

What Is Social Engineering, and Why It Matters to Your Insurance Coverage

When most people think about cyber risk, they picture hackers breaking through firewalls or planting malicious software. Some of the most damaging losses today do not involve technical hacking at all. They involve people. That is where social engineering comes in, and why it has become such a critical insurance issue for businesses of all sizes.

WHAT SOCIAL ENGINEERING REALLY MEANS

Social engineering is the act of manipulating people into doing something they would not normally do. The attacker does not break into a system. Instead, they gain trust, create urgency, or impersonate authority, and convince someone to take an action on their behalf.

In a business setting, this often looks like a realistic email from a senior executive asking for an urgent wire transfer, or a message that appears to come from a trusted vendor with updated payment instructions. The request feels familiar, legitimate, and time sensitive. An employee acts in good faith, and the funds are sent. By the time the fraud is discovered, the money is gone.

What makes social engineering so effective is that it exploits normal business behavior. People are trained to move quickly, trust internal communications, and help leadership meet deadlines. Attackers know this, and they design their scams around it.

WHY SOCIAL ENGINEERING LOSSES ARE INCREASING

Social engineering has grown rapidly in recent years for two main reasons.

First, businesses rely heavily on email and digital payments. Wire transfers, ACH payments, and electronic invoices are part of daily operations, which gives criminals more opportunity to insert themselves into legitimate workflows.

Second, attacks have become far more sophisticated. Criminals research company structures, use real names and titles, monitor payment timing, and increasingly use AI tools to mimic writing styles, voices, or even video calls. These are not obvious scam emails filled with typos. They often look exactly like normal business communication.



WHERE INSURANCE EXPECTATIONS AND REALITY DIVERGE

This is where insurance confusion begins.

After a loss, many companies assume their cyber insurance policy will respond. Others expect their crime or fraud coverage to step in. Too often, they discover that neither policy covers the loss the way they expected.

The reason is simple but counterintuitive. In most social engineering scenarios, no system was breached. No malware was deployed. No account was technically accessed without authorization. The payment was made voluntarily by an employee, even though it was based on fraudulent information.

From an insurance perspective, that distinction matters.

Many standard policies exclude losses caused by voluntary transfers of money, employee actions, or deception without a confirmed system intrusion. As a result, social engineering claims are frequently denied unless the policy specifically addresses this exposure.

HOW SOCIAL ENGINEERING COVERAGE WORKS

Coverage for social engineering usually exists, but it is rarely automatic.

It is typically added by endorsement to either a cyber policy or a commercial crime policy. The language may reference social engineering fraud, fraudulent instruction, impersonation fraud, or funds transfer fraud. While the labels differ, the intent is the same. The policy is designed to cover financial losses caused by deceptive instructions that appear to come from a trusted source.

This coverage almost always comes with lower limits than the rest of the policy. Default limits are commonly much lower than a typical wire transfer amount. It may also include strict conditions, such as dual authorization, call back verification, or documented payment procedures. If those controls are not followed exactly, coverage can be jeopardized.

In other words, having the endorsement is not enough. How it is written, how it is limited, and how it aligns with real business practices all matter.

WHY THIS RISK DESERVES ATTENTION NOW

Social engineering is not a rare or theoretical exposure. It is one of the most common causes of direct financial loss tied to cyber activity today. Unlike ransomware or data breaches, these losses are immediate, measurable, and often unrecoverable.

They also sit at the intersection of technology, finance, and human behavior, which makes them easy to overlook during insurance renewals. Many organizations do not realize they are underinsured until after a loss occurs.

CONCLUSION

Social engineering is not just a cybersecurity issue. It is a financial risk issue, an operational risk issue, and an insurance issue.

Understanding how your policies define social engineering, whether coverage exists, what limits apply, and what controls are required can make the difference between a covered loss and a denied claim. This is one of those areas where assumptions can be costly.

The best next step is a conversation. Sit down with your insurance advisor and review how your current policies address social engineering fraud. Ask what scenarios are covered, what are not, and whether your limits reflect your real exposure.

Because when it comes to social engineering, the question is not if an attempt will happen. It is whether you are prepared when one succeeds.

If you have questions specific to your business, or would like additional information, please reach out to your Navacord Insurance Services Alberta Inc. Advisor.

™@Local Touch. National Strength. Navacord and Navacord logo are Trademarks of Navacord. The information contained herein is general in nature and general insurance description only. The information is not intended to be insurance advice; nor does it amend, modify or supplement any insurance policy. Consult your actual policy or your broker for details regarding terms, conditions, coverage, exclusions, products, services and programs which may be available to you.

**LET US HELP YOU
MANAGE YOUR RISK**

9 Office Locations
Across Alberta and Interior BC

lloydsadd.com
AB.info@navacord.com

Local Touch. National Strength.™