FOOD PROCESSING

SPECIAL REPORT

The State of Cybersecurity in the Food & Beverage Industry

Sponsored by

FORTINET DRAGOS

Our Survey Gauges the State of Cybersecurity in the Food & Beverage Industry

As the industry increases its internet connectivity, it recognizes the need to ramp up protection against attacks.

By Food Processing

As the food & beverage industry works to catch up with other industries in general adoption of internet technologies (remote monitoring, cloud-based computing, Industrial Internet of Things), it's also ramping up its safeguards against cyberattacks.

Among 13 possible "technological improvements" listed in a survey undertaken by ***Food Processing*** and commissioned by cybersecurity technology leaders Dragos and Fortinet, cybersecurity was the highest priority for the

FIGURE 1

In which areas of technology does your agency/organization plan to invest or improve over the following timeframes?

	SHORT-TERM (0-12 MONTHS)	MEDIUM-TERM (1-2 YEARS)	LONG-TERM (3-5 YEARS)	NO PLANS TO INVEST
Machine/plant connectivity software	17%	28%	44%	11%
Enterprise resource planning	18%	36%	33%	13%
Business intelligence analytics platform	10%	36%	32%	21%
Internet of Things (IoT) solutions	14%	33%	30%	24%
Cybersecurity	30%	33%	30%	8%
Cloud computing	16%	36%	28%	21%
AI and digital twins	9%	26%	28%	38%
Asset management software	16%	32%	31%	22%
Computerized maintenance management systems (CMMS)	17%	31%	31%	22%
Utility billing/Customer interface	15%	33%	27%	26%
Software to integrate data silos	13%	28%	34%	26%
Process resiliency	11%	35%	34%	21%
Process safety	21%	27%	32%	20%

shortest term (over the next 0-12 months). It also received the most votes overall when adding together short-, medium- and long-term investments: 93% of respondents said they plan to invest in cybersecurity within five years. No other technology (see Fig. 1) received more than 89% of votes, although machine/plant connectivity was close.

That's no surprise considering respondents felt the potential exposure to cyberattacks is increasing. 14% say it has increased substantially and 33% see it increasing moderately; 44% believe the threat is about the same (see Fig. 2).

And 71% are worried that a cyberattack will result in harm to consumers, rather than just a financial or operational burden to the company; 25% are *very* worried (Fig. 3).

The general tone of the survey results showed the food & beverage industry is working to improve its digital connectivity. Nearly 90% of respondents said their companies give access to company servers and processes to personal devices and other remote devices (Fig. 10). As a result, concern is growing over the possibility of cyberattacks. Currently, the perceived threats are malware and ransomware (Fig. 11), and the foreseen repercussions (Fig. 4) are loss of productivity, loss of revenue, service interruptions and compliance issues. Food safety

FIGURE 2

Over the last 12 months, the potential security exposure to cyberattacks on my agency or organization has:

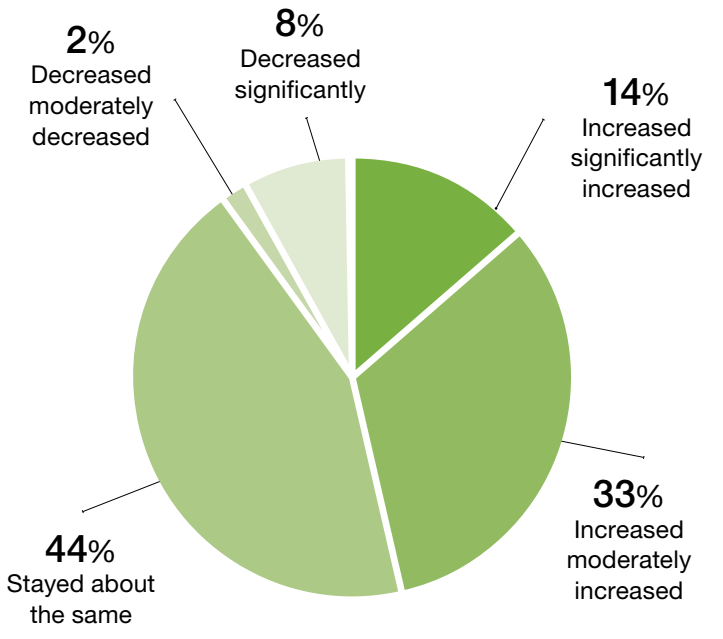
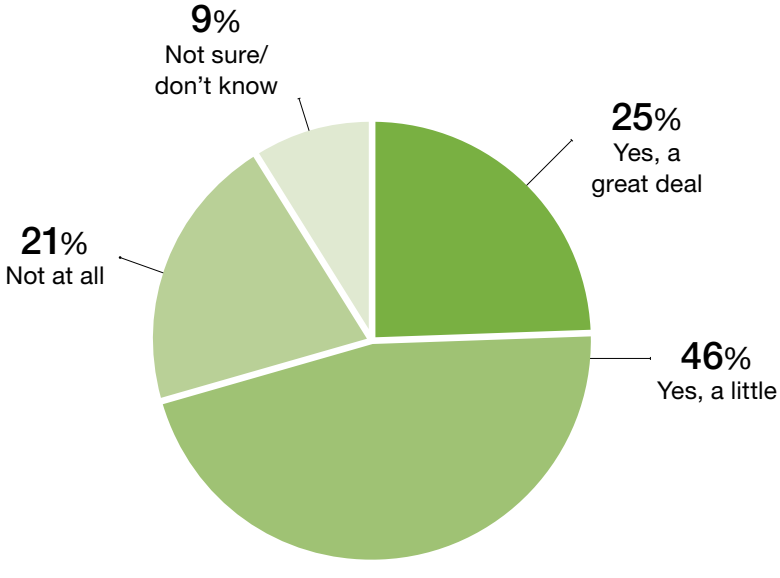


FIGURE 3

How worried are you that a cyberattack will result in harm to consumers rather than extortion (ransomware)?



concerns ("Threat to population/ public health") are surprisingly far down the list.

"Malware, ransomware in particular, have become a top priority for the industrial cybersecurity industry," says Kyle O'Meara, Principal Adversary Hunter at Dragos (www.dragos.com). "Having complete visibility of your OT network's assets, coupled with incident detection and event notification are critical steps in preventing these kind of threats."

Despite some recent high-profile incidents (JBS, MolsonCoors, Arizona Beverages, Schreiber Foods), the plurality of respondents (32%) reported no cyber incident in the past 12 months, and another 22% reported only one. In nearly half of those cases, the cause remains unknown; 42% said it was the result of phishing. Only 22% said it was a targeted attack – the result of an intruder trolling IP addresses for vulnerabilities (Fig. 5).

There were two top challenges to making progress on cybersecurity issues. Both "too much focus on running current operations" and "no perceived need by end users" were called either "challenging" or "very challenging" issues preventing more attention paid to cybersecurity (Fig. 12). Close behind was "poor understanding of what needs to change" (70%).

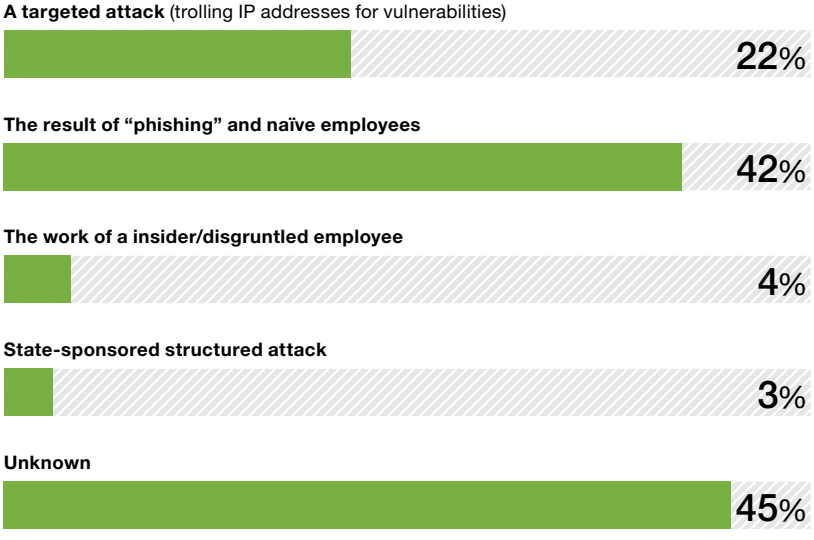
FIGURE 4

When it comes to cybersecurity concerns, how important are the following to your agency or organization?

	NOT AT ALL IMPORTANT	SOMEWHAT IMPORTANT	VERY IMPORTANT
Service interruptions	0%	31%	69%
Loss of productivity	2%	24%	74%
Threat to population / public health	10%	38%	53%
Product quality	4%	33%	63%
Corporate liability	1%	37%	62%
Compliance issues	4%	28%	68%
Loss of revenue	5%	24%	71%
Reputational harm	7%	28%	65%

FIGURE 5

What provoked any recent incidents?



"While most organizations recognize the need for diligence when defending from cyberattack, many seem to lack knowledge of what systems and processes need to be protected," says Chris Blauvelt, Director of Operational Technology for Fortinet (www.fortinet.com).

Surprisingly, 24% of respondents say their companies give no structured training in these issues to employees (Fig. 13). Another 18% termed it "casual continuing education though IT." 41% employ a required but internal program provided through their IT departments, and 18% were using third-party training required for all employees.

FIGURE 6

How would you describe your agency or organization's adoption of digital transformation technologies compared to others in your industry?

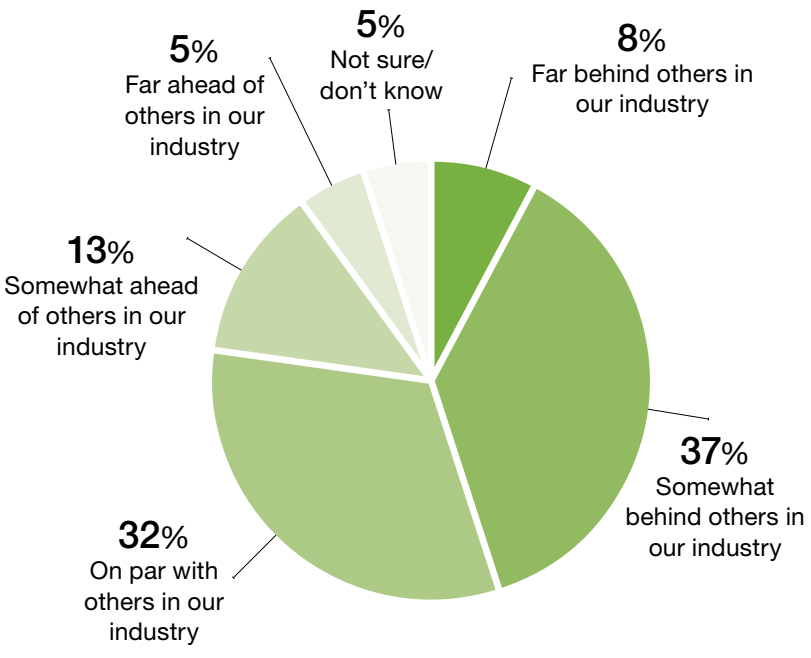


FIGURE 7

In which areas of cybersecurity does your agency/organization plan to invest or improve over the following timeframes?

	SHORT-TERM (0-12 MONTHS)	MEDIUM-TERM (1-2 YEARS)	LONG-TERM (3-5 YEARS)	NO PLANS TO INVEST
Network/asset visibility	28%	33%	20%	20%
Network/asset protection	34%	32%	22%	11%
Incident detection	40%	25%	22%	13%
Incident response	34%	28%	24%	15%
Incident recovery	33%	26%	28%	14%
Threat hunting	25%	26%	26%	25%
Response automation	20%	29%	29%	23%

BEHIND THE DIGITAL CURVE

Food & beverage processing has a reputation for being behind other industries in automation in general and digital transformation in particular. 45% of survey respondents think their organization is somewhat behind or far behind others in the industry in adoption of digital transformation technologies (Fig. 6).

For example, 38% have no plans to invest in the concepts of artificial intelligence and digital twins. 24% do not even see the need for the Industrial Internet of Things. 26% have no plans to invest in utility billing/customer interface nor software to integrate data silos.

Despite those answers, 92% of respondents voiced support for investment in cybersecurity, as we mentioned up front: 30% saying it's budgeted for in the next 0-12 months (the highest-ranked answer to this question), 33% predicting it will come in 1-2 years and another 30% saying it will be addressed in 3-5 years (back to Fig. 1).

Half think their current cyber defenses meet their organization's needs (combining "very well" with "extremely well"); another 36% say "moderately well." Only satisfaction with regulatory compliance systems was rated higher (Fig. 14).

In the short term (0-12 months) incident detection was the top priority for investment or improvement (Fig. 7). Longer off but in the foreseeable future, network/asset protection, incident recovery and incident response were of equal importance to incident detection. Nearly all the offered responses scored well above 80% for investment in at least the next five years; only threat-hunting and response automation – both implying a more sophisticated cybersecurity program – were embraced by less than three-quarters of respondents

The great majority place cybersecurity responsibility in the hands of their information technology people. Cross-tabulating size of the company with this question, it's not surprising that bigger companies have CIOs and CISOs or VPs of IT security; smaller companies put cybersecurity in the hands of their COOs and heads of operations. Bigger companies have created a head of operational technology security while smaller companies trust cybersecurity to their IT department. Across the size range, there is support for a long-term strategy – although smaller companies are a little more likely to employ outside consultants and look for best practices.

FIGURE 8

Which of these areas does your organization or agency have in place as a part of your cybersecurity strategy?

	YES	NO	DON'T KNOW
Increasing network visibility to connected users, devices and applications	69%	17%	14%
Threat intelligence	63%	19%	18%
Network segmentation	52%	20%	28%
Network behavioral and traffic analysis	57%	22%	21%
Identity and access management (i.e. remote access, etc)	74%	16%	10%
Cloud connectivity	63%	18%	19%
Endpoint detection, protection, response	52%	19%	29%
Air-gapped environment	27%	29%	45%
Software Bill-of-Materials (ie. SBOMs)	38%	22%	41%
Supply chain management	66%	14%	20%

Currently, the top cybersecurity tactic in these organizations is identity and access management (Fig. 8) – No. 1 among 10 possible answers, cited by 74% of respondents. Not far behind are situational awareness (increasing security team visibility to network action, movement, etc.) and supply chain management.

Over the next 12 months, cybersecurity measures will include improving a company's network visibility to connected users, devices and applications (33%), securing wireless access (31%), asset/vulnerability management (31%) and securing remote access (28%) (Fig. 15).

Nobody wants government or third-party mandates for anything, right? While the majority in this survey indeed voted that way, it was pretty close (Fig. 9). 45% said cybersecurity readiness should be mandated and codified somehow, either as part of a HACCP (hazard analysis and critical control points) plan or within Global Food Safety Initiative (GFSI)-recognized certifications. 55% said every company should determine its own approach to cybersecurity.

IN SUMMARY

The food & beverage industry is on a path toward digital transformation, slowly. Progress is being made toward the adoption of advanced technologies that increasingly connect plants and other operations to the internet. With that increased

FIGURE 9

Do you think cybersecurity should be mandated by government inspection authorities (FDA, USDA, others)?

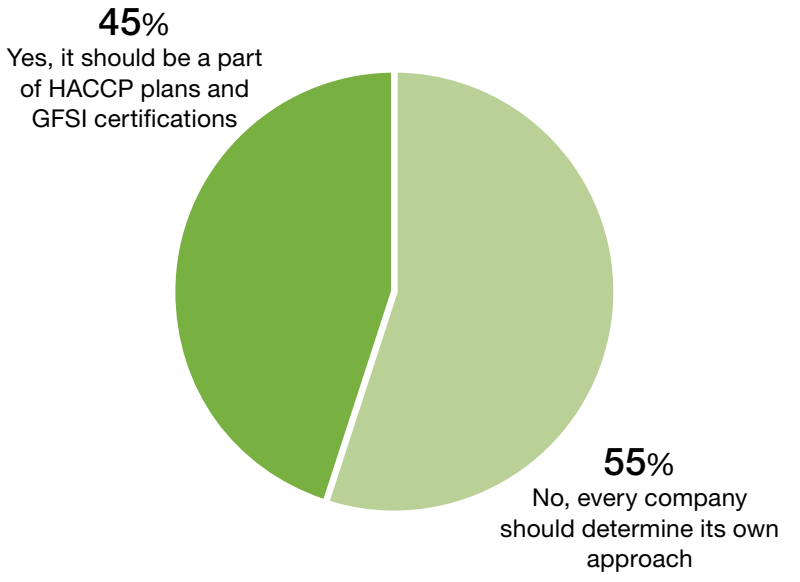
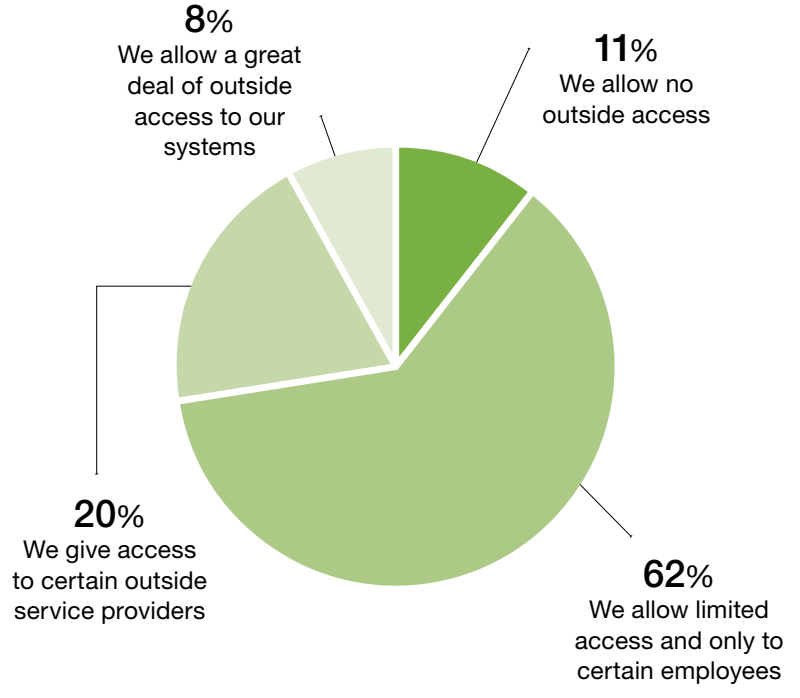


FIGURE 10

How much remote and/or personal device access do you allow currently?



connectivity comes increased risk of cyberattack.

The good news is the industry is cognizant of the need for better security. Better security positively impacts productivity and reduces loss of revenue due to an attack. Better security supports their priority to bring no harm to consumers. The ongoing challenge includes keeping current operations running while allocating funds to continue advancing systems.

The better news is that food & beverage processors realize that advanced automation and connectivity are inevitable progress in this business. Increasing network security, through investments in the people, processes and technologies that drive it, will be the key to unlocking operational benefits, better safety and more efficiency in the future.

FIGURE 11

Please rank the level of concern of agency or organization for the following types of cyberattacks.

ITEM	OVERALL	RANK DISTRIBUTION	SCORE	NO. OF RANKINGS
Malware	1		446	93
Ransomware	2		444	93
Existing/known vulnerabilities	3		286	90
Insider threat	4		255	89
Physical attack, i.e., USB stick	5		251	88
Social engineering	6		240	90

FIGURE 12

Which of the following are challenges to your agency or organization's progress when it comes to improving your cybersecurity technologies and systems?

	NOT CHALLENGING AT ALL	CHALLENGING	VERY CHALLENGING
No prioritized focus on use cases or technologies	35%	59%	6%
Poor understanding of what needs to change	30%	58%	12%
No clear ownership of change or innovation	37%	47%	16%
Lack of a clearly defined cybersecurity strategy	44%	43%	12%
Lack of empowering vision	32%	55%	13%
Inadequate budget	35%	44%	20%
Unclear mechanisms for access or procurement of funding	34%	50%	16%
Stop-and-go approaches according to funding cycles	33%	52%	15%
Too much focus on running current operations	21%	51%	28%
No perceived need by end users	29%	54%	18%

FIGURE 13

What level of cybersecurity training do you offer to your employees?

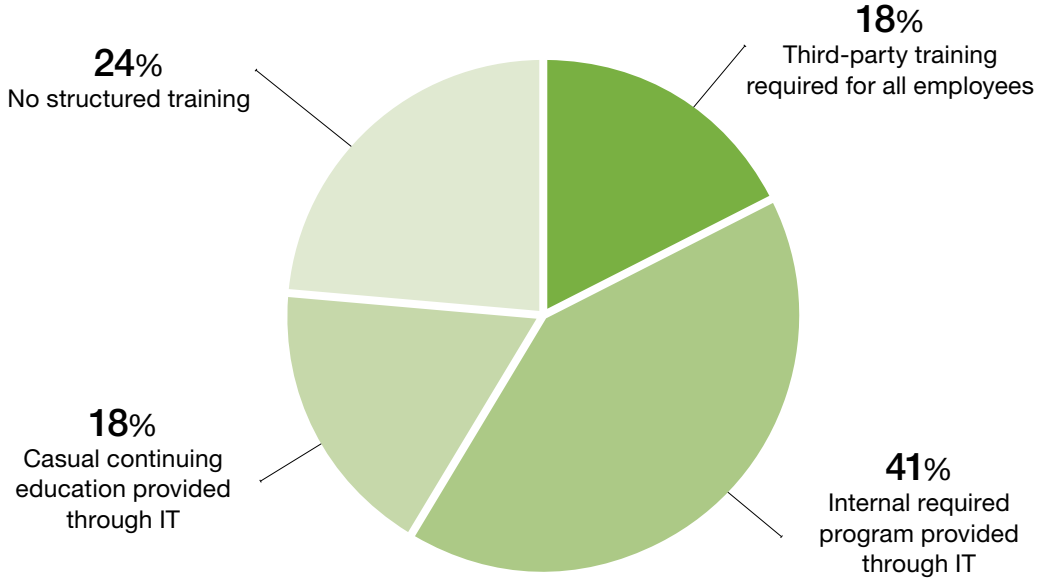


FIGURE 14

Rate how well your current technologies support your organization or agency's ability to meet the following strategic or operational needs:

	NOT AT ALL	SLIGHTLY	MODERATELY	VERY	EXTREMELY
Meet regulatory compliance	1%	8%	27%	52%	13%
Operational monitoring	3%	10%	40%	36%	12%
Operational control	4%	7%	50%	30%	10%
Manage infrastructure maintenance/repair/replacement	4%	15%	45%	29%	7%
Improving system resilience	4%	19%	45%	22%	10%
Cybersecurity	2%	12%	36%	38%	12%
Improving energy efficiency	8%	18%	43%	23%	9%
Predictive analytics/forecasting/ budgeting	4%	20%	46%	21%	9%
Integrating data silos (GIS, models, asset inventory, O&M, meters)	6%	25%	41%	23%	5%
Digital transformation	7%	22%	40%	26%	6%
Cloud computing	10%	17%	41%	26%	5%

FIGURE 15

Which of these areas is your organization or agency most focused on over the next 12 months to improve your cybersecurity preparedness?