A Bonus-Malus Framework for Cyber Risk Insurance and Optimal Cybersecurity Provisioning — Online Appendix

Qikun Xiang[1], Ariel Neufeld[1], Gareth W. Peters[2], Ido Nevat[3], and Anwitaman Datta[4]

[1]Division of Mathematical Sciences, Nanyang Technological University, Singapore
[2]Department of Statistics and Applied Probability, University of California Santa Barbara, USA
[3]TUMCREATE, Singapore
[4]School of Computer Science and Engineering, Nanyang Technological University, Singapore

1 Results with different h parameters

The experimental setting in this section is identical to the setting in Section 6 of the paper, except that the value of the h parameter in the loss severity distribution Tr-g-and-$h(\alpha, \varsigma, g, h)$ differs from the value 0.15 used in the paper.

1.1 Results when $h = 0.10$

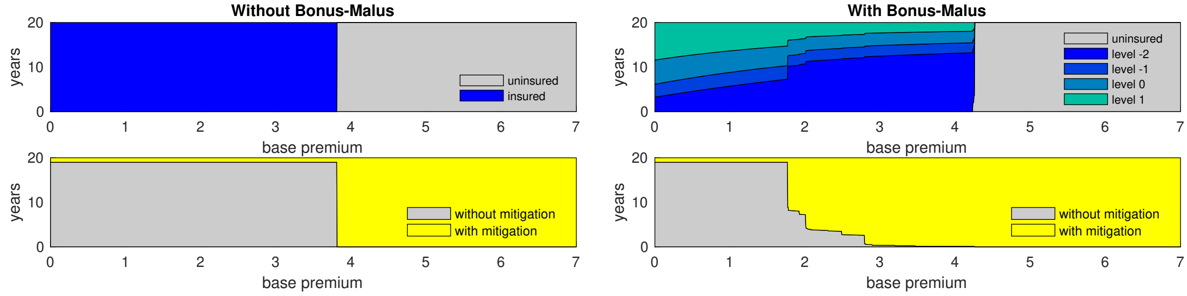

Figure 1: Modified setting with $h = 0.10$ – the retention rate of the cyber risk insurance policy and the expected years of adoption of the self-mitigation measure versus the base premium.

Figure 1 and Figure 2 show the experimental results when the severity distribution is Tr-g-and-$h(\alpha = 0, \varsigma = 1, g = 1.8, h = 0.10)$. In Figure 1, with the contract that does not have the Bonus-Malus system, the decisions of the insured are completely deterministic, that is, they do not depend on the realisation of the cyber loss events. When $p^{\mathcal{BM}}_{\text{base}} \leq 3.810$, the optimal strategy of the insured is to purchase the cyber risk insurance policy every year and only adopt the self-mitigation measure in the final policy year (due to the higher deductible in the final policy year). When $p^{\mathcal{BM}}_{\text{base}} \geq 3.815$, the optimal strategy of the insured is to never purchase the cyber risk insurance policy and always adopt the self-mitigation measure. Therefore, without the Bonus-Malus system, the issue of moral hazard is present and the insured will treat the cyber risk insurance policy and the self-mitigation measure as substitute goods. On the other hand, when the Bonus-Malus system is introduced to the cyber risk insurance policy, the decisions of the insured depend on the realisation of the cyber loss events. When $3.470 \leq p^{\mathcal{BM}}_{\text{base}} \leq 4.230$, the optimal strategy of the insured is to always purchase the cyber risk insurance policy and to adopt the self-mitigation measure except in year 19 when the Bonus-Malus level is equal to 1. When $4.235 \leq p^{\mathcal{BM}}_{\text{base}} \leq 4.255$, the optimal strategy of the insured is to adopt the self-mitigation measure except in year 19 when the insurance is active and the Bonus-Malus level is equal to 1, but to withdraw from the insurance contract whenever the expected future cost exceeds the expected future benefit of the insurance policy. As a result, the

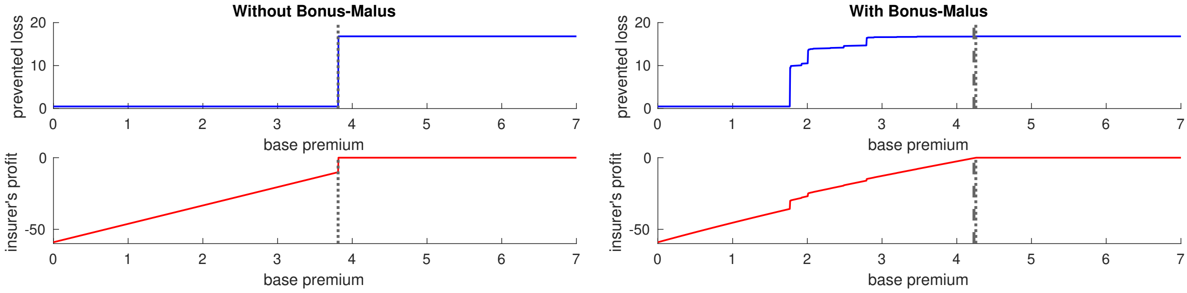

Figure 2: Modified setting with $h = 0.10$ – the discounted total expected loss prevented by the self-mitigation measure and the discounted expected profit (measured by the quantity $\overline{Z}_{\text{ins}} - \overline{Z}_{\text{cp}}$) of the insurer versus the base premium. Left panel: the contract without the Bonus-Malus system. The dashed lines indicate the highest base premium before the insured chooses not to purchase the cyber risk insurance policy. Right panel: the contract with the Bonus-Malus system. The dashed lines indicate the highest base premium before the retention rate drops below 100%. The dotted lines indicate the highest base premium before the insured chooses not to purchase the cyber risk insurance policy.

retention rate, i.e., the expected proportion of years the insured remains in the contract, drops when the base premium is increased. When $p^{\mathcal{BM}}_{\text{base}} \geq 4.260$, the optimal strategy of the insured is to never purchase the cyber risk insurance policy and always adopt the self-mitigation measure. Hence, compared with the contract without Bonus-Malus, the contract with Bonus-Malus incentivises the insured to adopt the self-mitigation measure in addition to purchasing the cyber risk insurance policy.

The left panel of Figure 2 shows that, in the case without Bonus-Malus, when $p^{\mathcal{BM}}_{\text{base}} \leq 3.810$, the insured will always purchase the cyber risk insurance policy but will only adopt the self-mitigation measure in the final policy year. Hence, the discounted total expected loss prevented stays at 0.495, while the discounted expected profit of the insurer increases as the base premium increases. When $p^{\mathcal{BM}}_{\text{base}} \geq 3.815$, the insured will not purchase the insurance policy but will always adopt the self-mitigation measure. As a result, the discounted total expected loss prevented will be 16.814 but the insurer will earn no profit. The most the insurer can gain before losing the insured is -10.124, when the base premium is set to 3.810. In contrast, in the case with the Bonus-Malus system, as shown in the right panel of Figure 2, the insurer can gain a discounted expected profit of at most -0.282 while always retaining the insured (i.e., the insured will never withdraw from the contract), when the base premium is set to 4.230. The insurer can gain a discounted expected profit of at most -0.057 before losing the insured, when the base premium is set to 4.255. With these two base premiums, the insured will adopt the self-mitigation measure except in year 19 when the insurance contract is active and the Bonus-Malus level is equal to 1, resulting in discounted total expected loss prevention of 16.759 and 16.770, respectively.

1.2 Results when $h = 0.20$

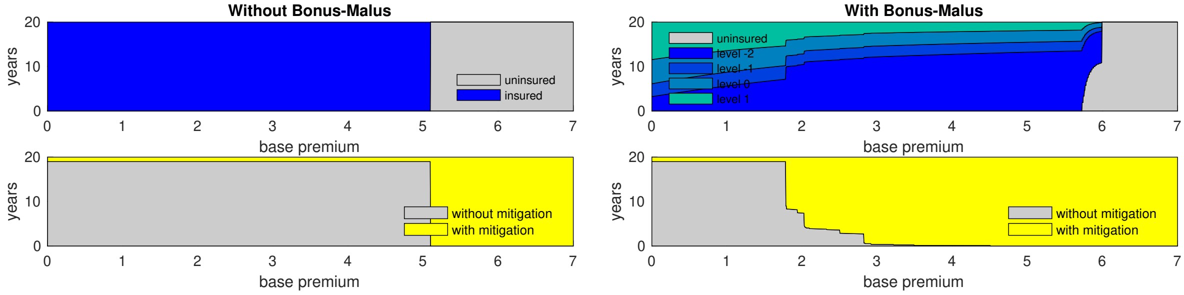

Figure 3: Modified setting with $h = 0.20$ – the retention rate of the cyber risk insurance policy and the expected years of adoption of the self-mitigation measure versus the base premium.

Figure 3 and Figure 4 show the experimental results when the severity distribution is Tr-g-and-h($\alpha =$

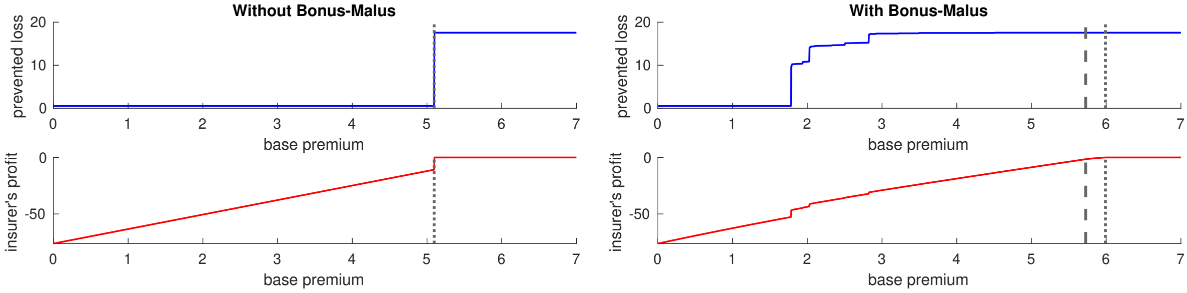

Figure 4: Modified setting with $h = 0.20$ – the discounted total expected loss prevented by the self-mitigation measure and the discounted expected profit (measured by the quantity $\overline{Z}_{\text{ins}} - \overline{Z}_{\text{cp}}$) of the insurer versus the base premium. Left panel: the contract without the Bonus-Malus system. The dashed lines indicate the highest base premium before the insured chooses not to purchase the cyber risk insurance policy. Right panel: the contract with the Bonus-Malus system. The dashed lines indicate the highest base premium before the retention rate drops below 100%. The dotted lines indicate the highest base premium before the insured chooses not to purchase the cyber risk insurance policy.

$0, \varsigma = 1, g = 1.8, h = 0.20$). In Figure 3, with the contract that does not have the Bonus-Malus system, the decisions of the insured are completely deterministic. When $p_{\text{base}}^{\mathcal{BM}} \leq 5.095$, the optimal strategy of the insured is to purchase the cyber risk insurance policy every year and only adopt the self-mitigation measure in the final policy year (due to the higher deductible in the final policy year). When $p_{\text{base}}^{\mathcal{BM}} \geq 5.100$, the optimal strategy of the insured is to never purchase the cyber risk insurance policy and always adopt the self-mitigation measure. Therefore, without the Bonus-Malus system, the issue of moral hazard is present and the insured will treat the cyber risk insurance policy and the self-mitigation measure as substitute goods. On the other hand, when the Bonus-Malus system is introduced to the cyber risk insurance contract, the decisions of the insured depend on the realisation of losses. When $4.510 \leq p_{\text{base}}^{\mathcal{BM}} \leq 5.725$, the optimal strategy of the insured is to always purchase the cyber risk insurance policy and adopt the self-mitigation measure. When $5.730 \leq p_{\text{base}}^{\mathcal{BM}} \leq 5.990$, the optimal strategy of the insured is to always adopt the self-mitigation measure, but to withdraw from the insurance contract whenever the expected future cost exceeds the expected future benefit of the insurance policy. As a result, the retention rate drops when the base premium is increased. When $p_{\text{base}}^{\mathcal{BM}} \geq 5.995$, the optimal strategy of the insured is to never purchase the cyber risk insurance policy and always adopt the self-mitigation measure. Hence, compared with the contract without Bonus-Malus, the contract with Bonus-Malus incentivises the insured to adopt the self-mitigation measure in addition to purchasing the cyber risk insurance policy.

The left panel of Figure 4 shows that, in the case without Bonus-Malus, when $p_{\text{base}}^{\mathcal{BM}} \leq 5.095$, the insured will always purchase the cyber risk insurance policy but will only adopt the self-mitigation measure in the final policy year. Hence, the discounted total expected loss prevented stays at 0.516, while the discounted expected profit of the insurer increases as the base premium increases. When $p_{\text{base}}^{\mathcal{BM}} \geq 5.100$, the insured will not purchase the insurance policy but will always adopt the self-mitigation measure. As a result, the discounted total expected loss prevented will be 17.561 but the insurer will earn no profit. The most the insurer can gain before losing the insured is -10.823, when the base premium is set to 5.095. In contrast, in the case with the Bonus-Malus system, as shown in the right panel of Figure 4, the insurer can gain a discounted expected profit of at most -1.558 while always retaining the insured, when the base premium is set to 5.725. The insurer can gain a discounted expected profit of at most -0.015 before losing the insured, when the base premium is set to 5.990. With both of these two base premiums, the insured will always adopt the self-mitigation measure, resulting in a discounted total expected loss prevention of 17.561.

1.3 Results when $h = 0.25$

Figure 5 and Figure 6 show the experimental results when the severity distribution is Tr-g-and-h($\alpha = 0, \varsigma = 1, g = 1.8, h = 0.25$). In Figure 5, with the contract that does not have the Bonus-Malus

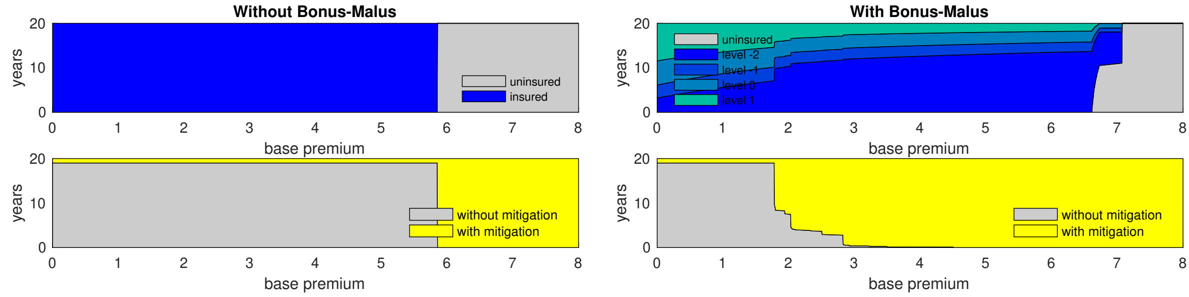

Figure 5: Modified setting with $h = 0.25$ – the retention rate of the cyber risk insurance policy and the expected years of adoption of the self-mitigation measure versus the base premium.

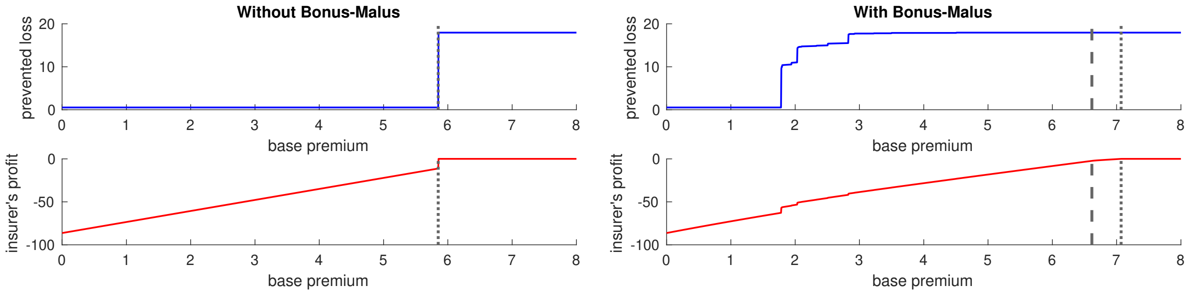

Figure 6: Modified setting with $h = 0.25$ – the discounted total expected loss prevented by the self-mitigation measure and the discounted expected profit (measured by the quantity $\overline{Z}_{\text{ins}} - \overline{Z}_{\text{cp}}$) of the insurer versus the base premium. Left panel: the contract without the Bonus-Malus system. The dashed lines indicate the highest base premium before the insured chooses not to purchase the cyber risk insurance policy. Right panel: the contract with the Bonus-Malus system. The dashed lines indicate the highest base premium before the retention rate drops below 100%. The dotted lines indicate the highest base premium before the insured chooses not to purchase the cyber risk insurance policy.

system, the decisions of the insured are completely deterministic. When $p_{\text{base}}^{\mathcal{BM}} \leq 5.850$, the optimal strategy of the insured is to purchase the cyber risk insurance policy every year and only adopt the self-mitigation measure in the final policy year (due to the higher deductible in the final policy year). When $p_{\text{base}}^{\mathcal{BM}} \geq 5.855$, the optimal strategy of the insured is to never purchase the cyber risk insurance policy and always adopt the self-mitigation measure. Therefore, without the Bonus-Malus system, the issue of moral hazard is present and the insured will treat the cyber risk insurance policy and the self-mitigation measure as substitute goods. On the other hand, when the Bonus-Malus system is introduced to the cyber risk insurance contract, the decisions of the insured depend on the realisation of losses. When $4.510 \leq p_{\text{base}}^{\mathcal{BM}} \leq 6.615$, the optimal strategy of the insured is to always purchase the cyber risk insurance policy and adopt the self-mitigation measure. When $6.620 \leq p_{\text{base}}^{\mathcal{BM}} \leq 7.070$, the optimal strategy of the insured is to always adopt the self-mitigation measure, but to withdraw from the insurance contract whenever the expected future cost exceeds the expected future benefit of the insurance policy. As a result, the retention rate drops when the base premium is increased. When $p_{\text{base}}^{\mathcal{BM}} \geq 7.075$, the optimal strategy of the insured is to never purchase the cyber risk insurance policy and always adopt the self-mitigation measure. Hence, compared with the contract without Bonus-Malus, the contract with Bonus-Malus incentivises the insured to adopt the self-mitigation measure in addition to purchasing the cyber risk insurance policy.

The left panel of Figure 6 shows that, in the case without Bonus-Malus, when $p_{\text{base}}^{\mathcal{BM}} \leq 5.850$, the insured will always purchase the cyber risk insurance policy but will only adopt the self-mitigation measure in the final policy year. Hence, the discounted total expected loss prevented stays at 0.528, while the discounted expected profit of the insurer increases as the base premium increases. When $p_{\text{base}}^{\mathcal{BM}} \geq 5.855$, the insured will not purchase the insurance policy but will always adopt the self-mitigation measure. As a result, the discounted total expected loss prevented will be 17.948 but the insurer will earn no profit. The most the insurer can gain before losing the insured is -11.256, when the base premium is set to 5.850. In contrast, in the case with the Bonus-Malus system, as shown in the right panel of Figure 6, the insurer can gain a discounted expected profit of at most -2.344 while always retaining the insured, when the base premium is set to 6.615. The insurer can gain a discounted expected profit of at most -0.001 before losing the insured, when the base premium is set to 7.070. With both of these two base premiums, the insured will always adopt the self-mitigation measure, resulting in a discounted total expected loss prevention of 17.948.

2 Results with a log-normal severity distribution

The experimental setting in this section is identical to the setting in Section 6 of the paper, except that the loss severity distribution is replaced by log-Normal(μ, σ^2) where the values of the parameters μ and σ^2 are chosen such that the first and second moments of log-Normal(μ, σ^2) match that of Tr-g-and-$h(\alpha = 0, \varsigma = 1, g = 1.8, h = 0.15)$. Another modification to the setting is that the annual investment $\beta(1)$ required by the self-mitigation measure is reduced to 0.3 from 0.5 in the original settings. The reason is that under this log-normal loss severity model, the loss reduction effect $\gamma(1)$ of the self-mitigation measure is much smaller compared to the truncated g-and-h model.

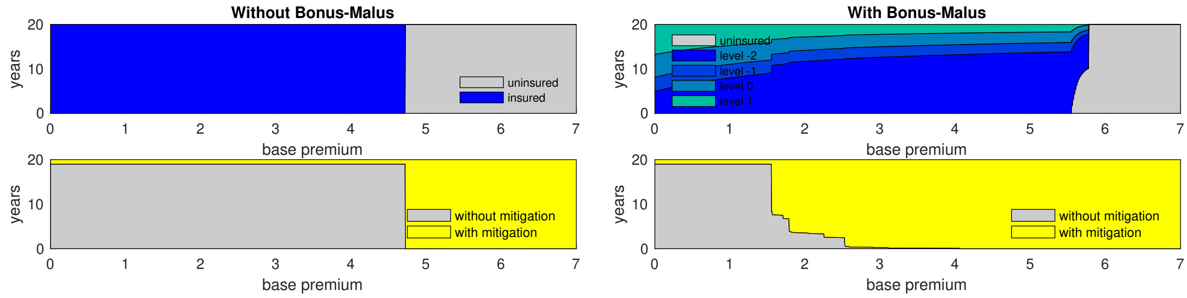

Figure 7: Modified setting with a log-normal severity distribution – the retention rate of the cyber risk insurance policy and the expected years of adoption of the self-mitigation measure versus the base premium.

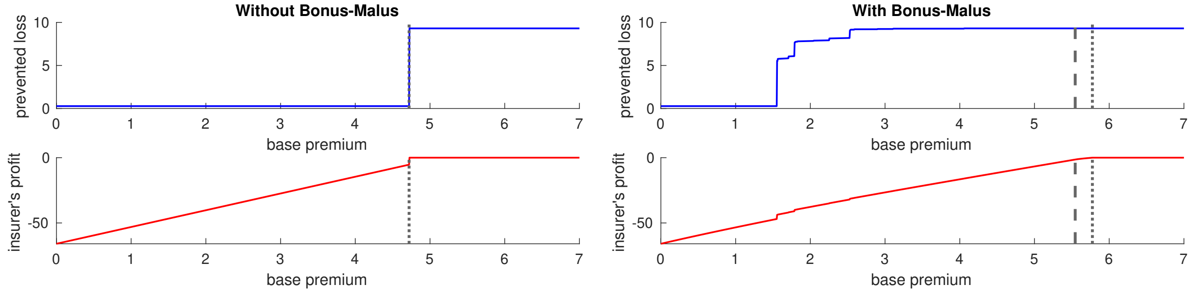

Figure 8: Modified setting with a log-normal severity distribution – the discounted total expected loss prevented by the self-mitigation measure and the discounted expected profit (measured by the quantity $\overline{Z}_{\text{ins}} - \overline{Z}_{\text{cp}}$) of the insurer versus the base premium. Left panel: the contract without the Bonus-Malus system. The dashed lines indicate the highest base premium before the insured chooses not to purchase the cyber risk insurance policy. Right panel: the contract with the Bonus-Malus system. The dashed lines indicate the highest base premium before the retention rate drops below 100%. The dotted lines indicate the highest base premium before the insured chooses not to purchase the cyber risk insurance policy.

Figure 7 and Figure 8 show the experimental results with the log-normal severity distribution. In Figure 7, with the contract that does not have the Bonus-Malus system, the decisions of the insured are completely deterministic. When $p_{\text{base}}^{\mathcal{BM}} \leq 4.720$, the optimal strategy of the insured is to purchase the cyber risk insurance policy every year and only adopt the self-mitigation measure in the final policy year (due to the higher deductible in the final policy year). When $p_{\text{base}}^{\mathcal{BM}} \geq 4.725$, the optimal strategy of the insured is to never purchase the cyber risk insurance policy and always adopt the self-mitigation measure. Therefore, without the Bonus-Malus system, the issue of moral hazard is present and the insured will treat the cyber risk insurance policy and the self-mitigation measure as substitute goods. On the other hand, when the Bonus-Malus system is introduced to the cyber risk insurance contract, the decisions of the insured depend on the realisation of losses. When $4.060 \leq p_{\text{base}}^{\mathcal{BM}} \leq 5.545$, the optimal strategy of the insured is to always purchase the cyber risk insurance policy and adopt the self-mitigation measure. When $5.550 \leq p_{\text{base}}^{\mathcal{BM}} \leq 5.775$, the optimal strategy of the insured is to always adopt the self-mitigation measure, but to withdraw from the insurance contract whenever the expected future cost exceeds the expected future benefit of the insurance policy. As a result, the retention rate drops when the base premium is increased. When $p_{\text{base}}^{\mathcal{BM}} \geq 5.780$, the optimal strategy of the insured is to never purchase the cyber risk insurance policy and always adopt the self-mitigation measure. Hence, compared with the contract without Bonus-Malus, the contract with Bonus-Malus incentivises the insured to adopt the self-mitigation measure in addition to purchasing the cyber risk insurance policy.

The left panel of Figure 8 shows that, in the case without Bonus-Malus, when $p_{\text{base}}^{\mathcal{BM}} \leq 5.4.720$, the insured will always purchase the cyber risk insurance policy but will only adopt the self-mitigation measure in the final policy year. Hence, the discounted total expected loss prevented stays at 0.274, while the discounted expected profit of the insurer increases as the base premium increases. When $p_{\text{base}}^{\mathcal{BM}} \geq 4.725$, the insured will not purchase the insurance policy but will always adopt the self-mitigation measure. As a result, the discounted total expected loss prevented will be 9.304 but the insurer will earn no profit. The most the insurer can gain before losing the insured is -5.355, when the base premium is set to 4.720. In contrast, in the case with the Bonus-Malus system, as shown in the right panel of Figure 8, the insurer can gain a discounted expected profit of at most -1.432 while always retaining the insured, when the base premium is set to 5.545. The insurer can gain a discounted expected profit of at most -0.008 before losing the insured, when the base premium is set to 5.775. With both of these two base premiums, the insured will always adopt the self-mitigation measure, resulting in a discounted total expected loss prevention of 9.304.