INDUSTRIAL CYBER SECURITY

Safely embrace the digital age with advanced solutions and services to reduce cyber risk.
THE RISKS TO INDUSTRIAL OPERATIONS HAVE CHANGED – HAVE YOU?
DIFFERENT SECURITY FOR DIGITAL TIMES

The risk to industrial operations from cyber incidents has markedly changed in the past several years. Powerful nation-state-level hacking tools are publicly accessible, and once-theoretical threats have been actualized, causing over a billion dollars in damage to manufacturers\(^1\). Cyberattacks in 2018 are ranked among the top three threats facing the world, according to the World Economic Forum\(^2\). At the same time, compelling new benefits from plant connectivity and data analytics are propelling industrials into the digital age.

While these are challenging forces, there is a rational strategy to reduce the risk of cyber disruption. Through a defense-in-depth approach, industrial companies can mature their cyber security measures to better protect against new and emerging threats. This same effort can simultaneously help modernize aging systems, and bring new functionality to improve plant operations.

Honeywell has a long history of reducing cyber risks across process control networks and enabling Connected Plants. We combine innovative industrial cyber security technologies with hard-to-find expertise to protect industrial assets, operations and people from digital-age threats. Through our worldwide Industrial Cyber Security Centers of Excellence, we help customers test their security against simulated attacks, educate teams, and trial state-of-the-art solutions. Every day, in regions across the globe, we work with refineries, paper plants, pharmaceutical companies, chemical companies, and many other manufacturers to minimize their cyber risks and maximize their productivity.

### Figure IV: The Evolving Risks Landscapes, 2015-2018

#### Top 5 Global Risks in Terms of Likelihood

<table>
<thead>
<tr>
<th>Year</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
<th>4th</th>
<th>5th</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>Interstate conflict with regional consequences</td>
<td>Extreme weather events</td>
<td>Large-scale involuntary migration</td>
<td>Extreme weather events</td>
<td>Extreme weather events</td>
</tr>
<tr>
<td>2016</td>
<td>Extreme weather events</td>
<td>Extreme weather events</td>
<td>Extreme weather events</td>
<td>Large-scale voluntary migration</td>
<td>Natural disasters</td>
</tr>
<tr>
<td>2017</td>
<td>Failure of national governance</td>
<td>Failure of climate change mitigation and adaptation</td>
<td>Major natural disasters</td>
<td>Extreme weather events</td>
<td>Cyberattacks</td>
</tr>
<tr>
<td>2018</td>
<td>State collapse or crisis</td>
<td>Interstate conflict with regional consequences</td>
<td>Large-scale terrorist attacks</td>
<td>Data theft or leak</td>
<td>Data fraud or theft</td>
</tr>
</tbody>
</table>

#### 2018 Top 5 Global Risks
- #3 Cyberattacks

### Top 100 U.S. Manufacturers: Cyber Security Concerns

Source: IBM 2017 X-Force Threat Intelligence Index

<table>
<thead>
<tr>
<th>Category</th>
<th>2017</th>
<th>2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber attacks cited as Risk in 10-k Filings</td>
<td>92%</td>
<td>+44%</td>
</tr>
</tbody>
</table>

1 - Source: http://www.securityweek.com/notpetya-attack-costs-big-companies-millions
TAKE A DEFENSE-IN-DEPTH APPROACH

Industrial companies can rapidly adapt to new levels of threats through a flexible and pragmatic defense-in-depth approach. The U.S. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) recommends defense-in-depth, a “holistic approach—one that uses specific countermeasures implemented in layers to create an aggregated, risk-based security posture—to defend against cyber security threats and vulnerabilities.”

By layering in technologies such as cyber risk monitoring across the process control network, and improving processes such as software patching on operational networks, vulnerabilities are less likely to be exploited, and incident response time can be shortened. The more efficiently and effectively companies can manage security, the better they can prevent or withstand a cyber incident.

Honeywell has over 50 years of process manufacturing experience and more than 200 industrial cyber security professionals to help you safely design, implement, and manage defense-in-depth measures. Our world-class resources include innovative software solutions, highly skilled consultants, technology partnerships, and global Centers of Excellence. For 24/7 support, Honeywell Managed Security Services can fully manage your industrial cyber security operations, including taking care of patching, reporting, and system access control activities and managing technologies for you.

MEASURE PROGRESS

ASSESS YOUR INDUSTRIAL CYBER SECURITY MATURITY LEVEL

Honeywell cyber security consultants can help you identify your company’s stage in terms of industrial cyber security maturity. Based on what people, process, and technology measures you have in place, a roadmap can be implemented to continually build cyber resilience and reduce risk. Immediate steps can be taken – such as performing a risk assessment and scanning all USB drives for malware – and more advanced measures – building a security program – can be integrated over time. By understanding the level of maturity, you can measure progress and align security to your most important assets, operations, and people.

Honeywell can help customers identify and evaluate their industrial cyber security maturity level, and then prioritize efforts to increase resilience and reduce risks.
PAIR SECURITY WITH YOUR DIGITAL TRANSFORMATION INITIATIVES

Approximately 64% of industrial companies recently surveyed have started a digital initiative or IIoT, or plan to within the next year. Yet very few have adopted the corresponding levels of security, whether related to people, process, or technology. Many of the industrial companies surveyed (45%) don’t have accountable cyber security leaders at the plant or enterprise level, and only 37% of plants are monitoring for suspicious behavior.

Today and moving forward, the risk of our times is digital in nature. It comes through knowing a specific technical protocol like ModBus and manipulating it to control an asset. Or obfuscating digital machine readings, so operators are blind to equipment that might be surpassing safety thresholds.

Now is the time to address the different types and levels of risk specific to your facilities, and plan security in from the outset. People, process, and technology are still at the core of industrial cyber security best practices, and these are exactly the aspects of business that digital transformation will overhaul. Pair security with your multi-year transformation initiatives now, so that countermeasures are built in every step of the way.

Honeywell Connected Plant initiatives can help drive your business outcomes, while ensuring cyber security is a fundamental part of your fully enabled transformation.

Source: LNS Research

Honeywell’s Security Consulting Services help manufacturers and critical infrastructure organizations manage the availability, reliability and safety of their industrial control systems (ICS) and plant operations amidst heightened cyber security risks. From assessments and audits to response and recovery, the portfolio of services leverages Honeywell’s industry-leading expertise and experience in process control environments and industrial cyber security. Having delivered more than 1,000 projects globally, Honeywell’s certified experts help users improve their cyber security posture.

Honeywell’s industrial cyber security know-how encompasses automation assets and their integrated communication networks—a distinct advantage in control system security. Honeywell’s architecture and methodology support IEC 62443 concepts, continually addressing cyber security throughout the industrial automation and control system lifecycle—from design and implementation to commissioning. Our vendor-agnostic solutions include security assessments and audits, architecture and design, network security, endpoint protection, situational awareness, and response and recovery.

Assessments and Audits

Customers rely on Honeywell’s comprehensive cyber security assessments to identify and evaluate their current security posture, and then prioritize efforts to reduce risks. Recurring assessments allow cyber security teams to track their milestones and the maturity of their security program over time to indicate progress toward achieving their desired assurance level.

Penetration Testing

As a stand-alone service or as part of an assessment engagement, CyberVantage Penetration Testing will put your cyber security program through its paces. Acting as “white hat” hackers, our experts provide a realistic simulation of an attack on the network within the parameters you define, and deliver a detailed report with recommendations for mitigating risks and vulnerabilities. Whether targeted against a single application, a network or entire facility, penetration testing enables businesses to see what an attack would look like.

Process Control Network Hardening

Honeywell’s experts will make your operational assets a more difficult target for cyber attackers. To reduce your attack surface, we identify weaknesses and implement best practices across people, processes and technology, improving your overall cyber security maturity. Providing advice, implementation and configuration services, we’ll help put in place multiple safe layers of defense across your operations to reduce the risk of cyber incidents.

Secure Network Refresh

Cyber security is an on-going process Honeywell is committed to providing end-to-end services to keep facilities protected across their operational lifecycle. The CyberVantage Secure Network Refresh service helps industrial operators improve process control network (PCN) performance and security by replacing older and obsolete network equipment that is particularly vulnerable to cyber security attacks.

Our consultants are deeply versed in both industrial operations and cyber security to help companies best:

• Assess their ICS Risks
• Design Robust Architectures
• Protect Networks and Endpoints
• Increase Situational Awareness
• Improve ICS Incident Response.

Make your systems more secure, keep them connected, and ensure they remain up and running for a safer, more reliable and more profitable business.
Over the past 10 years Honeywell has grown its Managed Industrial Cyber Security Services to a customer base of more than 400 sites worldwide. Honeywell’s new CyberVantage Managed Security Services today encompass all the traditional Managed Industrial Cyber Security Services, such as Secure Remote Access & Support, Automated Patch & Anti-Virus Delivery, and Continuous Security & Performance Monitoring, and Interactive Activity & Trend Reporting. However, to address customers’ new and more advanced cyber requirements, CyberVantage Managed Security Services also provides new cutting-edge services such as Security Device Management Service, 24x7 real-time monitoring and threat identification & notification as well as incident response support. In addition, many services can now be offered over multiple vendor control systems to deliver a more complete cyber security solution.
Benefits of Managed Security Services

- Increased cyber resilience - improves operating system security, robustness and stability to reduce the risk of downtime
- Expedited risk mitigation – remote experts ensure security work is skillfully completed
- Improved recovery time – on-call expertise delivers technical guidance as new ICS vulnerabilities are uncovered
- Better safety record - fewer service people on site reduces safety incidents and maintenance costs
- Consistent security management – dedicated professionals focus fully on operational management of your security solutions and needs.

Honeywell today offers both new customers and existing subscribers to our Managed Industrial Cyber Security Services the option of establishing their own Security Centers through the use of ICS Shield, the same technology platform employed in Honeywell’s Managed Security Centers.

CyberVantage Managed Security Services offers a set of managed services to ensure you get the most out of your software investment. The following outlines the full set suite of services in CyberVantage Managed Security Services offerings:

**Secure Remote Access and Support**
This service is provided to customers that desire a single secure solution for all remote connectivity. Honeywell’s secure access solution has the following enhanced security features:
- Highly Secure
- Exceptional Audit Capabilities

**Automated Patch and Anti-Virus Delivery**
Honeywell’s software updates undergo extensive application testing on systems emulating a customer’s production environment. Testing and qualification of newly released patches and anti-virus files adds to system stability by identifying and restricting potential ICS conflicts before implementation on site. This helps assure customers that installing Honeywell-approved releases will add to the reliability and security of their system. Honeywell’s secure connection approach is used to provide automatic, encrypted delivery of all patches and anti-virus files. This method is designed to reduce the potential for tampering, contamination, or modification of files from email transmissions or compromised portable media.

**Security Device Management**
Honeywell works with customers to provide the approved configurations, custom definitions, and ongoing monitoring required for the industrial manufacturing environment—adding real security to plant systems and operations. Our offering of CyberVantage Managed Security Services complement the Industrial Cyber Security Risk Manager solution. As Risk Manager identifies risks and notifies you of vulnerabilities, and help you implement countermeasures. In addition, Risk Manager can optionally be co-managed as a service to improve your situational awareness.

**Threat Detection and Vulnerability Identification**
- Installation & Maintenance of log collectors; support for deployment and configuration
- Streaming data into a hosted SIEM
- Centralized logging for Correlation and Analysis
- Monitoring/Alerting/Reporting
- Threat hunting & Incident Response support
- Data collection for incident investigations

**ICS Shield Services**
- ICS Shield software installation and support
- ICS Shield Hosting & Operations
SECURE MEDIA EXCHANGE (SMX): Protect Against New and Emerging USB-Borne Threats

Honeywell Secure Media Exchange (SMX) reduces cyber security risk and limits operational disruptions by monitoring, protecting, and logging use of removable media throughout industrial facilities. The SMX gateway security device simply resides in your physical “front desk” or the site location of your choice. A consumer-driven touch screen intuitively prompts visitors to insert their removable media as part of check in procedure. Malware and malicious USB behavior can be detected before threats can impact critical infrastructure. As part of an innovative private hybrid cloud subscription service (ATIX), managed by Honeywell, SMX delivers vendor agnostic ICS threat updates for evergreen protection.

ICS SHIELD: Safely Manage and Secure Your Connected Plant

Honeywell ICS Shield is an industrial cyber security software platform to simplify security operations management across diverse process control networks, sites and vendors. Safely transfer data across or between sites, and securely manage all remote access to industrial field assets through a single operations center. Field proven with more than 1 million industrial nodes managed globally, ICS Shield delivers unrivaled cyber security visibility, reliability and compliance for industrial plant operations.

RISK MANAGER: Measure, Monitor and Manage Cyber Risks

Honeywell Industrial Cyber Security Risk Manager provides operations, IT and leadership teams a single view of industrial cyber security across the enterprise. The first of its kind to use a business intelligence based approach to assess risk, Industrial Cyber Security Risk Manager provides a repeatable way to efficiently reduce security risks.
Honeywell Industrial Cyber Security Centers of Excellence (COE) provide state-of-the-art facilities and specialized technical personnel to help you simulate, validate, and accelerate your industrial cyber security initiatives – all in an exciting setting with world-class demonstration capabilities. By leveraging our COE resources, you can ultimately save time and budget, and avoid costly security mistakes as you improve your organization’s industrial cyber security maturity.

COEs help educate operators, engineers, as well as executive leadership, sharing the latest best practices to protect process control networks from current and emerging industrial cyber security threats. At our COEs worldwide, you can experience simulated control system cyber-attacks, safely test your industrial solutions, and try out both existing and experimental new security solutions.

Honeywell COEs specific to industrial cyber security are currently available in Atlanta, Georgia (USA), Dubai (UAE), and Singapore, and our Centers are open to any customer or interested party around the world. Our COE footprint continues to expand together with customer needs.
Honeywell is the leading provider of cyber security solutions that protect industrial assets, operations and people from digital-age threats.

With more than 15 years of cyber security expertise and more than 50 years of industrial domain expertise, Honeywell combines proven cyber security technology and industrial know-how to maximize productivity, reliability and safety. We provide innovative cyber security software, services and solutions to industrial and critical infrastructure customers around the world that protect industrial assets, operations and people. Our complete portfolio leverages Honeywell’s industry-leading expertise and experience in process control and cyber security. Years of providing industrial cyber security solutions have resulted in proprietary methodologies, best practices, and a comprehensive understanding of cyber security requirements for the process control domain.

Honeywell Credentials

Honeywell Industrial Cyber Security professionals have an unrivaled track record in process control and operational technology, cyber security and IT— an essential skill set combination for protecting plants and critical infrastructure. Certifications held by our global team include:

- Certified Information Systems Security Professional (CISSP)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Information Security Manager (CISM)
- Cisco Information Security Specialist (CISS)
- Certified Ethical Hacker (CEH)
- GIAC Certified Incident Handler (GCIH)

We’re foremost in the automation industry in our investment in cyber security technology for process control systems, including our state-of-the-art Cyber Security Centers of Excellence around the globe.

For More Information
To learn more about Honeywell’s Industrial Cyber Security Solutions, 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 Zunyi Road
Shanghai, China 200051
www.honeywellprocess.com

©2018 Honeywell International Inc.