Adulterating More Than Food
The Cyber Risk to Food Processing and Manufacturing
About FPDI

The Food Protection and Defense Institute (FPDI) at the University of Minnesota protects the global food supply through research, education, and the delivery of innovative solutions. We address vulnerabilities of the global food system through a comprehensive, farm-to-table view. We partner with industry, government, NGO/IGO, and academic stakeholders to help assure product integrity, supply chain resiliency, and brand protection throughout the food system.

foodprotection.umn.edu
# Table of Contents

**Executive Summary**  
1

**Adulterating More Than Food**  
2

**The Cyber Risk to Food Processing and Manufacturing**  
2

- How real is the cyber risk to Industrial Control Systems?  
  2
- How FPDI has addressed the risk  
  11
- Recommended actions for food companies  
  12
- Bibliography  
  14
Executive Summary

Almost every week brings news of a new cybersecurity incident. These typically effect companies and organizations in the financial, retail, or healthcare industries or, more recently, state and local governments. They also usually involve data breaches or other attacks that affect information technology (IT) systems. But what about the food industry and the industrial control systems (ICSs) it uses to process or manufacture food? Are these companies, their critical manufacturing technologies, and their customers also at risk from cyberattacks? The answer is unfortunately, yes, very much so.

For a cybersecurity risk to exist, there needs to be a vulnerability in a system that, if exploited, could lead to a bad consequence. In addition, there needs to be a threat that can exploit the vulnerability. These are the three factors of the Cyber Risk Equation, which is Risk = Vulnerability x Consequence x Threat. For a risk to exist, all three factors must be greater than zero—that is, they must exist. For ICSs in general, all three factors are present. Vulnerabilities are plentiful and many are easy to exploit. The consequences of exploiting them are real, as has been demonstrated by actual attacks that have destroyed equipment, caused environmental damage, and precipitated power outages, and more alarmingly, demonstrated the potential for injuring workers. Finally, as also demonstrated by these attacks, the threats are out there—people with the motivation, tools, and skill necessary to carry out an attack. If that wasn’t enough, the tools to carry out the attack are becoming more powerful and the skill required to use them is decreasing.

The food industry is not exempt from this risk. It is already a frequent target of criminals, including transnational criminal organizations engaged in large-scale food fraud, counterfeiting, theft, and smuggling. The potential consequences of an attack on industry ICSs are just as significant, including massive financial losses for companies and/or harmed customers. And, food industry ICSs not only have many of the same vulnerabilities as other sectors, but many unique ones as well. These include those stemming from the many companies still using ICSs that were developed before security was a concern and can’t be updated. Although other industries have been the primary target of attacks so far, it’s likely only a matter of time before the food industry is attacked as the others harden their defenses, and the threats seek easier prey.

Since 2016, the Food Protection and Defense Institute (FPDI) has conducted several projects to understand the cybersecurity risk to food industry ICSs and develop food industry-specific guidance and solutions. At convenings of cybersecurity and food experts from industry, government, and academia, FPDI has identified some of the key contributors to the food industry’s cybersecurity risk environment as well as key action steps food companies can take to protect themselves. The overarching, most important step is for companies to extend their food safety and food defense culture to cybersecurity, always remembering that insecure = unsafe.
Adulterating More Than Food
The Cyber Risk to Food Processing and Manufacturing

The food industry was filled with excitement in the 1990s and 2000s about how new computers and information technology could beneficially revolutionize the industrial control systems (ICSs) used in food processing and manufacturing. New hardware and software to control processing and manufacturing steps, generate and store data about those steps, and collect and share that data promised to speed production, reduce waste, cut costs, and make higher quality and safer products. Even as computer viruses and other malware plaguing the computers of their front office colleagues, plant floor operators were eagerly replacing analog controls with digital ones, attaching new sensors, and connecting everything to plant workstations and company networks—and then the internet—assuming their systems were safe from cyber-related risks.

These technological improvements to ICSs have largely delivered on their promised benefits for efficiency, quality, and safety. However, as the 21st century winds up its teens, that early excitement is yielding to the realization that computers and information technology have come with an unanticipated price: increased risk from malicious software and users that threaten product, consumer, plant, and personnel safety—and to company bottom lines.

How real is the cyber risk to Industrial Control Systems?

There are few things in life without risk. Company operations staff and leadership can rightly question whether, of all the things they should worry about, is the cybersecurity of ICSs one of them? To answer this, we first have to define some terms. For example, what is risk? Stated simply, risk is the likelihood that a threat exploiting a vulnerability will result in a bad consequence.

To understand if a risk exists, the component parts of this definition need to be evaluated. For instance, if a system has no vulnerabilities, or if exploiting the vulnerabilities has minimal or no consequences, then no risk exists. Also, there obviously needs to be some force that exploits a vulnerability. This is the threat. In the case of an intentionally caused bad event happening in an industrial control system, a threat is comprised of a

1. motivated attacker
2. with an effective weapon and
3. the skill to use it.

If there is no attacker or an attacker with no weapons or skill to exploit a vulnerability—and thus no threat—then again, no risk exists. For the risk to ICSs from cyber events to be real, all the factors of the risk equation (fig. 1) must be greater than zero. That is, all the factors must exist. So, do they?

1 “Malware,” short for malicious software, is used to describe the various types of software programs used in harmful ways against victims’ computers.
The vulnerabilities exist

At first, plant operators seemingly had little to worry about in their new systems. The National Institute of Standards and Technology (NIST) National Vulnerability Database catalogs 40,000 software and hardware vulnerabilities that were reported during 2000 to 2010, and these vulnerabilities affected systems of all types [1]. Yet, for that same period, researchers at the cybersecurity company FireEye identified only 149 vulnerabilities in industrial control system [2]. That disparity quickly changed.

They are plentiful and easy to exploit

In 2011 alone, researchers and manufacturers revealed over 200 ICS vulnerabilities [2]. The numbers increased every year afterward to early 2016, the end of the study period. So, industrial control system vulnerabilities exist and are plentiful. Of equal concern, however, is that the methods required to exploit many of the vulnerabilities are very simple [3]. For example, some devices have hard-coded passwords—that is, passwords that are written in the device’s source code, which can only be changed by the software’s author. These passwords are easily discoverable by hackers and knowing them can give one full control over the device.

Also, ICS vulnerabilities are widespread among manufacturers and component types. If vulnerabilities were limited to just particular ones, a company could avoid trouble by not using them. Instead, vulnerabilities have been discovered in many different components from a variety of vendors [3]–[5].

They are built in

With a closer look, it should be no surprise that so many vulnerabilities exist. Industrial control systems and the components that comprise them are designed for long service lives. Many systems still in use today were developed before cybersecurity was a concern. Thus, these systems were never designed to be secure from cyberattacks. They use hardware lacking the processing power and/or memory to incorporate security modifications, and they use old protocols for transmitting data—such as Ethernet/IP, FTP, Modbus, Omron FINS, Siemens S7, and Telnet—that lack basic security features. For example, many of these protocols assume the trustworthiness of the sending source and/or the data being sent and do not use modern security features that authenticate the sender or integrity check the data [6].

Compounding the issue in the food industry is that—as identified by Food Protection and Defense Institute researchers during facility assessments—many food industry ICSs use outdated operating systems (OSs). These include Windows 98, IBM AS 400, and early Linux. These also didn’t have security adequately incorporated into their design [7]. For both the OSs and data transmission protocols mentioned above, it’s like building a house without thinking to include door locks because no one had ever been robbed before. Most alarming, however, is how easily these ICSs using outdated protocols and OSs can be discovered on the internet. One recent study
used a specialized, publicly available search engine (Shodan) to identify over 170,000 host computers that exposed ICS components to the internet and used insecure protocols [8].

Unfortunately, even new ICS components continue to be developed with inadequate attention to security. A study of HMI² and SCADA³ systems identified many vulnerabilities that stemmed from poor software development practices [4]. This propensity for built-in vulnerabilities even extends to some of the most innovative ICS systems: robots and co-bots [5], [9].

The case of co-bots, which are robots designed to work alongside human workers, instead of in a physically secured area away from humans, is especially worrisome. A malicious actor exploiting a co-bot’s vulnerabilities could cause grave harm to the workers alongside it. In addition, mobile apps, which are becoming increasingly popular tools for monitoring and managing ICSs, have become another source of vulnerabilities. For example, a recent study identified nearly 150 vulnerabilities in thirty-four SCADA Android apps that could be exploited to cause damage [10].

A false sense of security

Even as security concerns began to arise for corporate and personal computers, plant operators trusted in the isolation of their systems from the enterprise business network and the public internet. As long as they maintained the physical security of their production facility through locks, gates, and guards, the “air-gap” (the lack of wired or wireless connections to a network outside the facility) would protect them. However, as many researcher have noted, the air-gap has long since proven to be more myth than reality [11], [12]. For instance, a truly air-gapped ICS could never be updated and would quickly become useless. Further, once computers showed up on the plant floor, the data they collected became too valuable to users throughout the company as well as to equipment vendors. Thus, the incentives to bridge the air-gap to access the data—with USB drives, wireless connections, and built-in vendor remote access—became far too great. Finally, even truly air-gapped systems are vulnerable, as demonstrated by researchers who have published a steady stream of research detailing methods to manipulate and steal data from air-gapped systems using their acoustic, optical, magnetic, electromagnetic, thermal, and other properties [13], [14].

The consequences are real

Nonetheless, per our equation above, all these vulnerabilities and more can exist, but if exploiting them causes no harm—that is, has no consequences—the vulnerabilities don’t matter. So we need to know what can someone with motivation and the tools and skill to exploit a vulnerability achieve?

---

² Human-Machine Interface, any machine with a user interface that allows an operator to control a device.
³ Supervisory Control and Data Acquisition, a system of software and hardware used to monitor and control dispersed industrial processes.
Real physical damage
The Department of Homeland Security (DHS) was very interested in this question. During 2006 in a project at Idaho National Laboratory codenamed “Aurora,” DHS conducted a test attack on a power plant. Researchers successfully hacked into a replica of a power plant’s control system and were able to destroy a generator [15]. Evidence is also provided by an even earlier incident. In 2000, a disgruntled former employee hacked into the SCADA system of the Maroochy Shire wastewater treatment plant in Queensland, Australia [16], [17]. For three months, until his arrest, he manipulated the system to deliberately release nearly a million liters of raw sewage into a local river and on parks and private property, causing extensive property and environmental damage.

A more dramatic example emerged with the discovery of the Stuxnet malware in 2010 [18]. During the preceding years, this malware—allegedly created by the governments of the United States and/or Israel—was deployed to damage centrifuges used by Iran to enrich uranium [19]. (Officially the enriched uranium was being created for energy use, but other nations—and ostensibly the attackers—believed it was for nuclear weapons.) Because Iran never officially acknowledged the impact of Stuxnet, it isn’t definitively known how successful Stuxnet was in its mission [20]. However, observers onsite at Iran’s uranium enrichment plant at Natanz estimate up to 1,000 centrifuges may have been destroyed [21], [22]. In another example, in 2014 the German government reported that year a German steel mill was subjected to a cyberattack on its ICSs, resulting in “massive damage” [23], [24]. (Again, the full details remain unknown because they also have never been released by the victim.)

More recently, electrical utilities in Ukraine were attacked in December 2015 and again in December 2016. The first attack was more widespread, affecting three regional power distribution centers and denying power to approximately 225 million people in the heart of winter [25]–[27]. The 2016 attack was more limited in impact—only shutting off power for over an hour to portions of Kiev, Ukraine’s capital [28]. But, it is considered more significant because the target, an electrical transmission substation, and the malware used demonstrated potential for more severe attacks that could leave many more people without power for months [29]–[31].

Threat to worker safety
Lastly, in 2017 the most dangerous ICS-focused malware so far was discovered in the workstations of a Saudi Arabian oil and gas facility after equipment began mysteriously shutting down, forcing the entire facility to stop operations [32]. Named “Triton” and “TRISIS” by the two security firms who discovered it, this malware was designed to interfere with the operations of safety instrumented systems (SISs) [33], [34]. SISs are designed to protect workers
by safely shutting down equipment if the SIS detects an unsafe operating condition. If they fail in this task, a piece of equipment could fail catastrophically and injure—or kill—any workers near it. The malware was discovered only because its designers had made a misconfiguration error, which caused the SIS to shutdown attached equipment when the attacker tried to reprogram the SIS [32], [33].

<table>
<thead>
<tr>
<th>Attack</th>
<th>Year</th>
<th>Activity</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maroochy Shire Wastewater Treatment Plant, Australia</td>
<td>2006</td>
<td>Released approximately 1 million liters of raw sewage</td>
<td>Property and environmental damage</td>
</tr>
<tr>
<td>Natanz Uranium Enrichment Plant, Iran</td>
<td>2010</td>
<td>Manipulated centrifuge rotation speed</td>
<td>Destroyed centrifuges</td>
</tr>
<tr>
<td>German steel mill</td>
<td>2014</td>
<td>unknown</td>
<td>“Massive damage,” per report of German government, but no details provided.</td>
</tr>
<tr>
<td>2015 Ukraine Electrical Grid Attack</td>
<td>2015</td>
<td>Operated circuit breakers at distribution substations to cut power. Disrupted utility operator monitoring and power restoration abilities.</td>
<td>1–6 hour wintertime power loss to approximately 225,000 customers in the Ivano-Frankivsk region of Ukraine.</td>
</tr>
<tr>
<td>2016 Ukraine Electrical Grid Attack</td>
<td>2016</td>
<td>Operated circuit breakers at transmission substation to cut off power. Disrupted utility operator monitoring and power restoration abilities.</td>
<td>1-hour wintertime power loss to portions of Kiev, capital of Ukraine</td>
</tr>
</tbody>
</table>

Figure 3: Select Major ICS Cyberattacks. Note the ICS equipment exploited in these attacks may also be used in the food industry.

Real financial harm
These examples are some of the most dramatic of ICS-related hacking attacks because they caused, or could have caused, physical damage ("kinetic attacks" in cybersecurity parlance). Fortunately these are still quite rare. Unfortunately, ICSS are also susceptible to some common attack types victimizing IT systems, such as ransomware, and these can cause painful financial losses. The notorious WannaCry and Petya/NotPetya attacks (the names given to the malware the attackers used) of 2017 forced several manufacturers of pharmaceuticals [35], automotive components [36]–[38], and food [39] to stop plant floor operations. However, the disruption of plant operations was a side effect of the malwares, which were designed to disable business enterprise applications running on Windows workstations.

Some prominent researchers agree, however, that ransomware targeting...
controllers and other ICS-specific components is on the horizon and have demonstrated disturbing proof-of-concept attacks on ICSs [40], [41]. The prospect of sophisticated ICS ransomware attacks is much more disturbing than typical ransomware attacks on enterprise applications. For typical attacks, the extortion threat is data loss on affected machines and the inability to use them for work. However, imagine a critical infrastructure ICS, such as for power generation or water treatment, that can’t be powered down while the ransomware is being removed being held hostage with the threat of damaging the system or its output.

Finally, in addition to these examples of actual events, it’s also useful to have a sense of the scale of potential consequences. The Common Vulnerability Scoring System (CVSS) was developed to measure the potential severity of IT vulnerabilities. In 2015 almost half (49%) of the ICS-related vulnerabilities identified were classified as high-risk in the CVSS (v. 3), and almost all the rest were medium risk [3]. To achieve this score, if attacked, the compromised system at a minimum would likely experience either a total loss of availability or a total loss of integrity.

Thus from actual incidents to a measurement of the impact of potential ones, we can see that the consequences of ICS cyberattacks are real. They range from major business disruption, destroyed equipment, and even to physical injury or death.

The threats are out there

We have now seen that two parts of our Cyber Risk Equation (Risk = Vulnerability x Consequence x Threat) exist for ICSs: Vulnerability and Consequence. What about the remaining one? The attacks above used to illustrate potential consequences make clear that threats—which consist of a motivated attackers with weapons and the skill to use them—certainly also exist. But it’s helpful to know more about the threats’ magnitude.

Attacks are frequent

In its FY 2016 report, the U.S. Department of Homeland Security (DHS) Industrial Control System Computer Emergency Response Team (ICS-CERT) stated that it responded to 290 attack incidents [42], [43]. Most of these had no impact on services, but 27 affected critical systems or critical systems management. In addition, in an experiment using ICS honeypots 4, evidence of an attack was recorded only eighteen hours after the first honeypot went online [44]. Over the next four weeks, thirty-nine attempts originating from fourteen countries were made to gain access to the systems and modify them. An example specific to the food industry is demonstrated by Ecolab. A company representative noted during a ProFood Tech presentation that the server for a new Ecolab clean-in-place optimization service was attacked 250,000 times in its first 30 days of operation [45]. However, the network is not the only route for attacks to begin. Research by Honeywell demonstrates that USB drives continue to be common vectors for malware, including some of the most potent strains that specifically target industrial control systems [46].

Powerful tools available

Further, people engaging in or planning attacks on industrial control systems have sophisticated malware tools at their disposal. Similar types of malware, including different versions of a common ancestor program, are classified into malware families. Currently, six malware

---

4 Internet-connected test systems designed to look like real, in-use ICSs to attackers and that can record attack activity.
families that focus on ICS have been identified on compromised systems (fig. 4). More are likely in development—including ransomware designed to specifically target ICSs. Although the ICS-focused malware in the table below (fig. 4) and used in attempts to cause physical damage were all likely developed by or with significant support from nation-states, criminal have proven adept at reusing/repurposing nation-state-developed malware for their own purposes [53]–[55].

This is more concerning in light of signs of rising criminal interest in ICSs [56], [57]. Further, the technical barriers to entry in cybercrime are continually falling. Skilled cybercriminals and malware authors find it more lucrative to tailor and sell their products and services to other criminals. Just as Software-as-a-Service platforms have increased in popularity in many industries, Malware-as-a-Service has taken root in the criminal world, affording the less skilled the chance to launch cyberattacks [58].

<table>
<thead>
<tr>
<th>ICS Malware Family</th>
<th>Primary ICS Component Affected</th>
<th>Use</th>
<th>Example attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stuxnet</td>
<td>Programmable Logic Control (PLC) devices</td>
<td>Physical destruction of manufacturing equipment</td>
<td>Natanz Uranium Enrichment Plant, Iran</td>
</tr>
<tr>
<td>Havex</td>
<td>Supervisory Control and Data Acquisition (SCADA) devices</td>
<td>Espionage, attack reconnaissance</td>
<td>Not implicated in any kinetic attacks, but Havex infections are widespread in the energy and pharmaceutical sectors [59].</td>
</tr>
<tr>
<td>BlackEnergy (v. 2 &amp; 3)</td>
<td>Human-Machine Interfaces (HMIs); Engineering Workstations; Servers</td>
<td>Attack reconnaissance, data destruction, software destruction (“bricking”) of network devices, service denial</td>
<td>2015 Ukraine Electrical Grid Attack</td>
</tr>
<tr>
<td>CRASHOVERRIDE/Industroyer</td>
<td>Supervisory Control and Data Acquisition (SCADA) devices; Human-Machine Interfaces (HMIs)</td>
<td>Attack reconnaissance, data destruction, service denial</td>
<td>2016 Ukraine Electrical Grid Attack</td>
</tr>
<tr>
<td>Triton/TRISIS/ HatMan</td>
<td>Safety Instrumented System (SIS) controllers</td>
<td>Unknown, but likely physical destruction of equipment</td>
<td>Unidentified Saudi Arabian oil &amp; gas facility</td>
</tr>
<tr>
<td>GreyEnergy</td>
<td>Engineering and/or Operator Workstations</td>
<td>Espionage, attack reconnaissance</td>
<td>Recently discovered and not used in a kinetic attack yet [50]. However, the malware is modular and could be so used.</td>
</tr>
</tbody>
</table>

Figure 4: Current Known ICS Malware Families

---

5 Stuxnet by the United States and/or Israel[19]; Havex, BlackEnergy, CRASHOVERRIDE, and GreyEnergy by Russia [30], [47]–[51]; the identity of the attackers using TRISIS is still unknown, but the malware development has been attributed to Russia [52].
Cyber risk is real...including to the Food Industry

We have now fully established that the risk to ICSs is real. There are 1) motivated hackers with powerful tools who can exploit 2) existing vulnerabilities to 3) cause significant damage. However, are the food industry and its ICSs at risk? Aren’t hackers only interested in energy companies and threatening the electrical grid or the promise of big hauls from the financial sector or extorting large payoffs from healthcare organizations?

Food industry threats exist

Sadly, the answer is no. Every part of the risk equation applies to the food industry too. The food industry is already a frequent target of motivated criminals. For example, transnational criminal organizations (TCOs) are heavily involved in large-scale food-related crimes such as counterfeiting, economically motivated adulteration, theft and resale, and smuggling. Well-known TCOs involved include the Camorra [60], ‘Ndrangheta [61], [62], and other Italian mafia clans [63] as well as the Perrones Orientales [64] and Knights Templar [65], [66]. Further, Food & Beverage routinely ranks as the first- or second-most stolen product category via cargo theft [67]–[73], which according to the FBI is usually perpetrated by organized crime [74]. And, it’s worth noting that many cargo thefts involve cyberattacks, such as when criminals hack into shipping systems to gather information on targets, steal company identities, and create fake bills of lading and manifests to facilitate fictitious pickups [75], [76].

Food industry vulnerabilities exist

As the energy, financial, and healthcare sectors harden their defenses in response to attacks, it’s safe to assume criminals and other threat actors will move on to lower hanging fruit. This could well be the food industry, which continues to use vulnerable ICSs that are discoverable on the internet [8]. Further, the Food Protection and Defense Institute (FPDI) at the University of Minnesota has discovered that food industry ICSs may be distinctly vulnerable to cyberattacks [77]. Food industry operations technology (OT) personnel, those responsible for operating and maintaining ICSs, are experts trained in food safety and production—and not in cybersecurity. Thus, even though ICS cybersecurity standards and best practices are well known and thoroughly documented, their complexity and volume overwhelm most food industry OT personnel. In addition, OT personnel aren’t trained to develop a mindset to suspect and detect hacks if something out of the ordinary happens.

Further, FPDI has determined during site visits and conversations with food companies that many ICS components in the industry operate with custom-written code produced in the 1990s and 2000s. This code presents several problems. First, the code can’t be updated because to do so would most likely require it to be completely rewritten, and further, the code authors have often long-since retired. Also, the code only works on the operating system current when the code was written, such as Windows 98. This requires companies to continue using outdated and insecure operating systems in their facilities. However, given that these components still successfully produce product, conscientious OT personnel and security vendors have difficulty persuading company leadership to invest in replacing the components since “they still work.”

Another food industry characteristic is the preponderance of small- and medium-sized companies in it: 74% of food manufacturing companies in the United States have fewer than 20 employees and 97% have fewer than
It may be tempting for small businesses to think there’s safety in their size, but unfortunately “security through obscurity” doesn’t work. Take the case of malicious email: research by Symantec indicates that for 2015–17, small business were targeted at least as often, if not more, than large businesses [79]–[81]. During that period, nearly 1 of every 250 emails contained malware. These malicious programs conduct ransomware attacks, espionage (including mapping of ICS networks to identify additional targets), and intellectual property theft, among other attacks. With business email users receiving nearly 100 emails daily, by some estimates [82], there are numerous opportunities for a successful compromise.

Further, small- and medium-sized companies—and even many large ones—outsource technology management of their IT systems and ICSs to managed service providers (MSPs). This has made MSPs an attractive target for hackers [83], who by targeting just one company, the MSP, compromise many others—the MSP’s clients. Finally, in addition to a history of being targeted by criminals (as mentioned above) the food industry also has a history of insider attacks—highlighted by three recent incidents of intentional adulteration by company employees [84]–[86]. This is notable because some security experts have identified the ICS insider attack, likely by a disgruntled employee, as the most likely type of cyberattack on ICSs [87].

Food industry consequences exist
What damage can be caused by a vulnerability being exploited? Along with the consequences mentioned in previous examples—financial costs from ransomware payouts and lost productivity, equipment damaged, and operators potentially seriously injured or worse—there are many others, and the food industry’s legacy systems make the consequences potentially more severe than for other industries. For example, mitigating an attack affecting programmable logic controllers (PLCs) would most likely require replacing the infected units. However, taking their place would be newer, different PLCs. This would require significant testing, potential system modifications, and a revalidation of the processing system to ensure product safety [88].

Also, food companies often have significant intellectual property in the form of recipes and processing parameters embedded in their ICSs. Analysis by Verizon of tens of thousands of incidents per year show the Manufacturing sector (of which the food industry is a component) is victimized by espionage cyberattacks more often than most other industries [89]–[93]. In some years espionage constitutes over 90% of all attack types [92]. The slow bleed of revenue from copycat products manufactured using information stolen from hacked ICSs could significantly weaken a company or even cause it to close.

However, the worst case scenario is if an attack on an ICS intentionally or unintentionally causes a food product to become unsafe, and it isn’t noticed until the product reaches consumers. The public health and business consequences of this scenario are potentially dire. In a critical infrastructure cyber risk assessment of the Food and Agriculture Sector (one of the 16 sectors designated as critical infrastructure by federal policy [94]), government and industry experts determined that although the cyber risk to the Sector as a whole was low, individual companies could suffer catastrophic consequences from such incidents [95].
How FPDI has addressed the risk

The Food Protection and Defense (FPDI) Institute recognized early the potential harm from cyberattacks against food manufacturing. In response, it has conducted a number of projects to more clearly understand the risks and to develop food industry-specific guidance and solutions. FPDI convened over 40 cybersecurity leaders from food and security companies, government agencies, and universities at the Food Industry Cybersecurity Summit. The assembled experts identified key knowledge gaps and risks (fig. 5) and determined initial steps companies could take to protect themselves. This meeting was followed by the Food Industry ICS Security Architecture Development Workshop. There, a subset of Cybersecurity Summit participants met for more focused discussions on developing tools to strengthen food industry cybersecurity.

Key contributors to the cybersecurity risk environment identified at the Food Industry Cybersecurity Summit:

Inherent ICS vulnerabilities, particularly in legacy systems
Many ICSs have vulnerabilities built in that can’t be easily remediated, yet they may be connected to workstations connected to corporate networks and the internet.

Lack of knowledge about how ICSs and IT systems interact
How these two vital systems interact is poorly understood. Too often, companies don’t even know how many ICS devices are connected to their networks, where they are, and who has access to them. One of the primary reasons for this knowledge gap is the cultural and communication divide between plant floor operations staff and IT personnel—the OT/IT divide.

Dependence on outsourced technology management by small- and mid-size companies
Cybersecurity risks are magnified for small- and mid-size companies who outsource technology management, for this almost always involves 3rd-party remote access—which introduces severe vulnerability. Further, these risks can be passed up the supply chain, even to larger companies who manage their own technology infrastructure.

Company leaders’ lack of awareness regarding cyber risks and threats
Senior executives and boards of directors often are not aware of—and do not understand—the risks of cyberattacks, particularly to control systems. Unfortunately, it can be hard to make the business case for adequately funding cybersecurity because the examples and data required to demonstrate the threats and quantify the consequences are difficult to acquire or are unavailable.

Poor coordination and information sharing among stakeholders
Companies and government agencies—and departments within them—too often work in isolation, ignorant of complimentary efforts and the availability of helpful information or tools. This disconnect handicaps cybersecurity efforts by everyone involved.
Recommended actions for food companies

FPDI has identified several critical steps food companies can take to protect themselves. If you’re not already doing all of them, start here. First:

Foster more communication between your OT and IT staff. This is critical for bridging the cultural gap and fully understanding how ICSs and IT systems interact. For starters, OT staff can help IT staff see how standard IT security solutions often won’t work for ICSs. IT staff can help their OT counterparts understand the risks to their systems and the company, and together they can develop processes and procedures to protect your systems that work for everyone.

Next, once your teams are beyond the introductions:

Begin conducting risk assessments that include inventorying both ICSs and IT systems. You know where all the physical doors and windows into your facility are and how they work, but do you know this about all your hardware and software? If not, how will you lock them? As the former head of the National Security Agency’s top hacking team has said, those wanting to attack a network put in the time “to know it better than the people who designed it and the people who are securing it” [96]. Also, strongly consider using 3rd-party cybersecurity audits of your process controls.

Cybersecurity has to become part of your operating culture:

Involve staff with cybersecurity expertise in the procurement and deployment process for ICS devices. They can save you from “buying problems” by purchasing vulnerable devices. Unfortunately, vendors too often package and market new “features” that are anything but when it comes to keeping your systems safe. You need a procurement team with the knowledge to negotiate with vendors for what your company really needs. In addition, have a team able to effectively vet the equipment before placing it on the service line.

There is also another way to leverage your company culture to enhance protection, and this may be the most important change to make of all:

Extend your food safety and food defense culture to cybersecurity. Plant workers are trained to incorporate food safety concerns into the plant workflow and manage food safety threats through good manufacturing workflow design. This can include incorporating best practices and standards into action steps in the workflow. Cybersecurity threats have to become part of this threat mitigation and safety enhancing process. Remember:

And finally:

Become involved. The food industry needs more representation in ICS- and cyber-related standards setting organizations, such as the ISA and in industry-government partnerships, such as the Food and Agriculture Sector Coordinating Council.

Insecure = Unsafe
FPDI has also developed food industry-specific cybersecurity tools and guidance as part of the Strengthening Food Industry Cybersecurity Capacity project. FPDI conducted this project to address key issues identified by stakeholders, and products from it include a set of Cyber Physical Security Principles (CPSP). The CPSP leverages food industry OT personnel’s experience with the Hazards Analysis Critical Control Point (HACCP) approach to mitigating risk by helping OT staff assimilate cybersecurity into their existing food safety culture. FPDI created the CPSP by mapping the seven HAACP principles to a set of vetted and widely accepted cyber defense best practices—the CIS Critical Security Controls.

Further, FPDI developed an industrial control system reference security architecture that was food-industry focused. A reference security architecture aids cybersecurity professionals and others by organizing industry standards and best practices that often exist in disparate sources into a single, comprehensible guide. The Food Industry ICS Reference Security Architecture developed by FPDI is based upon standards and best practices supported by 20 years of research and on analysis of other industries that employ similar industrial controls and have similar operational constraints.

The standards comprising the reference security architecture include the ICS-related standards corresponding to the five core functions identified in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). It also includes additional standards relevant to ICS in food manufacturing from NIST, the International Society of Automation (ISA), and the DHS Industrial Control System Cyber Emergency Response Team (ICS-CERT).

Performing assessments is a crucial prerequisite to implementing a reference security architecture. However, most assessment tools require answering an extensive set of questions about the ICS network, controls, and operations. Although effective, this approach requires a substantial cybersecurity background that OT personnel typically and understandably will not have. In response, FPDI tested a use case-based method to perform assessments and demonstrated this could be highly effective for the food industry. This method allows OT personnel to describe their product line by selecting from a set of use cases based on typical plant configurations. This approach allows them to leverage their broad experience in plant operations but does not require extensive cybersecurity knowledge.

More information about the Strengthening Food Industry Cybersecurity Capacity project, including results of pilot-testing the use case method and a subject matter expert survey, can be found in the project report available on FPDI’s web site.
The Cyber Risk to Food Processing and Manufacturing

Bibliography


D. Z. Morris, ”It fell off the back of the Internet": Freight thieves are becoming cybercriminals,” Fortune, 29-Jul-2015.


Photo credits

Cover: Original image, Brendan Aanes, CC BY-SA 2.0; Modification, Stephen Streng, CC BY-SA 2.0

P. 5: Original image, “Substation Dusk” by Patrick Finnegan, CC BY 2.0; Modification, Stephen Streng, CC BY 2.0

P. 10: Original image, Oregon Department of Agriculture
Author
Stephen Streng

FPDI Cybersecurity Project Team
Dr. John Larkin, Principal Investigator
Brian Isle, Cybersecurity Subject Matter Expert
John Hoffman, Senior Research Fellow
Lisa Brienzo, Project Manager
Stephen Streng, Analyst and Technical Writer
Mangaya Sivagnanam, Graduate Student Researcher
Kelvin Luu, Undergraduate Student Researcher

Food Protection and Defense Institute Leadership
Dr. Amy Kircher, Director
Dr. Jennifer van de Ligt, Associate Director
Some of the work described in this white paper was supported by the U.S. Department of Homeland Security S&T under Grant Award Number 2010-ST-061-FD0001 awarded to the Food Protection and Defense Institute at the University of Minnesota. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.