Global Insurance Market Opportunities

Silent Cyber Scenario: Opening the Flood Gates

By Jon Laux and Matt Honea

About the GIMO

Since its launch in September 2015, the Global Insurance Market Opportunities report has quickly become a leading thought leadership study and reference document for the re/insurance industry.

In 2018, we are taking a new approach to its distribution by publishing articles throughout the year under the banner of Global Insurance Market Opportunities, rather than launching the single, comprehensive report. In so doing, we aim to increase its utilization, bring our ideas to market as fast as possible to support further development with our re/insurance client partners, and make it easier for GIMO readers to digest the wealth of content generated annually.

This report was a collaboration with the Cyence Risk Analytics product team at **Guidewire**.

Over the past few years, cyber risk has moved from imagined scenarios to become a threat that is increasingly real and prevalent.

Cyber insurance products are growing quickly, but at roughly USD 4 billion in premiums they comprise less than 0.3 percent of the global property-casualty market. The greater concern for the insurance industry is the potential "silent cyber" risk residing in traditional property and casualty policies—this is the risk that a cyber event could trigger unexpected payouts under existing policy wordings.

Concerns about silent cyber risk are not unfounded. In December 2015, Ukraine experienced widespread power outages lasting about six hours due to malicious code. A further malware attack in 2017 caused widespread disruption to services throughout Ukraine, and spread to certain U.S. and European multinational companies operating there. This attack – referred to as NotPetya – generated claims both on property and affirmative cyber insurance policies. In mid-2018, an evolved version of the malware used against the Ukrainian power grid has successfully infected critical infrastructure in Eastern Europe. The level of sophistication behind this new malware – dubbed GreyEnergy – suggests that critical infrastructure remains both targeted and vulnerable.

Recognizing the potential for a cyberattack to cause potential physical damage and insurance claims in the U.S., Lloyd's of London and Cambridge University published a widely read report[1] on the potential consequences of a hypothetical attack on the Northeastern U.S. power grid, which include insurance claims spanning property, general liability, management liability and other policies. Other areas of critical infrastructure are also at risk but have been less scrutinized than power generation. In this paper, we create silent cyber scenarios in which a cyberattack on a hydroelectric dam in the United States impacts local businesses and homeowners.

1 https://www.lloyds.com/news-and-risk-insight/risk-reports/library/society-and-security/business-blackout

AON
Empower Results®

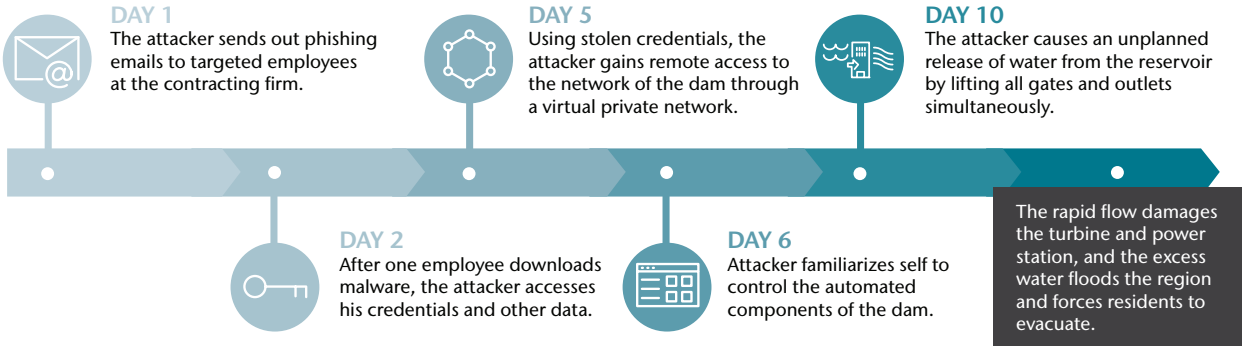
There are over 90,000 dams in the U.S., serving purposes including irrigation, hydroelectric power, flood control, and recreation. With the vast majority—93 percent—being owned and operated by state and local governments and private companies, most U.S. dams are not tightly regulated for cyber-security. Yet dam operators are increasingly automating control systems, both to realize efficiencies and to capture real-time data that improves dam safety and operation. While automation certainly has benefits, it also creates new risks. In 2013, an Iranian national, Hamid Firoozi, successfully breached the control system of a dam in Rye Brook, New York. Firoozi could have remotely operated the dam's gate if Rye Brook's electronic gate controls had not been taken offline for maintenance at that time.

Furthermore, recent assessments by the Department of Homeland Security and the Office of the Inspector General have highlighted poor security practices including weak network segmentation and access controls.

Dam Attack Scenarios

In these scenarios, a threat actor seeks to create massive disruption in the U.S. by causing flood damage. The threat actor identifies an engineering firm that has been contracted to support the IT systems at a hydroelectric dam, and through carefully crafted phishing emails, gains access to the engineers' system. Once in the engineers' network, the threat actor waits for an engineer to log in remotely to the dam's control systems and captures their login information. The threat actor then uses these credentials to access the system.

After several days of reconnaissance in the control system network, the threat actor has learned the commands used for the dam operations, including the controlled release of water by raising the gates and outlets. At this point, the threat actor executes a command to raise all gates and outlets to maximum height, causing an uncontrolled and unscheduled outflow of water. This sudden outflow damages the turbines at the hydroelectric power plant, as well as causing rapid and massive flooding downriver to homes and businesses.



Damage Impact to Insurers and Society

We analyzed the potential impacts of the scenarios at three U.S. dams, selected to reflect small, medium, and large exposure value, respectively. The dams have potential cyber exposure due to their use of technology and industrial control systems (ICS), and demonstrate a range of damage levels that could occur from a cyberattack.[2]

Characteristics	Dam 1	Dam 2	Dam 3
Construction type	Earth and rock fill embankment dam	Earth and rock fill embankment dam	Concrete gravity dam
Reservoir capacity	180,000,000 m^3	4,400,000,000 m^3	1,205,000,000 m^3
Floodplain population	115,000	170,000	695,000
Exposed value	$34.5 billion	$37.3 billion	$200.8 billion

If one of these scenarios were to occur, it would likely result in property, liability, and affirmative cyber insurance losses for the dam operator. For purposes of this study though, we are focusing on the much larger potential impacts resulting from downstream flood damages.

2 We acknowledge that this analysis is not exhaustive; while these dam structures may be representative of the water and wastewater sector at large, we excluded several potential complicating factors—loss of life, negative health effects, agricultural impacts, the breach of multiple dams in the same water system or that use the same IT contractors—from the model for the sake of simplicity.

With a team of flood modeling experts, we estimated economic and insured losses for both residential and commercial properties. Our key findings were that a cyberattack would cause:

1. Major impacts not only to dam operations but also to the resilience of local businesses and communities, with the highest economic loss estimated at USD 56 billion,
2. Silent cyber exposure to insurers, with total insured losses of up to USD 9.7 billion, and
3. A significant protection gap that would hurt homeowners and businesses if such an event were to occur, with only 12 percent insured in one of the dam scenarios.

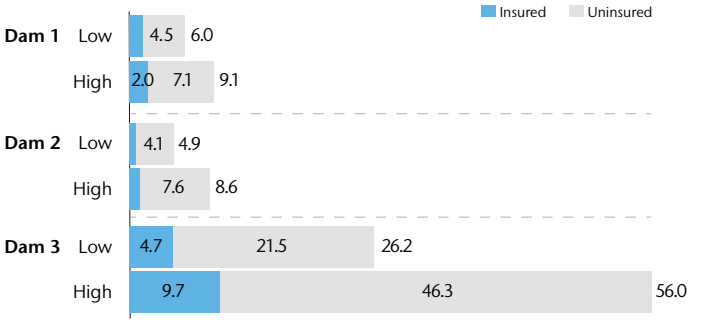
With up to USD 56 billion of economic loss estimated for Dam 3, these numbers certainly illustrate the potential damage from a cyberattack causing a flood.

Note that while Dam 3 shows the highest severity, this does not necessarily imply that it would have the lowest frequency. A threat actor looking to cause disruption to the U.S. would seek to cause the most extreme impacts possible - such is the nature of man-made catastrophes. As a result, the peril of cyber risk may actually "inflate" the tail or increase the likelihood of extreme events relative to what safety experts and flood modelers would expect to see from natural disasters and accidental failures.

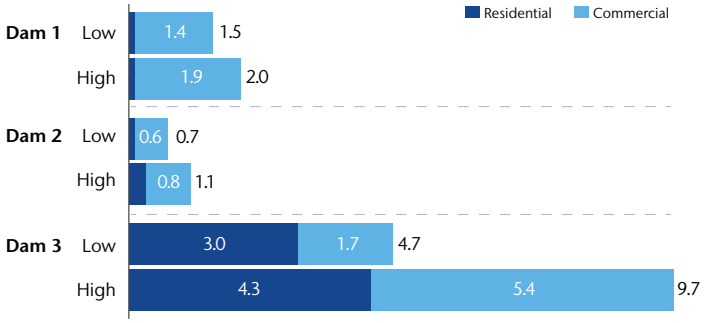
One striking finding is that in all the scenarios, the majority of the loss is uninsured. This is due to low take-up rates of flood insurance, which we will discuss in more detail below.

The losses that are insured are comprised of residential and commercial properties, with residential losses flowing almost entirely into the National Flood Insurance Program (NFIP). NFIP losses could range from negligible to approximately USD 4.4 billion on the high estimate for Dam 3. Commercial insurance losses range from USD 585 million up to USD 5.4 billion across the three dam variants.

Economic Loss Estimates (USD billions)



Insured Loss Estimates (USD billions)



Silent Cyber Implications

We define "silent cyber" exposure as the potential for cyber risk to trigger losses on policies where coverage is unintentional, unpriced, or both. "Unintentional" coverage means not explicitly excluded or affirmed (with any applicable sublimits). Flood policies have unintentional cyber risk because the proximate and covered cause of loss would be the flood—not the cyberattack causing the flood. Similarly, flood policies will not have priced for a rise in flood frequency or severity as a result of cyberattacks. As a result, we conclude that both residential and commercial flood policies will generally have silent cyber risk.

Protection Gap Implications

Although private insurance and the NFIP would each take a share of the loss, the vast majority of loss from these scenarios would remain uninsured. We estimate that of the homeowners affected, very few would have flood insurance, as areas downstream of these dams mostly fall outside of FEMA Special Flood Hazard Areas and take-up of flood insurance outside of those areas is extremely low. We also anticipate many businesses will lack coverage—particularly small businesses, where flood protection is not commonly part of property policies and must be purchased separately, typically from the NFIP. If such a cyberattack were to occur, it would further illustrate the significant protection gap that exists for flood risk in the U.S.

Reinsurance Implications

Generally, affected insurers would have protection from their reinsurers in these scenarios. Property reinsurance treaties provide for direct physical loss—which in these scenarios occurs as a result of a cyberattack. Often, this treaty protection is for named perils, so insurers should ensure that flood is on the list. Cyber-enabled flood damage could also have implications for reinsurers of the NFIP. In the scenarios for Dam 3, reinsurers would be exposed to loss.

Conclusion

These scenarios were created to illustrate how technology and connectivity, while generally seen as beneficial, could have unforeseen and undesirable consequences for businesses and homeowners, and by extension their insurers. Businesses must consider the security risks that new technologies could introduce into their environment, including potential impacts on their clients and communities.

Insurers must also consider how changing technologies can cause "established" perils such as flood to morph into new risks, with resulting changes to frequency and severity. By using scenarios such as these, insurers have the ability to stress test their portfolios against new and emerging perils created by cyber risk. With that knowledge, insurers can take steps to mitigate risk, through reinsurance as well as working with businesses to increase their resilience.

Lastly, we hope this paper draws additional attention to the importance of closing the protection gap as flood risk causes harm to society in the U.S. and around the world.

Learn More

For a detailed review of these scenarios, including key assumptions, additional loss detail, and deeper exploration of the cyber risks affecting critical infrastructure, access the full report at http://bit.ly/cyber-dam-scenario-report-2018.

A reference list is available in the full report.

About the Authors:

Jon Laux is a managing director with Aon's Reinsurance Solutions business and global head of Cyber Analytics. Jon leads a global team of actuaries, consultants, predictive modelers and experts in catastrophe risk focused on helping insurers to grow in cyber insurance and to manage cyber risk effectively through the development of leading edge analytical tools, business intelligence, and advisory services. This team manages the development of Aon CyberMetrica, our probabilistic model for quantifying cyber accumulation risk. He is a Fellow of the Casualty Actuarial Society. jonathan.laux@aon.com

Matthew Honea is the Director of Cyber for Guidewire who has worked extensively in the areas of threat intelligence, network defense, system forensics and discovery, enterprise security auditing, malware analysis and physical security. mhonea@guidewire.com

Other major contributors to this article include Dr. Yoshifumi Yamamoto, also part of the Cyence Risk Analytics team at Guidewire, and Craig Guiliano and Dr. Megan Hart at Aon.

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

www.aon.com

GDM08024

Empower Results®