CYBER-RISK
AN ONGOING THREAT

How cyber-attacks are impacting our industry, and what can be done about it

by Caitlin Gittins, Milling and Grain magazine

At the beginning of last year, we were met with the disconcerting news that AKVA group, a major technology supplier present in global markets, had been victim of a cyber-attack and was believed to have been a ransomware attack.

For those who aren't clear on what this means – it typically refers to hackers entering a company's system and encrypting their data, then forcing the company to pay a ransom in order to gain back access to that important data.

The more sophisticated cyber gangs will despatch customer service members to communicate with the company, in order to make the payment of the ransom seamless.

In the particular attack against AKVA, their cage-based technology was targeted, and the damage was considerable: it cost AKVA a total sum of US$6 million and continued to be a headache for the company as they recovered from the financial impact.

The vulnerability of the food production sector

This was not the only major cyber-attack on a company involved in food production that featured in 2021 – major meat processing company, JBS, was hit with a similar attack and suffered major disruption.

In June of 2021, the company was forced to pay a ransom of US$11 million to 'protect its customers', as stated by the company. On top of this, it was forced to stop cattle slaughtering at all US plants for a day, impacting on their food supply and potential leading to higher food prices for consumers.

Both of these major attacks – certainly not isolated examples of the disturbance cyber-attacks can bring about – demonstrate the vulnerability of the food production sector and subsequent impact this can have on the food supply chain, as well as companies' exposed weaknesses and losses suffered in the aftermath.

> **"If you haven't been attacked yet, you will be attacked – or you're already being attacked, and you just don't know it yet. On average, the threat actors are in your system for up to four months prior to executing their attack."**
>
> CyberAg founder Andrew Rose

Food security and increased production are key to meeting growing global demands for animal protein, both of which are at risk from cyber-attacks. A cursory Google search will reveal historically vulnerable sectors to cyber threats, such as healthcare or finance, but increasingly, the food production sector is falling prey to such attacks, which we need to be aware of.

The reason behind this seems to partly rest in the increasing digitisation of agriculture and aquaculture. Automation in these areas has led to the utilisation of a variety of technologies and machinery, such as smart agriculture sensors, crop monitoring equipment, and recirculating aquaculture systems (RAS), among others.

In making the shift towards automated processes rather than manual labour, companies have increased their 'attack surface', which refers to the different areas in a system which an attacker can target.

Targeting these technologies can result in a number of detrimental outcomes, which not only disrupts production, but can also reduce farmers' confidence in adopting new technologies, as an example.

Protecting against the exploitation of increasing connectivity

Automated processes and digitisation of food production are not likely to disappear any time soon – and nor should they. Instead, the industry needs to learn the best practice for protecting itself against the exploitation of increasing connectivity, which is where cybersecurity measures come in.

As International Aquafeed tech editor Erik Hempel pointed out in his column in November 2021 edition, "larger aquaculture companies should now take this threat seriously, perhaps even hire specialised IT experts."

Recognising that food production sectors are vulnerable to cyber-attacks and large food production companies can be targets, is part of taking the steps needed in order to encourage awareness around cybersecurity and to reduce the risk of such attacks from happening, to ensure food security and continued production.

To gain a better understanding of what our sector faces today in terms of risk, Milling and Grain magazine spoke to James Simison from Sunderland Marine, an insurance company exclusively servicing the marine and aquaculture sectors.

"I think it's a tough one to speak about [cyber risk]," Mr Simison explains. "You don't know whether the more you talk about it, the more air you're giving it." Certainly, events such as the attack on AKVA group and JBS occupied the headlines for months after, even appearing in news sites unrelated to the food production sector like the BBC.

In terms of cyber risk within our industry, Mr Simison sees it as being incredibly impactful, from his perspective as a risk surveyor, which he describes as being tasked with assisting their underwriters with understanding risks on a "more technical basis" as well as providing support to the farms on the risks they face.

"As a fish farmer, using a barge or on an onshore feeding facility for remote feeding, being locked out of the system is a serious risk. For conscientious farmers it would be tough to not have that ability to care for your stock and maintain high husbandry standards. Having back-up systems in place to ensure the continuity of husbandry if there is a critical event is key, be it a cyber-attack or a breakdown in the system."

Having a financial impact

Husbandry is hugely important for fish farmers, Mr Simison outlines. "With the values involved, we have to be thorough." This is where Sunderland Marine comes into play as an insurer, "We have to carry out surveys before the farms come on risk to make sure we are satisfied."

When asked about the importance of training employees on a fish farmer, Mr Simison stresses its role against the risks faced.

As he puts it succinctly, "Any company's only as good as its staff, the company's now putting a huge amount of resources into making sure staff are as good as they can be, and that's across the board."

Drawing on his own experience working at a fish farm – as Sunderland Marine's Aquaculture Department employ those with a fish farming background so their employees better understand what a fish farmer faces in their day-to-day operations – he explains that a combination of a degree and hands-on experience worked well for him.

"I worked on a salmon farm for two or three years through university. I knew how to be a freshwater salmon farmer, but by going from the university point of view, that was supplemented it with learning about virology, feed, feed formulation and all the different diseases."

Protecting against financial & mortality losses

Sunderland Marine offer stock mortality insurance which covers a number of risks within the aquaculture sector, including dieseas, theft, storms, predation, pollution, and others.

Their breadth of services highlights that while prevalent, cybersecurity is one of many risks facing aquaculture today, and those risks have grown and evolved during Mr Simison's time at the company.

"I started in 2013 [at Sunderland Marine], when I left Orkney and Shetland," Mr Simison explains. "Amoebic gill disease was just about coming onto the radar; you were maybe treating a couple of times a cycle."

"Sea lice weren't an issue in Orkney," he adds, describing it as a 'phenomenon' because of this. "As the years have gone by, we're seeing more and more treatments being carried out per year, and the knock-on effet this is having on production." The combination of having to treat against parasites and other pathogens, he outlines, proves an ongoing battle against the detrimental effects of climate change.

Mr Simison's overview of risks facing the aquaculture sector indicates that as an insurance company, to encompass and insure against a number of risks is not only important, but crucial, in order to protect companies from financial and mortality losses posed by the growing risks and climate change.

A sense of complacency

The number of cyber-attacks being carried out are not decreasing – in fact, due to increased connectivity as a consequence of the pandemic and a marked number of employees working from home, there was a 63 percent increase in cyber-attacks related to the pandemic.

Additionally, companies were forced to shift their working to cloud networks, which left this form of data and information sharing vulnerable to attack. It seems crucial, now more than ever, to ensure companies are properly educated and informed on how to protect themselves, and the food supply chains they service.

CyberAg is an organisation that does exactly that. As a non-profit programme and an initiative of the Eastern Shore Entrepreneurship Center (ESEC), CyberAg was founded to fill a "quiet space", its founder Andrew Rose explains.

"There was a sense of complacency in the agriculture sector about cybersecurity risks. And on the other side, this cybersecurity community didn't really understand the needs of the food and ag supply chain."

Mr Rose's allusion to "other places" that require the attention of this community, rings true when looking at the attacks carried out on the healthcare sector, for instance. There was an increase of attacks carried out between November and December in 2020 by 45 percent.

This, however, does not dismiss agriculture as an equally important sector in terms of what is at stake. Access to food is an "essential human need," as Mr Rose puts it.

Learn how to protect your equipment

This is where CyberAg comes in. As a non-profit organisation, they were founded with the intention of bringing a level of awareness and resource to the food supply chain that was missing.

They partner with resources and provide them to food and agriculture as needed, working closely with law enforcement where necessary. They also work closely with F3 Tech, another initiative of ESEC, which provides funding and support for start-ups.

When asked if Mr Rose thought the automation of technologies had increased the 'attack surface' of agriculture and led to attacks such as those on JBS, Mr Rose's answer was clear.

"There's a strong move because of a lack of labour to the automation of all aspects of agriculture," he explains. "When you

Primary steps towards securing your company

As outlined by CyberAg's founder Andrew Rose

1. Have multiple and secure backups- to ensure that your data isn't lost in an attack
2. Keep systems updated - don't wait for these updates to come
3. Ensure your company is informed - hold workshops and tabletop exercises and keep up-to-date with current and future threats
4. Keep to multi-factor authentication - this will help keep devices protected and reduce the risk of hacking
5. Keep in contact with your law enforcement - have a phone number ready to call should an attack occur
6. Be proactive in your prevention - don't wait for an attack to happen

have all those different things plugging into the network … your attack surface has now got much, much greater."

The technology contributing towards this increased attack surface encompasses a great deal of equipment in agriculture and aquaculture, but more importantly, those adopting it need to learn how to protect it.

"People are very eager to get something out there that performs the way you would expect it to, but then security is sometimes an afterthought … Then the attack surface is not only increased, but then the vulnerabilities are larger as well."

To ensure companies are best protected as technology and attacks evolve hand-in-hand, Mr Rose has advice to give on the best practices, suggesting that a prepared, careful outlook is best.

"If you haven't been attacked yet, you will be attacked – or you're already being attacked, and you just don't know it yet. On average, the threat actors are in your system for up to four months prior to executing their attack."

Other steps include being proactive, and not waiting for automatic updates to your system, but to manually update yourself; ensuring you are in possession of secure backups as gangs targeting companies will frequently destroy backups and relevant data; and to embrace multi-factor authentication.

These are a few of the steps that should be taken, representative of the "new normal" Mr Rose acknowledges. He also recommends running a tabletop simulation to see if you are able to manage your business without access to the internet and getting in touch with your local law enforcement.

"Do a one day where there's no internet. Could you run your business? How would you run your business?" Equally important is being in touch with the authorities. "Just having that number ready rather than waiting until the airbag doesn't go off after you hit the telephone pole."

Cyber threats are ever evolving

As cyber criminals look for new ways to gain access to companies' information and details, including the emergence of deepfakes and 'vishing', which is a combination of 'voice' and 'phishing': where attackers utilise phone calls to pretend to be an employee of a company to gain information, or a bank employee.

There's no doubt about it - cyber threats are ever evolving.

With the ever-evolving, ever-growing cyber threats, it seems easy to despair about the future of the industry and how it will manage. There is one, bright light at the end of the tunnel however: the work CyberAg and countless other organisations do in is invaluable, in educating and supporting industry.

They take on an invigorated, spirited attitude towards cyber threats as best summarised by Mr Rose: "We are no longer going to sit back and wait for the punch to come."

What is the current advice for companies looking to improve their security and protect themselves against potential cyber-attacks? There's an abundance of information out there, so it's easy to become bogged down in information; the primary steps towards securing as outlined by Mr Rose can be found in the adjacent panel.

For those readers who are interested in learning more about cybersecurity and threats in agriculture, Mr Rose will be attending and hosting a table at the Animal AgTech Innovation Summit in San Francisco.

The conference will be running for a full day on March 21, where it will be addressing current issues within agriculture.