WHITEPAPER

The Cost of Inaction:

Why Cybersecurity Complacency is an Existential Threat to Rural America's Financial and Physical Infrastructure

A FieldSafe Cyber Defense Publication

Authored by:
Dave Johnson, Cybersecurity Specialist, SunStream
JD Harris, CEO, Argent Reach
Mike Haldane, CEO, MarketWise Advising

SunStream | Argent Reach
2026

About FieldSafe

FieldSafe is a SunStream cybersecurity advisory offering for agricultural lending institutions, supported by specialist expertise from Argent Reach. FieldSafe brings together frontline incident response expertise, regulatory knowledge, and deep familiarity with the operational realities of Farm Credit to help institutions understand, govern, and reduce their exposure to a rapidly evolving threat landscape.

FieldSafe works alongside institutions to build incident ready programs that perform under real-world conditions, not just on audit day.

www.sunstreamservices.com/fieldsafe

© 2026 SunStream. FieldSafe is a SunStream initiative, in collaboration with Argent Reach. All rights reserved. |

Executive Summary

The cybersecurity conversation in rural America has been dominated by a single question: what does it cost to protect ourselves? This white paper argues that Farm Credit institutions and agricultural lenders are asking the wrong question. The more consequential question, and the one that regulators, boards, and community leaders are only beginning to reckon with, is what it costs to do nothing.

Farm Credit institutions and agricultural banks sit at the center of a web of rural economic interdependence. They provide the operating credit that finances planting, inputs, and equipment for the farming businesses and cooperatives they serve. When a Farm Credit institution is compromised by ransomware during spring planting, the harm does not stay within the institution. It propagates outward to farmers who cannot access operating lines when seed purchase windows close, to input suppliers whose receivables go uncollected, and to rural communities whose economic health is directly coupled to whether agricultural credit flows on time.

This paper examines the compounding costs of cybersecurity inaction across four dimensions: direct financial loss, operational disruption during critical seasonal windows, cascading harm to the borrowers and communities Farm Credit serves, and the long-term erosion of trust and institutional viability. It draws on documented incidents from agricultural lending and the broader rural infrastructure that farm businesses depend on. Those broader examples, drawn from rural water systems, electric co-ops, and grain cooperatives, are included not because FieldSafe serves every sector described, but because the communities Farm Credit institutions serve depend on all of these systems functioning together.

The finding is direct: inaction is not a neutral choice. For the farm businesses, cooperatives, and rural communities that depend on agricultural credit infrastructure, the cost of doing nothing is not theoretical. It is existential.

1. The Ecosystem That Farm Credit Serves

Farm Credit associations and agricultural lenders do not operate in isolation. They are the financial anchor of a rural economic ecosystem that includes the farm businesses they lend to, the input cooperatives and dealers those businesses depend on, the grain elevators and marketing cooperatives that handle production, the rural electric cooperatives that power farm operations, and the water and communications infrastructure that sustains rural communities. Understanding cybersecurity risk in agricultural lending requires understanding this ecosystem, because a disruption to any part of it creates consequences that ripple through the rest.

This interdependence is both the defining characteristic of rural economies and their primary vulnerability. In urban financial services, a borrower whose bank experiences a disruption can typically access credit through an alternative provider, use a different payment network, or manage a brief interruption without lasting harm. In rural agricultural lending, these alternatives frequently do not exist. For many agricultural borrowers, the Farm Credit association is not one of several options. It is the primary option. When it fails, there is no fallback.

The borrowers Farm Credit serves, the farm businesses and rural cooperatives that depend on seasonal operating credit, face an equally constrained environment. A farmer operating on a $2 million seasonal operating line does not have the financial reserves to absorb a two-week delay in accessing credit during planting season. An input cooperative that cannot receive payment from a lender whose systems are

© 2026 SunStream. FieldSafe is a SunStream initiative, in collaboration with Argent Reach. All rights reserved. |

locked by ransomware cannot easily float that receivable. The downstream cascade from a Farm Credit cybersecurity failure reaches into the agricultural supply chain in ways that compound rapidly and reverse slowly.

The Seasonal Dependency

Agricultural lending concentrates its most critical operations into narrow seasonal windows that have no equivalent in commercial banking. The spring operating line season, typically running from late February through early May, represents the majority of new loan origination for many Farm Credit associations. A cyber incident during this window does not create the same consequences as an incident in December. It creates borrower harm that cannot be fully reversed after the fact, and that may affect borrower relationships and credit quality for years.

The communities Farm Credit serves also depend on rural infrastructure, including electric cooperatives, water districts, and grain cooperatives, that shares many of the same cybersecurity vulnerabilities that agricultural lending institutions face. These sectors appear in this paper because the farm businesses and rural communities that Farm Credit serves cannot thrive if the surrounding infrastructure fails. The cybersecurity posture of Farm Credit institutions is embedded in a larger ecosystem and understanding that ecosystem context matters for appreciating the full scope of what is at stake.

2. What Has Already Happened: Documented Incidents

The case for cybersecurity investment in agricultural lending does not rest on hypothetical threat models. It rests on a documented and growing record of incidents that have caused real harm to agricultural lending institutions, their borrowers, and the rural communities they serve. The following examples are drawn from publicly reported incidents.

Agricultural Lending and Farm Credit Institutions

Agricultural lending institutions have experienced ransomware attacks that have locked loan origination and core banking systems during planting season, business email compromise schemes that have redirected wire and ACH payments tied to grain elevator settlements, and data breaches exposing borrowers' financial information. Most incidents are not reported publicly in detail. The documented pattern is consistent: attacks are timed to periods of maximum operational pressure, ransom demands are calibrated to the institution's urgency to restore function, and recovery timelines are structurally incompatible with the seasonal windows that define agricultural lending.

The Farm Credit Administration's CFR Part 609 cyber risk management rule, effective January 1, 2025, now requires Farm Credit System institutions to implement comprehensive cyber risk programs, in part because regulators recognized that the sector's previous approach was inadequate for the threat environment it faces. Institutions that cannot demonstrate structured governance programs and tested incident response capabilities face growing examination risk alongside the operational consequences of a poorly managed event.

The Cooperatives and Infrastructure Farm Credit Borrowers Depend On

© 2026 SunStream. FieldSafe is a SunStream initiative, in collaboration with Argent Reach. All rights reserved. |

In September 2021, NEW Cooperative, a Fort Dodge, Iowa grain cooperative with roughly 60 elevator locations, was hit by Black Matter ransomware. The co-op took its systems offline during harvest, fell back to paper tickets, and needed about eight weeks to fully rebuild. No lender systems were compromised, but the incident shows how a third-party outage can reach Farm Credit indirectly: producers' repayment depends on grain proceeds flowing on time, those proceeds are often pledged collateral, and cooperatives like NEW are themselves Farm Credit borrowers..

Rural electric cooperatives, which power the farming operations that Farm Credit finances, have experienced ransomware events that locked member management and billing systems for days or weeks. Rural water systems serving farm communities have faced control system compromises that threatened service continuity. In February 2021, allegedly a threat actor gained remote access to the water treatment system for Oldsmar, Florida and briefly altered chemical concentrations. In 2023 and 2024, a series of attacks targeted water and wastewater systems across the United States, exploiting industrial controllers running default credentials and accessible from the internet. These incidents affected the same rural communities that Farm Credit serves, and they illustrate the breadth of the threat environment in which agricultural lending institutions operate.

Institution Type	Risk Exposure and Consequence for Farm Credit Ecosystem
Farm Credit Associations and Ag Banks	Ransomware on loan origination and core banking; ACH fraud on settlement payments; regulatory exposure under CFR Part 609; borrower harm during seasonal windows
Farm producers (borrowers)	Payment diversion and wire fraud on equipment and land transactions; online banking account takeover; disruption of precision ag and livestock control systems; direct impact on loan repayment and operating liquidity
Agricultural Cooperatives (borrowers)	Ransomware on receiving and settlement systems; disruption of commodity transactions tied to Farm Credit loan performance; member financial distress
Rural Electric Cooperatives	Ransomware on billing and member systems; operational disruption to farming operations financed by Farm Credit; community-level service loss
Rural Water Districts	Industrial control system compromise; public health exposure; operational disruption to farm communities Farm Credit serves
Input Dealers and Suppliers	Business email compromise; payment diversion; disruption of the supply chain that operating credit is designed to finance

© 2026 SunStream. FieldSafe is a SunStream initiative, in collaboration with Argent Reach. All rights reserved. |

3. The Compounding Cost of Doing Nothing

Cybersecurity investment decisions at agricultural lending institutions are frequently framed as a cost question: how much does protection cost? This framing compares a known, immediate expense against a risk that feels uncertain and remote. The more accurate framing compares the cost of a proportionate program against the documented and compounding cost of an incident, including all of the ways that a cyber event creates harm beyond the institution's own technical recovery.

Direct Financial Loss

The direct financial costs of a significant cyber incident at an agricultural lending institution are substantial and frequently exceed what leadership expects. Ransom demands against financial institutions have ranged from tens of thousands to several million dollars, with average payments in the United States exceeding $1.5 million in recent years. Payment does not guarantee recovery: a significant percentage of organizations that pay ransoms do not receive fully functional restoration and must pursue backup recovery regardless.

Beyond the ransom itself, direct costs include forensic investigation, legal counsel, regulatory notification and response, system restoration and replacement, credit monitoring for affected individuals, and cyber insurance deductibles. For a mid-sized Farm Credit association, a total incident cost in the range of $2 million to $7 million is a documented range from comparable financial institutions. Many agricultural lending institutions carry cyber insurance, but coverage gaps are increasingly common as insurers tighten underwriting requirements around multi-factor authentication, offline backups, and endpoint detection.

Seasonal Consequences and Borrower Harm

For agricultural lenders, the timing of a cyber incident is as consequential as its severity. A ransomware event that takes a Farm Credit institution’s systems offline for two weeks in December causes disruption and recovery costs. The same event during the first two weeks of April, when operating line renewals are at peak volume and input purchase windows are closing, causes all of that plus borrower harm that cannot be fully reversed.

The seasonal consequence arithmetic is unforgiving. A farmer who cannot draw on an operating line during a planting window does not simply delay operations by two weeks. A meaningful delay may mean a changed crop mix, a reduced planted area, or in the worst circumstances, a missed season. The lender's systems come back online; the farmer's crop year does not restart. The lender measures its recovery in days. The borrower may measure the consequences in years, and the credit relationship may not survive them.

Cascading Community Harm

Farm Credit institutions are not analogous to commercial banks whose customers can route around a disruption. In most rural markets, the Farm Credit association is the primary agricultural credit provider. When it cannot function, there is no alternative. This absence of alternatives amplifies community harm from a cyber incident in ways that have no parallel in urban financial services.

The reputational consequences compound the operational ones. Farm Credit institutions operate on trust built over decades of relationship banking. A cyber incident that is disclosed late, that exposes borrower financial data, or that results in unreachable service during a critical period can damage that

© 2026 SunStream. FieldSafe is a SunStream initiative, in collaboration with Argent Reach. All rights reserved. |

trust in ways that take years to rebuild. In rural markets where membership relationships and community standing define institutional identity, reputational damage from a cyber event can have permanent effects on the institution's market position.

Regulatory and Legal Exposure

Farm Credit Administration's CFR Part 609, effective January 1, 2025, requires each Farm Credit System institution to implement a comprehensive cyber risk program commensurate with its size, risk profile, and operational complexity. Institutions that cannot demonstrate structured governance programs and tested incident response capabilities face growing examination risk alongside the operational consequences of a poorly managed event.

Legal exposure compounds the regulatory risk. Borrowers who suffer harm from a cybersecurity failure at their lending institution have pursued civil claims. Directors and officers who cannot demonstrate appropriate oversight of cybersecurity risk face personal liability exposure. The combination of regulatory penalties, litigation costs, and recovery expenses has proven financially destabilizing for some smaller institutions.

> **The Compliance Floor Is Not the Safety Ceiling**
>
> *Institutions that achieve regulatory compliance without achieving operational readiness have not solved the problem. They have documented it. The gap between passing a CFR Part 609 examination and surviving a ransomware event during planting season is where the real cost of inaction lives. Regulators evaluate governance frameworks. Attackers evaluate vulnerabilities. These are not the same assessment.*

4. The Existential Dimension

Most cybersecurity conversations focus on the costs the institution bears directly: recovery expenses, regulatory penalties, reputational damage. These are significant. But for Farm Credit institutions serving communities with no alternatives, the more important question is not what the institution loses in a cyber incident. It is what the borrowers and communities it serves lose.

When Institutions Cannot Recover Fully

Not every agricultural lending institution that experiences a significant cyber incident emerges fully intact. The combination of direct recovery costs, regulatory penalties, and reputational damage has in some cases proven too much for smaller institutions, leading to forced mergers, reduced service areas, or significant tightening of credit standards during recovery. For communities where a Farm Credit association provides the majority of agricultural credit, an institution that emerges weakened from a cyber event may serve its market less effectively for years afterward.

For farm businesses and cooperatives that depend on that credit, the consequences of a weakened lender are not abstract. Tightened underwriting standards, reduced local decision-making authority, and the loss of the relationship-based credit culture that distinguishes agricultural lending from commercial banking are consequences that affect borrowers directly and durably.

© 2026 SunStream. FieldSafe is a SunStream initiative, in collaboration with Argent Reach. All rights reserved. |

Food Security and National Resilience

The individual incidents described in Section 2 are significant in their local context. Aggregated, they reflect a pattern of increasing adversarial attention to agricultural finance and food production infrastructure. The Cybersecurity and Infrastructure Security Agency has designated food and agriculture as a critical infrastructure sector. The FBI and CISA have issued joint advisories specifically warning agricultural cooperatives and rural financial institutions of ransomware campaigns timed to critical operational periods.

Nation-state actors have demonstrated both the capability and the intent to target agricultural and financial infrastructure as part of broader efforts to create economic disruption. The Volt Typhoon campaign, publicly attributed to Chinese state-sponsored actors, targeted electric utilities and critical infrastructure providers for pre-positioning purposes. While the specific targets named in public advisories include utilities and communications providers rather than Farm Credit institutions directly, the agricultural ecosystem that Farm Credit finances, including the cooperatives, utilities, and supply chain infrastructure that borrowers depend on, sits squarely within the broader target profile. A Farm Credit institution that is not itself a named target is still embedded in an ecosystem that is.

The Nation-State Awareness

In 2023, U.S. government agencies publicly warned that nation-state actors had pre-positioned capabilities within U.S. critical infrastructure, including utilities and financial systems, for potential use in future conflict or as leverage in geopolitical disputes. Agricultural finance and food production infrastructure are explicitly identified in threat advisories as sectors of adversarial interest. Farm Credit institutions that operate without robust cybersecurity programs are part of a risk surface that extends beyond any single institution.

5. Why Inaction Persists: The Barriers to Investment

Understanding the cost of inaction does not automatically produce action. Agricultural lending institutions face specific barriers to cybersecurity investment that are worth examining directly, because solutions that do not address these barriers will not be adopted regardless of how compelling the risk case.

The Perceived Cost of Protection

The most commonly cited barrier to cybersecurity investment at agricultural lending institutions is cost. Cybersecurity is perceived as large, complex, and expensive, requiring specialized staff and technology that most institutions cannot afford. This perception is partially accurate and largely outdated. The managed security services market has matured significantly, and purpose-built offerings for agricultural lending institutions now provide meaningful protection at cost points accessible to Farm Credit associations and agricultural banks. The relevant comparison is not the cost of an enterprise security program at a major bank. It is the cost of a proportionate, sector-specific program against the documented cost of an incident.

The Expertise Gap

© 2026 SunStream. FieldSafe is a SunStream initiative, in collaboration with Argent Reach. All rights reserved. |

Many agricultural lending institutions have genuinely struggled to find cybersecurity expertise that understands their operational environment. A cybersecurity vendor whose practice was built serving commercial banks may not understand the seasonal risk dynamics of agricultural lending, the regulatory requirements specific to Farm Credit, or the borrower relationships that define how communication must be managed during an incident. The result is advice that is technically sound but operationally misaligned, and institutions that have tried to engage with the cybersecurity market and come away unconvinced that anything available fits their situation.

The Governance Gap

At many agricultural lending institutions, cybersecurity is treated as an IT department responsibility rather than a board-level governance issue. This framing creates a structural problem: the people responsible for cybersecurity decisions do not have the authority to make the investments required, and the people with that authority have not been given the information they need to understand why the investment is necessary. CFR Part 609 is changing this by requiring board-level engagement with cyber risk governance, but regulatory pressure is a lagging indicator. The best positioned institutions when the next significant incident occurs will be those whose boards addressed this before a regulatory requirement forced them to.

Barrier to Investment	The More Accurate Frame
We cannot afford a cybersecurity program	Compare the cost of a proportionate program against the documented cost of a single significant incident. A mid-sized Farm Credit association facing a planting-season ransomware event is looking at $2 million to $7 million in total incident costs.
We are too small to be a target	Attackers calibrate their demands to urgency, not institution size. Seasonal dependencies make agricultural lenders highly susceptible to pressure during critical windows.
We have not been attacked yet	Absence of a known past incident is not evidence of future immunity. Many intrusions go undetected for weeks or months before they become visible.
Our IT staff handles security	Cybersecurity is a governance and operational challenge, not just a technical one. Board-level engagement is now a regulatory requirement under CFR Part 609.
We passed our last examination	Examiners evaluate governance frameworks. Attackers evaluate vulnerabilities. Passing an audit does not mean the institution would survive an incident during planting season.

© 2026 SunStream. FieldSafe is a SunStream initiative, in collaboration with Argent Reach. All rights reserved. |

6. A Framework for Action: From Inaction to Proportionate Defense

The answer to the cost of inaction is not the adoption of an enterprise cybersecurity program designed for a major financial institution. It is the adoption of a proportionate, sector-specific program designed for the operational reality of an agricultural lending institution with the staffing, budget, and risk profile that actually exists. The following framework identifies the investments that deliver the greatest risk reduction for Farm Credit associations and agricultural banks at each stage of a cybersecurity maturity journey.

Foundation: The Non-Negotiable Baseline

The majority of successful attacks against agricultural lending institutions exploit failures at the baseline level, not sophisticated zero-day vulnerabilities. The baseline includes multi-factor authentication on all remote access and administrative accounts, offline and tested backups of critical systems including core banking and loan origination platforms, patching of internet-accessible systems within hours or days of vendor release, and elimination of default credentials on all network equipment and third-party applications. These are discipline measures more than technology investments. They require policy, process, and consistent follow-through. And they eliminate the attack vectors responsible for the majority of documented incidents against comparable institutions.

Protection: Continuous Monitoring and Detection

Beyond the baseline, agricultural lending institutions benefit most from continuous monitoring that identifies threats before they escalate into incidents. For most institutions, this means a managed security service providing 24/7 monitoring of network traffic, endpoint activity, and authentication events, with alerts and response support calibrated to the institution's operational environment and staffing constraints. The value of continuous monitoring is the reduction in dwell time, the period during which an attacker is active in the environment before detection, which is directly correlated with incident severity and recovery cost.

Resilience: Tested Response and Recovery

The investment that most directly addresses the cost of doing nothing is a tested incident response capability. As the Right of Bang white paper in this series examines in detail, there is a meaningful difference between having an incident response plan and having an incident response capability. For agricultural lending institutions, the most valuable resilience investments are tabletop exercises built around sector-specific scenarios including planting-season ransomware and harvest-period ACH fraud, pre-established relationships with cybersecurity legal counsel and forensic investigators, and continuity plans that are integrated with the institution's operational calendar and simulated against the seasonal scenarios that matter most.

A proportionate cybersecurity program for a mid-sized Farm Credit association delivers meaningful risk reduction at a fraction of the documented cost of a single incident, which for comparable financial institutions ranges from $2 million to $7 million. The return on investment is not ambiguous.

Conclusion: The Question Is Not Whether, But When

Farm Credit associations and agricultural lenders did not choose to become cybersecurity targets. They became targets because they are critical to the communities they serve, because their operational

© 2026 SunStream. FieldSafe is a SunStream initiative, in collaboration with Argent Reach. All rights reserved. |

calendars create predictable windows of maximum vulnerability, and because they have historically underinvested in defenses relative to the risk they carry.

The threat is not static. Ransomware operations have learned to time their attacks to create maximum pressure on institutions with seasonal dependencies. Social engineering schemes are becoming harder to detect and easier to execute at scale. Nation-state actors have pre-positioned capabilities in financial and agricultural infrastructure. The window for proactive investment, already narrower than it was five years ago, is narrowing further.

For the farm businesses, cooperatives, and rural communities that depend on Farm Credit institutions, a cyber incident at their lender is not only the institution's problem. It is a production problem, a cash flow problem, and in some circumstances a community stability problem. The cost of doing nothing at the institutional level is borne by the borrowers and communities the institution exists to serve.

FieldSafe was built to help Farm Credit institutions and agricultural lending organizations answer the cybersecurity challenge with proportionate, sector-specific programs that actually fit the operational reality of agricultural lending. The conversation starts with an honest assessment of where the institution stands, where the real risks are greatest, and what a practical plan to close the gaps looks like. Institutions that do that work before an incident occurs are the ones that come out the other side intact, with their borrower relationships, their regulatory standing, and their community trust preserved.

Disclaimer

This whitepaper is intended for informational and educational purposes only. It does not constitute legal, regulatory, or compliance advice. Agricultural lending institutions should consult qualified legal counsel and subject matter experts when developing cybersecurity programs and governance frameworks. The views expressed represent the perspectives of FieldSafe based on practitioner experience and publicly available information. Incident examples cited are drawn from publicly reported sources and are presented as illustrative of broader documented patterns.

© 2026 SunStream. FieldSafe is a SunStream initiative, in collaboration with Argent Reach. All rights reserved. |