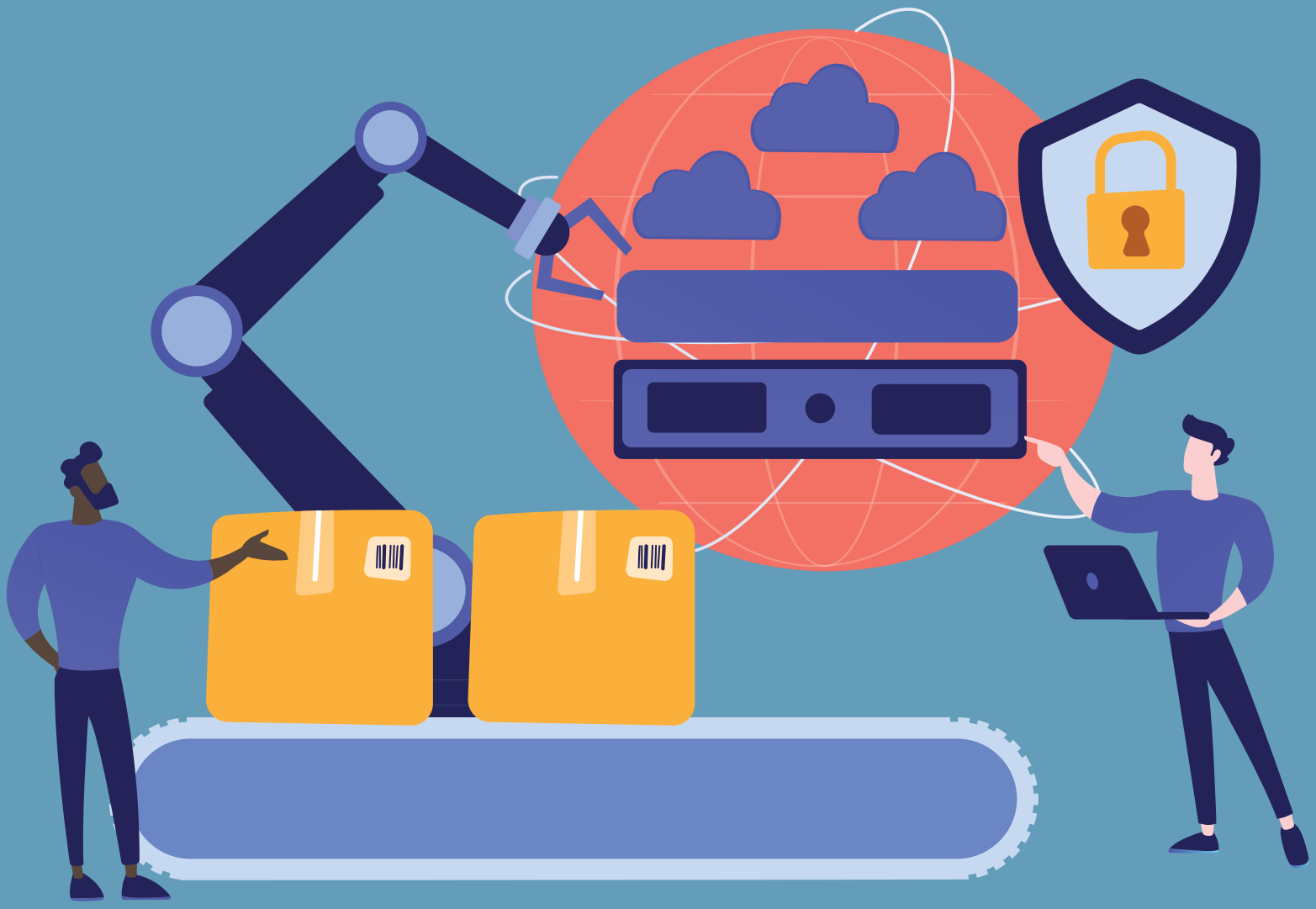
OCTOBER 2026

WHITE PAPER

Securing the Line: Managing Cybersecurity in Packaging and Processing Operations



PMMI Business Intelligence

BENEFACTOR PMMI FOUNDATION VISIONARY

pmmi.org/business-intelligence

CONTENTS

3 About the Report

3 Part One: Building Cybersecurity Into Equipment Requirements

6 Part Two: Preparing to Restore Production After an Incident

8 Conclusion

9 Additional Session Insights

ABOUT PMMI

PMMI is the leading global trade association for the packaging and processing industries. Our core purpose is to unite the packaging and processing industries across the supply chain, helping our members to exchange knowledge and ideas so that they can continue to succeed in a rapidly evolving global market. We represent over 1,000 companies from across the value chain, and we work with them every day to ensure they can keep on developing innovative manufacturing solutions.

ABOUT VISION 2030

PMMI's Vision 2030 focuses on the discovery, discussion and solutions to the industry's most significant challenges for OEMs and CPGs. It is a critical component of PMMI's suite of continuous improvement forums for its members and the consumer packaged goods (CPG) companies they serve.

Publication Date: October 2026

Jorge Izquierdo, Vice President, Market Development, PMMI
Rebecca Marquez, Director, Custom Research, PMMI
Grace Lee, Manager, Market Research, PMMI
Andrea Admana, Manager, Market Development, PMMI

© Copyright 2026 PMMI, The Association for Packaging and Processing Technologies, Inc. All rights reserved. The information contained herein shall not be distributed or shared by the recipient. No part of this document may be reproduced without the express written permission of PMMI.

About This Report

As packaging and processing systems become more connected, cybersecurity decisions increasingly intersect with equipment specifications, remote support, maintenance, and production recovery. A security issue can become an operational issue when it affects equipment availability or the ability to restart a line safely.

At a PMMI Vision 2030 Discovery Session during PACK EXPO International 2026, End Users and industry suppliers discussed two practical questions: What cybersecurity expectations belong in equipment requirements, and what information and coordination are needed to restore production after an incident? A facilitated panel discussion, roundtable conversations, and live polling informed the themes presented here.

The findings reflect participant experiences and priorities rather than a representative survey of the packaging and processing industry. Poll questions permitted multiple selections, so percentages should not be added together.

Two operational questions

1 What cybersecurity expectations belong in equipment requirements?

2 What information and coordination are needed to restore production?

Part One | Building Cybersecurity Into Equipment Requirements

Cybersecurity decisions made during procurement can shape integration and support

Cybersecurity expectations are not limited to the moment equipment connects to a plant network. They can influence the components specified, communication architecture, access permissions, and the ability of a supplier to support equipment after installation. Session participants described how requirements that emerge late in the purchasing process can create avoidable rework and negotiation.

One roundtable described equipment arriving with a remote-access arrangement that did not align with the plant's requirements. The teams worked through an alternative access approach and network configuration. Another discussion highlighted the value of settling controls-platform and program-access questions while equipment specifications are being developed. Both examples show how earlier communication can help avoid later changes.

Early coordination can help reconcile two legitimate operational needs. End Users often seek consistent cybersecurity and network practices across their facilities, while OEMs need reliable ways

to service equipment across customer sites with different requirements. Participants emphasized working through these expectations together so remote support can be both appropriately controlled and practical when a machine needs attention.

Remote access requires both secure controls and workable service arrangements

Remote connectivity can support troubleshooting and equipment service, but the discussions showed that the method of connection matters. Participants raised authentication, approval of access, visibility into remote activity, and compatibility with plant networking policies. The practical question is not simply whether remote access is permitted; it is how an authorized supplier can obtain the access needed to support a machine under the End User's security requirements.

Participants described secure remote support as a shared design consideration. Access methods need to fit the plant's cybersecurity practices while enabling equipment suppliers to provide timely troubleshooting and service. Defining the approach together can make both objectives easier to achieve.

PLANT NEEDS	**SHARED ARRANGEMENT**	SUPPLIER NEEDS
Security policies • Access approvals • Network standards	**Secure, workable remote support**	Timely service • Troubleshooting • Equipment expertise

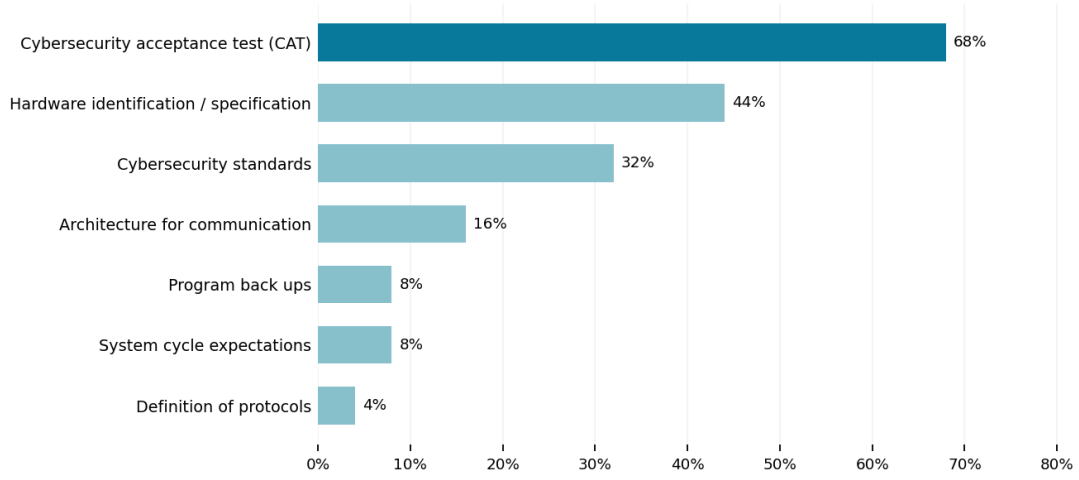
Illustration of complementary plant and equipment-service considerations raised during the session.

Acceptance testing emerged as a leading specification priority

Participants also discussed how to confirm that agreed cybersecurity requirements have been implemented. One proposal was to incorporate a cybersecurity acceptance test alongside established factory and site acceptance activities. The intent was to check relevant equipment and connectivity requirements before a machine is treated as ready for operation.

In a live multiple-selection poll, cybersecurity acceptance testing was the most frequently selected equipment-specification priority (68%; 17 of 25 respondents). Hardware identification/specification was selected by 44%, cybersecurity standards by 32%, and communication architecture by 16%. The poll reflects the priorities of this session's respondents, not an industry-wide ranking.

Equipment-specification priorities



Poll question: What cybersecurity requirements should be included in equipment specifications, factory acceptance testing, site acceptance testing and service agreements? n=25; multiple selections permitted.

Taken together, the discussions point to a broader definition of equipment readiness: not only whether a machine performs its intended function, but whether its connections, components, and access arrangements align with the operating environment.

Equipment longevity makes cybersecurity an ongoing consideration

The cybersecurity requirements established at purchase do not remain static over the life of a production asset. Participants discussed the difficulty of maintaining equipment as software versions, firmware, controls hardware, and supplier support change. Older devices may be difficult to patch or replace, and upgrades must be evaluated against compatibility and production needs.

Roundtable examples included aging controllers and unsupported software that could not be modernized easily without cost or disruption. Participants also noted that changes need to be tested carefully so a security-related update does not unintentionally affect equipment performance. The implication is that long-term supportability belongs in the same conversation as initial security specifications.

Part Two | Preparing to Restore Production After an Incident

A backup is only useful when it reflects the system that must be restored

When discussion shifted from prevention to recovery, participants focused on a deceptively simple question: What information would be needed to put the equipment back into a known, usable condition? PLC programs are part of that answer, but they may not be sufficient. Machine settings, firmware, network configurations, operator-interface files, recipes, and other critical information may also be necessary, depending on the equipment and process.

Participants distinguished between possessing a backup and possessing the correct backup. One table described how an original factory acceptance test file could become outdated after changes made during site acceptance and subsequent operations. If those changes are not captured, the available file may no longer represent the production system that needs to be recovered.

> *"Anything that has any kind of brain or IP address, you need to know what the backup is, or where to, or where to get it."*
>
> —Session participant

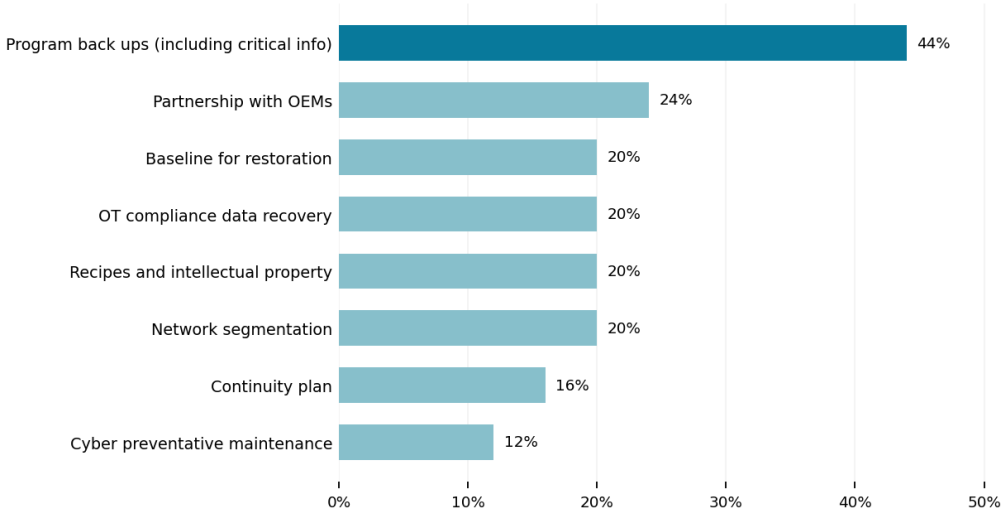
Programs / logic	Firmware / versions	Machine settings
Network configurations	Recipes / critical data	Verification records

Examples of information participants said may be needed to restore a production system; requirements vary by application.

The recovery discussion also included the value of maintaining backups that remain available if connected systems are compromised. Several participants described the need to identify where recoverable copies reside and who is responsible for keeping them current.

Recovery priorities

In the recovery-priorities poll, 44% of respondents selected program backups, including critical information. OEM partnership was selected by 24%, while restoration baselines, OT compliance data recovery, recipes or intellectual property, and network segmentation each received 20%. As with the specification poll, participants could select more than one item.



Poll question: What backups, equipment configurations, documentation and recovery procedures are necessary to restore a line safely and efficiently? n=25; multiple selections permitted.

Restoring equipment is not the same as safely restarting production

A recovered controller or computer may not by itself establish that a line is ready to operate. Participants emphasized the need to verify process conditions, operating parameters, and the integrity of information used to run production. This distinction is particularly important where incorrect settings or missing data could affect product quality or food safety.

The panel discussion contrasted restoring equipment functionality with confirming that the production process can resume safely. The relevant checks will vary by application: restarting a material-handling or packaging device is not necessarily the same task as restoring controls that govern critical processing conditions. The session did not establish one universal recovery procedure; it highlighted the need to understand what must be validated for a particular operation.

Recovery therefore depends on both technical restoration and operational verification. The discussion suggests that a useful recovery baseline includes not just software files, but the information needed to determine whether the restored system is functioning as intended.

Clear ownership and practiced coordination strengthen recovery readiness

Participants emphasized how recovery can require contributions from IT, OT and automation specialists, maintenance teams, and equipment suppliers. The appropriate roles depend on the systems involved and the organization's own arrangements. A recurring theme was the value of agreeing on responsibilities and points of contact before an incident, so each team can contribute its expertise during recovery.

> *"If this happens, who's responsible for what? Do they have the right context? Do they know who to talk to to get this resolved quickly?"*
>
> — Session participant

One roundtable emphasized that maintenance personnel may be the people physically working on equipment even when IT or automation teams own the restoration process. Another discussed incorporating recovery tests into site acceptance or preventive-maintenance activities. These comments point to the value of procedures that are understandable to the teams expected to use them, rather than plans that exist only as documents.

Equipment suppliers may contribute specialized knowledge of controls, configurations, and equipment-specific checks, while plant teams provide the operational context for restoration and restart. Participants described the value of coordinating these contributions within established access and incident-response arrangements. The central point was not that responsibility sits with one group, but that the different capabilities needed for recovery should work together.

Conclusion | Cybersecurity Readiness Spans the Equipment Lifecycle

The Vision 2030 discussion connected two issues that are often considered separately: defining cybersecurity expectations when equipment is purchased, and preparing to restore production if systems are disrupted. In both cases, participants returned to the same underlying need—clear information, agreed responsibilities, and practical coordination between End Users and their equipment and technology partners.

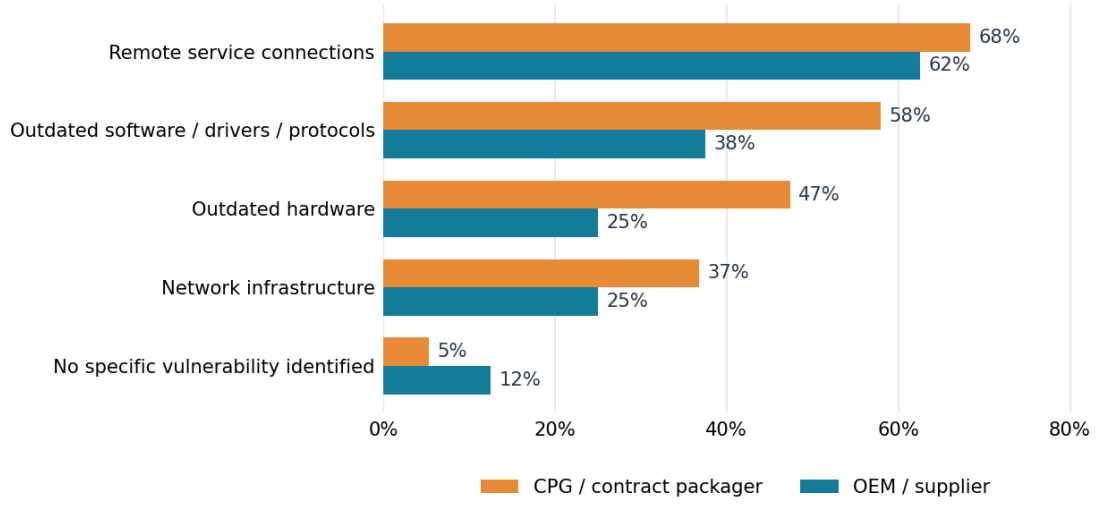
Across procurement, equipment operation, and recovery, the session highlighted opportunities for End Users, OEMs, component suppliers, and other technology partners to plan together. Clear specifications establish a common starting point; acceptance activities help test shared expectations; lifecycle discussions anticipate changing equipment needs; and recovery planning connects technical restoration with safe operational restart. Cybersecurity readiness emerges from these complementary efforts—not from any single team acting alone.

Additional Session Insights

Pre-registration feedback and live audience polls add context to the session discussions. These results describe the people who answered each question and should not be treated as representative industry estimates.

Pre-registration: Perceived cyber vulnerabilities

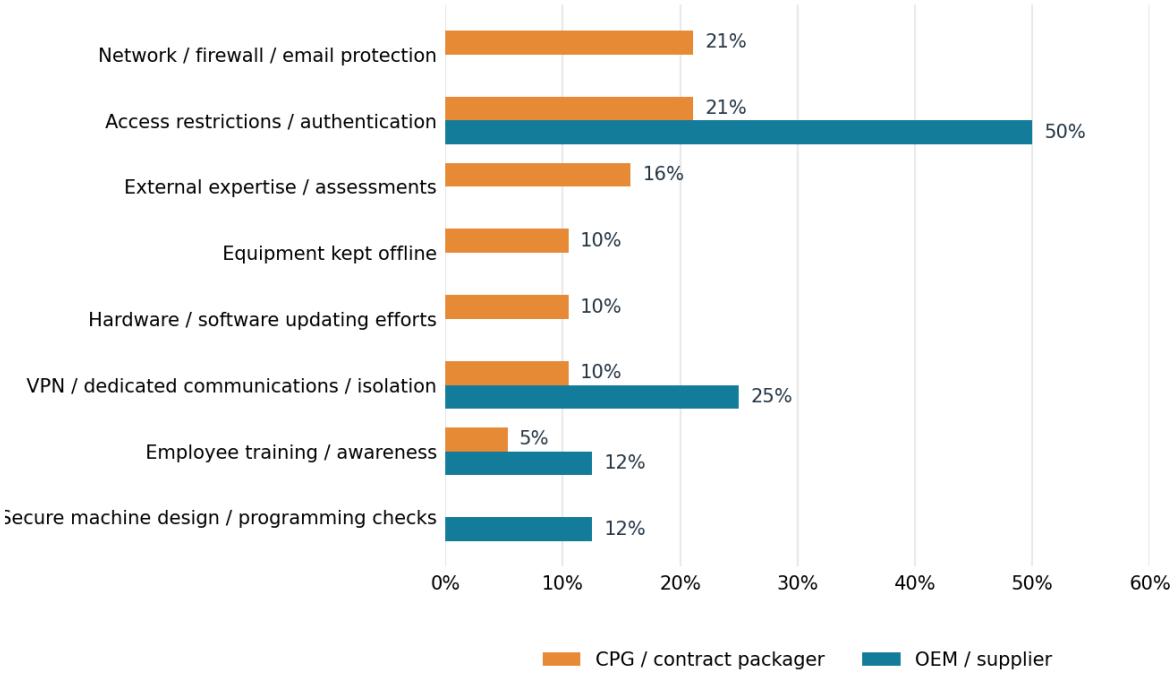
Across both respondent groups, remote service connections were the most frequently identified vulnerability. These responses were collected before the facilitated discussion and provide context for the emphasis on secure, workable remote access in Part One.



Pre-registration question: What do you think are the most significant cyber vulnerabilities in your operations? (If a cyberattack has occurred in your operations, where did it happen?)

Pre-registration: Protection measures underway

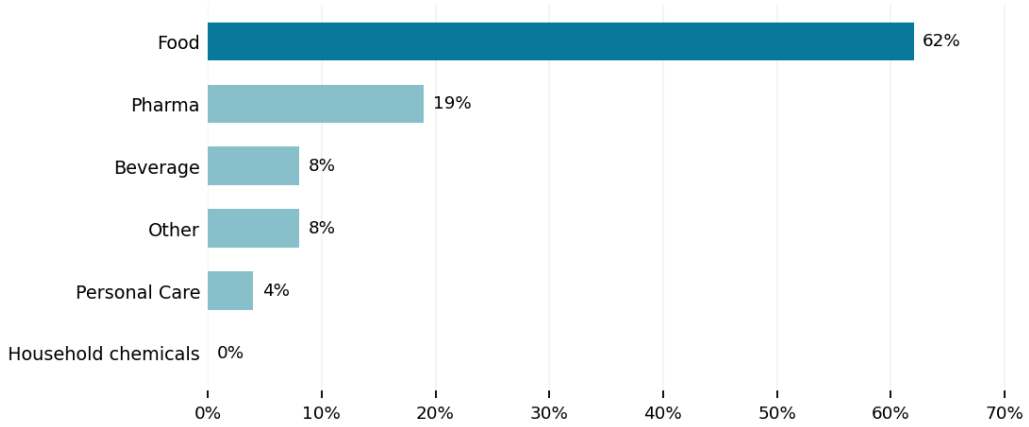
Respondents reported a range of security practices, including authentication and access restrictions, network protection, isolated connections, training, and equipment-related measures. The group comparisons are descriptive; some response categories may reflect how open-ended answers were classified.



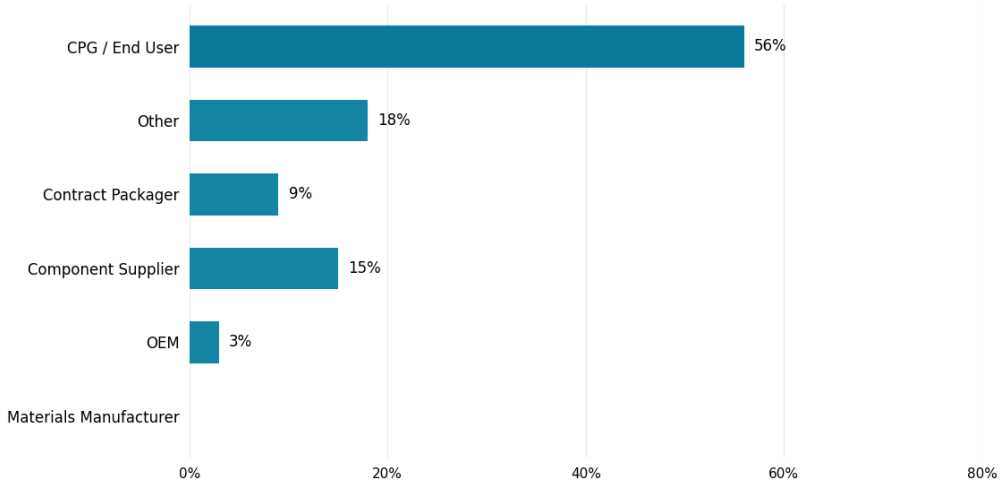
Pre-registration question: What has your company done to protect from cybersecurity incidents in your operations?

Who attended this Vision 2030 session?

The following charts provide a snapshot of the industries and company types represented at this Vision 2030 session, based on live polling responses. Respondent counts varied by question, so the results do not represent a complete attendee roster.



Live polling: What is your primary industry or industry you serve? n=26. Percentages are rounded and may total more than 100%.



Live polling: Which of these best describes your company? n=34.

PMMI Business Intelligence

PMMI HEADQUARTERS
12930 Worldgate Dr., Suite 200
Herndon, Virginia 20170
(571) 612-3200
businessintelligence@pmmi.org
www.pmmi.org

PMMI LATIN AMERICA
Homero 418 Piso 7
Col. Miguel Chapultepec
Miguel Hidalgo, D.F. 11570 Mexico
+ (52 55) 5545 4254

Visit PMMI's Business Intelligence Library for More!

Our most recent white papers



Managing Obsolescence



The Ripple Effect



From Complexity to Capability

For more information, contact:

Contact Rebecca Marquez, Director, Custom Research
Phone: 571-612-3205 Email: rmarquez@pmmi.org

Visit pmmi.org