plexal

CYBER SECURITY AND OUR FOOD SYSTEM:

THREATS AND OPPORTUNITIES

The most important sector – and the most unprepared?

The global, interconnected and increasingly digitised food system that the UK relies on has its fair share of problems. From the rising cost of the weekly shop and supply chain disruption due to labour shortages to wars affecting farmers' grain inputs and the impact food has on climate change, the system is under pressure at every point. But there's another, growing problem to add to the list: cyber

FOUR IN TEN BUSINESSES (39%) reported having cyber security breaches or attacks in a 12-month period, according to the Cyber Security Breaches Survey 2021[1].
Food is no exception.

From sensors, wearables, drones and connected tractors on farms to smart factories using operational technology and high-tech, lab grown food where intellectual property is closely guarded, the food sector has been undergoing rapid digitisation.

The pandemic has also meant that traditional criminal actors have moved online and into cybercrime opportunistically. With readily available toolkits making ransomware more accessible for these criminals, there are even more threat actors to contend with.

We're turning to technology to fix some of the food system's big problems by increasing yields, improving efficiency and minimising waste. But all this progress could be endangered if trust in foodtech becomes eroded because the sector hasn't protected itself.

On a societal level, policymakers and those closest to the government stress that our food system is resilient and that a cyber attack is unlikely to cause starvation or critical food shortages[2]. But attacks could add extra pressure that food and agriculture will struggle to cope with.

Scenarios could include fresh produce being wasted because of supply chain disruptions elsewhere along the chain, animal welfare issues because a setting has been tampered with, financial loss for farmers because of a data breach or mislabelling that puts lives at risk because an allergen hasn't been highlighted. At Plexal, we've produced this report to highlight both the unique characteristics of our food system and the ways in which cyber threats could impact it. Going a step further, we're also exploring opportunities for innovation, collaboration and education. We've zoomed in on food because it matters.

It's one of 13 sectors classified as being Critical National Infrastructure (CNI) by the UK government[3]. Meanwhile the agri-food sector contributed £128.7bn, or 9.8%, to national Gross Value Added in 2019 according to the most up-to-date count[4].

And yet the food and hospitality sector spends less on cyber security than entertainment and lags far behind financial services, which was the earliest adopter of cyber security. Few startups in Plexal's ecosystem focus on the food sector and many that have tried found that there's a lack of demand because margins are so tight and the importance of cyber hasn't been grasped by leadership teams.

Cyber criminals, meanwhile, are soon realising that food companies are ripe for the picking.

If you want a sector that's digitising while maintaining legacy infrastructure, hasn't adopted basic cyber hygiene and can have a major societal impact if there's a disruption, you can't do much better than food.

It's also a primal, emotive part of our critical national infrastructure: we all want reliable access to safe, affordable food we can trust and when that's called into question it threatens our very sense of security. As one interviewee who wished to stay anonymous put it, "when they come for the Jaffa Cakes, that's when people will start to care about the cyber threats to food".

The pandemic and subsequent labour shortages gave us a small glimpse into what a major food supply chain disruption could look like but it also showed that the system is resilient. However, it would be dangerous to become complacent.

In this report, we've used desktop research as well as interviews with security leaders, experts with government experience, startups, academics and industry voices to get a cross-cutting picture of the cyber threats and opportunities facing the food sector.

We've also ended the report with a set of ideas, recommendations and innovation opportunities as we see them. If you'd like to take any of these forward and be part of the solution, we'd love to hear from you. Don't wait for the Jaffa Cakes to run out.

ON THE MENU...

"The threat of cyber-attack to UK businesses, including those in the agri-food sector, is significant and growing."

United Kingdom Food Security Report 2021

THE STATE OF FOOD:

issues and challenges

CONCENTRATION

There is a high degree of horizontal and vertical integration in the agri-food sector and mergers and acquisitions are common, which makes farmers more reliant on a smaller number of suppliers and buyers. The top five manufacturers have a combined turnover of £30bn[5]. Consumers are also experiencing this: just four supermarkets enjoy market dominance[6].

Elsewhere, a desire to control the rich data being produced, such as plant genomics, chemical research, data from machinery and consumer information, is driving mega-mergers[7].

DEMAND AND SUPPLY

According to the United Nations (UN), there will be over nine billion mouths to feed by 2050, which means we may need to increase production by up to 70% . We need to use every good piece of technology we can find to improve yields and minimise food waste to achieve these goals.

WASTE AND THE ENVIRONMENT

According to the Boston Consulting Group, 1.6 billion tonnes of food is wasted in a year – that's a third of the total amount of food produced around the world[8].

Meanwhile, given the emissions that food is responsible for, the UN's Sustainable Development Goals have set a target of halving food loss and waste by 2030[9].

RISING COSTS

World food prices measured by the Food and Agriculture Organization were at an all-time high at the end of 2021[10] while consumers in the UK are feeling the impact of higher food prices[11].

The cost of fertiliser, fuel and other imputs is putting pressure on farmers while the war in Ukraine, a major exporter of cereals and other inputs, is exacerbating this. The British Egg Industry Council said that input costs had risen by about 30% since the war in Ukraine broke out[12].

This is making farmer sentiment dip and causing farmers to be concerned about supply chain disruptions[13].

The pressure on margins means companies have less to spend on cyber security, but also makes them less able to bounce back from a costly attack or data breach fine.

CURRENT GUIDANCE

The British Standards Institute developed PAS 96 in 2017 to make the food supply chain more resilient to threats like cybercrime and malicious contamination[14].

INVESTMENT IN CYBER

Food and hospitality is one of the sectors where it's most common for customers to pay online, (57% versus 30% overall) and firms in this sector are also more likely to use network-connected devices (59% versus 46% overall)[1].

Yet the sector lags behind finance (£22,050) and even entertainment ($1,940) when it comes to how much firms spend, on average, on cyber security[15].

Food and hospitality firms are less likely than others to have up-to-date malware protection (71% versus 83% overall) or network firewalls in place (66% versus 78% overall)[1]. Overall, 31% of businesses have a business continuity plan that covers cyber security[1], which could affect their ability to recover and reduce operational delays.

SUPPLY CHAIN DISRUPTIONS

Climate change, the pandemic, war, labour shortages, political events like Brexit and even a blockage in the Suez Canal have affected supply chains in recent years.

The Business Continuity Institute's report found that suppliers are using technology to manage disruptions while the number of supply chain disruptions organisations experienced in 2020 was higher than any other year in the report's history[16].

The same study also highlighted that cyber's impact on supply chains is becoming a concern: as businesses start to experience cyber-related delays in the supply chain, 52.9% of respondents are specifically concerned about cyber attacks or data breaches. This is ahead of natural disasters (52.9%), transport disruption (37.3%) and political unrest (40.2%).

THE PANDEMIC: TESTING TIMES

When the Environment, Food and Rural Affairs Committee gathered to assess the pandemic's impact on food supply, the verdict was that we had survived and were resilient, but we shouldn't be complacent[17].

"Food is a matter of national security. If you cannot feed a country, you do not have a country."

- Ian Wright CBE, Chief Executive Officer, Food and Drink Federation

"I would like to think some good comes out of this crisis, but it needs to because the sector was not in great shape. If it is going to go forward, we need to get some more value into the whole supply chain from the retail end right the way through to the farmgate end, otherwise it will be in trouble, particularly the beef sector."

- Nick Allen, Chief Executive, British Meat Processors Association

FOOD SYSTEMS AND NATIONAL SECURITY

The UK imports 46% of the food it consumes and no single country provides more than 11%[18].

But Timothy Lang, Emeritus Professor of Food Policy at the Centre for Food Policy at City University London, points out that supply chains have become long and complex. There is a network of primary producers, processors, manufacturers, packaging plans and distributors involved before food goes on the shelf[19]. An attack that causes disruption at any point could have a ripple effect.

SIGN OF RESILIENCE?

According to the United Kingdom Food Security Report 2021[20], 89% of UK food businesses managed to restore operations within 24 hours after a minor attack.

TECHNOLOGY AND THREATS

"As the agricultural industry embraces and champions new technology, it is increasingly important for farmers and rural communities to look at their growing exposure to cyber risks and how to best protect themselves and their data."

- Stuart Roberts, Deputy President of the National Farmers' Union, warned that the digitisation of farms is expanding the attack surface in a foreword to guidance to farmers by the National Cyber Security Centre (NCSC)[28]

From cloud-based point of sale technology to wearables on cows, technology is being introduced at every part of the supply chain. This is expanding the attack surface and adding even more complexity.

Kroll, a consultancy, analysed data breach notifications in 2020 and discovered that there had been a sharp increase in attacks on six industries that have traditionally been "under-attacked" – including the food and beverage sector. In fact, it found that data-breach notifications in the food and beverage industry went up by 1,300% in 2020[21].

BUSINESS AND SOCIETAL IMPACT at a glance

LIKELY

- Operational delays that affect costs and the price of food
- Data breach fines
- Financial loss because of ransom payments and recovery costs

POSSIBLE

- Spoilage and waste
- Loss of trade secrets or intellectual property
- Safety, contamination and mislabelling
- Innovation deficit because of a loss of confidence in foodtech

LESS LIKELY

- Panic buying because of upstream supply chain disruptions
- Animal welfare is compromised
- Supply distribution and delays affecting others in the chain
- Reputational damage

THREAT VECTORS

- Phishing
- Malware and ransomware
- Email compromise
- Software supply chain
- DoS and Botnet
- Jamming of satellites

RANSOMWARE SPOTLIGHT

"In addition to the direct cyber security threats posed by the Russian state, it became clear that many of the organised crime gangs launching ransomware attacks against Western targets were based in Russia."

- The NCSC's Annual Review 2021[33]

The NCSC says that ransomware is the biggest cyber threat the UK is facing[22]. It's been behind some of the biggest cyber incidents in the food sector so far, forcing global companies like JBS Foods to down tools and pay a ransom.

In the US, the FBI issued a notice warning the food and agriculture sector about ransomware attacks that could disrupt supply chains and cost businesses money: "As the sector moves to adopt more smart technologies and internet of things (IoT) processes the attack surface increases. Larger businesses are targeted based on their perceived ability to pay higher ransom demands, while smaller entities may be seen as soft targets, particularly those in the earlier stages of digitizing their processes, according to a private industry report[23]."

Threat actors:

- Hacktivists – for example, animal rights activists targeting poultry in transit
- Insider threat because of a lack of awareness and training
- Nation state – deliberate disruption or contamination
- Corporate espionage – to create reputational damage or steal intellectual property
- Criminal gangs – ransomware attacks to extort money

SMART FARMING – from soil to the cloud

Malwarebytes recorded a 607% increase in malware detections in the agriculture sector in 2020[24].

Agriculture 4.0 refers to the digitisation of the sector[25].

Tech examples:

- Drones, internet-connected tractors, robotics and sensors enable data on crops and soil to be collected, transferred to the cloud and analysed – often by a third party
- Livestock farmers putting wearables on animals and placing them in monitored environments helps optimise breeding schedules or temperatures
- Using the Internet of Things to adapt old machinery rather than forking out for huge upgrades[26]
- Automated poultry feeding system[27]
- Precision agriculture is being used to improve efficiency, standardisation and welfare, which can increase crop yields – helping the world produce more food[28]

Threat examples:

- A loss of integrity of automatic milking parlours could mean a batch is unnecessarily dumped by the milking machine
- Contamination of the milk storage vessel or spoiling of milk if the refrigeration settings are affected, which would affect the farm's profits
- Leaking of soil, crop, and agriculture purchasing data could affect a farmer's competitive advantage
- Data processing and analytics moving to the cloud gives attackers an easy entry point
- Smart farms often use third parties to analyse data on plant biology and genetics, agriculture economy, supply forecasts or disease predictions, which introduces third-party risk[29]

DISTRIBUTION, PACKING, PROCESSING

Tech examples:

- Online payment portals to manage and track livestock
- Using data to track food moving through a low temperature-controlled supply chain to prevent waste and spoilage
- Foodtech companies like TOMRA use sensor-based sorting and grading systems to help food suppliers maximise yields and optimise processes like sorting[30]
- Using blockchain to enable transparency, traceability and auditing

Threat examples:

- Compromising heating, ventilation and air conditioning systems to affect fresh foods like potatoes that need to be stored and moved at specific temperatures to comply with food safety regulation. Tampering with temperatures or changing settings could result in the spread of foodborne diseases[31].
- Mislabelling allergens
- Retailers typically use just-in-time ordering, which means they order stock to match demand on a day-by-day basis rather than holding a large inventory. So a disruption to logistics could impact what's on the shelf upstream even though there's enough stock in warehouses[32].
- Remotely immobilising distribution vehicles through telemetry systems

MANUFACTURING

An analysis by Verizon of cyber incidents showed that manufacturing – including food manufacturing – is one of the sectors most affected by cyber espionage[33].

Tech examples:
- AI and machine learning to perform predictive maintenance or for optimised sorting and inspection[34]
- Internet-connected devices that measure and monitor production processes. 5G networks will only make this more common.
- Lab-grown meat where investment is going into companies that are racing to make cultured meat cheaper by gaining a competitive advantage[35]

Threat examples:
- Food contamination and spoiling
- Food crime such as misrepresentation or adulteration
- Corporate espionage or insider threat that results in alarms being turned off, affecting temperatures and safety controls used to detect contaminants
- Theft of intellectual property and trade secrets through malware, phishing and social engineering targeting office-based employees. Industrial control systems (ICS) tend to hold intellectual property[36].

SPOTLIGHT ON INDUSTRIAL CONTROL SYSTEMS

As manufacturing embraces rapid digital transformation, industrial control systems (ICS) and operational technology weren't designed with cyber security in mind but are being connected to networks.

The Food Protection and Defense Institute warns that this introduces cyber vulnerabilities[37]. Bad actors could discover which ICS have outdated operating systems and exploit those weak points[38].

A cyber incident that affects the IT systems controlling food production could result in ratios, temperatures and ingredients being changed. This could contaminate food, costing the manufacturer financially if they have to throw away a spoiled batch. Worse, someone could eat adulterated food that makes them sick[39].

POINT OF SALE AND RETAIL

Tech example:
- Point of sale and ordering technology relies on automation and cloud computing
- Suppliers bypassing retailers and selling direct to the consumer using apps or ecommerce websites

The threat:
- Bad actors can disrupt point of sale technology and tills, as SPAR found out when a ransomware gang hacked the company that operates SPAR's tills and IT systems
- Interreference with satellites could affect the just-in-time ordering systems that retailers rely on

TRAINING, EDUCATION AND CULTURE

The food sector is playing catch-up when it comes to making sure the people working in food are equipped with training in basic cyber hygiene as well as the skills needed to keep ICS secure. They're working in complex environments where technology is often being layered onto older machinery and infrastructure[40].

The Food Protection and Defense Institute (FPDI) at the University of Minnesota found that food industry operations technology personnel, especially those responsible for operating and maintaining ICS, may be trained in production safety but they often lack cyber security skills[41].

IN THE REAL WORLD

These are some of the cyber incidents that have affected the food sector...

JBS FOODS

The ransomware attack on JBS Foods, the world's largest meat packer, is the largest known attack on a food manufacturer by a criminal gang at the time of writing. It's shone a light on the fact that a cyber attack could have big ramifications.

JBS Foods operates hundreds of plants in 15 countries, employing over 150,000 people. Its customers include supermarkets and fast food chains like McDonalds.

The cost was 10 days of disruption as 13 plants across the US and Australia were shut. And although the company sought out help from the authorities and third-party experts, it still paid a $11m ransom to the REvil ransomware group.

The US Department of Agriculture estimated that 94,000 head of cattle were processed on a Tuesday at the peak of the attack – 27,000 less than on the same day the previous week[42].

KP SNACKS

A ransomware campaign affecting KP Snacks' IT and communications systems appears to have given attackers access to employee and financial data, and resulted in some delivery delays as the company worked with a third party on its response.

Better Retailing reported that the company told its customers that because of the attack, it "cannot safely process orders or dispatch goods"[43].

CRYSTAL VALLEY COOPERATIVE

The agricultural cooperative works with crop farmers and livestock producers but was unable to take card payments after a ransomware attack shut down IT systems[44].

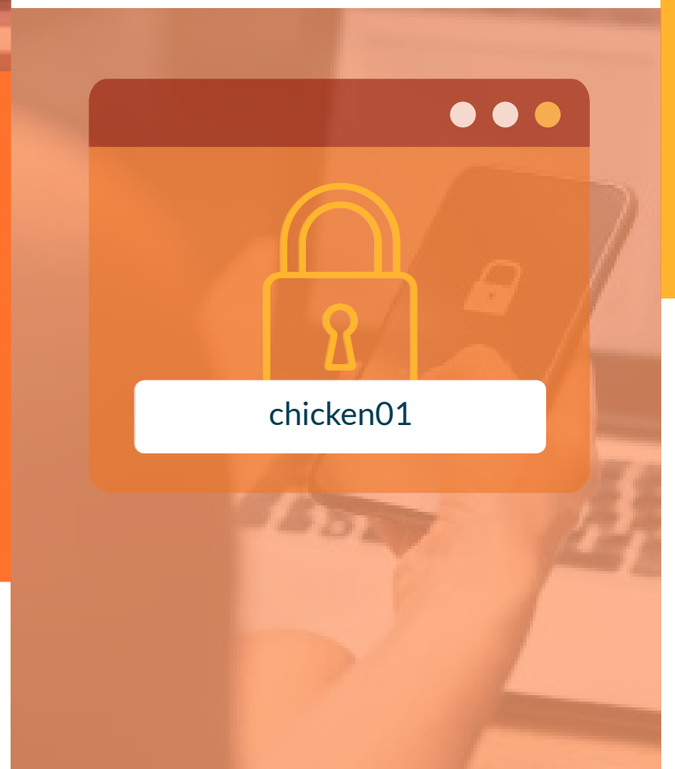
SPAR

Ransomware gang Vice Society claimed responsibility for a hack on James Hall & Company, which operates SPAR's tills and IT systems. It meant card payment machines in hundreds of UK branches couldn't operate. The disruption felt by consumers in this case was minimal as only a few shops had to be shut entirely[48].

NEW COOPERATIVE

BlackMatter demanded a $5.9m ransom from the Iowa-based farm service provider, causing its systems to go offline. The criminals accessed encrypted data and stole files like invoices, research and development documents and the source code to its soil-mapping technology[45].

After the attack, digital identity management firm FYEO discovered over 600 breached credentials connected to the company and the password "chicken1" was used over 10 times[46].



ANIMAL HEALTH EMERGENCY REPORTING DIAGNOSTIC SYSTEM, USAHERDS

This digital tool helps to track and trace animal diseases among livestock. Cyber security firm Mandiant believes that Chinese cyber espionage group APT41 exploited a vulnerability in USAHERDS. Mandiant also claims it warned the developer of USAHERDS that the app contained a hackable flaw[47].

EXPERT VIEWS

"We're more vulnerable than you imagine."

- Timothy Lang, Emeritus Professor of Food Policy, Centre for Food Policy

The problem of cyber insecurity isn't just a problem for companies: it's also about society. We need to increase public awareness and policymaker awareness of the importance of the black hole of food defence.

Even the biggest companies in the world – let alone SMEs – cannot possibly control their own cyber security. They can do a little bit of protection and risk management but they can't ultimately stop a megastate bringing down a satellite system or unleashing malware.

To start with, we need an assessment of the British food system and food defence: its fault lines and what we can do about them.

This should be a national discussion by policymakers that includes somebody who is responsible for food cyber security and answerable to Parliament as well as committees like the Environment, Food and Rural Affairs Committee and the Environmental Audit Committee. We're more vulnerable than you imagine, from a cyber security standpoint. Look at what happened to Tesco recently.

Britain has already forgotten the lessons of the Second World War and we don't regard food defence as part of what a nation state should look at. There's also got to be civic engagement, or the government will turn a blind eye to it.

"Even though we have a lot of resilience built into the UK's food sector and there are a large number of suppliers, it's not difficult to see major inconvenience – or possibly worse – because of an interruption to the food supply chain."

- Robert Hannigan, Chairman of Bluevoyant International and former Director of GCHQ

You can imagine scenarios where nation states try to destabilise a country's food supply chain, but that's an extreme case and it's a bit alarmist. Criminal activity, in particular ransomware campaigns, is more likely.

The main threat is to business interruption of the supply chain and right now, ransomware is the most likely threat. The issue is, if you take out one part of the food sector it can have a knock-on impact.

And the food sector relies on a just-in-time system. Margins are tight and there are lots of companies in the supply chain that haven't thought much about cyber security.

The danger is that criminals will seek out these less cyber-mature parts of the chain. So for a supermarket, for example, their networks might be well-protected but they're vulnerable to third parties – as a leading grocery chain found out.

We need to raise basic awareness and basic standards among small companies and non-traditional companies in the supply chain who don't think cyber affects them. On the other end of the scale, large food companies and supermarkets need to better understand their supply chain ecosystem. In an ideal world, they will help improve the security stance of their supply chain because it's good business and it's in the interest of our national resilience. It could be a virtuous circle.

Even though we have a lot of resilience built into the UK's food sector and there are a large number of suppliers, it's not difficult to see major inconvenience – or possibly worse – because of an interruption to the food supply chain.

Food is now considered critical national infrastructure (CNI) as our definition of CNI has broadened. The pandemic and the haulage strikes reinforced how fragile our just-in-time supply chain is.

"It's not clear to what extent security factors in the design of cloud-based systems farms are using. Our initial research shows that it doesn't play a big role."

- Awais Rashid, Professor, Department of Computer Science at the University of Bristol and Head of the Bristol Cyber Security Group

Critical national infrastructure (CNI) like water and power is increasingly connected to the internet but wasn't designed with security in mind. And it's exposed to cyber risks – as the recent attack on Ukraine's power grid shows.

Agritech is in a similar position, it's just ten years behind other CNI. Agritech relies on smart technologies but we don't clearly understand the vulnerabilities those technologies bring and what impact it could have on the food system.

For example, animals have wearables around their necks. If you compromise that, you can cause physical damage to the animals. If you compromise the cameras farmers use to monitor the health of animals, they're not getting information that can help prevent the spread of disease. Disruption to horticulture could create large-scale crop damage, impacting food supplies downstream.
But it's not clear to what extent security factors into the design of IoT-based systems farms are using. Our initial research shows that it doesn't play a big role.

In terms of who would want to create this kind of disruption, it could be hobbyist script kiddies or sophisticated actors such as organised crime or even nation states

Cyber security used to be about securing information and business or personal data. It's now also about the processes that produce power, water or food. We need to protect these processes.

In the context of food, we need solutions that protect both regular computer systems in farms and smart agritech devices. We also need to raise the baseline of cyber security. Farmers shouldn't have to be cyber experts so these solutions shouldn't be onerous. The solutions need to consider the context; you can't just retrofit enterprise products for farms or other critical infrastructure.

At the university we're using a tabletop testbed to test security solutions that can be applied to dairy farming and we report our findings to manufacturers so they can fix problems. We need to do much more research like this to understand the attack surface of food and how to build products that enable farmers to reap the benefits of technology without exposing themselves to cyber attacks.

"The wave of ransomware attacks in the last five years has changed the game and companies are now, quite frankly, petrified."

- Peter Gooch, Partner, Cyber Risk Services, Deloitte

On average, consumer packaged goods companies tend to be less secure because they're less regulated than other sectors – partly because the sort of data they handle is less sensitive than in financial services. Only in the last few years have they started to see that there's a real chance of operational disruption.

The wave of ransomware attacks in the last five years has changed the game and companies are now, quite frankly, petrified.

Industry may not mind about losing a bit of data here – they figure they can probably handle the reputational fallout. But they do mind if the business has to stop operations because they might not be able to recover. And yet most of these companies still aren't that well-prepared. It's a big job: you have to look at your culture and technology. It's a steep learning curve if you've not been prioritising cyber for the last 10-15 years.

Food is also a sector characterised by tight margins and high volumes so there's less cash to invest in something like cyber security – historically it's been hard to make the business case for it if you've not been the victim of an attack yet.

Food supply chains have become extremely complex and it's often the small companies that might be critical in a supply chain but don't have the budget for cyber. They could introduce risk into the system – either because they'll pass on malicious code or they'll experience disruption that will have a knock-on effect. The question is can they survive an operational disruption of one day? What about five, 15 or 30 days?

"We need to protect IoT devices and legacy hardware. There's definitely an opportunity for cyber startups to focus on this."

- Nadia Kadhim, CEO, Naq Cyber

We work with agricultural clients, one of whom took over the family farm and wanted to digitise its processes. That farmer was aware of issues like data protection and cyber security but on the whole, awareness is very low.

Our research uncovered some of the cyber risks affecting food and the entry points for disruption – everything from CCTV and drones that check on crops from above to cow milking machinery that's being connected to the internet.

Because anything connected to the internet can be breached, you could have a scenario where the settings of cow milking machinery are tampered with and the acceptable range is altered – which could result in people being sold unsafe milk. The business could lose contracts and it's also a danger to health.

At Naq Cyber, we made a conscious effort to crack the food and agriculture sector and we thought we would be tapping into a huge market. But that wasn't the case, the market for cyber just isn't there yet.

A lot of general cyber security best practice can be applied to food and farming, especially back-office operations. Farms, like so many small businesses, will be non-compliant with the law and could find themselves being fined.

There's also an opportunity for cyber startups to focus on protecting IoT devices and legacy hardware. Farmers think that these devices will be secure by design and that there's no risk, but that's really not the case.

"Food is behind ecommerce and finance but the penny is starting to drop."

- Chris Milnes, Lead Partner for the North East, Partners&

The pandemic changed the risk profile for our clients because supply chains shortened, which means that if one supplier experiences downtime it has a bigger impact. Lots of food businesses moved online and started selling directly to the consumer, digitising even further and changing their cyber risk profile.

We've seen an explosion of cyber-related claims over the past year across all sectors as criminals start attacking companies that haven't really invested in their cyber defences – and food has typically under-invested in cyber. Ransomware gangs are taking advantage of a lack of basic cyber hygiene to get into systems and businesses are being forced to pay Bitcoin or suffer delays to production. Whether you're making vehicle parts or pies, cyber criminals are coming for you.

One example of a threat is product safety and regulations around contaminants and labelling of allergens. The business and safety risks of ingredients or labels being altered are huge, which is forcing manufacturers to consider cyber risks that could lead to contamination. Food companies are not inherently more likely to be targeted but there are particular nuances that makes a cyber incident a threat to human health and safety.

From an insurer's point of view, we need to make sure clients are looking at their cyber risk posture, whether it's keeping software and hardware up to date or investing in education.

Food is behind ecommerce and finance but the penny is starting to drop. Cyber Essentials compliance is a start but it's quite vanilla. Food companies need to level up their cyber education and understand the business and reputational risks. This is a sector where margins are extremely tight. In this economic climate a hit could take months to recover from, which could be catastrophic. Smaller hits or ransom payments might not be business-ending but it affects profitability and this is what we're seeing among our client base.

The sector needs a wakeup call: just because you're further down the supply chain and you're a smaller brand doesn't mean you're safe.

"When you handle perishable goods, a delay of even just a few hours is incredibly critical."

- Toby Lewis, Global Head of Threat Analysis, Darktrace

Consumer-facing brands that care about reputational damage or food organisations handling perishable goods tend to be the ones that invest in cyber. With perishable goods, a delay of even just a few hours is incredibly critical.

Ransomware is a particular concern and what we're seeing is cyber espionage from nation states using similar tactics to criminal groups, and it's often hard to detect who's responsible.

Darktrace's AI-based approach to threat monitoring and management is very sector and threat agnostic. We've not had to reconfigure our core technology to protect food clients.

You could get ten different food companies in a room and each will use different technology stacks and have unique environments – so to assume that companies in the same sector have lots of similarities can be dangerous. With self-learning AI, you don't have any preconceptions and it learns from each situation.

"When they come for the Jaffa Cakes, that's when people will start to care about the cyber threats to food."

– Anonymous contributor

RECOMMENDATIONS, IDEAS AND OPPORTUNITIES

The food supply chain is entirely owned and operated by private businesses. But given how critical food is to our national security, the government can direct research, funding and innovation towards the most important areas...

POLICY, RESEARCH AND ECOSYSTEM

1. Defra, the Department for Digital, Culture, Media & Sport, the National Farmers Union, the Food Standards Agency and the NCSC can collaborate to review and prioritise threats, engage with the parts of the private sector most at risk and provide tailored cyber guidelines and advice. This will build on PAS 96 and the NCSC's existing sector-specific guidance for farmers.
2. Invest in applying existing research into the cyber implications of smart vehicles, the Internet of Things, 5G and drones to smart farming, including testing ideas and solutions in tabletop or real-world farm testbeds. Facilitate the sharing of insights, challenges and technology opportunities across domains.
3. Appoint a cabinet minister responsible for food, and enable cross-departmental collaboration between them and ministers responsible for cyber security and CNI.
4. Given that the National Cyber Strategy 2022 outlines a desire for the UK to be a "more influential and valued partner on the global stage, shaping the future frontiers of an open and stable international order while maintaining our freedom of action in cyberspace" , there's an opportunity to use Britain's soft power to share cyber security best practice, standards, research and cyber security technology with food sectors in the developing world that rely on technology to solve challenges like hunger, malnutrition, climate change and contamination.
5. Improve sector-wide awareness of the cyber risks to each part of the food chain, including SMEs. This should raise awareness of risks like reputational damage, financial costs, safety and the potential for fines.
6. The public sector can work with the private sector to make cyber security more accessible for SMEs and food organisations with smaller budgets. This will prevent supply chain vulnerabilities from entering via smaller, less protected suppliers.
7. Take a holistic definition of the food security threats that cyber could cause – while extensive shortages may be a less likely scenario food safety could also be affected.
8. The government can fund research, pilots and proofs of concepts to stimulate the supply and demand of security solutions for the food sector.

PRODUCTS AND INNOVATION

1. Pay particular attention to the threats of malware, ransomware and phishing when pitching cyber security solutions and developing or adapting new products for food clients.
2. There could be demand for supply chain security solutions such as always-on threat monitoring to help large companies have better oversight over their supply chain.
3. Explore opportunities to use existing AI technology for threat monitoring and response in the food sector without having to invest in altering the core product.
4. Start with cyber hygiene to raise standards. This could include password security, multi-factor authentication, firewalls and access controls.
5. Consider the context in which connected devices need to be protected and how legacy hardware is interacting with IoT, as well as the information the people using the machinery will need and their likely levels of cyber awareness.
6. Enable food businesses to build recovery and resilience plans – particularly in relation to ransomware. This could include network segmentation and air gaps, as well as following the NCSC's incident management guidance for what to do if you're attacked.
7. Address the lack of basic security controls and automated asset management for ICS networks.
8. Help food companies play catch-up with cyber and adjust their culture, processes and awareness levels.
9. There could be a market for immersive training that brings cyber security to life in food-specific contexts like fields and manufacturing plants where people interact with technology and food at the same time.
10. Patch vulnerabilities in outdated operational technology.
11. Follow the money. Sell to large food companies that are consumer-facing or target sectors like lab-grown meat where companies have received a large amount of investment.

REFERENCES

https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

https://research.nccgroup.com/wp-content/uploads/2020/07/agriculture-whitepaper-final-online.pdf

https://www.cpni.gov.uk/critical-national-infrastructure-0

https://www.gov.uk/government/statistics/food-statistics-pocketbook/food-statistics-in-your-pocket, while on a global level https://www.worldbank.org/en/topic/agriculture/overview#1

Feeding Britain: Our Food Problems and How to Fix Them, page 352

https://www.ipes-food.org/_img/upload/files/Concentration_FullReport.pdf

https://ourworldindata.org/future-population-growth

https://www.bcg.com/publications/2018/tackling-1.6-billion-ton-food-loss-and-waste-crisis.

https://www.un.org/sustainabledevelopment/sustainable-consumption-production/

https://www.just-food.com/news/food-related-global-commodity-prices-continue-upward-trend-fao/

https://foodfoundation.org.uk/initiatives/food-price-tracker

ahttps://www.ft.com/content/f42432cf-9cdb-48ee-abd5-d0f31428632c

https://www.agweb.com/news/business/taxes-and-finance/soaring-input-costs-cause-farmer-sentiments-drop-lowest-reading

https://www.bsigroup.com/en-GB/PAS-96/

https://specopssoft.com/blog/cyber-security-investing/

https://www.thebci.org/static/e02a3e5f-82e5-4ff1-b8bc61de9657e9c8/BCI-0007h-Supply-Chain-Resilience-ReportLow-Singles.pdf

https://committees.parliament.uk/oralevidence/412/pdf/

https://www.gov.uk/government/statistics/united-kingdom-food-security-report-2021/united-kingdom-food-security-report-2021-theme-2-uk-food-supply-sources#:~:text=Headline-,In%202020%2C%20the%20UK%20imported%2046%25%20of%20the%20food%20it,%C2%A321.4%20billion%20was%20exported.

Source: https://www.theguardian.com/uk-news/2021/jul/11/uk-food-supply-chain-vulnerable-to-cyber-attack-expert-warns

https://www.gov.uk/government/statistics/united-kingdom-food-security-report-2021

https://www.kroll.com/en/insights/publications/cyber/data-breach-outlook-2021

https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021/the-threa

https://s3.documentcloud.org/documents/21053966/fbi-bc-cyber-criminal-actors-targeting-the-food-and-agriculture-sector-with-ransomware-attacks.pdf

https://blog.malwarebytes.com/awareness/2021/09/fbi-warns-of-ransomware-threat-to-food-and-agriculture/

https://research.nccgroup.com/wp-content/uploads/2020/07/agriculture-whitepaper-final-online.pdf

https://foodanddrinknetwork-uk.co.uk/how-digitalisation-is-delivering-much-needed-efficiency-in-the-cold-chain/

https://www.bristol.ac.uk/cabot/what-we-do/cyber-security-food-security/

https://ieeexplore.ieee.org/document/9003290

https://ieeexplore.ieee.org/document/9003290

https://food.tomra.com/blog/how-digitalization-of-the-supply-chain-will-reduce-global-food-waste

https://ieeexplore.ieee.org/document/9003290

https://www.nature.com/articles/s43016-020-0097-7

https://www.verizon.com/business/resources/executivebriefs/2020/2020-cyber-espionage-executive-insights.pdf

https://www.mdpi.com/2305-6290/5/4/83/html

https://harperjames.co.uk/news/monopolising-cultured-meat-production

https://conservancy.umn.edu/bitstream/handle/11299/217703/FPDI-Food-ICS-Cybersecurity-White-Paper.pdf?sequence=1&isAllowed=y

https://foodprotection.umn.edu/research/food-and-cybersecurity

https://conservancy.umn.edu/bitstream/handle/11299/217703/FPDI-Food-ICS-Cybersecurity-White-Paper.pdf?sequence=1&isAllowed=y

https://www.tenable.com/blog/why-food-and-beverage-companies-should-crack-down-on-industrial-cyber-threat

https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/1708.pdf

https://ieeexplore.ieee.org/document/9003290

https://www.agweb.com/news/livestock/beef/us-cattle-slaughter-drops-27000-head-jbs-cyberattack-cripples-largest-beef

https://www.betterretailing.com/news/exclusive-kp-snacks-cyber-attack-hits-production-and-delivery-to-stores/

https://heimdalsecurity.com/blog/farming-cooperative-shut-down-by-ransomware/

https://www.wsj.com/articles/iowa-grain-cooperative-hit-by-cyberattack-linked-to-ransomware-group-11632172945

https://www.zdnet.com/article/after-ransomware-attack-company-finds-650-breached-credentials-from-new-cooperative-ceo-employees/

https://www.forbes.com/sites/leemathews/2022/03/14/china-linked-group-hacks-cow-monitoring-app-to-spy-on-six-states/?sh=2772532065c2

https://www.bbc.co.uk/news/uk-england-lancashire-59554433

https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

Registered address: c/o Delancey, 6th Floor, Lansdowne House,
Berkeley Square, London, W1J 6ER
Trading address: 14 East Bay Lane, The Press Centre, Here East
Queen Elizabeth Olympic Park, London, E15 2GW

Company Number: 10012478

Plexal (City) Limited
www.plexal.com

plexal