Beyond Insurance: Mitigating Cyber Risk In 2022

JANUARY 2022

Luke Tenery
Partner, StoneTurn
ltenery@stoneturn.com
+1 312 775 1210

Thomas McEwan
Manager, StoneTurn
tmcewan@stoneturn.com
+1 202 609 8373

Ross M. Rustici
Managing Director, StoneTurn
rrustici@stoneturn.com
+1 617 570 3716

by Luke Tenery, Thomas McEwan and Ross Rustici

Over the past two years cyber liability insurers have made clear their intentions to move toward increased restrictions, clarifications and controls over the cyber insurance market and claims solutions to reduce their incident exposure and overall claims costs.

Reported ransomware payments have more than doubled year over year since 2016, exploding in 2020 to exceed $400 million and reaching $590 million in the first half of 2021.[1] Some experts have blamed cyber insurance as subsidizing criminal activity.[2] In response to this, many major providers are cutting coverage in half while doubling premiums.

They are also devising and implementing additional exclusions specifically to protect themselves, including mandates for insureds to maintain their own cybersecurity programs and adding coinsurance requirements as leverage to force improved cyber-hygiene and incident response performance, while leaving insureds more exposed to the most common cyberattacks.

This trend is likely to expand in 2022 with more insurers looking to reduce their outlays around cyber and place a greater cost on the insured. This poses significant concerns for corporations that have previously relied upon insurance as a significant pillar of their mitigation and recovery plans. Going forward, insurance payouts will likely be smaller while the costs for coverage will increase.

Those that fail to adapt to this new state of play will find themselves with increasing exposure and liability without any source of significant commensurate

StoneTurn

remuneration. Should insurance policy coverages recede, preventive cybersecurity will become even more imperative and ideally cost-effective.

Transforming risk reduction policies from ones that outsource the financial burden to those that create a solid IT security foundation on the front end will end up paying dividends as the insurance market continues to adjust.

What will the new normal look like?

Starting in February 2021, insurers were looking to limit the costs associated with their cyber policies. London insurers[3] were discussing accelerated multi-year rate corrections, and the New York Department of Financial Services issued the "Cyber Insurance Risk Framework," calling on insurers to take more stringent measures in underwriting cyber risks.

In August, American International Group Inc. successfully introduced ransomware limits, coinsurance requirements and exclusions to its policies, all while expecting policyholders to absorb half the cost of losses written below the $30 million mark, acting as one of the first insurers to substantially limit their exposure to the costliest cyber intrusions.[4]

In December, Lloyd's of London updated the language in its cyber war and cyber operation exclusion clauses to expand their scope, stating in part pending attribution by the government of the state … the insurer may rely upon an inference which is objectively reasonable as to attribution of the cyber operation to another state or those acting on its behalf. It is agreed that during this period no loss shall be paid.

Moreover, if the insurer deems attribution is taking "an unreasonable length of time" or the state is unable to attribute the activity, "it shall be for the insurer to prove attribution by reference to such other evidence as is available."[5]

Of particular concern, the Lloyd's language would allow for blanket claim denials based on the amount of dubious attribution that exists in the public record. Today just about any malware or malcode used in an intrusion can be linked to a nation state attributed operation.

Even if Lloyd's limits its attribution-based denials to only government malware reports, there is sufficient overlap in tactics, techniques and procedures to render tying a hack to a tool used by a nation state actor as trivial.

This creates a clear trend in the marketplace. Insurance is going to have higher premiums and deductibles and include more exclusions. This means that instead of a clear strategy of risk transference, insurance is likely to siphon money out of security programs while providing substantially less value when an event does occur.

The full effect of these changes will take time to manifest as policies come up for renewal and changes are implemented in a staggered fashion. However, as more policies are renewed, we are likely to see a new normal that:

- Increases the sunk costs for businesses to carry an insurance policy;
- Reduces the value provided by that policy in terms of actual remuneration as well as technical support and mitigation;
- Increases the need for a larger security footprint; and
- Requires a reconsideration of corporate risk with cyber being a larger driver of the overall portfolio.

While this appears to be an overall negative trend for corporations that have thus far relied on risk transference as a strategy, should the insurance industry move aggressively in this manner there are two positive outcomes likely to occur.

First, spending on security programs will increase.

Provided that the increase in spending is focused on relevant security fundamentals, this will create a less hospitable environment for cyber criminal activity. Better patch management, basic security builds for new infrastructure, i.e., security by default, password management and multifactor authentication — all of these things, if applied appropriately, will significantly reduce the ability of the current crop of threat actors to successfully operate against victim networks and systems.

If risk cannot be transferred, there is increased incentive to get these basics right.

Second, the shape of the criminal activity is likely to adapt. It is often cheaper for insurers to pay ransomware operators than go through full mitigation. Insurance generally avoids supporting the process of remediation and full restoration. The economics for a corporation to pay a ransom directly are different than those of the insurers.

Corporations will have an incentive, if the insurance coverage is diminished, to pay for not only immediate incident mitigation but also long-term remediation as a way to reduce expected future costs. This increased focus on remediation will reduce incentive to pay large ransoms as the cost to remediate will exist regardless of how they handle initial mitigation efforts.

Payments will not go away overnight, but the amount ransomware groups can demand will diminish with insurance money being a reduced part of the equation. This will encourage some threat actors to move away from ransomware and toward other methods to monetize their capabilities.

Those that stay in the field will likely modify their approach to something that looks more like the spray-and-pray approach of the mid-2010s rather than the deliberate big game hunting of the last two to three years.

What does risk mitigation 2.0 look like?

These shifting trends in risk strategy, investments and, ultimately, threats will create a significantly different environment for corporate officers and legal counsel in the upcoming year. These decision-makers would do well to proactively reevaluate their risk tolerance strategy now rather than waiting and potentially being caught flat-footed in the event of a breach.

Relying on insurance companies to underwrite substantial financial cybersecurity risk is increasingly becoming an unviable strategy, and the insured are going to have to respond with changes to internal security practices.

To proactively address this incipient trend, executives should ask the following questions:

- What is our current insurance coverage and what exclusions already exist in the policy?
- Over the last 18 months what is the average effect of cyber events experienced by the company or industry benchmarks in direct and indirect losses?
- What is the average cost of a breach in our industry vertical?
- What is our current ability to identify and prevent malicious access to the most business-essential data or assets?

- What new rules and regulations is our industry subject to that could result in fines as a result of a data breach?

Once the executive team has a high-level understanding of current risk, it is time to have amore nuanced conversation about how to position for 2022. Assuming that coverage is going to decrease from cyber insurance, or become exceedingly more expensive — higher deductibles, more exclusions, etc. — what is the new total liability that the company is carrying based on historical costs as well as industry averages?

If risk transference is no longer a viable strategy, then it is best to work on targeted investments in the corporate security posture to reduce the likelihood of incurring the costs associated with a breach.

Companies that proactively assess the current state and anticipate the most likely scenarios as existing risk strategies change will be able to navigate and minimize their exposure. They will also have first mover advantage when it comes to hiring and retaining security talent.

Any company that chooses to in-source to mitigate risk will be facing an even tighter labor market. First mover advantage will reduce overall costs as 2022 sees increased demand for talent.

Failure to assess and plan will leave companies with unaccounted for residual risk, insufficient mitigation options during an event and higher costs for post-incident remediation as resources become more constrained with increased demand.

This article originally appeared in **Law360, January 2022.** All rights reserved.

About the Authors

Luke Tenery is a partner, Thomas McEwan is a manager and Ross Rustici is a managing director at StoneTurn Group LLP.

[1] FinCen Trend Analysis, Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021, (15 October 2021); https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomeware%20508%20FINAL.pdf.

[2] https://blog.morphisec.com/cyber-insurance-may-be-making-ransomware-worse-hereswhy; https://www.propublica.org/article/the-extortion-economy-how-insurance-companiesare-fueling-a-rise-in-ransomware-attacks.

[3] https://www.insuranceinsider.com/article/2876mmytwlmxq2wri18n4/london-cybermarket-heading-for-multi-year-correction-in-rates.

[4] https://www.insidepandc.com/article/2876n8ua7o41yv0aumfwg/aig-introducesransomware-co-insurance-and-sub-limits-at-1-1-cyber-renewals.

[5] https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx.