everbridge™

The ultimate operational resilience handbook

A practical guide for risk professionals to manage the multiple dimensions of operational resilience

Table of Contents

Introduction

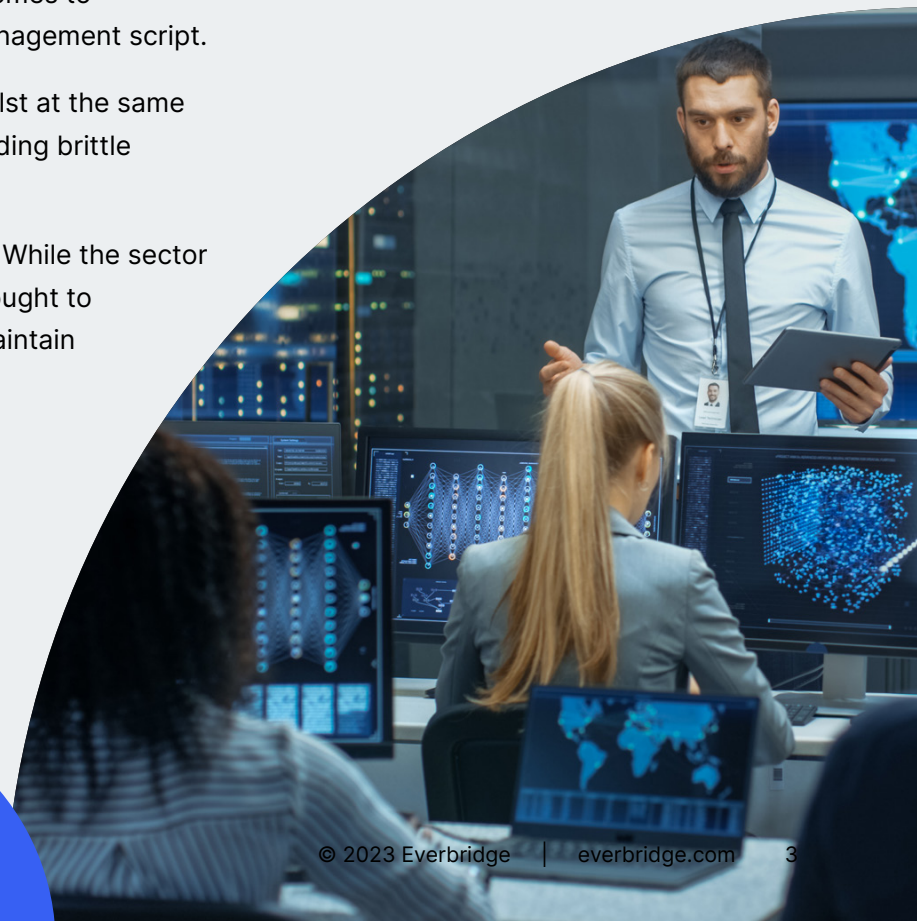
Nobody can argue that becoming more resilient isn't a good thing and the fact we live in such a volatile world, this has never been truer. Achieving operational resilience is inherently challenging for financial services given the increasing complexity of processes, technology infrastructure, and organizational silos.

Moreover, for an industry facing major regulatory and stakeholder pressure when it comes to operational resilience, it no longer has the luxury of sticking to a conventional risk management script.

So, how does a financial institution (FI) mitigate the rising threat of systemic risks whilst at the same time ensure total compliance, all without breaking the bank? To start with, by not building brittle systems that operate close to breaking point.

One of the learning points from the 2020 pandemic was 'build resilient organizations'. While the sector globally faced the new challenges created by the health crisis better than most, it brought to light the significance of a thorough and prepared operational resilience strategy to maintain business functions through unprecedented crises, whatever they may be.

It is for this reason that we created this handbook. By looking within our network, we have pooled seasoned experts and leading voices from the world of critical event management and operational risk management to offer you cutting-edge insights and best practices across the major disciplines of operational resilience to help you on your journey to becoming a future-fit organization.



Expert contributors

Jan Hickisch
VP Global Portfolio Strategy and Marketing, Atos
jan.hickisch@atos.net

"Jan is a seasoned communications specialist who has designed a variety of communication solutions across Development, Technical Sales, Product Management, Strategic Portfolio Management."

Owen Miles
Field Chief Technology Officer, Everbridge
Owen.Miles@everbridge.com

"Owen is a respected industry thought leader with more than 20 years of global experience in the Critical Event Management space. He has been helping customers to strategize and deliver actionable plans to keep their organizations' assets and people safe while protecting their brand and reputation."

Philip Nunn
Senior Director, Business Solutions-Sales
Philip.Nunn@everbridge.com

"Philip leads a global team of internal communication experts who specialise in helping organizations meet the increasingly complex challenge of effective employee communication."

Tracy Reinhold
Chief Security Officer, Everbridge
tracy.reinhold@everbridge.com

"Tracy is responsible for advancing Everbridge's enterprise-level security strategy, as well as working closely with customers and partners to optimise their approach to managing and responding to critical events."

© 2023 Everbridge

Foreword

As the financial services sector continues to navigate the new reality brought about by the COVID-19 pandemic, the need for robust operational resilience has been brought into sharper focus than ever before. Operational resilience is no longer just a 'nice to have', it's a non-negotiable component of any forward- thinking business.

Until recently, operational resilience was typically developed with a risk-avoidance mindset, primarily focused on the end goal of full recovery. Today however, given COVID-19's reinforcement of regulatory interest in operational resiliency and with organizations facing a greater variety of operational threats, the importance of demonstrating a firm is operationally resilient is much more than just assessing the strength of its business continuity and disaster recovery plans.

Implementing an operational resiliency framework is a far-reaching and complex endeavour, and whilst some firms are already heading down the path towards implementation, a large portion of the sector is still very much assessing what they need to do and how best to do it. Whichever category your business falls into, there is still time to design, adapt and run a program in a way that ensures you do it once and do it right before the regulators come knocking.

A stronger focus on regulation

In the US, another trio of supervisory bodies – the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation – released an inter-agency paper outlining sound practices drawn from existing regulations, guidance, statements, and common industry standards, designed to help large banks increase operational resilience.

In Europe, policymakers are also addressing the topic. In September 2020, the European Commission adopted the Digital Finance Package, and we anticipate the region taking a similar approach in relation to senior executive accountability as with the UK, particularly in relation to cyber resiliency.

In Hong Kong, the Monetary Authority (HKMA) has created the Supervisory Policy Manual which outlines the regulatory requirements for organizations to maintain sound and effective risk management practices, including operational risk management. This framework includes identifying critical parameters, a mapping exercise to identify the people, processes, technology, information, and facilities necessary to deliver critical operations. Also, within the framework are suggested risk management policies, scenario testing and incident management. The HKMA expects all organizations to have developed a framework by May 2023 and implemented it by 2026.

© 2023 Everbridge

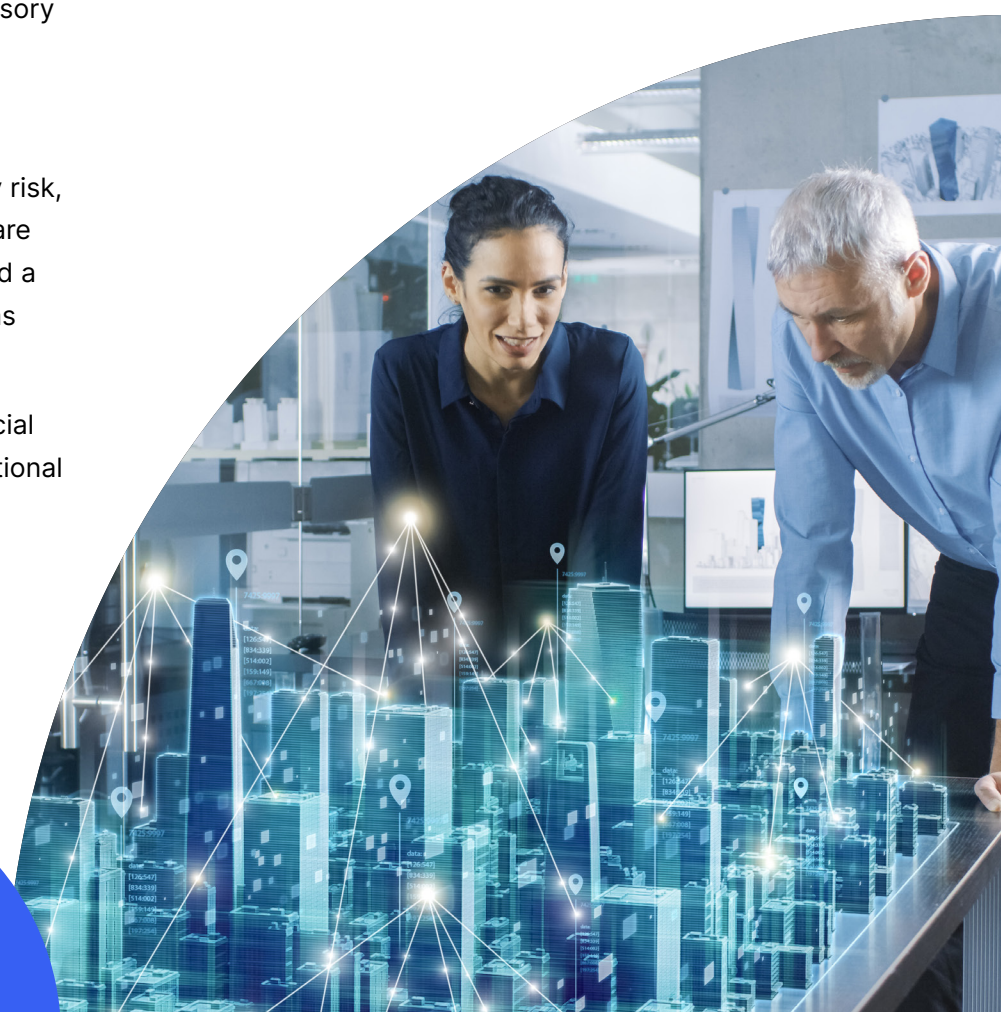
In India, operational resilience regulations are mainly governed by the Reserve Bank of India (RBI), which is the country's central bank and primary regulator of the financial sector. In 2021, the RBI issued a discussion paper on "Building a robust and resilient non-banking financial companies (NBFC) sector" that proposed various measures to strengthen the operational resilience of organizations. The paper suggested measures such as stress testing, business continuity planning, cyber security, and governance to mitigate operational risks faced by NBFCs.

And finally, taking a more global approach, the Basel Committee on Banking Supervision (BCBS) will be promoting cross-border regulatory convergence with its guidelines on operational resilience, which align closely to emerging supervisory expectations in several jurisdictions.

Future focus

While firms adapt and evolve their approach to managing operational resiliency risk, there will be significant changes to the overall discipline. Looking forward, we are likely to see significant improvements in data quality, increased automation, and a more sophisticated use of technology to proactively manage operational risk, as well as risk-related processes.

The current environment means that the stakes have never been higher. Financial services firms, senior leaders and risk professionals need to ensure that operational resilience is managed with enhanced vision and competencies, with the aim to protect the profitability and reputation of their organizations.



Business continuity risk

The events that unfolded during 2020 brought into stark reality that the way organizations approach building business continuity (BC) plans is no longer fit for purpose.

Prior to COVID-19, most plans were designed to deal with short-term events such as flooding or terrorist attacks, but the pandemic exposed that traditional ways of planning had substancial flaws.

The magnitude and duration of the crisis stressed the most robust continuity plans well beyond their original design parameters. And even firms that had pandemic response plans in place found they had not fully anticipated the level of social, economic, and operational disruption that would be caused.

Another issue that emerged was just how heedlessly businesses had been operating in our interconnected, integrated, complex and dynamic world for some time now, and that these tendencies accelerated, creating radical uncertainty and systemic risk.

Moving forward towards resiliency, the aperture setting for a new BC lens will have to be much wider and more all-encompassing. Financial services' business leaders need to seize the opportunity to understand the pandemic's enduring impact and reinforce continuity and resilience capabilities in anticipation of future turmoil.

The sector should learn from exercises, emerging threats, and even full-blown crises, then codify and produce a new working model to enable a far more sustainable and robust business continuity program, one which will ultimately enable firms to be better equipped to handle whatever critical event comes their way.

This means the sector must be prepared to challenge their current operating models. They should look at how work is being done and lean into a digital-first approach – developing, testing, and implementing effective formal processes and technologies that maximizes the synergy between their human and hybrid workforces.

By building operating models in this way, firms can be more sustainable and resilient to changes like those we saw during the pandemic. Indeed, these new operating models could potentially require less of a jump to a new recovery or continuity plan should something even more adverse occur in the future.

Financial services' business leaders need to seize the opportunity to understand the pandemic's enduring impact and reinforce **continuity and resilience** capabilities in anticipation of future turmoil.

© 2023 Everbridge

Expert insight

01. What are the tangible steps organizations can take today to enhance their resilience and preparedness going forward?

Tracy Reinhold (TR): Organizations should take the time now to establish a schedule of exercises to ensure they are prepared for business disruptions. Waiting only makes it harder for organizations to be prepared. Additionally, they should focus on exercises that allow them to recover from business disruptions regardless of the cause. Being too focused on a specific type of disruption actually serves to put blinders on the response team and does not allow them to prepare for the unexpected.

02. In your experience, do financial services firms adequately understand the business continuity risk environment? What more should they be prioritising to minimise their risk exposure?

TR: Financial services firms operate in a highly regulated industry and are generally required to demonstrate business continuity plans to their regulators on an annual basis. Based on this fact, most have developed plans to address business continuity, however, not all have embraced technology in their efforts to modernize their plans. Some still maintain printed binders which, when printed, are already outdated. Ensuring that the plans are digital and receive regular updates from the organization's HR teams is critical in keeping current with plan owners in the business lines.

Additionally, by creating hyperlinks to specific parts of the plan, they enable the business to actually use the plans as opposed to just maintaining them to show to regulators annually. Organizations should also use technology to enable the response teams once the plans are activated. This allows for a faster resolution to the disruption and provides an opportunity to return to revenue generation quicker.

03. What essential advice would you offer to executives on implementing a holistic operational resilience framework to help them make better decisions, and maximise value from business continuity management (BCM)?

TR: The key issue here is to avoid silos as plans are developed. Enterprise or operational resilience provides the ability of an organization to maintain an operational tempo that ensures success despite unexpected business disruptions. Organizations should consider what are the critical capabilities needed to run the business and then build a robust response capability to bring them back online quickly. Additionally, they should maintain an active intelligence feed that informs the business about emerging threats, so they have the chance to mitigate them before the manifest.

© 2023 Everbridge

Compliance & regulatory risk

For an industry that has been stung by fines and penalties totalling almost US$1 trillion over the last decade, understandably compliance and regulatory risk are never far from the thoughts of financial services (FS) providers.

Nonetheless the events of 2020 and 2021 have reshaped the landscape of FS regulation and the sector is having to navigate a global proliferation of diverse regulatory requirements, stakeholder expectations, and business model changes exposing them to a greater degree of compliance and regulatory risk than ever before.

Firms have found themselves having to be nimble in developing effective responses to regulatory improvisation such as the increased use of guidance and rulings to 'do the right thing' putting the impetus on firms to implement an overarching compliance program, one which meets extensive regulatory and public policy challenges and concerns, while, at the same time, recognizing and maximizing value.

This has forced a 'stress testing' of current models for regulatory compliance risk assessment and management, growing tension between the need for commercial viability and an accelerated regulatory focus.

While firms adapt to the ongoing pressures engendered by the regulatory changes introduced during the pandemic, lessons have already been learnt from the crisis in terms of the 'next normal' for regulatory compliance risk assessment and management. Discussions are in hand about whether there will be a return to 'business as usual' compliance or whether and how the 'BAU' model can be improved. What is needed now, however, is a clear consensus as to the direction of future regulation.

But the COVID-19 crisis has provided a wealth of data and valuable insights for the sector, all of which can be used to accelerate, or at least refocus, existing conversations about pursuing long-term priorities and how they are helped or hindered by pre-crisis modes of regulation. A refreshed notion of human worth and social inclusion seems to have a role to play in those dialogues. As a highly regulated industry, the sector has an important opportunity to show leadership here, not least from a reputational perspective.

© 2023 Everbridge

Expert insight

01. How can FS firms go about implementing an overarching compliance program that meets extensive regulatory and public policy challenges and concerns, while, at the same time, recognizing and maximizing value?

Philip Nunn (PN): A robust internal communication strategy must be at the heart of any organizational compliance program. Compliance officers must be equipped with the right communication tools and practices to effectively get their staff up to speed on new regulations and re-educate them on existing ones.

The effectiveness of such communications must be tracked and reported on. Mandatory employee acceptance of policies and processes must be incorporated into messaging to 'prove' their willingess to comply.

02. When companies undertake data processing activities – including handling, storage, and transfer – what regulatory risks do they need to manage?

Jan Hickisch (JH): Regulatory risks arise from violations of laws, regulations, policies, rules as well as societal, business, or ethical standards. Complexity increases the more countries you are serving,as laws, regulations and standards typically vary for different geographies and countries. And policies and rules may differ from client to client. So, companies require strong knowledge about local law and regulation.

In today's cloud world this is not just limited to the country the client has its headquarters, but in which countries the users of the client use the service, where the providers cloud datacentre is located, in which locations data will be processed, where backups will be stored, what subcontractors are involved and a lot more. A good example for that is GDPR, which defines strict rules, how to deal with personal data and what measures companies must implement to be compliant.

03. What overarching advice would you give companies in terms of planning for, implementing and enforcing compliance across their organization? What considerations should they make when developing and implementing appropriate policies and procedures?

PN: Ensuring that compliance activity is not considered an 'annual' exercise. Businesses can achieve competitive advantage/ differentiation by being able to demonstrate they are more than simply 'paper-compliant'. In other words, a holistic, always-on, culture of compliance is demonstrably in place right across the organization.

© 2023 Everbridge

Crisis management

COVID-19 provided all of us with an all-too-real lesson in the criticality of crisis management. The devastating and long-tailed social and economic crisis underscored the importance for a coordinated response to critical events and their aftermath, and accentuated the risks associated with uncoordinated and heavily bureaucratic approaches to crisis management.

For companies and boards managing crises, the pandemic brought about unprecedented challenges that in many ways fundamentally transformed the way we think about crisis management. It has also instigated some real changes to the discipline, and senior leaders and their crisis teams need to make sure the benefits of those changes are not squandered.

It also painted a clear picture of the true worth of many of the fundamentals that underpin good crisis planning and management in any environment – preparedness, transparency, engagement with regulators and employees, clear and timely communications, and proactivity.

Crisis communications planning has long been the hallmark of a well-managed critical event, and the importance of clear, action-oriented, and transparent communications to stakeholders has taken on an increased importance. The risks of poor communication have never been greater, as firms face scrutinity for poor or untimely communications.

A unified communication strategy, is essential. Ensuring consistency across all employees, investor and customer-facing channels and sending timely alerts about unforeseen changes will put stakeholders at ease and help messages reach the widest possible audience.

The best messaging, however, is only as good as the ability to get it out. If they haven't already then firms should consider and re-evaluate the effectiveness of internal and external communications mechanisms. In doing so, firms should focus on making sure that the communications channels are user-friendly, relevant, and ready for off-hours communications.

Times of crisis challenge every organization. Nevertheless, the survival and long-term success of a business depends on how well it responds during a crisis or critical event. The most effective firms in responding to a crisis are those that learn from prior experience, develop guidelines and tools, and empower those on the front lines and reward creative and responsible problem solving.

© 2023 Everbridge

Expert insight

01. Any sudden event that threatens a company's financial performance, reputation or relations with key stakeholders has the potential to become a full-blown crisis in short order. When the stakes are high and scrutiny intense, what role does the board play in crisis response?

Philip Nunn (PN): In times of crisis, the board's primary functions are to empower resolution and reassure stakeholders. Empowerment means expediting the efforts of key personnel to address and resolve the crisis. Stakeholder reassurance doesn't demand full transparency, but rather a proactivity in 'fronting up' to the issue.

Crisis impact research shows 53% of consumers expect brands to respond within an hour. Nearly 60% expect that response to come from the CEO.

02. How can financial services firms effectively manage their crisis communications to handle stakeholders' perception?

PN: Establish a single source of truth and ensure this is communicated (ideally at the same time) to everyone in the organization. Provide regular updates to keep everyone informed, even if there's nothing new to say. Failure to do this fosters a sense that information is being concealed and can result in the spread of rumours which may be amplified via social media.

Organizations whose executives don't proactively control the narrative in this way will often find that the narrative controls them – forcing them continually onto the back foot and at the mercy of the message.

03. How has crisis management technology evolved over the last 10 years, and what benefits do you see modern technology offering large financial services organizations when it comes to crisis management and preparation?

PN: Communication technology enables the rapid dissemination of information to everyone in the organization, regardless of where they're working, what their role is or what device they're using. Hospital workers on wards, manufacturing workers in warehouses, frontline retail staff and field-based salespeople can all be reached as quickly and easily as corporate office staff.

This removes any possibility of information black spots and ensures everyone has equal access to information. In doing so, collaboration is enhanced between employees involved in responding to the crisis, and nobody acts which could inflame the situation, however inadvertently.

© 2023 Everbridge

Environmental risk

Climate change will be a huge test of global resilience. For the financial services sector, it presents a huge opportunity to redefine not just how firms operate in the world, but it also offers the possibility to get past the controversial debates and 'do the right thing' because in this activist, social media-fuelled culture, failure to 'green' the global economy now will increase costs for society in the future.

But the sector has long come to terms with the fact that they need to demonstrate greater and sustainable environmental performance management to protect their brand and reputation. In fact, financial services' providers are ahead of the game when it comes to all things green, but the issue is still one that is a veritable bubbling pot of reputational and regulatory risk as pressure to demonstrate green credentials is mounting from all directions.

The regulatory and reporting landscape is expanding to ensure that climate-related financial risks are addressed throughout the financial system, investors are requiring greater transparency as to how green their investments are, and the accessibility of data means consumers and employees have woken to these issues and are not afraid to vote with their feet or wallets.

What's more, with this seismic shift in the consciousness of a firms' stakeholders, weaving climate change elements into an operational resilience framework and fostering a strong ethical culture – where environmental excellence becomes part of its strategic thinking – can significantly differentiate themselves from competitors.

For risk teams, climate-related emerging risks are already coming to the fore – and others will evolve. To be better prepared, they should consider using operational risk software to conduct scenario analysis exercises to help identify ways in which they may be impacted and suggest ways in which risks could potentially be mitigated.

Using such technologies hand in hand with creating transparent, accountable, and sustainable business cultures, the sector can take a significant step towards reducing the impact on our planet.

Ultimately though, managing climate-related risk is critical to ensure the resilience of a firms' business strategy. Embedding climate risk into the operational risk management framework is the key to this and needs to be at the top of the agenda across the sector, not just to meet regulatory and stakeholder demand, but to future-proof and future-ready business models for an increasingly climate-conscious world.

To be better prepared, risk teams should consider using **operational risk software** to conduct scenario analysis exercises to help identify ways in which they may be impacted and suggest ways in which risks could potentially be mitigated.

Expert insight

01. In recent years, there has been an unmistakeable cultural shift toward a global community with an increasing social and environmental conscience. National and international laws, regulations, policies, politics, and wide-ranging commercial pressures are all motivating businesses to address the ESG agenda. What is the role financial institutions play in this journey?

Jan Hickisch (JH): All industries are seeing increasing societal pressure for changes to economic behaviour to move beyond only growth outcomes and employ modelling for overall betterment such as equitable distribution of wealth. Theories including Doughnut Economics continue to gain traction, putting pressure on financial institutions to step up.

This presents itself as a grand opportunity for financial services organizations, as the current heart of the world's economic engine. Taking deeper responsibility over the assets they control to ensure fewer investments in oil and fossil fuels is one simple example.

Developing indicators that reward business resilience beyond monetary growth or hoarding is another – think of it as a credit score but for societal resilience. It begins with developing an underlying data landscape to help identify, assess, and maneuver towards "safe and just spaces for humanity."

02. Attitudes toward climate change have been evolving within the financial services industry for some time now, but the tempo has quickened in recent years. Despite an increasingly climate-conscious world, what do financial services firms need to do to ensure that climate risk is embed into their operational resilience framework?

JH: In general companies will have to assure, that all processes, deliverables, and assets are not only aware of sustainability, but ideally also contribute to a greener world by reducing CO2 emissions, energy consumption and reduction of the ecological footprint.

For the financial industry it will be important to create investment strategies and portfolio, which are preferring companies with long-term business strategies and prove ESG dedication. And they should lead by example offering new digital financial services with e-Consultation, digital sales assistants, paperless processes, and services with e-Signing of documents as well as sustainability rewarding policies.

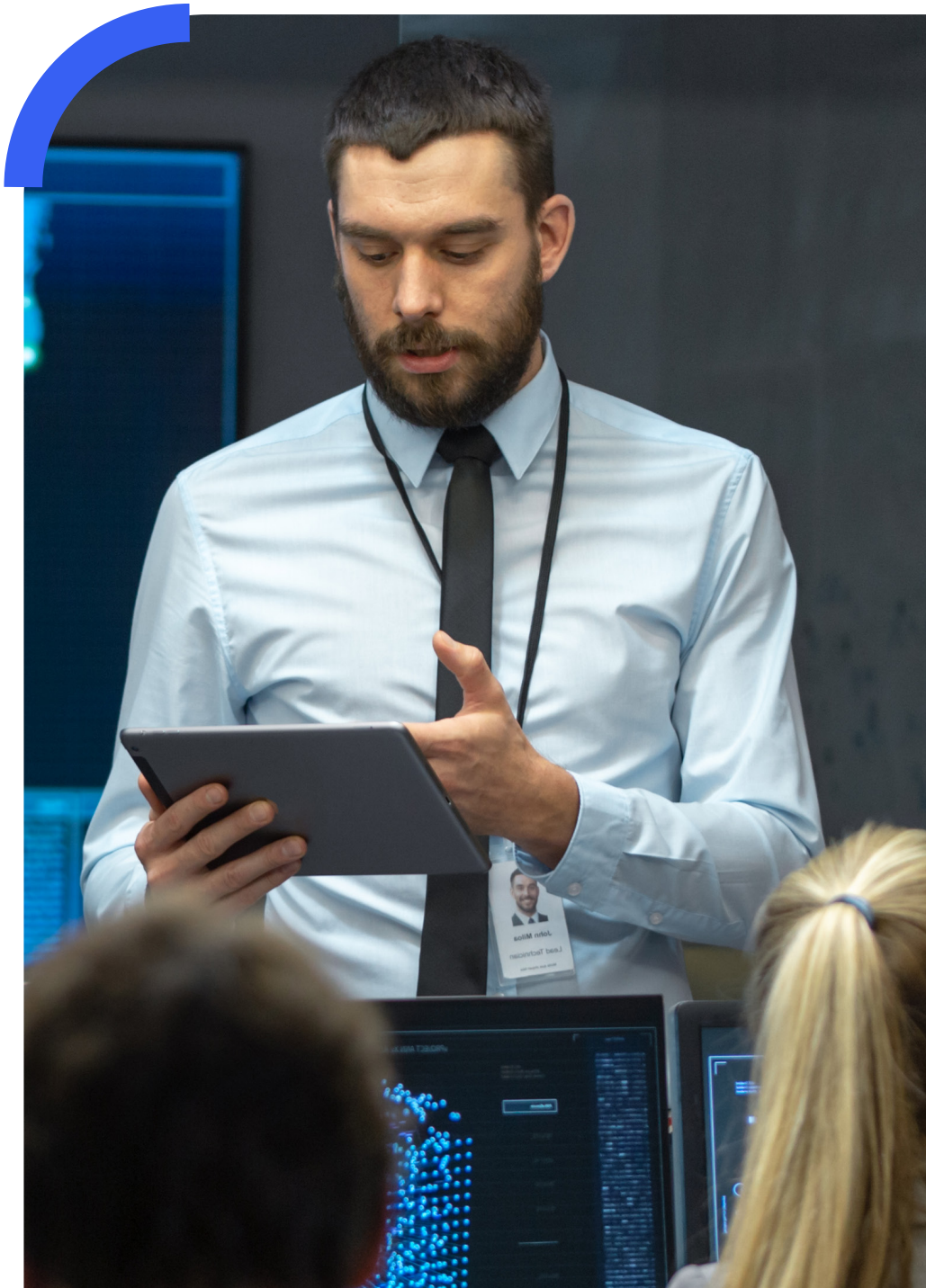
© 2023 Everbridge

03. While the pandemic has underscored the obvious need for strong and developed operational resilience programs, COVID-19 has also made it evident that resilience and ESG principles go hand in hand. But how can this growing consideration of ESG turn into real and lasting practices?

JH: While local law and regulation are needed for the day-to-day business and operations, international rules and policies are required to establish world-wide accepted practices for better sustainability, social and corporate responsibility.

This is about being better together, about the power of an ecosystem on the society and corporate level, participatory systems and open and standards-based frameworks and platforms, which endorse safe, secure, and resilient solutions. Rewarding better and best behavior, achieving higher ESG scores, motivating businesses to invest in long-term strategies, helping them to transform their and their client's businesses.

The digital world offers many ways with innovations and new technologies to better support businesses on their way to a more sustainable and more responsible future. AI, predictive and prescriptive analysis, automation, human to machine and machine to machine interactions will contribute and accelerate a new normality in the post COVID-19 era. But technology alone won't solve all the challenges; it requires change management and governance on all levels, for individuals, corporations, and society.



IT & cyber risk

In the last decade, financial institutions have poured countless resources into protecting their own networks and systems from cyberattacks. But with the pandemic having supercharged all things virtual, opportunistic hackers have upped their game, developing new tools to attack and infiltrate systems. Before the pandemic, about 20% of cyberattacks used previously unseen malware or methods. That rate rose to 35% during the height of the pandemic.

Ensuring resilience against disruptive cyberattacks is an impossibly broad task, risk and security teams are tackling everything from information security controls to scenarios and war games, third-party oversight, data protection, and fraud authentication processes.

In addition, risk and security teams are spending more time trying to figure out the harder-to-measure disruptive threats – cyber and physical – to their organization's networks. Malware, employee error, rising potential for employee malfeasance due to job cuts and redundancy, and plain old hardware failure can be just as crippling when it comes to a loss of operational functionality.

To tackle these issues head-on means old notions of impenetrable defences must be shelved to orchestrate a truly cyber resilient approach. But with budgets stretched and already over-burdened teams running at max, tackling wave after wave of cybercrime is no small feat.

Still, there can't be any more excuses as the global bill for cybercrime is skyrocketing and regulatory and stakeholder pressures are intensifying; meaning the time for passivity is over and a switch to a more cyber resiliency mindset needs to take place. It is only by thinking of overall network resiliency that firms can overcome existing threats as well as future threats from emerging technologies such as artificial intelligence, Internet of Things, and augmented reality.

The best response to cyber security threats is not to simply bolt a cyber security function next to existing capabilities. As with digital transformation, cyber resilience requires more organizational agility, therefore firms should use it as a lens through which to improve overall operational resilience. For example, the tools, techniques, and cultural responses to cyber security can also be used to strengthen traditional business continuity capabilities.

By taking this approach means firms have an opportunity to distinguish themselves as model industry leaders. Investing in cyber-physical security speaks to good governance, ESG and digital capability – all necessary traits for a future-ready organization.

© 2023 Everbridge

Expert insight

01. Data protection and privacy have continued to climb the corporate agenda. The pandemic sparked a mass migration of employees to remote working and opened up new attack vectors for malicious actors. With potential data breaches raising the financial and reputational risks, what steps should a financial institution take to create, develop, and implement cyber resilience?

Tracy Reinhold (TR): Resilience overall has been elevated due to the pandemic and this is not a bad thing. As it relates to data protection, the proper execution of the basis blocking and tackling are critical. First, patching must be done without fail or delay. Antivirus software must be installed and a complete understanding of the different versions of software used in the organization must be known and addressed.

Maintaining an up-to-date end of life schedule and an understanding of legacy systems is critical. One of the challenges with remote workers is the idea that they will use unauthorised devices to conduct company business. Oftentimes these devices do not have the necessary protections in place and may not be visible to the information security team. Conducting an engaging information security training for employees in also important and should address issues such as social engineering and phishing attacks.

02. How do you expect digital risk management to evolve in the months and years ahead? In an uncertain future, will a data-driven response to risk be indispensable?

TR: The intersection of digital and physical security is coming of age and the idea of continuing to treat them as different issues allows risk to grow. All things are becoming digital, and an organization must have an enterprise risk management thought process. Digital risk is huge, and the impacts are aligned with the size of the risk. However, physical risk to life is also important and is oftentimes facilitated by a digital attack. Therefore, having a total risk management practice is the best way to provide protection to the enterprise.

03. In your opinion, what are the major information technology and cyber security risks facing financial institutions today? How vulnerable are they to this risk?

TR: As with any business the risks are significant and the idea that you will be able to create a completely safe environment is false. There will always be risk and some of that risk can be mitigated by educating employees. For those institutions with a public facing aspect, there is also the risk of cyber being introduced by the physical access of a bad actor. Restrictions on data ports and other such measures help to defend against these types of attacks but cannot entirely prevent them.

Another risk is that which is introduced by third parties. A robust third- party risk program that includes cyber is extremely important in defending against these types of risk.

© 2023 Everbridge

People risk

It is near impossible to entirely insulate a financial services' firm from bad risk decisions taken by negligent or malicious individuals, in the same way that you cannot protect a firm from unforeseen critical events.

And as we have seen time and time again across the sector, when left unchecked, the human aspect of risk can be costly – both financially and reputationally. If firms do not navigate the challenges of people risk, then there is likely to be a serious regulatory reckoning. Especially given the legacy of misconduct following 2008, and as we emerge from the current health crisis, regulatory focus is firmly on conduct.

There is an opportunity for the sector in this defining moment. Abide by regulatory rules only as required or help lead the charge. Grudging and minimal compliance may keep a firm out of trouble today but will do little to gain stakeholders' trust or build future resilience.

The more forward-looking players have already spotted the potential of adopting a proactive stance with regulators and stakeholders by weaving accountability, ethics, and transparency into the fabric of their operations.

But it is worth noting that despite the best efforts of firms to educate employees, everyone across the organization will still have their own personal predisposition to risk. Nevertheless, it is possible for firms to establish the right kind of risk culture to try to protect operations and employees from something that could put the entire organization at risk further down the line.

To combat the varying forms of people risk, creating sound frontline attitudes and behaviours should be a firm's first line of defence. To enable this culture change, firms should look to modify processes such as training, rewards, and financial compensation, all of which can be effective methods for creating a culture that can deal with the human element of risk.

Still, those firms that understand the drivers of conduct risk can better understand whether their conduct risk frameworks are robust enough to mitigate against the risk of harm stemming from its activities or individual behaviours.

For an industry that has been plagued by conduct and culture risks it is imperative that firms in this new age of accountability identify and adopt the most ethical policies, be that data governance, anti-financial crime, or supply chains, to inoculate their business against legal and reputational challenges. Doing so will send out an important message that will not only help confer competitive advantage but will help foster better relations with all stakeholders – regulators and employees included.

© 2023 Everbridge

Expert insight

01. Because risk exists everywhere in an organization, how does a financial institution balance the management and mitigation of technical, process-driven risks vs. human, behavioural risks?

Tracy Reinhold: Technical and human risk have more in common than most people think. The idea of treating them as stand-alone problems actually creates a significant gap which allows risk to thrive. A potential approach would be to look across an entire enterprise and incorporate regulatory, technical, and human risk as the total risk picture. By doing this and collaborating between teams, the overall risk is diminished.

02. How should a company go about communicating its compliance vision to employees? In what ways can this vision be continually reinforced so that it does not become just a 'flavor of the month' issue?

Philip Nunn (PN): Everyone absorbs information differently, so the utilisation of different communication modalities is key to ensuring messaging is truly absorbed through an organization. Variety also ensures employees do not suffer from message 'fatigue'.

03. Since the COVID-19 pandemic, social considerations including prioritising employee health & safety as well as employee engagement, have guided many business decisions that have potential financial and reputational consequences. How companies addressed and responded to these challenges will be remembered by their employees for years to come and can potentially have a lasting impact on future employee behaviour including engagement, productivity, retention, and loyalty. What actions can firms undertake to mitigate this growing issue?

PN: Responsible employers will increasingly identify what employees need from them. In the future of work, employers will need to flex between functional messages, such as job enablement, health and wellness, to emotional messages, like purpose, community, and culture. Flexible working, career growth and personalization are likely to be among the biggest needs.

A colleague put this well – it's the duty to care, rather than the duty of care. People don't care how much you know until they know how much you care.

© 2023 Everbridge

Third-party & supply chain risk

Mitigating supply chain risk presents one of the greatest threats to global businesses, but very few businesses, regardless of sector, have full visibility over third-party subcontractors in their supply chain.

For the financial services industry, originally much of the focus was on cyber risks in third-party relationships, especially given that the industry is progressively outsourcing key activities to third parties. But now, owing to the pandemic, other risks are being amplified too, such as the financial viability risk of third parties, fourth-party risk, and concentration risk.

While many firms are on the right path to successful and automated Third-party Risk Management (TPRM), they are still yet to take the necessary steps to mature their program content and execution.

With regulatory activity rapidly picking up in this space, the sector needs to demonstrate more progress towards taking comprehensive steps to minimise the impact of third-party risks on business performance and reputation.

To ensure that their third parties not only comply with regulations, but also protect confidential IT information and avoid unethical practices, the scope of a firms' TPRM needs to expand beyond traditional surveys and assessments for third-party risks and compliance. Firms should be looking to transition away from "point-in-time" assessments towards a more continuous evaluation methodology that looks beyond a supplier's value or performance.

By using third-party risk data, statistics, and visualization to generate insights, firms can create and drive a risk-based approach that helps surface the parties within a supply chain that carry the highest level of risk. The data gathered from these TPRM activities will provide business intelligence that will lead to operational change and reduce risks throughout the vendor lifecycle.

Firms also need to realise employees need to become even more important as the first line of defence. To that end, organizations should provide employees with the right level of training and ongoing support. By embracing the need to empower their people to understand, implement and actively maintain policies and processes around third- party risk management, financial institutions will effectively manage the third-party ecosystem in such a way as to create a culture of transparency and accountability – a key regulatory focus!

© 2023 Everbridge

Expert insight

01. With the shift to remote and hybrid working, financial institutions have been left more exposed than ever to cyberattacks by high-tech antagonists, backdoor threats introduced via newly critical third-party suppliers, or hacker's intent on causing chaos. What advice would you give an organization looking to shore up their cyber defences?

Owen Miles (OM): The emergence of the global pandemic took the cyber security rulebook and threw it out the window. Online behaviour shifted, working environments were replaced, new technology entered working life and supply chain attacks gained steam for their success in accessing cross-sector critical data, leading to a loss in system integrity and placing security professionals on the back foot.

In terms of responding directly to a supply chain breach, relevant response teams must have access to enriched and augmented alert information across multiple monitoring systems. This allows those teams to take the appropriate resolution steps quickly, however this requires regular employee engagement, awareness, and training, particularly now given the disparate nature of the workforce.

And with security teams facing the thorny problem of managing cyber and privacy risks around information that travels to third parties and beyond, it's critical to know what steps third parties are taking to safeguard vital data and information further down the value chain.

Rigorous due diligence checks are required from all parties involved in a supply chain to ensure you have responsible custodians of valuable data. However, innovations in machine learning have massively streamlined this process – reducing the cost and time scale of screening a potentially huge number of vendors.

02. Supply chain cyberattacks are becoming more common and more sophisticated. More than half now use 'island hopping', where attackers target an organization by exploiting all those in its supply chain. What advice would you offer to financial institutions to help them ensure their most critical suppliers and partners are resilient?

OM: Historically supply chains have been under-considered when calculating risk, but the momentous disruption caused by the global pandemic has highlighted the critical business imperative to track the whole value chain of an organization. In response, firms have taken a clearer view of the full impacts and vulnerabilities of their end-to-end supply chains.

And whilst there's been an increased focus on greater investment in technology and processes to ensure that businesses have visibility along their entire supply chain, many unfortunately still rely on spreadsheets to monitor, measure, and report on disruptions. This antiquated dependency on legacy tools is a risk nightmare waiting to happen and fails to match the increasingly complexity of the current supply chain ecosystem.

© 2023 Everbridge

To prevent supply chain attacks, a hands-on approach is needed. Firms must invest in technologies, tools, and capabilities to mitigate risk – doing nothing simply isn't an option. However, these tools must be purposeful and well-integrated, only notifying when relevant action is needed, and targeting the appropriate decision makers. Otherwise, you face a workforce comprised of disgruntled employees with constant alert fatigue.

03. The past year and a half exposed a lot of risk and failures in supply chains. A lot of companies that thought that they had addressed single points of failure, realised that they hadn't. As we more forward, how can financial services companies best mitigate their supply chain risk?

OM: Unlike many other industries, financial services supply chain issues revolve around data. In the age of GDPR and privacy regulations in general, one of the biggest risks in the supply chain is the transfer of personal data between supplier and vendor. On a day-by-day basis financial services firms hand over large amounts of potentially sensitive data to third parties for processing.

The protection of this vital information is of paramount importance because any fallout from data breaches can be ugly and costly – both reputationally and financially. Therefore, firms need to treat their data like it's the gold bars locked up in the BoE. They need added layers of security much like alarms and really thick steel doors, but they also need to ensure to account for people risk because one wrong click on an email and a so-called impenetrable wall is rendered to a flimsy piece of tissue paper offering no barrier to a well-planned hack.

It's worth noting that monitoring technology can only take us so far, and the risk is that we over-notify employees and create a tolerance towards potentially critical alerts. However, the solution is not to monitor less, but it's to notify only when needed, providing a single enriched communications channel sourced from all technologies available. A resilient supply chain relies on communication with the right people, at the right time, with the right message.

everbridge™

About Everbridge

Everbridge, Inc. (NASDAQ: EVBG) empowers enterprises and government organizations to anticipate, mitigate, respond to, and recover stronger from critical events. In today's unpredictable world, resilient organizations minimize impact to people and operations, absorb stress, and return to productivity faster when deploying critical event management (CEM) technology. Everbridge digitizes organizational resilience by combining intelligent automation with the industry's most comprehensive risk data to Keep People Safe and Organizations Running™.

For more information, visit Everbridge.com, read the company blog, and follow us on LinkedIn and Twitter.

Get in touch to learn about Everbridge, empowering resilience.

everbridge™