H2-2022

SNAPSHOT

Developments in Cyber Risk Regulation

And How They Affect You

SAFE

INTRODUCTION

In March 2022, the US Securities and Exchange Commission (SEC) proposed landmark amendments to its existing rules to enforce better preparedness and resilience among global organizations. This sparked discussion among regulators across the globe – much of which we can observe in recent guidelines released during the second half of 2022.

The SEC proposals are significant. The move reflects grave concerns that global organizations are not managing cybersecurity risk effectively. Some commentators see a successful vote as the SEC foraying beyond disclosure regulation and using its position to directly mandate cyber risk quantification through regulation. Industry analysts and thought leaders such as Forrester, Gartner, Deloitte, and IDC have all weighed in on risk quantification during 2022, so it is unsurprising to find it in some guise within other, more recent regulatory developments.

The immediate future seems clear: global organizations will be required to adopt a more proactive approach to cyber risk reporting and disclosure of security gaps and breaches. However, rather than it being voluntary – as it has been up until now – leaders should expect to see these activities become legal mandates.

The most commonly deployed cybersecurity risk management solutions are not equipped to facilitate this shift in cyber risk reporting. This is why commentators, experts, and analysts are pointing towards Cyber Risk Quantification and Management (CRQM) as the solution to the broken state of cyber risk management – which is why it could play such a critical and pivotal role in any global organization's approach to these new regulatory mandates.

GLOBAL REGULATIONS AND HOW THEY AFFECT YOUR ORGANIZATION

Four themes have emerged across recent global regulatory developments:

1. Responsibility and accountability for cybersecurity risk, disclosure, and the impact of any breach, rests firmly with the organization's board.
2. Businesses should have a comprehensive and real-time view of their cybersecurity gaps and vulnerabilities. All stakeholders should know how efficient their cybersecurity strategies are.
3. Organizations that do not meet regulatory requirements, or fail to provide information in a consistent, comparable, and decision-useful manner, will face significant penalties.
4. Global commentators suggest that some regulators are moving towards mandatory cyber risk quantification.

In this review, explore the global developments in regulatory guidelines, what they mean for your organization and how cyber risk quantification can address these challenges.

DEVELOPMENTS BY REGION

THE UNITED STATES OF AMERICA

MARCH 2022: Two significant developments were announced: **The U.S Securities Exchange Commission (SEC) Proposal** and the **Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA).** The SEC proposal is intended to mandate cybersecurity risk disclosure, and CIRCIA is intended to provide the US federal government with a better informed approach towards cybersecurity breaches and ransomware attacks.

Whilst CIRCIA has already been signed into law, discussions on the SEC proposals continue with a decision likely to take place in 2023.

The proposed requirements	What this means for your business	How Cyber Risk Quantification and Management (CRQM) addresses the challenge
The proposal calls for mandatory, ongoing disclosures on companies' governance and risk management related to cybersecurity risk.	Technical cybersecurity data will no longer serve its purpose unless it is supplemented with the business impact of cybersecurity risk. You must be able to answer: *"What is the financial consequence of your cyber risk posture?"*	It enables you to calculate the estimated financial risk your organization faces due to cybersecurity gaps. You are also able to compare your organization's exposure vis-a-vis your industry benchmark and best practices.
SEC: The public company must disclose the incident within four days of a determination that an incident has taken place. CIRCIA: Critical infrastructure entities will have to report material cybersecurity incidents and ransomware payments to the CISA within 72 and 24 hours, respectively.	Your security team must have always-on, continuous visibility of enterprise-wide cybersecurity risk. You must have the capability to receive real-time alerts of cybersecurity breaches.	It provides continuous, dynamic, and real-time cybersecurity risk posture analysis to keep you informed of significant risks. When significant drops or changes in your cyber risk posture occur, such as an incident or breach, your CRQM platform will inform you immediately.
Ensure the senior management is effectively controlling known and unknown cybersecurity gaps.	Board oversight of cybersecurity initiatives is no longer optional. All members of the board must conduct and document their due diligence of enterprise cyber risk management strategies.	CRQM platforms give you visibility of where the greatest cybersecurity risks lie, and the understanding of the potential financial impact to the business. This enables informed decision making at both the CISO and Board-level to deploy more effective cybersecurity programs. You're also able to perform risk simulations for various cyber risk scenarios within your CRQM platform to understand the risk your business faces and reduce your exposure.

EUROPE

JUNE 2022: Digital Operational Resilience Act (DORA) is one of the most far-reaching regulatory updates to be introduced by the EU, targeting the internal approach to cybersecurity and resilience within organizations. Financial Services organizations are required to implement security controls that integrate overall resilience into their IT infrastructure. In addition, firms must use a governance-led approach to IT risk management through measures to enforce the identification and mitigation of cyber risks. The DORA framework is expected to come into effect during 2023.

The proposed requirements	What this means for your business	How Cyber Risk Quantification and Management (CRQM) addresses the challenge
Adopt and document regular digital testing measures.	Set-up and maintain resilient ICT systems and tools that minimize the impact of ICT risk. All sources of ICT risks should be continuously identified in order to set-up protection and prevention measures.	CRQM platforms automatically collect signals from assets within your estate and records your cyber risk posture over time. CRQM facilitates the move from manual, point-in-time testing to always-on, real-time analysis which can be produced on-demand to regulators and auditors.
Introduce an oversight framework for critical third-party providers.	With an increase in third and fourth-party vendors, your business will have to treat all external entities as extensions of itself and monitor their cybersecurity vulnerabilities.	Unlike other cyber risk management solutions, such as security ratings services, CRQM performs both an outside-in *and* inside-out analysis of third or 'nth'-party risk posture. This provides you with previously unknown visibility and critical data regarding the people, processes, and technology of your vendors.
Share information on cyber threat intelligence – security alerts, procedures and threat detection.	Organizations will require continuous and always-on monitoring of the external cybersecurity risk landscape and will need to compare this with the risk within their estate.	Advanced CRQM technologies can map internal cybersecurity vulnerabilities to the MITRE ATT&CK framework to establish where the greatest risks lie along the kill-chain.

NOVEMBER 2022: The Network and Information Security Directive 2 (NIS2) was passed to ensure a 'high common level of cybersecurity across the union'. It sets a baseline for cyber risk management and reporting obligations. NIS2 introduces stringent requirements for supply chain risk and places direct obligations on management bodies - such as the Board - to ensure effective implementation of the Directive.

Member states will have 21 months from entry into force to incorporate provisions into national law. Members can set out penalties for breaches of NIS2 of >EUR 10M or 2% of total global turnover (whichever is greater).

The proposed requirements	What this means for your business	How Cyber Risk Quantification and Management (CRQM) addresses the challenge
Entities must understand and regularly assess the vulnerabilities specific to each of their suppliers and service providers, the overall quality of their products and security practices, plus their secure development procedures.	Outside-in approaches are no longer enough and will not satisfy regulators. Organizations must quantify, address, and document the risk posed by third party vendors.	Advanced CRQM solutions offer both an inside-out and outside-in assessment of cyber risk to help you understand supply chain risk and target areas of critical concern.
Members of management bodies are required to follow regular training to gain sufficient knowledge and skills in order to apprehend and assess cybersecurity risk, and its impact on operations.	NIS2 imposes direct obligations on members of the Board and C-Suite to acquire the knowledge and skill to manage cybersecurity risk and manage its impact. Failing to do so may lead to personal fines and temporary withdrawal of managerial functions.	Education and training alone will not provide insight into the impact of cyber risk. Advanced CRQM solutions will give senior management the data and insights in a context that they will understand — turning technical analysis into estimated financial impact.
Entities must submit an initial notification within 24 hours of an incident being detected, followed by an intermediate update report. No later than 1 month after initial disclosure, entities must submit a detailed analysis of the incident.	NIS2 introduces specific requirements to be fullfilled at each stage of an incident. Firms must be able to provide detailed evidence proving readiness, resilience, and adherence to cybersecurity measures.	CRQM solutions document your cyber risk posture track the impact of your cybersecurity initiatives to help you document the before and after of an incident.
Entities should develop a culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced. Authorities will be granted powers to subject entities *at least* to: - regular audits based on risk assessments; - security scans based on objective, fair and transparent risk assessment criteria; - assessment of the cybersecurity measures adopted by the entity and evidence of policy implementation.	Cybersecurity risk management has been propelled to the forefront of the NIS2 Directive and specific activities have been mandated as a minimum baseline. Cybersecurity must be weaved into your organization's enterprise risk management practice. Not only must risk cyber risk management practices be defined, executed, and documented, but adherence and evidence of proactive execution of cyber risk management activities must be available upon request.	CRQM goes beyond traditional risk assessments by helping leaders move away from point-in-time assessments (which date almost instantly), to continuous assessment. Advanced CRQM solutions pull in telemetry from cybersecurity products already in-situ across your estate and aggregate the signals to provide your accurate, real-time cyber risk posture. This powerful automation makes both assessment and documentation available on-demand, ready for evidencing to regulators.

THE UNITED KINGDOM

NCSC-UK's annual release: Whilst not a regulation, NCSC-UK's advice echoes that of resilience and the importance of monitoring, assessing and prioritizing risk. It also suggests embedding cybersecurity as a core part of organizational risk management through use of regulation and other incentives.

Financial Conduct Authority (FCA) Operational Resilience Guidelines: Though released in March 2021, organizations had a milestone deadline to hit by 31 March 2022. The FCA stated that, "firms must have identified their important business services, set impact tolerances for the maximum tolerable disruption, and carried out mapping and testing to a level of sophistication necessary to do so. Firms must also have identified any vulnerabilities in their operational resilience".

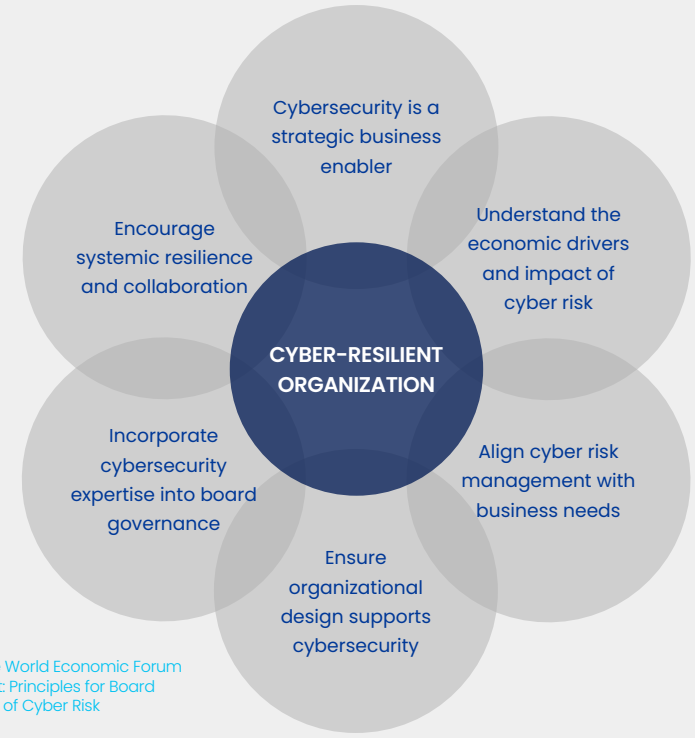
The proposed requirements	What this means for your business	How Cyber Risk Quantification and Management (CRQM) addresses the challenge
Map and test cybersecurity gaps to remain within impact tolerances.	Your business will first need to calculate its impact tolerance and compare it to industry benchmarks.	CRQM platforms empower you to measure the acceptable level of financial impact from cybersecurity incidents, including ransomware and data breaches.
Make necessary investments to enable consistent operations within impact tolerance.	Based on the calculated impact tolerance, your Board and Senior management will have to make decisions on risk management: add, remove, adjust security initiatives such as cyber insurance to remain within the threshold.	Advanced CRQM solutions suggest prioritized actionable insights to help you remain within your impact tolerance. This enables an approach that drives a better return on your security investments.
Identify vulnerabilities in operational resilience.	Organizations will be expected to defend their cybersecurity strategies in the event of a cyber attack. Board members and CXOs will be accountable for the cybersecurity posture of organizations.	Vulnerabilities are identified automatically using the signals collected from across your different technologies to establish the state of your operational resilience. In the event of a breach, CRQM platforms provide analysis of your cyber risk posture over time and documents the impact of your cybersecurity initiatives. CISOs and Board Members are equipped with the information they need to defend their strategies and prove their adherence.

AUSTRALIA

The Australian Cyber Security Agency (ACSC) released its annual report as a strong reminder that company boards should consider cyber resilience as part of their statutory responsibilities.

Its expanded **Security of Critical Infrastructure (SOCI) Act** will require critical infrastructure organizations to comply with new cyber risk management obligations.

The proposed requirements	What this means for your business	How Cyber Risk Quantification and Management (CRQM) addresses the challenge
Disclose operational and ownership information of assets and report cyber security incidents affecting critical infrastructure to the Australian Signals Directorate within 12 hours.	Your security team needs to possess continuous visibility of who owns and accesses each asset, why that access is required, and when it is used.	CRQM provides a continuous, always-on approach to managing cybersecurity risk related to access and ownership of critical assets. Real-time, dynamic, automatic, and continuous visibility will enable your business to remain proactive and promptly disclose any detected incidents.
Adopt, maintain, review, update, and comply with a critical infrastructure risk management program.	You will need to create and adopt a scalable, repeatable process for risk management which is regularly updated and centrally documented. You may need to move beyond manual documentation towards a more automated approach.	CRQM enables your business to automate cyber risk measurement and analysis. It provides and maintains a centralized repository of regulatory controls and drivers to help you fulfill your reporting requirements.
Submit an annual report within 90 days of the financial year-end to the relevant Commonwealth regulator.	Businesses dealing with critical infrastructure assets will have to create and send detailed annual reports of the measures in place to prove cybersecurity readiness and resilience.	Rather than pulling information and compiling reports manually, advanced CRQM platforms offer customizable report generation to provide information within minutes, on-demand, and in the language required by the regulator.



Source - The World Economic Forum (2021) Report: Principles for Board Governance of Cyber Risk

HOW CRQM PROMOTES CYBER RESILIENCE

CYBER RISK QUANTIFICATION AND MANAGEMENT

Ultimately, regulators are proposing and already implementing changes in the way that cybersecurity risk is reported. This is changing the state of play from a compliance perspective, but forcing change and improvement of the internal risk management processes within organizations themselves.

Cyber Risk Quantification and Management (CRQM) puts leaders from across the C-Suite, Board, Executive Committees, Risk, and Insurance firmly in the driving seat, **better enabling them to address questions from their regulators, investors, and customers – whilst making the most informed, data-driven decisions.**

CRQM for CEOs, CFOs, and Board Members:

- Understand the financial impact of cybersecurity risk on business revenue and growth.
- Gain real-time visibility to the compliance level of your cybersecurity plan against regulatory requirements.

CRQM for CISOs and CIOs:

- Confidently communicate your real-time cyber risk posture and impact tolerance to stakeholders.
- Integrate cybersecurity risk with operational risk management to ensure business continuity.
- Understand the return on investment across security initiatives: defense, mitigation, response, recovery, and insurance.

CRQM For Risk and Insurance Practitioners:

- Get a dollar-value metric to measure cybersecurity risk.
- Connect cybersecurity strategies to overall risk reduction and understand the risk being underwritten or transferred.

Safe Security enables organizations to proactively manage their cybersecurity risk with its advanced CRQM platform, SAFE.

To find out how it can help you transform your approach to cyber risk management, visit www.safe.security