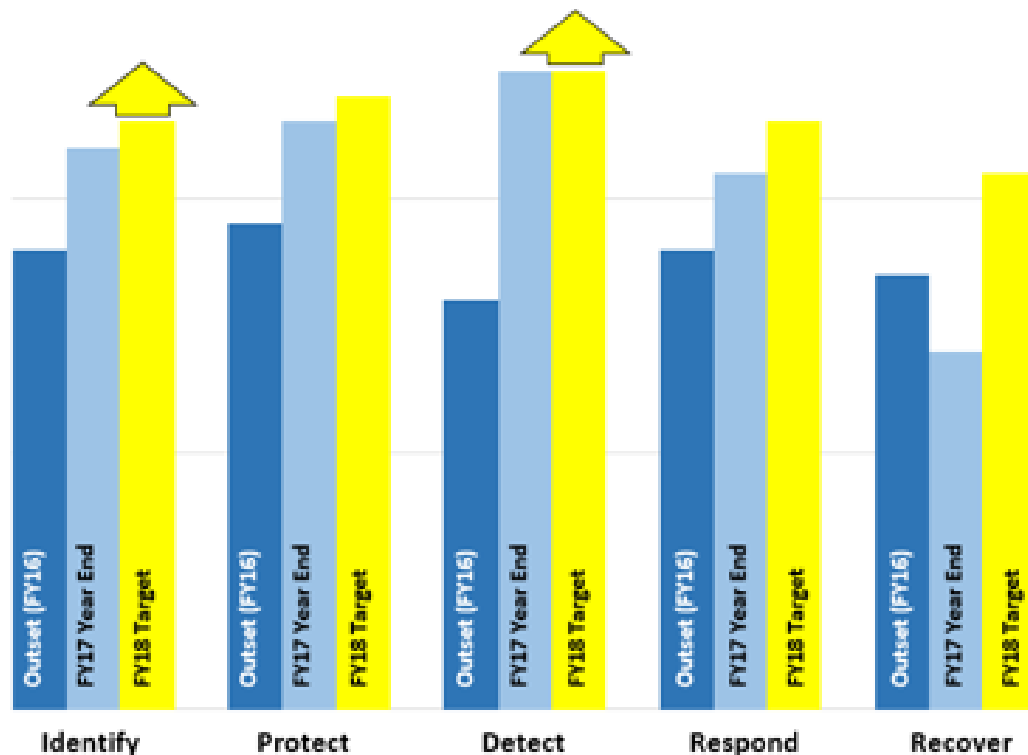
What problem are you trying to solve?

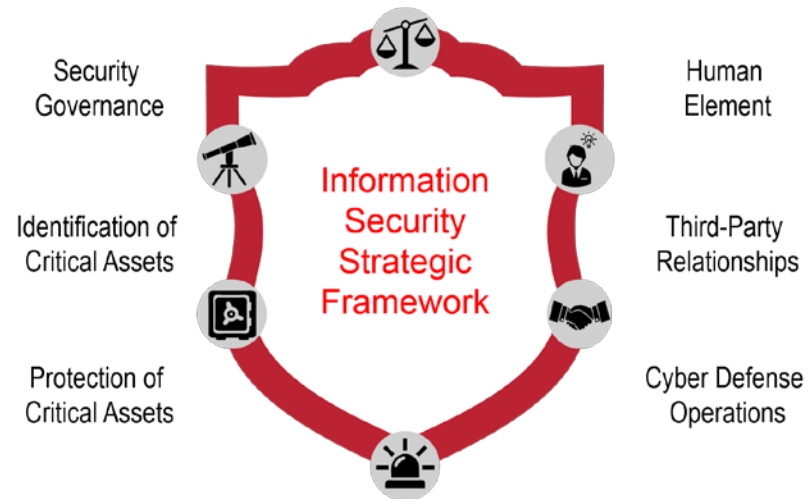|	
Lack of a strategic framework	Research NIST CSF
Leadership will not support your strategy	Use NIST CSF to develop a strategic roadmap using liaisons from each business and function from across the company
Lack of clear communication with customers or the Board	Use NIST CSF as the common language
Have a strategy for enterprise IT, but not for the rest of your company's cybersecurity ecosystem	Apply NIST CSF to another aspect of your ecosystem, e.g. supply chain, product security, delivery of services to your customers, …

Rockwell Automation

RSA Conference 2018
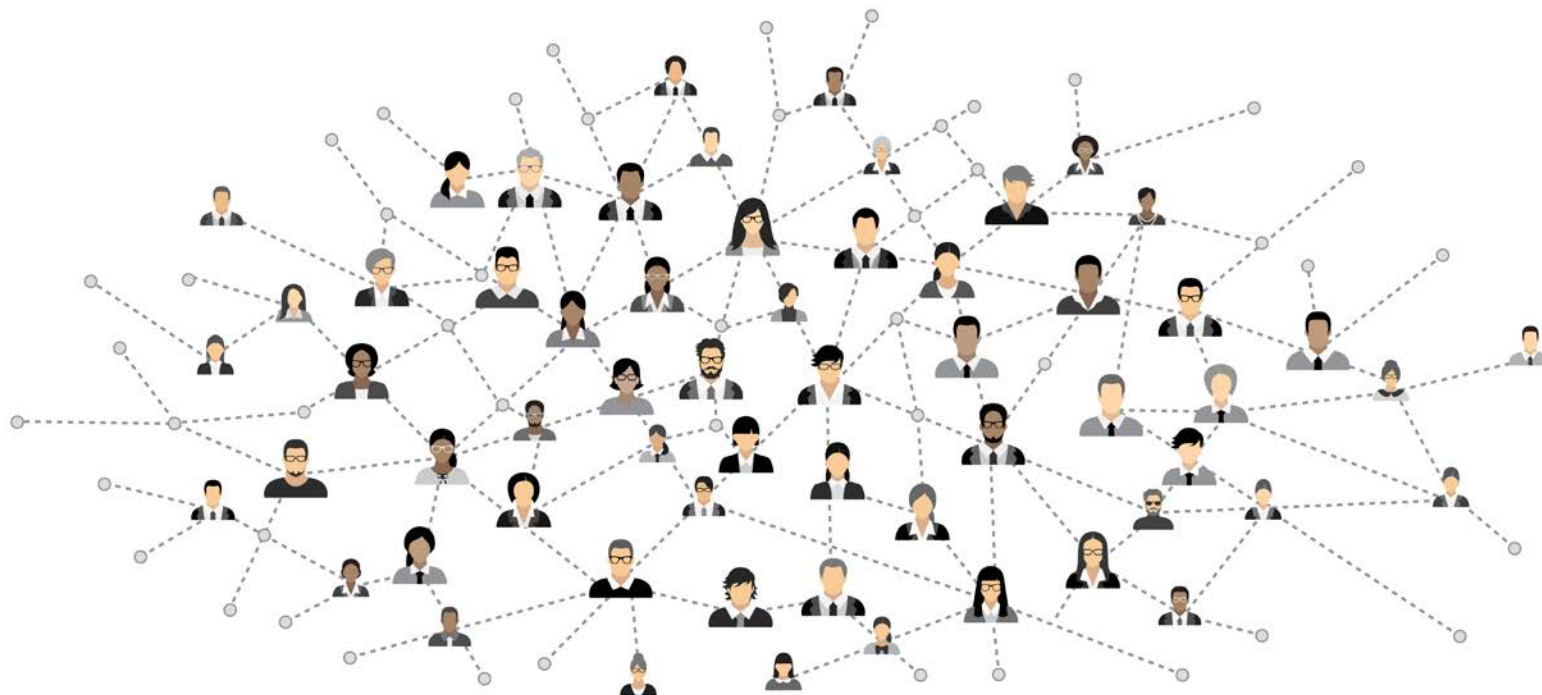
- Create a 3-year plan

- Create scoring charts to convey your plan

- Transform your plan into a visual representation that will resonate across your company

- Get to work!

- *P.S. – You should get buy-in since the planning process had representation from across the company*

Security Governance

Identification of Critical Assets

Protection of Critical Assets

Information Security Strategic Framework

Human Element

Third-Party Relationships

Cyber Defense Operations