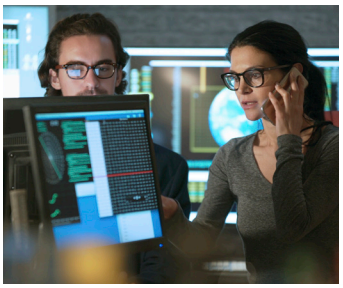
Preparing for a Cyber Attack



With the onset of the pandemic, much of the workforce transitioned to working remotely, creating an environment in which ransomware attacks have increased by 148%. Bad actors have discovered a rich environment of unsecured WiFi, vulnerable equipment and outdated intrusion prevention software. Attacks are not only more frequent, but they're also swifter – a new remote desktop protocol is discovered just 90 seconds after it's opened to the Internet. FCCS has been hyper-focused on researching best practices and ensuring that the Farm Credit System is properly guarded against cyber and ransom attacks.

According to Marsh Consulting, a global leader in insurance broking and risk management, ransomware has become an industry and every organization is a potential target. Those that take a robust approach to ransomware preparation can increase their odds of avoiding an attack, recover more quickly and minimize the impact of an attack.

"Most Farm Credit entities are already exercising great cyber hygiene by updating their IT systems regularly and performing necessary patches," says Naomi Baumann, Director of Claims & Loss Prevention, FCCS. "However, there is still the risk of cyber attacks, including ransomware, so it's imperative that each organization prepare for the eventuality of an attack."

Attacks now routinely disrupt operations for days or weeks; the average downtime in the fourth quarter of 2020 was 21 days. In addition to downtime, the remedial expenses and ransomware demands have skyrocketed. More than 70% of attacks now also include data exfiltration. Add regulatory and compliance considerations and the issue becomes even more complex. Companies with poor cyber hygiene can become low-hanging fruit.

To prevent or minimize the impacts of a cyber event, it's essential that every organization prepare and plan its response in advance of a cyber attack by developing – and keeping current – an effective cyber incident response plan (IRP) that includes ransomware scenarios. Once your incident response plan is in place, evaluate it with a hypothetical ransomware tabletop exercise.

Farm Credit entities should also develop a decision-making framework to analyze whether data and systems can be restored once a ransomware event occurs and whether it makes sense to pay an extortion demand. FCCS recommends engaging pre-approved Beazley counsel to help develop and review the framework.

Farm Credit organizations should establish ransom payment criteria, to include the amount of the initial extortion demand, the threat actor's track record and an estimate of the length of time to restore data and systems using the decryption code. Criteria should also address circumstances where the threat actor demands payment in exchange for not releasing stolen data to the public.

"Once a ransomware event occurs, we recommend reporting the incident to FCCS immediately so that we may facilitate discussions with Beazley and connect you with the appropriate experts who can assist in this area," says Naomi.

Marsh recommends having an external extortion service provider review your payment criteria, and also maintained as a resource in the event of an attack – they can typically provide threat intelligence, negotiate with threat actors, ensure compliance with regulations and restrictions, procuring cryptocurrency and conducting payment transactions. Organizations should also identify a law firm that specializes in cyber security and data protection and a digital forensics incident response provider.

"When identifying cyber attack response providers, we strongly recommend that Farm Credit organizations use vendors that are pre-approved by Beazley, our insurance provider, or to contact us if they want to engage a non pre-approved vendor so that we may have appropriate discussions with Beazley," says Naomi. "If an organization prefers to work with a vendor not included on Beazley's pre-approved list, please reach out to us to discuss next steps."

Underscoring incident preparedness and response is cyber insurance, which has continued to be a hot topic in the global insurance market and within Farm Credit.

"FCCS is continuing to increase the coverage limits for our cyber insurance program, as well as exploring the possibility of adding cyber insurance as an additional coverage to the self-insurance we have within The Farm Credit System Association Captive Insurance Company," says Lisa Parrinello, Director of Underwriting and Insurance Programs, FCCS. "We're expecting that the commercial insurance market will significantly increase rates, increase retentions and reduce coverage, but expect that adding this coverage to our System-owned insurance company will help to mitigate these market conditions. As we get closer to the 2022 insurance renewal, we will continue to advise on the state of the insurance market and our efforts to increase coverage limits."

FCCS is also available to review and provide feedback on Farm Credit organizations' IRPs, or to participate in tabletop exercises. Contact Naomi Baumann at 303.721.3263 for more information.

Article content courtesy of Marsh Consulting.