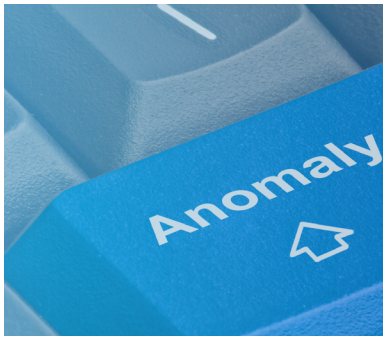
THE INSIDER THREAT:

Mitigating Risk Within the DNA of Your Organization

StoneTurn

Table of Contents



Introduction

Understanding and managing insider risks is not a new discipline. The manifestation of insider-related risks can be disastrous but the fact that these events are caused by people inside an organization rarely receives enough attention. That may be because we lack clarity about what insiders are and the threats they present. Every year, insiders cause long term and sometimes catastrophic damage to businesses of all sizes and in all sectors. It's just that we don't categorize many of these acts as insider acts. And so, we miss the opportunity to take a more systematic and holistic view of the risks posed by insiders.

WHAT IS INSIDER RISK

According to the UK's Centre for the Protection of National Infrastructure (CPNI), an insider is "a person who exploits, or has the intention to exploit, their legitimate access to an organization's assets for unauthorized purposes." This is anyone who is provided with access to an organization's assets (physical or virtual) and can therefore include contractors, sub-contractors, and partners. The risk can manifest itself as fraud, data loss or corruption, theft, sabotage, and the leaking of sensitive information. This risk can impair an organization's reputation and bottom line, and impact every employee, making the mitigation of insider risk a strategic imperative for all organizations, in the boardroom, the mailroom, and everywhere else in between. The impacts are often hard to define and long-term. For example, while it is possible to put direct losses from a fraud case, it is harder to identify the long-term damage to investor confidence, market reaction, and the resulting lost future earnings. The loss of IP can in some cases be terminal for a fledgling business.

Insider risks have evolved and adapted, becoming more complicated and pervasive. For example, many organizations that shifted to remote working to continue operating during COVID-19 lockdowns are now using, managing, and storing critical assets differently, without giving enough thought to how their people are interacting with their technology and what consequences may arise from unfettered insider access. In addition, the changing geopolitical landscape, including the invasion of Ukraine and the rise of China, among other factors are impacting business' risk profile.

WHY IT'S A PROBLEM

At the core of nearly every business is its people—they are the DNA, interwoven with their collective ideas, creativity, and judgement to make up the fabric of almost any organization's value proposition. And while humans are critical assets and the success of a business is frequently dependent upon them, they are also among the greatest and costliest risks.

To give an idea of how pervasive and costly the insider risk problem is, let's look at some numbers. The Association of Certified Fraud Examiners (ACFE), estimates that total global losses due to fraud are nearly $5.0 trillion dollars. Occupational fraud—fraud committed by an executive or employee—is responsible for approximately 40% of the total amount, or $2.0 trillion. In their 2021 study, the ACFE studied 2,110 cases in 133 countries, finding that each case averaged a loss of nearly $1.8 million. That translates into 5% of revenue lost to fraud annually.

These nation states have combined established techniques with technological advances to sharpen their effectiveness and pose a more persistent and more severe threat, including their continued and enhanced efforts to exploit insiders. Consequently, while organizations strengthen their cyber defenses against outsiders, they must also look to strengthen their personnel security defenses, otherwise they leave themselves vulnerable.

We have not painted this picture to portray the landscape as grim and without hope. On the contrary: we believe that with a deeper, more holistic understanding of the risks facing businesses today and the right infrastructure in place to safeguard internal systems and assets, organizations can be better positioned to mitigate insider risk.

Our insights are rooted in decades of experience, but are evolving to meet the challenges of the moment. As the landscape shifts and the risks evolve, we look forward to continuing the conversation.

Brad Wilson

Brad Wilson,
Managing Partner & CEO, StoneTurn

Good Governance: Accountability and Making It Work

Perhaps one of the biggest challenges to implementing an effective insider risk program is determining the governance structure to oversee and guide the program. Experience of managing insider risks shows that a single, accountable board-level ownership of personnel security risks, and the visible top down implementation of policies and expected behaviors, supported by good line management, will promote a consistent and compliant approach building a high trust security culture. But where do organizations begin in establishing this kind of accountability?

Effective corporate governance structures and C-Suite awareness of what insider risks are will promote effective holistic security strategies to manage them. Such an approach will ensure that all those with skin in the game are engaged in the risk management strategy. This will require participation from a number of internal departments, including human resources, cybersecurity, physical security, ethics and compliance, legal, and investigations. All of these stakeholders should have a clear and shared understanding of what insider risk is and agree to work on an enterprise-wide basis to manage it.

As part of an overarching protective security strategy, strong security governance will deter those who may want to harm the organization by creating an open and transparent organizational framework where security is actively promoted as the responsibility of all. This will also provide appropriate resources and support to promote a proportionate, dynamic, and holistic multi-disciplinary approach to manage insider risks. Positive and visible Board-level support and supporting governance for protective security is critical to demonstrate to the business the value placed on personnel and people security policies and procedures.

Strong security leadership supported by good governance, across an organization will:

- Ensure consistency and clear lines of responsibility for the management of security risk
- Foster a multi-disciplinary approach to managing insider risks
- Ensure proportionate and cost-effective use of resources
- Provide essential management information for the purposes of security planning and people management
- Provide a strong example that both develops and underpins an effective security culture
- Support efforts to build a dynamic and inclusive organization by promoting a speak-up culture

We note that Board-level support is not enough to constitute effective governance over the insider risk program. Individual accountability at the Board-level, an individual Board member assigned to the program, like any other Board committee, along with a dedicated C-suite champion is required for the program to be sustainable and most effective.

The accountable Board member should oversee and appoint an Insider Risk Working Group with key practitioners from stakeholder departments to manage insider risk. This group should be led by a senior practitioner from one of the stakeholder groups.

Establishing an Insider Risk Working Group

When examining insider risks over time, case studies are littered with stories where earlier intervention would have helped minimize or avoid damage, if concerted and joined up action had been taken earlier.

Bringing together a group of practitioners can be of immense benefit. They can act as a "critical friend" to any personnel security program. Perhaps more importantly, with some agreed principles, they can work through the practical problems and solutions when red flags are raised in the organization. In other words, they can help answer the question of "what do we do?" when a situation comes to light.

The multidisciplinary group will work across silos collating information and agreeing upon practical steps to safeguard the organization. The holistic use of targeted security measures and interventions (e.g., cyber/information, data analytics, personnel and physical) can help spot concerning workplace behaviors, and facilitate early intervention to reduce the potential of employees carrying out malicious attacks.

In addition, this group will be expected to produce periodic reports to the C-Suite on the program's effectiveness, key statistics, lessons learned, and improvements made over time. By learning from each incident and feeding any lessons learned into the risk assessment process, the organization can continually improve its management of employee risk.

The objectives of the Insider Risk Working Group will be to:

- Mitigate identified people risks (defined as counterproductive employees' behavior, whether inadvertent, negligent, or malicious, that can harm the organization)
- Develop an advance "response guidance" to an insider incident: how to respond, how to minimize damage and retain stakeholder trust
- Advise the Board of response to external and internal reputational damage
- Anticipate regulatory trends
- Anticipate the expectations of employees and wider stakeholders
- Reflect, strengthen, and contribute to the security culture of the organization
- Assess the evolving insider risk for the organization

Protecting against insider risk begins with accountability. A Working Group will help drive an organization's strategy and approach, and ensure departments and verticals within an organization are keeping close tabs on their areas of responsibility. Getting started may feel daunting, but by taking the plunge, organizations will be better protected in the long-term.

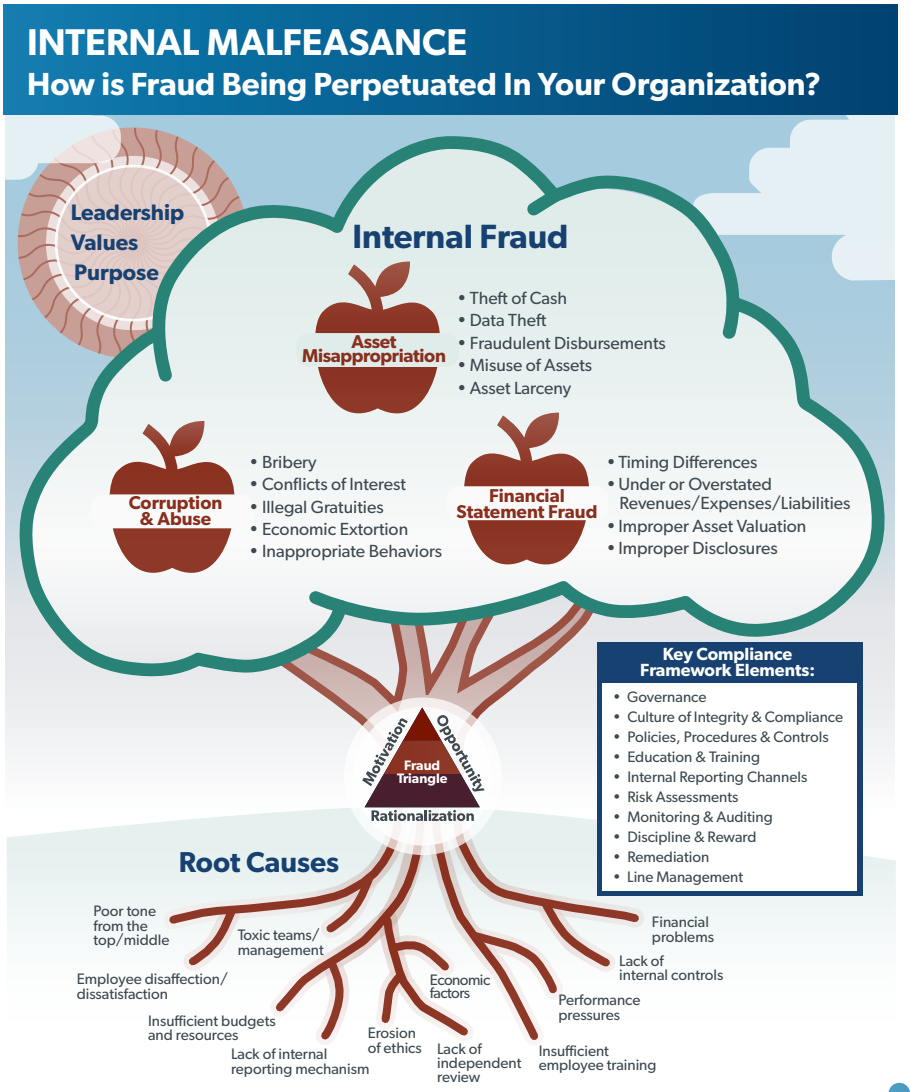
Insider Risk: The Human Factor

When people are involved, there will be behaviors. When there are behaviors, some will break the rules, some will cross ethical boundaries, and others will be desirable and appropriate. Organizations must pay attention to the human factor and be on the lookout for behaviors that are positively aligned to corporate values and policies, and those that are unethical and undesired behaviors.

However, things are not as simple as they first appear. How do we know that our decisions and behaviors are ethical and have integrity? Although we like to think we are making principled decisions, **research** tells us that we are not as ethical as we would like to believe.

Good people do bad things

Good people can do bad things without being aware that they are doing anything wrong. While we like to think of ourselves as fair, ethical, and lawful, science and experience show us that we are all capable of committing unethical acts. We can approve of the dishonest acts of others, for example, even when we believe we are doing the right thing. These are called ethical blind spots. In short, there is a gap between what we intend to do and our actual behavior. We recognize what we should do but we end up doing what we want to do. Research published in a **Harvard Business Review**



Source: ACFE Occupational fraud and abuse classification system.

article tells us that behavioral or ethical blindness is a "slippery slope" created by cognitive biases. The outcome of a decision has a disproportionate influence on an observer's perception of whether the behavior involved in the decision is ethical. That is, if the outcome is positive, the unethical behavior that took place to achieve that result tends to get overlooked, or even missed entirely.

Good people can do bad things without being aware that they are doing anything wrong. While we like to think of ourselves as fair, ethical, and lawful, science and experience show us that we are all capable of committing unethical acts.

Ethical fading

Why do we suffer from these ethical breakdowns and flawed decision-making processes? Are all human beings inherently bad people? There are good reasons why this happens. **"Ethical fading"** describes a phenomenon where the ethical aspects of an action disappear from our view. A common human psychological tendency is self-deception in order to rationalize actions, becoming an integral part of the "slippery slope." Our minds are subject to bounded ethicality or cognitive limitations that can make us unaware of the moral implications of our decisions.

Aspects of everyday work life, for example, business goals, reward and recognition, compliance requirements and performance objectives, can blind us to the ethical implications of a decision, so that our decision becomes a "business decision" rather than an "ethical decision," thus increasing the likelihood that we behave unethically.

For example: In professions that require employees to bill their hours, new employees may strongly believe that they would never bill hours they had not accrued. However, over time, the employee may find themselves short of their target billable hours. To make up the shortage, they add 15 minutes each across five projects on their timesheet. It's only 15 minutes per project, it's hardly a big deal, is it?

What is a big deal is what has happened to the employee psychologically. The ethical standards have now shifted, the line between what is ethical and unethical has changed, and the requirement to meet target billable hours has blinded the employee to any recognition of breaking ethical boundaries. Ethical fading has occurred. And it doesn't stop there. Ethical numbness begins to set in and each time the employee falsely charges time, it becomes less ethically painful and moral disengagement takes root, deep and hard to shift.

It becomes the right thing to do.

It's the human factor

Ethical breakdowns, the slippery slope, blind spots and ethical fading are all examples of insider risk. These do not occur due to external forces. They reflect the fact that as human beings, we all have an intrinsic susceptibility to undesired behaviors and flawed decision-making processes that will inevitably take place unless the conditions that we operate in are controlled and monitored with ethicality in mind.

Ethical breakdowns, the slippery slope, blind spots and ethical fading are all examples of insider risk.

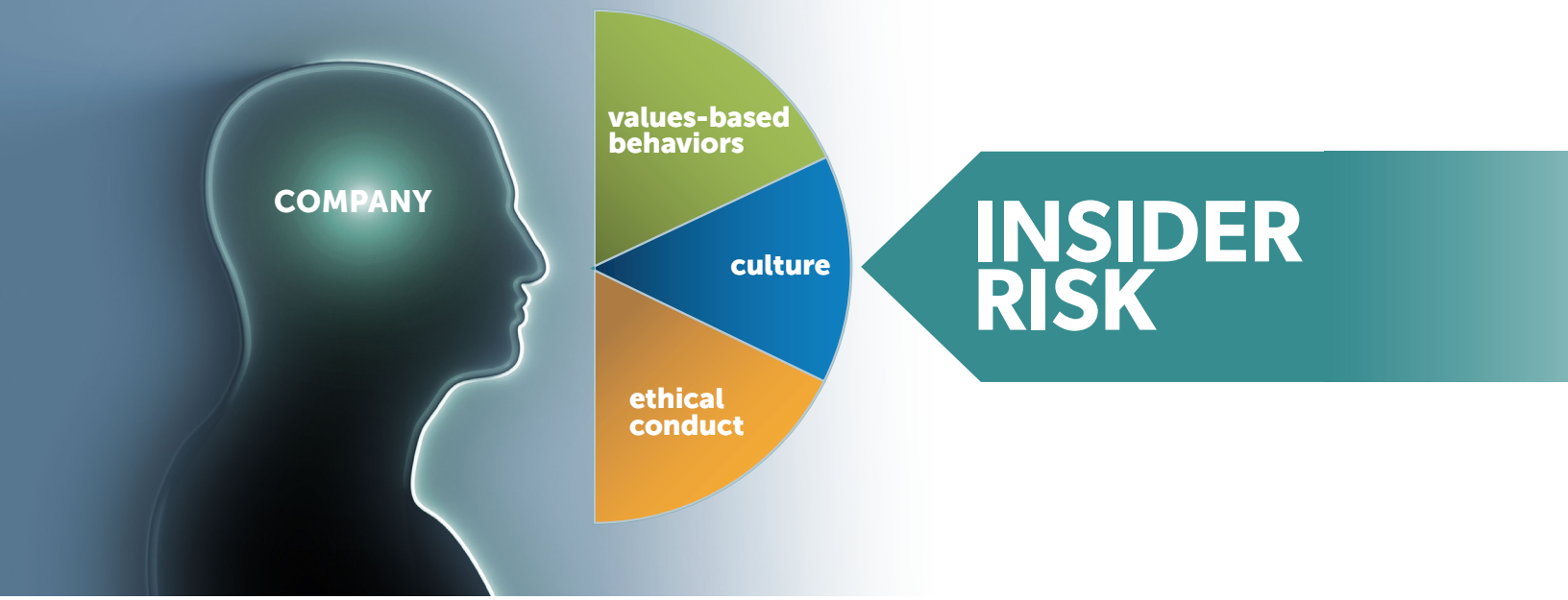
Organizations should monitor how they are creating institutions, structures, and incentives that increase the likelihood of bounded ethicality. Bounded ethicality describes the systemic and predictable ways in which people make decisions without realizing the implications of their behavior, including implicit prejudice and conflicts of interest. For example, even individuals who espouse equity and diversity, might discriminate based on gender or race without being aware of it. When companies allow these prejudices or conflicts of interest to remain unchecked, the consequences will be the boundedly unethical actions that will inevitably follow and ultimately cause harm.

Witting and unwitting; Malicious and non-malicious

One way to think about different types of insiders is to differentiate between the witting and unwitting and the malicious and non-malicious.

An unwitting and non-malicious insider would be someone who unknowingly breaks the rules (such as cyber ones). They aren't malicious and aren't aware that they are doing anything wrong but can still cause significant damage. Many organizations put huge effort into making people aware of cyber risks, for example, for this very reason. It may be that they were poorly trained or had simply forgotten what the rules were.

The witting but non-malicious is a person who knowingly breaks the rules but doesn't intend to cause harm. Typically, this is seen where people deliberately bypass controls (for example, in their minds, to be more efficient). The *witting and malicious insider* deliberately breaks the rule and intends to cause harm, such as stealing their organization's critical IP.



Addressing the human factor of insider risk

Human behavior is not all good or all bad. People can be ethical, and they can be unethical. Individuals can commit acts that are heinous, or heroic. Herein lie both the weakness and strength in combatting insider risk. We need to narrow the gap between intended and actual behavior, equip people to know what the right thing is to do, and address the psychological processes that create blind spots and lead to ethical breakdowns.

Organizations need to recognize that values-based behaviors, ethical conduct, and culture are a first line of defense to insider risk and are critical elements of any effective insider risk management framework.

Why rules alone are not enough

Implementing rules, regulations, policies, and procedures are necessary but insufficient on their own to mitigate insider risk. Controls are needed in any business process where we want groups to apply consistency, or when we need to remind people what to prioritize, especially when introducing a change. However, controls and supporting policies and procedures will not be enough as they presume decisions are always a choice between a "right way" and a "wrong way." Many decisions involve choices between two acceptable options, and as noted above, we need to challenge any blindness we may have on the ethicality of the path we choose to take.

There is a need to apply integrity-based principles, within the boundaries of accepted rules and laws, to elevate decision-making and expand horizons to include choices beyond what is right versus what is wrong. This is why organizations have codes of conduct and ethics and compliance teams, to help individuals navigate complexity and make the right decisions This will enable employees to broaden their decision-making thinking to not just what should they do in accordance with laws and rules, but what could they do, aligned with company policies and values. In this way we can start to challenge the gap between intended and actual behavior and interrupt the psychological processes that can lead us down the "slippery slope."

Disrupt the psychological processes that lead to ethical breakdowns by:

Educating, empowering and equipping

your leaders and employees to recognize their blind spots and why we often fall short of our own ethical standards – not because we are inherently bad, but because we are human beings.

Identifying

any hidden, but powerful, informal values or norms that motivate individual's choices and drive behaviors in the organization.

Implementing

integrity-based controls and principles into day-to-day decision-making processes to act as an ethical or moral compass that can navigate risk-based choices and uncover unintended consequences.

Next steps

Ethical breakdowns are an inherent part of the human condition and represent a contributor to insider risk in an organization. This is not going to change. There is no blueprint or "one size fits all" solution to address the sheer beauty and complexity that humans bring: blending innovation, creativity and diversity with blind spots, bias and prejudice. People make choices and choices make culture. Organizations need to make—and help others make—better choices.

Organizations need to be more vigilant about the human factor of insider risk.

Engage and empower your people to be more aware of their human vulnerabilities. Shape and design a cultural ecosystem built on corporate values and bounded by integrity-based policies, controls and procedures. And build a shared belief in doing the right thing across the organization, starting from the top and hardwiring it into a cultural norm of "the way we do things around here."

Strive to Understand Why Insiders Go Wrong

Uncovering unethical or malicious behavior by an employee can be perplexing for an organization and prove difficult to decode. Yet for David Burroughs and Nathan Fisher, years of experience investigating fraud and malfeasance in the private sector and within U.S. national security has shone a light on the motivating factors for insiders and key controls to mitigate threats. They share their unique perspective and tales from the frontline in this Q&A.

What are some of the most common motivations you've observed in cases involving insider risks?

Burroughs: People make poor decisions for different reasons. Circumstances can alter people's perspectives and ethics. Ego plays a significant role in insider behavior. For example, someone gets overlooked for a raise or promotion, feels underappreciated or feelings get hurt, and they decide to "show them just how good or how smart they are."

Some people look to exploit processes, asking "How can I beat the system?" This can often start as a small test transaction, or possibly even an unintentional act—such as accidentally expensing something an employee did not intend to—and if the transaction goes undetected, the act will likely grow into a larger scheme once the person realizes no one is watching.

Others are emboldened by a sense that their employer will not likely prosecute if the potential exists for reputational damage if their acts became publicly known. Greed is often a factor as well. Unless they make a spontaneous decision to take advantage of a vulnerability, insiders who commit crimes usually have to contemplate their actions and weigh the potential gains against the consequences of being caught. People rationalize their own behaviors all the time.

As an investigator, I believe empathy is a vital component in assessing behavior while trying to identify their motivation. I believe it is essential to try and understand what they felt and if possible, why? Empathy perspective often helps to put context to an insider's actions, and in turn can help to unlock what happened and why.

What are some examples of insider risks you've seen?

Burroughs: Each industry has unique risks and challenges when it comes to insider threats. Out of the many frauds I have investigated, a few stand out as relatively common across various industries. The Chief Financial Officer (CFO) of a global

company had exclusive control over the disbursement and reconciliation of all the finances. There were no financial controls or oversight, which enabled the CFO to approve loans to himself totaling in excess of $1 million over a two-year period.

In addition to his fiduciary duties, another CFO was also responsible for reconciling his company's credit card accounts. The CFO had not received anticipated bonuses or raises he felt entitled to because he worked so hard for the firm. He was a classic example of a disgruntled employee, and as a result, felt ***entitled*** to use company funds for personal expenses — a big party at his home costing thousands of dollars, trips, luxury goods, excessive bar tabs, massages, cash advances, you name it. He ended up stealing more than $325,000. Sometimes, the insider is the very person who is entrusted with the responsibility of protecting the company's financial wellbeing.

There was also the investigation which involved a bookkeeper at a large bank who was responsible for paying various vendors who serviced the bank. One day, she decided to test if she could pay her gas bill, and submitted the payment as if it was a vendor.

Once that payment cleared, she submitted several additional small payments which were not flagged or detected. Once she was confident there were no audit controls in place to catch these kinds of payments, she quickly escalated her purchases, eventually buying, cars, boats, personal watercraft, and even a home. It's a good example where the failure to have robust financial controls in place will allow even junior staffers the opportunity to exploit the process.

How can organizations identify insider threats?

Fisher: Incidents involving insiders can be hard to spot. Without traces of evidence, such as paper or digital trails, it's difficult to find the bad actors. Technology and related controls can help provide some insight, but often organizations must look for changes in an individual's behavior as the first indications. Changes in personality may be an indicator and can signal something is going on with that employee. Organizations should watch for changes in a colleague's demeanor, performance or how he or she interacts with others. Changes in financial habits—whether it's unusual or grandiose spending, or recent hardship—can be an indicator that something is amiss. Acting abnormally gregarious or suddenly preferring isolation may be red flags that warrant a closer look at an insider's activities.

Such abnormal behavior may manifest itself in the form of an insider refusing to take a vacation, or always being the first in and last out of the office. He or she may have a fear that their activities will be discovered if he or she is unavailable to answer questions about anomalies discovered in their absence. Demonstrating a new found interest in a particular area within the company outside of their scope of responsibilities may also be a cause of concern.

6 Categories of Motivation

There can be as many motivations behind undesired insider behavior as there are individuals, but most acts tend to fall into six categories. These are:

1. **Psychological.** This includes insiders who may be angry, stressed and/or depressed. For example, insiders may act in retaliation for some perceived slight, such as being overlooked for a promotion or bonus. Feelings that "I deserve this" or "I will show you I'm smarter than all of you" may serve to justify or rationalize an insider's bad acts.

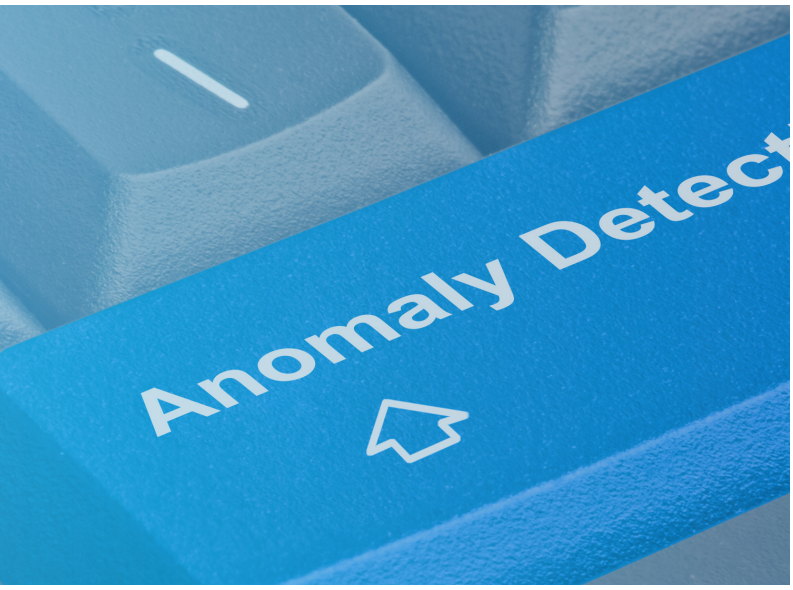
2. **Financial.** Debt, family illness, addictions to substances or gambling, and living beyond one's means can all serve as motivators for theft, embezzlement or conspiring with outsiders for financial gain. Outright greed is also a very strong motivator.

3. **Relational.** Insiders are sometimes approached to join a conspiracy against the organization. These schemes can take the form of an invitation by peers or, depending on the sensitivity of an insider's position, coerced participation through blackmail or extortion. The threat may come across as "If you don't do this," the conspirators will inform the insider's superiors or family members about some past transgression or compromising behavior.

4. **Environmental.** Poor controls and/or a poor culture in an organization can serve to motivate some individuals to commit acts of malice or even illegal behaviors. A perception that the likelihood of being caught or that a fellow colleague will report anything often contributes to an insider taking action.

5. **Situational.** Personnel who are isolated and have infrequent interactions with co-workers and supervisors are also a risk. With a greater number of individuals now working remotely, the opportunity to act when "no one is watching," is much more prevalent.

6. **Ideological.** Insiders also may find motivation in taking action for a cause or ambition, something they believe their actions will support. The English legend of Robin Hood, who purportedly robbed the rich to give to the poor, may have been fictional, but similar ideologies can be quite real.



How do insiders typically get caught?

Fisher: If control processes don't spot anomalies, sometimes insider activity will come to light when another employee says they noticed something. But this is dependent on employees feeling empowered to speak-up. This generally only occurs if there is a belief or a track record of the organization taking appropriate action in the past, when others had spoken up. Confidentiality and fear of potential retaliation may also impact an employee's willingness to come forward. The culture of the organization plays a direct role in establishing such reporting.

> *Watching for anomalies in employee behavior is the key, but it's important to look at the totality of indicators, not just one or two.*

An event may trigger someone at the organization to look into an instance that felt "off" and then the wrongdoing is discovered, such as someone coming into the physical workspace at off hours. I once had a case where a security guard flagged long, abnormal hours of an otherwise dedicated employee—late nights and early mornings. We discovered this employee was taking company information when nobody was watching, showing that these long hours are not always indicative of hard work or dedication to a company's mission.

Watching for anomalies in employee behavior is the key, but it's important to look at the totality of indicators, not just one or two. There may be good explanations for anomalous behaviors, and what matters is for organizations to understand what's going on with their employees.

Two Main Reasons Whistleblower—or Speak-Up—Programs Fail

1. **FEAR:** Insiders worry about retaliation or reprisal
2. **FUTILITY:** Insiders observe or sense the organization will not respond to concerns

Data Analytics: Tools to Visualize and Mitigate Insider Risks

Insider risk touches every department of an organization, from the Board, to senior management, the general counsel, and compliance team. For this reason, organizations of all sizes need actionable information that is relevant to each function, synthesized and presented in a way to allow reaction to that information. When properly configured to support those stakeholders, **data analytics** are powerful tools to assist with the identification and mitigation of insider risk.

One of the most useful capabilities of robust data analytics is the visualization of risk. Data can tell us a story about insiders' activities. Analytics help present that story by integrating multiple data sets and displaying them in a way that offers quick insights, such as through dashboards tailored to the C-suite, Board, general counsel, and other functions. This, coupled with human assessment and analysis, investigations, and experience, can help paint a clearer picture of an organization's risk profile.

There is a critical difference between the seemingly healthy organizations and an unhealthy one—yet data analytics can prove to be a powerful tool for both. For a seemingly healthy organization, skilled professionals can leverage data to help pinpoint where the highest risk may be. For an unhealthy organization, the data can demonstrate where things may have gone awry, and help dig for the needle in the haystack.

For example, an excessive number of transactions by an employee in sales might raise suspicions, as it did for one organization that discovered an employee was dining out with the same client multiple times every month, costing the company thousands of dollars. If manual processes are the sole backstop for reviewing and approving expenses, such activity might take a long time to discover. With the right data, and parameters set by the organization, suspicious behaviors can come to light much sooner and enable leaders to look closer before a problem transforms into a serious compliance matter.

There could be plausible reasons for frequent entertainment expenses relating to a client. It might represent additional business the organization has sought to acquire. But it also could be ill-advised and potentially illegal activity that might cause significant reputational damage, such as facilitation payments to government officials or worse. Either way, it's better for the organization to know about it and investigate.

Getting ahead of trends

One value proposition for data analytics is their ability to enable organizations to get ahead of trends before they become problematic. There is no substitute for knowing what's happening inside the organization in real time, and that knowledge is frequently available through the right analytics.

Once an organization has a handle on current activity, it can begin to move from current insight to foresight. That is, the organization can identify – and mitigate – future insider threats through predictive analytics.

A common misconception about predictive analytics is they require sophisticated systems for artificial intelligence and machine learning. AI and ML are indeed useful tools in analyzing volumes of data, but organizations can gain valuable insights through simple rule-based approaches If you observe X in the data, that might indicate a Y type of risk at a Z level of criticality.

Here's how that might look in practice: There is an instance in employee T&E data where the same employee has submitted duplicate receipts seeking reimbursement for both; that is marked as potential fraud with a risk level 2 on a scale of 1 to 5 (it could have been a one-off oversight). If repeated instances of such an anomaly by the same employee are observed over a period of time, the risk level could be marked as a 4 or a 5 as this could be an attempted fraud. An analytics solution could be developed to encode such IF-THEN-ELSE rules that would analyze data, assign risk types and scores and publish them in a dashboard for review and action—all in a fully automated fashion.

Collaborate to enrich data

Implementing data analytics to address insider risk in an optimal way requires a cultural aspect. Collaboration should occur in terms of people, data and processes. When an organization has a culture of collaboration and compliance, functions talk to and learn from each other, and inherently share information.

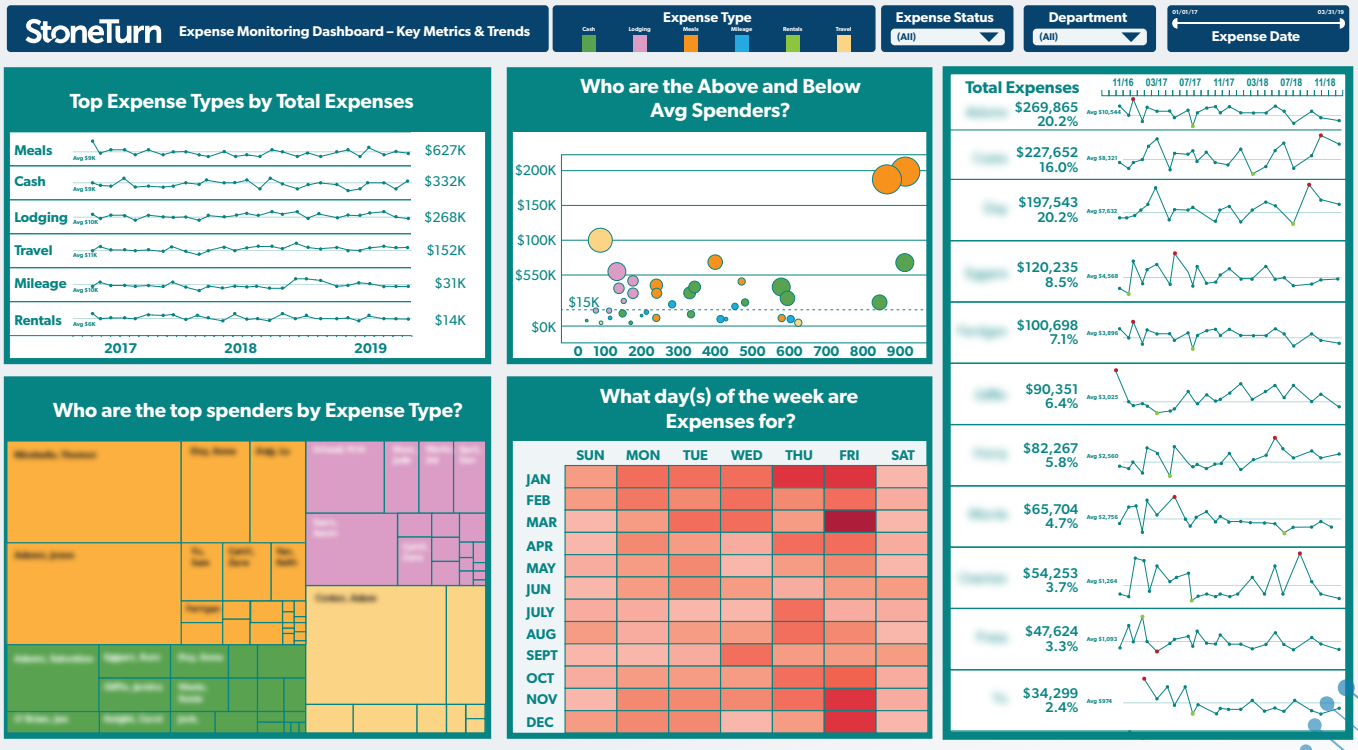
When an organization has a culture of collaboration and compliance, functions talk to and learn from each other, and inherently share information.

For example, the compliance data on trainings, hotline, conflict of interest, and gift registry in conjunction with HR data including performance

Sample Dashboard: Expenditure Abuse

Employee Expense Dashboard

A sample dashboard demonstrating risk patterns across multiple datasets.



StoneTurn

appraisals, organizational structure, employee relations, surveys, and more can offer a deeper view of potential insider risks as they relate to workplace misconduct. Add to that data from legal, internal audit and procurement, organizations will have an insider risk 360-degree dataset.

But it shouldn't stop at internal data sources. External data such as geodemographics, salary benchmarks and more can further enhance the power and specificity of insights. A retail company with multiple locations could for example leverage such data to keep tabs on gender-based pay discrimination, racial biases in hiring, among other risks.

Whistleblowing

In addition to data gathered by organizational leaders, insight on insider behavior can come from other employees, including whistleblower complaints. It is critical to monitor the action an organization takes when it receives a complaint. What data is collected about the whistleblower hotline? What is the substantiation rate for complaints? A **2020 study of internal whistleblowing systems** found that a 10% increase in whistleblower complaints was associated with a 2% reduction in government fines and a 1% decrease in settlement amounts. What an organization does with internal complaints matters, of course.

Take action now

There is no technology "solution" to manage insider risks. Data, if properly assembled, analyzed, and presented can aid in understanding the risks within the organization. The main lesson in using data analytics for insider risk management is don't wait until there's a problem. If there is room to improve and become more efficient while enhancing compliance, organizations should take action as soon as possible.

Tips for a Successful Analytics Assessment

- Obtain senior management buy-in and communication at outset
- Staff appropriately
- Don't try to force-fit a quantitative methodology
- Evaluate using a three-pronged approach: top-down, bottom-up and industry benchmarking
- Assess for future requirements, not current needs
- Prioritize outcomes and impact
- Don't forget about developing a roadmap for what's next

Cybersecurity Controls: One Step Ahead of Insiders

Wittingly or otherwise, **82% of global cyber incidents** involve the human element. Unfortunately, organizations do not necessarily appreciate the problem of insider risk until something occurs.

In cybersecurity, human insiders form part of an organization's perimeter defense – and are often its most significant vulnerability. From social engineering, to phishing attempts, to negligence and inadvertent mistakes, such as sending sensitive data to an incorrect email address, insiders play a central role in many of the incidents that compromise networks and data.

New situations tilt the balance of risk; recent years have demonstrated just how quickly new scenarios can alter business risk. It's imperative for organizations to analyze changes involving technology and reassess their vulnerabilities and efficacy of controls.

Four Types of Insider Threats in Cyber

Organizations across industries face varying threats as we have explored throughout this paper, but in general four types of cyber insider threats are prevalent:

1. **Sabotage.** An insider perpetrates destructive attacks, causing physical damage to servers or storage media and/or destroying data through malicious programs.
2. **Fraud.** Greed or financial distress may lead an insider to defraud the organization for personal gain. Misusing company funds to pay personal expenses is an example.
3. **Intellectual Property Theft.** Stealing trade secrets may be an act of revenge by a disgruntled employee. An insider may steal IP as part of a plan to set up a competing organization or commit the theft to sell it for financial gain.
4. **Corporate Espionage.** Competitors and other outsiders may entice insiders to provide them sensitive data or products to attain a competitive advantage.

Lifecycle of a Witting Insider Threat:

Motivation

What is the need or objective that persuades the insider to take action? Common examples include financial gain, ideology, grievances, revenge, or having been compromised and coerced into action by an outside party.

The Target

The insider identifies the capability or power they possess by virtue of their role and access within the organization.

The Scheme

The insider develops their plan for exploiting the vulnerability they have identified and leveraging it to achieve their underlying motivation.

Reconnaissance

The insider refines the plan by identifying potential obstacles and weaknesses in their plan. They may conduct surveillance, test controls and safeguards, or even perform rehearsals or dry-runs, making improvements based on feedback achieved.

Action

The insider executes the plan. Based on the underlying motivation, success achieved, and the insider's access, this may conclude the full extent of the insider's threat activity, or the insider may continue to leverage their persistent access to continuously exploit the vulnerability or plan additional threat actions.

Controls to Consider

A fundamental element to implement in cybersecurity is privilege controls. Not all employees require the same level of access to their organization's network drives and data to perform their jobs, so privileges should align with each employee's specific responsibilities. And those controls should be updated as the employee advances, takes on additional responsibilities, or has a change in employment status. The standard rule is that every employee should only have access to the data they need to perform their job function. All other data should be segregated.

Another control is regularly monitoring access, and tracking logins and data downloads. Red flags to watch for include unusual hours and days for logins, logins to unusual applications, increased data downloads, downloads to suspicious locations, and attempts to increase network privileges. Knowing what is "normal" for a given employee or role makes it easier to spot anomalous behavior.

Common methods employees use to steal data are to email it to a personal account, upload files to a personal cloud account or copying information to an external drive. As an example, a lower-level human resources employee might be upset at how a friend

at work was treated, so she downloads personnel files she should not have. In another scenario, a mid-level employee leaving to pursue a job at a competing company takes intellectual property data with him on a thumb drive.

Data loss prevention systems can track data leaving an organization's network according to customized parameters. When data transmissions fall outside those parameters or look abnormal, the systems can alert cybersecurity staff. Computer forensics can determine if a specific user sent or downloaded data in violation of company rules, and some organizations request such checks after an employee is terminated.

Among basic controls, long passwords that are difficult to break are effective in thwarting unauthorized access. The more characters a password has equates to longer time to attempt a brute force attack. Another control is multifactor authentication (MFA). The trend of "bring your own device" (BYOD) for work and personal communications is particularly risky, especially in the era of remote work. The best effective way to make remote work secure from cyber incidents is for the organization to supply the device and configure it for security.

Committing to Cybersecurity

The corporate world has a growing awareness of the need for security, thanks to the number of cyber incidents that occur every year. Commitments to improve cybersecurity are happening slowly, however, because they involve expense and behavior change. Many organizations are reluctant to invest in cybersecurity because they have a mentality that security does not improve the bottom line or they don't sense the immediate need. As a result, some try to make do with as little resourcing as possible, while others view cybersecurity as an area for potential cutbacks.

Insider risks aren't going away, and the impacts will increase in times of economic distress and uncertainty. Making organizations more secure involves a culture supported by the highest levels, spread throughout with continuous training, and budgeting appropriately for tools and resources.

Insider Threat Personas

What does an insider threat look like? Typically, an insider responsible for a cybersecurity incident falls into one of three categories:

COMPLACENT PERSON

Complacency may show up in employees who are indifferent, lazy, over assigned, overqualified or underqualified in their roles. Mislabeling, poor data storage and poor controls increase cybersecurity risks. Convenience and complacency often go hand in hand, such as keeping passwords on a sticky note attached to a user's desk or computer.

COMPROMISED USER

An insider may be coerced or threatened by outsiders into cooperating with a theft or data breach. In these situations, outsiders may try to exploit the insider's weakness or vulnerability, and the insider's behavior may be influenced by personal or family issues such as debt, illness, gambling, or addiction. A compromised insider might feel powerless to resist.

MALICIOUS EMPLOYEE

A malicious insider may seek to exploit or steal to enrich themselves or injure their organization. Disgruntled employees with access to sensitive data and locations can do a great deal of harm if left unmonitored.

Enhancing Controls and Oversight for the Long-Term

Several types of controls can be effective in reducing insider risks. Organizations should take a holistic view of their controls and protocols when considering their sufficiency. But above all, controls will only be effective if they are coordinated in a holistic way. Ensuring red flags are identified and communicated to those charged with managing the risk is the key to an effective program. These controls include:

Inventory Trade Secrets and Proprietary Information

Organizations should take stock of their confidential information and delineate trade secrets and other confidential or mission-critical information. Once identified and inventoried, information that is deemed a trade secret should be marked as such and a steward assigned to ensure the proper handling of the trade secret.

Employment Agreements

All company employees should execute non-disclosure agreements in which they agree to not share confidential information. Similarly, the company's code of business conduct and employee handbook should also cover confidentiality requirements and employees' obligations to raise incidents of breach of confidentiality or other proprietary data exfiltration or loss.

Physical Controls

Knowing whether someone is in the building at any given time can help to reduce opportunities for insider crime as well as provide critical information as to the whereabouts of personnel during crises such as fires, natural disasters or active shooter incidents. Robust physical controls also limit access to sensitive files or areas, such as server rooms. Organizations who fail to recognize physical vulnerabilities expose themselves to unnecessary risk of unauthorized access to important data and other assets, not only by insiders but also by third-party vendors such as maintenance personnel or after-hours cleaning services.

Personnel Controls

Because people represent the greatest vulnerability to any security program, organizations should have comprehensive procedures for conducting background checks and rescreening employees as they advance in the organization. Substance abuse policies as part of a code of conduct can assist in addressing anomalies in behavior that could result in criminal insider behavior. An employee assistance or confidential hotlines for individuals to seek help for themselves or others, or to share concerns or even report wrongdoing, are also important tools which help to bolster a better security infrastructure while reinforcing a strong employee focused culture.

Training

Upon employment, all colleagues should be trained regarding the nature of the company's trade secrets and the methods to and their responsibilities for protecting them. Training should include not only trade secret-specific training, but also encompass computer use, physical security measures leveraged by the company, and how to raise concerns via the firm's integrity hotline or other methods used by the company to identify and address concerns. Employees with particularly sensitive responsibilities should receive supplemental training as appropriate. All training should be recurring and continually updated to reflect changes in the business and the intellectual property that comprises trade secrets.

> *"An insider risk program can be scaled up (or down) and flexed depending on the size, risk profile and available resources of the organization. No two organizations are the same. Even for the smallest organizations, an assessment of the insider risk and the implementation of key controls will help mitigate the risk without requiring significant resources.*

Policies and Procedures for Handling Trade Secrets

Policies and procedures for trade secrets and confidential information should be developed to govern the access, use, and steps to protect the confidentiality of the trade secrets. Policies should include: a "need-to-know basis" for accessing trade secrets; restrictions on the sharing or transmittal of trade secret information; an affirmative duty for all employees to maintain the confidentiality of trade secrets; and processes for safe-guarding trade secrets such as clean desk policies.

Cyber Controls

Privilege management is a foundational form of cyber control. Not every employee needs to have administrator-level access to systems, networks, and data drives. Other forms of cyber controls that are essential are multi-factor authentication and long, complex passwords, which are difficult to hack. Systems and software that flag or identify potential unauthorized access or downloads provide necessary security for sensitive data. Critically, the people assessing alerts on the systems need to be aware of what insider activity could look like or they will miss important potential leads. Awareness for those involved in identifying and managing insider risks is vital.

Financial Controls

Check and balances, and the four eyes principle in approving disbursements, are valuable financial controls. Spot audits and/or random security checks can enhance these controls and make it harder for bad actors to evade detection.

Leadership Controls

Case after case has shown the biggest impact from insider threats can come from executives who have access to sensitive data and accounts. Direct reports and junior staff are less likely to question or report suspicious executive behavior. A successful strategy to minimize executive malfeasance is consistent and repeated evaluation, particularly as executives advance through their organizations. Periodic screening of C-suite personnel should occur in the same way that employees at other levels of the business undergo screenings. Anonymous feedback through a confidential hotline may prove invaluable to organizations in identifying problematic behavior, while addressing employees' fear of retaliation for stepping up and reporting it.

Exit Controls

For any exiting employee, there should be a comprehensive checklist to ensure all devices, credentials and access cards have been collected and deactivated. When high level leaders or those with access to valuable company intellectual property leave, an analysis may be considered for any exfiltration of data from the company's networks or systems, as well as a review of more manual methods such as printer logs. Organizations should also consider conducting exit interviews, both as a way to remind those leaving of their legal duties, and as a method of collecting valuable insights as to what is going on inside the organization.

It's also important to keep an eye on the "Outside Insider."

The past two years have given way to large-scale remote or hybrid work for most organizations. While the flexibility is largely seen as a benefit for most organizations, it has proven to come with risk: lax internal controls, oversight and cultural cohesion all contribute to an environment where insider risk can flourish. Employees who used to be internal 100% of the time are now operating in their home or remote offices. Organizations must be regularly testing and tuning their controls and systems to balance the need for ease of access with the ability to safeguard the crown jewels.

Assessing controls and setting up frameworks can be daunting, but organizations can begin by taking stock of what's at their fingertips. Provided below are checklists to consider and questions to ask to help jumpstart your program today.

Questions to Ask: Insider Risks Controls Cheat Sheet

Getting Started

- **Do you have sensitive IP?**
- **Would the loss of your IP** threaten the future of your business?
- **Is your business related to emergent new technologies** such as quantum computing, AI, fusion technology, bio pharma?
- **Are you or have you recently gone through** a period of significant change (such as growth, merger, takeover, contraction)?
- **Do you have or might you secure** government contracts?
- **Have you had any insider cases** that you know of, such as fraud, IP theft, theft, sabotage of facilities or data, or have you had any "bad leavers"?
- **Are you aware of any cyber-attacks** against your business?

Governance and Accountability

- **Who is accountable** for insider risk in your organization?
- **Do you have a program** to receive, escalate and report concerns raised internally?
- **What channels** do you use to receive concerns, beyond a whistleblowing hotline?
- **How do your organization's leaders** promote a culture of speaking up?
- **What training does your organization offer** on its code of conduct and to facilitate speaking up?
- **Do you regularly revisit and update** your code of conduct?
- **What policies, procedures and controls** does your organization use to drive responsiveness to concerns and accountability?
- **How does your organization measure** the effectiveness of its whistleblowing program?
- **How often does your organization test** its whistleblowing program?

Risk Mitigation and Incident Response

- **Does your organization** have an incident response process?
- **Do you have controls** to ensure that assets could not be acquired, used or disposed to commit or conceal misconduct?
- **Have you assessed** how the corporate culture and control environment impacted the occurrence and detection of the incident or misconduct?
- **Have you communicated** visible and clear policies, standards and procedures across the organization?
- **Are your policies** appropriately and effectively communicated to strategic third parties, such as joint venture partners, agents, suppliers, and customers?
- **Do you regularly evaluate** how information and communication issues may impact the occurrence and detection of the misconduct?
- **Did the process provide** for taking steps to remedy harm and avoid future misconduct? Did the organization take those steps?

Our Contributors

David Burroughs
Partner
dburroughs@stoneturn.com
+1 212 430 3454

Joshua Dennis
Partner
jdennis@stoneturn.com
+1 617 570 3789

Nathan Fisher
Managing Director
nfisher@stoneturn.com
+1 415 848 7613

Daron Hartvigsen
Managing Director
dhartvigsen@stoneturn.com
+1 202 609 7847

David Holley
Partner
dholley@stoneturn.com
+1 617 570 3798

Sarah Keeling
Partner
skeeling@stoneturn.com
+44 (0)20 7427 0417

Richard Mackintosh
Senior Adviser
rmackintosh@stoneturn.com
+44 (0)7814 489970

Mike Roos
Partner
mroos@stoneturn.com
+27 7987 49997

Luke Tenery
Partner
ltenery@stoneturn.com
+1 312 775 1210

Brad Wilson
Managing Partner,
Chief Executive Officer
bwilson@stoneturn.com
+1 617 570 3790

Special thanks to Tracey Groves, Ray Manna and Emilia Drozda

Leaving no stone unturned.

StoneTurn, a global advisory firm, assists companies, their counsel and government agencies on regulatory, risk and compliance issues, investigations and business disputes. We serve our clients from 15+ global offices across five continents.

StoneTurn.com

StoneTurn