Cyber Insurance

It's a cyber security industry tenet that the question for any business isn't "if" they'll have a breach, but "when" it will happen. When it does happen, the costs can be high, hitting both a company's balance sheet and its reputation.

For the past 15 years, FCC Services' Risk Management department has placed cyber security insurance coverage on behalf of all Farm Credit System entities. During this same period, the coverage has evolved and expanded to provide insurance protection against dynamic and emerging risks as a result of the rapidly changing technology landscape. For 2019, the per claim and annual aggregate limits were respectively increased to $65 million and $115 million for all Farm Credit entities combined.

"We increased the cyber insurance limits recognizing that continued consolidation within Farm Credit means greater concentration of assets under management aggregated within fewer organizations. This dynamic increases the potential for risk," says Larry Lawson, Executive Vice President, Risk Management and Insurance for FCC Services. "We continually assess the changing risk landscape for all lines of coverage, not only within Farm Credit but for the financial institution sector overall. This process helps in comparing and contrasting Farm Credit risks to those of other financial institutions and differentiates the System's risk profile from other insureds."

Cyber insurance covers multiple potential aspects of a cyber attack, including the costs of repairing and/or replacing damaged data, forensic specialists to identify what the breach entailed, privacy notification costs, and other expenses associated with mitigating the loss. The coverage also affords access to a number of additional services and experts provided by the panel of cyber insurers.

The exposure to cyber risks is real for Farm Credit entities – nearly 50 incidents have been reported since 2004, including nine in 2018.

"When you think about the size and scope of the Farm Credit System, it's surprising that we haven't had more incidents," says Don Sicard, FCC Services' Vice President, Risk Management and Insurance. "Attacks are going on every day across business sectors, especially financial institutions. The big breaches get reported, but most incidents are much smaller in impact, usually measured in hundreds of thousands of dollars, not millions."

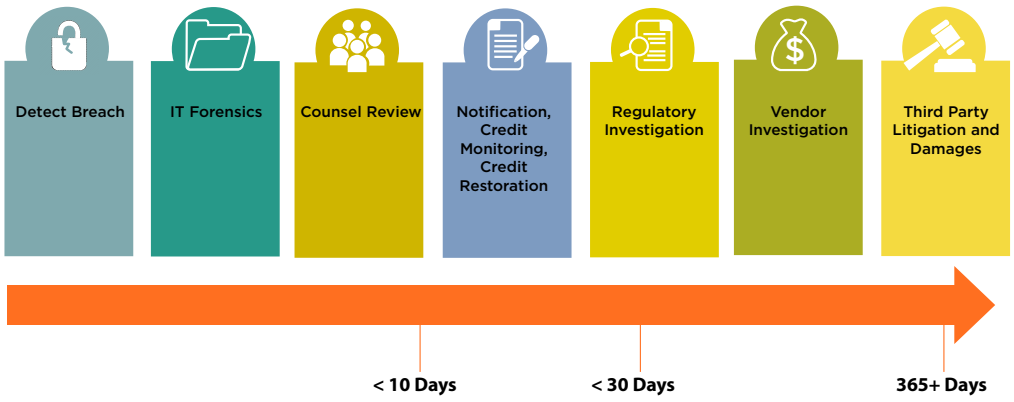
A cyber incident doesn't have to be a hacker breaching a system from afar: stolen laptops or servers storing Personal Identifiable Information (PII) are common risk exposures addressed by cyber insurance. And insiders can cause losses, too, either intentionally or accidentally through carelessness or manipulation by bad actors.

Most organizations today accept the notion that at some point they'll experience a breach, and so their focus is on mitigating risk exposure and understanding their cyber insurance coverages. When an institution does experience an incident or attack, the following steps are necessary to mitigate the potential for loss and reputational damage:

- Identify that a breach or cyber attack has occurred and the type of attack, such as malware, unauthorized network access, loss of equipment, social engineering attack or extortion.
- Immediately inform and involve your general counsel to maintain client/attorney privilege and provide guidance through the next stages of an investigation, notification and potential litigation.

- At the same time, take immediate action depending on the type of attack, including disabling the impacted accounts, changing passwords, filing a police report, etc. There are multiple short-term steps depending on the circumstances involved. FCC Services, with its specialized team of cyber insurance brokers and insurers, can assist in identifying appropriate steps and resources, including access to a myriad of IT, forensic and legal partnerships.
- Contact FCC Services by calling 800.233.8305 or completing a Network Security Claim Form located on our Risk Management website to initiate an incident report and/or claim notification.

Timeline of a Breach



Source: NetDiligence