



**OUR
WORK.**

OUR STORIES.

A collection of insights and stories from leading experts in the risk management industry covering key areas of organizational risk.



**LOWERS
& ASSOCIATES**

International Risk Mitigation Partners

FOREWORD

01

Every business begins with a purpose. For over 30 years, ours has been ensuring clients don't have to compromise on security to deliver on theirs. Our collaborative approach has helped businesses around the globe build a sense of well-being that protects their people, brand, and profits.

Right now, business owners are looking for useful strategies that provide a way forward. In this collection of stories, we share security tips, unique industry insights, and first-person accounts that have helped refine our purpose and that we believe can be applied to any industry.

This collection of stories and insights covers some of the most common areas of risk management we address. The truth is, stories of our work could fill volumes. For now, I hope you find value in what we share here and that it gives you a glimpse into the ways we can help your organization mitigate risk and protect against loss.

With gratitude,

Mark Lowers

Mark Lowers

President and Chief Executive Officer, Lowers & Associates



TABLE OF CONTENTS



03	Contributors
04	Separation of Duties
05	Access Control
06	Employee Screening
07	Process Innovation
08	Cash Handling
09	Business Continuity
10	Insurance Claims

11	Social Engineering
12	Standard Operating Procedures
13	Occupational Fraud
14	Experience and Training
15	Surveillance and Investigation
16	Proactive Communication
17	About Lowers & Associates

CONTRIBUTORS



**BRAD MOODY,
CFI, CFE**
Executive Vice President



**JON D.
GROSSMAN, J.D.**
EVP Consulting Practice



TOM DOLAN
Manager of Claims and
Research



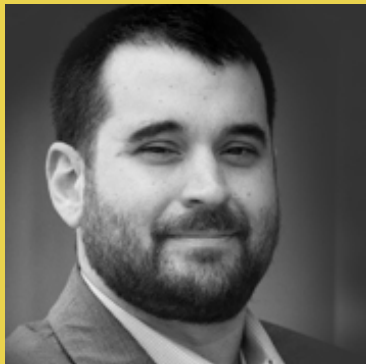
DANIEL COOTES
Client Relationship
Operations Manager



**KRISTOPHER
KEEFAVER**
Director of Clients, CIT,
Safety



CHRIS SOSNOSKI
Director of Information
Technology and Security



JOE LABROZZI
Chief Security Officer



NEIL WATSON
Director of Global
Operations



**KEITH GRAY,
CFE, CAMS**
VP, Client Relations

SEPARATION OF DUTIES

KEY CONTRIBUTOR



BRAD MOODY, CFI, CFE
Executive Vice President

WIRE FRAUD BEGINS AND ENDS WITH PEOPLE

It's hard to imagine that, on any given day, over \$3 trillion dollars moves via electronic transfer. Financial institutions make these B2B transactions happen seamlessly on a global scale, and we often take for granted the very simple instructions required (and accepted) between businesses that make single transactions of millions of dollars possible. Since organizations perform these transactions almost exclusively online, the Internet of things has an inherent opportunity for malicious redirection when company employees become complacent with routine wire instructions.

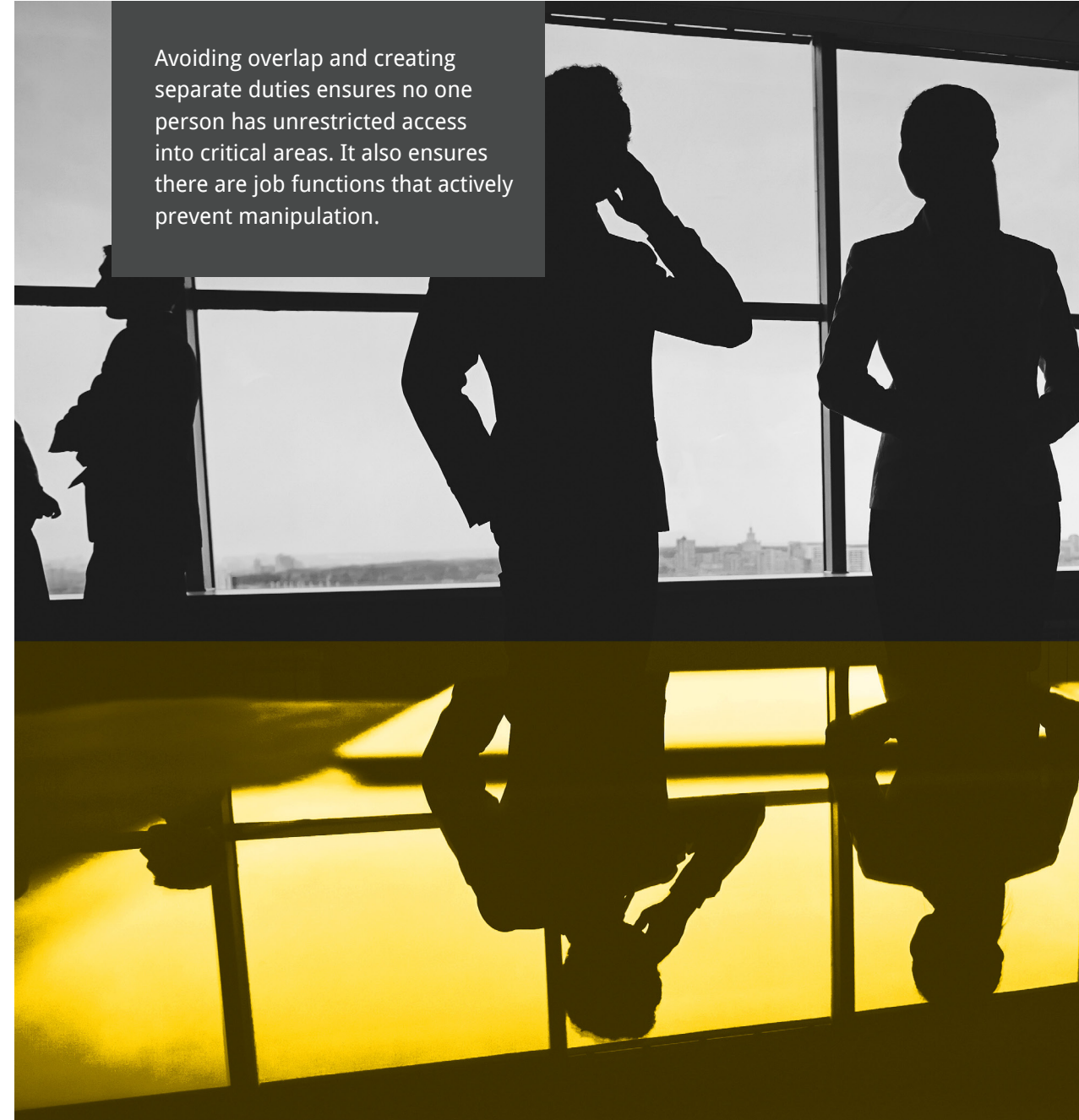
Responsible organizations follow robust, documented and accepted practices in an environment that embraces process. The culture of any high reliability organization allows employee intervention and systematic controls to prevent fraud opportunities. It may feel as if these processes are tedious and repetitive, however, at the end of the day, human actions allow fraud to exist.

Since 2016, it's estimated that over \$26 billion in fraud losses has come from wire funds transfers as the result of business email compromise alone. With the recent COVID-19 pandemic event, fraudsters have a new ability to exploit corporations, especially in highly impacted areas. It is important for organizations to maintain a culture of process and have contingency plans in place to allow transfers to continue seamlessly.

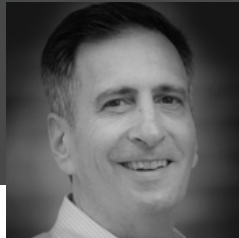
[READ THE FULL ARTICLE →](#)

EXPERT TIP

Avoiding overlap and creating separate duties ensures no one person has unrestricted access into critical areas. It also ensures there are job functions that actively prevent manipulation.



KEY CONTRIBUTOR



JON D. GROUSSMAN, J.D.
EVP Consulting Practice

IGNORANCE IS BLISS — UNTIL REALITY HITS

As COVID-19 restrictions are slowly lifted and businesses around the world contemplate re-opening, every owner should be using their time right now to examine what reopening in the current normal looks like. To provide some guidance for those reevaluating their security measures or that are specifically focused on reopening, here are 10 suggested actions ANY business can take to remove risk and eliminate potential for loss at any time.

1. Reassess security resource allocation based on operational need and risk.

If you have a business portfolio with multiple locations, consideration should be given to the specific business environment, nature of the threats, existence of any unusual circumstances, and the capacity of local law enforcement to respond.

2. Limit the number of entry/exit points for employees and visitors.

Tightly control ingress and egress for safety and security optimization. Examine operational feasibility before implementation.

3. Consider the reception area.

If security personnel are employed at the location, what role will they now play at the reception area to assist in the enforcement of new practices?

4. Access control measures and mechanisms dependent on fingerprint or a punch code require new safety protocols to be implemented.

This includes visitor management software and the use of tablets for registration.

5. CCTV coverage designed for cash handling or robbery identification should have expanded focal points to include more than just a face shot.

With the use of face masks becoming more frequent for the foreseeable future, at least one camera angle should include the entire body, including shoes (criminals typically do not ditch their shoes after committing a robbery).

EXPERT TIP

Right now, access control for employees and visitors should be top of mind. By limiting points of entry and exit, businesses can better maintain the safety measures implemented during the current pandemic.

Before re-opening, businesses should consider the security and legal implications of these measures; whether it's one door to a small neighborhood shop or fingerprint access to a sophisticated metropolis building, the details matter.



[READ ALL 10 TIPS →](#)

EMPLOYEE SCREENING

KEY CONTRIBUTOR



TOM DOLAN
Manager of Claims and Research



DUE DILIGENCE: YOUR LUCKY DAY?

Fraud is everywhere, but just a small amount of basic due diligence can help a business avoid it or other unnecessary risks. From a small-town pawnbroker that lost his business after hiring a friend whose felonious past was only revealed after a six-figure theft, to a multinational corporation that lost millions in fraudulent payments to a duplicitous supply contractor living well beyond his means, there are countless stories demonstrating the steep price paid by companies that trusted before verifying.

What is due diligence?

Due diligence is a specific but flexible process performed by qualified experts to identify and obtain disparate information to form a complete picture. In the above example, the research would have included the history and business filings of the company (as well as those of the principles, owners or key management) and any actual or perceived affiliations, to name a few.





Why do businesses need it?

New personnel or new partners can shape the future of your business. Whether it's a college coach, a board member or a supplier, the whole story matters and should include:

- Investigation of character
- Investments
- Acquisitions
- Mergers
- Assets identification (for debt enforcement and recovery)
- Location

What else should I know about due diligence?

It's always important to understand who you're working with to eliminate the potential for fraud. When doing your due diligence, here are some best practices:

-  **Access to public records.** A subject's criminal record (or lack thereof) is of prime importance, but equally significant may be history of litigation or bankruptcy. Even seemingly minor issues like traffic infractions may be indicative, especially when a subject has tallied dozens.
-  **Complete and comprehensive history.** The most thorough background investigations can reveal the truth of what's been put forward in a resume or MOU and what may have been deliberately omitted. Ask the questions that illuminate the answer.
-  **Asset verification.** Before entering into any formal arrangement, understand and confirm a potential partner's claimed resources and reveal when things don't add up. Don't underestimate the power of pressure in the Fraud Triangle.
-  **Social media review.** Despite its prevalence, not everyone uses it wisely. A review of both personal and corporate profiles can identify some of the most egregious red flags. Consider recurring sweeps to mitigate or uncover your exposure.

[READ THE FULL ARTICLE →](#)

EXPERT TIP

Proactive pre-employment screening is an important first step to get the right people on the team. The truth is, though, an individual background check is only guaranteed to be accurate the day it is processed. Recurring background screening – both for individuals and potential business partners – is equally essential to ensure the safety of employees, customers and the overall business.

Whether a local pawnbroker or a multinational corporation, verification should always outweigh blind trust in the due diligence process.

PROCESS INNOVATION

07

KEY CONTRIBUTOR



DANIEL COOTES

Client Relationship Operations Manager

ADAPT & OVERCOME: THE CASE FOR VIRTUAL SURVEYING

The best businesses right now are doing two things: 1) finding ways to stay open and 2) evaluating the future. The first step in achieving this is a holistic understanding of the business risks. That is, surveying.

For businesses considering a virtual survey, the team at Lowers & Associates has compiled a list of insights and considerations that may be helpful in your discovery process:

- ✓ The primary benefit of virtual surveying is that it can be conducted anytime, anywhere. With no travel, virtual surveying is one of the best ways forward-thinking businesses can control costs.
- ✓ Virtual surveys are less disruptive to the organization and provide quicker report-in-hand turn around. This can be a massive advantage for organizations pressed for time or with reduced staff capacity.
- ✓ Always a collaborative exercise and NEVER the “lesser of two evils,” virtual surveys can often provide deeper insights than those conducted in-person (sometimes business owners feel more at ease with a physical distance between themselves and the surveyor).
- ✓ Rapid advances in technology come with a learning curve. Leading risk mitigation consultants should be versed in a suite of technology applications to successfully execute a virtual survey.
- ✓ Information is information, right? Sort of. Asking the right questions matters, knowing how to analyze the answers makes all the difference, and consistency is king. Virtual or not, surveyors reviewing requested documentation and/or an audio/visual recording of the survey should be able to turn around the same exact results.

- ✓ Consistency is key in both business and surveying. Virtual surveyors should be able to hand over responsibilities to another surveyor if one should fall ill or become unavailable. Process can be both a businesses’ arrow and its Achilles Heel!
- ✓ Virtual surveying should include an ability to perform:
 - Pre- survey meetings
 - Staff competency and interviews
 - Reviews of day to day operations, site physical security, insurance, fiduciary controls, policy & procedure, vault construction, and crime and illegal activity (local and countrywide)
 - Facility design consultation
 - Follow up consultation meetings

[READ THE FULL ARTICLE →](#)

EXPERT TIP

Innovation is the result of process. Whether driven by external forces or natural progression, the upside can be transformational for an organization. With COVID demanding that every business adapt, no official playbook exists on creating a better normal – only an understanding that the way people work, purchase, learn, and interact has fundamentally changed. This might mean that the cook is now also the cashier, the data analyst receives guests in the afternoon, or that the CEO packs the van on Fridays. Whatever the innovation (or efficiency), the process MUST include proper training to ensure the security and safety of everyone performing a new responsibility, even if it’s temporarily.



CASH HANDLING

KEY CONTRIBUTOR



KRISTOPHER KEEFAUVER

Director of Clients, CIT, Safety

CASH: THE BENEVOLENT KING (OF EVERY CRIMINAL'S HEART)

"I knew him for years. He was like family. How could he do this to me and my business?"

It's an all-too-familiar question after a long-term or trusted employee is caught or suspected of stealing from a company. So, what happens that makes it all go so wrong?

Simply put, cash is the great attractor – while we all interpret that lure differently, its visceral, kindly promise of freedom occasionally becomes too irresistible for human nature to ignore. Many businesses are not aware of, or at least, are not able to consistently identify, hire, educate, and train around this fact. In CIT and security, the breakdown is most often in one or more of the "three P's" (Policy, Process, and Procedure), but it's certainly not an isolated phenomenon. Retail establishments, financial institutions, and more all struggle with it.

EXPERT TIP

Whether a financial institution, retail establishment or CIT business, complacency can be a real threat to future opportunity when it comes to handling cash. Over the years, we've found that low levels of security awareness are often to blame and disproportionately undermine attempts to build a culture of compliance among employees.

An independent review of security and operational procedures can help resolve conflicts and inadequacies to create a safer work environment for all.



So, what can be done to protect people, brands, and profits? Here are a few best practices that can be applied across any business, large or small.

Review your internal policies and processes and provide management oversight to ensure that procedures are being adhered to per company policy and that no one person has too much access to a particular asset or function, including:

- ✓ Access device (key, card, combination, code) controls.
- ✓ Dual control/custody system of checks and balances. Examples include verification of deposit preparation, either 2nd person or virtual (FaceTime, CCTV, Zoom, etc.), bank pick-ups and deposits in person (no night drops if only one person can perform), and confirm deposit or examine credibility of tamper proof deposit bag before leaving (bringing back deposit slip for verification and documentation).
- ✓ Utilize both employment background screening, regardless of relationship or previous work history, and a true continuous court records monitoring solution to get the whole picture.
- ✓ Require job-specific training that is documented and acknowledged via signature of the trainer and trainee to ensure adequacy, accuracy and completeness.
- ✓ Incorporate random and unannounced internal and external audits, testing the aforementioned policy, process, and procedure with staff. Examples may include cash drawer audits and cash drawer documentation.

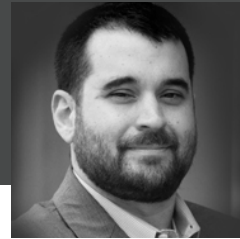
Remember, cash may be king, but it's still your kingdom.

[READ THE FULL ARTICLE →](#)

KEY CONTRIBUTOR



CHRIS SOSNOSKI
Director of Information
Technology and Security



JOE LABROZZI
Chief Security Officer

OUR STORY

When outside events upend normal operations, implementing a business continuity plan becomes top priority. Unfortunately, many companies get stuck during a crisis grappling with the roll-out of their plan or worse, building their plan.

When COVID-19 forced the Lowers & Associates team to go virtual, leadership leaned on an early investment in technology to seamlessly bring 550 people fully remote in just under 2 weeks with zero business interruption. Proactively identifying, assessing, budgeting for and testing the digital suite of tools required to do this years in advance enabled our rapid transition, but having an executable strategy and 100% buy-in from leadership was the foundation.



AUTHORING RESILIENCE DURING COVID-19

At their most basic, BCPs are the real-world response to the old “Hope for the best, plan for the worst” adage. It’s honest recognition that being stuck between a rock and hard place is better with a hammer, albeit with no guarantee that the hammer is big or small enough to be helpful.

Nonetheless, a well-conceived BCP provides peace of mind, like insurance does, with the added satisfaction that only authorship (or ownership?) brings. The rub, of course, is that every BCP is, at the end of the day, still just a plan. As boxer, actor, felon, playwright and corporate strategist ‘Iron’ Mike Tyson once famously said, “Everyone has a plan until they get punched in the mouth.”

For Lowers Risk Group, like many others, COVID hit our industry, our business – our people. We were fortunate, though: Our Business Continuity Plan was 5 years in the making. It didn’t matter, until it did.

Back in 2015, CTO David Lowers, Chief Security Officer Joe Labrozzi, and Director of IT and Security Chris Sosnoski recognized the need for our growing staff to have partially, if not fully, remote capabilities. What was initially driven by space concerns evolved with the access to and the ability of new technology to support fully secure, remote work that reduced cost, increased efficiency, and enabled greater flexibility that could support new business opportunities within Lowers Risk Group. With this foundation in place, Lowers, Sosnoski, and Labrozzi were able to take the organization’s global footprint of over 550 people (spread over 3 continents) to fully remote in less than 2 weeks with zero business interruption when COVID hit.

They shared their story and offered these takeaways to organizations:

- We started planning early and had explored the risk environment, developed the processes that would provide us a path of least resistance to continuity, and had leadership buy-in.
- We identified the right digital tools and had assessed, budgeted for, and tested them as part of the plan strategically; having to do this during COVID would have been very difficult.
- We were all aligned on the work that had to be done to achieve the vision; for us, that was finding a secure, scalable, and available environment to perform our risk mitigation work.

[READ THE FULL STORY →](#)

KEY CONTRIBUTOR



NEIL WATSON
Director of Global
Operations



KEITH GRAY, CFE, CAMS
VP, Client Relations

EMOTIONAL INTELLIGENCE & THE ALLURE OF INSURANCE FRAUD

Insurance loss happens for many reasons. When an event involves the loss of physical stock or damage to property, the loss is immediate, and it creates an urgent need for the business owner to settle the claim so that the business can resume operations and avoid further lost revenue.

This desire to quickly return to business as usual is a natural one, but in the wake of an event, it's not uncommon for the resolution process to test the business owners' resolve. And while most claims post-incident are legitimate, from time-to-time, human emotions will complicate the process and create an environment that enables fraudulent activity, sometimes in unexpected ways.

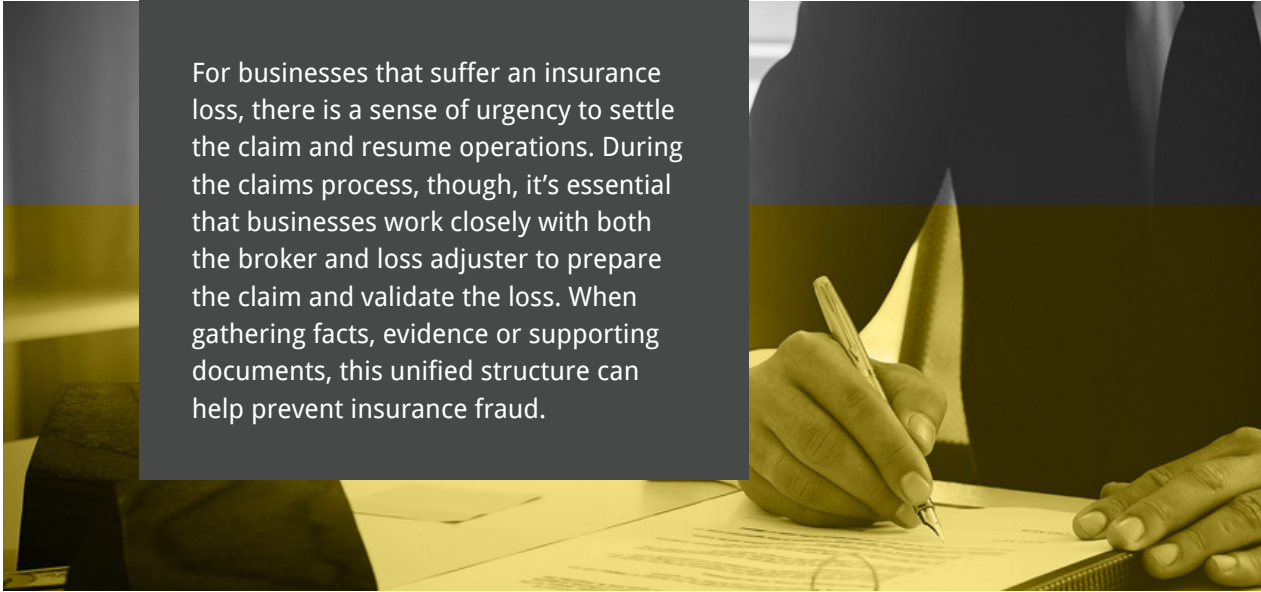
As an insured, it is important to work closely with your insurance broker and the loss adjuster in preparing your claim and validating your losses. Without this professional assistance and oversight, fraud can easily find its way into the conversation.

In such unprecedented times as these, the possibility of a spike in fraudulent claims is a real concern. There is an increase in both the pressure and opportunity factors, resulting in an increased likelihood that potential perpetrators may rationalize their fraudulent thoughts and act on them as a result.

What can you do about it?

Ideally insurers would commission a pre-risk survey to establish security protections, stock levels, and standard operating procedures to satisfy themselves that the risk meets their requirements. While this is recommended, it is not always feasible due to time or cost restraints.

EXPERT TIP



For businesses that suffer an insurance loss, there is a sense of urgency to settle the claim and resume operations. During the claims process, though, it's essential that businesses work closely with both the broker and loss adjuster to prepare the claim and validate the loss. When gathering facts, evidence or supporting documents, this unified structure can help prevent insurance fraud.

Post-event, once a claim has been filed, relying on the findings of a law enforcement investigation may not be feasible due to timing or any related circumstances related to the event (especially if it's large-scale or a natural disaster). And even if law enforcement is doing an investigation on an event, it may not be a priority, creating an extended period of uncertainty. Lastly, law enforcement may also be very hesitant to provide any info that they do have knowledge of, especially when it is an active investigation.

To manage this process, business owners and insurers need independent third parties that are flexible, have experience across multiple industries and can dedicate the appropriate time required to work through a claim (i.e. gathering facts, evidence and necessary documents) to support the basis of the claim. For truly complex fraud matters, business owners and insurers should expect the third party to have a Special Investigations Unit (SIU) with extensive experience in technical surveillance countermeasures (TSCM) and counterintelligence that regularly work on international assignments.

[READ THE FULL ARTICLE](#) →

SOCIAL ENGINEERING

KEY CONTRIBUTOR



BRAD MOODY, CFI, CFE
Executive Vice President

LIONS & LAMBS: A STORY OF SOCIAL ENGINEERING FRAUD

Brad Moody tells a story of social engineering fraud that, had the CEO created the culture of a high-reliability organization, may have had a different outcome.



One of the memorable jobs that has stuck with you involves the lion-loving CEO. What happened with that?

Brad Moody: I deployed to the location on behalf of our client, an insurance underwriter, to investigate a client of theirs that experienced a huge loss that may or may not have been a cyber event. Our job was to figure that out. What quickly became apparent was that the wire transfer process in place was well-documented, performed, and controlled.

EXPERT TIP

Social Engineering fraud, or “human hacking,” typically exploits and leverages human qualities like trust, helpfulness, and fear for financial gain. Organizations may have their control processes and technical security buttoned-up, but if employees are not trained and empowered to act against suspected fraud, the lion is going to eat the lamb’s lunch every day – or worse.



However, the CEO of this company was very aggressive and very intimidating to employees, and what looked like a cyber event was actually a social engineering fraud that was enabled by the CEO’s behavior.

What happened was, this CEO mentioned on social media that they’d be attending a conference at a specific time, and engaged with visible “marketing” dialog back and forth with the CFO of the same company (who was also set to attend this event), tagging one another in this public forum. Eventually, the controller of the company also got in on the discussion. For a bad actor, this was plenty of evidence that, during that time, certain high-level decision-makers would be absent from and perhaps not paying full attention to operational details.

The bad actor in this fraud did indeed take advantage of all this information and created a fake domain name, switching two letters in the company’s name, like a lowercase “l (el) and an uppercase I (eye)” scenario.

Using the fake domain, the actor developed a fake email trail that began with the fake CEO “emailing” the fake CFO about sending a wire transfer. Affirming this fraudulent transfer, the fake CEO email then forwarded the series of fraudulent messages to the REAL controller, demanding that this wire transfer be made, to the tune of over \$8 million.



What did your investigation reveal about how this happened and what was the coverage they had in place?

Brad Moody: Well, one of my recommendations ended up being around their control process. On paper, it looked good, but it was missing steps. There were obviously a few things that went wrong in this scenario, but clicking the Reply All button — that was bad. If the controller had typed in the email of the CEO and CFO, autofill would have helped the controller out. Likely, they would have noticed the discrepancy in time and there would have been at least some hesitation, for sure. But I’ve seen this exact thing happen now in three different fraud cases after the fact, so it continues to work for the bad guys.

This was a true breakdown in controls, driven by a lack of empowerment in the organization.

[READ THE FULL STORY →](#)

STANDARD OPERATING PROCEDURES

KEY CONTRIBUTOR



DANIEL COOTES

Client Relationship Operations Manager

SOPS AND PRECIOUS METALS: MINING YOUR OWN BUSINESS

Standard Operating Procedures (SOPs) are exactly what they say on the tin – a calculated and tested directive used as a foundation for an operation or individual tasking. Here, Daniel Cootes shares some insights into his experience assessing a mining operation in Asia whose SOPs weren't so much incorrect but existed in an environment where uncertainty was not a risk the insurer was willing to ignore.

Q: Walk us through securing a facility whose threats include local gangs, natural disasters, and ISIS. Where do you start?

Daniel Cootes: The thought process here begins with how to answer one question, really: Could an attacker cross this facility's perimeter, suppress the security onsite, get to the vault, breach that vault, take what they want and then get back out? Intelligence leads us to believe that, yes, this sort of attack is possible, but you also ask, is it likely?

EXPERT TIP

When properly developed and managed, SOPs help organizations avoid unnecessary risk. And as with any business function that supports both short and long-term strategy, managing SOPs involves regular reviews. Many organizations commit to the review process but fall short communicating the updates. Whether a business operates in a high-security environment or not, the real benefit of applying up-to-date SOPs is that compliance becomes a natural part of company culture, providing employees added confidence to perform their work.



Q: What recommendations did you end up making and how did you reach those conclusions?

Daniel Cootes: Given the parameters and all the different angles they had, I made some recommendations of what we thought was acceptable, the operation then came back with what they thought was acceptable based on their operational and cultural perspective. Ultimately, it's about being realistic, and how easy would it be for the operation to implement the updates. Something like this didn't need to be nuclear bomb proof, so we looked first at the gate and fencing that they had, for example. It was all about 10 years old and in the jungle, things get rotten quickly. We talked about upgrading their roving patrols. We also looked at upgrading their CCTV. Technology is so inexpensive, there's no excuse to not have it. There are some other very specific things we did for them that I won't go into, but a good deal of it comes back to their standard operating procedures and making sure their people are following those.

Q: SOPs are incredibly important, and you were able to assess this facility's risk entirely through a remote process – how did you do that?

Daniel Cootes: Lots of questions. I kind of like to start from the outside and work my way in. If I turned up at the site, I tried to build the picture of what was in front of me, and what would stop me from getting in. You just keep peeling back as many layers of the onion as possible and what it takes to get to the good stuff in the vault.

At the same time I'm asking these questions, I have to try and be realistic. I might want them to have a military response, but it's about understanding what they've got and how they can deploy it. I again would go back to the SOPs, who wrote them and how – was the person accredited? How old are the SOPs, what's changed since then? Have those updates been made and communicated?

For me, SOPs are key, keeping them relevant. They're awesome to have, but if they're stuck in a drawer and don't see the light of day for 10 years or until there's a problem, that's not going to work out for anyone real well, is it?

[READ THE FULL ARTICLE →](#)

OCCUPATIONAL FRAUD

KEY CONTRIBUTOR



KEITH GRAY, CFE, CAMS

VP, Client Relations



PEOPLE & PROCESS – THE LONG TAIL OF THE FRAUD TRIANGLE

In business, the concept of the Long Tail implies that an organization can find significant financial benefit selling small volumes of hard-to-find items to many niche customers. Meanwhile, in our work, the Fraud Triangle brings together Pressure, Opportunity and Rationalization to help explain WHY fraud happens.

In this story, Keith Gray blends insights from an epic eight-figure fraud with a few lesser examples to highlight how both people and process actually ALLOW fraud to happen within what could arguably be described as the Long Tail of the Fraud Triangle.

Q: In our work, we're often called in to evaluate and investigate the aftermath of fraud. Is there anything that surprises you when reviewing these fraud cases?

Keith Gray: I wouldn't say it's surprising, but I think it's always very interesting the lengths that people will go to in order to commit or sustain a fraud, complex or not. Unfortunately, what we see a lot, is that trust can lead to a lot of fraud.

Case in point, around the time of the Great Recession, the owner of a large privately held company had been orchestrating a large, ongoing fraud. When the economy was booming, this person was able to move funds around, misappropriating entrusted funds for personal gain through real estate, financial investments, vehicles, various things. When the economy was doing well, this person could always cash out to make things right, it was always in their back pocket. The person was also able to manipulate the vaults and move money around, essentially playing a shell game with the vault's contents to pull the wool over the bank's eyes or anyone that came in to audit the vault. There wasn't a good, coordinated effort to come in and do full vault counts or things like that.

Q: Why would doing a full vault count be important?

Keith Gray: As an independent auditor, we can go in and do a full vault count to get the whole picture. It's exactly the type of thing we push for. An individual bank can go in, but they are only going to see their funds, allowing the opportunity for the fraudster to play a shell game. In this case, the economic downturn aided in the discovery of the fraud. When the country sank into a recession, much of the value in those investments disappeared, so this individual could not make up what was taken.

During this timeframe, one of the bank customers did get a little uneasy, alerting the authorities, and bringing the situation to light. The next thing you know, \$90 million dollars is deemed to be missing. I spent about a year working that on behalf of a couple of clients, just trying to recreate it from the claim side.

Q: What is the mentality of the people that commit these frauds?

Keith Gray: The Fraud Triangle is the why, but the how is the breakdown in controls or the misplaced trust. The commonality is that the thief or fraudster is given the opportunity. Greed is a real thing, and once they realize there's an opportunity and they can get away with something a few times, I've seen a lot of frauds that have lasted 4 – 5 plus years without being discovered.

It's amazing how long and how much some fraudsters can get away with when there is zero independent oversight or SOPs.

[READ THE FULL STORY →](#)

EXPERT TIP

While employers endeavor to hire and retain honest team members, employee theft and fraud remains a reality. The Fraud Triangle explains why fraud happens, but the mechanics of theft and fraud are enabled by people exploiting ineffective processes.

Activities like reviewing and improving SOPs, internal controls and pre-employment screening help limit human capital risk, but to truly build a culture that embraces enterprise risk management means keeping all (or at least most) of the Fraud Triangle at bay.

EXPERIENCE AND TRAINING

KEY CONTRIBUTOR



NEIL WATSON

Director of Global Operations

WIN OR LEARN: THE FRAUDS THAT SHAPE OUR REALITY

A professional fraudster demonstrates, over time, more wins than losses, presuming s/he can stay out of jail. On the flipside, a certified investigator managing fraud claims also counts more wins than losses, a fact required to remain employed. The difference between fraud and investigator, winning and losing, aptitude and attitude is how the person in question applies loss knowledge to determine the future outcomes that shape their reality.

In his 30+ years of work, Neil has seen a few fraud cases, and in just the last 18 months, he's identified at least six potential fraud schemes in the specie market involving precious gems and rubies. However, it was one experience early in his career as a broker evaluating a purported high-value artifact that left him "crestfallen to learn the truth" but ultimately helped inform his approach every day thereafter.

EXPERT TIP

For any business professional, experience without training is self-limiting, and training without experience minimizes an ability to adapt. Tomorrow's best leaders drive innovation with this understanding, and security professionals actively apply their wide range of certified - and earned - knowledge to their client's advantage. Creating a secure environment for any organization embraces the known and unknown.



Your background is in specie. What type of frauds are most often presented to you and what do they involve?

Neil Watson: The frauds that come across our desks are usually for considerable values, hundreds of millions of dollars, sometimes up to \$1 billion. That's when the first red flag goes up. With a bit of research, there's usually precedent to be able to understand what's legitimate in the market and what needs a critical eye, regardless of the packaging and details we are shown.

It can get a little more challenging with goods that come from the process of gold refinement, scrap and earth, as there's lots of byproduct that comes out of a gold mine that can have a content of gold in it. We've seen clients who have been sold sacksful of dirt who then want to insure those bags, but they have been actively deceived. A proper eye and investigation early on can mitigate that, but you're typically sorting out either buyer naivety or straight up fraud with those.



You've been at this for over 30 years now. Have you ever been duped in your career?

Neil Watson: One that still sticks in my mind was when I was a broker. It was very early in my career, predating the Internet, email, all modern technology, and I had received a package for what was purported to be the world's largest gold Buddha. Someone wanted to insure it. The contact had taken the time to put together a stellar presentation. A beautiful packet with photographs, write-ups, certificates, it had everything. Obviously, whoever did this had gone to a great deal of effort to make this statue look legitimate.

As a young broker, to get this thing and have it drop in my lap, I was excited. I planned on trying to get coverage for it. With a couple phone calls though, I was sensing reluctance from the conman and it became apparent to me that this was maybe not a real thing. But I was holding out hope.

One of the reasons for that, is that at the time, I was doing things for the Royal Academy like Jeff Coons' "One Ball Total Equilibrium Tank," for \$5 million dollars. It made the idea of a giant, never-before-seen golden Buddha seem totally plausible. I had a good contact in Hong Kong, a wily old expat who'd been in the security industry for a long time and he just said, "No, mate. Absolutely not. It's not legit." I really trusted this guy, but I just couldn't believe it. Lo and behold, though, after a bit more investigation and questions, poof, this thing, my contact, the whole request, disappears up in smoke. I was truly crestfallen to learn the truth of the whole thing.

[READ THE FULL STORY →](#)

SURVEILLANCE AND INVESTIGATION

KEY CONTRIBUTOR



KRISTOPHER KEEFAUVER

Director of Clients, CIT, Safety

PRISON BREAK: HOW COLLABORATION IS CHANGING SECURITY FOR THE BETTER

Companies use a collaborative approach for a number of reasons, including the more immediately realized benefits of efficiency and cost savings. But additional benefits of employee engagement and cultural change are two other downstream reasons where collaboration creates a positive impact for organizations.

The positive impact of collaboration is clearly depicted in this Q&A with Kris Keefauver, as he recounts an investigation experience with a team of security officers that, until that point, were not empowered nor necessarily trained to take the steps required to work through a suspected crime.

Q: You recently represented L&A as the Interim Security Director for a healthcare organization. What did that look like and can you describe some of the issues they were dealing with?

Kristopher L. Keefauver: Our task was three-fold: 1) Complete a security risk assessment of the campus; 2) act as the interim security director; and 3) be involved in the remediation efforts for any of the findings and recommendations that were brought to light during the assessment. The organization had a staff of about 10 to 12 security officers, and our team was engaged to provide leadership and oversight while revamping the security department. The security team reported directly to us, we'd provide direction and supervision, and then report directly to the healthcare organization's COO.

Serving in these capacities, a lot of what we found was that the staff that was on site weren't necessarily aware of the policies, procedures, and processes that the healthcare organization had documented.

EXPERT TIP

The Rational Choice theory suggests criminals are less likely to commit a crime if they believe someone will see them or if there's a higher risk of being caught. In these instances, Closed-Circuit TV can be a significant and effective deterrent against crime. With digital technology more readily available to modern businesses, CCTV is accessible, serves as a form of formal surveillance and, when paired with proper investigation processes, actively aids the criminal justice system.

The organization had done a great job of detailing out all these policies and procedures to be followed, but somewhere along the line, the chain of command or the dissemination of that information didn't necessarily make it to the guard staff.

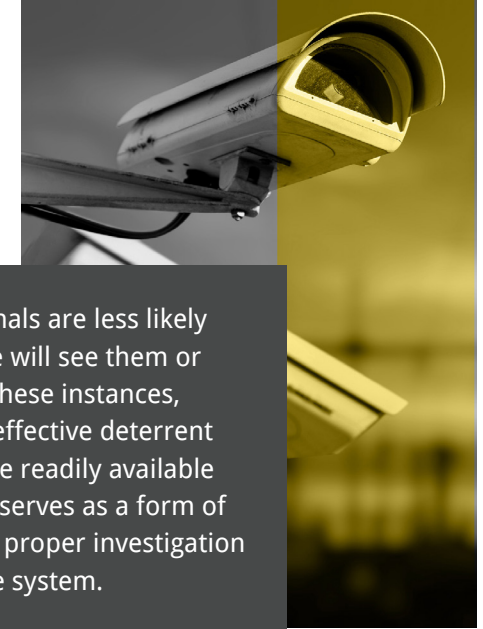
Q: In helping realign SOPs, revisiting hiring criteria and amplifying the need for training, you spent a lot of time on-site with your security officer team. Is there anything about the time or work together that stands out?

Keefauver: The most impactful moment for me happened at the end of a 12-hr shift. I was leaving work, heading down the stairs into the parking lot and ran into one of the security officers. After some small talk, he mentioned that they thought someone had stolen some shirts from the gift shop. I asked what their plan was, and he said, "Well, I'm going to go out in the parking lot to try and find her." I went along with him to the parking lot.

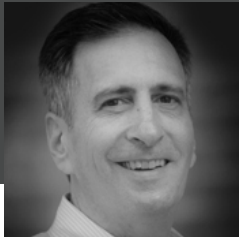
Needless to say, we didn't find her, so we came back in and talked to the other security officers, asking what they normally do in this situation. It was mentioned that there was one person that knew how to work the CCTV systems (self-taught), but that individual wasn't there; so essentially, the team was going to just let it go.

I talked to the gift shop employee and tried to get a description of the person, went to the CCTV system, and was able to locate the person based on the time she was in the gift shop, what she was wearing and other attributes.

[READ THE FULL STORY →](#)



KEY CONTRIBUTOR



JON D. GROUSSMAN, J.D.

EVP Consulting Practice

PROACTIVE COMMUNICATION: THE HUMAN ALGORITHM FOR MANAGING RISK

When it comes to mitigating risk, proactive communication's predictive capacity is less about mind-reading and more about behavior-reading. It enables a framework that employees can use to identify and communicate red flags before those red flags turn into bad behavior and a court case, or worse, yellow caution tape.

In this Q&A, Jon Groussman crystalizes the 'before and after of risk' using an example of a client that took a massive hit to employee morale and reputation that, had proactive communication and continuous monitoring been options, might have been avoidable.

Q: **This particular incident occurred at a research and manufacturing facility and involved a supervisor and an employee. Can you tell us what happened?**

Jon Groussman: I remember I'd gotten to the office a little bit early that day to do some catching-up. My phone rang right around 8:30 and it was an executive from a client's facility letting me know that they had an incident the night before at around 11pm. A supervisor on the overnight shift had brought a handgun into the facility, put the handgun to the head of one of the workers, and threatened to blow the co-worker's head off if he ever spoke to the supervisor again. The police were called, the supervisor was arrested for aggravated assault and possession of a firearm, banned from the property and then, of course, taken into custody.

Unfortunately, the executives didn't really know much about what actually went on during this 3rd shift which, for all intents and purposes, was an overnight shift.

EXPERT TIP

Organizations of all sizes can benefit from proactive communication. In a secure environment, it enables coordinated action and helps create cohesive, efficient workflows. Without proactive communication, safety compliance behavior suffers and workplace hazards are allowed to endure, negatively impacting employee morale and productivity.

A lot of times, not only in this environment, but in other environments that have shift workers or that are open 24 hours, the more senior management doesn't know what's actually happening during those hours. What develops then is a communication gap. I started to interview people.

Q: **You mentioned a pattern began to emerge. Were there red flags that went overlooked?**

Jon Groussman: There are almost always red flags; this kind of thing generally doesn't happen out of the blue. In speaking with people working that third shift, I was told the assailant took longer breaks than everybody else. As he was a supervisor, people didn't question it because he also got his job done. The problem was, we found out he was leaving the site – using the only camera that was well-positioned and functioning – to visit a neighboring community that was very well known for selling drugs. We could see his car come and go at the times when his colleagues said he would be on longer breaks, and this began happening more frequently in the months prior to the attack.

With that revelation, we went to law enforcement to see if he had a record or had any weapons issues beforehand. It turned out he'd been in court numerous times within that past year for purchasing drugs in the community I mentioned, but this client and facility didn't have a system in place to know that. Now remember, this was a person in a supervisory role with access to assets within this facility that a loss or accident could have been very bad. The materials and trade secrets were also very valuable on the secondary market, had he been desperate enough to need money for drugs or been coerced into stealing them. Had this client and facility utilized some type of continuous monitoring and had a disciplinary policy, this incident would have likely never happened because he would have been gone long before it happened.

[READ THE FULL STORY →](#)

ABOUT LOWERS & ASSOCIATES

L&A FOR INSURERS

Everywhere you need us to be.



Risk Assessments
& Evaluations



Strategy



Risk Mitigation
& Loss Prevention



Loss Recovery
& Claims

GO FORWARD WITH CONFIDENCE

Big or small, when problems must be solved, organizations around the globe trust the Lowers name.

Lowers & Associates (L&A) is an internationally-recognized risk mitigation and loss prevention firm that proudly operates under the Lowers Risk Group family of companies. L&A works with organizations operating in high-risk, highly-regulated industries and with organizations that operate with a risk management mindset.

Our work addresses a broad range of issues, including fraudulent claims investigations, audits for regulatory compliance, cybersecurity policies, litigation support, and security. Our experts have extensive experience in related disciplines such as risk management, accounting, law enforcement, physical security, information technology, and human resources. Our diverse professional backgrounds and depth of experience allow us to zero in on your organization's needs and provide the appropriate solutions to protect people, brands, and profits.

When it really matters, put Lowers on your side.



**LOWERS
& ASSOCIATES**

International Risk Mitigation Partners

Request a conversation at lowersrisk.com