Honeywell

STAFFING FOR CYBERSECURITY: 5 CONSIDERATIONS FOR PLANT MANAGERS

This white paper provides perspectives for industrial operators determining their approach to cybersecurity staffing and its ROI within process control industries. It outlines five categories of considerations and offers recommendations for decision-making and next steps. The recommendations in this document will help managers identify the business, technical, market and other factors relevant to deciding how to resource day-to-day cybersecurity operations and the reasons for doing so.

Introduction

Operationalizing cybersecurity has been a major challenge for the process control industries. With a priority to maintain uptime, plant managers may need to put off updating security: ironically, implementing cybersecurity across process control networks can be seen as increasing risk. In the past, operations have preferred to isolate these systems from those of the rest of the company, including IT.

Security is increasingly being driven to the forefront, however, and plant management is now required to perform cyber resilience activities that are deemed critical. A number of trends are driving this:

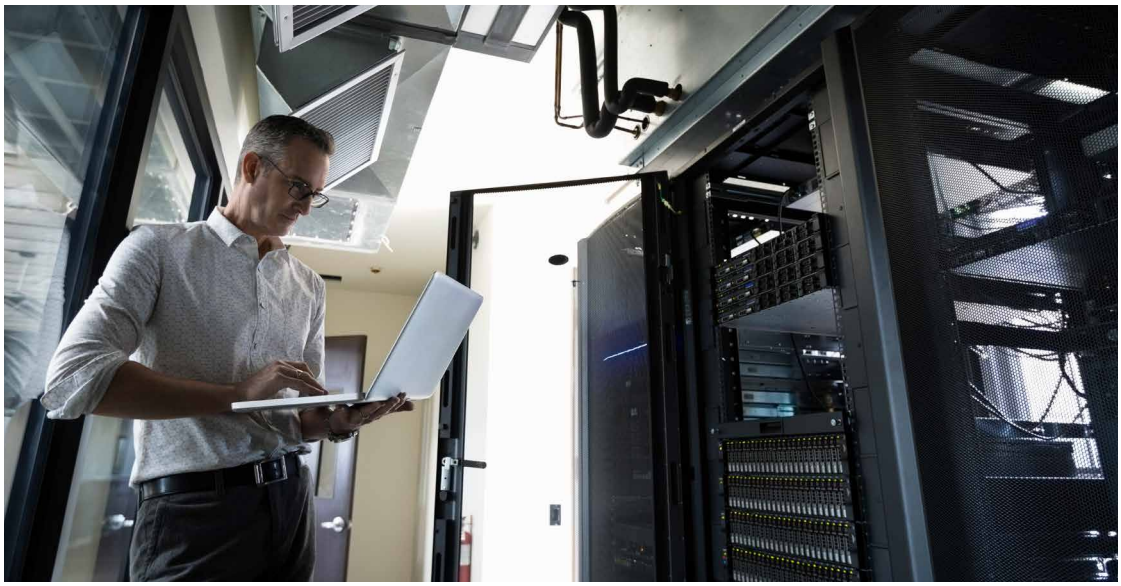
Increased regulation – A range of organizations are requiring plants to comply with increased security demands, including industry-specific regulations (e.g. NERC-CIP for utilities), government regulations (e.g. NIST Cybersecurity Framework), and regional or country-specific initiatives (e.g. the European Union Directive for critical infrastructure).

Board-level attention – Due in part to high profile cyber attacks that have disrupted businesses and placed companies in the headlines, executive boards are increasingly requesting to see and review cybersecurity policies, and are seeking to understand how critical assets for operations are assessed, defended, remediated, and managed day-to-day. Boards are accountable for human safety and environmental issues that can be caused by cybersecurity incidents and, naturally, are looking to reduce risk wherever feasible.

Targeted industrial Cybersecurity attacks – Recent studies regarding USB usage in industrial control environments found that 44% of locations studied faced a security issue because of removable media brought into the facility – and that is only one of many threat vectors that malicious actors are exploiting in their attempts to disrupt operations. Clear warnings from government entities (such as the Department of Homeland Defense and FBI) have highlighted threats specifically targeting sectors such as energy. In the USB research, 26% of the threats found had the potential to cause loss of view or loss of control to operators. Threats targeting ICS continue to advance and require risk reduction measures.

Considering the inevitability of increasing industrial cybersecurity work needed, operators are considering a variety of resourcing models. These often include a combination of in-house personnel and remote personnel, as well as trusted providers (such as Honeywell) who can deliver 24/7 security expertise together with deep process control network understanding, sensitivity and clearance.

Considerations for Determining Cybersecurity Resourcing Models



Five factors must be considered before determining how and where day-to-day cybersecurity work will be completed.

1 - Current Staffing

Honeywell has found that operational personnel are often thinly stretched, and typically work on multiple priorities together with cybersecurity – if they are working on security tasks at all. It is recommended that plant managers identify who, if anyone, is currently supporting security tasks, using a methodology similar to that below:

Staff Member	Key Security Tasks	% of Time on Tasks (daily, monthly, quarterly or annually)
[name or ID#]	[listing – see below for NIST guidance on what to ask about]	

Once you have core data collected in such a table, determine if you have any gaps, by comparing it with the spectrum of necessary cybersecurity activity taken from the NIST Cybersecurity Framework. This identifies the basic work scope for defending industrial networks:

- Identify – Manage cybersecurity risk to systems, assets, data, and capabilities.
  - This might include performing industrial cybersecurity assessments, checking system inventories, reviewing operating system metrics, verifying credentials listings or remote access requests.
- Protect – Ensure delivery of critical infrastructure services.
  - This might include reviewing daily threat

reports, ICS-CERT updates, peer information sharing networks, and other sources of threat intelligence, as well as designing, implementing or maintaining industrial cybersecurity solutions.

- Detect – Identify the occurrence of a cybersecurity event.
  - This might include reviewing SIEM data, reviewing security solution dashboards, checking cybersecurity analyst reports, performing penetration testing to detect weaknesses, or managing intrusion detection or other security solutions.
- Respond – Take action regarding a detected cybersecurity event.
  - This might include selectively bringing down systems, isolating systems, performing forensics using specialized tools and knowledge, communicating with experts internally and externally, locating and applying required patches, performing remediation work, salvaging data, or notifying regulatory bodies to meet legal requirements.
- Recover – Maintain plans for resilience and restore any capabilities or services that were impaired due to a cybersecurity event.
  - This might include procuring back-up systems from local or remote locations, re-installing software, restoring systems following operating procedures, testing availability of services internally or to customers, or deploying temporary systems or solutions.

Considering industrial facilities have traditionally been kept separate from other networks or connectivity, some organizations are not aware of the basic efforts noted above. As benefits from connected plant or digital transformation initiatives continue to drive more plant connectivity, however, it is essential those resourcing security can scope and support these critical activities moving forward.

2 - Threat Levels

The second consideration after internal staff scoping is understanding threat levels specific to your organization and industry.

For companies in the oil & gas, power, water and manufacturing sectors, among others, industrial cybersecurity experts have already verified that targeted threats are a serious concern. If your organization has not recently completed an industrial cybersecurity assessment, performed by properly trained experts in both operations and cybersecurity, that step is recommended.

By leveraging external expertise to objectively review your plant, a detailed scope can be delivered that can help you determine proper resourcing. Industrial cybersecurity assessment reports (such as those from Honeywell), typically list and prioritize necessary work, such as closing down previously unknown open connections, migrating away from easily exploitable machines or operating systems, and upgrading software to improve encryption levels.

With an understanding of the current status, remediation work, and more importantly, the potential impact of such work on the organization, plant managers can consider whether current resources are available to perform the highest priority work. Explanations and education included in the report can also be helpful to enlighten non-cyber stakeholders who influence your cybersecurity resourcing.

Review your latest assessment recommendations in light of your current staffing situation as scoped in consideration number one. Is your current staff aligned to the same priorities? Does your staff have the knowledge, certifications, training, and capacity required to execute the highest priority work?

It is not unusual to discover that in-house staff are clustered around one aspect of NIST work, such as Protect, with significant gaps for staffing in other key areas such as Respond, for example. Consider carefully which types of work from the NIST model and the assessment recommendations may be better suited to your team's skillsets – and which they may struggle to perform regularly due to a lack of expertise.

Develop a simple table to help rapidly identify potential gaps in skillsets:

Resource	Expertise Addresses Threats?	Cybersecurity Expertise	Operations Expertise	When can the resource execute security work?	How efficiently can the resource execute?	How often can the resource execute?
[employee or ID#]	Yes/No [if yes, identify which mapping]	Yes/No [if yes, list specific skills]	Yes/No [if yes, list specific skills]	<1 week <1 month <1 quarter <1 year	• Faster than external provider • Same as external provider • Slower than external provider (metric)	• Every week • Every month • Every quarter • Once a year • Never

These considerations may uncover patterns that suggest leveraging providers outside of your staff. You may have personnel deeply skilled in a particular domain, but no personnel who understand industrial protocols in terms of their exploitability by a hacker. You may have IT personnel you can tap for overall cybersecurity policies, but nobody who can safely harden OT systems without any risk to operations.

In some cases, if the work gap's threat severity and the work's articulated impact on operations are both high, the work might be expedited by outsourcing to a provider who routinely and efficiently performs this work. In other cases, you may find that repeated tasks such as patching (see below) are absorbing a large proportion of staff's time, and, regardless of threat level, such work is best outsourced in order to free them up for other priority work.

Plants should also consider which work could require internal systems access or employee status that could preclude a service provider from doing it. They may need to itemize out or shift portions of the workload accordingly. Some choose to augment their staffing by allowing service providers' staff on site together with plant employees. In many cases, however, remote support for process control networks is an acceptable resourcing model, and with the right technologies and people in place, there will be little difference between employees and hired providers in terms of service levels. Particularly for multi-site operations with facilities in hard-to-reach destinations, a remote staffing model can be both efficient and effective.

Particularly in highly targeted industries, the threat level will dictate the need for expertise. Whether that expertise is in-house, remote or partner-provided is a secondary consideration. More important is to implement the highest priority work that will reduce risk for the organization as quickly as possible.

3 - Patching Needs

Practically every process control network needs efficiency gains when it comes to applying software patches to secure operational systems. While several super majors have advanced practices for this key work, the bulk of industrials get to patching when they can, if they can, and include "sneaker-net" manual work as part of the effort.

As you further weigh resourcing model options, review the threat levels (as above) and apply that thinking to the important effort of patching. The case of WannaCry, a prominent global cybersecurity attack from recent years, is a useful reference. Those organizations that used partner providers to perform patching found they had no business or operational downtime due to the attack. As part of the service level agreements they had in place with providers (like Honeywell) performing the security management work, any patches to secure against high-profile threats had already been applied and had eliminated any risk to operations.

For those organizations where heavily burdened internal staff were tasked with patching, by contrast, time delays, incorrect patch application,

or a lack of knowledge of such high impact threats opened up many a process control network to damage. In addition, weeks of work then ensued to troubleshoot, test, and rapidly apply patches just for that threat. Regular patch updates simply handled as part of routine security management services can avoid this work all together.

This is an important point: looking back at the NIST framework, Respond efforts are often totally overlooked by organizations, but can consume significant resources when called on. As you estimate resources for patch management, recognize that regular, frequent, ongoing work scoped for service providers can lower resourcing need for Respond work.

Overall, do not underestimate the expertise, time, and criticality of software patching. Particularly in operational networks, where legacy equipment may have to remain in place for years before an upgrade is possible, this security work may absorb the bulk of a security team's bandwidth. Knowing how to resource this set of work, such as turning it over to a service provider, can have a significant impact on your team.

4 - Monitoring Needs

The majority of industrial cybersecurity best practices recommend monitoring process control networks for unusual behavior or non-conformity with baseline metrics. A fourth consideration for resourcing is, therefore, how you want to monitor industrial cybersecurity efficacy, and who will perform this work.

Technical solutions can automate and simplify some of the monitoring effort. By working with experts, you can identify an appropriate risk appetite for your organization, as well as useful threat indicators. Monitoring for these can then help focus your own resources on where to take action, rather than spending time reviewing irrelevant data or tracking down portions of data manually.

Service providers can also perform this entire set of work for you, even remotely. Based on your assessment of team skillsets according to consideration number two, identify who on your team, if anyone, can continuously monitor your process control network. And consider who, if anyone, understands enough to identify the meaning and context of an identified alert.

Often, plant managers prefer to be notified only if something significant occurs. In these cases, service providers can perform the majority of monitoring, analyzing, and alerting, following alert procedures defined as part of the up-front service level agreement. Using advanced technical solutions for risk management, providers can also map out who will take which follow-up actions, if and when an issue is identified.

5 - Reporting Needs

Particularly in highly regulated industries, there is a requirement to report on security events or alerts. Not following prescribed procedures can result in fines or penalties. In addition, in the world of industrial cybersecurity, every nanosecond counts, and the faster an analyst receives and reviews necessary information, the better the chances are of preventing or mitigating an incident.

Consider who in your organization needs regular updates regarding industrial cybersecurity status, information, alerts, and overall strategy. Similar to monitoring, some service providers can handle reporting, even automating specific data views or reports for your stakeholders.

Based on your evaluation in the steps above, consider how many stakeholders you need to report to, where they are physically located (since it may impact regulations), and how much of your team's time will be required to support these reporting needs.

Operators who have streamlined and clarified reporting benefit from increased agility, and an improved ability to articulate why security investments or efforts are needed. For example, periodic reports showing security solution server performance can identify when a machine is reaching capacity, allowing the team to upgrade it before it has issues that impair key security functionality. Similarly, keeping the CFO or other executives informed can enhance their ability to respond quickly to boards or inquiring bodies where you are unreachable.

Conclusion

Industrial cybersecurity is a dynamic and important domain, yet many operators struggle to properly support it amidst their operational demands. Using the considerations above, however, operators can better identify and scope the type of work and related skills they need to follow industrial cybersecurity best practices.

Accordingly, they can design resource models that tap into both their in-house and remote capacities, as well as external experts for a more efficient, agile and effective approach to defending their process control networks.

For More Information

To learn more about Honeywell's Managed Industrial Cybersecurity Services, visit www.becybersecure.com or contact your Honeywell account manager.

Honeywell Process Solutions

1250 West Sam Houston Parkway South
Houston, TX 77042
Honeywell House, Arlington Business Park
Bracknell, Berkshire, England RG12 1EB
Shanghai City Centre, 100 Junyi Road
Shanghai, China 20051
www.honeywellprocess.com

WP-19-01-ENG | 01/19
© 2019 Honeywell International Inc.

Honeywell