Incentivizing Cyber Security: A Case for Cyber Insurance

Jason D. Christopher
In the wake of recent events—Ukraine, Shamoon v2, WannaCry—providing cyber security continues to be an enigma. Unlike traditional engineering problems, we cannot define the constraints and rules adequately. We lack the data and models to describe the variables, let alone the mathematical function. Our field discusses the problem in terms of colors (red, yellow, green) and scorecards. Despite these seemingly insurmountable issues, there is a clear path to solving cyber risk—because it has been done before.

**Risk and the Seven Seas**

Hundreds of years ago, maritime risk was similarly seen as “unsolvable.” There were storms and shipwrecks—and pirates on the high seas. Companies were losing millions in investments and international trade was impacted.

Fast forward to today. There are still deadly storms, and we still have pirates. But no one would say maritime risk is unsolvable. A majority of international trade occurs via waterways, and luxury cruising is widely popular and safe. So what happened? Yes, the industry enjoyed technology growth—ship hulls changed from wood to steel, sails were replaced by steam or even nuclear power; lighthouses were erected. And, sure, companies had access to more data about threats, both natural and manmade, including pirates. But what was the driving force behind those changes? Investment was always there, so was the technology. The missing piece was the data. And the data came from an unlikely source—insurance companies.

In the 1800s, Lloyd’s of London, which started in a small coffeehouse, began examining the problem of maritime risk. They had data from trade routes, losses and impacts, and the frequency of those losses based on external factors (storms, shipwrecks, coastal regions, pirates, etc.). That information, combined with their confidence in a model they created, enabled Lloyd’s to establish an insurance market and drive positive investment. If a company wanted a lower rate to buy maritime insurance, they would need to have proactive controls, better technology and follow best practices. Lloyd’s effectively drove innovation by insuring the maritime industry had incentives to improve. The better a company was at managing maritime risk, the lower their rate and, of course, the less likely Lloyd’s would need to pay on a claim. Lloyd’s made money, and companies had insurance in case something went wrong. It was a win-win situation.
Fast forward to today. The cyber risk challenge has the same elements of a problem solved long ago. Cyber security risk is largely seen as “unsolvable.” A majority of international trade occurs via digital means and channels. And yes, we have pirates, too. So what are we missing in order to have the same success ensuring security that our maritime counterparts have today?

First and foremost, we are missing data. I’m not talking about data at the macro level. While we undoubtedly need to focus more on gathering meaningful incident data and sharing it wisely, there is a lot of information at the organization level that most risk management teams ignore. For example: What’s the cost associated with a cyber incident? What controls do we have in place to prevent losses due to a cyber attack? Organizations can answer those questions without drawing on external sources and can use the information to quantify and demonstrate the effectiveness of their cyber security programs.

Secondly, we lack incentives. As with the pre-Lloyd’s maritime situation, security professionals do not have appropriate ways to improve their cyber posture. If a cyber security team is doing a good job, its members receive congratulations, and the management team considers it to be “business as usual.” But if an incident or a breach occurs, the CISO could be out of the job. In that instance, it’s a lose-lose situation. The situation is compounded by the fact that most teams either do not report to executives or lack the language and data to communicate and meaningfully impact executive decisions. This, again, goes back to the “red, yellow, green” metrics that our industry is desperately trying to evolve.

To approach this problem, organizations need to use the data they have, quantify and model their exposure, and adopt a language that executives understand. Cyber insurance, luckily, can help with each of those aspects.
The financial and business impact models to quantify risk already exist. The challenge for security personnel is to adapt those models to the cyber security environment. One popular way to view cyber risk is by classifying potential losses due to cyber security incidents in terms of financial and physical impacts. Figure 1 illustrates the quadrant diagram commonly used to detail those losses.

The quadrants cover how these damages might impact first parties (you and your company) and third parties (customers, partners and suppliers). Some of the damages are pretty cut and dry. For example, discussions of first-party financial damages are relatively common for security professionals. Mature security departments should know their response costs, legal expenses and associated revenue losses due to cyber security incidents. The trick to modeling this to look at extreme, yet plausible, events. What would a ransomware attack look like if it hit a valuable data center? What if the organization could not access operation systems?

Figure 1. The Quadrant Diagram of Cyber Risk Impacts

The quadrants cover how these damages might impact first parties (you and your company) and third parties (customers, partners and suppliers). Some of the damages are pretty cut and dry. For example, discussions of first-party financial damages are relatively common for security professionals. Mature security departments should know their response costs, legal expenses and associated revenue losses due to cyber security incidents. The trick to modeling this to look at extreme, yet plausible, events. What would a ransomware attack look like if it hit a valuable data center? What if the organization could not access operation systems?

1 SANS would like to thank Axio for the use of the quadrant figures in this paper.
Security professionals should already be running table top exercises. Creating the model would require the organization to pull together information, in dollar values, to quantify the losses based on those sorts of exercises. Figure 2 provides suggestions on the types of loss data to extrapolate from exercise results.

Security and insurance professionals can similarly gather data for third-party financial damages. Much of this data is available from past incidents and can easily be included in a model. The costs of credit card monitoring, for example, are quite public.
Figure 3 lists damages third parties could seek to recover.

By combining the first two quadrants, companies will have a good idea of the out-of-pocket costs associated with certain types of cyber security incidents. There are, however, an increasing number of cyber security attacks that go beyond mere data breach. Our industry is seeing an increase in specialized attacks on cyber-physical systems, which include both industrial control systems (ICS) and building management systems (BMS). These systems do not just hit the pocket book in the traditional sense, they can also have devastating impacts to the real world.
Potential impacts include equipment breakdown, environmental hazards or even loss of life. Just as for financial damages, there could be instances where a cyber security incident physically affects not only your equipment, but that of third parties as well. These impact categories are operationally defined in the last two quadrants, detailed in Figure 4.

Security and insurance professionals understand that these types of data are available. Companies already collect this type of data for property and casualty insurance, for example. Financial officers may be able to shed further insights into what line items go into each type of expense, but none of the inputs here should be mysterious. The trick, really, is examining the damages under the lens of cyber security. The trickier part is developing a model that can ingest the right data and provide reasonable assurances on what the affects might look like. There are a few different schools of thought how to display those models, including providing simple ranges within engineering norms to performing flashy Monte Carlo analysis with flashier Bayesian networks. How each model works for your organization may vary, but knowing that they exist is a great start to quantifying your cyber risk.
Cyber Insurance Coverage

Having the right data and models in place is only the beginning. To truly incentivize cyber security, there needs to be an active suite of products that can cover each potential impact or loss due to a cyber security incident. There are many cyber insurance products on the market today. Like any security control, there are multiple flavors and coverages that organizations can use to build their cyber insurance portfolio. Data breach coverage, for example would include some of the financial damages and serve as a more traditional cyber insurance policy, but equipment damage and environmental cleanup would not be included in that type of policy. Instead, insurance buyers would need to examine their property and casualty policies for terms related to cyber security triggers. Although most of the policies have exemptions that preclude coverage of cyber security incidents, certain products provide stop-gap measures to mitigate those deficiencies. Interestingly, companies may already have coverage, but they may not fully understand what it includes. Obtaining the right types of coverage and ensuring that they provide adequate protection for your company is crucial. Failing to do so would be similar to purchasing a traditional security control—like a firewall or application whitelisting—but not tailoring it for your environment. Haphazard security extends to insurance policies, too.

Imagine the following case where an organization collected its data for all four quadrants in the quantification exercise described earlier. They found damages in three quadrants, as illustrated in Figure 5.

Figure 5. Damages Incurred in the Quantification Exercise
Upon examining their insurance portfolio, which would have damage limits and exemptions, they find that they have partial coverage on the first-party financial damages, full coverage on third-party physical (property) damage, and no coverage on first-party property damages (see Figure 6).

In this hypothetical example, the organization needs to take steps to tailor its insurance response to ensure adequate coverage. That customization of the policy would, in turn, ensure that the investment in insurance is well-spent and appropriate managed.

Figure 6. Insurance Coverage for Damages
When appropriately managed, cyber insurance can become another tool in the risk management toolbox. For decades, we have discussed accepting, mitigating, tolerating or transferring risks associated with cyber security. As a profession, we have become experts at the first three: We are always accepting, mitigating or tolerating cyber risk. We hardly ever discuss transferring it, though. Transferring risk requires a keen understanding of the affects and losses due to a cyber security attack, as well as the mechanism to transfer those potential expenses. Insurance is one of those transfer mechanisms. Partnering with an insurer transfers the financial responsibility for the risks a security team manages to the insurer. There are perks to such arrangements.

During a cyber security incident, insurers can provide funding for forensic firms, ransomware specialists, breach coaches, lawyers and more. These services are vital during an incident, but they are not services for which a security team has additional funding.

As an organization becomes better at measuring and managing its cyber security program, it may be able to decrease its insurance rates and still receive the same (or better) coverage. Insurance companies are incentivized to ensure that their clients have good cyber security programs. No one wants to see a catastrophic incident.

Having cyber security technology is not a silver bullet to protect against breach or loss, and simply having cyber risk management does not provide one either. If your organization does not have basic protections in place, it would not be prudent to invest in cyber insurance. Likewise, any investment in insurance should be part of an overall risk management approach that includes sustaining and improving a living and evolving cyber security program.

When data, models and insurance coverage are combined, organizations can start to truly manage their cyber risk and become cyber resilient. Security is more than technical controls, and insurance can help provide true financial controls to cyber security. Moreover, insurance is something that speaks to executives. They are well aware that having insurance transfers risk from the business. By building the tripod of data, risk models and insurance coverage to accommodate discovered risks, cyber risk can be solved, just as maritime risk was solved in the 19th century.
Jason D. Christopher is the chief technology officer for Axio. His responsibilities include providing technical leadership on security and resilience issues relevant to Axio, its partners and clients, and the development of all Axio technology platforms for security metrics and benchmarking.

Prior to joining Axio, Jason led the research for cyber security metrics and information assurance at the Electric Power Research Institute. Previously, he was the technical lead for cyber security capability and risk management at the U.S. Department of Energy, where he managed the Cybersecurity for Energy Delivery Systems Operations program, which included the Cybersecurity Capability Maturity Model and other collaborative efforts. Jason also served as the program lead for both Critical Infrastructure Protection Standards and Smart Grid Security at the Federal Energy Regulatory Commission.

Jason has worked on a variety of infrastructure projects, particularly in the field of industrial control systems design and implementation. He has also researched and designed technology systems across multiple industries, including energy, water, transportation and communications. He has been a representative on the Federal Smart Grid Task Force, the Critical Infrastructure Protection Committee (CIPC) and other technical committees.

Independent of his work at Axio, Jason is a member on the Institute of Electrical and Electronics Engineers (IEEE-USA) Energy Policy, Communications Policy, and Research & Development Policy committees. Over the past decade, Jason has focused on the development of cyber security standards and practices for the nation’s critical infrastructure. He is also an instructor in the industrial control systems (ICS) program at SANS.

Outside of the workplace, Jason focuses on science, technology, engineering and mathematics (STEM) education issues. He has lectured at several universities across the country and developed cross-disciplinary courses focusing on resilience, sustainable energy and community design.

Jason holds a Bachelor of Science degree and Master of Engineering degree from the State University of New York at Binghamton, and a Master of Engineering degree in electrical engineering from Cornell University.
## Upcoming SANS Training

Click here to view a list of all SANS Courses

<table>
<thead>
<tr>
<th></th>
<th>Online</th>
<th>Anytime</th>
<th>Self Paced</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS OnDemand</td>
<td>OnlineUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>