PROTECTING OPERATIONAL TECHNOLOGY IN FACILITIES FROM CYBER THREATS

Constraints and realities.

Honeywell 2021
Building Trends Series

Honeywell

OVERVIEW

Our increasingly connected buildings have expanded the Operational Technology threat footprint

Close attention to cybersecurity issues is not new. Over the last decade, governments and corporations have invested heavily in information technology (IT) security research, resources, training and defensive initiatives directed at predicting and mitigating the risk of cyber threats.

This typically benefits corporate IT systems, focusing on protecting personal information, proprietary company software or data. However, operational technology (OT) systems are often overlooked. OT systems monitor, control and protect processes, equipment and operational environments. In buildings this means assets like HVAC, building management and security systems. From an IT department's perspective, OT systems have been out of sight and thus haven't always had the same level of monitoring or maintenance hygiene.

In the past, it was common practice to "air-gap" control system networks — in other words, disconnect them both directly and indirectly from the Internet — as they typically didn't need to interact with Internet-based services (such as those enabled by the Cloud) or other corporate networks. This was widely considered sufficient as an OT security measure, but this is no longer operationally feasible in today's connected world. Smart devices are proliferating rapidly throughout connected buildings as an enterprise-wide view of building control systems and sensors is essential to drive productivity, operational efficiency and improved response time to events, while ensuring a sustainable building ecosystem.

"This evolution will likely continue as more control systems such as HVAC, energy metering, power management, lighting and fire protection and alarms converge in a connected environment," said Mirel Sehic, global cybersecurity director, Honeywell Building Technologies.

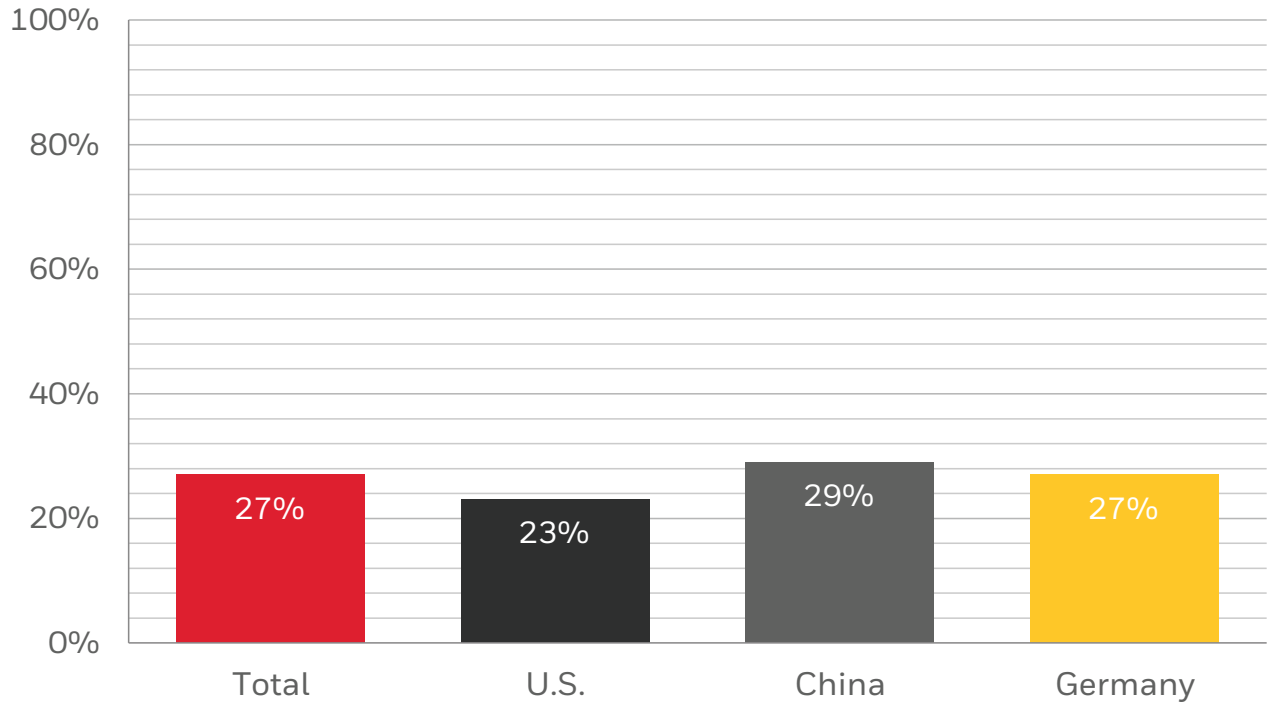
"The impact of cyber incidents can go beyond mere financial loss; operational and reputational damage can be equally devastating if not more so. By understanding the cybersecurity risks surrounding building OT systems, facility managers and IT personnel alike can better position themselves to make smart buying decisions, implement targeted OT security controls and maintain heightened cyber resilience across OT environments."

SURVEY REVEALS OT CYBER AWARENESS & PAIN POINTS

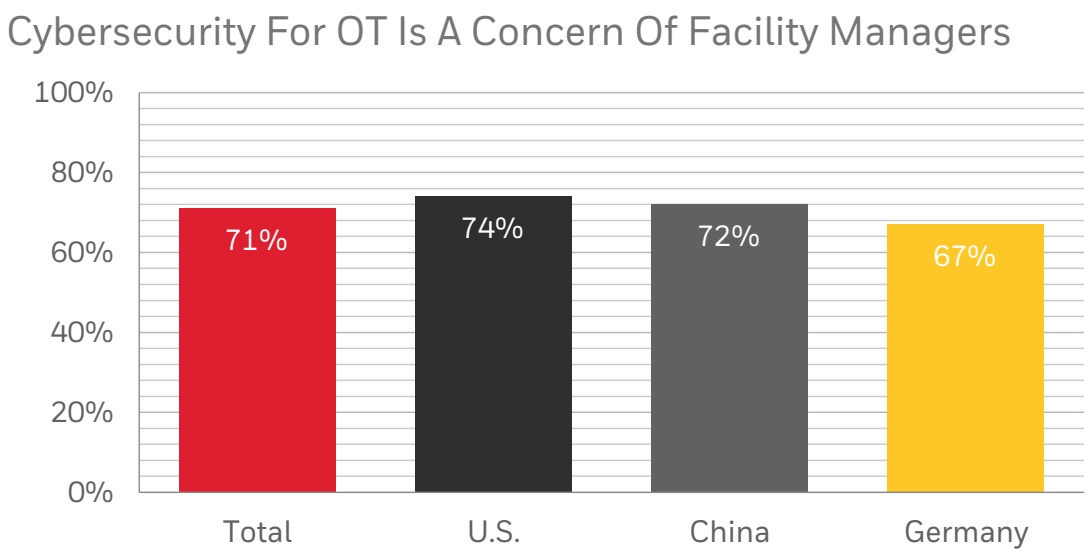
A recent survey conducted by Honeywell Building Technologies sheds light on the OT cybersecurity challenges, concerns and priorities of surveyed facility managers in the United States, Germany and China across four sectors — education, healthcare, data centers and commercial real estate.

The survey results from all countries and sectors found that more than 1 in 4 (27%) respondents have experienced a cyber breach of their OT systems in the last 12 months. Notably, 33% of surveyed education facility managers reported such an incident — eight percentage points higher than respondents in the data center sector, who reported the next highest incidence (26%).

My Facility Has Experienced A Cybersecurity Breach During Past 12 Months



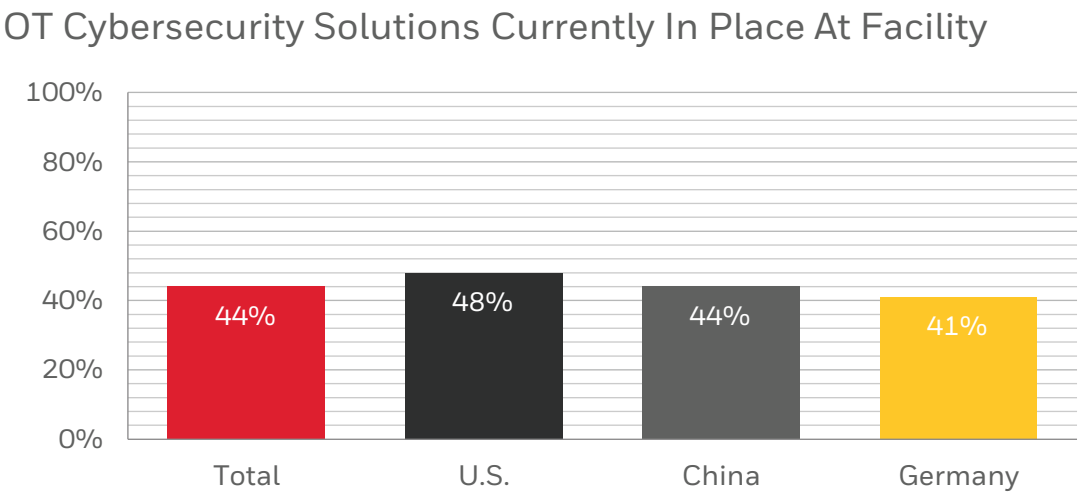
SURVEY REVEALS OT CYBER AWARENESS & PAIN POINTS



More than 7 in 10 (71%) of surveyed facility managers consider OT cybersecurity either a "concern" or "worry." Those working in data centers expressed the highest level of concern, with 74% responding cybersecurity for OT is a concern.

Among the three countries, 74% of surveyed U.S. facility managers say that cybersecurity for OT is a concern – more so, in fact, than for Chinese or German respondents.

Notably, only 44% of respondents across all sectors currently have a cybersecurity system in place to protect their OT systems from potential threats.



Data center respondents predictably lead the sectors, with 51% having a solution, while healthcare facilities trail the other sectors with a surprisingly low 39%. U.S. facilities lead the countries, with 48% of respondents report having an OT cyber solution.

SURVEY REVEALS OT CYBER AWARENESS & PAIN POINTS

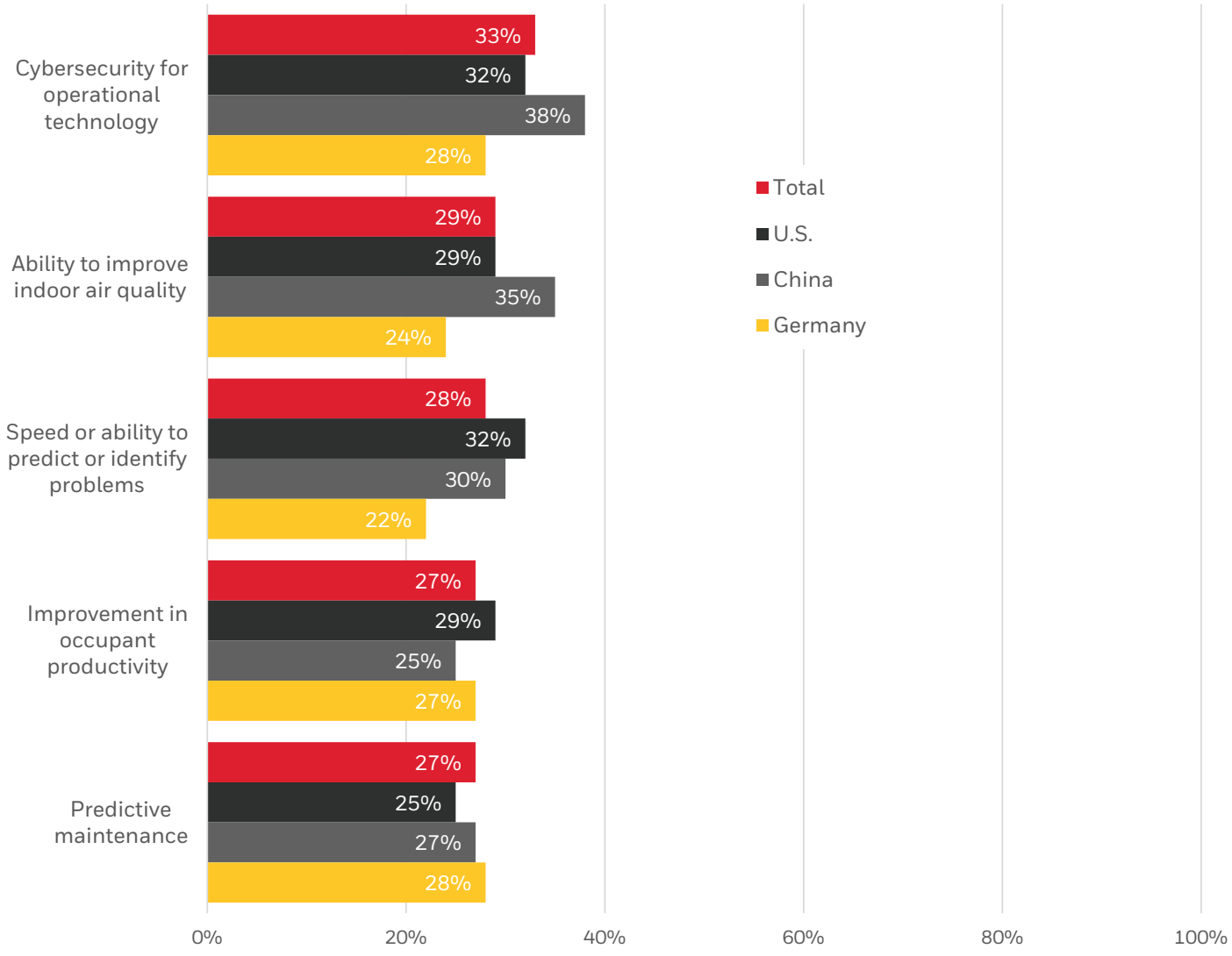
Top Difficulties for Facility Managers

	Total	United States	China	Germany
1	Managing OT cybersecurity **31%**	Managing OT cybersecurity **32%**	Implementing upgrades or new solutions **33%**	Managing OT cybersecurity **33%**
2	Keeping pace with technological change **31%**	Managing the facility remotely **32%**	Meeting evolving occupant demands **32%**	Budgeting for upgrades or new solutions **32%**
3	Implementing upgrades or new solutions **30%**	Keeping pace with technological change **30%**	Keeping pace with technological change **31%**	Keeping pace with technological change **31%**
4	Managing the facility remotely **30%**	Creating a healthier, safer environment for occupants **29%**	Managing OT cybersecurity **30%**	Minimizing downtime or disruption **30%**
5	Budgeting for upgrades or new solutions **30%**	Minimizing downtime or disruption **29%**	Managing the facility remotely **32%**	Implementing upgrades or new solutions **33%**

SURVEY REVEALS OT CYBER AWARENESS & PAIN POINTS

As for which building upgrade surveyed facility managers believe would provide the greatest benefit to occupants and other stakeholders, more respondents (33%) cited OT cybersecurity than any other improvement. Surveyed facility managers in China had the highest response for the benefits of OT cybersecurity with 38%.

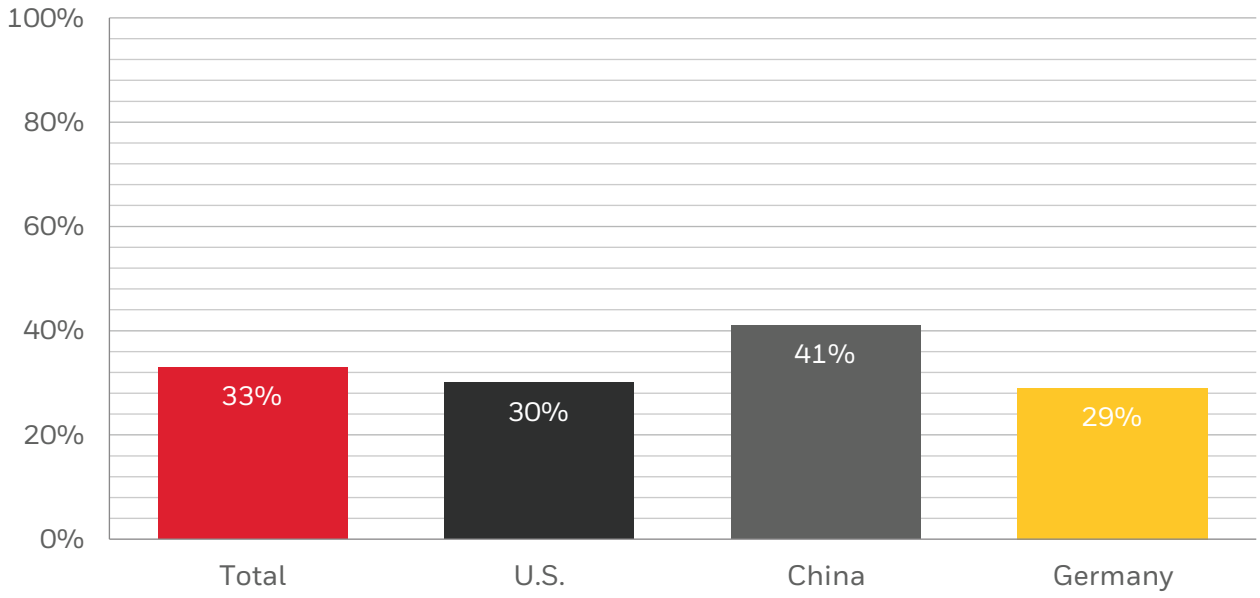
Upgrades That Would Provide The Greatest Benefit For Occupants and Stakeholders



SURVEY REVEALS OT CYBER AWARENESS & PAIN POINTS

Aligning with this response, 41% of Chinese respondents said they're most likely of all countries to invest in an OT cybersecurity solution over the next 12 to 18 months — eight percentage points higher than the 33% average for all three countries.

OT Cybersecurity Solutions Investment Over Next 12-18 Month



OT CYBERSECURITY: A LOOK FORWARD

Organizations leading digital transformation are developing enterprise-wide cybersecurity solutions that drive greater consistency and protection across operational technology environments.

Installing technology to integrate all building management systems into a single platform would aggregate data from across disparate systems into a single source allowing facility managers to better develop insights, make informed decisions, potentially reduce costs and improve their cybersecurity management efficiency.

"Conversations about cybersecurity often focus on IT and safeguarding data and assets, but OT cybersecurity is just as critical when you think of the potential effects," said Sehic.

"Imagine a ransomware attack on a hospital's OT system where staff are locked out of their computers. A building's OT environment should be monitored and maintained just like an IT system and should not be overlooked."

As OT and IT systems continue to converge, it's more essential than ever for organizations to assess potential cyber risk across their OT environments and take action to enhance their security posture. The threat landscape continues to evolve at dizzying speed, and facility managers can provide critical insider's input in developing and implementing a vigilant cybersecurity strategy to protect vital OT systems.

METHODOLOGY

The Honeywell survey was conducted online by KRC Research (http://www.krcresearch.com/) among facility managers in three markets: United States, Germany and China.

Honeywell Building Technologies
715 Peachtree St. NE
Atlanta, Georgia 30308
honeywell.com

THE FUTURE IS WHAT WE MAKE IT

Honeywell