Newsweek VANTAGE

WEATHERING THE PERFECT STORM

SECURING THE CYBER-PHYSICAL SYSTEMS OF CRITICAL INFRASTRUCTURE

Sponsored by:

NOZOMI NETWORKS

SIEMENS Ingenuity for life

yubico

In association with:

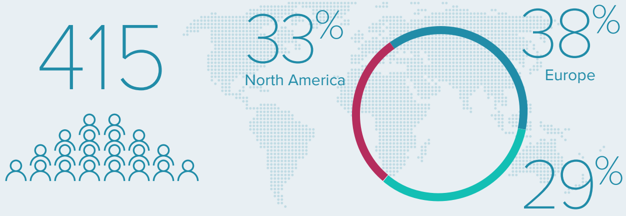
ISA

CONTENTS

EXECUTIVE SUMMARY

1 Purpose of the survey

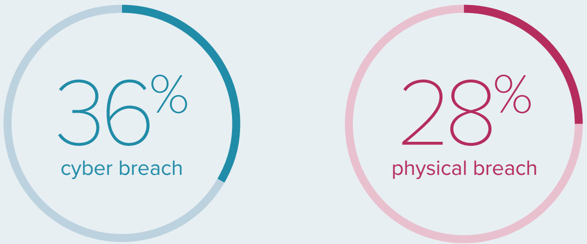
The survey tested the proposition that when it comes to security, critical infrastructure organizations have not focused enough on taking a holistic approach to the digital and physical realms. The survey of **415** executives worldwide shows that many are, in fact, focusing on it, but it is hard to balance security and operational performance.



Source: Newsweek Vantage

2 Motivator for a holistic security strategy

More than a third say that an actual cyber breach has caused them to develop a holistic approach to their organization's cyber/physical security. More than a quarter say the same of a physical breach.



Source: Newsweek Vantage

3 Cyber-physical threats are real

Almost all the executives say their organization has suffered at least one security incident in the past 12 months and half has experienced two or more.

The numbers show clearly the need for a cyber-physical security strategy. For the largest proportion, the threat was a cyber incursion into IT systems. More than a third says it was a physical incursion into IT systems and almost as many say it was a physical incursion into OT systems.

For nearly two thirds, the source of vulnerability was insecure IT systems, a third said it was a lack of IT/OT integration, and more than a quarter pointed to a lack of secure physical access controls.

53% cyber incursion

37% physical incursion IT

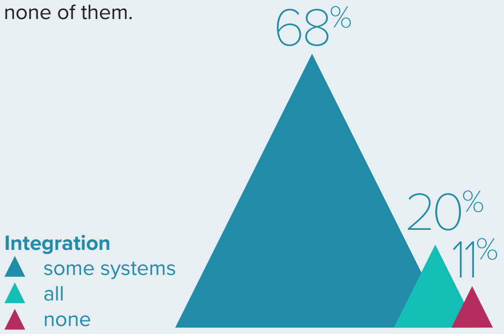
32% physical incursion OT

Source: Newsweek Vantage

Actors: Almost three in five say the biggest threat comes from current and former employees (both intentional or inadvertent). Half says cyber-criminals are the biggest threat, while one in eight point to a threat from terrorists and state-sponsored actors.

4 Level of integration in cyber-physical security

In response to these threats, **two thirds** have integrated some of their IT, OT and physical systems, and the process is continuing. A **fifth** have integrated all their systems. A **tenth** have integrated none of them.



Source: Newsweek Vantage

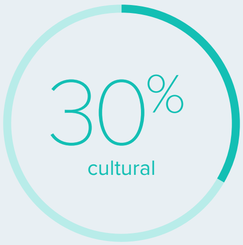
Why are so many taking a holistic approach? Operational performance seems to outweigh security as a driver. Executives see the main advantages of integration to be more responsiveness and better decision-making. The fewest say integration was motivated by the need for stronger security. But experts say a holistic approach to cyber-physical security should precede steps to improve operational performance.

5 Obstacles to integration

OT and IT do not work well together, despite many years of discussion. The survey shows that the main internal obstacles, both organizational and technical, to a holistic approach are big differences between IT and OT in such areas as risk tolerances and operating environments.

Nearly **a third** says the chief obstacle is cultural – i.e., resistance to change. If there was less resistance, IT and OT personnel would have settled their differences by now.

The main external obstacle to a holistic approach is that industry standards for security systems are not used widely enough, even though they are available.



Source: Newsweek Vantage

6 Overcoming obstacles

Since the source of friction is largely an issue involving people and their attitudes to work and their colleagues, it is logical that executives say the way to solve this is a more harmonious approach to cyber-physical security systems among the people working in critical infrastructure. Nearly half the executives surveyed say that the best way to implement a holistic approach to cyber-physical security is a detailed action plan of integration supported by IT/OT/physical security teams. To change the culture, they say that security teams must include IT/OT/physical security personnel.

This piece of common sense is, sadly, not common in critical infrastructure. The report ends by outlining some of the ways organizations can create a culture that supports, even champions, cyber-physical security.

1. THE PERFECT STORM

On March 16th, 2020 the US Department of Health and Human Services confirmed it was hit by a cyberattack a day earlier, after it "became aware of a significant increase in activity in HHS cyber infrastructure."[1] Bloomberg was the first to report the attack, citing anonymous sources that the hacking involved "multiple incidents" and appeared to be part of a campaign of disruption and disinformation intended to undermine the response to the coronavirus pandemic.[2] The attack may have been linked to a text message-based disinformation campaign that falsely suggested there would be a nationwide quarantine in the US.

Cyber security experts have warned that hospitals and healthcare groups could be targeted by nation states or cyber criminals at a time when they are overwhelmed by the COVID-19 outbreak around the world. The result of such attacks would be little less than a "perfect storm", in which disinformation fuels public unease while slowing the response of health authorities to the rapidly spreading coronavirus.

Cyber-physical systems are engineered systems that orchestrate sensing, computation, control, networking and analytics to interact with the physical world (including humans) and enable safe, real-time, secure, reliable, resilient and adaptable performance.

Such a scenario might have seemed far-fetched even a few months ago, but the number and severity of cyber incidents are growing rapidly as the world becomes increasingly connected. As the information technology (IT) and operational technology (OT) domains converge, critical infrastructure organizations are exposed to new cyber threats just like any other industry. A study in 2019 by Siemens and the Ponemon Institute found that 56% of more than 1,700 respondents in global utility industries reported at least one shutdown or operational data loss per year[3] due to a cyber event. And the risk of such an incident grows in proportion to the number of Internet-connected devices—a number projected to hit 42 billion globally by 2025.[4]

Cyberattacks on critical infrastructure are not a new threat. The earliest can be traced back to the late 1990s. Since that time they have increased rapidly in number and complexity, adversely affecting pipelines, power grids, telecommunication networks, ports, dams, banks, healthcare systems and more. Such sectors are in the path of a potentially catastrophic storm. Worse, while substantial resources are generally channeled to mitigate a wide range of physical and operational risks to infrastructure assets, far less attention is paid to potential cybersecurity incidents.[5]

Newsweek Vantage, in association with Siemens, Nozomi Networks and Yubico, and with guidance from the International Society of Automation, has conducted a global survey of more than 400 executives to determine whether critical infrastructure organizations have focused enough on the interdependence of the digital and physical dimensions of cyber-physical systems. If critical infrastructure organizations are to prevent a catastrophic event, they must evolve a comprehensive understanding of the ever-developing risks facing cyber-physical systems. Further, they must implement a cybersecurity strategy that integrates the management of all the relevant cyber/digital and physical layers of protection.

> *If critical infrastructure organizations are to prevent a catastrophic event, they must evolve a comprehensive understanding of the ever-developing risks facing cyber-physical systems.*

2. THE MAIN FINDINGS

Based on an analysis of the survey results and interviews with subject-matter experts, the report finds the following key points:

- The design of a secure cyber-physical system depends on a clear threat analysis. The biggest sources of vulnerability are current and former employees, more so, even, than cyber-criminals. Terrorists and state-sponsored actors are considered less of a threat, even though much of the publicity around cyberattacks against critical infrastructure has focused on these areas. That being said, a terrorist or state-sponsored incident has the potential to be far more damaging than one caused by criminals or employees.
- A comprehensive approach to security is required to protect critical infrastructure against cyber threats from within and without. Almost nine in 10 respondents have integrated some or all of their IT, OT and physical systems, but this does not mean they are doing so to enhance security; only a few said this was the purpose. Instead, most aim to take advantage of the greater responsiveness and enhanced operational control that comes from a holistic approach. A possible cause for concern: a quarter of those that have integrated at least some physical-OT systems with networks seem to think their existing security systems are adequate. Improved security is not an alternative to "greater responsiveness and operational control," but rather a prerequisite. Pursuit of the business needs without considering security beforehand increases the risk of potentially serious consequences.
- The implementation of a holistic approach to securing cyber-physical systems faces both internal and external obstacles. The internal hurdles are largely the result of differing perspectives among IT and OT professionals; it was rated as the top technical and organizational obstacle. Externally, security standards for cyber-physical systems are available but not widely used. Unfortunately, there is no imperative to implement them, nor effective guidance on how to do so.
- To overcome these difficulties, critical infrastructure organizations need firm leadership to ensure IT and OT are fully aligned. They must build teams that include the skills of IT, OT and physical security management to design resilient cyber-physical systems. This often entails creating a new culture where cybersecurity is regarded as everybody's responsibility, not just that of IT professionals. If all employees in the organization are held accountable for their knowledge of cyber-physical security and behavior, this would be quantifiable and would likely generate significant results.

3. A MORE COMPREHENSIVE VIEW

Before analyzing the main findings in more detail, it is worth describing briefly how research on the topic has evolved. Discussion of IT/OT convergence emerged in the 1990s when it first began to become practical to connect production control systems to other parts of the enterprise to optimize operations. After the attacks on the World Trade Center in 2001, organizations paid more attention to security, but by that time, systems were already being connected. In 2011, the research and consulting firm Gartner urged IT leaders to prepare for a transition toward "converging, aligning and integrating of IT and OT environments."[6] This became more urgent with the proliferation of components and equipment connected to the Internet, while control systems are now almost all online.

A 2014 survey published by Siemens was among the first to apply the convergence concept to the utilities industry.[7] Several other papers have gone further to focus on the new risks that are created by connections between IT and OT systems, exposing previously isolated operational systems to cyber threats.

More recently, security professionals and planners have turned their attention to the relationship between IT/OT systems and the physical realm. In 2019, the Australian Strategic Policy Institute published a report[8] which identifies "cyber-physical convergence" as an emerging security issue:

> *While this brings many benefits, it also brings new types of risks to be managed—a cyberattack on OT systems can have consequences in the physical world and, in the context of a critical national infrastructure provider, those physical consequences can have a potentially major impact on society. Insecure OT systems can also be a back door to allow attackers to penetrate IT systems that were otherwise thought to be well secured.*

The study found that 80% of respondents working at 12 major Australian infrastructure organizations had shared their experiences and best practices between the IT and OT functions. But many felt there remained substantial room for improvement. Fully half the respondents emphasized the need to enhance their understanding of both the degree of convergence in their systems, and to ensure that theirs was a comprehensive view of risks and associated vulnerabilities.

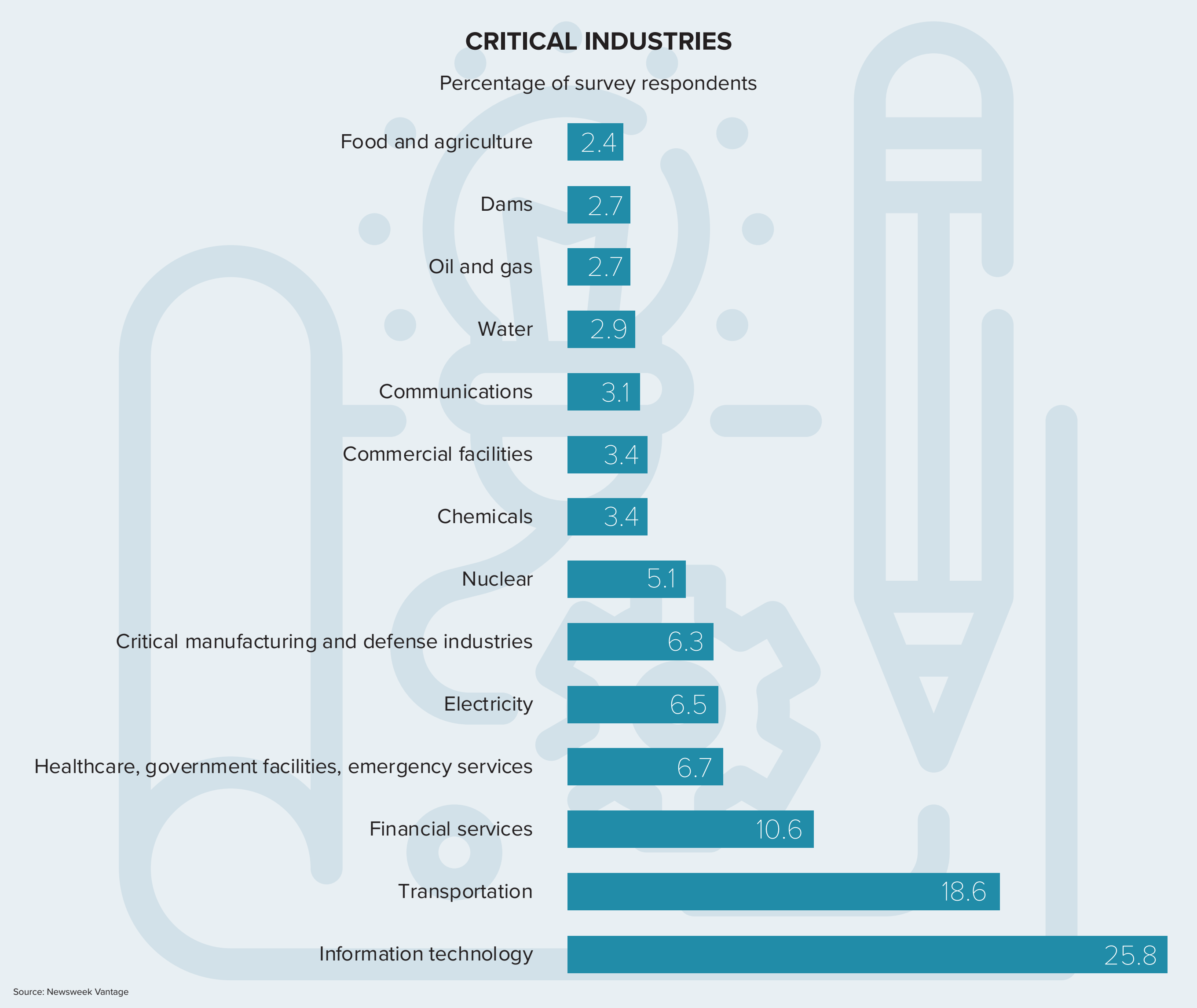
Such concerns have led researchers to broaden the discussion to encompass "cyber-physical systems". One working definition of CPS is as follows: "Engineered systems that orchestrate sensing, computation, control, networking and analytics to interact with the physical world (including humans) and enable safe, real-time, secure, reliable, resilient and adaptable performance."[9]

The published reports on cyber-physical systems are generally aimed at technical audiences and are not survey-based. By contrast, *Weathering the perfect storm* broadens the topic to cover critical infrastructure around the world, collecting empirical evidence based on interviews with subject-matter experts and an online survey of 415 executives from 16 industries defined by the US Department of Homeland Security as critical infrastructure sectors.[10] To ensure a comprehensive view of cyber-physical systems, the survey draws responses not only from the IT, cybersecurity, and operations functions, but also engineering and physical security as well.

Respondents from Europe comprised 38% of executives, North America comprised 33% and Asia-Pacific 29%. Variations in responses among the three regions were not significant.

4. THE THREAT FROM WITHIN AND WITHOUT

The best place to begin the analysis of the findings is to examine the threats perceived by critical infrastructure executives. The risk of cyberattack is a function of the source of the threat, the level of vulnerability and the potential consequences. Critical infrastructure faces similar threats and vulnerabilities as the rest of the economy—what sets it apart is the severity of the consequences. In the US, the Department of Homeland Security includes 16 sectors, "whose assets, systems, and networks, whether physical or virtual, are considered so vital... that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety."[11] As well as the more obvious industries such as electric utilities and transportation systems, the list includes national monuments, where an attack might cause a large loss of life or damage the nation's morale.[12]



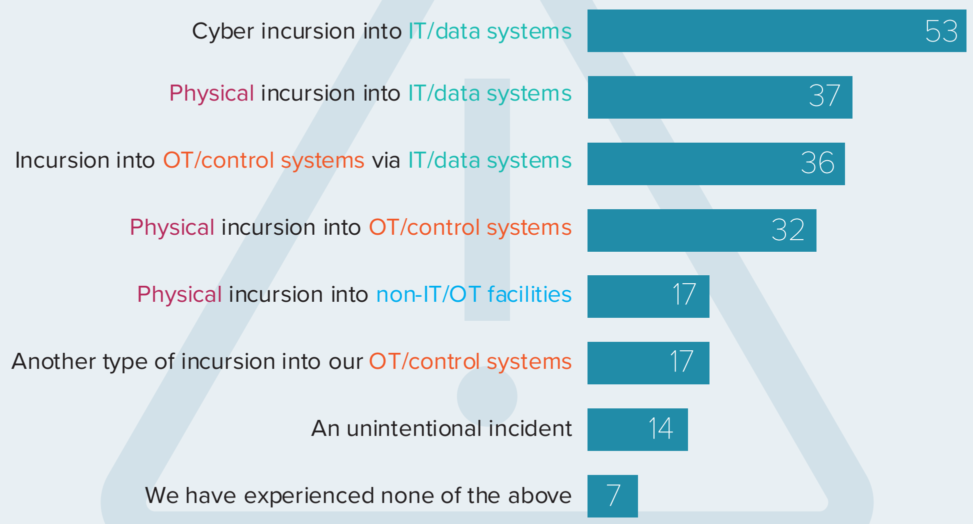
Source: Newsweek Vantage

One advantage of an anonymous survey, such as this, is that respondents are generally more forthcoming about the threats their organizations have faced. The results are a useful, and somewhat chilling, reality check, showing clearly both a need for effective cyber-physical security for critical infrastructure and where the gravest threats are coming from. Nearly nine in 10 executives say their organization has experienced a security incident in the previous 12 months and more than half have suffered two or more.

VECTORS OF ATTACK

Which of the following types of security incident has your organization experienced over past 12 months? Select all that apply

Percentage of survey respondents



Source: Newsweek Vantage

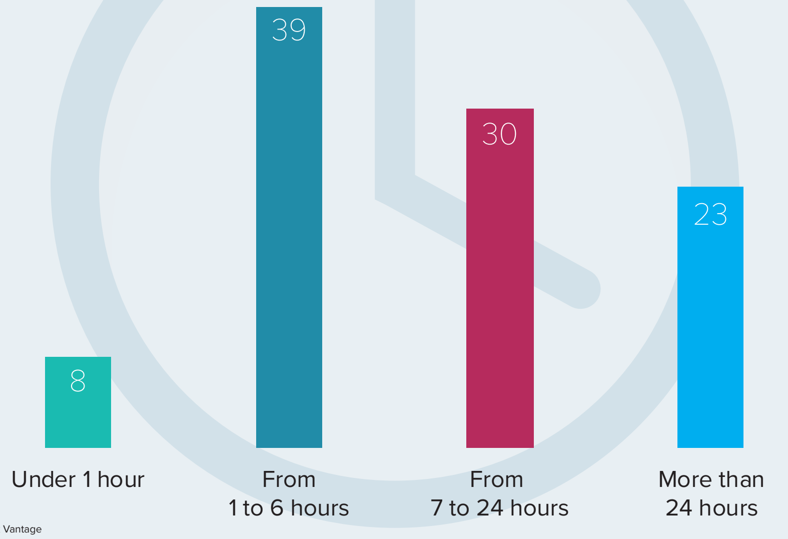
Some 53% of these incidents were cyber incursions into IT/data systems. But there were also plenty of physical incursions into both IT and OT systems, underlining the need for an approach that manages both the digital and kinetic worlds. Strikingly, there were double the number of physical incursions into IT and OT systems as in non-IT/OT systems.

Detection and response time is another major potential pain point. Respondents were asked to focus on the most serious incident of the previous 12 months: how much time had elapsed between the moment of compromise and discovery? Nearly a quarter said the time until detection exceeded 24 hours, a worryingly high number.

ELEMENT OF SURPRISE

Regarding the most serious incident, how much time elapsed between the moment of compromise and discovery?

Percentage of survey respondents



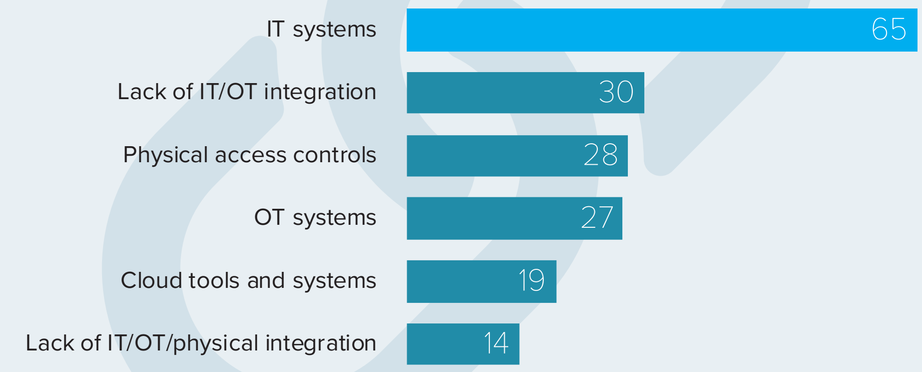
Source: Newsweek Vantage

Given the high frequency of incursions into IT systems, it is not surprising that IT systems are seen as by far the greatest organizational vulnerability—cited by almost two in three executives, more than twice as frequently as other areas. Many executives also point to a lack of IT/OT integration as a potential weak point. It appears that, for many organizations, greater IT/OT integration poses a conundrum: it may well help to reduce the risk of penetration of any given system while actually increasing overall vulnerability.

THE WEAKEST LINKS

Regarding the most serious incident in the past 12 months, please select the options below that most closely describe the source of the vulnerability. Select all that apply.

Percentage of survey respondents



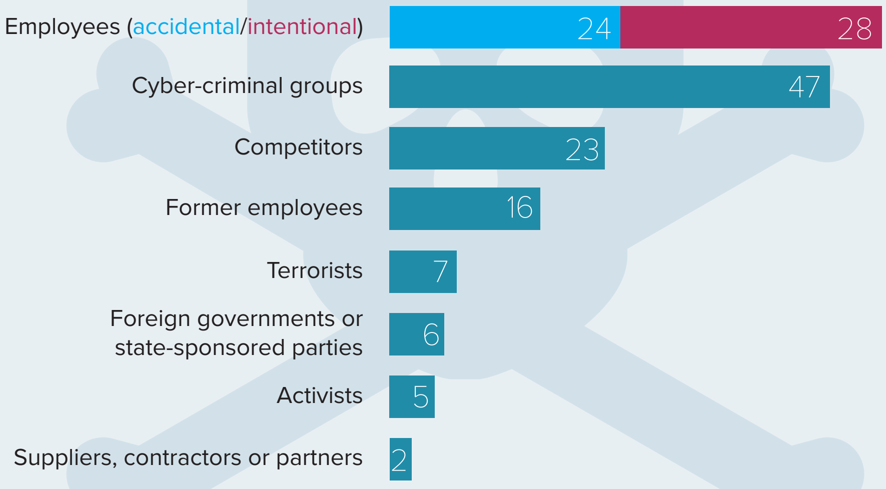
Source: Newsweek Vantage

Having considered which systems were most vulnerable, executives were asked which threat actors pose the greatest threat to critical infrastructure organizations' operational security. Nearly half (47%) say cyber-criminals pose the biggest risk. But more see former and current employees as an even greater threat. Taken together, current and former employees are regarded as the greatest risk overall (executives could choose up to two options).

ERRANT INSIDERS

Which of the following actors do your consider the biggest threat to your organization's operational security? Select up to two.

Percentage of survey respondents



Source: Newsweek Vantage

"Most organizations focus on the technical aspects of building a digital perimeter around a facility, but the incident that worries me most is the disgruntled employee or somebody who can get inside, because even if the system is completely isolated, an insider can enter the network," says Steven Mustard, a subject-matter expert at the International Society of Automation and author of *Mission Critical Operations Primer*. "Cybersecurity technology is important, but actually, the people, the process and the awareness are the things organizations need to work on."

Cyber-physical systems are vulnerable to compromise by employees on a number of levels, credentials being the most notable. Rich Armour, a senior advisor for Nozomi Networks and former Chief Information Security Officer at General Motors, says the key to securing assets against current or former employees is "the really rigorous management of credentials. If Joe used to work in robotics, make sure his credentials are removed from all those systems as soon as Joe is transferred or terminated, all accounts are locked and any access to sensitive equipment is blocked, enterprise-wide." Armour adds: "There must be no unauthorized sharing of credentials. This would create an unauthorized access path for an individual who might leave the company but still have working credentials."

Despite the finding that terrorists and state-sponsored actors are considerably less of a threat than criminals or employees, the spectacular nature of some reportedly state-sponsored cyberattacks on critical infrastructure lead to an outsized sense of threat in the public consciousness. These include the Stuxnet[13], a malicious computer worm that targeted SCADA systems and is thought to have been responsible for causing substantial damage to Iran's nuclear program before its discovery in 2010. Another is a cyberattack on Ukraine's power grid[14] in 2015, during which hackers compromised three energy distribution companies and disrupted electricity supply to consumers. The former was reported to have been developed by the US and Israel, the latter by Russia.

"State actors do not tend to attack broadly but have more specific objectives to steal from, or destroy, a specific target," says Daniel Henriksen, Head of Legal & Security Management at Intility, a managed service provider, which provides a complete platform service for multi-cloud IT environments. "Criminals will focus on getting money from wherever they can and destroy things in their wake."

The simplest way for an organization to avoid being targeted by criminals, says Henriksen, is to raise the overall cybersecurity level higher than its neighbors: "If a hacker knocks on the door and sees it is secure, they move on." Having examined the threats posed from inside and outside the organization, the analysis looks at how these enterprises are responding to them and whether they are integrating their cyber-physical security to mitigate the risk of attack.

> *"Most organizations focus on the technical aspects of building a digital perimeter around a facility, but the incident that worries me most is the disgruntled employee or somebody who can get inside, because even if the system is completely isolated, an insider can enter the network"*
>
> — Steven Mustard,
> International Society of Automation

5. THE BENEFITS AND PITFALLS OF INTEGRATION

The state of integration between cyber/digital and physical systems varies widely in critical infrastructure. For many, the level of integration will largely depend on the individual circumstances facing the organization. Some believe they stand to lose far more in terms of heightened vulnerability to cyberattack than they might gain from operational efficiencies (such as South Staffordshire plc—see section 6). Others believe they will see far more benefits than costs and have made full systems integration a top priority. "The main challenge is very often to achieve a balance between the need for functionality and for security," says Daniel Henriksen.

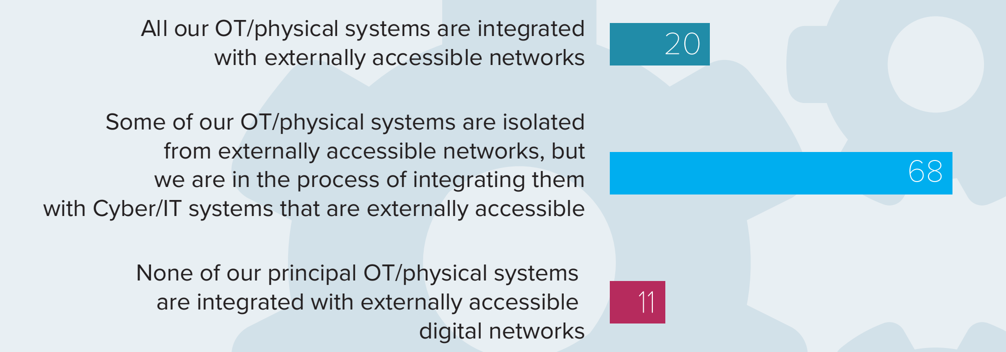
The survey shows where executives draw the line. Only one in five executives say that all their systems are fully integrated with externally accessible systems. "This low figure stems from fact that, for many, there is no drive to integrate for the sake of it," says Hannes Barth, General Manager of Siemens Ruggedcom, part of Digital Industries. "It occurs as a byproduct of initiatives to boost performance or drive real-time transparency that lead to IT/OT integration through data exchange."

At the opposite end of the spectrum of integration, a mere one in 10 executives say that none of their systems are integrated. The large majority are in the middle: More than two-thirds say that some of their OT/physical systems are isolated from IT, but the integration process continues. Among critical infrastructure sectors, executives in transportation are most likely to have integrated fully (29%), while the energy sector is least likely to have done so (14%). Integration sometimes occurs in an unplanned fashion, as a result of using common networking technology, and this may lead to unanticipated consequences.

FEW FULLY INTEGRATED

Which of the following statements best describes the state of integration between your organization's cyber systems and OT/physical systems?

Percentage of survey respondents



Source: Newsweek Vantage

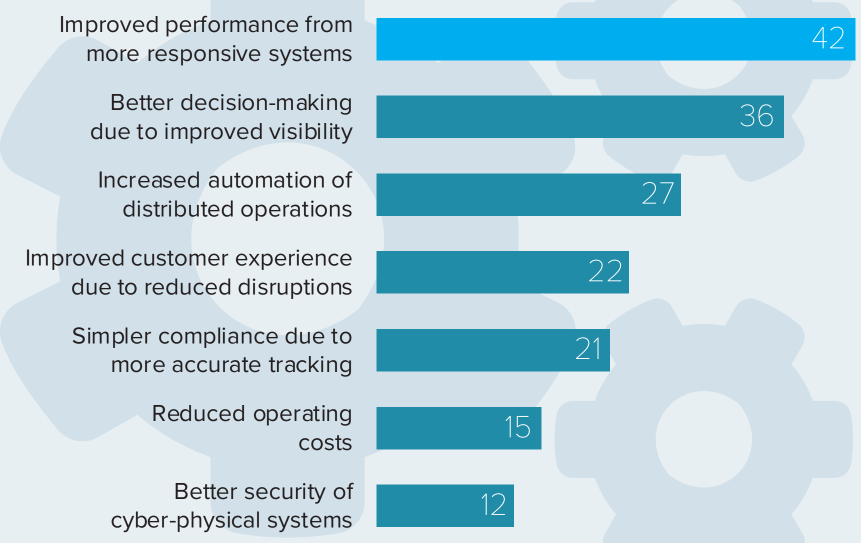
One reason for the wide variation among industries, says Eric Cosman, president of the International Society of Automation, is because some organizations 'make to stock' and others 'make to order'. As an example of making to stock, a bulk chemical facility can store its output in tanks—it doesn't have to communicate every hour with the business offices, because it knows what to make and when. An automotive manufacturer, by contrast, makes to order, delivering cars and components 'just in time'. The manufacturer's OT systems have to be tightly integrated on an hourly basis with both the business and its supply chain. The demand for integration between cyber/digital and physical systems, therefore, is likely to be higher for the manufacturer than for the chemical facility.

Even so, there are limits to how much industries differ in terms of their level of integration. "It has become increasingly difficult to avoid the integration of technology for computing and communications, since virtually all OT systems now use the same commercial, off-the-shelf products as those used for office and business systems," says Cosman. Some industry analysts beg to differ. Siemens's Barth says his and "many other companies" have created customized cybersecurity solutions that avoid this issue.

DRIVERS OF INTEGRATION

Which of the following benefits have been most important in driving the convergence of cyber and OT/physical systems? Select up to two

Percentage of survey respondents who have partially or fully integrated systems



Source: Newsweek Vantage

The 88% of respondents whose organizations have integrated some or all of their systems say they have seen substantial benefits as a result. Higher responsiveness leading to improved performance is the most common benefit—crucial for quickly detecting a security breach. Other enhancements include tighter operational control, as well as the improved decision-making capabilities that come with increased visibility, greater automation and improved customer experience. The least frequently cited benefit is greater security, which is hardly surprising given the greater exposure that comes with higher connectivity.

“Organizations know the cybersecurity risk will increase with integration and it will only be done if it drives productivity improvements. Our customers accept these risks only because there are big benefits from integration when they deploy, for example, artificial intelligence and predictive maintenance technologies,” says Barth.

But executives are not necessarily thinking about the cybersecurity effects when they plan for integration, according to Steven Mustard. “The Internet of things, for example, enables the business to be more productive but it also creates more vulnerability. Executives think they can worry about cybersecurity afterward, but, by then, it’s too late because the vulnerability is baked in.” Most of the work of systems integration is performed on brownfield sites, where organizations must make do with legacy systems. “You can’t rip them out, so you have to work around them,” he says.

Newer sites are not necessarily more secure, however. Mustard is the cybersecurity advisor to a large, new offshore oilfield being developed in the Gulf of Mexico. “You’d think it would be more secure than a brownfield site,” says Mustard. “But it takes years for standards to be embedded in solutions, and the options chosen at the start of the project may not reflect the current standards.”

Despite the greater vulnerabilities faced by their most critical systems, almost one-quarter of executives from partially or fully integrated organizations say their existing security systems are adequate. A more appropriate response to this integration would likely be to strengthen security systems. More reassuringly, however, 70% of respondents whose organizations are integrating digital, OT and physical systems are either addressing the most pressing vulnerabilities or adopting a holistic approach.

Despite the greater vulnerabilities faced by their most critical systems, almost a quarter of executives from partially or fully integrated organizations say their existing security systems are adequate.

The implications of these findings are clear. "Asset owners must understand and accept the fact that electronic or information-based systems are capable of affecting the physical infrastructure of their facilities," says Cosman. If the computers controlling physical assets such as the valves and sensors are connected to a network that also connects to a business system using common technology, then access to the physical systems becomes possible via network incursion.

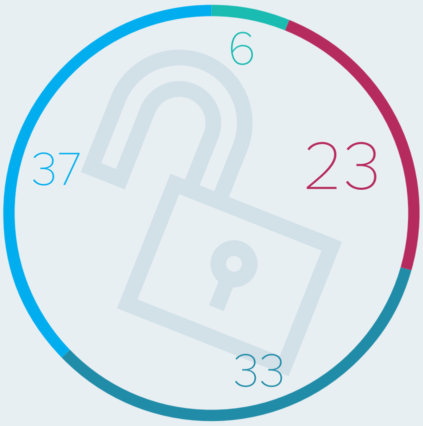
In a consulting assignment in the healthcare sector, Cosman heard reports of primary care systems sharing a network with the lighting system and the elevators, theoretically enabling an intruder to compromise the elevator and then find their way to the intensive care unit. "Isolation is no longer an option, but the real message to an asset owner is: if you connect two things, do so with a clear purpose and understand the possible consequences," says Cosman.

APPROACHES TO SECURITY

Which of the following statements best describes the strategy adopted by your organization's senior leaders for maintaining the security of integrated systems?

Percentage of survey respondents

- 🟦 We recognize that integration of cyber/digital and OT/physical systems creates new vulnerabilities, and our IT and OT teams are in the process of addressing them
- 🟦 We recognize that integration of cyber/digital and OT/physical systems creates new vulnerabilities, and we have adopted a holistic approach
- 🟥 **We consider the benefits of IT/OT convergence to outweigh the additional security risks and we believe that existing security systems are adequate**
- 🟩 We consider the benefits of IT/OT convergence to outweigh the additional security risks, but we believe that existing security systems are not yet adequate



Source: Newsweek Vantage

Some cyber experts call for network segmentation, requiring the user to show credentials to pass from one part to another, as noted in section four. According to Rich Armour, in the digital realm "it is more secure to operate on the principle of zero trust networking, where I assume that bad guys are in the network and therefore I implement a different level of security and scrutiny of all the traffic that enters a sensitive space."

The same goes for the physical world as well. "If you don't have network access control, somebody entering a facility can simply plug into a network port and then they have access to sensitive data," continues Armour. "You have to assume all the cyber-physical systems have gaps that will be exploited, and so design each sensitive asset with its own protective layer."

One example of a critical infrastructure organization that is taking great care to ensure its OT systems are protected is a British utilities supplier on the leading edge of its industry when it comes to cybersecurity.

> *"If you don't have network access control, somebody entering a facility can simply plug into a network port and then they have access to sensitive data"*
>
> — Rich Armour, former Chief Information Security Officer at General Motors

6. UPGRADING A WATER UTILITY'S SYSTEMS

South Staffordshire plc is a water utility with 1.7 million customers in two areas of central England that are 130 miles apart. It is currently replacing its SCADA and upgrading its telemetry network, installing one of the first fully internet-protocol-enabled networks in the UK water industry. The new system will standardize the IP for communications across its SCADA, providing a single view at group level of the entire infrastructure, whether it be IT, OT or corporate trends. "This gives us better governance, assurance and reduces the number of blind spots," says Ivan Miskin, director of group IT at South Staffordshire. "Because we are one of the first, we are being extra cautious, putting a level of management over and above what we do today from a security standpoint, expanding the scope to ensure the controls cover IT and OT."

Previously the company's OT systems were secure from cyberattack by virtue of the fact that they were not IP-enabled, says Sean Smith, head of operational technology at South Staffordshire. But times have changed. "Now, the IP-enabled network is doubling in size," says Smith. "The design of our cybersecurity defenses is of paramount importance. We want the benefits of an IP-enabled world, so we need to ensure the new system is locked down and secure." To this end, the company has added substantial protection to the network architecture, including multiple firewalls and separation within the network to create additional levels of security.

"In the unlikely event our cyber defenses are compromised and unauthorized access is detected, the system will respond by closing down the access route, thus preventing any damage to assets or systems," says Smith.

The new system, due for completion in 2021, will be able to detect any unusual activity on the network, raising a flag and checking whether it is approved. If it has not been approved, the system will cross-check the programmable logic controller (PLC) code against central codes, immediately detecting any unauthorized changes. If any change is made to the PLC that controls all the physical elements of the plants, such as pumping stations, this too will be flagged and cross-checked.

South Staffordshire will continue to segregate physically its IT and OT systems to comply with industry regulations.[15] But the system is designed to enable OT data to flow in one direction to be collected centrally, thus strengthening controls and enabling repairs to be done faster. Beyond this level of coordination, however, the physical integration of OT and IT systems is not a high priority, says Miskin. "Nobody wants to expose themselves to a potential cyber event. If we had a data breach across our OT systems and water became contaminated, it could potentially lead to fatalities, and so we have to be very careful not to join them up," he says. South Staffordshire therefore collects and analyzes its data enterprise-wide, without the risk of an OT breach.

Senior management understands, however, that field operators will need to be trained to become cyber-aware. "There will have to be a culture shift," says Smith. The best technology and most resilient processes still require the right skills and work attitudes to prevent a cyber event. For some organizations, a cultural change comes after a data breach, not before.

7. HURDLES TO THE HOLISTIC APPROACH

The difficulties of implementing a holistic approach to securing cyber-physical systems come in three main forms, organizational, technical and external, and the survey probed each of them in turn.

Organizational

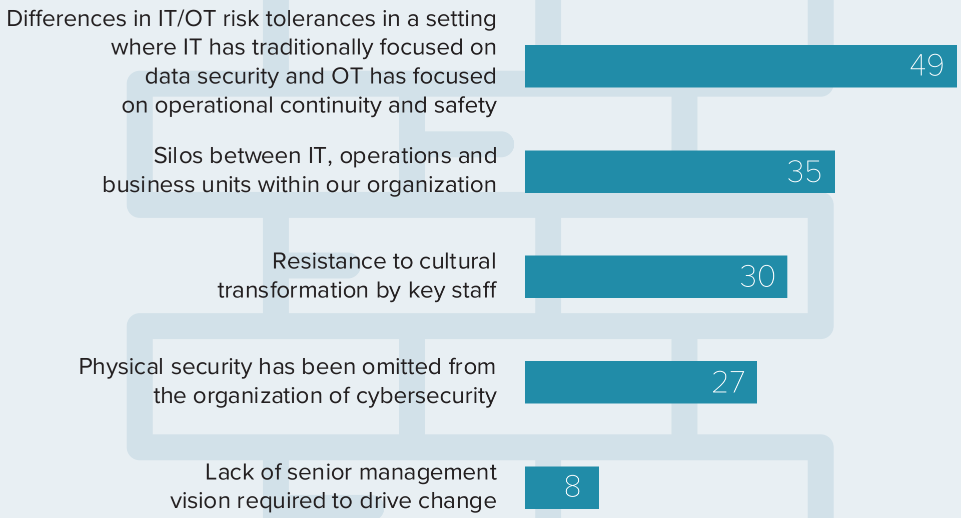
The main structural obstacle to achieving a holistic approach is that IT and OT do not see eye to eye on what needs to be secured, leading to different priorities in terms of risk management. IT has traditionally focused on data security, in which a cyber threat could result in the theft of millions of dollars of intellectual property, corporate financials, and employee or customer information. By contrast, OT has focused on operational continuity and safety. A cyber threat could have devastating physical consequences to critical infrastructure and services, employees, human life, and safety and the environment.

In the survey, almost half say that the differing risk tolerances of IT and OT are the key problem, considerably more than the next-biggest hurdle, the silos among IT, operations and business units within the organization. It is worth noting that more than a quarter say the main obstacle they face is that physical security has been omitted from the organization of cybersecurity, a reflection of the fact that many organizations are not taking a comprehensive approach to the issue.

IT AND OT ARE FAR APART

Which of the following factors are the most important organizational obstacles to achieving a holistic approach to securing cyber-physical systems? Choose up to two.

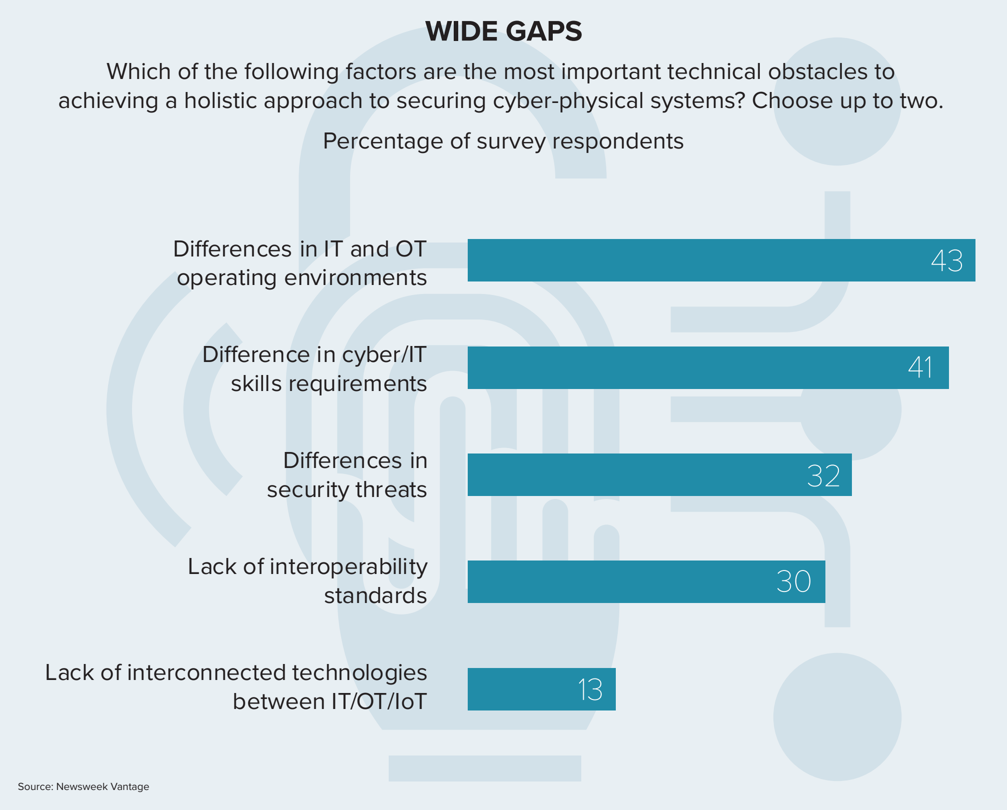
Percentage of survey respondents



Source: Newsweek Vantage

Technical

The technical obstacles are also dominated by the contrasting viewpoints of IT and OT: surveyed executives say their operating environments are very different, as are their perceived security threats and interoperability standards. All of these have a technical aspect, but one thing they don’t see is a lack of interconnected technologies: only one in eight say this is a significant obstacle. Technology is not pushing IT and OT apart, quite the opposite for most organizations.



WIDE GAPS

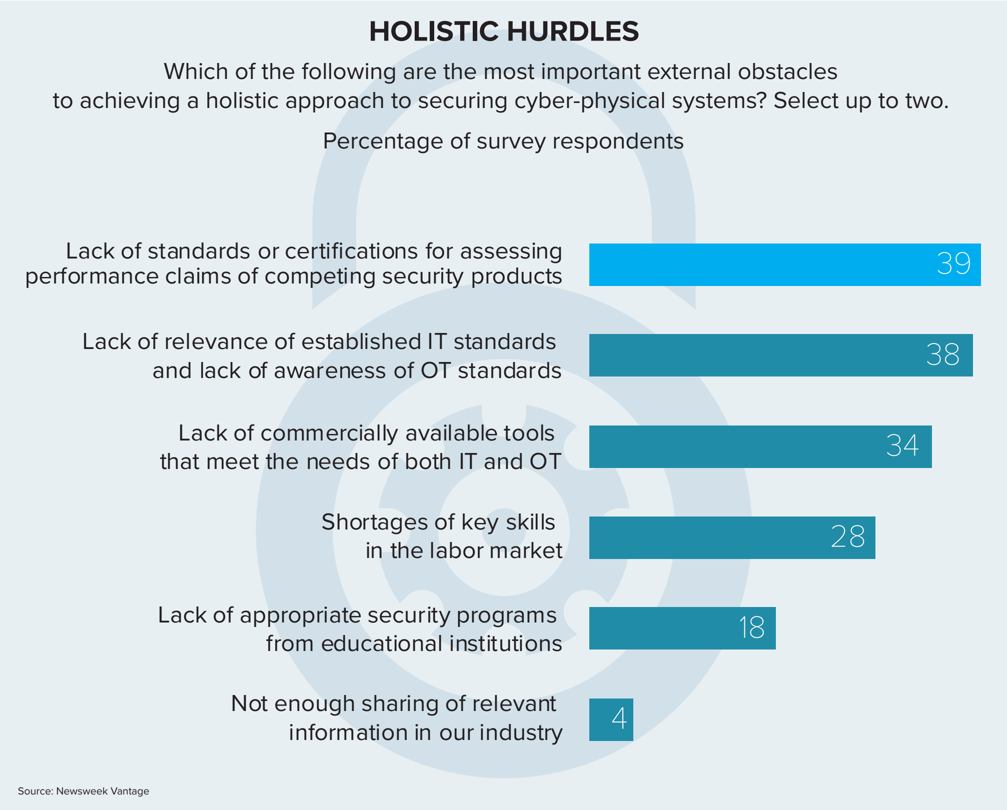
Which of the following factors are the most important technical obstacles to achieving a holistic approach to securing cyber-physical systems? Choose up to two.

Percentage of survey respondents

Source: Newsweek Vantage

External

The chief external obstacle to a holistic approach to cyber-physical systems can be summed up as a lack of adherence to standards. Respondents say there are not enough appropriate industry yardsticks for assessing the performance claims of competing security products. They also cite a lack of commercially available solutions that meet the needs of both IT and OT.



HOLISTIC HURDLES

Which of the following are the most important external obstacles to achieving a holistic approach to securing cyber-physical systems? Select up to two.

Percentage of survey respondents

Source: Newsweek Vantage

“I see the immaturity of the market as the key factor, especially when it comes to more advanced technologies,” says Hannes Barth. “The company has a picture of what it wants to do. It asks suppliers for what it wants and gets very different answers. The customers need a solution dedicated to OT and its special requirements. However, for the OT side of the market, standards and even terminology are still being developed. This is why critical infrastructure organizations start with pilot projects until they can drive toward full-scale implementation.”

Eric Cosman is the co-chair of the ISA99[16] committee which has focused on setting standards for industrial automation and control systems security since 2002. He has worked on the asset side of the transaction, evaluating the claims of suppliers. “If you have a long relationship with a supplier, then there is a certain degree of trust, but you still need to verify the claims by checking that the service or product has been certified by a third party,” he says.

Cosman concedes that he often hears complaints about needless duplication among the industry security standards, but “the adoption of these standards has also been somewhat haphazard. I believe this is why the standards community must shift emphasis from the ‘what’ to the ‘how’, in terms of using the standards, through case studies and proven accepted practices.”

To elaborate, Cosman outlines a three-step program to overcome the problem of multiple standards in the field of cybersecurity.

a) Assess the gap between the current and desired states, by creating an inventory of systems and devices, including a description of how each is used and for what purpose. From this, determine the future state to be aimed for.

b) Identify and become familiar with applicable standards, guidelines and practices. In some cases, this choice is obvious (e.g., the North American Electric Reliability Corporation’s critical infrastructure plan[17]), while in other cases there may be more options.

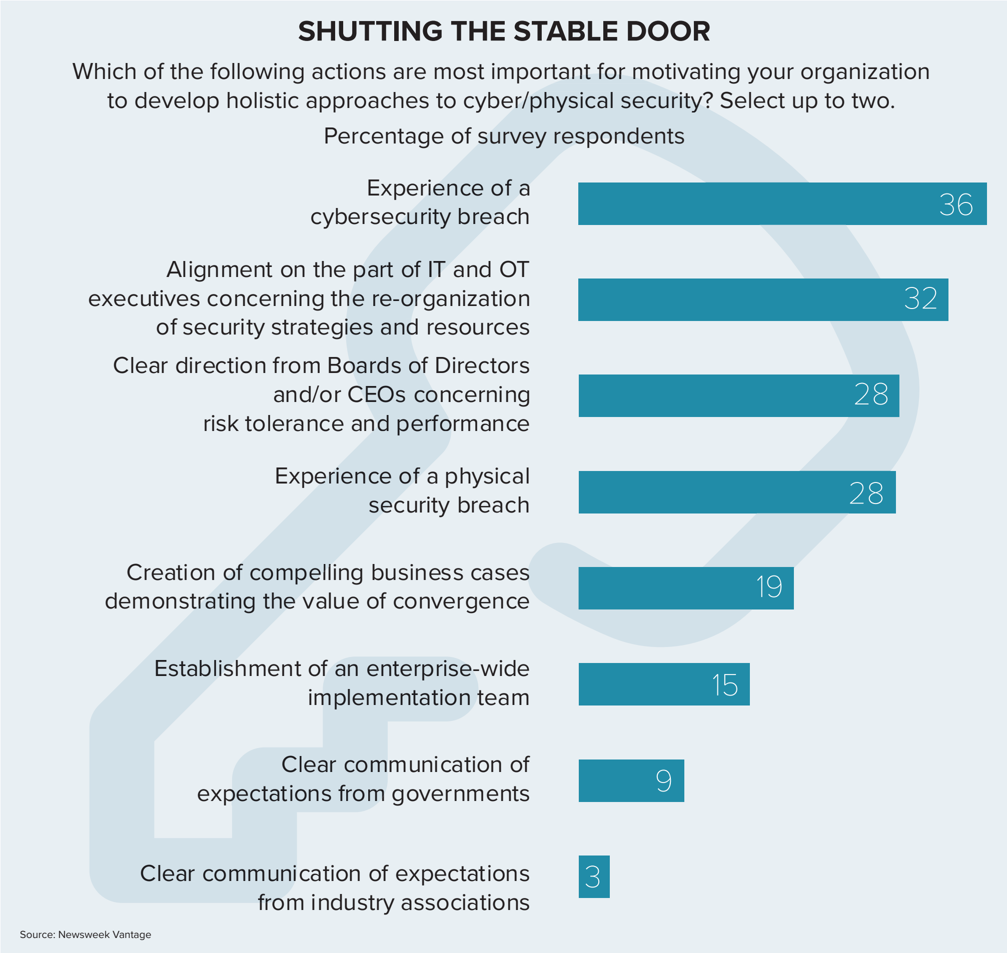
c) Make a detailed assessment of risk for the entire facility, possibly combining it with assessment conducted for the purpose of physical safety. The outcome should consist of a prioritized list of areas for improvement, from which to create an implementation plan.

Having examined some of the main obstacles to a holistic cyber-physical security strategy, the report turns to perhaps the biggest challenge of all: the need for all employees from the top to bottom to be accountable for this crucial aspect of the organization.

8. CHANGING MINDS

As in so many areas of risk management, it often takes a crisis to change an organization. Alas, cybersecurity is no different. Executives included in the survey were asked to select the two prime motivators that had caused them to develop holistic approaches to cyber-physical security. The most frequently chosen: experiencing a cybersecurity breach, with 36%, while a further 28% suffered a physical breach before being spurred to action. By contrast, governmental regulations play a much less significant role.

“Without a crisis, it’s hard to change a culture,” says Steven Mustard, who cites the example of a security breach of the SCADA system at Maroochy Water Services in Queensland, Australia in 2000. A hacker, angry at not being hired by the local authority, used a laptop computer and a radio transmitter to take control of 150 pumping stations for three months, releasing untreated sewage into a stormwater drain from where it flowed to local waterways.


SHUTTING THE STABLE DOOR

Which of the following actions are most important for motivating your organization to develop holistic approaches to cyber/physical security? Select up to two.

Percentage of survey respondents

Source: Newsweek Vantage

“Marine life died, the creek water turned black and the stench was unbearable for residents,” according to Janelle Bryant of the Australian Environmental Protection Agency.[18] The perpetrator was eventually caught and jailed, and the government department responsible enacted a range of measures to improve cybersecurity.[19] The horses having already escaped, the barn door was then securely bolted.

Such incidents demonstrate the need for a holistic approach to cyber-physical systems before the event rather than after. For many organizations, the critical factor for making this happen is firm leadership. “A good culture from a cybersecurity standpoint begins at the top, when senior management actually become involved. At most organizations, that doesn’t happen before they are hit by a cyber incident,” says Daniel Henriksen.

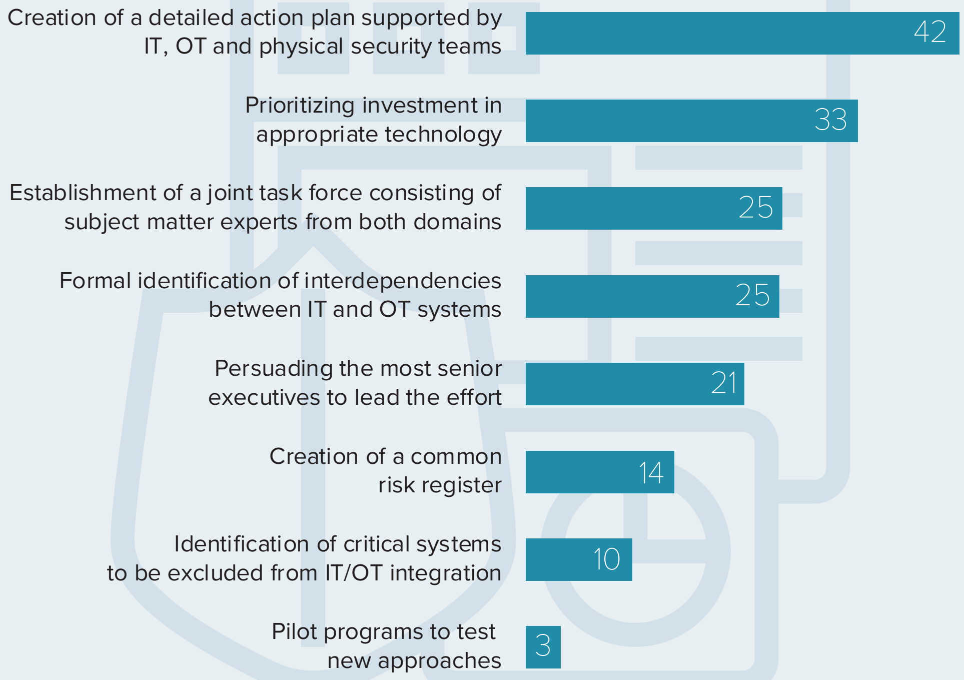
This is borne out by the survey data demonstrating that clear direction from the board of directors and the chief executive is a prime motivator for cybersecurity improvements. On this point, there is an unusual contrast between the opinion of CEOs and other executives. CEOs are twice as likely as other executives to believe that directions from the leaders are a top motivator, indicating that executives may not always see eye to eye on the organization’s cyber-physical security strategy.

Once senior management takes an active role in setting cybersecurity strategy, the data shows that careful planning is critical for success, along with broad-based support and appropriate investments. Respondents add that other elements remain important but are less critical to success, such as the formal identification of interdependences between IT and OT or identifying the critical systems to be excluded from integration.

GET BROAD BUY-IN

Which of the following are most important for implementing a holistic approach to cyber/physical security? Choose up to two.

Percentage of survey respondents



Source: Newsweek Vantage

In terms of overcoming the cultural obstacles to a holistic approach, executives say that the most important factors are to build a team that includes skills of IT, OT and physical security, along with cross-training of the teams from the three areas. “Most organizations struggle to imagine what a holistic approach to cybersecurity looks like,” says Siemens’s Hannes Barth.

What is the key to a successful holistic strategy that is most overlooked? “The whole ‘people’ aspect,” says Barth. “To have the right team to ensure the mindset is right so that the security tools are used and developed properly. This is something that money can’t buy. You can pay for the training, but after that, you have to build and maintain a team yourself.”

Once the organization has developed its holistic strategy toward securing cyber-physical systems, surveyed executives selected the following four elements that most effectively ensure it operates well:

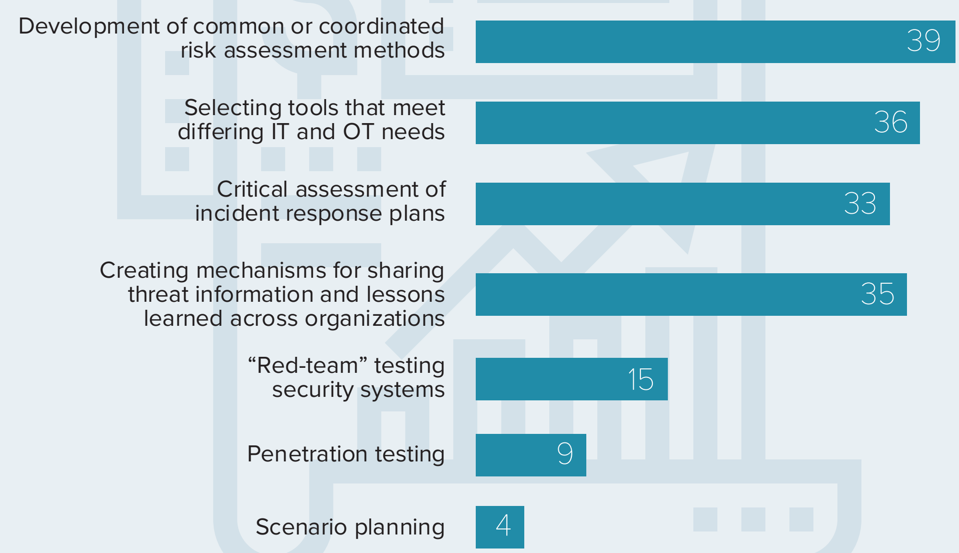
1. Development of coordinated risk assessment methods.
2. Selection of tools that meet differing IT and OT needs.
3. Creation of mechanisms for sharing threat information and learning the lessons drawn from the experience of multiple organizations.
4. Critical assessment of incident response plans.

This report has examined some of the main challenges organizations face in taking a comprehensive approach to the security of cyber-physical systems as well as methods for meeting those challenges. Next, the report concludes by reviewing some of the basic lessons to be drawn from the survey findings and the views of the subject-matter experts.

ASSESS RISK COMPREHENSIVELY

Which of the following are most important for ensuring the effective operation of a holistic approach to IT/OT security? Select up to two.

Percentage of survey respondents



Source: Newsweek Vantage

9. UNCOMMON SENSE

The skills, techniques and processes for securing digital and physical assets must evolve rapidly to mitigate the ever-growing threat of cyberattack. The risk will continue to increase as technologies converge and hackers become more adept at using technology for their own ends. The trend toward greater integration of IT, OT and physical assets will endure and possibly accelerate.

The imperatives of digital transformation make this unfolding reality all the more inevitable; even if competition is not a factor for a public utility, for example, customers are continually demanding better and more transparent services. And governments are raising the regulatory bar. Customer service and compliance will increasingly require the use of AI and machine learning.

Standing pat is not an option, so what lessons should readers draw? As Steven Mustard says, “the actions organizations need to take are not technically difficult—they’re culturally difficult.” It is painful to alter habits of thought and traditional business practices; the survey data demonstrates that employee resistance to cultural change is one of the primary obstacles to holistic cyber-physical security.

When contemplating a big cultural shift, it is worth breaking such a daunting task into a few manageable elements.

Cyber-physical standards need to be applied and, where possible, raised. As the report has shown, there are standards for the cybersecurity of automation and control systems, and they should be universally adopted. The fact that there are several standards is not a good reason for asset owners and vendors to fail to apply them. The same goes for certification. Right now, engineers can work on the security of control systems without a relevant certificate. If project managers need a certificate to work on such projects, it makes no sense to ignore this stipulation for cybersecurity.

Do things in the right order. Set up a good structure of governance for cyber-physical security, with clear lines of accountability. Sources, such as the US National Institute of Standards and Technology Cybersecurity Framework,[20] describe a systematic approach with references to applicable standards for each step. Train all personnel thoroughly on their cyber-physical responsibilities. Design the organization’s policies and procedures to align with those pertaining to cybersecurity and vice versa. Only then decide on what technologies to invest in that will support the other elements. “Most organizations do it backwards,” says Mustard.

Don’t punish people if they admit to having made a mistake. Organizations tend to penalize those who make errors. Instead they should encourage personnel to own up when a cybersecurity breach occurs or, even better, when they recognize and disclose a mistake that might lead to an incident. A failure is an opportunity to learn how to do things better.

Treat cyber-physical security in the same way as physical safety. The safety of employees and the public is considered of paramount importance at every organization and is regarded as the business of everybody in the organization. There is no reason why cyber-physical security should not be treated in the same way.

Cyber-physical security is not like going on a diet. It’s a change of lifestyle. Organizations should not treat the task as completed after taking all the requisite steps in a holistic implementation program. The job of securing assets and employee behavior needs to be continually updated because threats and vulnerabilities will change all the time.

When the security of cyber-physical systems is framed in this way, the fundamental steps of implementation may seem commonsensical. But often the most basic procedures are the ones that are ignored. Samuel Taylor Coleridge said that “common sense in an uncommon degree is what the world calls wisdom.” So, be wise before the event. It doesn’t have to take a catastrophe to spur organizations to do the right thing.

SURVEY METHOD AND DEMOGRAPHICS

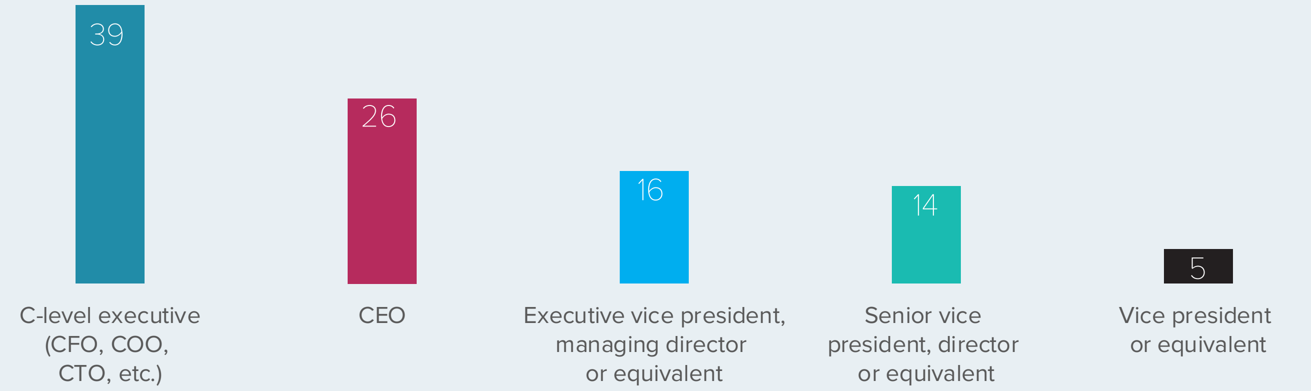
The questionnaire was framed around the hypothesis that "the convergence of the IT and OT domains has exposed critical infrastructure facilities to new cyber threats. Most critical infrastructure organizations recognize these threats and are sharing experience and knowledge across the IT/OT interface. But they have not focused enough on the interdependence of the cyber/digital and physical dimensions of cyber-physical systems."

To test the hypothesis, PureProfile was commissioned by Newsweek Vantage to field a confidential, global online survey between December 2019 and January 2020. A total of 415 executives, mostly C-level, responded from 16 industries defined by the US Department of Homeland Security as critical infrastructure sectors. For the purpose of the survey, the energy sector was sub-divided into oil & gas production, electricity generation, transmission and distribution. The energy sector also contains "nuclear reactors, material and waste" and "dams" for purposes of this survey.

Respondents from Europe comprised 38%, North America comprised 33% and Asia-Pacific 29%. To cover functions responsible for cyber-physical systems, the survey drew responses from IT, cybersecurity, operations, engineering and physical security. Almost two thirds of those surveyed worked in organizations with an annual budget of $1 billion or more. We thank those who participated in the survey.

JOB TITLE

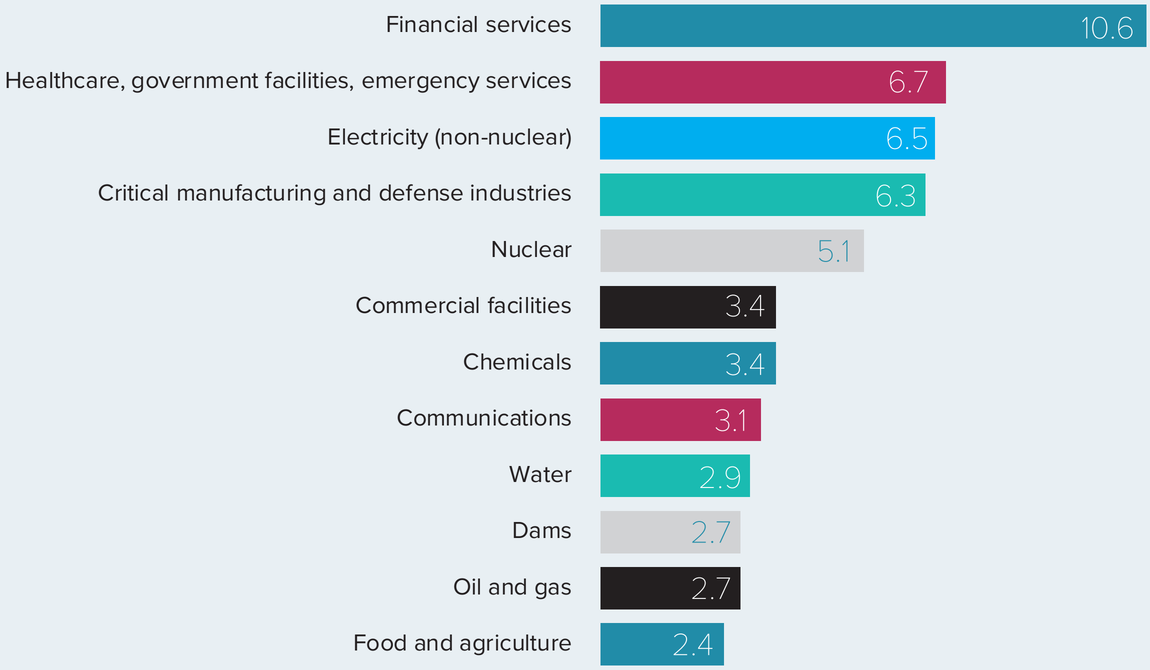
Percentage of survey respondents



Source: Newsweek Vantage

SECTORS

Percentage of survey respondents

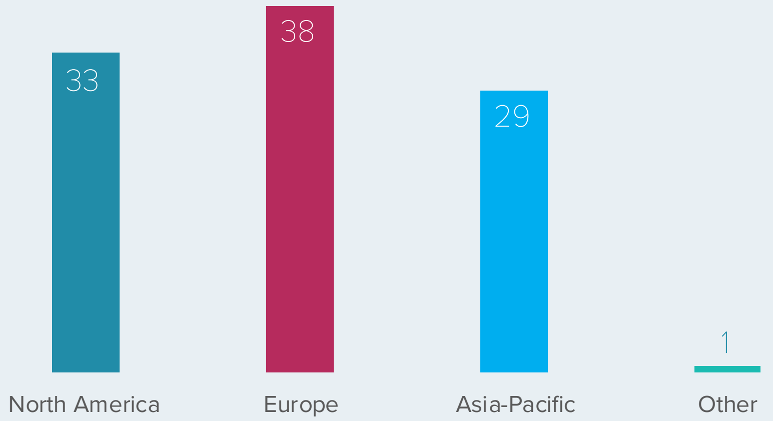


Source: Newsweek Vantage

REGION

In which region are you personally located?

Percentage of survey respondents

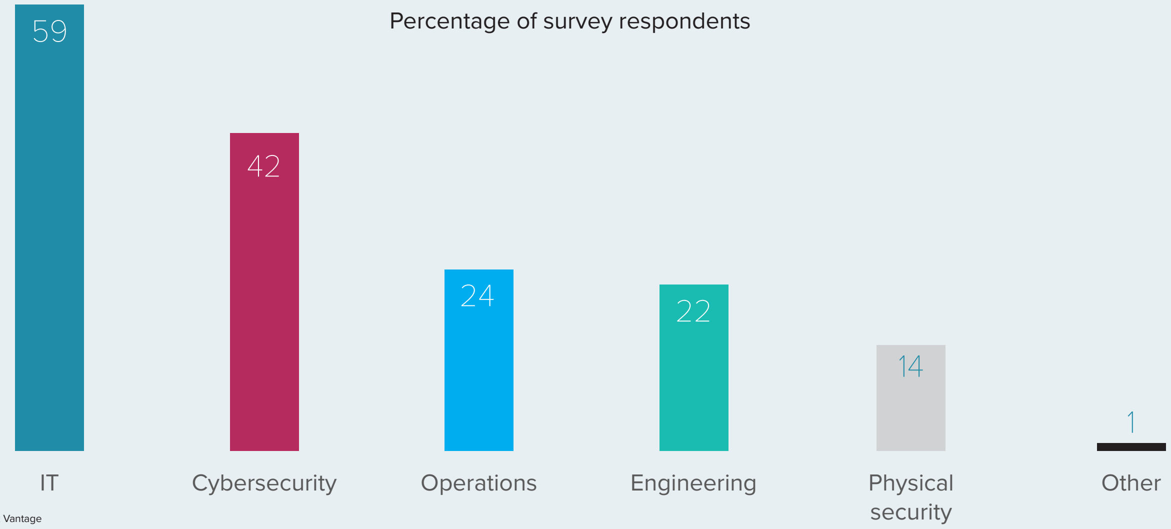


Source: Newsweek Vantage

FUNCTIONS

Select all that apply

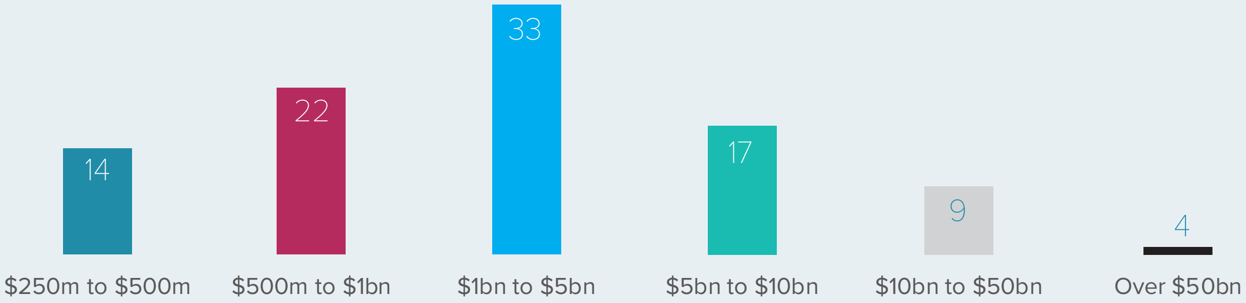
Percentage of survey respondents



Source: Newsweek Vantage

ANNUAL BUDGET

Percentage of survey respondents



Source: Newsweek Vantage

References

1 https://www.ft.com/content/a4ac1ad1-0c86-4c7a-a6ac-d5296cbaecb8

2 https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response

3 "Caught in the crosshairs: Are utilities keeping up with the industrial cyber threat?" October 2019.

4 https://www.idc.com/getdoc.jsp?containerId=prUS45213219

5 https://www.mckinsey.com/industries/capital-projects-and-infrastructure/our-insights/critical-resilience-adapting-infrastructure-to-repel-cyberthreats

6 https://blogs.gartner.com/kristian-steenstrup/2011/03/16/the-strategy-value-and-risk-of-itot-convergence/

7 https://zpryme.com/media/infographics/infographic-2014-utility-itot-convergence-survey/

8 https://www.aspi.org.au/report/protecting-critical-national-infrastructure-era-it-and-ot-convergence

9 See also definition and background in https://ptolemy.berkeley.edu/projects/cps/

10 https://www.cisa.gov/critical-infrastructure-sectors

11 ibid

12 https://fas.org/irp/crs/RL31556.pdf

13 https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

14 https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

15 For example, UK Security of Network & Information Systems Regulations. See https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018

16 This committee is the principal source of the ISA/IEC 62443 standards.

17 https://www.nerc.com/comm/CIPC/Pages/default.aspx

18 https://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

19 "Lessons learned from the Maroochy water breach," Jill Slay and Michael Miller, International Federation for Information Processing, 2008

20 https://www.nist.gov/cyberframework

Weathering the Perfect Storm was researched and written by Newsweek Vantage and sponsored by Nozomi, Siemens and Yubico, in association with ISA.

Editorial: Nigel Holloway, with assistance from Stéphane Côté and Kenneth Waldie

Design: Links Design Ltd

Publication date: March 2020

Newsweek Vantage retains sole responsibility for the content in this report. The views expressed do not necessarily reflect the opinions of our sponsors or partners.

Disclaimer

While every effort has been taken to verify the accuracy of the information presented, neither Newsweek nor Think Big Partners WLL nor any of their affiliates can accept any responsibility or liability for reliance by any person on this information.