GARP Risk Institute

BUILDING OPERATIONAL RESILIENCE

The Critical Need to Learn from Failure

Foreword

By anyone's standards, the scale of prudential and conduct-related failures in the financial system over the past decade has been staggering. The failures have shaped the regulatory response and influenced developments in risk management. What's more, they provide fertile ground for learning.

This three-article series – written by Jo Paisley, Co-President, GARP Risk Institute; Dr. Mike Humphrey, former Head of Security, UK National Crime Agency; and Caroline Stroud and Emma Rachmaninov, Partners, and Holly Insley, Senior Associate, of Freshfields Bruckhaus Deringer LLP – demonstrates, from different points of view, that the lessons that arise out of mistakes can be turned into essential building blocks of an organization's resilience.

Of course, the past may not be a good guide to the scale and nature of potential losses in the future. Since the threat landscape is constantly evolving, it's not enough to have learned lessons from the past - learning needs to be forward-looking, too.

Increased digitalization and changes in the technology that supports it, for example, raise new security and technology risks. Increased reliance on outsourcing – for example, via cloud computing, open banking and fintech partnerships – further raises firms' vulnerabilities, particularly to third-party vendor risk. Greater regulatory safeguards on data privacy and protection raise the prospect of larger fines and increased reputational risk in the case of breaches.

Moreover, the consequences of operational outages and failures are changing: firms that display any sort of IT weakness themselves become targets for fraudsters. As a consequence of all of these issues, the likelihood and potential costs of operational failures are rising.

Regulators are, in turn, changing their approach. Rather than focusing on financial resilience (as they did in the wake of the financial crisis), they are now requiring firms to prove their operational resilience. Indeed, firms are being asked to plan on the basis that they will experience some sort of failure. Managing this rapid and disruptive change is becoming a key priority for firms, clients, regulators and politicians.

So, if we can expect more frequent operational incidents or failures at firms, with potentially more substantial and unpredictable impacts on both individual firms and the financial system, is it time to start thinking about failure in a different and more proactive way?

Each of the three articles in this series provides a unique perspective on learning from failure.

Insights from Across Industries

Not all failures are the same. Even so, some industries facing similar types of failures (for example, resulting in loss of life) have proven better than others at hard-wiring learning from failure into their risk management. Industries such as aviation and health care offer valuable insights into the value of both collecting and learning from good-quality incidents data, as well as the critical roles of culture, organizational and regulatory structures.

Creating Effective Incident Reporting

Collecting comprehensive incident data is challenging. People find it difficult to admit when things go wrong, and even making reporting mandatory doesn't always work. Drawing on his own original research, Dr. Mike Humphrey explores the critical success factors for building an effective incident reporting system. Good-quality data on accidents and near misses are vital to our ability to understand the root causes of failures, their frequency and the threat landscape.

The Critical Connection Between Culture and Misconduct Failures

Even with good-quality data, it takes the right business culture and openness to learning to make a difference. Misconduct risk is one of the most significant areas of cultural failure over the past 10 years. Lawyers at Freshfields Bruckhaus Deringer provide an external perspective on misconduct cases in banks over the past decade, examining the common themes.

Insights from Across Industries

By Jo Paisley, Co-President, GARP Risk Institute

Things will go wrong – a key issue for operational resilience is how we respond when they do. To be able to respond well to operational failures requires insight, preparation and practice, as well as an ability to learn from errors. This is easier in a culture where staff acknowledge mistakes, there is an effective system for staff to record them, and the organization is open to learning from them.

In a joint 2018 discussion paper, three UK regulators (the Bank of England, the Prudential Regulation Authority and the Financial Conduct Authority) noted that the financial system needs to be able to absorb shocks, rather than contribute to them. "The financial sector needs an approach to operational risk management that includes preventative measures and the capabilities – in terms of people, processes and organizational culture – to adapt and recover when things go wrong," the regulators elaborated.

It's helpful to recognize that there are different types of failure that warrant different types of responses. In a paper Dr. Amy Edmondson wrote for the Harvard Business Review, she cites three broad categories of failure: preventable, complexity-related and intelligent.

- *Preventable failures in predictable operations* are "bad." These involve deviations from routine procedures in, say, a manufacturing process. Some firms have built continual learning into their production processes to ensure continuous improvement.

- *Unavoidable failures in complex systems* arise when there is a high level of uncertainty in the work environment, for example when triaging patients in a hospital emergency room or running a fast-growing start-up. Even minor process failures in these circumstances can - in combination - lead to catastrophic failures. As she notes, "To consider them bad is not just a misunderstanding of how complex systems work; it is counterproductive." Small process failures are inevitable, but avoiding consequential failures means rapidly identifying and correcting them.

- *Intelligent failures at the frontier*, in contrast, can be considered as 'good,' as they can help firms discover new drugs, new products and new ways of doing things that provide a competitive edge. One of the interesting features of today's financial services industry is the clash of cultures between the 'fail fast, learn fast' mentality of innovative fintechs and the more traditional approach of 'avoid failure, and then look for who to blame when things go wrong.'

Disaster Prevention Challenges

From an operational resilience point of view, paying attention to preventable (even quite minor) failings makes a lot of sense, as these can in combination trigger a catastrophic process failure. Evidence of this has been found in several public enquiries investigating the causes of various disasters.

Consider, for example, the UK, enquiries into the Bradford Football Club fire, the sinking of the Herald of Free Enterprise and the Kings Cross Underground fire. What did all three of these disasters have in common? All were the culmination of a number of smaller events, including design and management deficiencies.

Each disaster could have been averted – or, at the very least, mitigated – if the smaller trigger events had been identified, reported and tackled. The general lesson is that an industry that does not learn from past failures is doomed to repeat them.

In the case of the enquiry into the Bradford fire, the report highlighted that many of the safety-related recommendations were in fact identified in previous reports into other football-related disasters, but had not been put in place. In other words, the industry did not learn from previous failures.

The 1987 sinking of the Herald of Free Enterprise ferry, which resulted in the loss of 188 lives, was another classic example of not learning from previous minor incidents. Prior to the disaster, several minor incidents had been noted by members of the ferry's crew – but were either not officially reported or dismissed by management as 'exaggerations.' In the ensuing Sheen investigation, management failure was cited as a prime reason for the disaster.

This practice of ignoring, dismissing or marginalizing previous related incidents is part of a larger, even more troubling pattern of behaviour. In the wake of a major disaster, people take much more care, their attitude to risk changes and policies and processes are introduced to prevent reoccurrence. However, these efforts can soon dissipate, allowing things to revert to a norm in which trigger events were missed, ignored or not reported properly.

So, even if we know it makes sense to learn from failure, we can see it's hard.

How Different Industries Learn from Failure

In the context of aircraft safety, aviation is one of the most advanced industries to embrace learning from failures. As we will see, other industries have tried to learn from them.

Aviation

Planes have two black boxes: one records the instructions that are sent to all on-board electronic systems; the other is a voice recorder in the cockpit.

These boxes provide a rich source of data for independent investigators to study in the event of accidents and near misses. Lessons are learned from these incidents for the good of the industry – a system that "Black Box Thinking" author Matthew Syed has called an 'open loop.'

A 'no-blame culture' has been institutionalized in this industry, because any evidence compiled by accident investigators is inadmissible in court. This provides the incentive for individuals to speak up. Syed refers to this mindset and approach as 'black box thinking.'

Airlines must implement recommendations, and the data underlying the report should be made available to all pilots. This transparency aids learning across other airlines.

Of course, if an investigation found that a person had been negligent, then blame and punishment would be justified. But the starting point is not to seek out who is to blame – it is to learn the lessons.

The key factors at work are the source of data on failures and near misses, independent investigators and sharing lessons across the industry. Cultural factors – such as breaking down hierarchies and encouraging people to speak up – are also critical. But it has taken around a decade to get to this state of maturity.

Health Care

Other sectors, such as health care, have tried to learn from this approach. For example, the UK's National Health Service (NHS) has taken steps to ensure that learning from adverse events is built into their culture and operations. They've noted that when things go wrong, the response has often been to identify who to blame—but the focus of investigations should, rather, be the events immediately preceding a failure.

The NHS recognizes that failure can sometimes be the result of negligent or criminal behaviour, but that it is more often the result of a huge number of factors that are way beyond the remit of one individual. It is the *system*, rather, that needs analysis.

Similar to Edmondson's distinction between preventable and unavoidable failures, the NHS distinguishes between active failures and latent conditions. It defines *active failures as* 'unsafe acts' (typically short-lived and often unpredictable) committed by those working at the sharp end of a system. *Latent conditions,* in contrast, can develop over time and lie dormant before combining with other factors or active failures to breach a system's safety defences. They are long-lived and, unlike many active failures, can be identified and removed before they cause an adverse event.

By examining the latent conditions at work, it is possible to remove these factors and help reduce the likelihood of an extreme adverse outcome.

In the early part of this century, the NHS placed an emphasis on four key areas: (1) a unified mechanism for reporting and analysis when things go wrong; (2) a more open culture in which errors or service failures can be reported and discussed; (3) mechanisms for ensuring that, where lessons are identified, the necessary changes are put into practice; and (4) a much wider appreciation of the value of the system approach in preventing, analyzing and learning from errors.

Over the past six years, public failures have forced the NHS to reconsider its approach to failure. For example, the 2013 Berwick review set out the key lessons learned from some failures at some UK hospitals, most notably urging the NHS to embrace wholeheartedly an ethic of learning. The Secretary of State for Health subsequently announced, in July 2015, that the NHS would set up a new independent investigation branch, modelled on the Air Accident Investigation Branch used in the aviation industry.

The Healthcare Safety Investigation Branch was launched in April 2017. This body investigates up to 30 safety incidents a year, placing an emphasis on learning rather than blaming. The lessons can then be shared across hospitals to try to make sure that mistakes aren't repeated and that the system is more resilient.

The health care industry has certainly taken a more robust approach, but only time will tell if it is as effective as the aviation plan-of-attack for learning from failure.

Armed forces

The US Army has also developed an approach that aims to learn the lessons from failure. The US Army's After

Action Review (AAR) process involves a systematic debriefing after every mission, project, or critical activity. This process is framed by four simple questions:

- What did we set out to do?
- What actually happened?
- Why did it happen?
- What do we do next time? (Which activities do we sustain, and which do we improve?)

Lessons move through the chain of command and are shared through sanctioned websites. Then the results are codified by the Center for Army Lessons Learned (CALL).

Lessons for Financial Firms

So, how applicable is this for financial services? After all, lives are not typically at risk and errors are not always as immediately obvious as a plane crash; indeed, sometimes they take many years to come to light.

David Blake and Matthew Roy recently argued that insights from the learning culture in aviation were highly relevant to the pension industry. In their report, Bringing Black Box Thinking to the Pensions Industry, they set out their argument for how 'black box thinking' could be applied to trustees of defined benefit (DB) pension schemes.

After interviewing UK DB pensions leaders and experts, they found evidence of a 'closed loop' mindset, including not setting strong measurable targets; inertia in decision making; herding behaviour; shifting goal posts; failing to take ownership of mistakes; and blaming others.

Blake and Roy also argue that organizations must create structures to mitigate human cognitive biases. The key is to have a *mindset* that constantly questions the status quo and seeks improvement, and they suggest various ways to break "group think" and introduce better measurement.

The pensions regulator, the authors contend, should be a clearing house for post-mortems of failed schemes - akin to the role that accident investigators have in aviation. If this role were to be set up, they argue it could help reduce the likelihood of common mistakes (such as, inappropriate hedging) being made across schemes.

While we can encourage individual banks, insurance companies and asset managers to embrace a learning culture, should the industry go further and create structures where there is more sharing of information on failure across the industry for the good of all firms? Clearly, this would need to be in areas where there is no danger of firms being perceived as colluding. What's more, for firms to want to share data, it would have to be in areas that are not regarded as sources of competitive advantage.

One such area is cybersecurity. Initiatives in the UK, such as the Cyber Security Information Sharing Partnership (CiSP), aim to improve the sharing of cybersecurity incident information at a national level. However, it is commonly believed that there is significant under-reporting of incidents within firms. Without improvement at this lower level, national incident sharing initiatives cannot become as effective or institutionalized as in the aviation industry.

Parting Thoughts

Perhaps it's not just managers who think about failures in the wrong way – maybe we all do: firms, regulators, politicians and the public. The knee-jerk reaction of asking 'who is to blame?' is counterproductive.

Equally, it is a challenge to achieve the right balance between a no-blame culture and instilling a strong sense of accountability.

In the UK, the Treasury Committee's November 2018 inquiry into IT failures in the financial services sector provides a good example of the obstacles standing in the way of implementing no-blame cultures. Citing an "astonishing" number of recent technology failures Nicky Morgan, a Member of Parliament (MP) and the chair of the Treasury Committee, said "Millions of customers have been affected by the uncertainty and disruption caused by failures of banking IT systems. Measly apologies and hollow words from financial services institutions will not suffice when consumers aren't able to access their own money and face delays in paying bills."

It's not surprising that there is anger over these incidents. However, rather than start with the tone of blame, perhaps a more productive approach is to ask *why* there is a growing number of incidents. What does it signify and what are the lessons? Are these incidents symptoms of preventable failures in predictable operations or unavoidable failures in complex systems?

Looking across industries, the following ingredients appear to be required for effectively embedding learning from failure: a no-blame culture to encourage people to speak up; effective incident reporting/data capture; and a culture or mindset that embraces learning from failure.

For the learnings to be spread across an industry, there is the further need for an independent body to analyze failures, understand the key lessons and promote lessons learned. It is probably easier when lives are at risk, because this raises the stakes in a way that gets our attention.

In a recent speech, Sam Woods, CEO of the Prudential Regulation Authority (PRA) recognized the distinction between topics where the incentives of firms and the regulator can be aligned and those where they are not.

Examples of the former are cyber risk and operational resilience, where firms and the regulator should be on the same side, sharing information. Under those scenarios, the PRA will act as a 'good cop.' In other areas, such as ring-fencing, accountability, pay and internal models, the PRA will tend to be 'bad cop.'

Undoubtedly, there are areas in between. But the 'good cop' role sounds similar to an industry mechanism for learning from failure. This raises some interesting, highly relevant questions:

- Can financial institutions and regulators work jointly to aggregate data on failures/near misses and share best practices?
- Can a regulator simultaneously be a good cop and a bad cop? Do they have the right resources/skills base to be able to do this?
- Might the possibility of blame and the bad cop role be enough to put firms off reporting honest mistakes that might help the sector learn from failures?
- Would learning from common failures in financial services be better served through the creation of an independent body, similar to the approach in health care?

Although it isn't clear what the role of the regulator should be, nor the best organizational structure to achieve this, it is clear that good-quality data on failures and near misses are the bedrock.

About the Author

Jo Paisley, Co-President, GARP Risk Institute, served as the Global Head of Stress Testing at HSBC from 2015-17, and as a stress testing advisor at two other UK banks. As the Director of the Supervisory Risk Specialists Division at the Prudential Regulation Authority, she was also intimately involved in the design and execution of the UK's first concurrent stress test in 2014.

Creating Effective Incident Reporting

By Dr. Mike Humphrey, former Head of Security, UK National Crime Agency

Effective reporting of security incidents is vital. However, today, many incidents still go unreported.

What are the barriers to good-quality reporting and how can institutions overcome these? The lessons are broad and are not simply for information security; indeed, they apply to any areas where individuals must report when things go wrong.

The Case for Good-Quality Incident Data

Security professionals and academics believe that the true scale of information security incidents is unknown due to under-reporting. For example, at a conference of chief information security officers (CISOs) in July 2017, members of the audience were asked the following question: "How confident are you that your staff know how to report strange activity or a potential security incident?" Only 22% said they were very confident, while 50% were fairly confident and 28% had low confidence.

This is a real problem for risk management, which relies on accurate and comprehensive empirical incident report data to make informed risk assessment and risk management judgements. When such data are partial, decisions related to resourcing and expenditure may be focussed on the wrong issues. Moreover, there is a danger that incidents that are reported are given higher prominence, simply because that is the only available information.

For example, electronically gathered incident reports from audit logs or intrusion detection systems (IDS) are automatically generated and are therefore more readily visible. Since they are tangible, these incident logs are often used to justify risk-based decisions. However, without a wider perspective of the true nature of the type and volume of incidents and near misses, this may give undue prominence to the electronic log indicators while masking the real threat.

This perceived lack of data could also undermine efforts to share incident and threat information between communities. While providing some basis for risk assessment and management, incidents that are reported, may contain unknown biases that could affect any such assessments. If organizations have little to share, then there is little to gain.

But there are also increasing pressures from regulators in the form of mandatory reporting of security incidents (e.g., via GDPR legislation). So, for both reputational and regulatory reasons, firms need to know what is happening to their data assets and the possible security incidents that could lead to breaches. For these tasks, they need staff to report incidents. Indeed, when assessing risk, information security incidents that rely upon staff to report are equally important as electronically-gathered incident reports.

Why Don't People Report Incidents?

There are a host of reasons people don't report incidents. For starters, if you expect to be blamed for making an error, or you expect that no one will notice, then there is an incentive to simply not report it.

But there are a host of other reasons for not reporting. Often people don't think an incident is serious enough to bother reporting. This was confirmed by research by Plews and Ogan, who also found that if a mistake is corrected for the future, individuals often then decided that they don't need to report it.

Making incident reporting mandatory doesn't always work. For example, Soderburg observed that patient safety incidents at health care facilities were not being reported, despite it being a mandatory requirement.

Rank can affect reporting too. Indeed, research has shown that doctors are far less likely to report incidents than nurses.

Another study found that new recruits were treated differently than existing employees, with fewer incidents made by new staff reported as security incidents. Without a central record of these incidents, it is harder to learn lessons and improve training for new recruits. Moreover, there's evidence that users often interpret formal work requirements in a local way, and then play out the processes to suit the informal element of their environment.

The complexity of a system can be a key factor inhibiting reporting. For example, if you can't understand how the whole system works, then you are unlikely to understand the significance of a local failure. So, you may not see the need to report – or you may not understand what needs to be reported.

Overcoming Barriers: Critical Success Factors

Most organizations have considerable avenues open for staff to report incidents, including forms, emails, intranet, phone lines and direct communication with line managers. But are these channels fit for purpose?

An effective system of reporting needs to factor in human behaviours and their attitude to risk. Through a series of studies with information security professionals, our research identified four critical success factors (CSFS) for effective incident reporting:

- Recognition by senior management that incidents will happen, and that employees must play a full and active part in the incident management process
- Easy processes for creating and submitting a report. If reporting incidents is difficult, individuals will be less likely to submit them. This may particularly affect the reporting of near misses
- Rapid, useful, accessible and intelligible feedback to the reporting community
- Incident analysis that considers root causes and wider systems and processes, not just the initial impact assessment

These factors complement the five stages in the British Standard ISO/IEC 27035 approach to managing incidents.

Parting Thoughts

Incidents, like accidents, will happen. They are often preventable, but still occur. Accepting your organization will inevitably be, or has already been, subject to a security incident, the key thing is to make sure you are ready.

Keep in mind that you have to worry about third-party vendors as well as your internal data and systems. If one of your key suppliers gets hacked, your company's sensitive data could very well be compromised. In any outsourcing arrangement, your organization is still responsible for the privacy and security of its data (including customer information) and still must report incidents.

FOUNDATIONAL QUESTIONS

For Practitioners

- Do you have a clear and well-understood incident reporting system?
- Is it supported - and, importantly, also followed - by senior management?
- Does your company have a blame culture or a learning culture?
- Are those who report incidents supported to demonstrate to others that it is a learning culture?
- Do you have a tested plan to put in place when a breach occurs?
- Do you have prepared media lines to answer questions in the immediate aftermath of an incident and to hold the fort until more facts are known?

For Regulators

- Is the intention to punish or improve companies subject to a data breach?
- Do you encourage learning?
- Do you have rules in place to ensure that organizations that commit infractions are not just punished but actually learn from their mistakes?
- Do you focus on the overall process of incident reporting, as opposed to the incident that was the subject of regulatory intervention?

About the Author

Dr. Mike Humphrey was a police officer for 30 years, working in a variety of operational, research and planning, and IT roles, including being Head of Security at the UK National Crime Agency. He is a fellow of the Institute of Information Security Professionals and an elected member of the UK Information Assurance Advisory Council's (IAAC) management committee.

The Critical Connection Between Culture and Misconduct Failures

By Caroline Stroud and Emma Rachmaninov, Partners, and Holly Insley, Senior Associate, of Freshfields Bruckhaus Deringer LLP

Misconduct is one of the most significant symptoms of cultural failure and examples of it have been rife in the financial services sector over the past 10 years. What are its common causes and potential lessons?

From a regulatory perspective, the belief that culture and conduct risk are inextricably linked has been made clear. The UK's Financial Conduct Authority has stated that culture is a priority area and has made no secret of its view that the conduct failings of recent years have been driven by the culture of financial services firms. The Financial Stability Board, moreover, recently published a toolkit on mitigating misconduct risk including cultural drivers of misconduct.

William Dudley, former President and CEO of the Federal Reserve Bank of New York, captured the significance of misconduct during a banking culture panel he participated in last year. "I think there's a pretty broad acceptance of the notion that regulation and compliance only takes you so far, and that bad conduct really does undermine the effectiveness of the financial system, because it basically reduces trust," Dudley said. "You need a good regulatory regime supplemented by various good conduct and culture in the organizations."

Whether or not an organization is subject to the expectations and scrutiny of a regulator, there is widespread acceptance that achieving the 'right' corporate culture can go a long way toward helping to manage risk. A core part of risk management is developing a corporate culture where expectations as to behaviour are clear, appropriate behaviour is rewarded (and inappropriate behaviour punished) and employees are empowered to speak up if they spot an issue.

Lessons Learned from Experience

Faced with the need to focus on culture, an obvious question is where to start. There is a rich body of academic and regulatory material on culture, and a range of views on how best to measure and influence culture in the workplace. Given that culture is a behavioural set of norms, some firms are looking to behavioural science to predict and measure cultural drivers as part of their assurance processes.

As lawyers at an international law firm, we have a wealth of experience in investigations and have seen first-hand the consequences of misconduct, including, for example, regulatory breaches and boardroom disputes.

Drawing upon our experience of investigations across a range of sectors and geographies, we recently carried out an empirical analysis of the underlying cultural factors that may have allowed misconduct to take place, whether as a direct cause or by creating an environment in which misconduct was able to flourish.

Cultural Drivers of Misconduct

We identified 12 cultural factors present in environments in which misconduct or other problems occurred. The 12 factors identified through our research are grouped into three categories, depending on the frequency with which they arose.

There are many examples of each of these factors arising in practice and there is frequently a degree of overlap between them. Not all of these factors can – or should, necessarily – be eliminated. Instead, the focus should be on identifying whether they are present, considering what risks they may pose and deciding what steps could be taken to reduce those risks.

Let's now focus on 3 of the 12 factors that most commonly arose: strong personalities; lack of speak-up culture; and highly technical areas. What's their impact, and what actions can be taken to reduce the risk that they pose?

Strong Personalities

The presence of strong personalities within a business is almost inevitable. Successful leaders tend – and often need – to have strong personalities. This can bring with it many positives, such as the ability to drive change, motivate and inspire.

The potential risky behaviour that we have seen arising around strong personalities includes excessive deference from junior staff, and a lack of challenge or scrutiny from the oversight and control functions. (When an individual has handpicked subordinates, who see their loyalty as being to their manager rather than to the organization, the former can be particularly problematic.)

TOP CULTURAL FACTORS IN MISCONDUCT

Inadequate challenge and scrutiny can often arise in smaller overseas offices. In such locations, distance from head office can have an impact on the degree of oversight that is exercised and the extent to which local employees feel there is anything they can do to raise their concerns.

Closer to home, these obstacles may arise in businesses where a particular individual has had a huge amount of success and is highly respected, to the extent that no-one contemplates that they might be doing something wrong. Consequently, red flags may be overlooked.

Alternatively, employees may feel that very charismatic, respected and successful senior people (particularly those who have a close relationship with management) are untouchable. Indeed, there may be a 'culture of fear' or 'cult of personality' around such people – or a belief that concerns will not be taken seriously, even if they are raised.

The culture of fear can also impact the risks that team members are prepared to take. We have seen examples of a domineering personality who focusses on the business outcome he or she wants to achieve, and then leaves others to work out how to achieve it. The fear of failing to meet that challenge may then lead more junior employees to take inappropriate risks to achieve results.

Where there is a strong personality driving teams to achieve results, the importance of a strong second line of defense is heightened. However, there may be significant pressure on legal and compliance not to stand in the way of business results, and executives in the second line may be pushed to answer a very narrow question ("Is it legal?"), rather than stepping back to ask whether something is appropriate or gives rise to other concerns.

Given that the presence of strong personalities in the business world is inevitable, the challenge for companies is to identify where their own strong personalities sit; be aware of the risks that can be created by those strong personalities; and think about how to manage the risks. This may require a combination of robust challenge or oversight from other strong personalities; a strong second line of defence; proper appraisal and development of strong personalities as they rise up the corporate ladder; and a strong speak-up culture, with routes for reporting and escalation that allow employees

to raise their concerns anonymously and/or to bypass any perceived allies of the strong personality.

When evaluating an organization's governance structures, consideration must be given to both the roles in the structure and the individuals who fill them. This is crucial to governance effectiveness.

Speak-Up Culture

Unfortunately, "whistleblowing" does appear to have an image problem – a lot of the headlines around whistleblowing are either framed in a relatively negative light, or suggest that it is an act with significant consequences.

Concerns that blowing the whistle may result in a formal investigation and the involvement of legal and compliance may be off-putting. Alternatively, employees may be mindful of incidences they have seen of whistleblowing being "weaponized" – for example, being used cynically to attack (potentially legitimate) redundancy or performance management exercises and increase a departing employee's negotiating leverage. This image problem can lead to a real reluctance to raise concerns.

Fear of negative consequences may also be a significant factor in generating a reluctance by employees to raise concerns.

In a survey carried out by Freshfields of 2,500 managers across the US, Europe and Asia, almost one in five respondents said that they thought the average employee would expect to be treated less favorably if they blew the whistle. Moreover, 55% of respondents thought that concerns about damage to reputation and career prospects would prevent whistleblowing in their organization. The negative consequences feared by whistleblowers may often be more perception than reality - but in either case, the impact on speak-up culture is significant.

Trying to strengthen speak-up culture is a focus for many organizations. They appreciate the importance of issues being brought to their attention early – and, ideally, being flagged to them directly. However, transforming this aspect of an organization's culture can be a slow process, and the harm done by whistleblowers who feel ignored or neglected can be extensive.

In many cases, whistleblowers may believe incorrectly that their concerns have been ignored (simply because they are not told otherwise), so improving feedback processes can be an important tool in trying to overcome the 'futility' factor.

Organizations may need to think not just about 'speak up' but also 'listen up' – for example, training managers on what to do if employees raise concerns with them, so that they respond appropriately. Indeed, it's helpful to encourage managers (especially those who are viewed as strong personalities) to demonstrate openness and responsiveness to employees who raise concerns. This can be made part of the appraisal process – to really test whether they are demonstrating the required behaviour.

Other options include rewarding employees who have spoken up – either through financial rewards, recognition in their appraisals or even just a simple "thank you" from senior management.

Striking the right balance in relation to feedback is difficult. The issues raised by a whistleblower may be sensitive, and, in some cases, could be the subject of regulatory or even criminal proceedings. What's more, confidentiality is a requirement in certain jurisdictions, and disclosing details of the outcome of an investigation could involve divulging confidential or business-sensitive information.

For all of these reasons, businesses are typically unable or unwilling to recognize "compliance champions" publicly. However, even a high-level response – an acknowledgement of receipt, a confirmation that an investigation has been or will be undertaken, or an expression of thanks for raising the issue – may go a long way to overcoming the perception that speaking up is a pointless exercise.

Highly Technical Areas

As with strong personalities, it is inevitable that some businesses will have areas that are highly technical. This is not, intrinsically, a problem.

However, the risk that can arise is that if, say, a particular product or business is extremely technical, only a few individuals will be able to understand it fully. This, in turn, can mean that problems are harder to spot.

In the course of our investigations work, we have seen examples of products having been developed that were so complex that the risk committee members who were responsible for approving them did not fully understand the overall product. (While particular members may have understood aspects of the product, there was no individual who could step back and understand the whole.)

In another case, the only individual on the risk committee who understood the product completely had also been involved in its design and had a financial interest in its success, giving rise to a conflict of interest.

Where something is highly technical, there is also a question around the level of delegation that may be

appropriate – as well as who should be responsible for seeking the necessary legal or compliance sign-off.

Junior employees who are tasked with seeking legal advice on a complex product or strategy, may lack a thorough understanding of it. In turn, they may not ask the correct questions of the legal team. Combined with, say, a failure by the legal team to probe further and to ensure that they fully appreciate the context, such inadequacies could result in failure to identify a major regulatory breach.

Eliminating complexity is unlikely to be a practical answer to this potential risk factor, so businesses need to consider what else they can do to manage the risk created by highly-technical areas. This might include, for example, giving thought to whether the risk committee or compliance team is staffed by individuals with sufficient technical expertise - and whether those with the technical expertise also need training on the wider regulatory and reputational considerations.

Organizations can also seek to ensure that the importance of asking questions is understood and accepted. When an area needs more explanation, senior managers should take the lead in saying "I don't understand" – and should encourage all of their team members to do the same.

Where Next?

It is incredibly important to continue to learn lessons from the problems that arise, while simultaneously thinking about everyday steps that can be taken to manage the sources of risk that have been identified.

'Lessons learned' exercises tend to focus on one particular issue, instead of looking holistically across a range of issues. The tendency in the aftermath of a crisis is to focus on the immediate conduct and systems and controls issues, rather than the impact of the corporate cultural environment in which the problems occurred.

Standing back and looking holistically at the organization's recent (and more historic) experience is likely to be more culturally revealing. This exercise may yield factors like the 12 cited earlier in this article, offering valuable data points to look at in developing culture in a practical and meaningful way.

It is important to remember that corporate cultures are not always simply 'good' or 'bad' – particular features can have both positive and negative consequences. For example, collaborative and supportive environments may be rewarding to work in, but also make individuals reluctant to challenge others or have difficult conversations with underperformers who make mistakes and expose the organization to regulatory risks.

The key for organizations is to identify the risks or vulnerabilities arising from their own corporate culture and to think in practical ways about how to address those.

Having identified their list, as they move toward managing risk, firms can then ask themselves important questions at all levels, from the board to middle management. For example, we have a whistleblowing policy and a hotline, but what do our employees really feel about whistleblowing? We know we have a strong personality in this area of the business, so who is the counter to that person? From a risk and compliance perspective, who really understands the technical aspects of the business and can provide the right scrutiny?

Using past experience to think about culture, and to ask the important questions, can play a vital role in developing a culture-focused risk management strategy.

About the Authors

Caroline Stroud is a partner in the Global Investigations practice at Freshfields Bruckhaus Deringer LLP. She specializes in workplace investigations into misconduct and has extensive experience in reviewing whistleblowing procedures, conducting "lessons learned" exercises and analyzing culture within a business.

Emma Rachmaninov is a regulatory partner in the Financial Institutions Group at Freshfields Bruckhaus Deringer LLP. She regularly advises financial institutions on culture and governance matters, including in relation to the UK's Senior Managers and Certification Regime.

Holly Insley is a senior associate on the People and Reward team at Freshfields Bruckhaus Deringer LLP, and a member of the Global Investigations practice. She advises financial services clients on executive remuneration issues, hiring and firing and the investigation of suspected misconduct.

Postscript

As the financial system becomes operationally more interconnected and complex, operational resilience will be strengthened if we start thinking about operational failures in a different way. This is definitely going to be challenging, but it's something that risk practitioners and regulators should consider.

Three key questions are particularly pertinent. How can we engender the same sense of importance to operational risk events as in a health and safety environment where people's lives are at risk? Is it reasonable to assume that operational failures have the potential to cascade through the financial system in unpredictable ways? And what institutional set up is required to encourage learning from failure, given the thrust of regulation has been to drive greater accountability?

There is no panacea, but there are specific steps risk practitioners and regulators can take to address failure issues. Practitioners should proactively support a learning culture and ensure that there is a clear and well-understood incident reporting system that is supported by senior management. Moreover, each firm should have an effective resilience plan that can be activated immediately after a breach occurs.

Regulators, meanwhile, should have rules in place to ensure that organizations that commit infractions are not just punished but actually learn from their mistakes.

The GARP Risk Institute welcomes feedback on these questions or any other aspect of this set of articles.

About GARP

The Global Association of Risk Professionals is a non-partisan, not-for-profit membership organization. GARP offers risk certification – the Financial Risk Manager (FRM®) and Energy Risk Professional (ERP®) - and educational programs for professionals at financial institutions, government agencies, central banks, academia and corporations. Through the GARP Benchmarking Initiative and GARP Risk Institute, GARP sponsors research in risk management and promotes collaboration among practitioners, academics and regulators to promote a culture of risk awareness.

Founded in 1996, governed by a Board of Trustees, GARP is headquartered in Jersey City, NJ, with offices in London, Washington, D.C. and Beijing.

GARP | Global Association of Risk Professionals

Creating a culture of risk awareness®

New York
111 Town Square Place
14th Floor
Jersey City, New Jersey
07310 USA
+1 201.719.7210

London
17 Devonshire Square
4th Floor
London, EC2M 4SQ
UK
+44 (0) 20.7397.9630

Washington D.C.
1001 19th Street North,
#1200
Arlington, Virginia
22209 USA
+1 703.420.0920

Beijing
Unit 1010 Financial Street Centre
No 9A, Financial Street,
Xicheng District
Beijing 100033 P.R. China
+86 (010) 5737.9835