The Who, What, When, and Why: Cyber Insurance – Mandatory or Optional?

In a Nutshell:

In 1666 the Great Fire of London turned fire insurance from a novel experiment into a cornerstone of urban risk management. It demonstrated that collective preparedness and pooled risk are essential to societal resilience. Today, the relentless surge of cyberattacks poses a similar challenge in the digital realm, forcing policy-makers and organisations to rethink how they manage cyber threats.

As economic losses mount, the debate over whether cyber insurance should become mandatory is intensifying across policy, legal, and risk management circles. Are we approaching a tipping point where cyber insurance shifts from a niche product to a standard, and potentially mandatory, safeguard in our digital age?

Who (would be impacted by mandatory cyber-insurance)**?**

Mandatory cyber insurance would have a widespread impact across various sectors and roles within organisations. All businesses and organisations, ranging from SMEs to large corporations, would be affected, especially those that handle sensitive data or provide critical services, as they face heightened cyber risks.

Decision-Makers: Within these organisations, key individuals responsible for insurance decisions—such as Chief Financial Officers (CFOs), Chief Risk Officers (CROs), Heads of Risk, Legal & Compliance officers, Procurement managers, and Chief Information Security Officers (CISOs)—would play pivotal roles in implementing and overseeing mandatory cyber insurance policies.

Regulators, Policymakers & Insurers: Beyond organisations themselves, regulators and policymakers considering minimum insurance standards would be deeply involved in defining and enforcing mandatory requirements. Insurers and brokers would also be significantly impacted as they adapt their coverage offerings, pricing, and market standards to meet new regulatory demands and customer needs.

Security Specialists: Finally, cybersecurity professionals, including advisors and risk officers, would play an essential role in managing organisational resilience and ensuring compliance with mandatory insurance frameworks.

Together, these stakeholders form an interconnected ecosystem that would collectively respond to the shift toward mandatory cyber insurance.

What (is at stake)**?**

Some proposals suggest making cyber insurance mandatory across the board, while others would see such mandates extend only to organisations exceeding a certain size, operating critical infrastructure, handling particularly sensitive personal data, or maintaining cross-border digital operations.

Cybersecurity insurance is not a monolith, with different policies covering different elements of risk. **Data breach coverage** covers costs related to forensic investigations, PR, notification- and legal costs resulting from a breach. **Cyber liability insurance**, on the other hand, provides third-party liability protection for damage caused by cyber incidents or ensuing third-party (customer) claims and legal

fees (especially relevant for service providers and digital platforms). Finally, **technology errors and omissions** (Tech E&O) policies cover failures or mistakes in digital products or services like software bugs, missed deadlines, contractual breaches, etc. (especially relevant for IT service firms and software vendors).

It is important to understand that cyber insurance *is not* a substitute for sound cybersecurity practices. Instead, insurance, whether mandatory or voluntary, must be seen as complementary, rather than an alternative to, robust cybersecurity hygiene.

As pointed out by Allianz, Swiss Re and Munich Re, cyber maturity is essential to qualifying for meaningful coverage. Considering that in Switzerland a mere 16-24% of organisations say that they are 'extremely confident' about their compliance with best practices around security and data protection, this may be cause for concern. Insurers insist that policyholders maintain documented, effective security controls (e.g. multi-factor authentication and endpoint detection) that go far beyond basic certifications like ISO 27001, demanding advanced measures and incident response plans. Where these controls are lacking or disclosures are incomplete, claims are denied (some reports indicate that as many as 44% of claims are rejected).

When (can we expect legislative decisions)**?**

- **Current status**: As of mid-2025, cyber insurance is not mandatory for businesses in Switzerland or the EU, though it is strongly recommended and sometimes effectively required through third-party contracts or sectoral regulation (e.g., in financial services).

- **Momentum**: Periodic regulatory reviews and public consultations are ongoing in several European countries with calls for mandates often peaking after major incidents.

- **Future outlook**: The question is expected to continue gaining traction as high-profile cyber-attacks and regulatory scrutiny increase, especially for organisations exposed to systemic risk or holding large amounts of particularly sensitive data.

Why (SHOULD cyber-insurance be made mandatory)**?**

- **Systemic Risk Management**: Universal coverage would pool risk across the economy, helping society absorb and recover from major cyber incidents (similar to car or fire insurance).

- **Raising the Baseline**: Cyber insurance requires organisations to meet minimum cybersecurity standards to qualify for coverage. This means that insurers have the potential to drive better security practices via coverage prerequisites (e.g., requiring multi-factor authentication, regular backups), improving the overall cyber hygiene of the business ecosystem and helping to reduce the overall incidence and impact of cyberattacks.

- **Protection Against Existential Risks**: Cyberattacks can threaten the survival of a business. Mandatory insurance would ensure that companies are financially protected from potentially catastrophic operational and reputational losses, much like how fire insurance is required for physical assets.

- **Protects Smaller Businesses**: Small and medium-sized enterprises (SMEs) are particularly vulnerable to cybercrime but are often least prepared. Mandatory insurance would provide a safety net for these organisations, helping them recover from attacks that could otherwise

be ruinous.

- **Financial Resilience**: Insurance ensures that all victims—not just the best prepared—have the resources to recover, minimising business closure or systemic supply chain collapse after large-scale attacks.

- **Regulatory Clarity**: A mandate could standardise expectations and close coverage gaps, especially for smaller firms that might otherwise neglect cyber risk.

- **Consumer Data Protection**: As more companies transact online and store personal data, mandatory insurance would encourage organisations to take greater care when handling consumer information, helping to limit the impact of breaches on individuals (data subjects).

Why (SHOULDN'T cyber-insurance be made mandatory)**?**

- **Market Readiness**: The cyber insurance market is volatile. Premiums are rising, coverage is narrowing, and many insurers exclude payouts related to ransomware or nation-state attacks (ransomware currently being one of the most common attacks). Mandating insurance could force businesses to buy expensive policies that do not actually protect them.

- **Compliance vs. Security**: There is a risk that a mandate could encourage a "tick-box" mentality, with organisations prioritising the purchasing of insurance over genuine investment in prevention and risk management (every dollar spent on insurance is a dollar that could be used on security).

- **Affordability and Access/ Cost Burden (especially for SMEs)**: Smaller companies or high-risk industries may find it increasingly difficult or cost-prohibitive to obtain meaningful coverage. Mandatory insurance could disproportionately burden SMEs with financial strain due to rising premiums. As the frequency and severity of attacks grow, insurance costs are expected to increase, potentially making compliance unaffordable for some.

- **Moral Hazard**: If insurance is universal and generous, some firms may underinvest in their own cyber defenses, relying on payouts to recover from incidents.

- **False Sense of Security**: Requiring insurance may lead some organisations to believe insurance alone is enough, reducing motivation to invest in robust prevention and detection steps (beyond what is required by the insurance company). Insurance is intended to be a last resort, not a substitute for real risk management.

- **Limited and Uneven Coverage**: Many cyber insurance policies have exclusions and may not cover key threats like ransomware payments, supply chain attacks, or business interruption. Mandatory minimum policies might offer only narrow protection, leaving companies underinsured or with misunderstood exposure.

- **Operational Complexity and Denied Claims**: Cyber insurance policies often require strict compliance with security controls and clear documentation. Claiming insurance can be time-consuming, complex, and sometimes unsuccessful if the insurer deems requirements have not been met or interprets policy exclusions narrowly.

- **Incentivises Higher Ransom Demands**: Cybercriminals may target insured companies with larger ransom demands, assuming insurers will pay (parallel to drug companies negotiating

with insurance companies on drug prices rather than end patients, resulting in exorbitant prices for certain drugs). This could further incentivise cybercrime and inflate overall costs for businesses and insurers alike.

- **Fragmentation and Complexity**: Different sectors have different risk profiles; a one-size-fits-all mandate may not suit all enterprises or industries.

Conclusion

The prospect of mandatory cyber insurance pits collective risk management and resilience against concerns about market maturity, affordability, and real security outcomes. Policymakers face tough choices: How can society be protected from the systemic impacts of cyberattacks without stifling business or fuelling a costly compliance arms race? As the debate evolves, organisations should expect growing pressure to demonstrate either robust cyber insurance coverage or equivalent risk management—whether mandatory or not.

Find out more:

- Cyber Insurance Denial: Why 44% of Claims Get Rejected (and How to Avoid It)
- Claims issues to watch: Cyber claims | AGCS
- Navigating the rising tide of latent cyber insurance claims: A call for vigilance and strategic action | Munich Re
- Reality check on the future of the cyber insurance market | Swiss Re
- Mid-year state of the cyber market update

Interested in what cyber insurance mandates could mean for your company?

Joshua Bucheli (cyberunity AG) and John Corona (Osmond GmbH) look forward to hearing from you!

Stay tuned for more – look out for our next cyberbyte issue!