Improving ICS Cyber Security Consistency
Using Managed Security Services

Mark Littlejohn
October 3, 2018
Common Cyber Concerns: Typical Attack Vectors*

- **Brought in by employees, contractors, security guards, etc.**
  - Removal media (e.g. USB) considered #2 ICS threat
  - Laptops, phones, FitBit, Hot Spots and IoT equivalents
- **Multiple unsecure points of connectivity to ICS environment**
  - Multiple vendors accessing ICS environments
  - Ad-hoc remote access solutions
- **Unsecured wireless devices**
  - Unsecure switch and router configurations
  - Rouge access points
- **Access from external/business network**
  - Network scanning/probing due to poor firewall ACLs
  - Relay servers not hardened
- **Vector source not known 38% of the time**

*ICS-CERT and BSI Publications on Cyber Security
54% of industrials surveyed reporting a cyber incident in 2017

$4 Million
Average cost of a data breach now stands at about $4 million

$14.2 Million
Cost of a ransomware attack on a 100 MBPD facility (17.8 day denial of service)

58.5 days
Average time it takes to resolve malicious insider attacks.
A predicted global shortfall of 3.5 million cyber security jobs by 2021 up from 1 million openings last year. 
– Cybersecurity Ventures, 2018

51% of organizations report having a problematic shortage of cyber security skills in 2018, up from 45% in 2017
- ESG Research, 2018

Cyber security jobs forecasts have been unable to keep pace with the dramatic rise in cyber crime, which is predicted to cost the world $6 trillion annually by 2021, up from $3 trillion in 2015.
– Cybersecurity Ventures, 2018
## Outsourcing: The efficient answer to Cyber Security

### Refining related example of cost and time savings

<table>
<thead>
<tr>
<th>Cost Impact</th>
<th>One Site</th>
<th>Fifteen Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automated patching and antivirus updates</strong></td>
<td>Engineering cost saving: Assumption:-</td>
<td>$12K* 15 = $225K</td>
</tr>
<tr>
<td>avoid need to have 1 employee each month</td>
<td>• 10 hrs per month</td>
<td></td>
</tr>
<tr>
<td>perform patching one node at a time</td>
<td>• Burden rate: $125/hr</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• T&amp;L expenses not included</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10hrs a mth * 12 * $125/hr = $15K</td>
<td></td>
</tr>
<tr>
<td><strong>Secure Remote Access</strong></td>
<td>Engineering cost saving: Assumption:-</td>
<td>$30K* 15 = $450K</td>
</tr>
<tr>
<td>avoids trip to site to deal with specific issues</td>
<td>• 20 hrs per month</td>
<td></td>
</tr>
<tr>
<td>(series issues)</td>
<td>• Burden rate: $125/hr</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• T&amp;L expenses not included</td>
<td></td>
</tr>
<tr>
<td></td>
<td>20hrs a mth * 12 * $125/hr = $30k</td>
<td></td>
</tr>
<tr>
<td><strong>Regulatory Penalty</strong></td>
<td>Regulatory Violation Penalty: Assumption:-</td>
<td>$1.2Mil* 15 = $18Mil</td>
</tr>
<tr>
<td>resulting from cyber intrusion. Assumption:</td>
<td>• State: Texas</td>
<td></td>
</tr>
<tr>
<td>Stuxnet-type APT causing uncontrolled</td>
<td>• $10,000/day violation of safety or the</td>
<td></td>
</tr>
<tr>
<td>chemical reaction with safety &amp; environment</td>
<td>prevention or control of pollution.</td>
<td></td>
</tr>
<tr>
<td>impact.</td>
<td>• Impact: Uncontrolled chemical reaction.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Total days for violation: 4 months</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$10K<em>4</em>30 = $1.2Mil</td>
<td></td>
</tr>
<tr>
<td><strong>Avoidance of down time</strong></td>
<td>Production Loss: Assumption:-</td>
<td></td>
</tr>
<tr>
<td>(assume 17.8 days) by preventing Ransomware-</td>
<td>• Probability:-</td>
<td>$513k* 15 = $7.7Mil</td>
</tr>
<tr>
<td>type cyber attack</td>
<td>- vertical - manufacturing (18%):</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- site - refinery (20%)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 17.8 days downtime</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Global refining margin: $8/barrel</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Production: 100MBPD (1000 barrel per day)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(0.18<em>0.2)<em>17.8</em>$8</em>100,000 = $513k</td>
<td></td>
</tr>
<tr>
<td><strong>Improved safety</strong></td>
<td>Staff downtime per year: Assumption:-</td>
<td></td>
</tr>
<tr>
<td>- secure remote access avoid staff</td>
<td>• 22 days sick leave + 38 days hospitalization</td>
<td></td>
</tr>
<tr>
<td>downtime due to hazardous environment eg.</td>
<td>• Staffing: 5 engineers, Burden rate: $125/hr</td>
<td></td>
</tr>
<tr>
<td>radioactive material handling</td>
<td>• Medical bills/insurance not included</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Life insurance death-claims not included</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$125<em>8</em>60*5=$300k</td>
<td>$300*15= $4.5Mil</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td>$2.058Mil</td>
<td>$30.87Mil</td>
</tr>
</tbody>
</table>
Introducing: Honeywell Industrial Cyber Security

Delivered with Trusted Field Cyber Experts & Managed Security Services

- Current State Analysis
- Secure Design and Optimization
- Zone & Conduit Separation

- Policy and Procedures
- Secure Network Refresh
- Firewall, Next Gen Firewall
- Intrusion Detection & Prevention
- Access Control

- Industrial Patching & Anti-Virus
- Industrial Application Whitelisting
- End Node Hardening
- SMX Portable Media/USB Security

- Assessments & Audits
  - Vulnerability & Risk Assessments
  - Network & Wireless Assessments
  - Cyber Security/Compliance Audits
  - Industrial Penetration Testing
  - ICS Shield & Risk Manager

- Architecture & Design
- Network Security
- Endpoint Protection
- Situational Awareness
- Response & Recovery

- PEOPLE
  - PROCESS
  - TECHNOLOGY

- Continuous Monitoring
- Asset Inventory & Management
- Industrial Risk Manager
- SIEM
- Compliance & Reporting
- Awareness & Training
- Advanced Threat Intelligence Exchange (ATIX)

- Backup and Recovery
- Incident Response Planning
- Incident Response: On Site & Remote
- Forensics & Analysis

- Awareness & Training
- Advanced Threat Intelligence Exchange (ATIX)

- Forensics & Analysis
- Cyber Security/Compliance Audits
- Industrial Penetration Testing
- ICS Shield & Risk Manager
Honeywell Provides Full Solutions for Industrial Cyber Security

**INDUSTRIAL SECURITY CONSULTING**
- Industrial security program development
- Assessment services
- Architecture and design
- Implementation and systems integration
- Operational service and support
- Compliance audit & reporting

**INTEGRATED SECURITY TECHNOLOGY**
- Whitelisting
- Antivirus
- Next-generation Firewall
- IDS/IPS
- Security Information & Event Management (SIEM)
- Threat Intelligence

**MANAGED SECURITY SERVICES**
- Secure remote access
- Continuous monitoring and alerting
- Automated patch & antivirus updates
- Security device management
- SIEM hosting and analytics
- Incident response support
- Hosting, management and operation of ICS Shield®

**CYBER SECURITY SOFTWARE**
- ICS Shield® platform for cyber security operations
- Industrial Cyber Security Risk Manager: Enterprise and Site
- Secure Media Exchange (SMX)
- Advanced Threat Intelligence Exchange (ATIX)
- Industrial assessment software & tools
CyberVantage Managed Services

Significantly reduce time, effort, and expense required for cyber security

- **Secure Remote Access and Support**
  - Highly secure remote access solution
  - Encrypted, two-factor authentication
  - Complete auditing: reporting & video playback

- **Patch and Anti-Virus Automation**
  - Tested and qualified patches for operating systems & DCS software
  - Tested and qualified anti-malware signature file updates
  - Multi-Vendor Support

- **Security and Performance Monitoring**
  - Comprehensive system health & cybersecurity monitoring
  - 24x7 alerts, routine performance and compliance reporting
  - Agentless, simple deployment

- **Security Device Management**
  - Management, Rule Changes, Monitoring, and Updates for your PCN security appliances
  - Firewall/NextGen, Intrusion Detection, ICS Shield, Risk Manager, etc.

- **SIEM Hosting and Analytics**
  - Consolidation of logs from all devices in one location
  - 24x7 real-time monitoring and threat identification & notification
  - Incident Response support
Managed Security Service Centers “Follow the Sun”
Global Presence

24/7 Expertise to Reduce Operational Downtime and Lower Cyber Risk

Cyber Security Centers of Excellence Around the World
ICS Shield – the Technology Enabler

Top-down ICS/DCS Security Management

• Automates top-down integrated approach for deployment and enforcement of plant-wide security controls
• Based on proven/tested technology acquired through Nextnine acquisition – over 6000 global installations
• Delivers unrivaled visibility, reliability and compliance for industrial plant operations
• Enables security of remote field assets from a single operations center

Key Features:
• Secure remote access
• Secure file transfer
• Automated patch and AV updates
• Asset discovery
• Performance/health monitoring
• Compliance reporting
Honeywell CyberVantage Managed Services

What is included?

ICS Shield software installation and support:
- Install, configure and testing of software to ensure it works properly
- User support – setting up proper user access and connection restrictions to various sites/assets
- Asset support – making sure all assets/nodes are configured in system properly
- On-going maintenance and software support for all system components
- Monitoring of software (e.g. VSEs and service center software to ensure it is all working correctly)
- Technical training for system users and administrators

ICS Shield hosting and operation:
- Full management of purchased ICS Shield components and capabilities
- Continuous troubleshooting and day to day operations
- Active reporting/alerting - monitor alerts 24/7 and notify of potential threats to the environment; periodic reports to help identify risks and compliance issues
- Supply of control system security patches and anti-virus updates at no additional cost (qualified list to be provided by vendor)
- Anti-virus and patching configuration support (ePO, SEPM, WSUS) for PCN systems
- Secure file transfer support in moving files in and out of ICS environment
ICS Shield Deployment

Distributed architecture and secure tunnel from plants to center

- Install SC at the data center
- Install VSEs at each plant
- Establish a secure tunnel, outbound, using port 443, TLS encrypted
- One FW rule to manage all remote connections

Hosted by Honeywell or in Your Datacenter
## CyberVantage Managed Services

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Highly secure remote access solution</td>
<td>• Tested and qualified patches for operating systems &amp; DCS software</td>
<td>• Comprehensive system health &amp; cybersecurity monitoring</td>
<td>• Management, Rule Changes, Monitoring, and Updates for your PCN security appliances</td>
<td>• Consolidation of logs from all devices in one location</td>
</tr>
<tr>
<td></td>
<td>• Encrypted, two-factor authentication</td>
<td>• Tested and qualified anti-malware signature file updates</td>
<td>• 24x7 alerts, routine performance and compliance reporting</td>
<td>• 24x7 real-time monitoring and threat identification &amp; notification</td>
</tr>
<tr>
<td></td>
<td>• Complete auditing: reporting &amp; video playback</td>
<td>• Multi-Vendor Support</td>
<td>• Agentless, simple deployment</td>
<td>• Incident Response support</td>
</tr>
</tbody>
</table>

---

Significantly reduce time, effort, and expense required for cyber security
ICS Shield Hosting & Operations

Patch and Antivirus Automation

Common for Antivirus and Patch updates
- Automated, secure transfer of Security update files
- Honeywell tested and qualified on equivalent release
- Maintains integrity of files through Secure Connection’s encrypted file transfer. Avoids file modification risk via transfers by email or portable media

Antivirus Automation
- McAfee or Symantec
- Provides a local source of current, qualified signature files for installation
- Central management reduces manual, administrative work
- Reduces delays required to obtain current files and patches

Optional Services Include
- On-site Server & PC installations (in coordination with Honeywell Field Service Engineer)
- Checks to assure latest signatures are installed
- Configuration of automated, staggered signature deployment.
ICS Shield Hosting & Operations

OS Patch Automation

Third Party

Automated, secure transfer of Security update files
- WSUS content and meta data
- Honeywell QPL
- Third Party QPL

Application importing the QPL in the WSUS server

Third Party QPL requirements:
- Based on a structured input file from the Third Party

Prevent Exploits, Infections and Application Malfunction
ICS Shield Hosting & Operations

Security and Performance Monitoring

Continuous Monitoring
- Agentless monitoring solution for system, network and security performance and health
- Tested to ensure no impact on systems
- Automated monitoring of critical ICS configuration and security parameters
- Intelligent analysis based on Honeywell engineering & expertise

Alerts / Situational Awareness
- 24/7 automated, proactive alerting for all monitored devices
- Equipment and device specific thresholds
- Managed Security Service Center automatically generates an alert email or SMS text to site specified contact
- Alert messages may include attached troubleshooting techniques
ICS Shield Hosting & Operations

What Is Monitored?

<table>
<thead>
<tr>
<th>Windows and 3rd Party Nodes</th>
<th>Servers &amp; Stations</th>
<th>TPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Availability</td>
<td>- Process History Database</td>
<td>- ESVT</td>
</tr>
<tr>
<td>- CPU</td>
<td>- Stations</td>
<td>- HM</td>
</tr>
<tr>
<td>- System Memory</td>
<td>- Servers</td>
<td>- GUS</td>
</tr>
<tr>
<td>- Critical Exploision</td>
<td>- e-Server</td>
<td>- NIM</td>
</tr>
<tr>
<td>- Installed Software</td>
<td>- Experience</td>
<td>- APP</td>
</tr>
<tr>
<td>- 3rd Party</td>
<td>- Backup Restore</td>
<td>- ES-T</td>
</tr>
<tr>
<td>- Servers &amp; Stations</td>
<td>- Virtualization</td>
<td></td>
</tr>
</tbody>
</table>

Performance Analyzers for 550+ Critical Parameters
ICS Shield Hosting & Operations

Key Items to Monitor

- Prevent Exploits, Infections and Application Malfunction

Administrative Changes
- GPO Modifications, Group Additions, Enabling USB Devices

System Audit Logs
- Unauthorized Access, Disabling Controls, Configuration Changes

Network Activity Logs
- ACL Rules, Utilization Spikes, Passwords/Strings

System Audit Logs
- Unauthorized Access, Disabling Controls, Configuration Changes

Software Update Compliance
- Aging for Virus Signatures, Security Patches, Software Updates

System Availability/Performance
- Application Health, CPU Utilization, Hardware Errors

Virus Infections
ICS Shield Hosting & Operations

Activity and Trend Reporting

Trend Analysis Complements Alerts
- Ability to catch degrading conditions
- Captures & reports frequency of intermittent issues

Critical Parameter Reports
- Actionable reports of critical system & network information plus security issues
- Out-of-date installation status for Anti-Malware signatures & Windows™ patches
- Inventory of all detected networked equipment
- Key source of data for compliance documentation

Compliance & Health Reports
- Comprehensive, detailed reports including long term trends, plus expert analysis

Audit
- Audit capability including access to session recordings
Security Device Management

Outsource Device Management to Honeywell

Key Features:

- Periodic configuration review
- Implement configuration changes through a change management process.
- Review and follow up on alerts
- Delivery of system updates and signature files

- Making approved changes
- Periodic Health Checks
- Monitoring/Alerting/Reporting

- Software & Signature updates
- Firewalls, IDS, Risk Manager, etc.
SIEM Data Collection & Analytics

Outsourced Security Monitoring & Response support

Why
• Centralized logging – quickly deployed
• Correlation and analysis - fast
• Actionable insight into state and evolution
• Threat hunting
• Extensible, customizable, vendor/solutions integrated

Key Features:
• Installation & Maintenance of log collectors; support for deployment and configuration
• Streaming data into a hosted SIEM
• Monitoring/Alerting/Reporting
• Incident Response support

Detailed monitoring for all devices in your PCN
Honeywell CyberVantage Managed Services

How do we do it?

• ICS Shield software installation and support
• ICS Shield and operation
• Security Device Management
• SIEM log collection and analytics

Based on a Proven Operations Platform - Over 6000 Installs
VALUE AT EVERY LEVEL OF CYBER SECURITY MATURITY

ALL LEVELS 1-5
- Industrial security program development
- Assessment services
- Architecture and design
- Implementation and systems integration
- Operational service and support
- Compliance audit & reporting

LEVELS 1-5
- Patching & Antivirus
- Security Information & Event Management (SIEM)
- Next-generation Firewall
- Threat Intelligence
- IDS/IPS
- Whitelisting

LEVELS 2-5
- ICS Shield Secure remote access
- Continuous monitoring and alerting
- Automated patch & antivirus updates
- Incident response & recovery & back up
- Security device co-management
Hosting, management and operation of ICS Shield
OT SOC management & operations

LEVELS 2-5
- ICS Shield platform for cyber security operations
- Risk Manager: Enterprise and Site
- Secure Media Exchange (SMX)
- Advanced Threat Intelligence Exchange (ATIX)
Providing the Next Level of Enterprise-wide Industrial Cyber Security

ICS Shield

Key Benefits:
• Gain visibility
• Reduce operational risk
• Improve reliability
• Support compliance
• Increase productivity
• Lower operating cost

Multi-Site, Multi-Vendor, Scalable Cyber Security Management

1. Enterprise-wide and site cyber security
2. Multi-vendor cyber security across control systems
3. Professional cyber security field services
4. CyberVantage Managed Services expert support
5. Cyber Security software

ICS Shield
• Secure remote access
• Secure file transfer
• Automated patch and AV updates
• Asset discovery
• Performance/health monitoring
• Compliance

Risk Manager cyber security monitoring and reporting

Secure Media Exchange (SMX) removable media protection (USB)

Advanced Threat Intelligence Exchange (ATIX)
Why Customers Choose Honeywell

End-To-End Solutions

• Partner for industry proven cyber security products, services and solutions
• Scalable and flexible enterprise-wide deployments
• Operational Technology (OT) domain expertise
• Vendor neutral solutions, services and technology
• Global capabilities and local presence

We Protect Industrial Assets, Operations and People
Thank You

www.becybersecure.com
Honeywell is building a smarter, safer, and more sustainable world

THAT’S THE POWER OF CONNECTED
THAT’S THE POWER OF HONEYWELL

Connected Aircraft • Connected Automobile • Connected Home • Connected Building
Connected Plant • Connected Supply Chain • Connected Worker

Honeywell
THE POWER OF CONNECTED