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
Who is Rockwell Automation?

$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

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

ABOVE-MARKET GROWTH | PRODUCTIVITY | INTELLECTUAL CAPITAL => VALUE CREATION
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
Failure in Translation

Mokusatsu: One Word, Two Lessons

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

Unclassified

Source: National Security Agency
Purpose of the Presentation: A Common Language

THE CORPORATE SECURITY ECOSYSTEM

- Information Technology
- Third Parties
- Customers
- Product Security
- Supply Chain

IT

OT

Connected Services
The Beginning of our Journey: A New CISO

CISO 1.0

Extended Security Team
- Business and functional liaison network
- Partnership with IT

Foundational Programs
- Secure Development Environment
- Insider Risk Program
- Third-Party Risk Program

CISO 2.0

Risk-Based Approach to Developing a Strategy

NIST Cyber Security Framework

Identify
- Risk Assessment
- Business Impact Analysis

Protect
- Risk Management
- System and Network Security

Detect
- Incident Response
- Security Monitoring

Respond
- Security Awareness
- Incident Handling

Recover
- Business Resilience
- Backup and Recovery

Rockwell Automation

RSA Conference 2018
Transformation to Rockwell Automation’s Culture

- **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.
The Rockwell Automation Information Security Framework

- Security Governance
- Identification of Critical Assets
- Protection of Critical Assets
- Human Element
- Third-Party Relationships
- Cyber Defense Operations
The Rockwell Automation Manufacturing Security Framework

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

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

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

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

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

**Cyber Defense**
Defined at the enterprise and refined for specific manufacturing use cases related to critical assets.
Transforming How we Message to Customers

Before
Identify & Protect

During
Detect

After
Respond & Recover

Attack Continuum
Into the Fire --- How NIST CSF Helped With our Customers

Petya/NotPetya
Ransomware
Tales from the Crypt

Ooops, your important files are encrypted!

Now what?
Into the Fire --- How NIST CSF Helped Internally
### NIST CSF Helps us to Adapt to the Changing Threat Environment

**Increasing Risk**

**2011 – 2017**
- 1. Hackers, cyber-criminals, and nation states target PII and financial data at specific firms

**2007 – 2014**
- 2. Limited nation state cyber sabotage attacks targeted at individual companies

**2016 – 2017**
- 3. Global nation state attacks use cyber weapons
- 4. Regional regulations
- 5. New vulnerabilities could expose global eco-systems

---

*Image: RSA Conference 2018*
A Common Language with the Board
# Where to From Here?

## What problem are you trying to solve?

<table>
<thead>
<tr>
<th>Lack of a strategic framework</th>
<th>Research NIST CSF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leadership will not support your strategy</td>
<td>Use NIST CSF to develop a strategic roadmap using liaisons from each business and function from across the company</td>
</tr>
<tr>
<td>Lack of clear communication with customers or the Board</td>
<td>Use NIST CSF as the common language</td>
</tr>
<tr>
<td>Have a strategy for enterprise IT, but not for the rest of your company’s cybersecurity ecosystem</td>
<td>Apply NIST CSF to another aspect of your ecosystem, e.g. supply chain, product security, delivery of services to your customers, ...</td>
</tr>
</tbody>
</table>
How to Conduct a NIST CSF Workshop
Creating the Strategic plan

- 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
It Doesn’t End Here
THANK YOU

Thank you Tim Casey from Intel Corporation for his help getting started on our use of the NIST CSF!