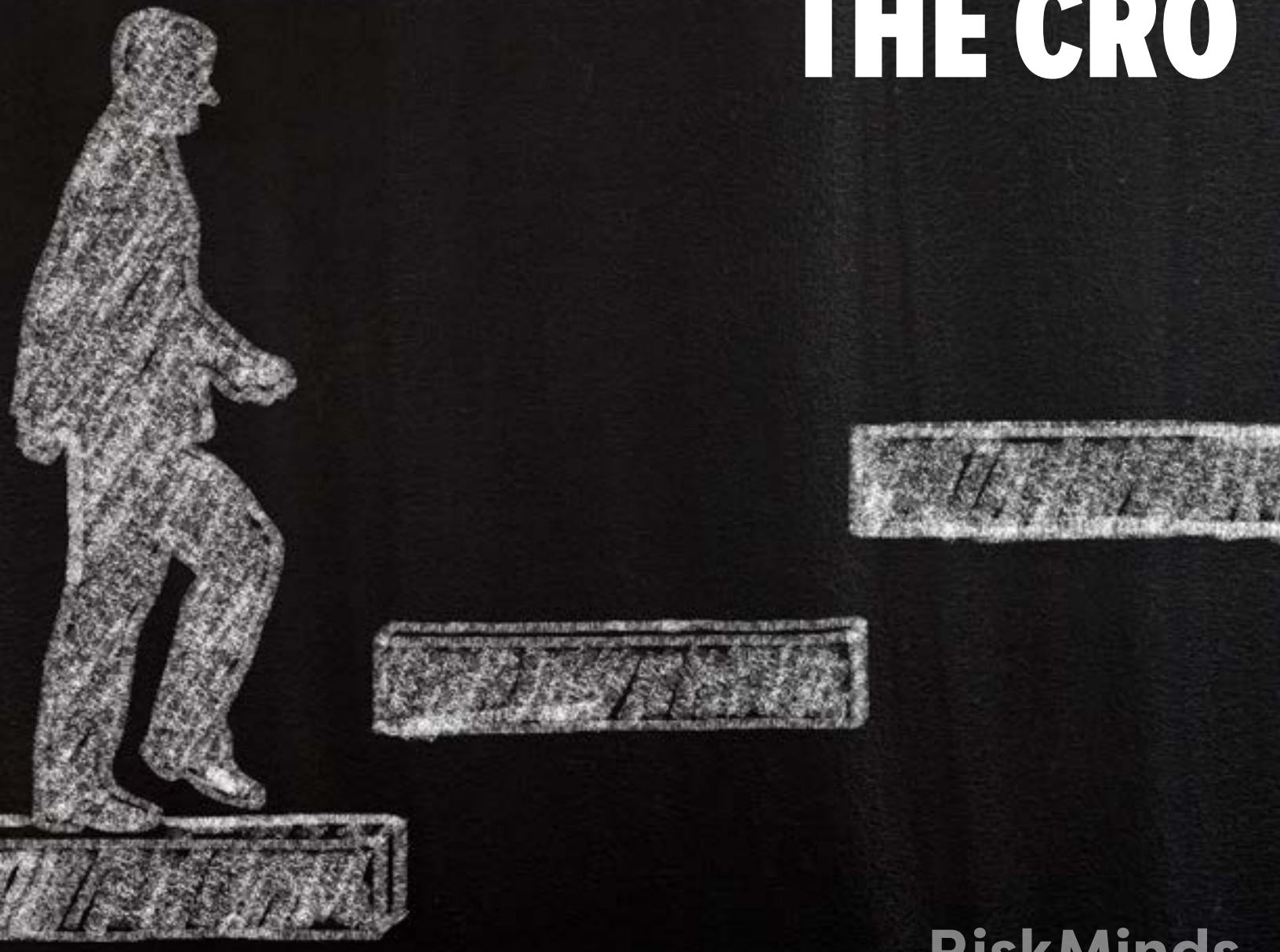
THE EVOLVING ROLE OF THE CRO



RiskMinds 365

RISKMINDS

Ed Stapley
Editor-in-Chief, RiskMinds International

Ana-Luiza Olanescu
Editor-in-Chief, RiskMinds Insurance, Asia & Americas

Charlie Burgess
Digital Content Editor

Georgia Hood & Josef Lanjri
Business Development Managers

CONTRIBUTORS

Dr John Lee
Country CEO, Maybank Singapore

Karen Tan
Chief Risk Officer Reinsurance Asia, Swiss Re

Thomas Hardin
Owner, Tipper X Advisors LLC

Stephen Cobb
Senior Security Researcher, ESET

INTRODUCTION

10 years on from the financial crisis it is safe to say that the risk management landscape has grown and developed, but has it really dramatically changed?

Regulations such as FRTB, recovery & resolution, IFRS 9 and stress testing requirements, as well as the recent GDPR and PSD2 regulations, are undoubtedly helping to make banking a safer and more responsible sector. CROs are keeping a keen eye on the advancements in AI, computing and technology which continue to pose major threats to financial institutions, as well as the opportunity to digitally transform the business and reap the rewards. Another fundamental risk, that is not new but continues to dominate the discussion is and will be critical across every part of business, is risk culture. A poor risk culture can incentivise the wrong types of behaviours and result in large losses through rogue or insider trading, damage to reputational risk or a lack of team diversity.

In this edition of the quartlerly RiskMinds eMagazine, we will be diving into these key risks in the context of the developing role of the CRO.

We hope you enjoy it.

The RiskMinds365 team

CONTENTS

ARE RISK MANAGEMENT AND BUSINESS CULTURE WHERE WE WANT THEM TO BE?

Dr. John Lee

It has been 10 years since the Global Financial Crisis (GFC). Financial institutions lost significant trust from the general public after the GFC. Many new regulations have since been introduced and imposed on financial institutions, including regulations relating to conduct, ethics and compensation. It is still early days to see whether the impact on these regulations has improved the culture of financial institutions. Conduct, ethics and culture are ultimately about human mindset and behaviours. It is not something that can change overnight. However, it is not clear that human mindset and behaviours can indeed be regulated. We need to go back to the basics of what doing the right thing means rather than through regulations. We need to instill the need and importance of social responsibilities into the corporate culture and mindset of people.

Many organisations have embarked on corporate philanthropy, that is, developing a Corporate Social Responsibility (CSR) strategy and implementing CSR activities to demonstrate that they are a more socially responsible organisation. The litmus test of the success of these philanthropic efforts is the sustainability of these efforts and the commitment from the employees over time, and ultimately resulting in a better corporate culture. For CSR to be sustainable, we need to embed CSR into our day-to-day business. Embedding CSR means that organisations must be measured not only on maximising the return to their shareholders, but also their return to the community and society at large. Shareholders of these organisations must hold the management more accountable for their CSR progress and be active in their advocacy of doing the right thing.

Similarly, employees must be measured and compensated for doing the right thing not only from a financial perspective, but also from the perspective of conduct, ethics and culture perspective, before a fundamental change in mindset could happen. In fact, it is equally important to reward someone for doing the right thing as well as penalising a person for doing the wrong thing. Often, for conduct and ethical issues, the focus is on penalising. Employees are often not encouraged or motivated enough to do the right thing.

For financial institutions, in addition to the usual CSR efforts, their business activities need to also put in place a sustainability agenda. This is why increasingly we are seeing financial institutions doing more in this aspect and adopting an Environment, Social and Governance (ESG) framework within their business activities. Financial institutions want to ensure that their business activities are more socially responsible. For example, at Maybank, we have a mission statement of 'Humanising Financial Services'. One of the tenets of this mission statement is providing everyone with access to financing, whereby the idea of 'access' is not just about access in terms of funding, but also about assisting and empowering our communities to save, invest and improve their living standards in the long term. Additionally, financial institutions with an ESG framework can play a leading role and become part of an important movement to shift overall corporate practices across industries towards greater accountability and increased mindfulness over ethical conduct for a sustainable planet.

"Conduct, ethics and culture are ultimately about human mindset and behaviours. It is not something that can change overnight."

Employees must also be encouraged to do social volunteering work. Through volunteering their time and service, hopefully employees will build a greater sense of purpose, humility and ultimately understand what doing the right thing means. It is through these organisations and people changes that will align the right conduct, ethics and culture in organisations.

In summary, we are moving in the right direction where we are seeing positive improvements in the culture of organisations. All stakeholders, namely shareholders, management, employees, the community and society at large, have a role to play on this journey. Despite what has been achieved across the industry, much more work needs to be done to raise the bar to yield higher standards for a brighter future.

BEHIND THE BUZZWORDS: THE RISKS AND REWARDS OF FINTECH

RiskMinds 365

The finance industry is facing change of unprecedented speed. To keep up, banks are embracing innovation and charging ahead with FinTech strategies. But, it's important to get behind the buzzwords, and understand the reality and risks of new technologies.

Artificial Intelligence & Machine Learning

AI and Machine Learning is having one of the largest impacts on finance today. It is already being deployed in investment management, fraud detection and risk management.

What are the risks?

Most AI solutions are provided by external companies, increasing a bank's third party risk. There are also no international regulatory standards, so should this new technology lead to losses, there may be a lack of clarity about where responsibility for this falls.

Blockchain

There are a lot of big expectations around distributed ledger technologies, and investment is pouring into blockchain especially.

What are the risks?

Blockchain is not a silver bullet, and improper implementation could harm rather than help. Like AI, regulators are still working with exchanges to explore what oversight should look like. Integrating blockchain with legacy systems can also cause cyber security risks, which are harder to manage than within a private infrastructure.

Digital Banking

Digital banking is removing the need for costly physical infrastructure, as customers go online and payments go card and contactless.

What are the risks?

Digital transformation has made the financial industry more vulnerable to cyber-attacks, theft and fraud. And it isn't just money up for grabs, often criminals and hackers go after customer data, which leads to reputational risk down the line.

RegTech

After the global financial crisis, regulation become more complex. Through digitisation and automation, RegTech can be a cost-effective solution.

What are the risks?

Partnering with RegTech firms often means sharing sensitive data, opening companies up to additional risks. And, while the technology can speed up and simplify processes, humans will still be needed to oversee it.

Risk managers should take a step back to evaluate their bank's innovation strategies to identify the risks lurking behind the

WOMEN IN RISK: GETTING A SEAT AT THE TABLE TO INFLUENCE RISK TAKING

Karen Tan

As part of our #WomeninRisk series, highlighting inspirational women in risk management, we spoke with Karen Tan, Chief Risk Officer Reinsurance Asia at Swiss Re about her thoughts about diversity in the industry and where risk management is going. Karen will be speaking at RiskMinds Asia on how to incorporate sustainability and climate change into risk management decisions.

How did you start your career?

I am an actuary by training, and started in medical insurance costing and product design based in Singapore. My career then brought me to Switzerland, where I soon had the opportunity to embark on an exciting set of developments linked to new solvency and capital regimes being developed in Europe (e.g. Solvency II). My last role in Switzerland was Chief Actuary for Zurich Life Insurance Company, before I moved with the family back to Singapore to be Swiss Re's CRO Reinsurance Asia in 2014.

Why do we see so few women in risk leadership?

I beg to differ. At Swiss Re Group, we have quite a few women in our Risk Management Leadership. Women hold the positions of CRO Corporate Solutions, Head of Qualitative Risk Management, Head of P&C Risk Management, CRO Reinsurance Americas, and CRO of Reinsurance Asia. That's 5 out of 13 Managing Directors in the Risk function. Elsewhere, I also know some impressive female CROs including Alison Martin from Zurich Insurance.

It also is very important to develop trust and good relationships with stakeholders. I think many women do this quite well – we just need the confidence to speak up, and back our points up with good rationale and evidence where appropriate.

What can companies do to attract more women (and retain them?)

There is a range of things companies can do. In my opinion, providing support for new mothers returning to work is critical. This can range from (depending on the size of the operation) having nursing rooms, to allowing flexible working times and arrangements for working from home. This allows parents (fathers too, of course) to visit schools, be involved in their children's activities or even bring them to the doctors.

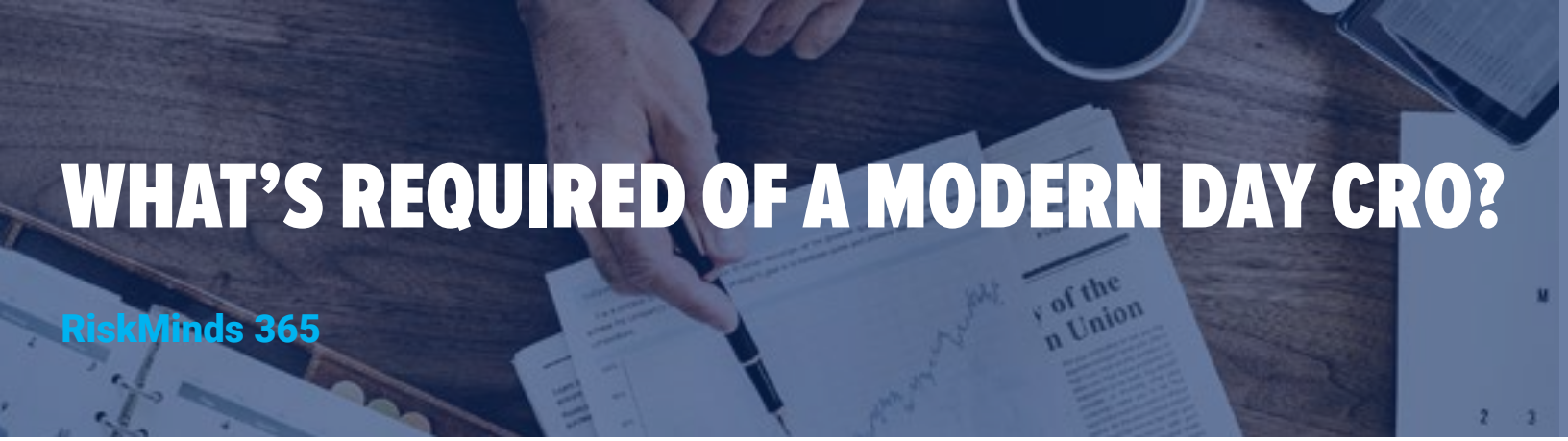
Do you have any advice for women starting a career in risk management?

Just do it! Learn as much as possible about the business, be curious, and build skills. Risk Management is a very interesting function to work in. We get a rare opportunity to be exposed to every part of the business value chain. In many companies, especially in financial institutions, the positions of CROs have been elevated over the last 10 years, to provide a more immediate and visible risk view to top management and Boards.

What does the future of risk management have in store?

I believe risk management will have an ever increasing impact on how companies do business.

Companies across the spectrum need to further embrace and improve their risk management frameworks to be fit for purpose. News today disseminate with simple taps and shares on a smartphone. We must proactively manage risks, build trust and deliver sustainable value!



WHAT'S REQUIRED OF A MODERN DAY CRO?

RiskMinds 365

Perhaps no role has changed in recent years quite as much as that of the CRO – the Chief Risk Officer. CROs are no longer the back-office workers they once were in the 1990s when the role was popularized, having moved well beyond a technical role to one that encompasses all manner of skills and capabilities. Technology remains central to CRO responsibilities, though, and as technology continues to advance and play a larger role in bank strategies, CROs need to make sure they stay afoot of developments.

So, what should a modern CRO look like?

Soft skills in high demand

Risk management draws on a blend of specialised statistical, actuarial, financial and economic modelling skills, and while it is crucial for a CRO to have this technical expertise, it's the soft skills like relationship management, clear communication and having the ability to earn trust on the board that are essential to separate a risk analyst from CRO.

In many organisations, the risk team encompasses multiple people with a broad range of capabilities and areas of speciality, from information security specialists, regulatory compliance professionals to lawyers and actuaries. The CRO needs to have the capability to bring those people together, to manage them and to motivate them.

Recent years have seen increasing shareholder engagement, whether it is activist hedge funds or institutional investors who see interactions with their portfolio companies as an important part of their fiduciary duty. Investors are looking for warning signs that signal downside risk—CROs should have a role in crafting responses to shareholder engagement where risk factors are at issue, perhaps even working more closely with investor relations to craft outreach and keep their company's shareholder base happy.

Peter Grewal, Group Chief Risk Officer at QBE Insurance adds that a CRO also has to be able to deliver information, "It's straight forward to produce a report which captures facts, issues and events, but what people are really looking for is your opinion. You have to have the courage and the right capabilities to be able to deliver that opinion in a way that makes it relevant."

Managing the risk landscape

How can CROs manage the shifting risk landscape of today?

Fabrice Brossart, Chief Risk Officer at AIG EMEA highlights the challenge, "we all know what the threats are, the question is how do you go about analysing them and how do you go about prioritising them? That should be something that changes on a regular basis."

Where CROs could add value to the board is in connecting the dots of emerging risks, keeping in mind that rarely are threats so tidily categorizable as "IT" or "culture" or "compliance." A crucial part of the CROs role is understanding the interconnectedness of risks, filtering, prioritising and highlighting how relevant they are to the organisation.

Crisis management versus strategic driving

Dealing with a crisis when it happens is a key role for the CRO, but the success ofr failure of this management has strong ties to how the company prepared itself. As with most things, being proactive rather than reactive ensures that any crisis is much more manageable (or perhaps completely avoidable).

The nature of potential crises is constantly shifting, but there are some which banks have on high priority, including cyber-attacks, regulatory compliance, and macroeconomic trends.

When it comes to preparation, the CRO also carries a lot of the burden. War-gaming, simulation exercises—the bread and butter of risk management—are crucial aspects of the CROs job, ones that have not seen their importance diminish. Being a CRO remains a deeply practical role, one that requires constant planning and execution.,

On the other side of the coin, driving strategy and identifying opportunities are functions the CRO is becoming more and more involved in. This is where soft skills come in handy, as building trust with the C-suite and board is crucial. Fabrice continues, "it doesn't always mean that the CRO ends up shaping the strategy, but we help management have a clear view – they make their decisions with more information, even if we say go left and they end up going right."

And it isn't just the quantitative aspect that the CRO brings to the table, real value is being found by bringing risk managers to assess the achievability of a plan and the quality of the assumptions that have been made during its formation.

"Equally, you have to be able to prepare the board in case their strategic assumptions don't work out," explains Alex Duncan, Chief Risk Officer at Just. "Being able to have a conversation about possible futures is a powerful tool to help bring about a richer conversation in the boardroom."

Tomorrow's CRO talent

CROs need to prepare for the future and ensure they are finding the right talent for their teams, something which can prove difficult to do. It is an unfortunate reality for banks that they are struggling in the competition for talent with fintech start-ups and the general tech sphere, even consulting. At least in the U.S., consulting has become the prime destination for top business school talent, leaving many banks to wonder how to continue attracting talent. Finding junior talent should concern banks that are looking to groom the next generation of risk leadership.

Alex Duncan thinks, "where do we fish for the future CROs? What I'm looking for goes beyond the technical; it's a breadth of experience. Ideally it includes some commercial knowledge as well as interpersonal skills." while Fabrice believes a key skill to recruit for is flexibility to be able to plan in the medium term as well as helping a business manage a crisis. For PeterGrewal, leadership skills have to be top notch, because the CRO has a massive influence on organizational culture as well as keeping risks at bay.

MINIMISING CONDUCT FAILURE AND MANAGING HUMAN RISK

Tipper X - Thomas Hardin

"It is one of the biggest mysteries on Wall Street: Who is Tipper X, the secret witness at the center of the biggest insider-trading case in a generation? The answer is Thomas Hardin — a young investment analyst who, the authorities claim, traded on inside information and may now lead prosecutors to other crucial players…" – New York Times, January 12, 2010

In 2007, while working at a small hedge fund in NYC as a 29-year-old technology stock analyst, I received illegal inside information from another investor on four occasions: three tips regarding upcoming corporate M&A deals and one tip with information about a company's quarterly earnings announcement. Based on the behavior I was observing in the industry at the time, I talked myself into placing the trades. "Who am I hurting?", "everyone is doing it," "I'm still a good person" -- the all too common excuses for unethical (or illegal) behavior. Ultimately, my faulty rationalizations led to a career ending, life-altering situation. In July 2008, I was approached by FBI agents on the street outside my apartment in Manhattan and presented the opportunity to help the U.S. government build larger cases. I became known as "Tipper X" and was credited with assisting the FBI in over 20 of the 80+ cases in Operation Perfect Hedge, a Wall Street house cleaning campaign that morphed into the largest insider trading investigation of a generation.

Having no plans to ever speak about my experience (who would want to talk about the worst thing they ever did to an audience?), I was asked by the FBI in 2016 to speak to their rookie agent class about my case, and from there I have made it my life's mission to assist risk and compliance officers in the training of staff. More than just "scaring them straight," my goal is to educate on exactly what I was thinking as a young professional, by exposing the extremely faulty rationalisations I made and then showing how risk, surveillance and compliance professionals can keep their employees from suffering the same fate. From my own experience and through now 150 speaking and client consultations over the past two years, below are some areas for firms to consider with regard to minimising conduct failure and better managing human risk in the organisation:

Isolated desicion making

When I received illegal inside information, I went through a poor series of rationalisations to justify the trades. The bigger picture takeaway here is I engaged in "isolated decision making" and when I think about my behavior, and study the crimes of others in similar situations, one of the common threads to weave together is the idea of an individual making a decision, or several decisions, in isolation. I did not talk to anyone else at my firm before placing the trades. Firms today need to think about their exposure in the organisation to individuals who may be more prone to this type of decision making.

Thinly-supervised employees in remote offices

As I look at other individuals charged in the larger era of cases known as Operation Perfect Hedge and in my corporate talks today, another major takeaway to think about with regard to conduct risk are thinly-supervised employees who may be operating out of remote offices. In my presentations to firms with global office footprints, I sometimes find the line of questioning during my talks from younger professionals to be as to how close they can get to the line. I think extra education for younger professionals here is extremely important!

Importance of professional mentorship

In my 20s, I did not have a professional mentor. Had I spoken to anyone outside of my firm and explained what I saw occurring in the industry, the right person would have certainly guided me in the right direction. It's important for companies today to maintain either formal or informal mentorship programs for younger professionals.

Tone at the top vs. mood in the middle

Regulators worldwide, rightly so, are focused on tone at the top. However, I would argue from my experience that it's the "mood in the middle" that drives misconduct. Does what is said at the top in annual chairman letters and board meetings trickle down to how middle managers conduct day to day business and set goals and incentives?

"The cover up is worse than the crime"

It is vitally important to create a culture where people are not just comfortable raising issues but expected to raise issues. I feel the industry still has more work to do in this area.

Thomas will be discussing his story and recommendatins in more detail at RiskMinds Internatiomal this year.

IS TECHNOLOGY OUTPACING RISK MANAGEMENT?

Stephen Cobb

In 2017, two strains of malicious code negatively impacted a wide range of organizations in multiple sectors of industry, in scores of countries, across several continents. Known as WannaCry and NotPetya, these were by no means the only malware-based cyber crime campaigns conducted that year, but these two alone generated costs well into the billions of dollars; and they illustrated just how hard it is to manage the risks inherent in the massively complex, multi-dimensional matrix of digital technology upon which much of modern life now depends.

Given the rapid rate at which "digital transformation" is predicted to bring even more of such technology into organisations in the near future, it seems reasonable to ask whether or not technology is outpacing risk management. To help answer this question we can consider risk management in three parts: the discovery of risks, the assessment of risks, and the identification of suitable means by which to avoid or minimize the impact of technology risks.

Discovering the risks

Discovering the risks inherent in the deployment of digital technology is no easy task. Not only does it require skills and abilities that are in short supply, it takes a certain mindset as well. Consider what happened in January of 2018: the world learned of a serious vulnerability affecting some three billion CPUs, the Central Processing Units at the heart of computing devices, everything from servers to laptops, smartphones to tablets, even smart TVs.

As hardware and software vendors scrambled to respond to this unprecedented situation, two key data points for risk-minded analysts emerged: the vulnerability arose from chip design goals that prioritised performance over security, and the reason it took more than two decades to surface was because vulnerability researchers assumed "the chipmakers would have uncovered such a glaring security hole during testing and would never have shipped chips with a vulnerability like that".

Not only are technology risks technically difficult to discover, finding them requires constant questioning of assumptions. Consider cryptography, one of the linchpins of digital transformation. In 2017 we learned that millions of encryption keys, used for everything from software code-signing to national identity cards, were open to exploitation via a flaw in the way the encryption was implemented, despite being certified to multiple internationally-recognized security standards. That problem was around for five years before it was discovered.

Assessing the risks

Moving from the discovery of technology risks to the assessment of risks, things get even harder, largely because of a lack of good data. For example, while the US government can tell you how many banks were robbed in a year it cannot tell you how many cyber crimes were committed. Enquirers are referred to studies performed by commercial entities that sell security services – hardly an objective source (and furthermore, many commercial surveys use flawed methodologies and are not consistent over time, making it very difficult to tell if things are getting better or worse, and by how much).

Vendor studies of technology risk can lead to a skewed focus on each new threat wave for which solutions have been developed. The cumulative nature of technology risks is obscured. For example, ransomware for commercial gain was the center of attention when NotPetya struck, but NotPetya was brickware– a system destroyer – not ransomware; moreover, it had geo-political objectives yet inflicted damage on commercial systems. In response there was new focus on the risks from state-aligned attacks, but we recently detected new brickware, posing as ransomware, written simply for bragging rights – the motive for most of last century's malware. In other words, from a cyber perspective, technology risks are cumulative, unpredictable, and inadequately quantified.

Minimising the risks

When it comes to identifying the means to avoid and minimise the impact of technology risks, cyber security conferences like Black Hat or RSA are one place to look. In recent years vendors at these events have been betting big on artificial intelligence (AI) as the latest and greatest hope for defeating cyber criminals and managing technology risks. However, the case for AI solutions, as articulated by their developers and backers, often boils down to this: technology is now so complex that we cannot rely on humans to safely manage and defend it.

This does not bode well for the future of risk management if you look at AI in the light of four things we know about humans and technology: humans consistently over-estimate the net benefits of new technology; early warnings about technology risks are usually ignored; many technology threats are asymmetric; and many bad actors – both criminal and state-aligned – are now highly skilled, well-funded, and blurring the lines between crime, espionage, and geo-political aggression.

The collision between these realities and the risk-reduction potential of AI is impressively documented in "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation" a report by a large group of experts that appeared in February of 2018. The scenarios they outlined should concern every CRO. For me, the likely scenario is this: organisations will rely too heavily on AI-based security that is then defeated by the malicious use of AI, whose development efforts are not hampered by constraints like false positives and accidental damage to systems and data.

In his 2018 RSA Conference keynote, the CEO of RSA Security warned: "Our collective risk as an industry is that we fail to avoid a breach of trust in technology itself." Just a few days earlier I had surveyed American adults, asking: "How much risk do you believe criminals hacking into computer systems pose to human health, safety, or prosperity?" A solid 70% rate the risk as either serious or very high.

That survey was conducted before the FBI warned Americans that unspecified bad actors are now using powerful multi-stage malware to take over their routers. More than 100 million US households and small businesses use a router to network their computers, tablets, and other digital devices, like "smart" phones, thermostats, alarms, cameras, door locks, and TVs. Many people are just now learning how hard these devices are to secure, and how much damage they can do in the wrong hands.

In short, technology risks are getting harder to find, measure, and avoid. At the same time, we face a rising tide of digital transformation – including bold new technology like AI and 5G – even as stormy geo-political conflicts are increasingly acted out in cyberspace and criminals get ever more cyber-savvy. It is hard to see how risk management will be able to keep pace.

JOIN THE CONVERSATION
#RISKMINDS