All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Cyber (whatever that is) insurance yet again?

There seems to be a lot of media these days about cyber-insurance. This is not the first time this has come up, and in the past, it has largely been a failure. Normally I would now talk about the misuse of the term “cyber”, but for this article only, I will let it go. That's because this is the first time I think it has a real chance of success, and I think that's pretty important.

But success at what?

In order for insurance to work, several things have to be true. It's not just a matter of some insurer offering to fix or pay for what happened. The insured has to pay for the insurance, and it has to be profitable for the insurer as well as a benefit to the insured. And perhaps even more important to me, effective insurance drives improvements by the insured.

It's about the pool

If you ever had a pool, you know that children have a tendency to want to jump in and also have a tendency to drown. That's why you need to have an enclosure around a pool. It's in the building codes for a lot of places, and it's most certainly a condition of insurance against death by drowning in your pool. This probably wasn't so the first time an insurer paid off a claim for a drowning, but it has been for a long time. That's because insurers figured out that there is a level of diligence required in order to safely operate a pool, and to get insurance for your pool against drownings, they figured you had to be diligent to some reasonable level. As an alternative, you could pay a far higher premium and let children drown in your pool, but even this is not really tolerable to insurers or society as a whole.

The pool is a good analogy to the cyber insurance world. In the early days of cyber insurance, and largely but increasingly less today, you can get insurance for cyber-events without having a diligent protection program. Insurers have started asking questions, like whether you have a firewall, but that's not really enough for something so complicated. If you don't have a firewall, you don't likely have a computer, because most computers today have firewalls built into the software. But the “Yes” answer to that question is not adequate to indicate diligence or to differentiate between diligence and negligence. While there are standards, you can follow them and still be negligent and you can not follow them and be diligent. There are no current equivalents of building codes, so nobody comes and inspects your protection systems from the city / county to verify that they won't fall over in the next cyber storm.

Not that kind of pool... the other kind

But I digress (as usual). The pool that has everything to do with insurance is the pool of insured parties who the insurer uses to spread risk. Insurance is a form of betting, and like the house in gambling institutions, the idea is that the bank always wins in the long run. That's because the bank, or in this case the insurer, isn't really making individual bets. Rather, they are making a statistical bet regarding the pool of insured parties. As the pool gets bigger and you get better statistics on the nature of losses smeared out over the pool, you start to be able to understand the bets you are making on a statistical basis and turn them into decisions about the rates you have to charge and deductibles you require in order to make money.

The making money part is really important, and it is a good thing. The insurer then benefits and as more and more insurers are able to benefit, they create a market that tends to have profit margins in a reasonable range, so they all make money and compete on their ability to sell, make better decisions on risks and rates, and offer different coverage. But this is only the beginning of the story.

It's a good deal for the insured as well

Insurance also works because the insured benefit from the bet. In particular, people who are insured by choice do so in order to pay a little bit more every day to avoid losing a lot in case something bad happens. Sure, they are losing money in the bet as a pool, but individuals are deferring their risk of catastrophic loss by paying a certain day-to-day loss which they can afford. It's good for them and it's good for society, because if your house burns down after you have done the reasonable and prudent things to protect it from fire, you would either have to be homeless, have enough cash and/or income to replace it and live in a hotel in the meanwhile, or government (i.e., the rest of the overall risk pool) would have to find a place for you to live. Instead of government doing this, with insurance you have a choice of what you are willing to pay day-to-day in exchange for what your circumstance will be if something really bad happens.

The more the insurers know about how to make good bets, the better it is for the insured. That's right. Organizations that do a good job of protection benefit all the more by having lower rates and deductibles and being able to get better coverage. But in order to do this, the insured have to tell the insurer things about how they do protection. Otherwise, the insurer can't make good judgments and give lower rates where deserved. Of course if you don't do a good job of protection, you will have higher rates, and you deserve them. And if you do a bad enough job, you cannot get insurance, which means you will self-insure, which for many companies means you will go out of business as soon as you sustain enough damage.

So what has been missing?

In order to make good bets, you need good statistical knowledge. But in order to get good statistical knowledge, you need reasonably accurate data about the things that correlate losses to behaviors and conditions. And that's what we are largely missing. We cannot do effective risk management because we don't measure the conditions and the losses and correlate them. And that's what has to change.

Insurance companies can change that, and it's time they did. It's really not that complicated. Insurers have a right to know the conditions effecting what they are insuring. This includes the relevant details about events that have taken and are taking place regarding what they are insuring as well as the protections associated with what they are insuring and any changes to those conditions over time. If your house has a fire suppression system and it is insured on that basis, when you disable the system, the insurer will no longer have to pay unless you notify them, and then they will have the option of changing rates and terms of insurance. If you have a fire and don't report it to the insurance company, you cannot get the insurance payoff, and it won't get applied to your deductible. Perhaps more importantly, if you don't report it, the insurer may not pay off on a larger fire because the smaller fire you didn't report may be relevant to the cause of the larger fire that could have been mitigated if the insurer knew about it. The obligation to report then drives the ability to gather statistics and perform better risk analysis by the insurer, which also drives lower rates for better protection systems.

How does that benefit society as a whole?

For the insured who is getting higher rates because the insurance rates than they “deserve” this is a great potential boon in that they may get far lower rates. But that's just the beginning of the benefits. The insurance company rates, for insurance companies wise enough to apply themselves to it, will be lower or higher depending on the factors that turn out to be important (statistically) in determining outcomes.

For example, if separation of duties and risk aggregation limits turn out to be very highly correlated to loss levels and/or event rates, the cost of insurance will be highly correlated to those factors, and companies will be able to directly decide whether to improve those areas by the effect such a change has on insurance rates. If the improvements are cost effective relative to insurance, they have financial motivation to make those changes. If not, it is better for them to transfer the risks. This then leads to the true cost of protection or the lack thereof, and creates market and pricing information on products and services.

For effective protective products and services, the cost will be determined by the markets, and for ineffective ones, those who seek to sell them will not be able to get enough income to justify the cost of keeping them on the market. Innovation that improves protection effectiveness at a price that sells well will meet this criterion because it is more cost effective than the insurance alternative.

Knowing the insurance cost gives us the information to decide on protection as individuals and enterprises, but also benefits society as a whole. As the aggregate social costs of poor protection are folded into prices and other competitive factors as well as changes to the social environment.

For example, increased surveillance in the society is done by enterprises, in no small part, because they are desperate to find out what is going awry and what to do about it. It is expensive, time consuming, invasive, and usually only part of investigative processes after the harm is done.

There is a financial and social cost to changing passwords, replacing credit cards, having to check your bills every month for frauds, and hearing every week or two about another personal data leak from a company holding your information. Confidence lowers, transactions are less trusted, and the system seems to have more and more weight and worries.

> Why would any rational society want to spend its time worrying about such minutia instead of working toward a vision of the future?

The great hope is that through insurance, all of this will no longer be on our individual and corporate plates. Rather, we will be insured. I don't worry about credit card losses because, by law, my losses are limited to $50 and by contract in most cases to $0. But debit cards are completely different. The bad guys can empty your account and you lose. So of course, we move toward debit cards to move the burden and the risk away from the credit card companies to the consumers.

What we should be doing is building the statistical data and performing the analysis required to determine what works and what doesn't, systematically testing out new ideas against ground truth, and finding what works and doesn't, then doing what works and not what doesn't.

What if it doesn't correlate?

There is, of course and as always, a potential big problem. What if we do all this work, seek out the things that work and don't, drill down to the level it takes to get good facts, gather all the history data, and we find out that it doesn't correlate? What if we try more and different things, and it still doesn't correlate? What if we innovate and try thing after thing after thing and there just isn't a rational way to make good bets? Maybe we find out that there is no rational decision-making in the field and that it's all a big crap shoot anyway.

> **That would be a stunning and extremely important result. It would surprise everyone who has ever worked these issues, and of course, it would make for a helter-skelter world. This would indeed be revolutionary to more or less everything in our belief systems.**

However, I am quite certain that I will not be surprised in that way. My experience tells me that different approaches work better or worse in different circumstances, and that what we need to get things in hand is to do a proper job of getting the relevant data and analyzing it. It won't be perfect and it might not be pretty, but we will get the answers if we spend the time and money it takes to get them. Here are some counter-arguments:

- The attackers keep evolving, so whatever you know today will change tomorrow.
  - Actually, they don't. Attacks today are much like they were 30 years ago. The main difference is scale. And scale is something we can change to the advantage of the defender by reducing just a bit in efficiency. But more on that some other day...
- The technology keeps changing, so all your data will be old before you can use it.
  - Not really. While things are faster, cheaper, smaller, less power consumptive, and more capable, and while we have added better sensors, actuators, and analysis tools, in terms of the things that effect protection effectiveness, very little has changed or is changing. However, the ways people are using technologies has certainly left a lot of holes, and stacking on “crap on crap” that barely functions and will fail when tested maliciously is quite common.

My experience tells me that folks who know more and work harder at it do better in protection than those who don't. My experience tells me that in a few hours I can tell the difference between those who know and do and those who don't know and don't do. If the organization is organized to know and do protection well, it succeeds and has lower costs for better outcomes.

But I think there is a bigger point to be made.

Summary

I think the key point is that society is ready to stop thinking of information technology as new and cool and ready to start really embracing it as a permanent part of the way the World is and will be. The use of standard approaches and well understood methods, some inefficiency in exchange for effectiveness, and the movement toward zoning, inspections, and insurance in the same way as other areas of our lives is an idea whose time has finally come. We need to start measuring this as a society, insurance has been the way this has worked for field after field after field, and I think it will work in this field as well. I think we are at the point where we can and we must do this, and that's why I think it will work this time – or perhaps next time...

