Cyber Risk Management:

Does cyber risk get enough boardroom airtime?

Camms.

Software to change tomorrow.

Part 1

The ever-growing threat posed to businesses by cyber-attacks

As Benjamin Franklin once said: "Out of adversity comes opportunity". Unfortunately, for businesses the world over the rapid spread of Covid-19 has created a perfect storm for cybercriminals – fear, uncertainty, vulnerability, widespread remote working and increased online activity – who have seized this opportunity to escalate their nefarious activities.

Has it taken a crippling global pandemic for cyber risk to evolve from an IT issue to a top board priority and for organisations to realise the importance of establishing a proactive cyber risk strategy? It is not as if cyber-attacks were not on the risk radar before the pandemic. Awareness of the cyber threat has grown rapidly in recent years, driven by businesses increasing reliance on data and IT systems – and an escalation of high-profile incidents.

The rise of cyber risk

The first cyber-attack to hit the headlines was a complete accident, devoid of any malicious intent. In 1988, Robert Tappan Morris – a graduate student in the US – created a computer programme to assess the size of a relatively new creation called the internet. Unfortunately for Robert, he was unaware of what his creation was capable of, causing it to inadvertently execute the world's first Distributed Denial of Service (DDoS) attack – infecting up to 60,000 computers. Over 20 years on from this mishap, the exponential growth of the internet – and our reliance on it – has meant cyber-attacks are no longer avoidable mistakes; they are a sophisticated and coordinated assault on our private data.

New digital technologies offer a litany of advantages and opportunities for businesses – from an increase in productivity and efficiency to larger markets in which to operate. But they also open the door to cybercriminals who attempt to exploit them using innovative methods. Cybercrime's sophistication and scope subsequently evolve with the new technologies that enable it. Take cryptocurrencies and anonymous browsers, for example, which facilitate the proliferation of cybercrime by protecting criminals' identities – allowing hackers to extort money without leaving a footprint.

By its very nature, cybercrime must evolve to be effective. This means cybercriminals are constantly developing innovative attacks to fit new trends while tweaking existing attacks to avoid detection. So, as modern IT infrastructures become increasingly complex and the attacks used to circumvent them follow suit, the amount of virtual ground that needs safeguarding is constantly expanding.

The growth of cyber risk

It is easy to get bogged down in the numbers when researching the amount of cybercrime in the world, such is the volume of stats available on this hot topic. However, it all confirms one thing: the number of cyber-attacks has been on an upward trajectory since the start of the millennium – and is showing no signs of stopping.

This has caused cybercrime to evolve into the world's biggest criminal growth industry – it is estimated that global cybercrime cost will reach $10.5 trillion annually by 2025, up from $3 trillion in 2015 (Source: Cybercrime Magazine). If we scratch the surface of this data, we can see how cybercriminals are conducting these malicious attacks and the alarming rate they are increasing at:

Business detections of ransomware rose 365% from Q2 2018 to Q2 2019.

Source: Malwarebytes

Spoofing or business email compromise attacks against businesses rose by 250% in 2018.

Source: Industry Week

Nearly 90% of global organisations were targeted with business email compromises and spear phishing attacks in 2019.

Source: Helpnet Security

This pre-pandemic proliferation of cyber-attacks was causing quite a stir: in their 9th Risk Barometer, Allianz ranked cyber incidents (39% of responses) as the most important business risk globally for 2020 – knocking business disruption off the top spot for the first time in seven years. Back in 2013, cyber incidents ranked only 15th with just 6 per cent of responses. Allianz highlighted that cyber incidents have become more damaging and expensive for businesses – often resulting in lawsuits and litigation after the event.

Cyber-attacks have not only gained notoriety because of their sheer volume; the financial impact has proved relentless as well. For example, US organisations face the highest data breach costs in the world with an average of $8.64 million per breach – up 5.3% from 2019. In the UK, the cost is $3.9 million and in Australia it is $2.15 million, which represents an increase of 4% and 9.4% from 2019 respectively.

Source: Capita

The growing scope of cyber-attacks

The pervasive nature of cyberattacks is not the only reason the financial cost of cybercrime is rising; their scope is also expanding – making them an existential threat to some businesses. Organisations of all sizes are at risk of cyberattack – 43% of attacks are aimed at small businesses, many of which lack the resources required to combat them or recover once compromised. However, it is incidents that target large organisations with vast customer bases that grab the headlines.

Source: CNBC

There was a time – not so long ago – when a breach that compromised the data of a few million people would have been big news. Today, however, these are an all-too-common occurrence that pales into insignificance when compared with some of the mindboggling numbers linked to high profile breaches.

The top three breaches of the 21st Century, in terms of the number of people whose data was compromised for malicious intent, are:

Adobe:

In October 2013 it was reported that 153 million user records had been compromised.

Adult Friend Finder:

In October 2016, 412.2 million customer accounts were compromised.

Canva:

In May 2019, 137 million user accounts were compromised.

Source: CSO Online

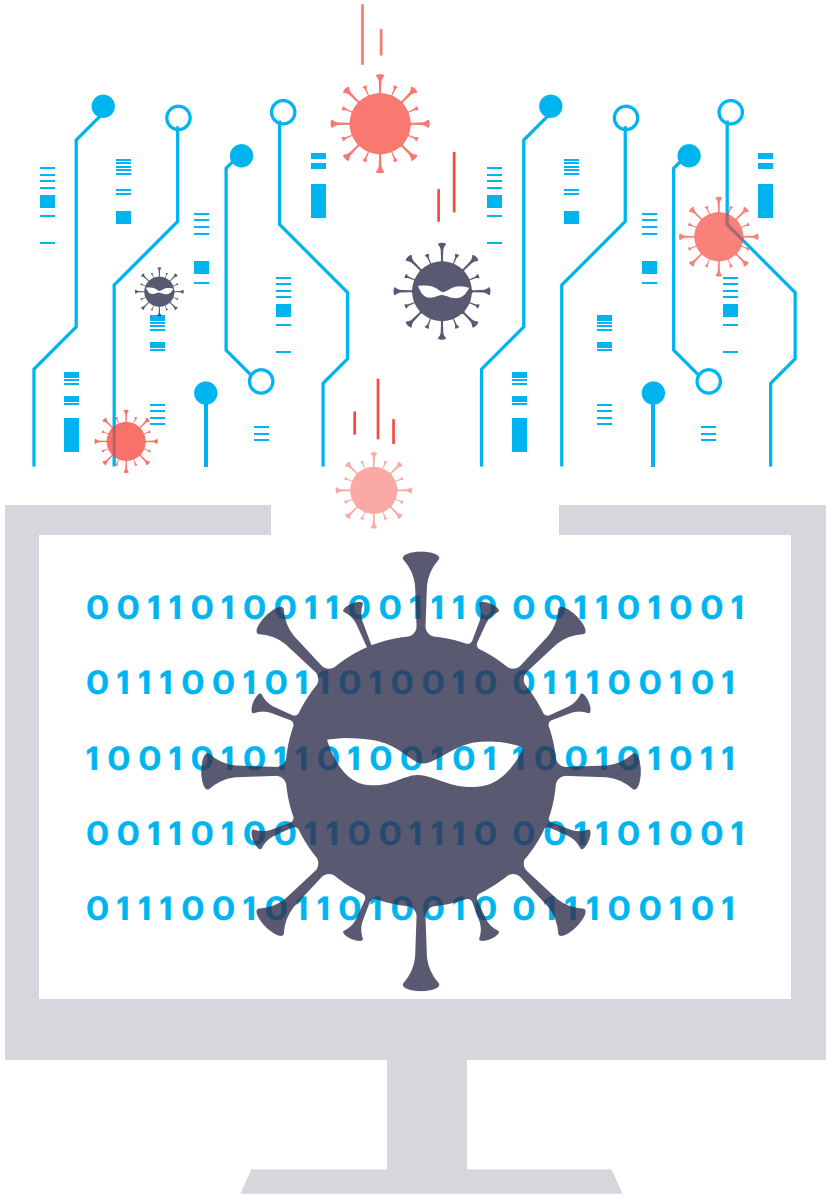
As you can see, the cyber threat landscape was already a rocky one before the Covid-19 pandemic struck in March 2020 – when things went from bad to worse.

Covid-19

Boards that still needed persuading about the merits of establishing a proactive cyber risk strategy that considers the entire business, were left in little doubt after the rapid spread of Covid-19 blindsided society. The pandemic was like a slap in the face as it suddenly reshaped the workplace landscape overnight. Businesses were forced to shutter their doors and shift to remote working at scale, following the introduction of emergency lockdown measures across the world. As business models altered and digital footprints expanded, the attack surface suddenly widened for cybercriminals.

Cyber-attacks have subsequently escalated in frequency and scope in the wake of lockdown restrictions, first implemented in March 2020. These unscrupulous individuals are cashing in on increased workloads, unfamiliar ways of working and heightened stress levels by developing themed phishing and social engineering attacks that use Covid-19 as bait – and the impact is staggering. In March 2020 alone, email scams related to Covid-19 surged 667%. By May, almost half (46%) of global businesses had experienced at least one cybersecurity threat, and the FBI had identified an 800% increase in reported cybercrimes. Third-party cyber risks also began expanding due to supply chain disruptions caused by lockdown restrictions and the subsequent need to seek new vendors.

This cyber onslaught against businesses throughout the world and across all industries poses the question: what is at stake for them?



Part 2

What are the consequences of cyber-attacks?

Cyber-attacks are often labelled a white-collar crime. According to the FBI: "These crimes are characterized by deceit, concealment, or violation of trust and are not dependent on the application or threat of physical force or violence. The motivation behind these crimes is financial – to obtain or avoid losing money, property, or services or to secure a personal or business advantage."

So, are corporate cyber-attacks victimless crimes because no one gets hurt? This depends on what your definition of getting hurt is. Ask this question to the board of any business that has fallen victim to an attack, and they will confirm that the financial, operational, and reputational implications can be crippling.

Intellectual property losses

Intellectual property (IP) is the lifeblood of many businesses, supporting innovation, growth, and differentiation. However, it is customer information theft that grabs all the headlines, whereas IP loss is among the hidden or less visible costs of a cyber-attack. The difference between the two is simple: the business owns the IP – this might include patented information and trademarked material, client lists, and commercially sensitive data. Therefore, they may have an obligation to shareholders and stakeholders to identify what has been stolen, review the potential impact and loss, and seek potential recovery as quickly as possible.

A deleterious trait of the malicious software used during cyber-attacks is the difficulty of detection. Attacks – and subsequent data theft – can occur for an extended period before the victim detects their IP is being compromised. Significant IP theft can, therefore, have a devastating impact on a business's competitive advantage.

All too often, management are only required to provide IP reports to the board of directors infrequently or, worse, when litigation is on the horizon. Thankfully, the current corporate governance climate is bucking this trend by imposing higher expectations for board oversight and more risk of personal liability when directors get it wrong. Consequently, IP management must be considered a primary issue for oversight by the board – and cybersecurity should underpin this.

Legal expenses

The escalation of the cyber threat has brought regulatory standards into sharp focus for corporate decision-makers. Regulators expect personal information to be protected and systems to be resilient to both accidental data leakage and deliberate attacks. Recent regulatory changes, such as the US Securities and Exchange Commission's cybersecurity guidance and new data privacy laws – most notably the General Data Protection Regulation (GDPR) in the EU and the California Consumer Privacy Act – have shone the spotlight on business's risk focus for cybersecurity and data privacy.

According to the UK's National Cyber Security Centre: "the General Data Protection Regulation (GDPR) requires that personal data must be processed securely using appropriate technical and organisational measures." Under the GDPR, businesses that target or collect data related to people in the EU must manage risk appropriately. Failure to comply can result in significant financial penalties.

A total of €158.5m ($193.4m / £142.7m) in GDPR fines were imposed in the 12 months from 28 January 2020 – a 39% increase on the previous 20-month period. Let's take a closer look at three of the biggest fines since the regulation was applied on 25 May 2018:

Source: DLA Piper

Google: In January 2019, the French National Commission on Informatics and Liberty fined the tech giant €50 million – the biggest GDPR fine to date – because people were "not sufficiently informed" about how Google collected data to personalise advertising.

Source: CNIL

British Airways: In October 2020, BA was fined £20 million by the Information Commissioner's Office (ICO) – reduced from £183 due to the economic impact of Covid-19 – for a personal data breach that compromised more than 400,000 customers.

Source: ICO

Marriott International: In July 2019, the ICO issued an intent to fine the hospitality company more than £99 million – reduced to £18.4 million due to the pandemic – for a major data breach resulting from a cyber-attack that may have compromised the personal details of up to 339 million guests.

Source: ICO

Significant data breach fines are a wake-up call for boards to prioritise cybersecurity. Money talks, and in a post-GDPR world, businesses with lacklustre security are being forced to finally take notice of this very real threat – and implement proactive measures that mitigates it.

Reputational damage

Reputation is fragile in the corporate world. American investor, business tycoon, and philanthropist Warren Buffet famously said: "it takes 20 years to build a reputation and five minutes to ruin it... If you think about that, you will do things differently". Wise words, especially when considered in the context of cybercrime. Trust is an essential element of the customer relationship; if that trust is eroded by a cyber-attack, reputation will be damaged in an instant.

Society is connected like never before – not only does this mean the attack surface is growing exponentially for cybercriminals; it means bad news travels fast. An avoidable breach that compromises customer data can have a devastating and long-lasting impact on a business: lost confidence, negative press, identity theft, and difficulties attracting new customers, future investment, and new employees. According to CISCO's Benchmark Report 2020, the number of organisations that have reported reputational damage from data breaches has risen from 26% to 33%.

Boards have traditionally viewed reputational risk as an outcome: the result of other core business-related risks, such as cybercrime. The logic being: if we take care of those other risks, reputation will take of itself. However, the failure of boards to provide cyber risk management with the necessary oversight often hampers this approach.

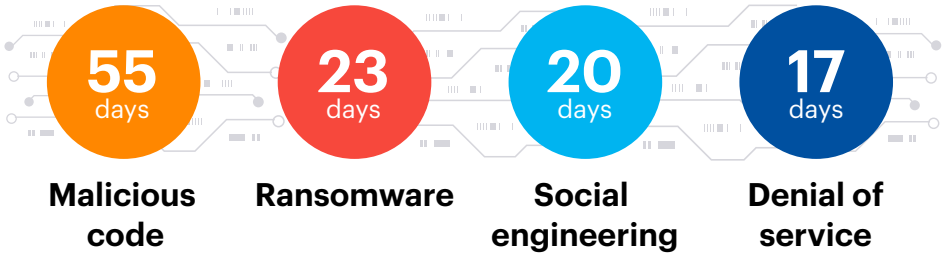
Business disruption

While proactive cybersecurity measures that prevent incidents from occurring must be the board's priority, reactive provisions should also be made. A cyber incident response plan is a set of actions that not only enables a business to detect cyber-attacks in a fast and coordinated manner; it also provides a roadmap for responding to them effectively. Unfortunately, they are often overlooked: in the UK for example, 70% of organisations currently do not have a plan in place, leaving them exposed to business disruption in the event of an attack.

Source: IT Governance

Any business that is the victim of a cyber-attack must take the time to investigate how it occurred and what information (if any) was lost, before reporting the incident to the relevant regulatory authority – keeping shareholders informed throughout. For example, Article 33 of the GDPR requires organisations that have identified a breach to "where feasible" notify the appropriate supervisory authority within 72 hours of becoming aware of it. This process often requires them to refocus vital resources, which can have a detrimental impact on business efficiency.

The average time it takes businesses to resolve cyber-attacks once they have been detected is staggering:



Source: Accenture

This is made more concerning when we consider that on average it took organisations 207 days to detect a breach in 2020, giving cybercriminals almost seven months to harvest and exploit compromised information.

Source: Capita

Administrative cost

The financial implications of cyber-attacks are significant and varied: legal costs, business disruption costs, the cost of reputational damage. There is another cost that must be taken into consideration if a business fails to prevent itself from becoming the victim of cybercrime: administrative costs. These are required to correct the impact of an attack, such as rebuilding client confidence, communicating with the relevant authorities, and restoring the organisation's business to previous levels.

It's one thing knowing how pervasive cybercrime has become over the last two decades, but it's up to those that sit at the head of a company (the board of directors) to understand how pernicious the impact can be. Cyber-attacks can present near existential threats to a business. Any other scenario with the potential to disrupt operations, damage reputation and generate costs to this degree would be identified and managed as an important business risk by the board. Take the US for example, where just one in three mid-market companies reviews cyber risk and management at board level or has a board member with specific responsibility; and around six in ten do not have a cyber incident response plan in place.

Source: Grant Thornton

Part 3

What is the role of the board?

Cybercrime is not a burgeoning criminal industry; it is an established threat with severe consequences that cannot be ignored by businesses – and it is up to the board to lead the fight back. The ever-widening attack surface has forced investors and regulators to increasingly challenge boards to extend their oversight of cybersecurity and provide greater transparency around major breaches and their impact on the business. To achieve this, they must recognise that cybersecurity is one of the top enterprise-wide risk management issues facing their organisation – not just an IT issue – and understand the potential consequences of failing to mitigate cyber-attacks. This will help them establish a proactive cybersecurity strategy that's underpinned by the business's most valuable asset: people.

Traditionally, boards have associated cybersecurity solely with IT – a rigid approach that fails to recognise that it is a business risk issue, not just a technology issue. However, the evolution of the modern risk landscape means they now have a duty to oversee the management of cybersecurity – including oversight of appropriate risk mitigation strategies, systems, processes, culture and controls. Get this right and cybersecurity can do even more than safeguard the business; it can create opportunities to find new revenue streams and innovate – rather than being an overhead cost.

The board's duties generally fall within six categories in the context of cybersecurity, which are illustrated in the graphic below:

Governance

To ensure their organisation is both secure and resilient, the board must play a leading governance role in cyber risk management and decision making. Effective corporate governance starts with the board's ability to understand the issues and risks the organisation is facing today and into the future.

The astronomical fines dished out by global data regulators – the UK's ICO, the US Federal Trade Commission and the Australian Privacy Commissioner – in recent times have caught the attention of corporate leaders. These self-inflicted wounds are helping organisations recognise the importance of boardroom leadership on cyber risk. They are becoming acutely aware that adopting a proactive approach to improving cybersecurity governance – joining the dots between IT and the business to prevent cyber-attacks from occurring – can help them address the evolving threat and implications of a major cybersecurity breach more selectively.

How the board organises itself is also essential to effective governance. Increasingly, boardroom leaders are coordinating their efforts through focused cybersecurity committees. This facilitates effective channels of communication, enabling them to provide management with a clear perspective of how the business could be impacted and ensure they have the skills, resources, and process in place to mitigate cyber-attacks – and potential damages.

Strategy and Risk

Organisations with a blinkered view of cybersecurity – those that look at it solely through a technological lens – will be limited to technical reporting that lacks an enterprise-wide strategic overlay. For effective oversight, boards should challenge senior management to establish a clear and concise cybersecurity strategy, along with systems and controls to monitor its implementation. This requires effective communication between the board and management that facilitates the sharing of accurate and useful information, including metrics to track performance and provide accountability.

The board is ultimately accountable for overseeing the application of an appropriate cybersecurity strategy – key responsibilities include:

- Establishing their organisation's appetite for cyber risk.
- Defining the outcomes that are most important to guide cybersecurity investment.
- Fostering a culture of cybersecurity and resilience.

There is no "one-size-fits-all" cybersecurity strategy because no two businesses are the same. However, the US National Institute of Standards and Technology's cybersecurity framework provides five functions that can be communicated by the board to those responsible for developing and implementing the strategy: the management.

This will provide a solid foundation from which they can build:

Identify
Develop an organisational understanding of the overall cyber risk context.

Protect
Deploy safeguards to prevent intrusions.

Detect
Enable timely discovery of a cybersecurity breach to limit the harm from intrusions.

Respond
Implement plans and activities to contain any damage resulting from a cybersecurity breach.

Recover
Develop plans and activities to resume normal operations following a cybersecurity event.

Boards should encourage a risk-based approach to their cybersecurity strategy. Unlike a prevention-based approach – which acts as a flimsy perimeter defence against a variety of threats – this focuses on prioritising and protecting key assets: third-party information, intellectual property and critical process control networks. Because they are more bespoke, risk-based defences can detect and respond to threats before assets are compromised and stop cybercriminals from inflicting other forms of disruptive and reputational damage.

Talent

Traditionally, corporate boards comprise of Chief Executive Officers and financial or sector experts. More recently, the proliferation of cyber-attacks has raised the level of awareness for cybersecurity oversight. Many organisations have realised that to maximise shareholder values, they must treat cyber risks as business-level risks at the highest governance level.

In the US, for example, the National Association of Corporate Directors (NACD) has stressed the need for corporate boards to improve their cybersecurity proficiency and governance capabilities. In its "Director's Handbook for Cybersecurity", NACD states: "All boards should have the ability to understand cyber threats and assess management's capability of dealing with cyber-related issues".

Shareholders have also been pressurising boards to strengthen cybersecurity oversight: a report by Gibson Dunn reveals that 36% of all shareholder proposals (the largest subcategory) during the 2018 proxy season sought social or environmental performance measures, which include cybersecurity and data privacy, in executive compensation.

To address this, the board might support a shift in focus for the incumbent Chief Information Security Officer (CISO) from a traditional technical approach to information security to a more business-focused, risk management mindset; or they might create a Chief Cybercrime Officer (CCO) role, who – working in harmony with the CISO – will provide a link between the board and the rest of the company to mitigate cyber risk and work collaboratively to resolve issues as they arise.

Compliance

The board must know what cyber regulations, laws and standards apply to its sector and business, before establishing an effective governance structure with clear accountabilities. This will foster a culture that reinforces better cyber risk and compliance management across three vital layers: business and operations, compliance and risk functions, and audit.

For example, the UK's Financial Conduct Authority describes compliance with the GDPR as a boardroom responsibility and requires organisations to produce evidence to demonstrate the steps that they have taken to comply if requested – essential actions that will help mitigate enforcement measures. Similar laws now apply to personal data security in California, with more to follow elsewhere.

Culture

Cybersecurity should be managed through the lens of the entire organisation – and it is up to the board to set the tone. For positive values and behaviour to permeate through the organisation, the board must lead by example. Each employee must understand that everyone has an equally important role and obligation to protect the organisation from cyber-attacks. This will foster a culture of accountability, collaboration and education, with all efforts geared toward supporting the cybersecurity strategy and mitigating risks.

The holy grail of a top-down and bottom-up culture can only be achieved with effective channels of communication and it is up to the board to establish them – from consulting the wider business on policies and processes to spreading the cybersecurity message throughout the organisation. Failure to achieve this will leave stakeholders at all levels feeling disenfranchised and disengaged.

Ensuring the board is engaged with cyber risk

For the board to be able to meet these requirements they must be engaged with cyber risk. This will enable them to understand the importance of cybersecurity to the organisation and why they should be involved – rather than simply paying lip service to it. To achieve this, several key factors must be addressed to provide relevant information to the board:

- Integrate cybersecurity into the organisation's objectives and risks to build trust and create value.
- Ensure key performance indicators for cybersecurity are not highly technical and unrelated to what is important to the business. This will facilitate the integration of cybersecurity into the organisation's objectives and risks, by highlighting their business value – such as customer satisfaction and reputation.
- Promote assurance and accreditation frameworks that demonstrate the organisation's cyber risk is under control. Cyber posture assessments can be used to communicate cyber risk management practices and principles clearly and concisely, while still providing the necessary assurance.
- Aggregate cyber risk so it is dealt with at the relevant level of the organisation. This can be achieved by assuring the appropriate level of information is contained in the strategic risk register and feeding it into the relevant risk profiles. Consider how this information will be cascaded down into operational risk registers and incorporated into resource allocation decisions.

Part 4

The role of an integrated risk management system

Having understood and accepted the level of threat posed by cyber risk, the board must explore innovative and proactive countermeasures. Business solutions are vital tools for managing cyber risks, strategies and projects. The challenge is integrating software that can drive meaningful decision-making from a risk perspective using data that is aligned to business objectives and KPIs. Achieve this and the business will be well-placed to adapt and be resilient during normal business operations and through disruptive events. With integrated solutions in risk, strategy, projects and people, Camms business software helps organisations make the right decisions, manage risks and align their talents.

Camms.Risk – a cloud-based SaaS solution – enables organisations to drive risk, incident and compliance management across all IT systems and processes. The solution uses a modular approach, allowing organisations to scale and mature their risk management processes at their own pace without the need to purchase disparate systems to cater to different requirement. **Camms.Risk** comprises seven modules:

Risk, treatment and control management
Embeds cyber risk management into the business's culture, so it can identify, track and manage risks effectively.

Audit management
Schedules and manages internal and external audits and utilises the results.

Incident management
Facilitates incident and near misses reporting in real-time, and the investigation process post-event.

Compliance management
Identifies areas of non-compliance to drive business action and address legislative changes.

Stakeholder dashboarding
Intuitive functionality provides executives and the board with key information when they need it.

Analytics and ad hoc reporting
Built-in dashboards and standard reports provide critical insights and executive reporting.

API integration and library
Seamlessly integrates all Camms software with your broader IT ecosystem and transfers data both in and out of our solutions.

Adopting a comprehensive approach to managing cyber risk will facilitate the transparent flow of relevant information from the top-down, and the creation of a proactive cybersecurity culture from the bottom-up – empowering the right people to make the right decisions at the right time. Never has this been more important to a business's current and future success. As cyber-attacks become more sophisticated and prevalent – a perpetual trend that requires proactive action – and the consequences cause increasing financial, operational, and reputational damage, boards must engage with and extend their superintendence of cybersecurity.

Camms.Risk provides them – and the business as a whole – with the right level of oversight and action on cyber risks by integrating it into enterprise risk processes, making the business more resilient.

Driving positive change using technology

Camms business solutions have the power to integrate meaningful risk, strategy, project, and people solutions, helping you make the right decisions, manage risks, align talent and focus on what matters.

Our team would love to learn about your company and its 2021 risk and resilience needs. Request a demo with us today!

Request demo

Camms.

Software to change tomorrow.

cammsgroup.com