FEATURE

Does cyber insurance make us more (or less) secure?

Underwriting cyber risk remains more art than science, but in the absence of regulation, cyber insurance might still be the best hope for improving cybersecurity practices across the board — at least for now.

By J.M. Porup

Senior Writer, CSO

JUN 18, 2018 3:00 AM PDT

If data is the new oil, then we're looking at pelicans soaked in crude on a beach.

When an oil tanker goes down or an oil rig explodes, dumping millions of gallons of petroleum into the ocean, we clean up the spill, we look for first causes, and we hold the company — even individuals — responsible for the harm they've caused to a shared resource: the environment we all live in.

[Watch out for 7 common modeling mistakes | Get the latest from CSO by signing up for our newsletters.]

When a company like Equifax commits gross negligence for failing to secure our data, and a breach pumps 147.9 million records onto the internet, the company's directors keep their jobs, their cyber insurance policy pays out, and the company posts a profit.

The Equifax breach harmed pretty much every adult in the U.S., and the company has yet to face any real consequences for its incompetence. Is this the future of cyber risk insurance — commit gross negligence and get away with it?

[redacted]

Maybe. Maybe not. CSO talked to more than a dozen cyber insurance experts and reviewed hundreds of pages of documents on the current state of the cyber insurance market. Here's what we found.

The moral hazard of cyber risk insurance

"Moral hazard" is the term insurance wonks use to discuss the misplaced incentives that insurance can create. It's not a new problem; it has been a part of insurance underwriting since the days of sail. Just as car insurance might encourage bad driving, or fire insurance might encourage people not to install smoke detectors, cyber insurance might encourage incompetent security practices. Why bother doing the right thing if insurance is going to pay you to do the wrong thing?

The time-tested strategy by insurance carriers to limit moral hazard is to use insurance deductibles and co-pays, and to cap maximum payouts. That way the insured shares in the financial risk and is motivated to drive safely, to install smoke detectors, and to deploy strong cybersecurity controls in their enterprise.

The moral hazard of cyber insurance haunts boardrooms. The market remains in its infancy, and insurance carriers are still grappling with how to deal with this problem. Non-technical C-suite executives looking to manage cyber risk can and do fall into this trap. If you're paying for insurance, why bother applying strong cybersecurity controls? It's cheaper and easier to just hang out for the insurance payout and not bother doing the hard work of improving your security posture.

"The inevitable tension for firms," a Rand Corporation study of cyber insurance policies concluded, "is whether to invest in ex ante security controls in order to reduce the probability of loss, or to transfer the risk (cost) to an insurer."

That might be a conversation between just the company and their insurance carrier if breaches affected only shareholders. For example, insurance began in the age of sail, when sending ships on long international voyages was risky. Ships sank, pirates attacked, storms happened, etc. If a ship carrying spices from India goes down, the only people harmed are the shareholders (and the sailors, of course, the usual footnotes to history). If Equifax gets breached, the harm affects all of society.

Because of the moral hazard it creates, cyber insurance might be uniquely unfit to deal with these massive third-party harms to society at large. However, absent regulation, or even a government willing to regulate, cyber insurance might still be the best hope for improving cybersecurity practices across the board — at least for now.

The Wild West of cyber insurance

Cyber insurance has been around, in one form or another, for the last 20 years, since the dot-com bubble burst in the late 1990s, and has grown dramatically since then, Christian Stanley of Lloyd's of London tells CSO. "Lloyd's has about a third of the global market share," Stanley says. "Year on year it's dramatically increased compared to other lines of business."

Most cyber insurance policies continue to be written for U.S. companies, although that's beginning to change. Market demands for different kinds of cyber insurance are also in flux, driven both by legislation as well as emerging technical risks. Companies looking to buy cyber insurance can purchase either standalone policies or extend existing policies to include cyber risks.

"Initially in 2003 with the laws that came into effect in California, there was a privacy breach focus," Stanley says. "In the last couple of years, business interruption has become the bigger driver of buyers coming to the market."

Cyber insurance policies can be complex and tricky to understand, and anxious C-suite executives are buying cyber insurance often without understanding the full extent of what policies cover and what they don't. To grow the market and diversify the risk, insurance companies are taking on all comers, often with no adequate measure of the true risk any given insured enterprise faces.

Both insurance carriers and enterprise buyers of cyber insurance are groping their way forward in the dark, a potentially dangerous scenario. Most insurance carriers, however, are aware of this blind spot, and researching how to better measure and quantify cyber risk.

Measuring cyber risk is very different than in other domains. If you want to rate the risk of an earthquake or a hurricane, the actuarial science is sound. A data center in a hundred-year flood plain can expect a catastrophic flood once in a hundred years. Cyber risk, on the other hand, remains far harder to quantify — a problem, it must be noted, the insurance business is working hard to solve.

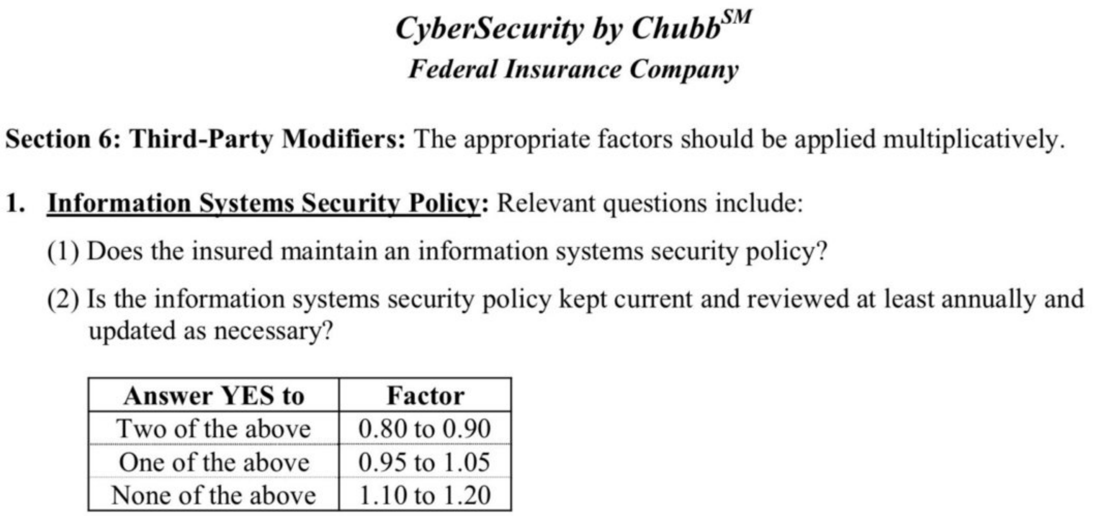
Measuring cyber risk

Measuring cyber risk is an unsolved problem. How can insurance carriers effectively measure cyber risk? How can they price policies in a way that's fair? How can companies acting in good faith shop for, and purchase, the best cyber risk policy that's right for them? What does a policy cover, and — importantly — what does it not? How can insurance companies leverage premiums to encourage strong security practices, and prevent the moral hazard?

These remain unanswered questions across the industry. Many smart people are working hard to answer them, though. For now, underwriting cyber risk remains more art than science, and until recently has been based exclusively on questionnaires.

A company applying for cyber risk insurance typically fills out a questionnaire, part legal disclosure, part opportunity for self-audit, with a tiny bit of actuarial science thrown in. "If you go out and shop for breach insurance, the insurer is going to send you a questionnaire," Doug Clare, vice president of product management at FICO, says. "Is there a CISO at your company? What kind of data do you have? How many records? Are you storing credit card information? Do you have a disaster recovery plan? Do you encrypt data?"

Because many cyber risk insurance policies are so-called "admitted" policies, meaning they are registered with state insurance commissioners in the U.S. to receive some protection in case of bankruptcy, those questionnaires are public documents. (Some cyber risk insurance policies are non-admitted and are thus less regulated and more opaque in their workings.) For example, the state of Pennsylvania publishes all insurance policies admitted in that state.



CyberSecurity by Chubb^{SM}
Federal Insurance Company

Section 6: Third-Party Modifiers: The appropriate factors should be applied multiplicatively.

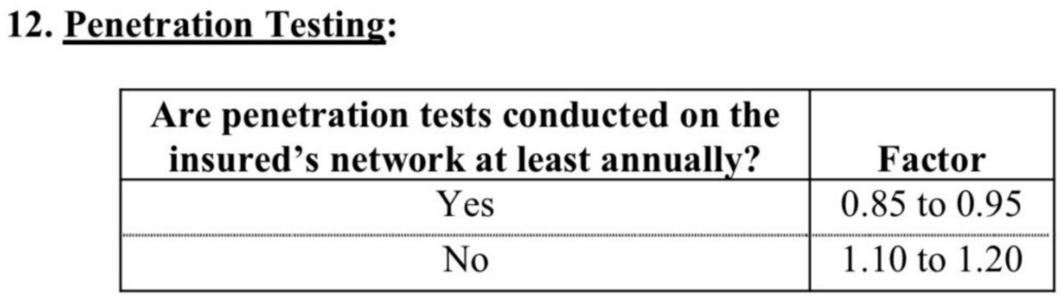
1. **Information Systems Security Policy:** Relevant questions include:

(1) Does the insured maintain an information systems security policy?

(2) Is the information systems security policy kept current and reviewed at least annually and updated as necessary?

Answer YES to	Factor
Two of the above	0.80 to 0.90
One of the above	0.95 to 1.05
None of the above	1.10 to 1.20

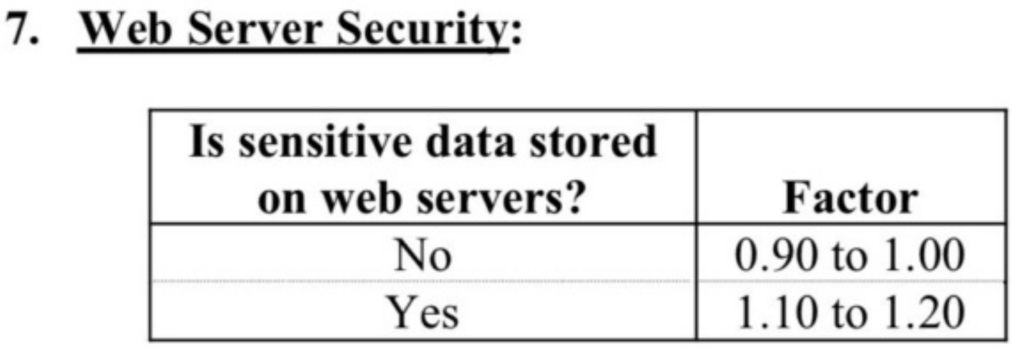
Chubb



12. **Penetration Testing:**

Are penetration tests conducted on the insured's network at least annually?	Factor
Yes	0.85 to 0.95
No	1.10 to 1.20

Chubb



7. **Web Server Security:**

Is sensitive data stored on web servers?	Factor
No	0.90 to 1.00
Yes	1.10 to 1.20

Chubb

Questions from a Chubb cyber insurance questionnaire

Researchers at the Rand Corporation examined more than 180 cyber insurance policies in 2017, including questionnaires used by admitted carriers in New York, California and Pennsylvania. Sasha Romanosky, one of the Rand researchers, explains to CSO how this questionnaire-based underwriting works.

"[Insurance carriers] would start off with a base premium from a lookup table," he says, "and then say, 'if you're in the retail industry we're going to modify that by 1.2 or something, then a battery of questions: Is there any third-party outsourcing? Then multiply that premium by a question on laptop policy' ... the result is a linear product of a bunch of those numbers."

"Some of the policies don't even ask any security information at all," he adds. "They assess your premium based on industry and size. Others go so far as to modify that base premium by different characteristics of the firm."

This subjective method of measuring cyber risk concerns many in the industry, however, and insurance carriers are struggling to quantify cyber risk to put their underwriting on a more sound actuarial footing.

Page 1 of 2 ›

You May Also Like

Recommended by

9 considerations for selecting a DLP solution: An unusual approach

IBM, Intel, AMD take different routes to hardware-based encryption

6 top security technologies to protect remote workers

FEATURE

Does cyber insurance make us more (or less) secure?

Underwriting cyber risk remains more art than science, but in the absence of regulation, cyber insurance might still be the best hope for improving cybersecurity practices across the board — at least for now.

By J.M. Porup

Senior Writer, CSO

JUN 18, 2018 3:00 AM PDT

‹ Page 2 of 2

Quantifying cyber risk

Insurance is all about the data. In a perfect world, if you knew exactly how often *Bad Things Happen*, you could perfectly predict how often any given company might suffer a *Bad Thing*. The result would be fair insurance premiums that spread the risk across a large pool of companies, to the betterment of all society.

Alas, that is not the world we live in — at least, not yet.

To make things worse, even if you had a complete set of data for every cyber incident for the last 20 years, it wouldn't make measuring risk much easier, as threats are constantly evolving. The holy grail for cyber insurance carriers, therefore, is real-time data about today's threats, to anticipate threats just over the event horizon.

In pursuit of that goal, over the last several years companies like FICO, BitSight, SecurityScorecard, and risk modeling companies like AIR Worldwide and RMS, have begun researching how to quantify the problem in real time. Many scan the entire IPv4 address space once a week, web-scrape SEC filings looking for breach notifications, analyze who is using what cloud provider, and so forth. Several sources told CSO they welcomed the advent of the GDPR breach notification law as a way to acquire more and better data to model cyber risk.

"What I hope is that insurance companies will figure this out in an objective, justifiable way what kind of security controls work and which don't," Romanosky says. "Everyone would like to see something objective and quantifiable, it makes everyone's life easier. We all have this sense that if we could turn everything into a score, it would be easier for us to decide and to rank things."

These efforts to quantify cyber risk focus on uncovering correlations between a company's public-facing security posture before and during a security incident, and compare breached companies with those that have not (yet) suffered a breach. Correlation is not causation, of course, but at macro scale in the insurance business, correlation is sound actuarial science. It's all about the statistics.

Turns out there is a significant difference between companies that have suffered a breach and those that have not, Clare says. "The FICO enterprise security score is essentially a machine learning model trained against examplars — several thousand breached organizations and many more thousands non-breached organizations," Clare says. "We look objectively at the problem, and we associate what we can observe in terms of internet-facing network assets against a corpus of breach exemplars."

FICO, of course, are the same folks that do consumer credit scores and have been around since 1956. A few years ago, it decided to get into the cyber game and bought QuadMetrics, one of the most respected startups in this space. QuadMetrics emerged out of the University of Michigan with initial funding from the Department of Homeland Security.

Just as a credit score might look at factors such as paying your bills on time, or current salary, or employment history, a FICO security score also looks at several dozen features, what Clare says are indicators of security "sloppiness."

While Clare emphasizes that the machine learning features FICO uses are proprietary, he gave CSO three examples. Poor certificate management, such as expired TLS certificates, or use of self-signed certificates, is a red flag, and suggests substandard security practices. Compromised endpoint devices sending spam are likewise an indicator that something might be amiss. Running a public-facing NTP server is also a sign a company may have sloppy security practices.

"Unless you're trying to serve time to the internet, why do you have an NTP server that responds to a ping?" Clare asks. "What else are you exposing that you shouldn't be exposing to the internet?"

While an exposed NTP server might never be the cause of a breach, it is, Clare says, representative of a company's security posture. "If you're not cleaning that stuff up, and don't even know you have it, what else don't you know?"

Security scoring metrics are one of the major trends developing in cyber insurance today and make possible cyber insurance at scale. "You might be able to [use questionnaires] for a handful or a few dozen of your very significant clients, the top 100, or the top 200 clients of yours, but how do you scale it?" Christos Mitas, vice president of model development at RMS, asks. "If you're trying to target the small and medium enterprise market, there's not an easy way to do that."

Drawbacks of security scores

Everyone in the cyber insurance business seems to agree that security scores in combination with subjective questionnaires are superior to questionnaires alone, but security scores have their own drawbacks. "It's kind of like assessing your house by looking at a picture of the outside," Romanosky says. What if the basement is flooded, or the kitchen needs to be remodeled? An attractive exterior could hide severe structural issues.

A company that knew, or was able to guess, what external factors underwriters are looking at could, in theory, game the system by just fixing the public-facing bits that affected their insurance premiums, and not bother to secure the rest. As a result, what security metrics companies really want is a look inside the house, Scott Stransky, assistant vice president and principal scientist for AIR Worldwide, says.

"AIR is part of the Verisk family," Stransky says. "They have a team on the property side, and what they do is literally go around from business to business and they go inside the business in the physical sense. They inspect the sprinkler system, the elevator, the server rooms. Now we know all about that building."

Verisk uses this data to model fire risk, among other things, for example. In a similar way, Stransky suggests, the future of cyber risk modeling might be an inside look at an enterprise's network and systems. "Can we stick this flash drive into your system?" Stransky suggests AIR might one day ask clients. "If you do this, we're able to give you discounts on your insurance."

Quantifying cyber risk for any given company is a hard problem, but what really keeps people like Stransky up at night is the interconnected, and interdependent, nature of the internet. A key strategy of insurance carriers is to diversify their risk portfolio — if every insured company gets hit by an attack at the same time, the resulting claims would bankrupt the insurance carrier.

Worse, if the insurance carrier itself faces the same risk as their clients, that's a recipe for disaster. "We do have a real problem with cyber insurance's ability to not carry the same risk it is insuring," Éireann Leverett, founder and CEO of Concinnity Risks, tells CSO. "If you insure against floods, you don't want your headquarters in New Orleans. You don't want to be a victim of the same risk you are insuring against. How does someone insure against cyber risk without potentially being at risk of a cyber event themselves?"

The increasingly centralized dependence on cloud providers, in particular, has a lot of insurance carriers worried. An attack, or an accidental failure, of a top-three cloud provider could cause widespread outages leading to billions of dollars in losses within a few days, a joint report by Lloyd's and AIR concluded earlier this year.

What happens if AWS goes down?

Insurance wonks talk about "cat risk," short for catastrophic risk. Insurance carriers themselves have insurance — so-called re-insurers — and at a macro scale, re-insurers are thinking out loud about how to mitigate cat risk in the cyber insurance market.

In a report entitled "Cloud Down," Lloyd's of London and AIR Worldwide examined the systemic risk posed by widespread reliance on centralized cloud service providers, especially Amazon's Web Services (AWS), which has more than 30 percent of the cloud provider market as of this writing.

"Given the state of the cyber insurance industry today," the report concludes, "a cyber incident that takes a top three cloud provider offline in the US for three to six days would result in ground-up loss central estimates between $6.9 and $14.7 billion and between $1.5 and $2.8 billion in industry insured losses."

That kind of systemic risk is like if you only insure houses in South Florida against hurricanes. If a hurricane destroys all those houses, your insurance carrier goes out of business. Likewise, if all your customers use AWS, and AWS goes down, your insurance carrier might go bankrupt trying to pay all those claims at once.

"Security breaches are bad, but tend to impact one company at a time," Stransky says. "Limits are relatively low, insurers can handle payouts like that. On the other hand," he points out, "with business interruption, now imagine a major cloud provider like AWS failing. Now it's not just one company being impacted; it's multiple companies that rely upon that cloud."

The report emphasizes that both accidents and malicious adversaries could take a cloud provider offline and disrupt business for the cloud's customers. The report cites the April, 2011 AWS outage that cascaded across multiple availability zones in Amazon's U.S. East region.

Even more terrifying than cat risk is the worrisome cocktail of moral hazard and cat risk combined. If everyone passes the buck, and nobody does the hard work to secure all the things, then we face potentially catastrophic consequences, not just for shareholders, but for society as a whole.

Worse, companies acting in good faith, who perform their due diligence, who purchase cyber insurance to transfer only residual risk, who consider cat risk and deploy adequate redundancies, working their hardest to do the right thing could still be severely damaged by a nation-state attacker. Dealing with incompetent enterprise security is a solvable problem, given appropriate regulatory and fiscal incentives. Dealing with nation-state attackers determined to engage in espionage or sabotage is a different kind of problem entirely.

How, if at all, can cyber insurance deal with the risk of cyber war?

Insuring against cyber war

Crack open a typical consumer insurance policy, and you will notice that your car insurance does not cover acts of war or terrorism, among other standard exclusions. When it comes to cyber risk, however, any enterprise doing anything remotely interesting has nation-state attackers in their threat model. Such adversaries may want to steal intellectual property, or spy on international trade deals, steal customer databases for espionage purposes, or even disrupt business operations.

"A big topic of interest in cyber insurance are exclusions," Clare says. "Do the customers — the insured — understand the exclusions? Are they appropriate? Should they be pushed back on? That's an open debate and constitutes something that's payable versus that's not payable."

Insuring against the background noise of the internet — automated attacks like Conficker, easily mitigated XSS or SQLi attacks, and so forth — is one thing. Insuring against a determined human attacker with the resources of a nation-state is problematic, to say the least. Defending against an advanced persistent threat (APT) in the private sector is extremely difficult, and enterprises are asking insurance carriers for policies that cover cyber war. With some exceptions, most cyber insurance carriers are refusing to insure against such risks.

"War is not insurable," Mitas says.

Things get tricky in the cyber domain, though. What, exactly, is "cyber war"? If a foreign army invades and a tank crushes your car, it's clear your car insurance isn't going to pay out. The nebulous definition of what constitutes "cyber war" makes this less obvious. Most cyber insurance policies contain a war exclusion, but what does it exclude, and when does that exclusion kick in? The plausibly deniable nature of many possible acts of "cyber war" makes insurance carriers uneasy.

"Many [cyber] policies have a war and terrorism exclusion within them," Stanley tells CSO. "Of course, one of the challenges is that as soon as there is a cyber attack, you don't know who's done it. It could be a spotty kid in his bedroom, or an Eastern European gang, or the North Korean cyber army. Even if you think it is them, the first thing they are going to do is deny it. So that is definitely a challenge."

Not everyone agrees that cyber terrorism is uninsurable, however. Leverett compares malicious actors online to piracy in the days of sail. "Piracy didn't go away, but global trade on the high seas became safer and safer over time," Leverett says. "The insurance business played a role in that. In some cases, insurers would hire former pirates to come and live in London and tell them how piracy worked. Once they even installed a pirate as a governor of one of the West Indies islands."

Nation-state hackers can do more than sink a ship or two, though, and can create chaos at scale. A common, but by no means universal, exclusion denies claims based on damage to physical property or loss of human life. For instance, an act of "cyber war" that destroyed a business-critical database might be covered, but an act of sabotage by a foreign power — attributed or not — that causes your factory generator to explode, destroying the facility and killing employees, might not be covered. "It's an open question still, and quite worrisome for the whole industry," Mitas says.

Is a "cyber 9/11" or Hurricane Andrew on its way?

When Hurricane Andrew smashed its way through South Florida in 1992, not only were the people of Florida devastated, so were their insurers. Too many insurance carriers under-rated the risk of such a catastrophic storm, and many of those insurance carriers went bankrupt. The hurricane was a wake-up call to the insurance market to re-assess how they modeled cat risk. We may be in a similar situation today.

Insurance carriers want to sell cyber insurance based on quantified risk, with lower premiums for enterprises that deploy strong security controls. That's the world we *want* to live in, but it's not the world we *do* live in today. How we get from here to there is less clear, and some insurance experts worry we may need to suffer a catastrophic loss event before we understand the true nature of the risk.

"Today if you live in Texas, you can get hail resistant shingling on your house, and if you do that, the insurer will give you a cheaper insurance policy, because your house is less likely to suffer a loss in a hailstorm," Stransky says. "Frankly the only way to get there is a major cyber event. We had to have Hurricane Andrew to understand hurricane risk. We hate to say it, but it will probably take a big event to shake up the market."

Such a catastrophic event, in an interconnected world, could cause a domino effect that would wreak havoc across the internet. In one blow it would bankrupt enterprises and insurance carriers, and throw the matter into the lap of the so-called "insurer of last resort" — the government.

The savings and loan scandal of the 1980s offers a warning. Savings and loans across the United States engaged in gross negligence, offering bad loans to customers who couldn't repay them. When those borrowers defaulted en masse, the savings and loans failed and went clamoring to the FSLIC — the government-run insurer — to be made whole. The resulting bailout cost American taxpayers more than $100 billion.

To avoid such a scenario, security professionals need to overcome their knee-jerk dismissiveness of cyber insurance, Leverett says. "Many hackers probably haven't read Ralph Nader's 'Unsafe at Any Speed,'" he says. "Reading about how that consumer rights activism changed an entire industry — the auto industry — and forced them into something more than compliance, which was actual liability.... I think that could happen here, if we put the right amount of pressure."