WHITEPAPER

Right of Bang:

When the Plan Fails and the Clock is Running

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
July 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 resilience programs that perform under real-world conditions, not just on audit day.

Executive Summary

Every agricultural lending institution has a cyber incident response plan. Very few of them have tested whether that plan actually works when the pressure is real, the timeline is compressed, and the decisions have to be made by people who have never been in that situation before.

The military concept of "Right of Bang" refers to what happens after an event that cannot be reversed, meaning after the explosion, after the breach, and after the ransomware has deployed. It is the window in which every decision matters and in which organizations that have prepared perform dramatically better than those that have only planned.

For agricultural lending institutions, that window is uniquely dangerous. A poorly managed cyber incident during planting season or harvest settlement does not stay contained to the institution's systems. It cascades into borrower harm, regulatory scrutiny, and reputational damage within days, sometimes within hours. The consequences of getting it wrong are measured not just in recovery costs but in the financial stability of the farms and rural communities these institutions exist to serve.

This whitepaper examines what consistently breaks in the critical hours and days following a cyber event, why those failures are predictable and preventable, and what a resilience program designed for real-world performance rather than audit compliance looks like for agricultural lending institutions. Institutions that have done this work before an incident occurs are the ones that come out the other side intact.

1. The Difference Between a Plan and a Capability

There is a meaningful and often overlooked distinction between having an incident response plan and having an incident response capability. Most agricultural lending institutions have the former. Very few have built the latter.

The plan is a document. It describes what should happen when a cyber incident occurs: who gets called; what systems get isolated; how communications flow; and when regulators get notified. Plans can be thorough, well-structured, and expertly formatted. They can satisfy every examiner’s checkbox and pass every audit review. And they can fail completely when the situation they describe actually arrives.

A capability is what happens when the document meets reality. It is the muscle memory built through practice, the decision authority that holds under pressure, the communication channels that function when primary systems are down, and the leadership confidence that comes from having navigated a simulated crisis before facing a real one. Capabilities are built through testing. They cannot be written into existence.

The gap between plans and capabilities is widest in organizations that have never experienced a significant incident. Agricultural lending institutions, which have historically faced lower cyber threat volumes than commercial banks, are particularly susceptible to this gap. Their plans are often adequate on paper and entirely untested in practice. The first real test of those plans is the incident itself.

> **The Planning Paradox**
>
> *Institutions that invest the most in developing detailed incident response plans often invest the least in testing them. The existence of a comprehensive plan can create a false sense of readiness that actually reduces the urgency to build real capability. The plan becomes the destination rather than the starting point.*

This white paper is not an argument against planning. Plans matter. But in agricultural lending institutions specifically, the planning instinct has outpaced the testing instinct by a wide margin, and that imbalance creates risk that no amount of additional planning will address.

2. What Consistently Breaks: The Anatomy of Incident Response Failure

Cyber incident response failures in agricultural lending institutions are not random. The same failure modes appear repeatedly, across institutions of different sizes, with different technology stacks and different regulatory environments. Understanding these patterns is the first step toward preventing them.

Decision Authority That Evaporates Under Pressure

The most common and most consequential failure in incident response is the collapse of decision-making authority at the moment it is most needed. Every incident response plan assigns roles and responsibilities. In practice, those assignments frequently break down when the incident is real.

The breakdown follows a predictable pattern. The person formally designated as the incident commander is often the CISO or IT Director, because they're someone with strong cybersecurity and technical knowledge. However, they often possess limited organizational authority over lending operations, legal, or communications. Most have never experienced an actual incident, much less the hundreds that are necessary to do the role well. When the incident escalates and requires decisions that affect loan processing, borrower communications, or regulatory notification, the designated incident commander finds themselves without the authority or experience to make those calls. They escalate to the CEO or CFO. Those leaders, who have not rehearsed the scenario and are receiving fragmented information under pressure, and are even less qualified in cyber, slow the response while they seek clarity that may not be available.

In agricultural lending institutions, this authority gap is often compounded by geography. Senior leadership may be distributed across multiple offices or traveling during critical periods. The incident may surface first with a junior IT staff member at 11 PM on a Thursday in early April. The chain of escalation to someone with real authority to authorize a system shutdown or approve an external communication may take hours, even when the attacker is still active in the environment.

Communication Failures Between IT, Legal, and Executive Leadership

The second consistent failure mode is the breakdown of communication between the three functions that must work in close coordination during a cyber incident: IT, legal counsel, and executive leadership. Each of these groups has a different vocabulary, a different set of priorities, and a different frame for what the incident means. Under pressure, without a shared structure for communication, they frequently talk past each other in ways that slow the response and create compounding errors.

IT teams communicate in technical terms that legal counsel and executive leaders may not understand or may misinterpret. Legal counsel, appropriately focused on privilege protection and regulatory liability, may create communication barriers that IT and operations need to cross to do their jobs. Executive leaders, seeking information to manage board and regulatory relationships, may pull senior IT staff away from containment work to answer questions that could wait. The result is a fragmented response in which each function is working hard and the overall effort is not coordinated.

Agricultural lending institutions face a specific version of this problem. Many do not retain dedicated cybersecurity legal counsel and must engage outside counsel for the first time during an active incident. That engagement itself takes time and requires briefings that pull resources from the response. The institution's primary legal relationship is often with an agricultural lending specialist who has limited cybersecurity regulatory expertise. The mismatch between the counsel the institution has and the counsel an active cyber incident requires is a predictable and often unaddressed gap.

Operational Continuity Plans That Were Never Integrated with Business Reality

Most agricultural lending institutions have business continuity plans that describe how operations will continue if key systems become unavailable. Those plans are typically written to satisfy regulatory requirements and are reviewed on an annual cycle. They are rarely tested in scenarios that reflect the actual operational demands of the institution at its most vulnerable moments.

The consequence is continuity plans that fail at exactly the points of greatest need. A plan may describe manual loan processing procedures, but those procedures may not account for the volume of operating line renewals that occur during a two-week window in March. It may describe alternative communication channels, but those channels may not be accessible if the institution's Microsoft 365 environment, which many ag lenders run on a single tenant, is compromised or taken offline during containment. It may describe recovery time objectives without accounting for the fact that core banking system restoration from backup may take 48 to 72 hours, a timeline that is incompatible with the institution's obligation to process harvest settlement payments that are due within 24 hours.

The gap between the continuity plan and business reality is not a failure of the people who wrote the plan. It is a failure of a planning process that does not require integration with the institution's actual operational calendar, transaction volume, and system dependencies. Until those plans are tested against real scenarios, the gap remains invisible.

Regulatory Notification Failures

Agricultural lending institutions subject to FCA oversight, as well as those subject to state and federal banking regulations, have specific notification obligations when a cyber incident occurs. Those obligations include defined timelines for notifying regulators, defined content requirements for the initial notification, and ongoing reporting obligations as the incident develops. In practice, these requirements are frequently handled incorrectly during active incidents.

The failures take several forms. Notification is made too late because the institution spent too much time in internal deliberation before confirming that a reportable incident had occurred. Notification is made with incomplete or inaccurate information because the initial assessment was premature. Notification is made to the wrong regulatory body because the institution's primary regulatory relationship does not cover all the notification requirements triggered by the incident. And in some cases, notification is not made at all because the institution's legal counsel and executive leadership were not aligned when the notification threshold had been met.

Each of these failures creates regulatory exposure that compounds the operational damage of the incident itself. Regulators who receive timely, accurate, and complete notification are meaningfully

more cooperative partners in the recovery process than regulators who learn about an incident through other channels or receive notification that appears to have been delayed or managed strategically.

What the Plan Says	What Happens in Practice
Incident commander activates response team within 30 minutes	Incident commander is unreachable; escalation chain takes 2–4 hours
Legal counsel engaged immediately upon confirmation	Outside counsel not retained; agricultural attorney engaged without cyber expertise
Regulatory notification within 36 hours	Notification delayed pending internal alignment on what to disclose
Manual backup processes activated for loan operations	Backup procedures not documented for current system versions; staff unfamiliar
Executive leadership briefed hourly	Briefings pull senior IT staff from containment; response slows
Recovery completed within defined RTO	Core banking restoration takes 3x longer than plan assumed

3. The Agricultural Lending Context: Why the Stakes Are Higher

Cyber incident response failures are costly in any financial institution. In agricultural lending, the cost structure is different in ways that make the consequences of those failures more severe and more immediate.

Seasonal Concentration and the Unforgiving Calendar

Agricultural lending operations are compressed into 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 and agricultural banks. Harvest settlement, running from September through November, represents the majority of large payment processing. Equipment and real estate activity peaks in ways tied to commodity cycles and tax planning.

A cyber incident that disrupts operations during these windows does not have the luxury of a recovery timeline measured in weeks. An institution that cannot process operating line renewals in March is creating cash flow crises for borrowers who need to purchase seed, fertilizer, and fuel before the planting window closes. An institution that cannot process ACH payments during harvest settlement is creating relationship and reputational damage with grain elevators, co-ops, and borrowers that may take years to repair.

The recovery timeline for a significant ransomware event, which is typically measured in days to weeks for initial restoration and months for full recovery, is structurally incompatible with the tolerance for operational disruption that agricultural lending's seasonal calendar allows. This mismatch is the defining feature of cyber risk in this sector, and it is the reason that incident response capability matters more here than in almost any other financial services context.

Borrower Vulnerability and the Downstream Cascade

Agricultural borrowers operate on thin margins and with limited financial reserves relative to commercial borrowers of comparable loan size. A farmer managing a $2 million operating line does not have the same financial cushion as a commercial real estate developer with the same loan balance. Delays in loan processing, payment execution, or account access create downstream consequences for borrowers that are qualitatively different from the consequences that commercial banking customers experience during the same disruption.

A lender that cannot process a planting-season operating line draw because its loan origination system is offline may be creating a situation where a borrower cannot purchase inputs that have a finite availability window. The failure is not just operational. It is potentially existential for the borrower's season. The lender's recovery from the incident is measured in days. The borrower's recovery from a missed planting window may be measured in years.

This downstream cascade dynamic means that incident response in agricultural lending carries a stakeholder accountability dimension that does not exist in most other financial services contexts. Getting the response right is not just about protecting the institution; it’s about protecting the borrowers who depend on the institution's ability to function.

The Regulatory Dimension in Farm Credit

Farm Credit System institutions operate under FCA oversight with specific cybersecurity examination expectations that are increasing in rigor. Institutions that experience a cyber incident and manage it poorly face a regulatory examination process that can extend well beyond the incident itself, requiring extensive documentation of what happened, what was known when, what decisions were made, and what remediation steps were taken.

An institution that can demonstrate a well-executed incident response, with timely notification, effective containment, documented decision-making, and appropriate borrower communication, is in a substantially stronger regulatory position than one whose response was chaotic, late-notifying, and poorly documented. The quality of the incident response shapes the regulatory relationship for years afterward.

> **The Examiner's Frame**
>
> *Examiners reviewing a post-incident institution are not asking whether the cyber event could have been prevented. They are asking whether the institution's response demonstrates that its governance, risk management, and operational frameworks are sound. A well-executed response to*

> *a significant incident can actually strengthen an examiner's confidence in an institution's management. A poorly executed response to a minor incident can raise fundamental questions about governance quality.*

4. Right of Bang: What the Critical Window Requires

The military concept of Right of Bang emerged from training programs designed to prepare soldiers for the moments immediately following an explosive event, because the disorienting, high-stakes window in which the right response is critical, is not instinctive and must be trained. The parallel to cyber incident response is direct and intentional.

The Right of Bang window in a cyber incident is roughly the first 24 to 72 hours after detection, the period during which the most consequential decisions are made under the worst conditions. Systems may be compromised or offline. Information is incomplete and rapidly changing. Leadership is stressed and may be receiving conflicting advice. Attackers may still be active in the environment. External parties, including counsel, regulators, vendors, and insurers, are entering the picture simultaneously and asking different questions of the same people.

What the Right of Bang window requires is not a better plan. It requires leaders who have rehearsed the scenario, decision frameworks that do not require full information to operate, communication structures that function under pressure, and pre-established relationships with the external parties who will need to be engaged. It requires, in short, capability rather than documentation.

The First Hour: Containment and Activation

The decisions made in the first hour after a cyber incident is detected shape everything that follows. Containment decisions, such as what to isolate, what to shut down, and what to preserve, affect the attacker's ability to continue operating in the environment, the institution's ability to recover quickly, and the forensic evidence available for subsequent investigation. Getting these decisions right requires pre-established authority and pre-established criteria.

Institutions that perform well in the first hour share several characteristics. They have a pre-designated, experienced, incident commander with clear authority to make containment decisions without seeking approval. They have an on-call escalation structure that reaches someone with that authority regardless of the time of day or day of week. They have a documented triage framework that tells the first responder what questions to ask and what actions to take before the full team is assembled. And they have a communication channel that is typically an out-of-band channel that does not depend on the institution's primary collaboration tools, so that the initial team can coordinate confidentially.

For most agricultural lending institutions, the first-hour structure is the piece of incident response capability that is most often missing. The plan may describe what should happen, but the practice required to make it actually happen under pressure has not occurred.

The First 24 Hours: Decisions Under Incomplete Information

The decision framework for the first 24 hours must be designed explicitly for a context in which full information will not be available and waiting for it is not an option. The institution will need to make decisions about whether to notify regulators before it fully understands the scope of the incident. It will need to make decisions about borrower communication before it can fully describe what happened. It will need to make decisions about whether to pay a ransom demand (but please don't!) before it knows whether its backups are recoverable.

Institutions that manage this window well do so because they have pre-established decision criteria. The ransom payment question, for example, should be resolved before the incident occurs. The decision framework, including who makes the call, what factors are weighed, what the default position is, and what authorities must be consulted, should be documented and tested, not improvised under pressure. The same applies to the regulatory notification threshold, the borrower communication trigger, and the decision to engage law enforcement.

Pre-establishing these decision frameworks does not eliminate the difficulty of the decisions. It eliminates the time and coordination cost of defining the framework while also managing an active incident. That time and coordination cost, in a 24-hour window, is often the difference between a well-managed and a poorly managed response.

The First 72 Hours: Operational Continuity and Stakeholder Management

The 72-hour window is where business continuity plans are tested and where many agricultural lending institutions discover that their plans do not reflect operational reality. The focus shifts from containment to continuity, where the goal is keeping as much of the institution's essential function operating as possible while full recovery proceeds.

For agricultural lending institutions, the essential function question must be answered before the incident occurs. Which systems, if unavailable, create borrower harm? Which payment processes cannot be delayed without creating downstream consequences? Which borrower-facing functions must be maintained regardless of the state of back-end systems? These questions should drive the prioritization of continuity investments and the design of manual backup procedures, and they should be answered in collaboration with lending leadership, not just IT.

Stakeholder management during the 72-hour window includes borrower communication, board communication, regulator communication, law enforcement communication, and in some cases media communication. Each of these audiences requires a different message at a different level of detail. Pre-drafted communication templates for each stakeholder type, at each stage of the response, dramatically reduce the time and coordination burden of stakeholder management during the incident itself.

Decision	Pre-Incident: Define the Framework	Right of Bang: Execute Against It
Ransom payment	Establish default position, decision authority, consultation	Execute against pre-established framework; do not improvise under attacker's deadline

	requirements, and payment mechanism if applicable	
Regulatory notification	Define notification threshold, required content, timing standard, and responsible party for each regulatory relationship	Notify per framework; document timing and content of each notification
System shutdown	Define shutdown criteria, authorization chain, and backup activation sequence for each critical system	Activate per framework; document decision and rationale
Borrower communication	Define trigger criteria, message templates, and authorized communicators for each borrower segment	Deploy pre-approved communications; do not improvise messaging under pressure
Law enforcement engagement	Establish default position and pre-identify appropriate contacts at FBI cyber division and local field offices	Engage per pre-established decision; provide pre-organized documentation package
External counsel activation	Retain cyber-specialized legal counsel before incident; establish engagement protocol and retainer	Activate per protocol; avoid first-engagement delay during active incident

5. Redesigning for Real-World Performance

The path from a compliance-oriented incident response program to a capability-oriented one requires changes in four areas, including testing discipline, governance design, integration with operations, and external relationship management. None of these changes are technically complex. All of them require institutional commitment to doing something that most agricultural lending institutions have not yet completed: treating incident response as an operational capability that must be maintained, not a policy requirement that must be satisfied.

Tabletop Exercises Designed for Agricultural Lending Reality

Tabletop exercises are the primary mechanism through which incident response plans become incident response capabilities. Most agricultural lending institutions that conduct tabletops run generic scenarios drawn from industry frameworks or vendor templates. Those scenarios are useful as starting points, but insufficient as the primary test of readiness.

Tabletop exercises for agricultural lending institutions should be built around the scenarios that are most consequential for this sector specifically: ransomware deploying on the first Monday of operating line season; a deepfake voice call successfully authorizing a $1.8 million ACH transfer to a fraudulent

grain elevator account; a core banking system outage coinciding with the last day of harvest settlement processing; or a vendor platform breach exposing borrower financial data during a period when the CISO is traveling and the IT director is managing a concurrent system migration.

These scenarios should involve all the stakeholders who would be involved in a real incident: lending leadership, not just IT; the CEO and CFO, not just the risk function; outside counsel, if a relationship exists; and board members, who in a real incident will be asking questions that leadership must be prepared to answer. The exercise should be followed by a structured after-action review that identifies specific gaps in authority, communication, process, and capability; and those gaps should drive a remediation plan with assigned owners and deadlines.

Incident Command Structures That Hold Under Pressure

The incident command structure is the most critical element of incident response design, and the element most often designed for audit compliance rather than operational reality. A structure that looks clean on paper but concentrates authority in someone who lacks the proper experience or organizational reach, or that creates decision bottlenecks by requiring consensus among parties who may be unavailable, will fail under pressure regardless of how well it is documented.

Effective incident command structures for agricultural lending institutions share several design principles. Authority is pre-delegated: the incident commander has explicit, pre-authorized authority to make containment, communication, and operational decisions up to a defined threshold without seeking approval. Backup designees are identified for every critical role: if the primary incident commander is unreachable, the secondary has the same authority and has rehearsed the same scenarios. The structure is flattened for speed: the number of people who must be consulted before a time-sensitive decision is made is minimized. And the structure is tested: every person in the command structure has participated in at least one tabletop exercise in which they actually made the decisions their role requires.

Integration with the Agricultural Lending Operational Calendar

Incident response programs that are not integrated with the institution's operational calendar will fail to account for the periods of greatest risk and greatest consequence. That integration requires explicit documentation of the institution's seasonal risk windows, the systems and processes that are most critical during each window, the manual backup procedures for those systems and processes, and the communication priorities for each period.

Concretely, this means that an agricultural lending institution's continuity plan should describe different operating modes for March-April operating line season and September-October harvest settlement than for the lower activity periods of December and January. It should identify the specific loan processing, payment execution, and borrower communication functions that cannot be interrupted during each window and describe the manual procedures and staffing required to maintain them. And it should be tested in scenarios set during those high-risk windows, not in the generic scenarios that most tabletop exercises use.

Pre-Established External Relationships

The external parties that must be engaged during a cyber incident, meaning legal counsel, cyber insurance carriers, forensic investigators, law enforcement, core banking system vendors, ransomware negotiators, and regulatory liaisons should all be identified and relationships established before the incident occurs. An institution engaging outside cyber counsel for the first time during an active incident is simultaneously managing the incident and managing a new relationship, a combination that adds time, cost, and friction at exactly the wrong moment.

For agricultural lending institutions, the most critical pre-established relationship is often the one most frequently missing: a retainer engagement with legal counsel who has specific cybersecurity regulatory expertise and experience with FCA examination requirements. The institution's primary agricultural lending counsel, however excellent in that domain, is unlikely to be the right counsel for a cyber incident involving regulatory notification, potential class action exposure, and law enforcement coordination. Having that counsel identified, retained on a basic level, and briefed on the institution's environment before the incident occurs is one of the highest-value preparedness investments an agricultural lending institution can make.

6. The Readiness Assessment: Where to Start

For agricultural lending institutions assessing their current state of incident response readiness, the following framework identifies the most consequential gaps and the sequence in which to address them. It is not a comprehensive audit checklist. It is a prioritized starting point for institutions that want to move from compliance posture to operational capability.

Readiness Element	Compliance Posture	Capability Posture
Incident response plan	Plan exists and has been reviewed by legal and risk; updated annually	Plan has been tested in realistic tabletop; gaps identified and remediated; updated after each exercise
Decision authority	Roles and responsibilities documented in plan	Authority pre-delegated with explicit thresholds; backup designees identified and rehearsed; authority tested in tabletop
Regulatory notification	Notification requirements documented; responsible party identified	Notification templates pre-drafted; timing framework established; practice notifications completed with regulatory liaison
Legal counsel	Primary agricultural lending counsel identified	Cyber-specialized counsel retained; briefed on institution environment; engagement

		protocol established; retainers signed with DFIR team, if external
Continuity plan	Manual procedures documented for critical systems	Procedures tested against current system versions; seasonal operational demands incorporated; volume assumptions validated
Tabletop exercises	Annual generic scenario completed	Sector-specific scenarios completed semi-annually; all stakeholders including CEO, CFO, and board members participate; after-action remediation tracked
External relationships	Cyber insurance carrier identified; FBI contact listed in plan	Forensic investigator on retainer; carrier pre-notification process established; law enforcement relationship current
Communication templates	General notification language in plan	Templates drafted for each stakeholder type at each incident stage; approved by legal and communications; stored out-of-band

The gap between the compliance posture and the capability posture in each row represents the investment required to convert a plan into a capability. For most agricultural lending institutions, moving from compliance to capability across all eight elements is a 12 to 18-month program, not a single project. The appropriate starting point is the element that represents the greatest consequence gap for the institution's specific situation, typically decision authority, legal counsel, or continuity plan integration with the operational calendar.

Where to Begin

Institutions that are uncertain about where to start should ask one question: if ransomware was deployed in our environment tonight, who would make the decision to shut down our core banking system, and does that person have the authority, the information, and the backup to make that call at 2 AM? If the answer to any part of that question is unknown, the incident command structure is the right starting point.

Conclusion: The Test is the Training

The phrase "Right of Bang" is ultimately about acceptance. It accepts that events will occur that cannot be prevented. It accepts that the question of consequence is not whether, but when. And it accepts that

the only meaningful preparation for that moment is the work done before it arrives; not the document written to describe what should happen, but the practice undertaken to build the capability to make it happen.

Agricultural lending institutions that have not tested their incident response programs are carrying risk that their plans cannot measure and their audits cannot detect. The plan passes the review. The capability has never been demonstrated. The gap between those two things is invisible until the moment it becomes catastrophic.

The good news is that the gap is closable. *Effective* tabletop exercises, pre-established decision frameworks, integrated continuity planning, and the right external relationships are not technologically complex investments. They are discipline investments, meaning the discipline to test what has been written, to involve the people who will actually make decisions in the scenarios that will actually require them, and to treat incident response readiness as an ongoing operational capability rather than an annual compliance exercise.

For farm credit institutions, where a poorly managed incident during planting or harvest settlement can cascade into borrower harm and regulatory consequences within days, that discipline is not optional. It is the difference between an institution that weathers a cyber event and one that is defined by it.

FieldSafe works with agricultural lending institutions at exactly this point: assessing where the real gaps are, designing resilience programs that account for the sector's specific operational realities, and building the testing and practice discipline that converts plans into capabilities. Institutions that have done this work before an incident occurs are the ones that come out the other side intact.

About FieldSafe

FieldSafe is a cybersecurity advisory offering purpose-built consulting and managed services for agricultural lending institutions, developed by SunStream in collaboration with Argent Reach. FieldSafe brings together incident response expertise, regulatory knowledge, and deep familiarity with the operational realities of farm credit. FieldSafe helps institutions understand the specific shape of the risks they face and build the governance structures and resilience programs to manage them effectively.

www.sunstreamservices.com/fieldsafe

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 incident response programs and cybersecurity governance frameworks. The views expressed represent the perspectives of FieldSafe based on practitioner experience and publicly available information.