A Coordinated Defense to Cyber Risk

Cyber risk is an amorphous threat that demands a coordinated defense from companies, their insurance carriers, and security and privacy professionals.

The exposure is multifaceted, varies from business to business, and continues to evolve. In addition to purchasing cyber insurance, companies can bolster their defenses against this risk by conducting targeted risk assessments and implementing appropriate security controls — but the challenge lies in identifying which security programs and controls an organization needs most, and which vendors provide the best service.

All companies, but especially small- to medium-sized businesses with more limited resources, want to see improvement of their risk profiles translate into discounted insurance premiums. However, lack of alignment between IT security vendors and underwriters can make that connection difficult to attain, minimizing the value of loss control services. Current underwriting processes typically don’t allow underwriters the opportunity to ask insureds many questions about their security and privacy improvements, and vendors often view insurance as a separate offering, if not an afterthought.

“Part of the challenge has been that you have two different industries — IT security and insurance — working in silos to address a singular risk challenge. Naturally, security professionals think about risk and control mechanisms differently than insurance professionals, and speak different languages,” said Tom Kang, enterprise cyber underwriting & product lead, The Hartford.

Many insurers make recommendations on well-vetted service providers, but traditionally there has not been a high rate of engagement because insureds could not see how those services impact their cost of insurance.

“A lot of underwriters are watching what the corporate risk teams are doing and the policies that are in place. This is not a one-size-fits-all solution, but it is something we can offer that will help them make a decision,” said Tim Marlin, head of cyber underwriting at Hartford Financial Products.

“An insurance policy should help you get better. Not just on the front end before there’s a claim, but after a claim as well.”

— Tim Marlin, head of cyber underwriting, Hartford Financial Products

“Because cyber risk was emerging so quickly, insureds were often on their own when it came to risk control, underwriters were evaluating an emerging risk and hoping they got it right, and then claims were their own animal,” said Tim Marlin, head of cyber underwriting at Hartford Financial Products.

“But now that the risk is more mature, our views need to mature as well. As we gather more claims data, the industry needs to implement a better, more coordinated strategy than the ad hoc approach that often prevails. Risk control, underwriting and claim response should be thought of as parts of a continuum.”

Insurers pay a key role in driving best practices and can help clients align every part of their cyber risk strategy. By thinking through their risk holistically, insurers can help buyers identify their key exposures, establish internal risk mitigation, transfer the risk through cyber insurance, and respond to a breach.

“Insurers themselves have a market-wide view of the risk from underwriting and claims data and benchmarking,” Kang said. “They can help insureds understand whether they are doing the right thing when it comes to identifying and securing their critical assets, compiling with a dizzying array of regulations in this space, and direct them to the right resources.”

“We believe aligning the solutions — between security and insurance — and providing the right incentives to our clients can make a real difference.”

— Tom Kang, enterprise cyber underwriting & product lead, The Hartford

“Because cyber risk was emerging so quickly, insureds were often on their own when it came to risk control, underwriters were evaluating an emerging risk and hoping they got it right, and then claims were their own animal,” said Tim Marlin, head of cyber underwriting at Hartford Financial Products.

“But now that the risk is more mature, our views need to mature as well. As we gather more claims data, the industry needs to implement a better, more coordinated strategy than the ad hoc approach that often prevails. Risk control, underwriting and claim response should be thought of as parts of a continuum.”

Insurers pay a key role in driving best practices and can help clients align every part of their cyber risk strategy. By thinking through their risk holistically, insurers can help buyers identify their key exposures, establish internal risk mitigation, transfer the risk through cyber insurance, and respond to a breach.

“Insurers themselves have a market-wide view of the risk from underwriting and claims data and benchmarking,” Kang said. “They can help insureds understand whether they are doing the right thing when it comes to identifying and securing their critical assets, compiling with a dizzying array of regulations in this space, and direct them to the right resources.”

“We believe aligning the solutions — between security and insurance — and providing the right incentives to our clients can make a real difference.”

— Tom Kang, enterprise cyber underwriting & product lead, The Hartford

Many insurers make recommendations on well-vetted service providers, but traditionally there has not been a high rate of engagement because insureds could not see how these services impact their cost of insurance.

“Most insureds and brokers want to see their investment in these services have some kind of impact on premium, and historically insurers have not had much of a response,” Marlin said. “Some provide value-added services packaged with the policy. But including those services doesn’t generally move the premium or risk mitigation needle in any material way for organizations, whether they are mid-sized or large.”

“The Hartford goes a step further beyond just finding the best vendors in the business. If clients use approved service providers and services, they can report it to The Hartford’s underwriters, who will factor the risk controls into calculations of the insurance premium.

“These are vendors we trust to help our clients get better at managing cyber risk,” Marlin said. “If they are strengthening their security, it feeds directly into our underwriting process and results in a premium incentive.”

By connecting the use of risk control services to insurance cost savings, The Hartford incentivizes clients to implement best practices in cyber risk mitigation and reduce their exposure to loss.

FROM COVERAGE TO BREACH RESPONSE

Carriers can also work more closely with brokers and insureds to help them determine what the most appropriate coverage is for their particular business. An organization’s size and function both influence what type of coverage is required.

Small and mid-sized companies with limited resources, for example, may be less inclined to purchase a monoline cyber product than to embed coverage within a different policy, like General Liability or E&O — where cyber coverage originated.

“When you think about the risk holistically, you can more thoughtfully plan what risk you will retain, mitigate or transfer. Part of thinking about the risk holistically also includes developing a robust cyber incident response plan, and thinking carefully about recovery and necessary improvements,” Kang said.

Beyond the traditional response services that are often included in cyber insurance, companies can bolster their defenses against this risk by conducting targeted risk assessments and implementing appropriate security controls — but the challenge lies in identifying which security programs and controls an organization needs most, and which vendors provide the best service.

All companies, but especially small- to medium-sized businesses with more limited resources, want to see improvement of their risk profiles translate into discounted insurance premiums. However, lack of alignment between IT security vendors and underwriters can make that connection difficult to attain, minimizing the value of loss control services. Current underwriting processes typically don’t allow underwriters the opportunity to ask insureds many questions about their security and privacy improvements, and vendors often view insurance as a separate offering, if not an afterthought.

“Part of the challenge has been that you have two different industries — IT security and insurance — working in silos to address a singular risk challenge. Naturally, security professionals think about risk and control mechanisms differently than insurance professionals, and speak different languages,” said Tom Kang, enterprise cyber underwriting & product lead, The Hartford.

Many insurers make recommendations on well-vetted service providers, but traditionally there has not been a high rate of engagement because insureds could not see how these services impact their cost of insurance.

“Most insureds and brokers want to see their investment in these services have some kind of impact on premium, and historically insurers have not had much of a response,” Marlin said. “Some provide value-added services packaged with the policy. But including those services doesn’t generally move the premium or risk mitigation needle in any material way for organizations, whether they are mid-sized or large.”

“The Hartford goes a step further beyond just finding the best vendors in the business. If clients use approved service providers and services, they can report it to The Hartford’s underwriters, who will factor the risk controls into calculations of the insurance premium.

“These are vendors we trust to help our clients get better at managing cyber risk,” Marlin said. “If they are strengthening their security, it feeds directly into our underwriting process and results in a premium incentive.”

By connecting the use of risk control services to insurance cost savings, The Hartford incentivizes clients to implement best practices in cyber risk mitigation and reduce their exposure to loss.

FROM COVERAGE TO BREACH RESPONSE

Carriers can also work more closely with brokers and insureds to help them determine what the most appropriate coverage is for their particular business. An organization’s size and function both influence what type of coverage is required.

Small and mid-sized companies with limited resources, for example, may be less inclined to purchase a monoline cyber product than to embed coverage within a different policy, like General Liability or E&O — where cyber coverage originated.

“When you think about the risk holistically, you can more thoughtfully plan what risk you will retain, mitigate or transfer. Part of thinking about the risk holistically also includes developing a robust cyber incident response plan, and thinking carefully about recovery and necessary improvements,” Kang said.

Beyond the traditional response services that are often included in cyber insurance, companies can bolster their defenses against this risk by conducting targeted risk assessments and implementing appropriate security controls — but the challenge lies in identifying which security programs and controls an organization needs most, and which vendors provide the best service.

All companies, but especially small- to medium-sized businesses with more limited resources, want to see improvement of their risk profiles translate into discounted insurance premiums. However, lack of alignment between IT security vendors and underwriters can make that connection difficult to attain, minimizing the value of loss control services. Current underwriting processes typically don’t allow underwriters the opportunity to ask insureds many questions about their security and privacy improvements, and vendors often view insurance as a separate offering, if not an afterthought.

“Part of the challenge has been that you have two different industries — IT security and insurance — working in silos to address a singular risk challenge. Naturally, security professionals think about risk and control mechanisms differently than insurance professionals, and speak different languages,” said Tom Kang, enterprise cyber underwriting & product lead, The Hartford.

Many insurers make recommendations on well-vetted service providers, but traditionally there has not been a high rate of engagement because insureds could not see how these services impact their cost of insurance.

“When you think about the risk holistically, you can more thoughtfully plan what risk you will retain, mitigate or transfer. Part of thinking about the risk holistically also includes developing a robust cyber incident response plan, and thinking carefully about recovery and necessary improvements,” Kang said.