5 PRINCIPLES FOR

Designing a Successful Governance Model

FOR OT CYBER SECURITY

GOVERNANCE IN OT

WHAT IS THE RIGHT GOVERNANCE MODEL FOR OT CYBER SECURITY?

Governance: Who has authority? Who is accountable? These are the two most important questions in reducing cyber risk to operations.

There are “big G” Governance questions such as:

- Who should set the overall OT cyber security agenda?
- What metrics should be achieved?
- Who should have authority to make the ultimate risk tradeoffs?
- Who is accountable if a cyber security incident occurs?

There are also “small g” governance questions such as:

- Who will decide whether to patch a specific device or create a mitigation plan?
- What tools will a business use to address cyber risks?
- Should a specific device be replaced if its firmware is out of date, or can it wait until the next upgrade cycle?

More than talent, tools, or tactics, governance is the most fundamental decision to get right in order to achieve success is defending critical infrastructure.

We often hear debates about the involvement and authority of IT and OT departments in governing security. Should the CISO, Head of Operations, or CIO lead the charge? Who should control the security decisions on OT assets within a plant or SCADA environment?

If the CISO is held accountable, shouldn't they also be the one to make cyber security decisions? If the CISO holds authority and accountability, shouldn't they also hold the budget and resources?

In today's large and complex industrial organizations, two themes emerge:

1. There is no "one-size-fits-all" answer: The right governance structure depends on the culture and existing model of the rest of the organization

2. There is no "single point of authority and accountability" for all decisions: The right governance involves coordination and shared decision-rights across IT, security and risk management, operations, and finance.

Although it would be nice to have a standard construct where accountability and authority are vested in one person or organizational function, this is nearly impossible given the realities of managing operations, assets and processes.

If the right answer is critical to OT cyber security success, yet it is so varied, how do you design the right approach for your unique organizational needs?

There are five key principles to establishing the right governance model for OT cyber security:

C-SUITE ALIGNMENT

GO WITH THE FLOW

DETERMINE SPEND

ADOPT KPIs

GET TACTICAL

ONE: SECURE C-SUITE ALIGNMENT

Achieving the right governance model requires clear alignment from the C-suite to determine the risks to operations, the risk appetite of senior leadership and board of directors, a rough cost estimate to achieve different levels of security maturity, and how the senior team will make decisions in each area.

The natural leader for this exercise is the CISO. While a CISO wears many hats, leading a coordinated effort across the C-suite is crucial for success in security governance. This does not necessarily mean the CISO is granted authority to make all decisions. Rather, the CISO plays the role of an influencer when seeking alignment in decision-making, taking into consideration the expectation of balancing resources across the business.

Although specific governance models often focus on where authority and accountability reside, many RACI charts quickly become mundane exercises without a shared understanding of objectives and priorities from leadership.

C-suite alignment ensures budgets, metrics, and resources are based on agreed upon objectives. If you find yourself midway through the OT cyber security journey, the best option is to reset and establish agreement on key objectives to encourage future progress.

TWO: GO WITH THE FLOW [CASE STUDY]

A very successful OT cyber security governance execution comes from a utility holding company, built on a culture of individual business unit independence and ownership of their own results.

The company's incumbent governance model used the distributed business unit P&L ownership model, as seen by industrial organizations such as Emerson Electric, Illinois Tool Works, and Danaher.

The distributed business unit model intends to identify clear accountabilities around the "what," such as targets and objectives, while allowing management of each business unit full authority as to the "how," the strategies and tactics used to deliver results.

The senior team at this utility holding company established a very clear, top-down directive, prescribing the cyber security objectives and standards each business unit was expected to achieve, down to the specific maturity levels of each sub-control, according to CSC Top 20 Control standards.

The CISO was heavily involved in shaping the processes and desired outcomes, but the "how" was left to the discretion of each business unit. While the business units were given authority to make decisions, they must fall within the specific set of objectives and metrics.

They needed to make decisions such as selecting the appropriate tools to deploy, balancing compensation controls, documenting specific approaches to achieving least-privilege settings, and determining action plans for incident response.

As with any approach, there are weaknesses. A few that come to mind are duplicating efforts, the inefficient use of underlying tools, missed opportunity to apply corporate best-in-class approach to each business unit, the need for additional cyber security expertise where talent is limited, and the focus being limited to a set of standards, rather than reducing threats or time to remediation.

While these limitations may be glaring to some, keep in mind this organization did not have a culture of centralized experts or top-down directives of shared tools or infrastructure. To create such a model would require opposition to the primary mode of operation. Had the CISO tried to push in this direction, it would most likely end in failure because it was not in the organization's DNA.

No governance model is perfect. Successfully OT cyber security leaders take time to understand the overall governance culture of their organization and build a model that works with the current flow, rather than trying to force-fit a theoretically "better" governance model. At that point, the CISO will address gaps in the approach to ensure limitations do not become hindrances.

THREE: DETERMINE HOLISTIC CYBER SPEND

One of the most challenging aspects of governance is aligning budgets with accountability. In many organizations, cyber security spend is distributed across the company.

Distributing cyber security spend across an organization may look something like this:

- Plants have responsibility for the budgets of their OT systems including updates, patches, and ongoing management
- Corporate IT manages budgets of network gear and segmentation
- CISO oversees spend on security-specific initiatives, such as anti-malware or monitoring logs for threat detection
- HR holds budget for training and awareness development
- Facilities management is responsible for building systems, which are critical to operations

In this type of distributed environment, capturing total cyber security spend and prioritizing future budget for new protective or detective measures is difficult. But there are different ways to adapt to this situation.

Some companies create a shadow accounting system, aggregating spend from various business units into a holistic cyber security budget. Others ask business units to achieve established objectives while managing overall budgets in line with typical year-over-year increases, making trade-offs for spending on cyber security vs. other items.

Still, other companies manage security compliance plant-by-plant to ensure budgets take cyber security into account as one key element to measure.

Whether your organization uses one of these models or another alternative, it is important to gain visibility into total cyber security spend in order to align budget authority with security accountability for effective risk management.

FOUR: ADOPT SCORECARDS & KPIs

Successful OT organizations run on metrics, targets, detailed procedures, and tactical results that are monitored on an hourly, daily, and weekly basis.

Cyber security objectives are often too subtle or aspirational: *reduce vulnerabilities, identify potential malware, identify attackers, improve incident response by x%, etc.*

The best OT cyber security approaches work with the flow of operations management to transform subtle objectives into tactical targets and metrics that can be displayed on simple red, yellow, and green charts.

Let's look at an example of an industrial organization who used this operational approach effectively. After adopting the NIST Cyber Security Framework, they implemented a set of measures to be tracked on a weekly, monthly and quarterly basis.

Each control area had a set of targets and metrics, such as the number of critical patches not deployed, number of machines without a backup in the last week, number of false positive alerts, time spent by operational personnel responding to false alarms, etc.

The corporate SOC analyzing threat data was treated like an upstream supplier of material. They were held to standards for threat detection quality and timeliness. The data was shared regularly between operations and the SOC to ensure accountability to one another. When items were not “in the green,” remediation plans were put in place, as they would for a product quality metric.

Operations is accustomed to managing a balanced scorecard of KPIs beyond product volume and cost. In addition to operational metrics, they manage occupational safety, environmental quality and product quality.

Including cyber security as an additional element to the balanced scorecard, organizations align accountability with the authority to assign resources and take action.

FIVE: GET TACTICAL

The NIST CSF contains five core areas and 98 specific subcategories. CSC 20 has over 140 sub-controls. It is not practical for a high-level governance model to succeed across the entirety of these sub-elements.

Just as operations does, the OT cyber security team should build detailed procedures identifying accountable parties and their levels of authority for specific deliverables.

Governance tends to break down at the microlevel. For instance, in the Identify component of NIST CSF, who oversees the asset database with required information? The IT department may take ownership, but an OT team could argue that running IT tools on OT networks is not safe or appropriate.

In some organizations, the information gathered from plant-level assets may be excessive to what corporate requires from a cyber security management point of view. In other organizations, there is an ongoing debate whether to patch a critical device immediately, leave it until an outage occurs, or leave it semi-permanently until the device is upgraded.

In critical operations, where a wrong, or even a correct, but delayed decision leads to lost production, injury, or even death, detailed and assigned decision-rights are crucial. Successful operators take time to thoroughly document the decision rights, as well as details such as who will take necessary actions in maintenance and quality.

These five principles should serve as a guide to designing an OT cyber security governance model that works with an organization's current methods of running operations.

About Verve Industrial

With over 25 years of OT expertise, Verve Industrial is an industrial control systems cyber security company. Verve partners with clients to bridge IT OT security challenges in industrial environments.

The Verve Security Center provides robust asset inventory, vulnerability assessment, threat detection and the ability to safely remediate risks in a unified software-based platform. Growing our customer base 5x from 2018 to 2019, Verve Industrial serves industries across utilities (such as power, oil & gas, water), manufacturing, healthcare, and building controls. To learn more about Verve Industrial, please visit us at www.verveindustrial.com

VERVE
INDUSTRIAL PROTECTION