Honeywell
THE POWER OF CONNECTED

Industrial Cyber Security

INDUSTRIAL CYBER SECURITY RISK MANAGER & ENTERPRISE RISK MANAGER

New multi-site solution to measure, monitor and manage the cyber security risks that matter most.

“Industrial facilities have clearly become targets for cyber-attacks. Safety and operational continuity demand a clear understanding of these serious, dynamic risks and a program to ensure that they remain within acceptable levels. While most organizations recognize this need, operational people often lack the expertise to properly assess and manage cyber risks. So, we applaud Honeywell’s development of Cyber Security Risk Manager. From what we’ve seen, it is a comprehensive, yet understandable, solution that should meet the needs of operational, automation, and manufacturing IT personnel.”

Sid Snitkin, Vice-President, ARC Advisory Group.

CYBER ASSURANCE: A MASSIVE CHALLENGE

Cyber threats to industrial control systems have rapidly emerged as key risks to safety, efficiency and continued production across the process industry..

Information coming from LNS Research[1] reveals that 53% or more than half of the 130 respondents from industrial companies surveyed reported working in a facility that has already had a cyber security breach. However, less than half of them (37%) reported adoption of real-time monitoring of the assets on their control network.

The study which also covers strategic decision makers from industrial companies on their approach to the Industrial Internet of Things (IIoT) and the use of industrial cyber security technologies and best practices, suggests that cyber security must be part of a CEO's agenda and central to business strategy. No longer an afterthought, security at every level should be a prerequisite for adoption of new technologies and all plant expansions.

At the same time, leadership teams across industrial organizations today, are under immense pressure to update their policies and infrastructure regarding cyber security, or face serious fines and potential business damages. Regulatory authorities are increasing demand for cyber vigilance, while legal and risk management teams want proof of cyber resilience to prevent liability issues.

"It is no longer sufficient that organizations should have security in the board; it will increasingly become a legal requirement."

—Security Week, discussing Cyber security Disclosure Act of 2017new US federal legislation

[1] *Putting Industrial Cyber Security at the Top of the CEO Agenda, LNS Research 2017*

THE COST OF MANAGING CYBER RISK

Security breach costs are high and rising around the globe especially in the industrial sector.

According to a 2017 study, it was reported that the utilities and energy industry segment has the second highest average annualized cost of cyber crime at US$17.2mil, not very far behind the financial services sector (US$18.28mil).

Based on a 16.8 recovery-days model for a Denial-of-Service attack[1] scenario, a 100mbpd refinery plant at gross refining margin of US$9.45/ barrel[2] may record a US$$15.9mil production loss. This figure quite closely matches the referred study's estimates. But if the same attack results an uncontrolled chemical reaction leading to a 4-month long pollution situation, the same company may incur further liability of a regulatory fine [3] up to US$1.2mil.

The good news, however, is that such liabilities can be prevented. As we consider the growth of Connected Plant initiatives and IIoT across plant infrastructure, integrating cyber security controls and risk reduction, can offer beyond just more secure operations but also liberating the cyber encumbrances that restrict innovations towards gaining and maintaining a competitive advantage.

[1] Cost of Cyber Crime Study, Ponemon Institute & Accenture, 2017, pages 20, 28

[2] Based on 1Q17 gross refining margin average from four US major oil refiners, Market Realist report (Michelle Rey, Jul 14, 2017)

[3] Texas' maximum penalty for violation of oil and gas pollution is $10,000 per day. Natural Resources Code Title 3 " Oil & Gas" Chapter 81, Railroad Commission of Texas (www.statutes.legis.state.tx.us/Docs/NR/htm/NR.81.htm#81.0531)

EFFICIENCY GAINS: FROM 15 HOURS TO 15 MINUTES, $18,000 A YEAR

With the right tools, industrial companies can save millions.

To avoid an outage or an onset of an attack, industrial companies would need:

- Real time access to the security posture of their industrial networks
- Aggregated reporting of security risks across all plants or sites
- Contextualized information about threat impact to operations and decision support for prioritizing corrective action

The first step to risk reduction is to rapidly move away from non-existent or ad hoc security toward clearly defined, managed and optimized security.

Start at the beginning with the basics across people, process and technologies, including assessing gaps and risk levels, and securing glaring vulnerabilities.

But how does an industrial plant operator, for example, convert a US$18,000 annual cost of managing risk to an annual savings of US$18,000?

Manual process of monitoring & measuring cyber risk	Annual Cost*	What can be done to convert these to savings?	Annual Savings
Risk data collection (8 hours a month)	$9,600	Automated real-time data collection	$9,600
Risk data normalization (3 hours a month)	$3,600	At-a-glance dashboard with normalized data	$3,600
Risk data analysis (2 hours a month)	$2,400	Visualized risk indicators with advisory guidance to remediate	$2,400
Risk data reporting (2 hours a month)	$2,400	Easy reports & notifications	$2,400
	$18,000	→	$18,000

*assumption: $100 hourly rate

RISK MANAGER & ENTERPRISE RISK MANAGER, MARKET-LEADING SOLUTIONS FOR INDUSTRIAL CONTROL SYSTEMS

Proactively Measure, Monitor, and Manage Cyber Security Risk

Honeywell's Industrial Cyber Security Risk Manager brings live, plant-wide visibility to industrial cyber security risks. With the new release, the Enterprise Risk Manager allows for multi-site visibility of Risk Manager data in a consolidated view for complete situational awareness. From a central dashboard view, enterprises today, can promote standardized policies and procedures across plants, further cutting the costs, effort and time required for businesses to understand and prioritize their resources to manage cyber risks. Ultimately, Risk Manager will help keep industrial processes safer and more secure, providing an effective response to an ever increasing cyber threat.

INDUSTRY-LEADING TECHNOLOGIES FROM PEOPLE WHO KNOW DISTRIBUTED CONTROL SYSTEMS

Address cyber security challenges in ways not previously possible.

Most cyber security tools detect threats after they've occurred. Risk Manager continuously monitors for indicators of risk, employing powerful proprietary algorithms to constantly identify and analyze cyber vulnerabilities and threats. This proactive detection of risk indicators gives you early insight, more offensive control and more opportunities to eliminate vulnerabilities before they are exploited.

Risk Manager detects and monitors risk originating from 4 sources:

- Endpoint Security
- Patches
- Network Security
- Backup.

The control network is monitored and most servers, workstations, controllers, firewalls, routers and switches are discovered, allowing you to develop meaningful metrics for threat measurement and developing a plan of action.

With Risk Manager, There's No Need to Be a Cyber Security Expert

Risk Manager understands cyber security so you don't have to. It also understands distributed control systems, which is why Risk Manager ensures that devices are ready and safe to monitor before doing anything—so that security monitoring won't impact asset availability. Through a user-friendly interface, Risk Manager allows all levels of users to accelerate their protection efforts, prioritize, and focus on managing those risks that are most important for maintaining reliable plant operations.

Live Monitoring of Devices Throughout the Process Control Network

Control Engineers and Operators must have a full view of their infrastructure, its connections and applications to identify changes an attacker might make in the environment. However an abundance of data from disparate sources can quickly overwhelm staff. Risk Manager provides a consolidated view of contextualized risk information generated by various security solutions, maximizing your investments.

Risk Manager integrates with leading network and endpoint security controls to accurately measure threats as they occur, and also integrates with enterprise security platforms such as Security Information and Event Management systems (SIEMs).

Risk Manager understands that in distributed control systems, networks and devices are interconnected to form systems that are greater than the sum of their parts. Using proprietary algorithms, Risk Manager is able to understand the relationships between zones or devices and to determine how a specific vulnerability or threat to one area might impact other network areas.

Operate at Peak Performance

Risk Manager monitors and reports on patches and prescribes a risk value accordingly. You're then able to better address the never-ending patch management problem by understanding how missing patches impact overall risk to devices, zones or even the entire site.

The Right Context for Your Environment

Most existing cyber security solutions are designed with enterprise IT in mind. However, distributed control systems require specialized capabilities to collect the correct data points from their industrial networks and assess them against relevant criteria for engineers and operators. To achieve this, Risk Manager focuses primarily on industrial cyber security requirements covering the following actions:

- Evaluates indicators of risk using patented algorithms to generate accurate risk scores in line with industry risk management standards
- Monitors risk continuously, in real-time, to provide immediate notification when unacceptable risk is present
- Translates complex indicators of vulnerabilities and threats into metrics that can be used by control engineers and operators without cyber security experience
- Tracks and inventories assets on the network
- Detects the presence of new or unknown devices on the network, so they can be properly managed
- Performs "low-impact" discovery and monitoring of key assets within the Industrial Automation and Control System to maintain reliability while monitoring for risk.

Is Your Cyber Security Maturity Level Improving?

Risk Manager generates trending analytics based on the amount and type of risk you are willing to accept in pursuit of your business goals, and the maximum risk you are willing to take regarding each relevant risk. Risk Manager will help you allocate resources based on your particular KPIs and you will easily be able to gauge the impact of your decisions over time.

Break Down Communication Silos

Risk Manager allows users to search, sort and filter to get just the right information. When something important happens, automatic notifications are sent to ensure that nothing is missed. Built-in reports mean that site-wide cyber security data can be shared more easily with plant personnel, auditors and executives— without the tech talk.

Align with Industry Standards

Several standards and frameworks including ISA99/IEC 62443 and the ISO 27000 series identify continuous monitoring as a critical cyber security program component. Risk Manager simplifies industrial security reporting with less disruption or network delays than manual reporting or IT solution retrofitting.

REDUCE THE COMPLEXITIES OF CYBER SECURITY

Realize your Industrial Cyber Security Program

Risk Manager helps expedite the transformation of cyber security strategies into prioritized, measured and managed risk reduction efforts. It is best used as part of an DCS cyber security program that also includes threat remediation activities, counter measure and controls augmentation, and other defense-in-depth practices.

Proactively Address C-Suite Industrial Cyber Security Priorities

Risk Manager provides executives with the DCS status and risk metrics they need to make informed decisions on cyber security compliance, liability and resilience issues.

BENEFITS OF THE RISK MANAGER SOLUTION

PROACTIVELY
identifies vulnerabilities and threats that could impact the Industrial Control System

EXTENSIVE
industrial security visibility by monitoring network and system devices, network traffic, and rogue devices

REDUCES
reliance on cyber security expertise through easy-to-use interface and actionable remediation guidance

WORKS
with non-Honeywell systems—vendor neutral technology

DESIGNED
for industrial operations—low impact technology that won't disrupt plant operations or cause network delays.

LIVE
data collection and analytics platform that continuously monitors for indicators of cyber security risk

MANAGE MULTI-SITE CYBER RISK WITH ENTERPRISE RISK MANAGER

The Enterprise Risk Manager offers powerful features to improve visibility, cut cost and simplify risk analysis and reporting across multi-sites.

Enterprise Risk Manager (ERM)

ERM can provide real-time visibility of over 20 different Risk Manager sites in a single dashboard at the Level 4 Business Network. Head office users can now quickly detect and drill down to issues at remote sites and integrate the plants with standardized cyber security risk reporting and policies.

Secure information forwarding to SIEM

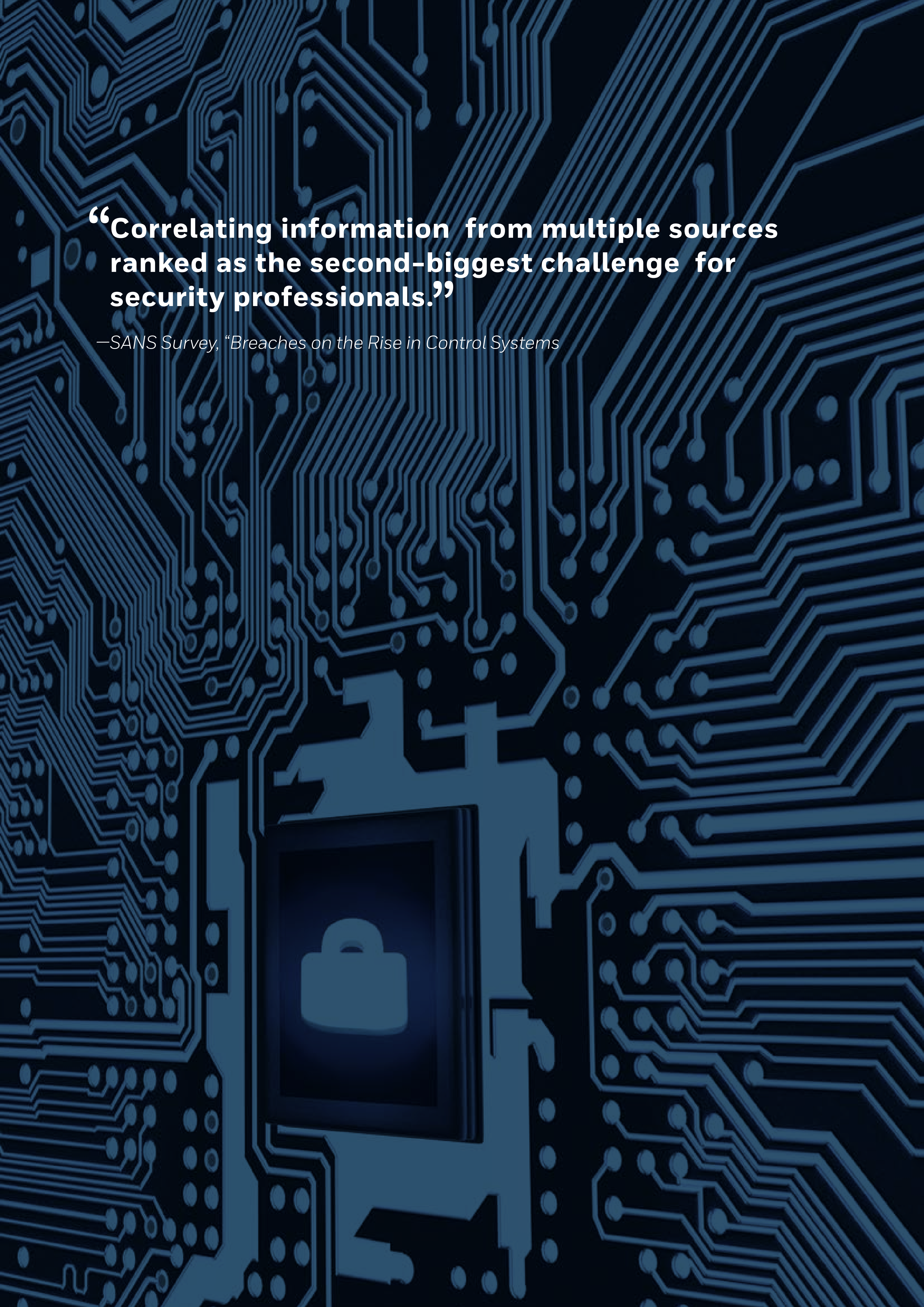
ERM's syslog forwarding displaces the need for investment in third-party syslog collection software, removes concerns of compatibility with industrial control systems, and accelerates risk analysis for operational technology (OT) & IT teams.

Analysis Views

Analysis Views empower threat analysis with simplified and standardized reporting. Drag-and-drop report creation facilitates risk analytics, saving time when performing comparisons and promoting comprehension by turning data into actionable information.

You Don't Have to Go it Alone

Risk Manager monitors, measures and manages cyber risk in a way not previously possible, but nothing replaces human insight. If your staff lacks the bandwidth for leveraging Risk Manager to it's fullest potential, Honeywell can help. Our Managed Industrial Cyber Security Services offering includes remote support that helps maximize the benefits of Risk Manager.



“Correlating information from multiple sources ranked as the second-biggest challenge for security professionals.”

—SANS Survey, “Breaches on the Rise in Control Systems

HOW HONEYWELL CAN HELP

Recent years have seen a major increase in security incidents related to industrial control systems. As new threats emerge and the industrial security landscape evolves, you need an experienced and trusted partner to help protect the availability, reliability and safety of your plant automation system, as well as safeguard people and processes involved in all facets of your operation.

Honeywell Industrial Cyber Security Solutions are specifically designed to defend your control infrastructure and plant operations. These broad solutions leverage our industry-leading process control and cyber security know-how, recognized expertise and advanced technology, combined with partnerships delivering cutting-edge offerings from leading cyber security partners, including McAfee, Palo Alto Networks and others.

Honeywell is a proven industrial cyber security partner that offers:

- Tailored solutions to efficiently secure industrial controls, without impacting processes
- Global/regional industrial cyber security service hubs close to our customers
- Extensive coverage of industrial control networks
- Ability to support our customers from security assessments to cyber security program development
- Track record of completing over 1,000 global industrial cyber security engagements
- Mature solutions with 300+ managed industrial cyber security sites.

At Honeywell we are ready to help you protect your current operation or securely build the next. For more infomration visit becybersecure.com

For more information

To learn more about Honeywell's Industrial Cyber Security Risk Manager, visit www.becybersecure.com or contact your Honeywell account manager.

Honeywell Process Solutions

1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Skimped Hill Lane
Bracknell, Berkshire, England RG12 1EB UK

Building #1, 555 Huanke Road
Zhangjiang Hi-Tech Industrial Park
Pudong New Area, Shanghai 201203

www.honeywellprocess.com

Honeywell