

# **BUILDING RESILIENCE, THROUGH VISIBILITY.**

Cybersecurity

---

Whitepaper

---



**Honeywell**

# Cybersecurity Whitepaper

August 2018

This whitepaper is proprietary to Honeywell. This information is supplied without liability for errors or omissions. No part of this document can be reproduced, used or disclosed in any way, without the prior written consent of Honeywell. The copyright and foregoing restriction of reproduction, use, and disclosure extend to all media in which this information may be embodied.



# CONTENTS

**04**

Synopsis

**06**

Operational Technology in the Digital Age

**11**

Resilience in the face of cybercrime

**14**

Honeywell's approach to cyber intelligence

**15**

Taking action: next steps to a cyber smart strategy



# SYNOPSIS

Close attention to Cybersecurity issues is not new. Over the last decade governments and corporations alike have invested heavily in ongoing Information Technology (IT) security research, resources, training and defender initiatives (offensive and defensive) directed at predicting and mitigating the risk of cyber-threats worldwide. As a result, there is a heightened level of security awareness available in the corporate IT systems environment and furthermore tighter controls on information security in general.

This increased focus and awareness has often been beneficial for securing corporate and more traditional IT systems, such as mail servers and public web servers. However Operational Technology (OT) like building control systems, are often overlooked, potentially vulnerable resulting in a "weak link" in the organization. These OT systems have often been out of sight for internal IT departments, and as such haven't always had the same level of monitoring or maintenance hygiene.

The advent of the Internet of Things (IoT) and demand for smart technology in an increasingly 'connected' world is a contributor to the expanding threat footprint in the OT space. In the past, it has often been common practice to air gap control system networks as they typically didn't need to interact with other corporate systems or the Internet. In theory, having this disconnection has been a sufficient security measure, however this is often no longer operationally feasible in today's connected world. Across all industries, including smart cities, connected buildings, critical infrastructure, etc. there is a rise in smart devices, and the intelligent analytics derived from connecting almost any "thing" to a network in order to deliver additional insights, essential cost savings and operational efficiencies. This evolution will likely continue and be embraced as organizations seek out increased efficiencies and compete in a more global landscape, with that, it's

important that Cybersecurity is a built-in consideration to mitigate the potential introduction of additional cyber risks.

According to the Cybersecurity Ventures report 2017, cybercrime will cost the world US\$6 trillion annually by 2021, up from US\$3 trillion in 2015 and the average cost per breach sitting at around US\$3.79 million<sup>1</sup>. Alarmingly, IBM Managed Security Services (MSS) data reveals there has been a 110% increase in attacks on industrial control systems since 2016<sup>2</sup> - a threat landscape that is predicted to grow at a phenomenal rate to 2020 and beyond.

And the impact of cyber incidents can go beyond mere financial measures – operational and reputational damage can be equally significant if not more critical.

By understanding Cybersecurity risks around OT, decision makers are better placed to make smart buying decisions, implement targeted OT security controls, educate personnel in effective procedural measures and maintain heightened cyber resilience across OT environments.

Critically: Time is of the essence. If organizations are to better protect themselves in the rapidly evolving and dynamic threat landscape brought about by digitization, the need for education and action is now upon us.

Developing a cyber smart strategy is a journey – one that involves ongoing assessment of internal processes and procedures, staff awareness programs and adoption of next-generation monitoring applications – all of which are specific to a set of defined organizational requirements. Working with a trusted solution provider, with deep knowledge of the OT systems you want to protect, will help accelerate this process and identify practical recommendations for enhanced resilience and risk reduction.

1 <https://www.herjavecgroup.com/cybercrime-report-2017>

2 <https://securityintelligence.com/attacks-targeting-industrial-control-systems-ics-up-110-percent/>

## CYBERSECURITY INSIGHTS

**US\$6Trillion**

Expected cybercrime damage cost p/a by 2021<sup>1</sup>

**US\$3.79m**

Average cost of data breach<sup>2</sup>



Control systems need to be monitored and maintained like any IT system

**80%**

Of companies expect an increase in cyber risk over coming years<sup>3</sup>



Not being internet connected doesn't mean systems are secure

**110%**

Increase in attacks against control systems in 2016<sup>4</sup>

1 <https://1c7fab3im83f5gqiw2qqs2k-wpengine.netdna-ssl.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf>

2 <https://www.oasis-open.org/events/sites/oasis-open.org.events/files/Day2-Session4-Allor.pdf>

3 [https://www.raytheon.com/sites/default/files/2018-02/2018\\_Global\\_Cyber\\_Megatrends.pdf](https://www.raytheon.com/sites/default/files/2018-02/2018_Global_Cyber_Megatrends.pdf)

4 <http://www.ibm.com/security/services/managed-security-services/?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US>



# OPERATIONAL TECHNOLOGY IN THE DIGITAL AGE

OT is the hardware and software that monitors and controls physical devices. Put simply, OT is the use of computers to supervise, monitor and/or alter the physical state of a system, such as the control network for a building system or the airfield lighting system for an airport. Unlike IT where the prime responsibilities include supporting people in open networked environments, OT systems traditionally support the machines and process equipment operated in a controlled, closed and at times proprietary manner.

In our connected world, there is a steady move towards open systems and integration, as well as convergence with other OT systems and even corporate IT environments. Physical devices are becoming 'smart' with a growing need for administrators of OT environments to control physical devices remotely, and gain visibility through better, more fluid monitoring mechanisms, e.g. single pane of glass, alerting etc.

Moreover, technology advances in Cloud Computing, Data Analytics, machine to machine (M2M) communication and machine learning have further enhanced the OT landscape. For instance, the capacity to analyze data from physical devices in real-time to support immediate and even predictive decisions often presents an unprecedented advantage over traditional capabilities and lifecycle cost efficiencies. Yet these efficiencies are often accompanied by heightened Cybersecurity risk to the enterprise if not done correctly.



## SMART BUILDINGS AND SMART CITIES OF THE FUTURE

Buildings are rapidly embracing digitization. Today, an enterprise-wide view of integrated building control systems and sensors is typically essential to drive increased productivity, operational efficiency and improved response

time to events. More and more control systems such as heating, ventilation, and air conditioning (HVAC), energy metering and power management, lighting, fire protection and alarms, access control, CCTV surveillance, and voice

and data communications, converge in a connected environment – transforming the way buildings and their occupants operate and interact with each other.



### Internet of Things (IoT)

20+ Billion Devices  
by 2020\*

<https://www.gartner.com/newsroom/id/3165317>



### Cloud and Big Data

Digital universe is doubling in size every two years, and by 2020 will reach 44 zettabytes, or 44 trillion gigabytes\*

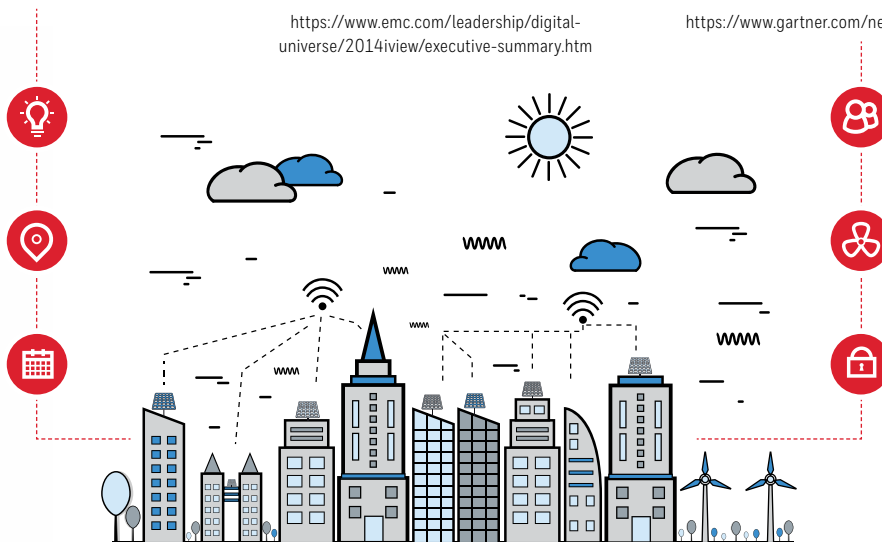
<https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm>



### Connected & Integrated

Buildings accounted for 45% of total connected things in 2015, expected to rise to 81% by 2020\*

<https://www.gartner.com/newsroom/id/3165317>



In the smart building, analytics, actions and accountability are often key. Massive amounts of data typically traverse edge devices, analyzed locally for quick-turn actions and in-depth intelligence gained through overlaying cloud analytics. It is this Big Data that delivers insights essential to enhance safety, security and occupant experiences – allowing organizations to essentially move from preventative to predictive operations. In our digital age, the demand for device availability and rapid spread of connectivity requirements is astonishing. In fact, by 2030 it is expected that 20 to 50 billion “things” will be linked via the Internet of Things (IoT).<sup>1</sup>

To promote optimal success, many organizations embrace the connected environment and simultaneously adopt a defense-in-depth approach to the heightened Cybersecurity risks that can be introduced in this environment. According to IDC FutureScape: Worldwide IoT 2018 Predictions, by 2020 the potential Cybersecurity and physical safety concerns associated with IoT devices will pressure CIOs at G2000 companies to increase IoT security spending by up to 25%.<sup>2</sup>

IDC predicts: “The industries that are expected to spend the most on IoT solutions in 2018 are manufacturing (\$189 billion), transportation (\$85 billion), and utilities (\$73 billion). Cross-Industry IoT spending, which represent use cases common to all industries, such as connected vehicles and smart buildings, will be nearly \$92 billion in 2018 and rank among the top areas of spending throughout the five-year forecast.”<sup>3</sup>

1 <http://securitymiddleeast.com/2018/02/23/3800-cyber-attacks-smart-home-daily-cyber-security-solutions-smart-buildings-intersec-forum/>

2 <https://www.idc.com/getdoc.jsp?containerId=US43193617>

3 <https://www.idc.com/getdoc.jsp?containerId=prUS43295217>

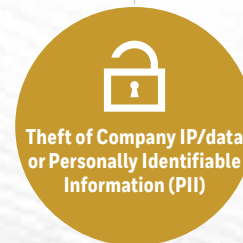
## CYBER-SMART IN THE BUILT ENVIRONMENT

Pervasiveness of technology, ubiquitous connectivity, and the rapidly - evolving uptake of connected technologies will likely continue to impact and influence how smart buildings are operated, which raises the need for protection against cyber risks significantly.

Building a strong Cybersecurity ecosystem requires an understanding of attacker motives and the breadth of common cyber risk scenarios. Attacker motives often shift and change almost as fast as technology evolves, however the top three attacker motives remain constant and include: financial gain, disruption of service and theft of personally identifiable information and company IP/data.

Unfortunately, OT systems can present easy targets. Often, common OT communication protocols are designed without stringent security measures, many corporate environments continue to operate on outdated software and personnel neglect to update default passwords on embedded accounts or personal devices. Successful exploitation of any number of these common security vulnerabilities can be far reaching, including the loss of operations, revenue, shut down of infrastructure and, even more catastrophic, loss of physical well-being.

### TOP THREE ATTACKER MOTIVES



“ In the world of Cybersecurity, if you are standing still you are going backwards. The Cybersecurity environment is constantly evolving, and we need to be adaptive and proactive.”

- Dan Tehan, The Minister Assisting the Prime Minister [Australia] for Cybersecurity (2017)



## UNDERSTANDING YOUR OT CYBER RISKS IN BUILDINGS

Within the smart building environment, common cyber risk scenarios include potential attacks on:

### AVAILABILITY OF CONTROL SYSTEMS

---

- Disabling the integrity of business operations
- Downtime of security, access control, or other critical control systems

### POWER MANAGEMENT FUNCTIONS CAUSING SHUTDOWN

---

- Damaging IT equipment
- Taking business-critical applications offline
- Impacting customer services

### TEMPERATURE SETTINGS ON HVAC SYSTEMS

---

- Disrupting business
- Causing loss of productivity
- Potentially injuring occupants

### INTERNET-CONNECTED PHYSICAL SECURITY SYSTEMS


---

- Accessing sensitive business or employee information
- Compromising customer data
- Locking out staff and customers



We often find that OT systems are outside of the IT department's view or even responsibility. It's important for organizations to ensure that all of their systems (IT or OT) are procured, deployed, maintained and monitored with Cybersecurity in mind. There are often gaps in responsibility between the business function, IT department, and control system vendor which quickly become clear after a cyber incident – which is too late.”

- Brodie Raffaele, Global Director ICT and Cybersecurity,  
Honeywell Building Solutions



While the impact of a successful attack on smart buildings is often felt immediately, the potential financial and reputational damage can stretch far beyond the recovery of services. A Frost and Sullivan Report<sup>1</sup> lists the following potential cost impacts on an organization:

- System repairs and retrofit costs
- Personnel redeployment cost to implement manual checks in place of automated systems
- Cost of record/data/IP loss
- Construction/redevelopment/decommissioning costs
- Legal and other investigation costs
- Mitigation costs
- Costs associated with reputation loss

These cost impacts can be correlated back to the sharp rise in cyber attacks thwarting organizations. According to research presented by Ponemon Institute, successful breaches per company are on the rise with the average global probability of a breach over the next 24 months at over 27%<sup>2</sup>. Notably, recent memorable attacks WannaCry and (Not) Petya Ransomware significantly disrupted small, medium and large global organizations.

Unfortunately, there is no infallible solution to prevent a cyber attacks but there are certain key measures that can be implemented to enhance an organization's resilience to cybercrime.

1 The 2015 (ISC)2 Global Information Security Workforce Study, Frost & Sullivan

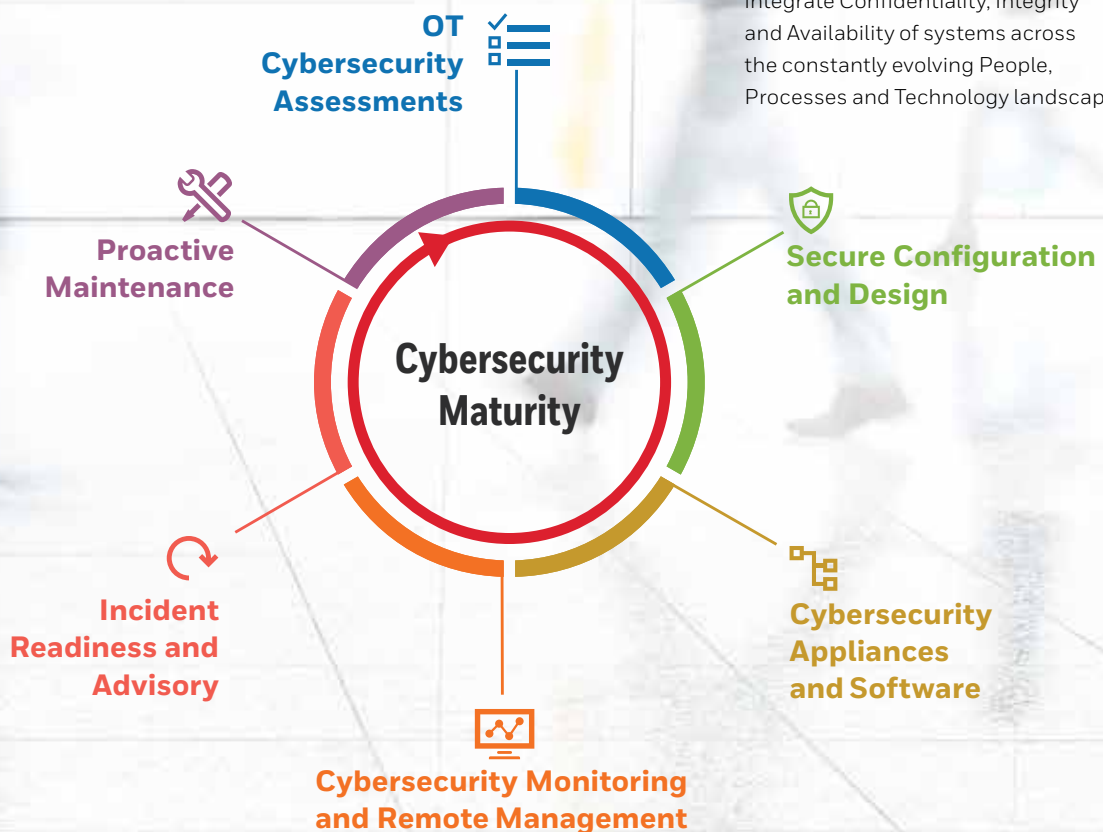
2 <https://www.ibm.com/security/data-breach>

# RESILIENCE IN THE FACE OF CYBERCRIME

Maintaining a more secure and resilient OT and/or converged IT/OT environment requires a wide-ranging strategy that includes personnel awareness training, implementation of robust security governance and process, and investment in the right technology. The strategy also typically requires support from C-level executives and ultimately, association with a trusted solution provider with the capability to leverage industry intelligence and provide the assistance needed to help drive the strategy to completion.

As a leading buildings technology systems integrator and manufacturer of building - related systems, Honeywell brings decades of industry knowledge and expertise to help understand and proactively monitor the complete converged IT/OT infrastructure and assess the health of systems for key Cybersecurity risk indicators. Our focus is on driving heightened awareness around cybersecurity, leveraging a strong understanding of control systems which form part of our DNA.

Without doubt, securing technology is a top priority in cybercrime resilience. On implementation, software needs to be securely configured and kept up to date with the latest patches and product releases. Similarly, the security of applications also frequently depends on the security of the network, secure web connections, intelligent system encryption options and the integrity of disaster recovery procedures. Yet, Cybersecurity is also heavily dependent on the people who use the technology, and the processes and procedures in place to enforce proper use of the technology. Honeywell is well-equipped to integrate Confidentiality, Integrity and Availability of systems across the constantly evolving People, Processes and Technology landscape.



People are often the weakest link in a Cybersecurity strategy. It can be as simple as the improper use of a smart device, downloading malware from an email attachment or not updating password credentials.

Regular Cybersecurity awareness training is essential to keep staff abreast of risks and mitigation measures. Equally important are regular compliance reviews and a whole-of-enterprise process

framework to implement and maintain Cybersecurity maturity. The first step in this lifecycle is to conduct a thorough Cybersecurity vulnerability assessment.

## HONEYWELL'S FOCUS ON CYBERSECURITY

Honeywell is a global software-industrial company that invents and manufactures technologies to address some of the world's most critical challenges around energy, safety, security, productivity, and global urbanization. We are uniquely positioned to blend physical products with software to support connected systems that are aimed at improving homes, buildings, factories, utilities, vehicles and aircraft, and that promote a safer, more comfortable and more productive world. Due to our background working on industrial and critical infrastructure, and our focus on connected technologies, we are also engaged in manufacturing, deploying and maintaining Cybersecurity products and solutions.

## HONEYWELL CYBERSECURITY ASSESSMENTS

A formal threat and risk assessment is the essential 'first step' for determining vulnerabilities in your cyber defense profile, and typically underpins the processes and procedures for holistic risk mitigation. Conducted regularly by trained and experienced staff, Honeywell's Cybersecurity assessments can provide benefits including:



### ASSET INVENTORY

Staff must know what is—and is not—on their OT networks. Security assessments routinely discover undocumented devices, as well as the absence of expected assets.



### NETWORK TRAFFIC BASELINING

OT networks are largely deterministic, so it is possible to identify normal operations traffic and use this 'fingerprint' to identify anomalous activity.



### SECURITY BREACH DETECTION

Many infiltrations of OT networks are discovered only during the in-depth examination conducted during an assessment.



### VULNERABILITY IDENTIFICATION

Security weaknesses of OT and network equipment are discovered by vendors, clients and researchers on an ongoing basis. Assessments are underpinned with the knowledge of current information on vulnerabilities, providing a checklist from which assessors work.



### CONFIRMATION OF REMEDIATION

Each assessment includes a list of challenges to potentially address and is to be used as a baseline for Cybersecurity improvement bringing OT systems into an enhanced level of compliance.

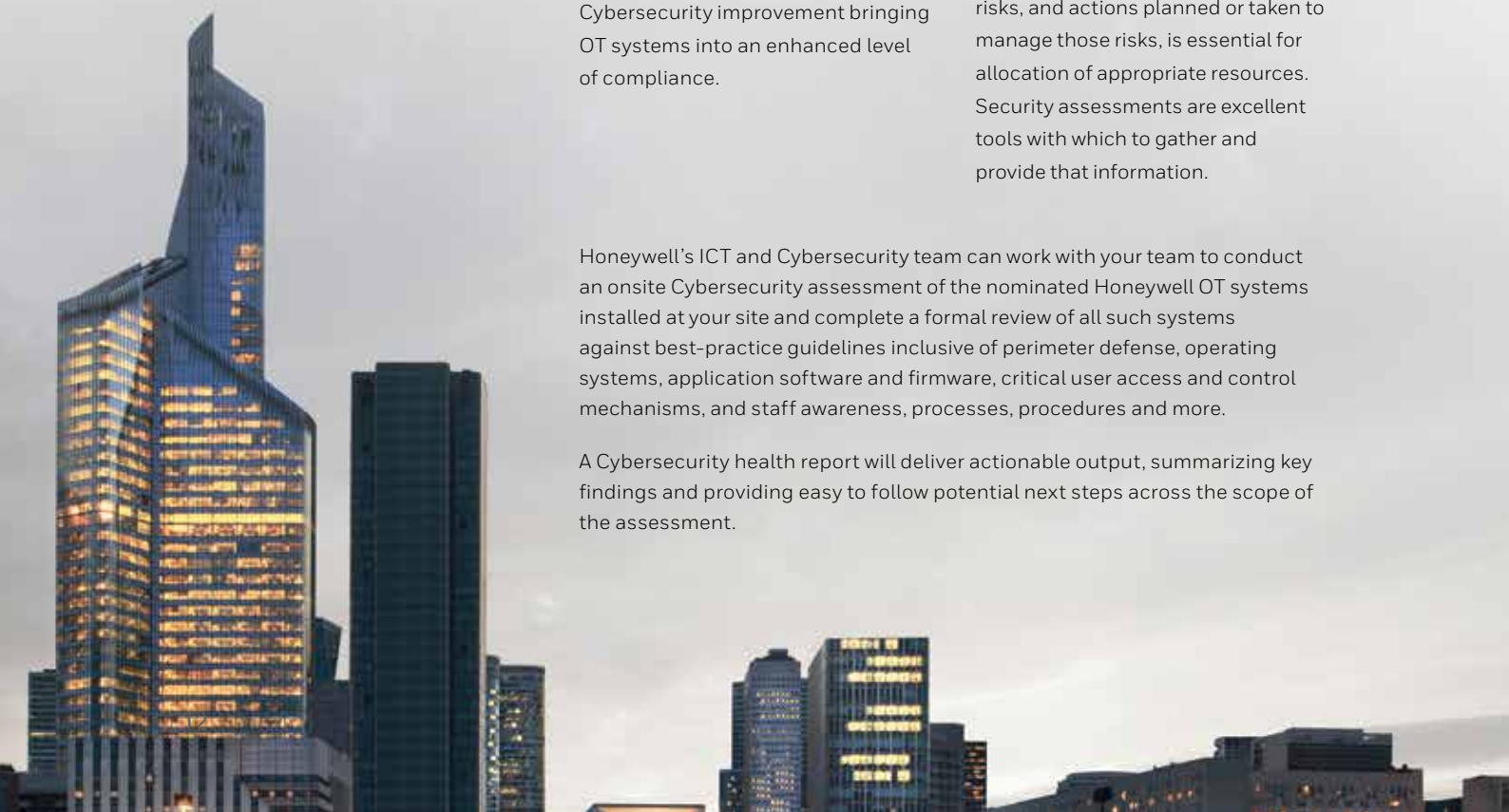


### SECURITY POSTURE INSIGHT

Senior stakeholders need metrics to guide business decisions. Information regarding Cybersecurity risks, and actions planned or taken to manage those risks, is essential for allocation of appropriate resources. Security assessments are excellent tools with which to gather and provide that information.

Honeywell's ICT and Cybersecurity team can work with your team to conduct an onsite Cybersecurity assessment of the nominated Honeywell OT systems installed at your site and complete a formal review of all such systems against best-practice guidelines inclusive of perimeter defense, operating systems, application software and firmware, critical user access and control mechanisms, and staff awareness, processes, procedures and more.

A Cybersecurity health report will deliver actionable output, summarizing key findings and providing easy to follow potential next steps across the scope of the assessment.





## SIMPLE STEPS TO A SAFER OT ENVIRONMENT

In addition to conducting Cybersecurity threat assessments, there are simple steps that organizations can take to enhance the Cybersecurity maturity of their OT systems.

### Maintain currency over infrastructure and applications

Outdated and unsupported software can cost an organization a lot more than an upgrade. Focus on outcome-based software assurance for your core building management systems so that your facility is operating on a current and secure environment at all times without large upfront capital outlay.

### Apply OT application updates and keep current

It's important for not only the operating system to be kept up to date, but also the OT applications themselves. Vendors regularly release new software versions, updates and firmware. These should be included in the regular patch management schedule.

### Install an effective firewall

Firewalls monitor and control incoming and outgoing network traffic based on predetermined security rules. Firewall rules should be robust, maintained and tested.

### Awareness

Educate users to take care when opening emails and attachments as these are common attack vectors. Ensuring building control system servers and workstations are not being used for email or general web browsing, and are logically separated if running on a converged network. Continually inform and educate users on the use of USB media, how to identify scams, malicious links, and social engineering attempts.



### Apply Operating System (OS) updates

Not applying patches will often leave the door open for attack. Cyber attacks readily exploit flaws (vulnerabilities) in a system in order to execute the intended threat. The timeframe between an exploit and when a patch is released is continually getting shorter.

### Ensure you have the latest anti-virus software installed

Anti-virus software is only as good as its latest update. It is a key defense to prevent, detect and remove malicious software.

### Backup your environment at all times

On hand backups remain one of the fastest methods to restoration and continued business operations should your system become infected. Ensure you have copies of the most recent backup stored offline or in a disconnected state to reduce infection susceptibility.

### OT/business & IT collaboration

It's important that the Cybersecurity responsibility of OT systems is clearly defined and understood within an organization. The business teams responsible for deploying and utilizing operational technology should either have a strong ICT & Cybersecurity capability within their department, or collaborate with their internal & external IT teams to support activities outside of their capability.

These are the first steps to decreasing an organization's Cybersecurity threat footprint. Further mitigation techniques may include next generation applications and dedicated Cybersecurity monitoring software solutions.



# HONEYWELL'S APPROACH TO CYBER INTELLIGENCE



At Honeywell we have been living and breathing control systems since the mid-1970s, and our principals for protecting OT environments against unwarranted compromise have been, and continue to be, a core pillar in our deployment framework.”

- Mirel Sehic, Global Director Cybersecurity, Honeywell Building Solutions

Honeywell has been recognized as an industry leader in OT control systems for more than 30 years. Our customers operate some of the world's most complex facilities including international airports, government departments, defense

agencies, large commercial buildings, hospitals and health care precincts, data centers and places of mass gathering.

In keeping with our commitment to our customer base and industry, we

have accelerated our investment in Cybersecurity offerings, people and processes over the last five years to help organizations mitigate exposure to attackers while making smarter decisions to improve safety and productivity in the face of cybercrime.



**ICT and Cybersecurity Center of Excellence**  
Center of Excellence leverages global knowledge locally



**Expertise and Industry Collaboration**  
Powerful knowledge of buildings and OT delivers meaning and ongoing engagement



**Continuous Improvement**  
Holistic approach focused on training, process and technology

## OUR KEY TACTICS INCLUDE



# TAKING ACTION: NEXT STEPS TO A CYBER SMART STRATEGY

Organizations in control of critical infrastructure, smart buildings and the smart cities of our future cannot ignore the cybercrime risks inherent in OT systems, integration of IoT connectivity and the evolving digitization of industrial environments. A primary defense against attackers is to work together to build and deploy intelligent mitigation strategies founded on known vulnerabilities and expert defense-in-depth tools, processes and procedures. Regular Cybersecurity assessments are an essential first step in the journey to a whole-of-enterprise cyber smart strategy.

As an industry leader and trusted solution provider, Honeywell brings expertise to help in deploying a holistic approach to Cybersecurity audits, assist in the implementation of targeted security controls and help to mitigate against financial, operational and reputation damage.

Today Honeywell is actively engaged with government and industry bodies including the US Department of Homeland Securities ICS-CERT, and the Australian Cyber Emergency Response Team (AusCert) to keep abreast of changes in the threat landscape, collaborate on mitigation strategies, and proliferate this intelligence.

Cybersecurity is a continual improvement journey, and climbing up the maturity ladder will often take time. The key is to make a start, and at Honeywell we will help you expedite this journey.



The ACIC has worked with external partners, such as Honeywell, to mitigate high-risk security threats. Honeywell is an important partner in strengthening our ability to make Australia safer.”

- Chris Dawson, CEO,  
Australian Criminal Intelligence Commission



**For more information**

[www.BuildingSolutions.Honeywell.com](http://www.BuildingSolutions.Honeywell.com)

**Honeywell Building Technologies**

1985 Douglas Drive North  
Golden Valley, MN 55422-3992  
Tel: 1-800-345-6770  
[www.Honeywell.com](http://www.Honeywell.com)

Cybersecurity-WP | 09/19  
© 2019 Honeywell International Inc.

**Honeywell**