iSMG
INFORMATION SECURITY
MEDIA GROUP

SURVEY RESULTS

Securing Industry 4.0

Manage Cyber Risk in Smart Manufacturing Operations

paloalto NETWORKS

accenture

Table of Contents

This survey was conducted in the winter of 2021-2022. Focused across sectors, the study attracted more than 100 responses. Of the respondents, 42% come from pharmaceuticals, medical devices and healthcare products manufacturing and 44% come from enterprises of 1,000 to 5,000 employees

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us @AccentureSecure on Twitter, LinkedIn or visit us at accenture.com/security.

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

Letter from the Editor

TOM FIELD
SVP, Editorial, ISMG
tfield@ismg.io

Field is responsible for all of ISMG's 28 global media properties and its team of journalists. He also helped to develop and lead ISMG's award-winning summit series that has brought together security practitioners and industry influencers from around the world, as well as ISMG's series of exclusive executive roundtables.

Welcome to the report summarizing the survey Securing Industry 4.0: Manage Cyber Risk in Smart Manufacturing Operations.

The backdrop of this study is: We're in the fourth Industrial Revolution, and it arrived faster than anyone could have planned. It came with smart devices, automation, cloud migration and a new streamlined ability to engage with customers and partners.

But it also brought with it the vulnerabilities inherent in legacy technology, the disconnect of OT, an enlarged attack surface and increased attention from nation-state and criminal adversaries who seek to disrupt operations or steal intellectual property.

The key question for survey respondents: How prepared are you to secure Industry 4.0? Areas of focus include:

- The state of Industry 4.0 cybersecurity;
- Key digital transformation initiatives;
- The potential barriers inhibiting digital transformation initiatives.

More than just survey results, this report offers expert analysis on why and how enterprises are securing Industry 4.0 and how they might measure their progress along the way. This report intends to go beyond the survey statistics to tell you not just what respondents said but how to put these results to work to enhance your own journey.

Best,

Tom Field
SVP, Editorial, Information Security Media Group

Executive Summary

COVID-19 was not the catalyst for Industry 4.0, but it certainly was an accelerant.

For most manufacturing companies, the road to “smart” began long ago with the introduction of automation, some cloud migration and tighter digital integration along the supply chain.

The pandemic of 2020 introduced two new dynamics:

- **Compressed Transformation**: Forced by quarantine to deploy remote workforces, rely more on cloud services and apps and conduct business primarily through digital channels, manufacturing companies – like most global enterprises – compressed a decade of digital transformation into months. Suddenly, the future was for enterprises seeking to migrate more to the cloud and refresh their legacy IT and OT environments.

- **Heightened Cyberthreats**: Build a larger potential digital attack surface, and the adversaries will come. Having undergone their own digital transformation and adopted more automated tools, cyberthreat actors including criminal gangs and nation-states stepped up their efforts to steal credentials, disrupt operations and extort victims through the spread of ransomware. But suddenly it was harder to distinguish between cybercriminals and nation-state actors – their tactics and tools are similar – and incidents such as SolarWinds, Colonial Pipeline and Kaseya proved that companies are no longer a target because of their size, sector or brand. Now they also are targets because of the technology they use and the partners they choose.

50%

of survey respondents believe they are above average or superior when comparing their cybersecurity posture to peer enterprises.

80%

say they either are well on the way or getting started toward becoming a “smart manufacturing company.”

70%

say their key digital transformation initiatives include cloud migration of infrastructure and/or apps.

This new reality is the backdrop to this survey about securing Industry 4.0 and how security/ technology leaders will manage cyber risk in their increasingly smart manufacturing operations.

Some themes that emerge in the survey findings:

Confidence

There is a level of confidence among respondents, 50% of whom say they are above average or superior when comparing their cybersecurity posture to peer enterprises, and 80% of whom say they either are well on the way or getting started toward becoming a “smart manufacturing company.”

Vulnerability

Beneath this confidence, there is concern about risks inherent in cloud migration and legacy technology – particularly in the OT environment. Asked what new digital initiatives create the greatest cyber risk, 57% say cloud migration of infrastructure and/or apps. Asked what barriers might inhibit their digital transformation, respondents cite: human resources - we lack the people/ skills (57%) and legacy technology burden - it’s too much to refresh (50%).

Ambition

Despite the threat landscape and perceived barriers, these manufacturing companies stick to the modernization mission. Nearly all (98%) expect level or increased budgeting for digital transformation initiatives in the year ahead, and they are targeting investments that can move their missions forward:

- Cloud security measures - 49%
- Zero trust security model - 39%
- Identity and access management - 37%
- Legacy OT refresh - 33%

Partnership

Just as respondents recognize supply chain risk from their business partnerships, they also see the need to move forward with third parties that can lend a hand with expertise and technology. Asked whether they have the internal capacity to forge ahead alone or if they will rely on third-party assistance, 75% of respondents say they either “absolutely need third-party guidance” or “will blend internal/external resources.”

These survey responses provide a fresh look at the state of migration to Industry 4.0, and survey sponsors from Palo Alto Networks and Accenture Security offer fresh insight into what the results mean – and how to put them to work.

“Delivering security takes clear strategic intent, a nimble governance model, alignment – across the IT organization and the rest of the business,” says Paul Brownlee, North American lead, operational technology, Accenture. “Success comes faster when security is a part of the solution to the business problem.”

“I see this report as a good way to see where you stand and maybe have some ideas of what you need to research to invest,” says Del Rodillas, global head, manufacturing and energy industry strategy and solutions, Palo Alto Networks. “If there are new concepts that you haven’t heard about, I certainly would hope that you can spend the time to understand what this technology is and how it could be applied, so that you broaden your view on the security as you become a smart manufacturing organization.”

Read on for an overview of the key survey findings and then the detailed analysis from Brownlee and Rodillas.

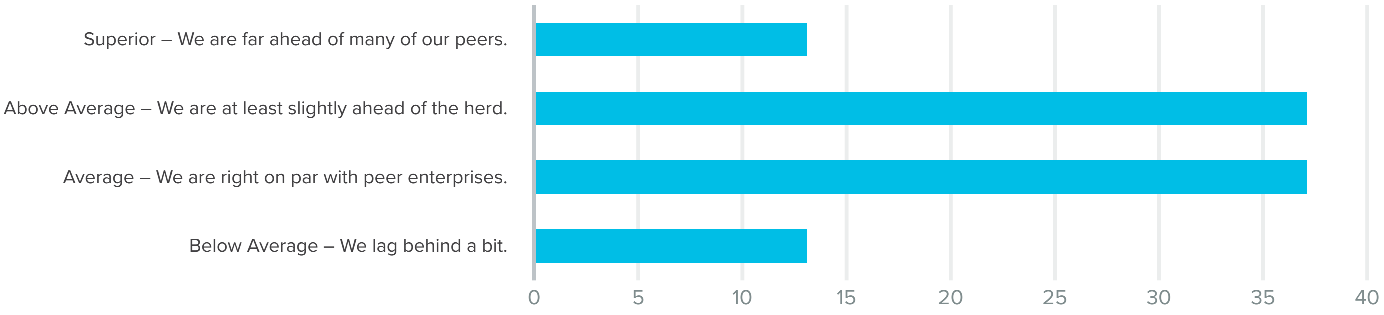
Baseline Questions

In this opening section, the report details the general attitude of respondents toward their enterprise's current cybersecurity posture and state of digital transformation – how "smart" do the respondents perceive their enterprise to be?

Key statistic: Only 20% of respondents report they are "Not Quite" on the road to Industry 4.0, saying, "We are inhibited by legacy technology and lack of human and financial resources, and the greater attack surface and threat landscape are intimidating. We are laggards among our peers."

Full responses:

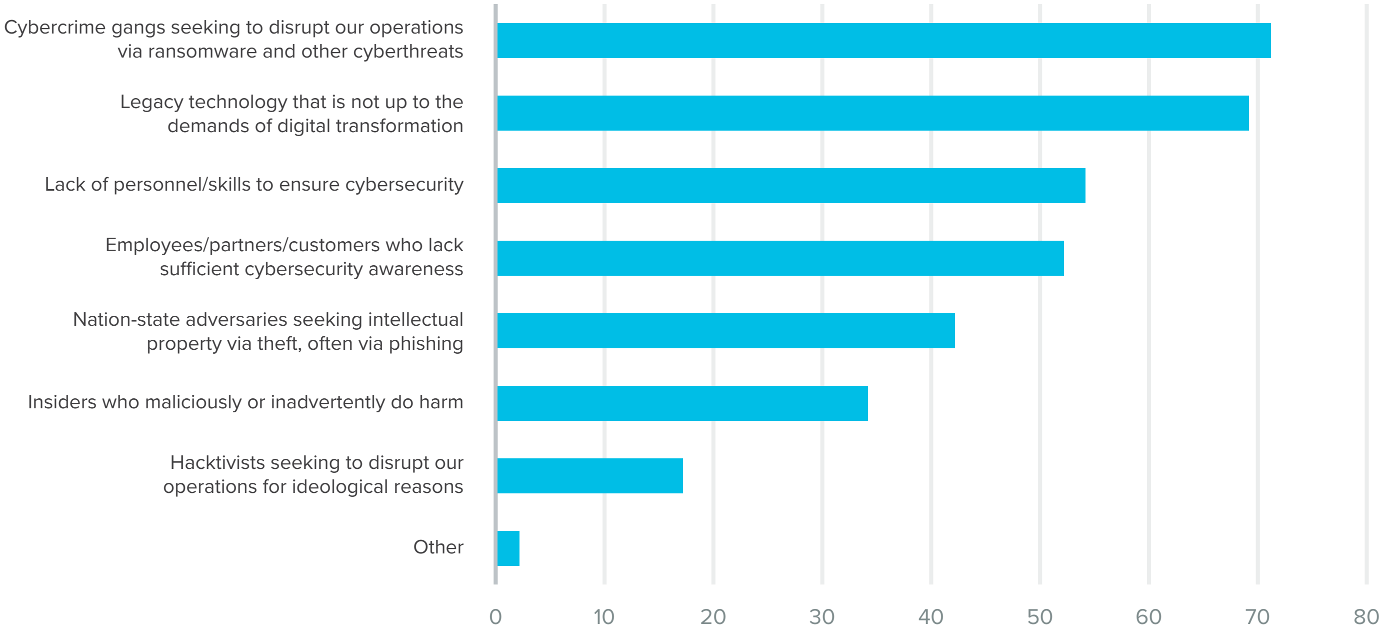
Based on what you know of peer manufacturing companies, how would you assess your enterprise's current cybersecurity posture?



In this first "take the pulse" question, just over half of respondents say their enterprises are above average or superior in cybersecurity posture when compared to peers in their sectors.

Fair assessment or false confidence? Subsequent questions and responses take a deeper dive into true strengths and potential vulnerabilities.

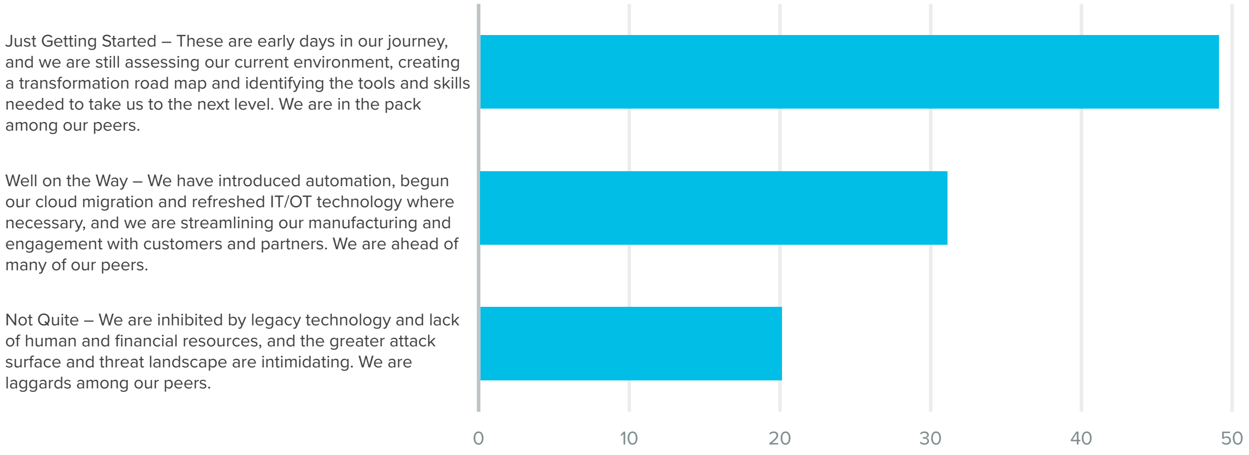
What do you see as the greatest cybersecurity threats to your OT/ manufacturing environments today?



It is key to point out: This survey was administered before hostilities broke out in Eastern Europe, raising heightened concerns about nation-state cyberthreats.

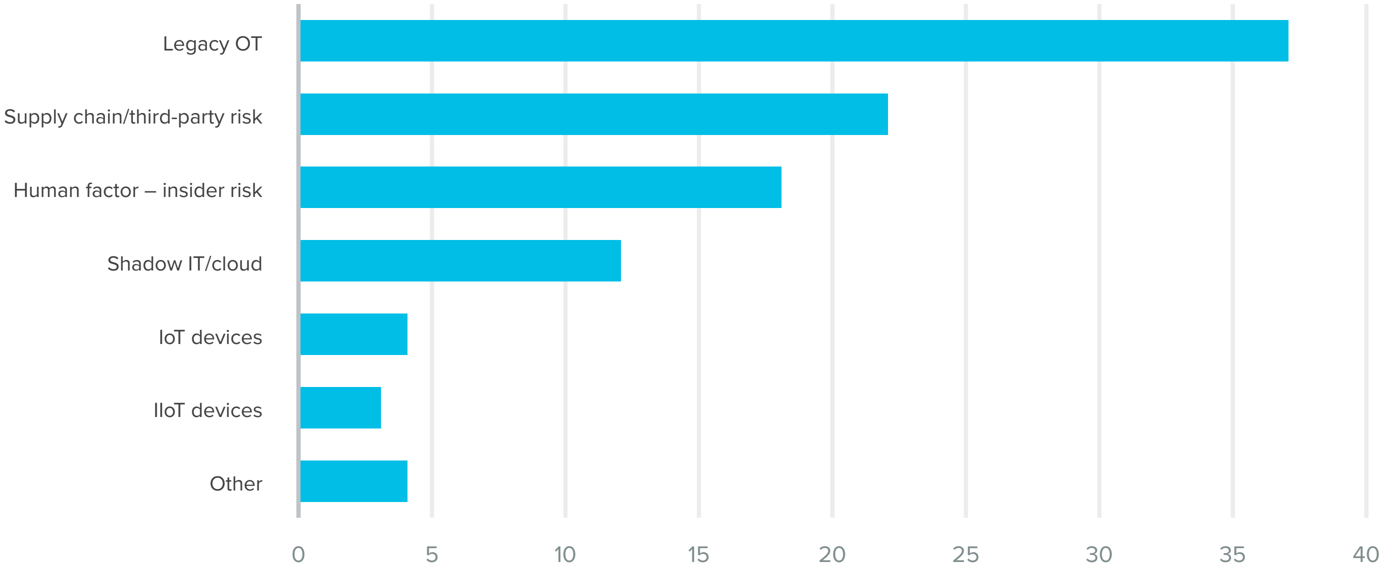
When asked, then, what they see as the greatest cyberthreats to their OT/manufacturing environments, 72% of respondents choose cybercrime gangs seeking to disrupt operations via ransomware and other threats. But nearly as many (69%) cite legacy technology that is not up to the demands of digital transformation.

To what degree do you consider your enterprise to be a "smart manufacturing" company today?



Asked to rate to what degree their enterprise is a “smart” manufacturing company today, not quite one-third chose “Well on the Way,” while nearly 50% say “Just Getting Started,” meaning: “These are early days in our journey, and we are still assessing our current environment, creating a transformation road map and identifying the tools and skills needed to take us to the next level. We are in the pack among our peers.”

Wherever you are on the road to smart manufacturing, where do you perceive your enterprise to be most vulnerable today?



Asked where they perceive themselves to be most vulnerable on this journey to “smart” manufacturing, respondents again use the word “legacy.” Thirty-eight percent say their enterprise is most vulnerable through legacy operational technology, while 22% cite supply chain/third-party risk.

The next section delves deeper into the actual state of smart manufacturing and specific initiatives currently underway.

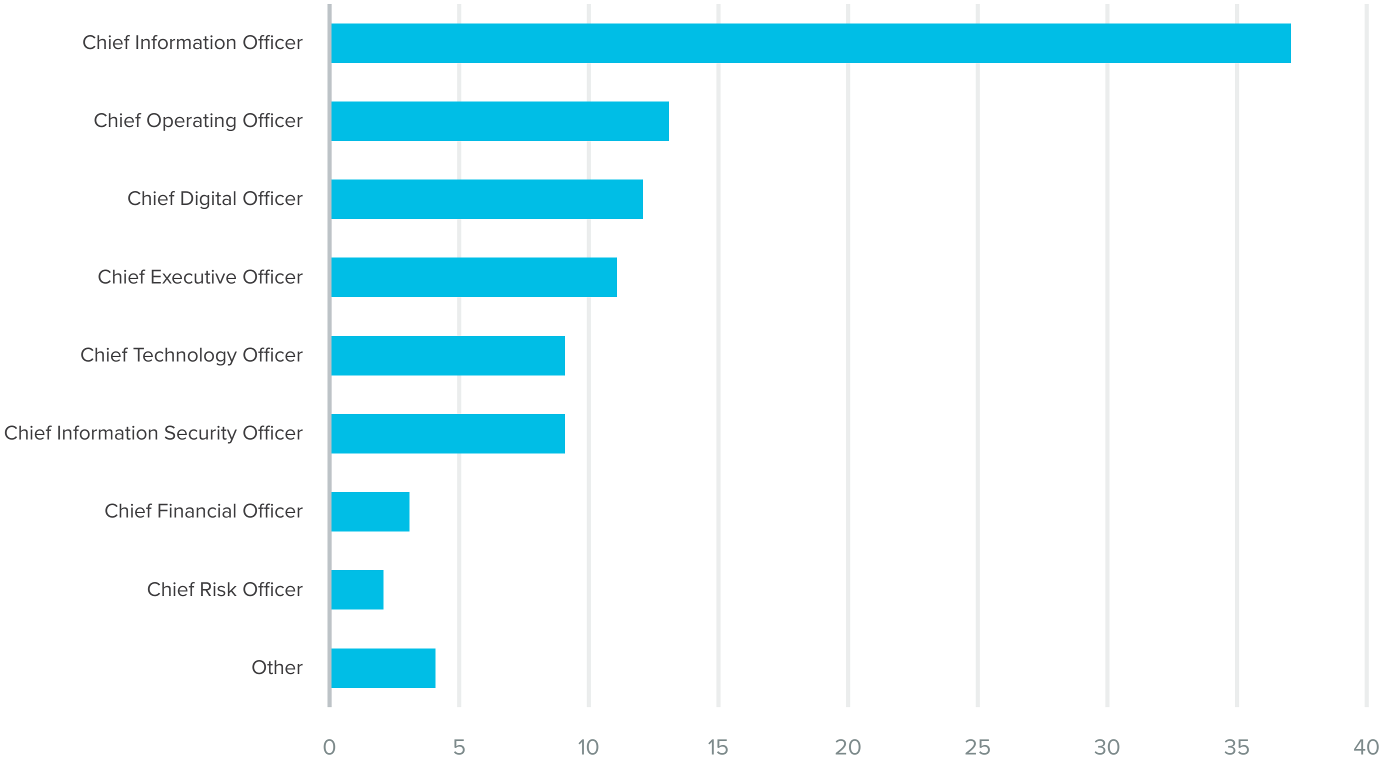
The State of Smart Manufacturing

This section focuses on specific digital transformation initiatives and their perceived impact on productivity and profitability. Key statistics:

- 57% say cloud migration creates the most new cyber risk.
- 72% have invested in endpoint protection to help mitigate this risk.

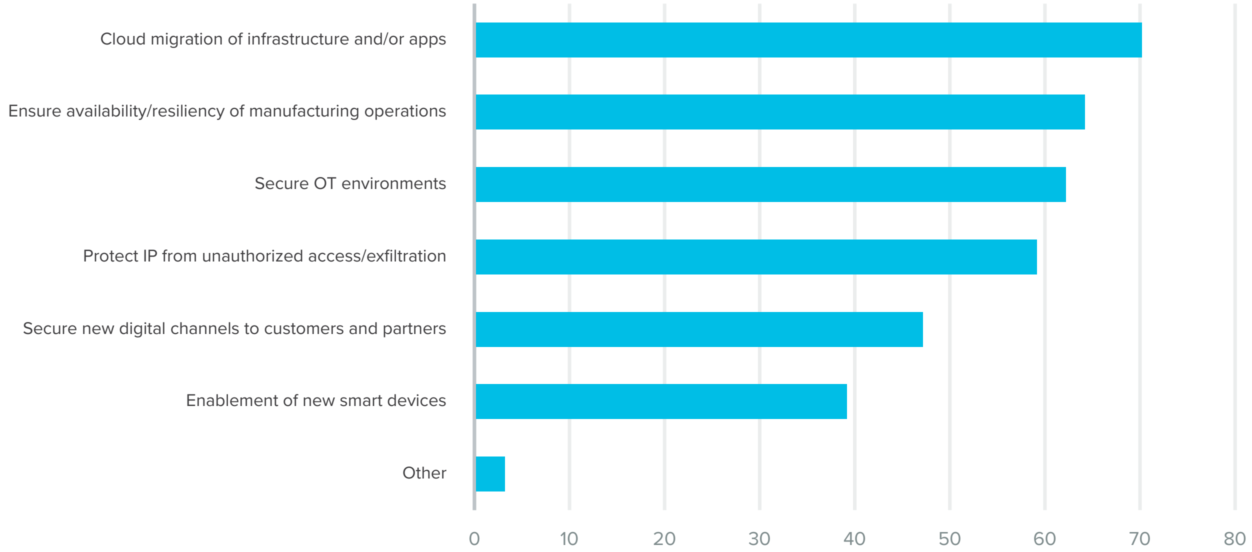
Full results follow:

Who in your enterprise currently owns responsibility for your digital transformation initiatives?



Far and away, the CIO (38%) is the executive who owns primary responsibility for digital transformation initiatives, followed by the COO (13%) and CDO (12%) as distant second and third.

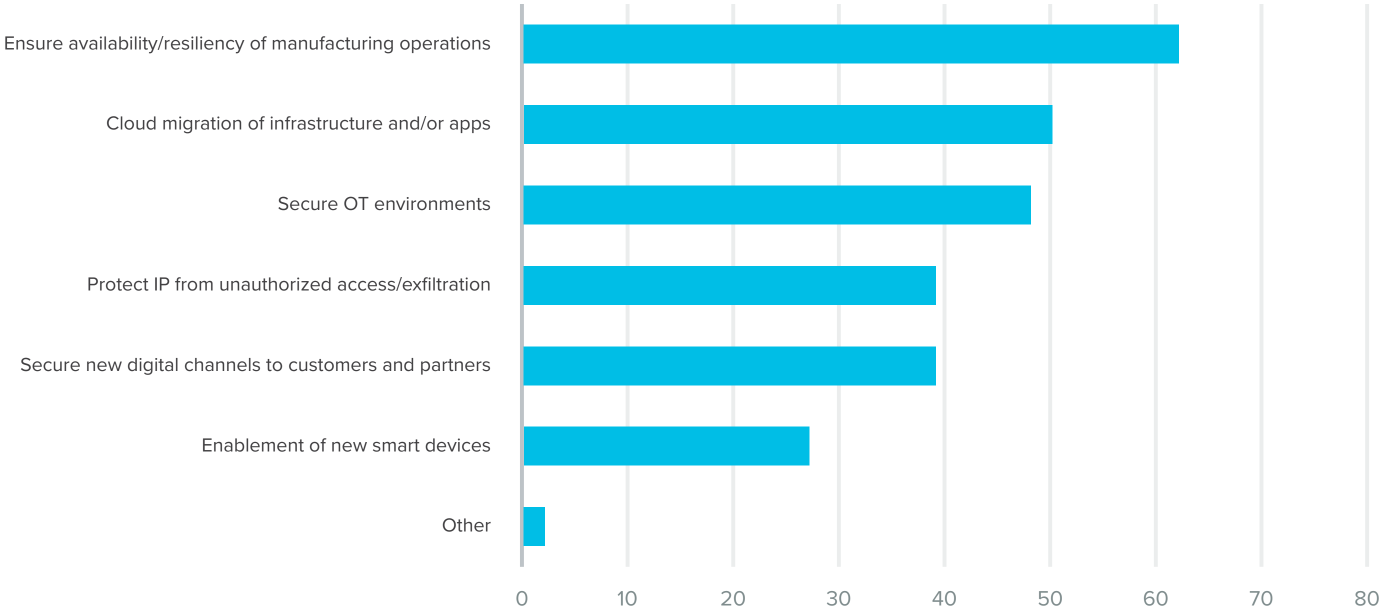
What are your enterprise’s current areas of focus in terms of digital transformation initiatives?



Asked to name their enterprise’s current areas of digital transformation initiatives, respondents choose these top three: Cloud migration of infrastructure and/or apps - 70%; Ensure availability/ resiliency of manufacturing operations - 65%; Secure OT environments - 62%.

Compare this list with the next, which covers the initiatives that may have the biggest impact on productivity and profitability.

Which of the initiatives may have the biggest impact on productivity and profitability?

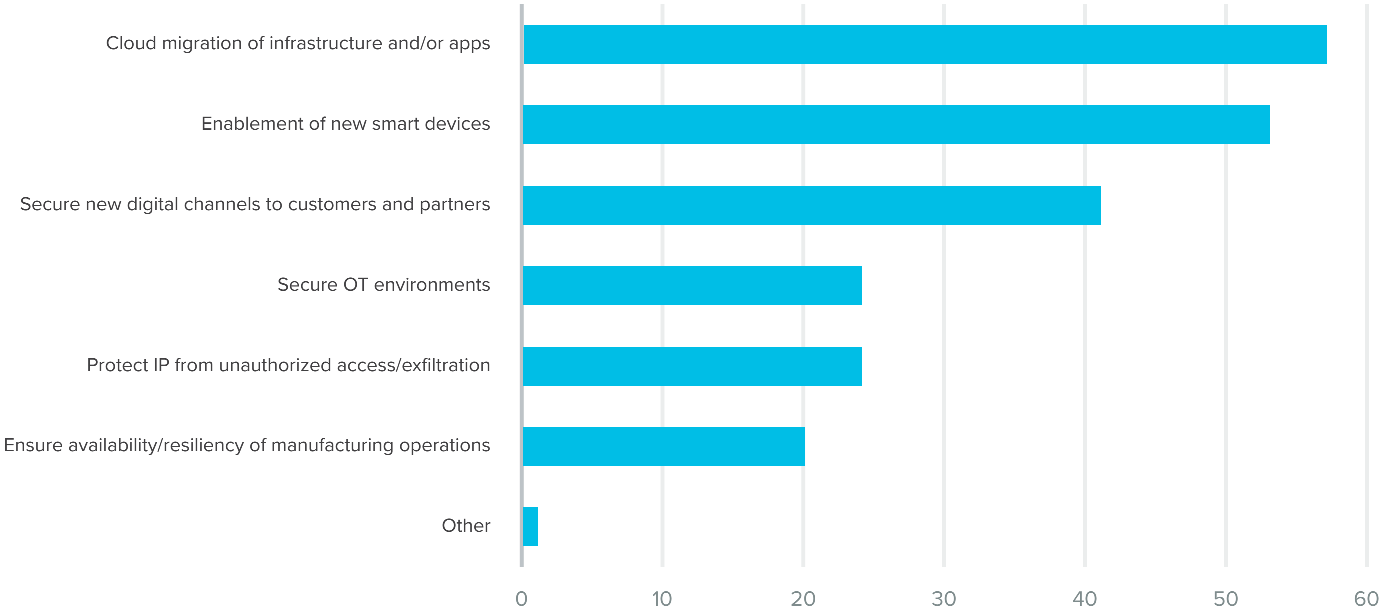


Here, the top three responses are the same, but in slightly different order:

- Ensure availability/resiliency of manufacturing operations - 63%
- Cloud migration of infrastructure and/or apps - 50%
- Secure OT environments - 48%

Next, see which of these same projects is perceived as creating the greatest new cyber risks.

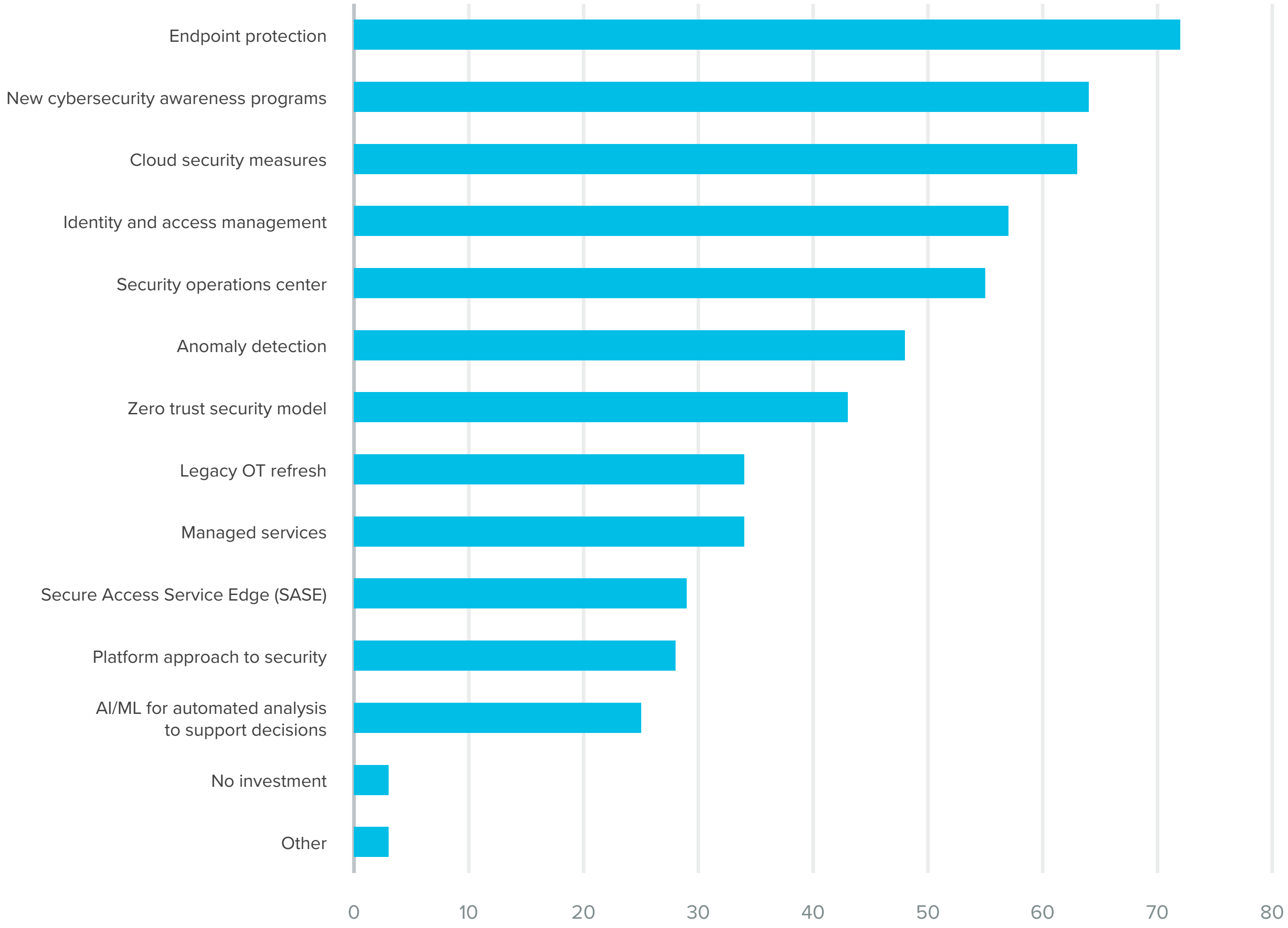
Which of the initiatives could create the most new cyber risk?



A slight variation on the previous selections, survey respondents say these are the top three initiatives that could create the most new cyber risk:

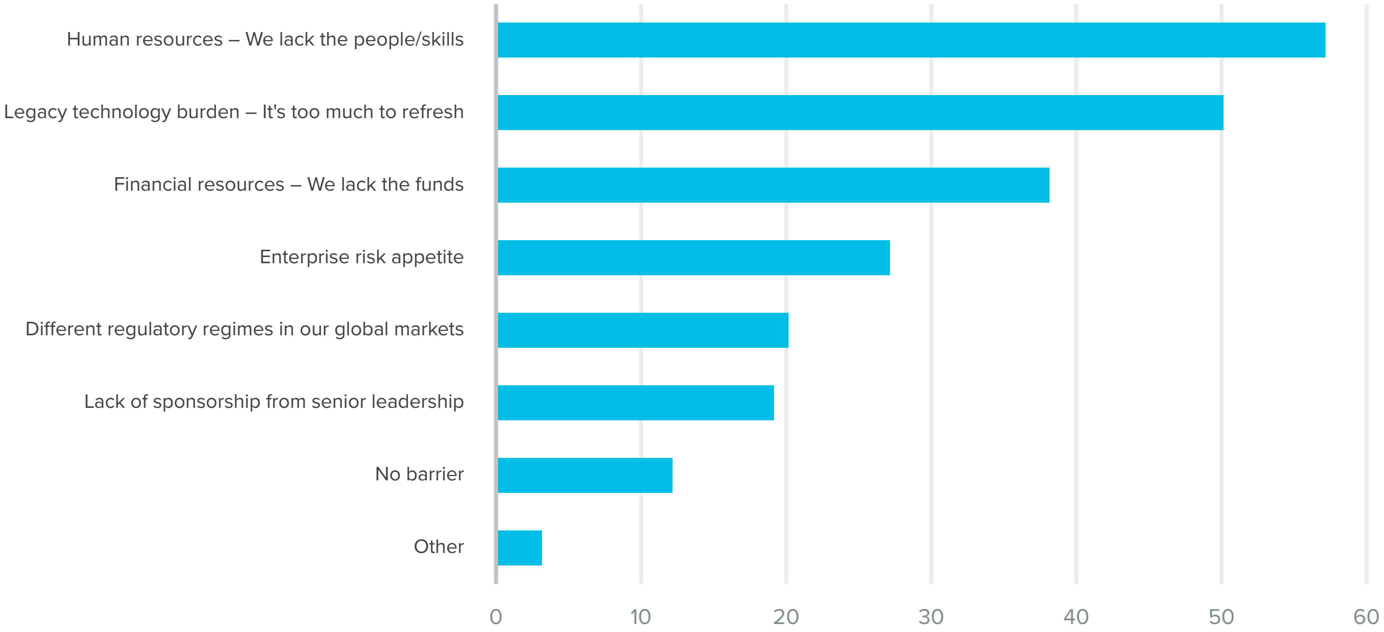
- Cloud migration of infrastructure and/or apps - 57%
- Enablement of new smart devices - 53%
- Secure new digital channels to customers and partners - 41%

What approaches and technologies have you invested in to better manage these operational risks?



Asked which approaches/technologies they have invested in to better manage these risks, respondents claim endpoint protection (72%), new awareness programs (65%) and cloud security (63%) as their top three.

What, if any, are the barriers inhibiting your digital transformation initiatives?



Finally, in this section, respondents are asked what, if any, barriers might inhibit these digital transformation initiatives they have declared. The top two responses – common themes again – are human resources (57%) and legacy technology burden (50%).

The next section showcases budgets and plans for further investments in 2022 and 2023.

The top two barriers that might inhibit declared digital transformation initiatives: human resources (57%) and legacy technology burden (50%)

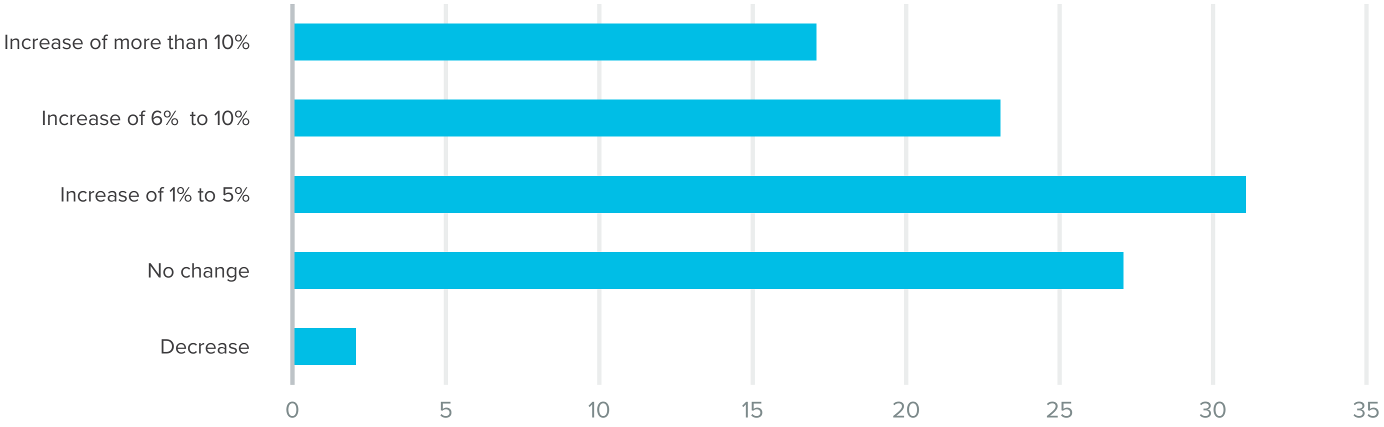
2022 Investments

Respondents paint an optimistic view of the future: 98% expect level or increased budgets for digital transformation initiatives in the year ahead. Key areas of planned investments:

- Cloud migration of infrastructure and/or apps - 56%
- Secure OT environments - 53%

Read on for further details about likely investments and the need for third-party assistance.

How will your budget for digital transformation initiatives change in 2022?

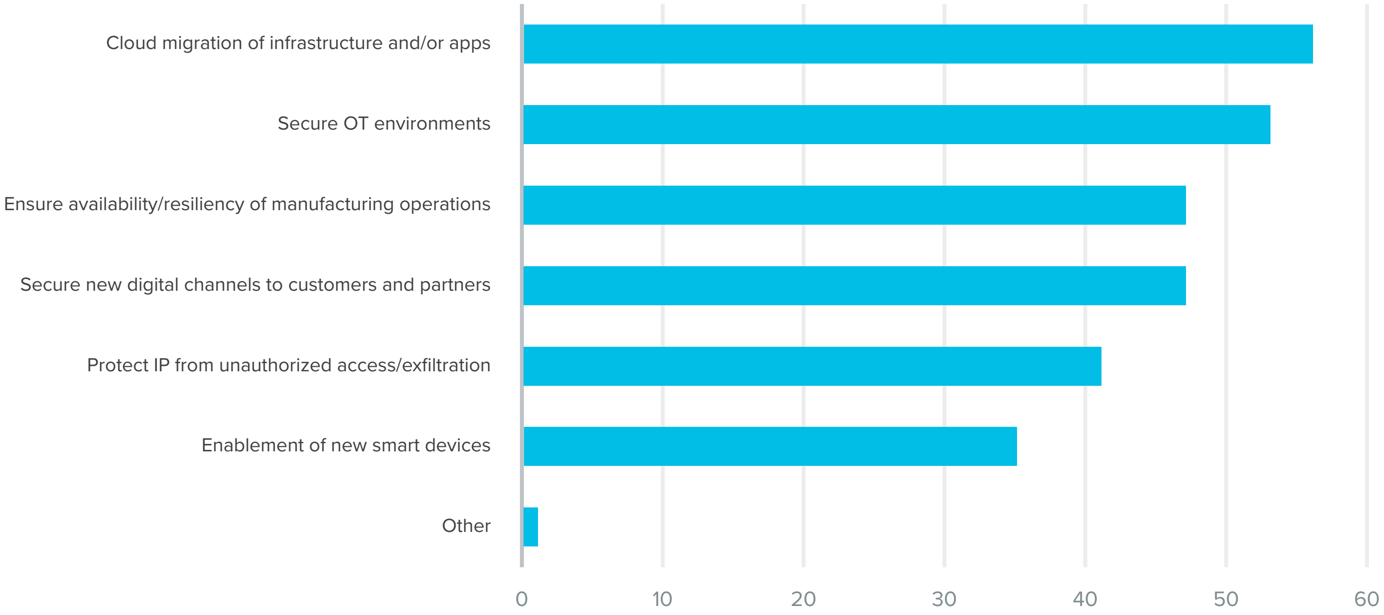


The appetite for digital transformation remains large. Nearly 100% of respondents expect steady or increased funding in the year ahead. Thirty-two percent foresee increases of 1% to 5%.

Where will those funds be earmarked?

When it comes to the budget, nearly 100% of respondents expect steady or increased funding in the year ahead.

What will be your enterprise's key areas of focus in terms of digital transformation initiatives in 2022?

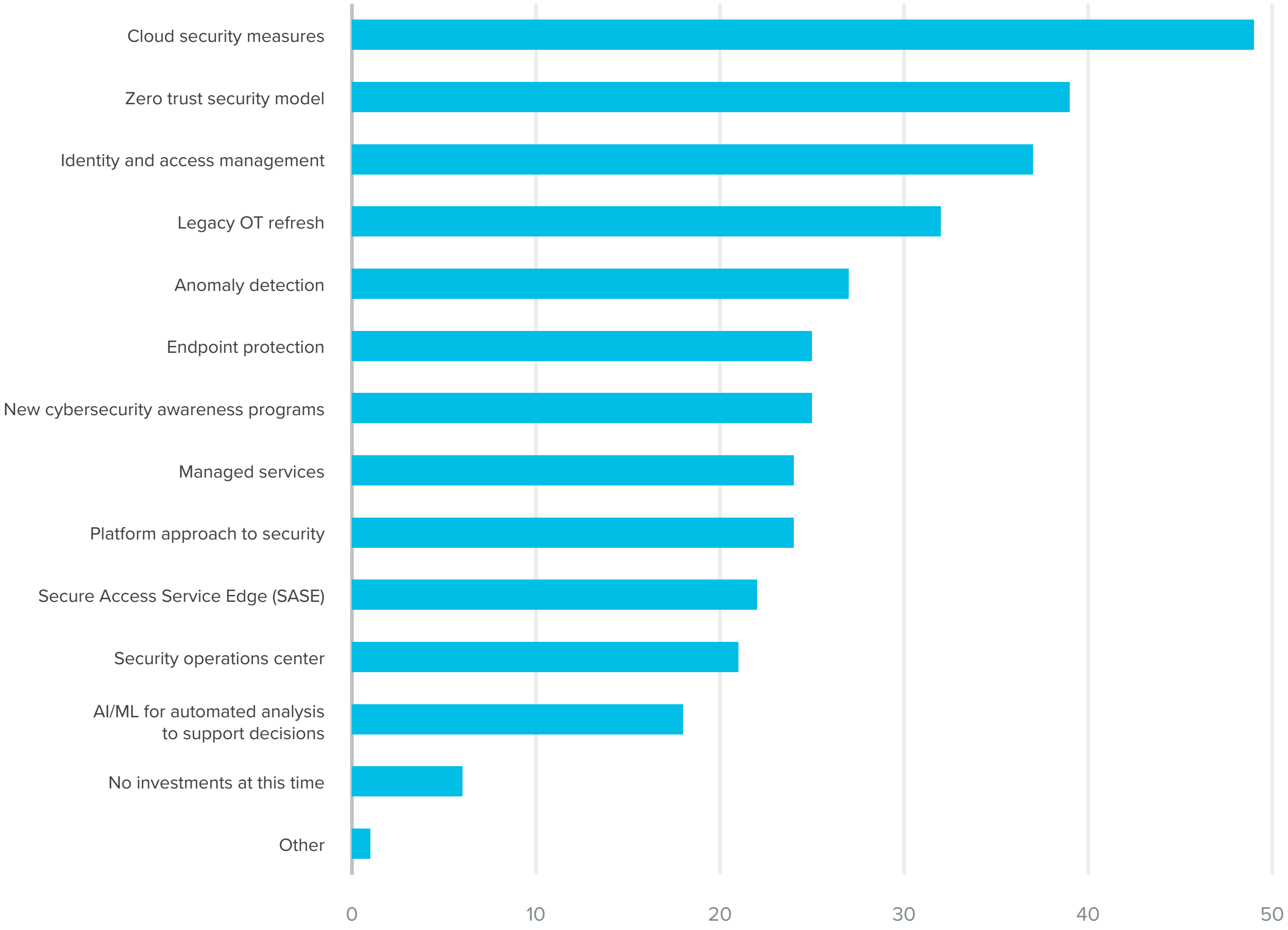


Top general areas of focus will be:

- Cloud migration of infrastructure and/or apps - 56%
- Secure OT environments - 53%
- Ensure availability/resiliency of manufacturing operations - 47%
- Secure new digital channels to customers and partners - 47%

The top two focus areas for digital transformation initiatives in 2022 are cloud migration of infrastructure and/or apps (56%) and secure OT environments (53).

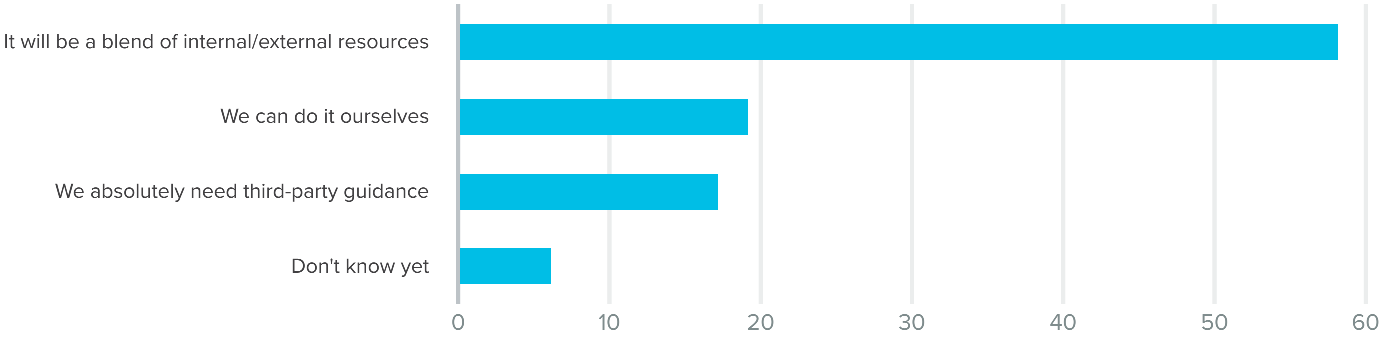
Which specific digital transformation investments do you expect to make in 2022?



The top three specific planned investments are:

- Cloud security measures - 49%
- Zero trust security model - 39%
- Identity and access management - 37%

14. Does your enterprise have the capacity to manage this transformation internally, or will you rely on third-party guidance?



A vast majority of respondents recognize that this Industry 4.0 journey is not one they will undertake alone. Only 19% of respondents say “we can do it ourselves.” Three-quarters of the survey pool (75%) say either that they absolutely need third-party guidance (17%) or that they will use a blend of internal/external resources (58%).

With these findings in mind, the next section details conclusions about the survey and how to consider the path forward for these manufacturing enterprises.

A vast majority of respondents recognize that this Industry 4.0 journey is not one they will undertake alone.

Conclusions

As this report winds down to conclusions and expert analysis, it is useful to revisit the statistics that opened this examination:

- 50% of survey respondents believe they are above average or superior when comparing their cybersecurity posture to peer enterprises.
- 80% say they either are well on the way or getting started toward becoming a "smart manufacturing company."
- 70% say their key digital transformation initiatives include cloud migration of infrastructure and/or apps.

Given these statements and an interpretation of the remainder of the survey responses, this study boils down to these conclusions:

The Future Is Now

Emboldened by their own ambition and boosted by two years of accelerated digital transformation, manufacturing entities are doing many of the right things to embrace Industry 4.0. Cloud migration, enhanced business resiliency, a focus on refreshing and securing legacy IT and OT environments – these are further steps toward becoming truly "smart" enterprises. The future will be defined by automation, smart devices and digitally connected supply chains. The biggest barrier between present and future is the delicate state of legacy technologies.

The Past Is a Burden

Whether legacy IT or OT, some systems cannot even be patched, so manufacturing companies are burdened by technologies that leave them vulnerable to attack. As organizations look to fulfill the goals they state in this report –cloud migration, enablement of smart devices, securing digital channels with customers and partners – they must address head-on the primary issues that will hold them back: human resources and legacy technology burden.

Smart Means Secure

As manufacturing enterprises seek to become "smarter" through their new digital transformation initiatives, they must simultaneously seek to be "more secure." Failure to emphasize smart manufacturing security is a plan to fail. Organizations must increase research and investment in

OT security – especially as they get into new frontiers for the smart manufacturing infrastructure, such as cloud, and as the threat from cybercriminals escalates.

The Path Forward Is in Partnership

As encouraging as it is to see organizations receive additional funding for digital transformation initiatives and have plans to embrace zero trust architecture as they expand cloud migration and improve IAM, budget and ambition alone will not overcome the deficit of human resources and the drawback of legacy technology. This is where partnerships can play a critical role, providing access to hardware, cloud apps/services and deep industry expertise. Three-quarters of survey respondents embrace this reality, saying they either need third-party guidance or will march forward with a blend of internal/external resources.

To quote Del Rodillas, global head, manufacturing and energy industry strategy and solutions at survey co-sponsor Palo Alto Networks: "Whether you are a smart manufacturer that's trying to look at security capabilities today, or trying to develop a plan for the future, we cover these elements and allow you to pick and choose what is most appropriate for your state, your maturity level."

In the next and final section, Rodillas and Paul Brownlee, North American lead, operational technology, Accenture, weigh in with their analysis of the survey findings and insights on how best to put them to work.

> "We allow you to pick and choose what is most appropriate for your state, your maturity level."
>
> Del Rodillas, Palo Alto Networks

SURVEY ANALYSIS

Securing Industry 4.0

Executive Insights on What Survey Results Mean – and How to Put Them to Work

ISMG's Tom Field discussed the survey results with Del Rodillas, global head, manufacturing and energy industry strategy and solutions, Palo Alto Networks, and Paul Brownlee, North American lead, operational technology, Accenture. This is an excerpt of that conversation.

The Results: Gut Reaction

TOM FIELD: What were your gut reactions to the survey responses? What surprised you most when you saw these?

DEL RODILLAS: What probably surprised me the most was the answer to the question that asked, "What are your enterprise's current areas of focus in terms of digital transformation?" What was strikingly low, in my opinion, was the focus on OT security, which was at 62% or something like that. To me, being security-minded, this needs to be more like 100%.

Considering just job number one in manufacturing is keeping uptime high – where you can have actual physical downtime if something bad happened – with that potential impact in play, I would've thought that over 90% would've been more sensitive or prioritizing that aspect of the work activities.

Smart Companies

FIELD: Eighty percent of the respondents said that they're either well on their way or getting started toward becoming a smart manufacturing company. How does that stat compare to what you see across sectors?

RODILLAS: It's very encouraging, first of all, to hear that many of the respondents are modernizing. But from my standpoint, it's probably a little bit more accelerated than what I thought it would be. If you had asked me a few years ago what I was seeing, I would say people were still quite hesitant to go into a deep dive in things, for example, with IoT. But just about every customer that I'm talking to right now has some kind of IoT initiative that they're either in the middle of doing or planning.

PAUL BROWNLEE: I see lots of folks doing POCs. Some are at scale, but most are disjointed efforts that are not centralized or driven by IT. In POCs, security gets overlooked and when they go to scale it, that becomes a problem. Security should be an enabler if you do it upfront. DevSecOps is making a big difference. Every company is a developer these days and needs to enable OT end to end.

Survey Priorities

FIELD: In our survey, there were three consistent areas of focus in the responses: cloud migration, OT environments and ensuring availability and resiliency. How do these jibe with the trends you see?

RODILLAS: Yes, absolutely availability, resiliency. That is not surprising to me. I see a lot of investments around predictive maintenance, where organizations are trying to see when their asset might be breaking down or when their asset may be needing some kind of servicing so that they could prevent a “lines down” situation and extend the life of their equipment. To me, there are a lot of huge returns on that. Others are also using digital twin technologies to model their systems and also anticipate any disruptions or breakdown. So definitely anything that can help along those lines, I see a lot of manufacturers ready to invest there.

If you look at the cloud migration, a lot of the brains or the machine learning or the big data is happening in the cloud. So it doesn’t surprise me that a lot of organizations are starting to be more cloud-connected from their manufacturing environments. That’s where the server resources reside, and a lot of these guys don’t want to develop these apps themselves in a local data center. They treat this as a software as a service, so that definitely makes sense.

BROWNLEE: What companies move to the cloud differs by industry and company. You need to understand where the edge is on what to move to the cloud. This is also true with OT. The benefits outweigh the costs. One area to think about is continuity planning. Everyone wants to increase uptime, and everyone has experienced the impact of downtime. Business continuity security planning is vital for success in these three areas.

The Barriers

FIELD: What barriers do you typically see inhibiting any organization’s digital transformation initiatives?

RODILLAS: The obvious ones: Funding and headcount are really limited. You have to triage where you want to put these people. It’s hard not only in smart manufacturing, but even cybersecurity for smart manufacturing, which is even more of a unicorn profile in terms of talent.

The other one that I’ve seen, that’s more directly in my line of work as far as investment in security, is being able to manage cyber risk. So I ran into an end user who had invested millions of dollars on a homegrown IoT solution. They did a pilot on one production line, and they were ready to roll that out. And then the CIO stepped in and said, “Well, if we had some kind of a cyberthreat on one

> “Just about every customer that I’m talking to right now has some kind of IoT initiative that they’re either in the middle of doing or planning.”
>
> – Del Rodillas

> “The main issue with all legacy equipment is not addressed or solved by any of the top three investments noted. For example, endpoint protection doesn’t make its way into OT.”
>
> – Paul Brownlee

of our lines being sourced from this IoT system, would we be able to prevent that from pivoting across all of the lines?” The answer was no, because the reality is that in a lot of manufacturing environments, the factory floor is a big flat network. That has to do with a lot of the historical reasons for when they created the network to begin with. But I see a lot of organizations holding back the modernization because they don’t have a good cybersecurity system in place to protect the factory.

The last piece that I see as an inhibiting factor is when the IT teams and the OT teams don’t work together. They may be at odds in terms of getting something out and getting the returns, and making it very easy to access – high availability versus managing the cyber risk and having some controls. Sometimes these things are at odds, and when there’s no agreement, it might prevent progress.

BROWNLEE: Three key areas:

- Outdated infrastructure;
- Scalability (POC to scale) across multiple locations or enterprisewide;
- Seeing security as an enabler, not as an inhibitor.

Threat Landscape

FIELD: What do you see as the dominant threats to these environments?

RODILLAS: Manufacturing has a lot of legacy systems and vulnerabilities. And as the connectivity increases from the factory floor out into the cloud, you’re going to have a bigger attack surface. So the biggest threat that I see is attacks that use ransomware. The cybercriminals have begun to pick up on the mother lode that exists there in terms of extracted ransom, because organizations, if they’re losing tens of thousands, hundreds of thousands, maybe even millions of dollars by the hour – to ask for $5 million, $10 million is nothing compared to what the downside is for that organization.

BROWNLEE: Again, three key points:

- Lack of personnel with skills, and accidental/self-inflected wounds due mainly to manufacturing not being connected into IT;
- Change management and thinking through how jobs are changing based on a mature IT program extending into OT;
- Understanding the life cycle of IT assets versus physical assets. There are different replacement times for IT and OT equipment. Legacy systems are not hardened to known vulnerabilities today.

Future Investments

FIELD: How do you respond to the investments the respondents identified as their defensive priorities for the coming year?

BROWNLEE: The main issue with all legacy equipment is not addressed or solved by any of the top three investments noted. For example, endpoint protection doesn’t make its way into OT.

RODILLAS: I saw a good portion of organizations that wanted to develop that employee awareness just to make sure they knew what some of the cyber risks were. And I think that’s pretty standard. I also saw some organizations put emphasis on the actual end devices, what they call endpoint security. It’s another great place. And with respect to endpoint security, you need to consider that your old endpoint security technologies, like antivirus and host IPS, which were based on known signatures, are not so useful these days, especially as attackers develop new attacks that static solutions are incapable of detecting.

Also, look at these technologies that allow you to detect the zero-days or these malicious behaviors where things like machine learning-based tools and sandboxing technologies can be really useful. I speak a lot about zero trust when I engage with our manufacturing users to help them understand what it is and the benefits in terms of being able to manage your risk, reduce your attack surface and increase your protection surface.

> "I speak a lot about zero trust when I engage with our manufacturing users to help them understand what it is and the benefits."
>
> – Del Rodillas

Looking Forward

FIELD: What are your recommendations that the audience consider to enhance their abilities to be able to secure Industry 4.0?

BROWNLEE: Focusing on the right thing – availability, security – is not the problem. The "how to" is where the issue lies. So is understanding where to stop so you are managing risk to a reasonable level and can then continue to monitor, making sure the risk stays in balance.

RODILLAS: It's important to collaborate with the operations side of the house and understand the areas that they're investing in, and develop your plan and your security investment plan around an aligned approach or aligned set of priorities. When we look at the technologies that are out there, the most important one – going back to this concept of zero trust – is thinking about what tools can help you realize the controls that you need to get that granular.

So things like next-generation firewalls are concepts that may have had a lot of usage already on the IT side but are very relevant to the smart manufacturing environments, where very granular policies can be applied to the traffic that you would find in a factory floor, to the devices that you would find, to the way that users interact in a much more granular level than may have existed in the past.

The other area that organizations need to think about, and it's coming up quick as we see more modernization, is the move of the factory floor or the operational technology environment up into the cloud, up into 5G, as IoT usage increases. Cloud-based security is not well understood by most operations in organizations. But in order to have this completeness of security, securing the cloud environment and understanding your potential exposure is going to be critical, especially as you're trying to modernize and become smart.

Partnership

FIELD: What role do you see for partners such as yourself?

RODILLAS: From what we hear, a lot of organizations are being challenged because they don't have the resources or the know-how. And for them to try to develop that internally is going to be a pretty tall order. You don't necessarily have that time. Attackers aren't sleeping. So I don't think waiting is an option. I think where you can make the most of that is to try to bring in some expertise, because a little awareness and offloading of work to experts can go a long way. Service providers have a very important role in helping organizations quickly get their security posture up to a certain workable level and educating them to do that function on their own.

BROWNLEE: Capability and scale are two big issues for clients. Service providers can help with the transformation journey as well as with the transition to ongoing management.

About Palo Alto Networks

FIELD: What do you want our audience to know specifically about Palo Alto Networks and Accenture Security, and how you're helping customers to secure Industry 4.0?

RODILLAS: Palo Alto Networks had its roots in the IT environment. A lot of organizations may not be familiar with what we do for OT. And we have over 11,000 manufacturing customers; a good portion of them use us for both IT and OT. Our core technology, the next-generation firewall, allows you to get better visibility and segmentation into your plant environments in a way that's minimally disruptive. You don't have to redesign your network. You could overlay our technology and get that next-generation security in a minimally disruptive way. And we also have technologies that allow you to secure the cloud as you expand your OT into the cloud, get a sense of what kind of attack surface and manage that attack surface more effectively. If you modernize for IoT or 5G or SD-WAN, the same technology is available. Our firewall is a platform. And we also have capabilities to help you automate a lot of these capabilities or security functions via our Cortex platform.

We have the network security, which is our Strata offering; our cloud security, which is our Prisma offering; and our SOC offering, which is our Cortex. Together, these three capabilities make up our portfolio. And whether you are a smart manufacturer that's trying to look at security capabilities today, or trying to develop a plan for the future, we cover these elements and allow you to pick and choose what is most appropriate for your state, your maturity level.

BROWNLEE: Two key takeaways:

- End-to-end security services from cloud/platform/data/OT security;
- Working with Accenture's Industry X teams to build smart manufacturing solutions with security included from the beginning.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organisation devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU INFO SECURITY® Just for Credit Unions GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk® TODAY CAREERS INFO SECURITY® ~~Data Breach~~. Prevention. Response. Notification. TODAY CyberEd.io

iSMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io