TOP 3 MEGATRENDS DRIVING OT CYBERSECURITY

As organizations look to automation for a competitive advantage, the cybersecurity threat landscape in operational technology (OT) continues to expand, making it increasingly important for organizations to stay ahead of the curve. In this paper, we examine the megatrends shaping the future of OT cybersecurity and the measures organizations can take to protect themselves.

INCREASED THREATS TO OT ENVIRONMENTS

The number of cyber-attacks involving OT systems has been steadily increasing in recent years, highlighting the need for organizations to prioritize the security of these critical systems. Some of the reasons attacks on operational environments are increasing include:

- Bad actors now realize these environments tend to be under-protected.
- The proliferation of industrial internet of things (IIoT) devices and connected systems in OT environments has created new attack surfaces and increased the potential for security breaches.
- The complexity of securing OT systems is increasing.

The global cost of cybercrime is escalating, with a portion of this multi-trillion dollar cybercrime cost number being attributed to attacks on operational technology environments. This highlights the growing threat to OT environments and the need for organizations to improve their cybersecurity measures to protect against attacks, especially since OT systems play a critical role in the safe and effective functioning of industrial processes.

SHIFTING CYBER CONTROL TO THE C-SUITE

Responsibility and decision-making on OT cybersecurity continues to shift from operations to more traditional information technology (IT) structures with a Chief Technology Officer (CTO) or Chief Information Security Officer (CISO). The integration of OT systems with IT systems has led to this shift in the management of cybersecurity.

In the past, operational technology systems were often managed separately from IT systems, with different teams responsible for each. As the use of digital technologies in industrial control systems (ICS) has increased, it has become increasingly common for organizations to adopt a more centralized approach to managing cybersecurity, with responsibility for both IT and OT systems falling under the CTO or CISO.

However, this shift doesn't always best address the unique challenges (and catastrophic perils) posed in improving security for applicable OT systems. The application of cybersecurity in IT vs OT environments is very different, with OT requiring more specialized knowledge, monitoring, and management capabilities to help ensure operations are not inadvertently disrupted.

INCREASING INTEREST IN REGULATING CYBER

Lawmakers continue to implement stricter rules and standards impacting cybersecurity while seeking greater transparency on incident reporting. Several recent actions have been addressed by lawmakers to improve the cybersecurity posture on OT and critical infrastructure. Some examples include:

- The EU Agency for Cybersecurity (ENISA) has developed a set of guidelines for securing industrial control systems in the EU, which provide recommendations on best practices for securing OT systems.
- The National Institute of Standards and Technology (NIST) has released a new concept paper for the NIST

2.0 Cybersecurity Framework. There will likely be potential significant updates to the NIST Cybersecurity Framework, to increase the ability to support critical infrastructure and other organizations as they try to minimize cyber risk. The paper is a concept draft subject to industry feedback at this juncture.

- The US enacted the Cyber Incident Reporting for Critical Infrastructure Act Of 2022. The proposal requires critical infrastructure owners and operators to report cybersecurity incidents within 72 hours. The legislation is subject to a 24-month implementation period as standards for reporting are being developed by the USG. Incident reporting requirements are being proposed globally, and other key examples of such include NIS 2 Directive in the EU and a similar proposal from India Cert-In.
- There is also motivation globally by lawmakers in various countries to identify what constitutes critical based on threats faced and risk. The US is looking to establish and update its existing framework for "systematically critical infrastructure" as is Australia and the EU.

These are just a few examples of a global trend where lawmakers seek to improve the posture of cybersecurity for critical infrastructure. Organizations operating in different regions and industries may be subject to varying laws and regulations. It is important for these organizations to stay informed about the latest legal requirements and best practices for better securing their systems while remaining compliant with governing regimes.

WHAT SHOULD ENTERPRISES DO IN RESPONSE?

To help combat concerning megatrends, we recommend focusing on 4 critical outcomes:

1. **Reduce your OT cybersecurity risk.**
   Honeywell offers certain Honeywell OT cybersecurity solutions that are designed to help you gain ongoing visibility and insight into your cybersecurity posture. Allowing you to help identify indicators of a cyberattack within seconds.
2. **Increase your cybersecurity resiliency.**
   When you do experience a breach, Honeywell OT cybersecurity offers certain professional services and product solutions that are designed to help you recover and get operations back.
3. **Better manage the cost of cybersecurity.**
   Reduce the cost and potential cyber vulnerabilities of multiple OT cyber vendors and in-house solutions by selecting a vendor that has multiple offerings. For example, Honeywell offers certain Honeywell OT cybersecurity solutions that, in some cases, may be able to reduce the cost of threat monitoring by up to 80% versus an in-house equivalent solution.
4. **Help ensure business continuity.**
   Help avoid downtime, which can cost millions – in a typical refinery, the cost can be potentially $1M+ per hour. Honeywell offers certain Honeywell OT cybersecurity solutions that are designed to help you manage your operations with minimal disruptions.

A cybersecurity journey can be better with an experienced provider. Contact Honeywell to request an OT cybersecurity consultation.