How to Build a Successful Business Case for OT Cybersecurity

CS4CA USA 2024

*Scan the **QR code** to learn more about this session!*

VERVE
A ROCKWELL AUTOMATION COMPANY

Agenda

- Introductions
- Setting the Stage
- Solution?
  - Data! But with Context
  - A Plan
  - Measure and Maintain
- Summary
- Questions

VERVE
A ROCKWELL AUTOMATION COMPANY

Introduction

Rick Kaun, VP Solutions

- 22 years providing ICS security solutions
- Formerly worked for Matrikon -> Honeywell
- Significant experience in NERC CIP, TSA standards
- Significant experience in non-regulated such as NIST-CSF, CIs18, etc.
- Always provide vendor-agnostic holistic program solutions

VERVE
A ROCKWELL AUTOMATION COMPANY

Verve Industrial

- ~30 years of securing industrial environments based on deep controls system expertise
- Verve Security Center 15 years in development specifically for OT environments
- OT security platform that brings the best of IT security into the complex OT environment
- Combined with Rockwell Automation in November 2023

Setting the Stage

- Business case usually includes:
  - Problem statement (clearly defined)
  - Proposed solution
  - Cost/timing to deploy
  - Results - Quantifiable, demonstrable, etc

VERVE
A ROCKWELL AUTOMATION COMPANY

Challenge for OT

- Problem statement (clearly defined)
  - Do we know how big the problem is? (Assessment output? Conjecture?)
  - Do we know what our priority is? (Vuln list is non-contextual)
- Proposed Solution
  - How far do we go? What does ‘done’ look like?
- Cost/timing to deploy
  - Depends on answers from above – if we can’t give an idea as to how big how can we get it supported?
- Results - Quantifiable, demonstrable, etc.
  - How do we measure success? Track over time? Ensure ‘staying’ power?
  - Sustainable improvement is biggest win – but at what cost to achieve AND maintain?

VERVE
A ROCKWELL AUTOMATION COMPANY

Solution?

- 3-pronged approach that will show thought leadership, use of empirical data and an eye towards life 'post project' or what the 'real' cost will be.
  - First – Data collection – and import to a multi-dimensional or contextual view
  - Second – A reasonable plan – stages, deliverables, targeted against what 'done' looks like
  - Third – a measurement/maintenance plan

- Result is a plan to get started, identify early the true gap, plans then become much more accurate and long-term commitment is minimized. So, we are building a sustainable, cost-effective path forward.

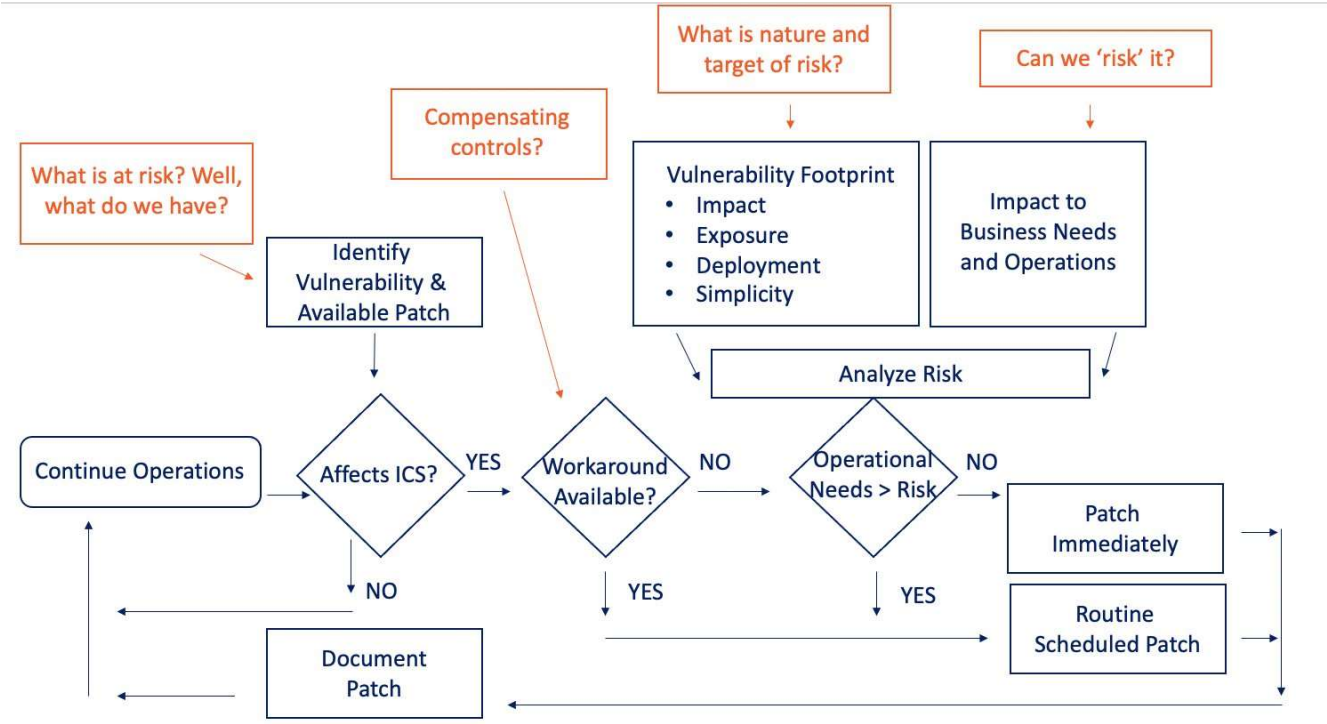
VERVE
A ROCKWELL AUTOMATION COMPANY

Data Collection

- Common Options:
  - Pitch an assessment – have one of the 'Big 4' come in and go over your environment, people, processes, etc. with a big measuring stick
    - Output – a clear list of deficiencies with priority rankings attached
    - Cons
      - This is a point in time assessment, It will change - likely immediately.
      - This is also a 'linear approach' and takes lots of time to execute
      - May only really confirm that which you already suspect
  - Use existing 'tools' to provide 'insight' – Such as vulnerability tools, packet capture intrusion detection, etc.
    - Output – an indicator of 'risk' – though it is a single view
    - Cons – no context – 23,917 vulns – is not a helpful stat

Data Collection – Tech Enabled Assessment with Context

- Build a 360-degree view of the assets
  - Data is key – but data without context is useless
  - True risk is calculated based on a number of factors – look at Patch Decision Tree



VERVE
A ROCKWELL AUTOMATION COMPANY

Data Collection – Tech Enabled Assessment with Context

- Resulting score is contextual not conjecture

Use Case: Create Asset Risk Score

Criticality/Impact of System
- Safety systems
- Control over critical processes
  - Device functionality
  - Process criticality
- Access into other parts of network
- Presence of critical programming software
- Network devices necessary to communicate between assets

Risk Components
- Vulnerabilities
- User/account status
- Configuration insecurities
- AV/Whitelisting information
- Backup status

User-visible label by perceived criticality and risk (also by type)	Backend score ranges (normalized out of 100)
Critical	76-100
High	51-75
Medium	26-50
Low	1-25

VERVE
A ROCKWELL AUTOMATION COMPANY

Data Collection – to refresh…

- Multiple data sources for input mean a more robust and focused ‘real risk’
  - Contextual data removes noise
  - Allows for the org to set a ‘reasonable’ risk tolerance
    - Risk outside or above the tolerance becomes impetus to act with specific priorities and urgency

- Focusing on the asset relative to operational impact removes speculation and hyperbole
- Incorporating policy/procedure collection and analysis as well as staffing levels and behaviors further enhances planning
  - This also allows for better management and maintenance planning

- Benefit: We have sorted through the noise to uncover the true amount of work required
- Now it is time to turn to planning

VERVE
A ROCKWELL AUTOMATION COMPANY

Data Collection – to refresh…

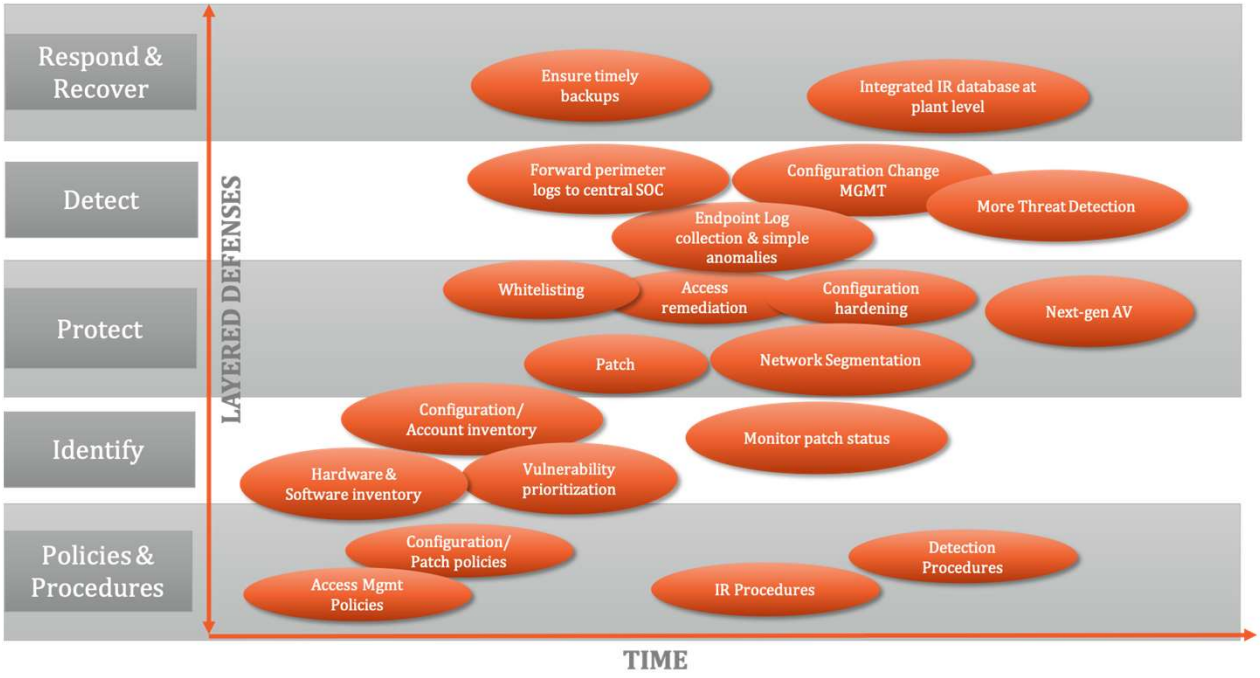
- Once we have gathered the data, we need to analyze it to better categorize the needs and the priorities.
- Scope must include:
  - People, Process and Technology
  - Must have a desired 'end game' (recommend this is defined ahead of data gathering but here is where it really counts
  - Mechanism for maintenance

- Objective here is to build a plan that is:
  - Scalable over time and budget and/or across multiple sites
  - Sustainable – no room for sunk cost or wasted time/resources
  - Prioritized risk reduction
  - Measurement to ensure adherence and progress
  - Minimal residual cost (i.e., can't be a maintenance nightmare)

VERVE
A ROCKWELL AUTOMATION COMPANY

Planning Phase – Objective defined

- Now to plan against industry standard or regulatory/board mandate as needed



VERVE
A ROCKWELL AUTOMATION COMPANY

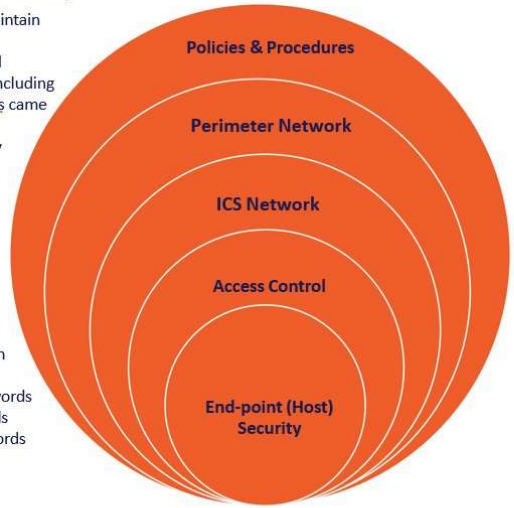
Planning Phase – Objective defined

- Individual findings span the entirety of a security program

Assessment: Typical findings

Policies & Procedures (Critical Risk) – (observed)

- No knowledge of or procedure to maintain network connectivity
- No asset identification, inventory and management policy or procedure – including not knowing where particular devices came from or what their purpose is
- No patch/change management policy
- No standard account & password management procedure
- Physical security control unclear



Network Architecture (Critical Risk)

- Access to internet from ICS network
- Weak firewall rules allow all enterprise traffic into OT
- Devices dual-homed around critical firewalls
- Lack of network monitoring or management
- VLAN separation allows east-west traffic without control
- Network devices communicating over clear text
- No hardware protection of insecure OT devices
- Multiple 5G devices routing around OT firewalls, but connected to control system network

Access Control (Critical Risk)

- No network access control
- Dozens of dormant accounts on each device
- Dozens of accounts with aged passwords
- Many devices with default passwords and/or network devices with passwords stored in clear text in configuration
- Many shared accounts on critical systems
- No monitoring/control for remote access

End-Point (High Risk)

- No accurate asset inventory to identify potential critical vulnerabilities
- Close to 100 missing critical missing patches on the average Windows device (including RCE, Wannacry, Blue keep)
- Hundreds of critical vulnerabilities on PLCs & embedded devices
- Network devices out-of-support
- Most devices not compliant with core security hardened configurations
- Significant number of unnecessary software programs
- No log management or incident response capabilities

VERVE
A ROCKWELL AUTOMATION COMPANY

Planning Phase – follow the money?

- Next step is to overlay site, geographic, revenue, legacy and regulatory inputs into findings

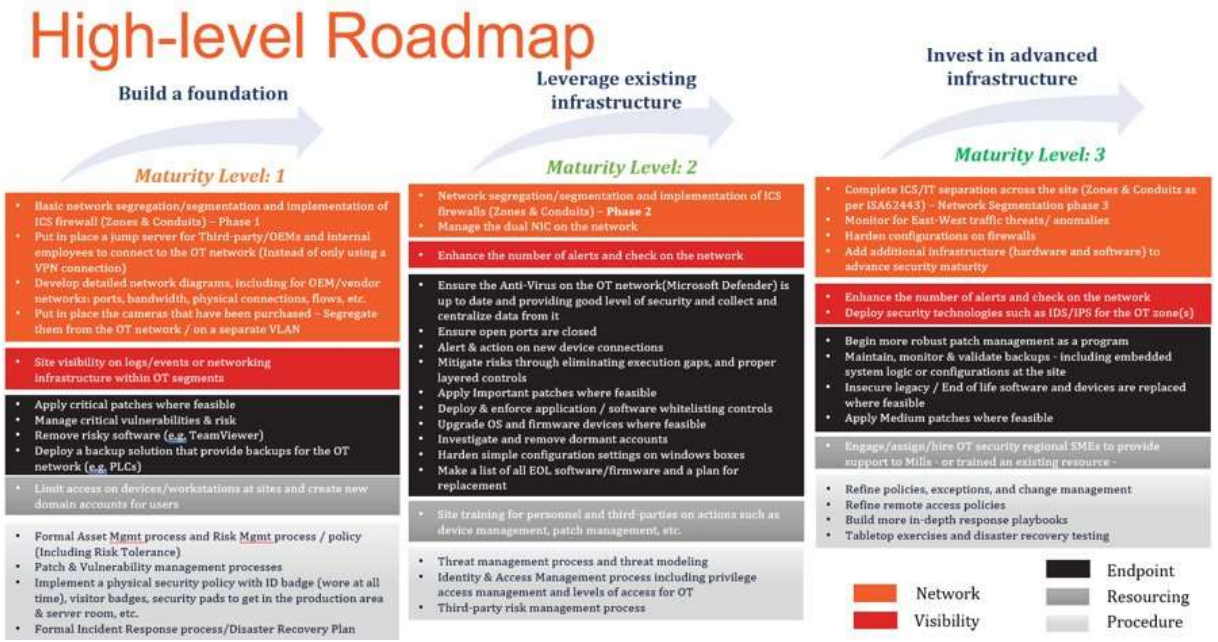
Site prioritization is more than $$ generated

Example site selection criteria across these fundamental domains should be considered:

VERVE
A ROCKWELL AUTOMATION COMPANY

Planning Phase – Roadmap

- Allows for a staged approach
  - Fundamental needs
  - Programmatic needs
  - Capital project needs



VERVE
A ROCKWELL AUTOMATION COMPANY

Planning Phase – to refresh…

- Remember – we are building a 'business case' or program proposal – we must think like the boss
- A plan is essential
- The plan must be practical
  - Must address real risk that is outside the organizations risk tolerance
  - The deployment/improvement of the program must be scaled to allow for time, resources and other practical considerations

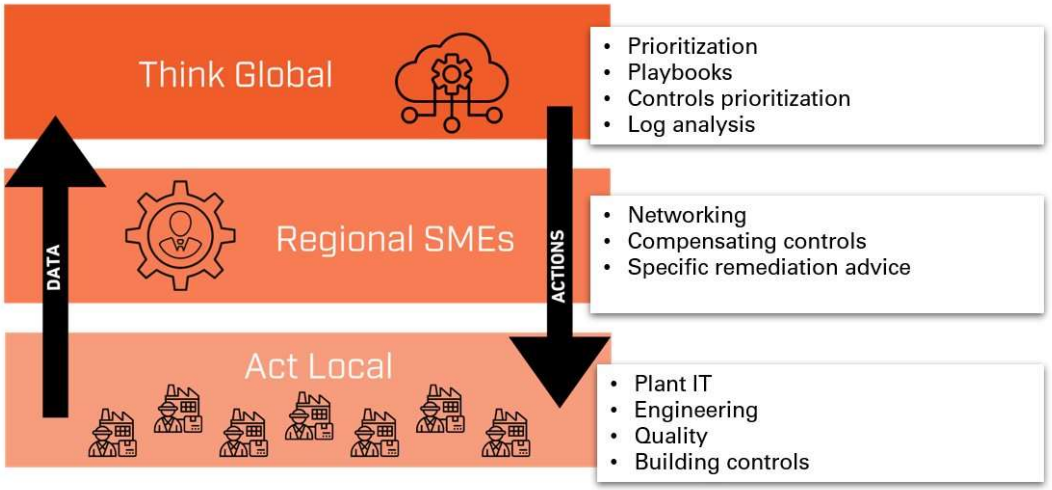
- This approach allows you to present a scalable, sustainable, practical approach to improvement – again – we are not ringing the alarm or crying wolf – we are building something reasonable, built on evidence as measured against corporate risk aversion and real world trends

- Now time for the bonus – how it will all be measured and maintained

VERVE
A ROCKWELL AUTOMATION COMPANY

Measure and Maintain

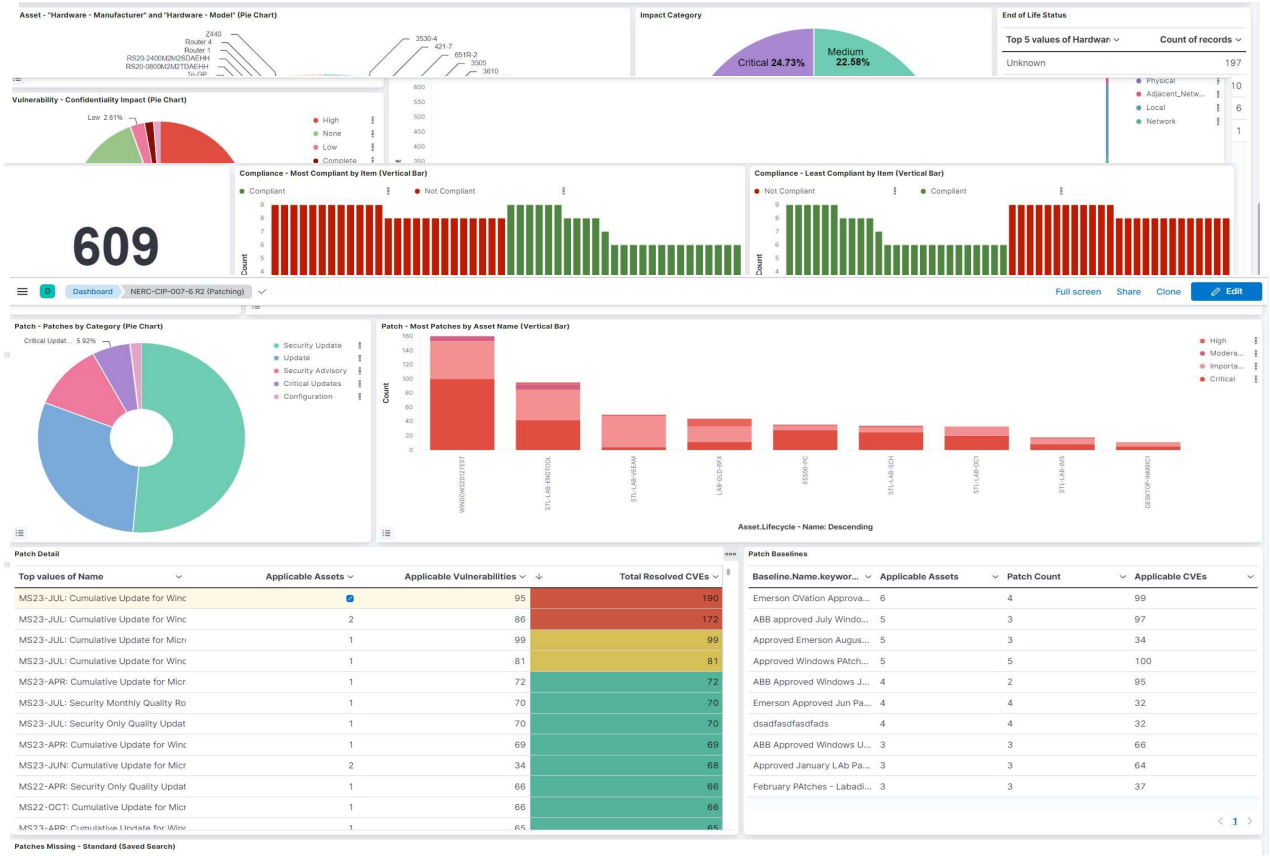
- Anyone can buy technology – not everyone gets sustained value from it
- A solid 'business plan' needs to include recurring or ongoing costs and be able to prove the spend is having an impact
- The only way to do this for a multi-discipline security program across multiple sites and facilities is through automated updates
- A centralized view is also key
- The combination of the above is what we call 'Think Global, Act Local'



VERVE
A ROCKWELL AUTOMATION COMPANY

Measure and Maintain

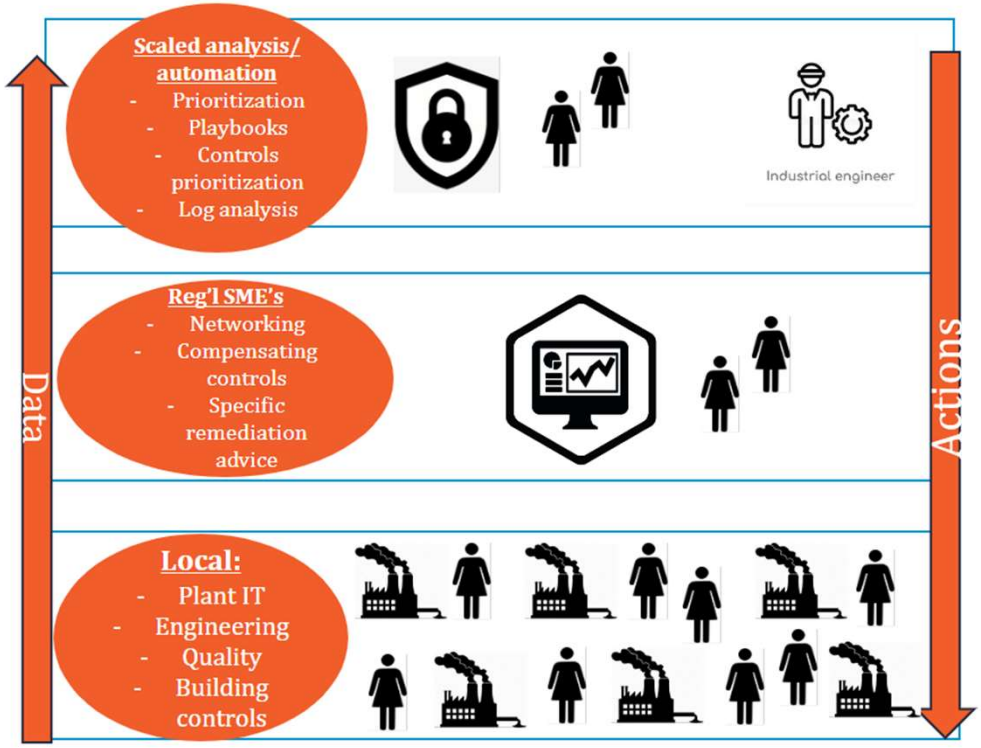
- Any number of specific practices and disciplines can be tracked/reported on with this approach such as:
  - Vulnerability tracking
  - Asset Risk Score
  - End of life status
  - Patch levels
  - Configuration status (least privilege)
  - Backup/AV status, etc.



VERVE
A ROCKWELL AUTOMATION COMPANY

Use case: Up to 70% cost reduction with “Think Global:Act Local” architecture model

1. Think Global: Scale analysis in centralized Platform (Gather data from all sites into centralized database for vulnerability and risk analysis and remediation/response planning)
2. Leverage regional SMEs with access to same platform for specific security advice
3. Act Local: Operations control over actions. : provide automation to plant/regional personnel to enable them to take action in way that is sensitive to requirements of operational environment. etc.



VERVE
A ROCKWELL AUTOMATION COMPANY

Key organizational principles

Build alignment at the top

- Work through rigorous process of risk assessment & risk acceptance
- Align on objective and metrics to measure (pick a standard)
- Build a cyber security portfolio of initiatives
- Clarify senior-level responsibilities

Follow the money

- Analyze total spend on cyber-related expenses across functions and business units
- Determine budget commitment to cyber security as percentage of revenue/IT/etc.
- Allocate budgets across BUs/functions aligned with risk

Think Global: Act Local

- Centralize analysis, planning and reporting
- Ensure local/OT control over actions that impact operations (patching)

Use balanced scorecards & KPIs

- Review current operations and IT-balanced scorecards
- Add cyber security targets as defined in the specific objectives
- Include metrics in annual process review

Get tactical

- Develop detailed accountabilities and authority across all 7 key functions w/in cyber security (O&M, analysis)
- Build detailed operational action plans (safety, product quality) to be followed
- Link actions to specific outcomes

VERVE
A ROCKWELL AUTOMATION COMPANY

Summary

- This ‘tech enabled’ assessment provides significant benefits such as:
  - Contextual risk analysis
  - A ‘right sized’ approach to activity and urgency
  - Ability to begin remediation
  - The creation of a long term, staged approach to security
  - Management, maintenance and reporting with minimal staff impact (recurring costs)
  - An accelerated cyber security maturity journey
  - Maximum ROI and minimal TCO

VERVE
A ROCKWELL AUTOMATION COMPANY

Thank You

Rick Kaun

rkaun@verveindustrial.com

P: 403-827-5794

verveindustrial.com

VERVE

*Scan the QR code to **learn more** and **Contact Us** or **Schedule a Demo!***