
# Social Engineering Fraud Is Surging. Your Insurance Assumptions May Be Wrong.

**By Nelson Kefauver, Head of Financial & Professional Lines, North America, and Aaron Belair, President, Technology & Life Science, North America, Intact Specialty Solutions**

Social engineering has always been about people. What is different now is the payoff. More attacks aim to move money, not just steal data. One convincing email can redirect a vendor payment, drain a treasury account, or trigger an urgent wire that never should have left the building.

This is not a side issue for Chief Information Security Officers ("CISOs") and their teams. You are accountable for business resilience. Social engineering fraud is a business loss that often enters through security channels and then lands as a financial event. It can bypass the incident patterns your playbooks are designed to catch. It can also reveal a second issue: teams assume insurance will cover the loss, then discover the coverage picture is more complicated than expected.

In 2024 alone, the FBI's Internet Crime Complaint Center (IC3) reported $16.6 billion in total losses, up 33% year over year, with fraud representing the bulk of those losses. While dealing with a loss is the worst time to learn what your policies do and do not say.

## Why These Attacks Keep Working

Attackers don't need to beat your strongest defenses if they can target what your organization does every day. A common pattern starts with email compromise or impersonation. The attacker watches real threads, learns who approves invoices, how vendors submit changes, and who can override processes. Then they step in at the right moment with a simple request. The message looks routine.

These attacks work because they match how modern organizations operate. Email is still treated like an authority channel. Workflow steps exist, but they are often informal and split across teams. Finance wants speed. Procurement wants to keep vendors satisfied. Security wants controls. Fraud thrives in the seams between those goals.

Deception is also improving. Generative AI makes it easier to write emails that sound like a real executive or vendor contact. Deepfake voice and video can add urgency. Verizon's 2024 Data Breach Investigations Report found that the "human element" was a component of 68% of breaches, underscoring how often people and process are part of the failure path.

## The Insurance Assumption That Causes Real Damage

When a social engineering event begins in an inbox, many teams assume cyber insurance will cover the loss. The logic is understandable, but insurance policy form wording may apply differently. Many social engineering losses are classified as fraud or theft, which have traditionally been addressed under crime coverage. Some cyber policies include funds transfer fraud or social engineering coverage, but coverage can be less common, narrowly defined, or dependent on specific conditions. It may require an endorsement. It may be capped by a sublimit smaller than the loss. It may require evidence that specific verification steps were followed. It may apply to unauthorized access, while the loss came from an authorized transfer induced by deception.

This is where disputes often begin. Once funds are gone, teams are forced to debate definitions. Was it computer fraud or social engineering? Was the transfer voluntary? Did the organization follow required procedures? In a crisis, those questions are hard to answer quickly and clearly.

CISOs do not negotiate policies, but security leaders are often asked to provide the facts that shape how an event is characterized. Log data, identity findings, and a reconstruction of the attacker's path can influence how the loss is evaluated.

## Why CISOs Should Care, Even If Insurance Sits Elsewhere

Social engineering fraud can be a direct enterprise risk. It creates three downstream problems that CISOs often take on, at least in part.

First, it can cause a significant financial loss without ransomware, data exfiltration, or a headline-grabbing breach. Second, it can still trigger a demanding response: forensics, email containment, legal coordination, vendor outreach, executive updates, and board questions. Third, it can create governance fallout when leadership realizes risk transfer is not the same as risk control.

This is where CISOs can lead across functions. Not as insurance specialists, but by pushing for clarity. What types of fraud do we face? Which controls are in place? Which policy is expected to respond? What conditions must be met for coverage to apply? These are operational questions that matter before an incident, not after.

## The Line Between Crime and Cyber, and Why It Blurs

No two organizations have identical coverage. Policy wording varies. Endorsements differ. Requirements change based on industry, size, and risk profile. Still, the distinction is useful.

Cyber insurance is generally designed to respond to events like ransomware, extortion, incident response costs, privacy liability, and business interruption tied to a covered cyber event. Crime coverage is generally designed to respond to theft and fraud, including certain types of funds transfer loss.

Social engineering fraud often lives in the overlap because it is cyber-enabled, while the loss is financial and may result from a human-authorized action. Some organizations find they have partial coverage under one policy, partial coverage under another, or coverage that depends on procedures that were never clearly communicated to the teams handling payments.

For CISOs, the takeaway is straightforward. If your organization treats this as someone else's problem, you will still get pulled into it. The better approach is to align security controls and payment controls with how your coverage actually works.

## Controls That Reduce Both Compromise and Loss Severity

The strongest programs treat social engineering as a system problem. Start with email trust and identity hardening. Domain authentication controls like Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) can reduce spoofing and improve detection when configured correctly. Pair that with monitoring for suspicious mailbox behavior, such as auto-forwarding rules, unusual Open Authorization (OAuth) app permissions, and atypical login patterns. Many fraud events begin with quiet access and patient surveillance.

Next, focus on accounts closest to money movement. That includes finance teams, vendor managers, and executives who can approve exceptions. Strong Multi-Factor Authentication (MFA) is a baseline

requirement. Conditional access can reduce risk further by blocking anomalous logins and requiring step-up authentication when a location, device, or behavior looks wrong.

Then tighten payment change governance. Bank detail changes should be treated as high-risk requests, not routine updates. Out-of-band verification matters because it breaks the attacker's control of the communication channel. Separation of duties reduces single points of failure. A short delay on first-time payments or changed instructions can help as well. Many successful frauds depend on speed and silence.

Training should reinforce these controls, not replace them. The goal is to set expectations: verify before you pay, slow down when urgency appears, and escalate when something feels off. If leadership wants safety, leadership has to signal that safety matters more than convenience.

Finally, test the full response path. Run a tabletop exercise focused on wire fraud, not ransomware. Include security, treasury, finance operations, legal, and risk. Define who calls the bank, who preserves evidence, who notifies insurers, and what documentation is needed. In many cases, the difference between partial recovery and total loss is measured in hours.

## A Better Operating Rhythm for the Next 12 Months

CISOs should map the scenarios most likely in their environment: vendor bank changes, executive wire requests, payroll diversion, and procurement impersonation. Identify where email is treated as proof and where verification is weak. Then align controls to those weak points, especially around identity, mailbox integrity, and payment authorization.

At the same time, pressure test insurance assumptions before a crisis. A short cross-functional working session with security, finance, and risk can surface gaps that would otherwise appear at the worst time. The goal is no surprises.

Social engineering fraud is more than a cybersecurity story. It is a business resilience story. CISOs who treat it that way can reduce losses, shorten recovery time, and build confidence that does not depend on guesswork.

Company, a Pennsylvania insurer. Each of these insurers maintains its principal place of business at 605 Highway 169 N, Plymouth, MN 55441. For information about Intact Insurance Specialty Solutions products and services available in Canada, visit intactspecialty.ca, and for information about Intact Financial Corporation, visit intactfc.com .

**About the Authors**

Nelson Kefauver is Head of Financial and Professional Lines, North America, and Aaron Belair is President, Technology and Life Science, North America, at Intact Insurance Specialty Solutions.

Together, they help organizations strengthen cyber resilience by aligning security controls with insurance coverage, particularly for risks such as social engineering fraud and funds transfer loss. Their combined expertise spans underwriting and risk strategy across technology, life sciences, and financial sectors, bridging the gap between cyber threats and effective risk transfer.