INCENTIVIZING CYBER SECURITY INVESTMENT IN THE POWER SECTOR USING AN EXTENDED CYBER INSURANCE FRAMEWORK

JINUGU RANJITH[1]PUJITHA MANDAPATI, SWAPNA PADAKANTI
4.DHARAVATH BHADRU, 5.T.VEERA BABU
EMAIL:ranjithjinugu@gmail.com
[1]Assistant Professor, Department of Computer Engineering, Ellenki college of Engineering and Technonlogy, patelguda (vi), near BHEL ameenpur (m), Sangareddy Dist. Telangana 502319.

Abstract

CollaborationbetweentheDHSCybersecurityandInfrastructureSecurityAgency(CISA)and public-sectorpartnershasrevealedthatadearthofcyber-incidentdatacombinedwiththe unpredictabilityofcyberattackshavecontributedtoashortfallinfirst-partycyberinsurance protectioninthecriticalinfrastructurecommunity.Thisresearchexploresthefoundationsof insurancetheoryandadoptsbehavioralmanipulationmethodstoincentivizecyber-security investment. We validate the model by applying power industry performance data from 2013-2015 to assess risk facing the industry. Results show that the model can successfully discriminatebetweenindividualpowercompaniesaswellasgeographicregionsonthebasis of risk and can recommend cyber risk-management strategies tailored to individual risk profiles. The adoption of this framework could invite more market participation, which will createamorerobustcyber-incidentreportingenvironment,contributingdirectlytotheDHS goal of creating a national cyber- incident datarepository.

Introduction

Cyberincidentshavebridgedthedividefromdatacompromisetophysicaleffects.TheStuxnet worm's physical destruction of Iranian centrifuges and the recent cyber induced Ukrainian poweroutagesprovideevidencethatattitudesmusttransitionfrom"whatif?"to"whenwill cyberattacksresultinphysicaldamageinthepowersector?"[1]TheDepartmentofHomeland Security's (DHS) most recent fiscal year's Strategic Plan emphasizes this shift in focus by highlighting cyber security of critical infrastructure as a top priority of their cyber mission.[2] Thepowerindustry'sviability,asthefoundationofallothercriticalinfrastructure'sfunctional capability, is crucial to the national security and well-being of the United States. However, the ownership of the power enterprise remains largely private, presenting regulatory and practicalchallengesinimplementingeffectivesecuritymeasuresacrosstheindustry.[3]

To date, the primary concern of critical infrastructure (CI) operators is to ensure system availability and reliability, while the security of their control systems is considered a secondaryobjective.[4]Theconflictbetweenavailabilityandsecurityisunderstandable,given thatsecurityoftencomplicatesoperations.However,asmorecontrolsystemsareretrofitted forremotemanagementorinternetworkedwith enterprisebusinesssystems,theybecome exposedandvulnerabletocyberthreatsnotforeseenwheninitiallydeveloped.[5]Convincing CI asset owners to further strain budgets by investing in security that may or may not preventdamageisahardsell.Itisdifficulttobalanceavailabilityandreliabilitywithsecurity, andthis,combinedwiththeburgeoningcostsofcyberriskmanagement,presentsahurdle for effective cyber-security implementation in industrial control system dominated sectors, especially the powersector.

Cyber insurance is beginning to garner

attention as a first-party risk management method in the critical infrastructure community. However, the insurance industry is not yet mature enoughtoprovidecost-effectiverisk-transfermechanismstocriticalinfrastructureowners.[6] Collaboration between the DHS Cybersecurity and Infrastructure Security Agency (CISA) (formerlytheNationalProtectionandPrograms Directorate),andpublicpartnershasrevealed thatdataconcernsandtheunpredictabilityofcyberattackscontributetothelackofrobust policy options for critical infrastructure in today's market. To combat these concerns, CISA workingsessionshavedevelopedthreevectorstoencouragemoreparticipationbyinsurers inthecyber-insurancearena:(1)betterinformationsharing,(2)cyber-incidentanalysis,and (3) enterprise risk management (ERM).[7] The establishment of the Cyber Incident Data and AnalysisWorkingGroup(CIDAWG)hasledto moreworkingsessionsbetweenstakeholders in the insurance, cyber security, and critical infrastructure communities which have laid the groundwork for data sharing, analysis, and risk management.[8] However, while there is progress,theGovernmentAccountabilityOffice(GAO)reportsthatthelackofanoverarching data-reportingstructurecontinuestolimittheeffectivenessofvulnerabilityreporting,which remainsacontributingfactortothelackofmaturityinthecyber-insurancemarket.[9]

Practical Implications

Thisresearchproposesanextendedinsuranceframeworktoassessthecyber-riskprofilesof theU.S.powerenterprise.Theframeworkconsidersindustry-providedreliabilityindicators, estimated loss ratios, and various insurance features to recommend an optimal insurance packagethatminimizesrisktoboththeinsuranceofferorandinsuredparty.Minimizingrisk through the adoption of this framework should result in a more robust cyber-insurance marketplace for critical infrastructure companies and should lead to a stronger cyber-securityposturefortheentirepowerenterprise. Asthemarketplacegrows,insurerswillbegin to assume the role of a de facto regulatory authority—power companies seeking to offset riskviainsurancemayneedtomeetbaselinesecurityrequirementssetforthbyinsurersto be eligible for coverage. Furthermore, this framework exemplifies how coverage could be made more affordable by incentivizing cyber- security investment using policy structure as atool.Finally,ascompetitionforbusinessincreases,powercompaniesshouldbegintosee agrowingvarietyofproductsinthemarket,pavingthewayformorecoverageoptionsand, ultimately, moreparticipation.

Perhaps more importantly though, the adoption of the framework will contribute to CISA's working session vectors by creating a better data- sharing environment. This will further the ERM goal by providing the capability to perform comprehensive risk management for individualcompanies,whichwouldalsobescalabletotheentireenterprise.Datacollection andanalysisbytheinsuranceproviderspresents possibilitiesforthedevelopmentofsecurity policy "best practices," likely executed via minimum baselines for coverage, or through continuous improvement of coverage options themselves. Not only would data analysis becomeprevalentforinsuranceprovidersandtheircustomers,butthisresearchcandirectly benefit CIDAWG's goal of establishing a cyber- incident data repository.[10] There is great potentialfortheaggregationandanalysisofcyber-incidentdataacrossthecyber-insurance industry,allowingfordetectionofpatterns,identificationofhigh-riskareas,andmaybeeven activeeliminationofthreats,leadingtoabettersecuritypostureattheenterpriselevel.

Incentives Through Insurance

Early theoretical research in insurance economics led to the belief that self-protection could be encouraged by market insurance if the costs of insurance were inversely related to the quantity of self-protection. [12] Since then, the role of insurance has changed from a pure risk-transfer mechanism into a de facto regulatory authority. [13] The ability of the insurance industry to react quickly in a dynamic environment coupled with the desire to maximize profits naturally led to the manipulation of the insured's behavior by insurance companiesthroughinsurancecontractstructure.[14]Maturearmsoftheinsuranceindustry—auto, earthquake, flood, and medical all feature negative and positive incentives aimed at

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-3, ISSUE-10, 2016
DOI: 10.21276/ijcesr.2016.3.10.2

reducingtheprobabilitythatalosseventwillocc ur.Insuranceelementssuchascoinsurance anddeductiblesareapplicabletocyber-insurancepoliciesandareincludedintheextend ed cyber-insurance framework to incentivize power companies to engage in risk-reduction measures as a condition of the insurance contractoffering.

Methodology

This research evaluates whether using the common insurance features of deductibles and coinsurance can incentivize self-investment in cyber security. In order to perform this evaluation,theauthorsextendedaframeworkin troducedbyYoungetal.forincorporating insurance into critical infrastructure risk strategies to include deductible and coinsurance options. [15] The research methodology consists of two stages: the first stage describes the approachusedtoincorporatetheadditionalinsu rancecomponentsnotaddressedbyYoung et al. The second stage describes the statistical approach used to validate the extended model'sfunctionalityusingreal-worldreliabilitydataprovidedbythepowerindu strythrough self-reporting. Of particular interest is the impact of the model's effect on risks faced by a particularNationalEnergyReliabilityCorporat ion(NERC)regionintheUnitedStatesandthe power industry as awhole.

Extended Cyber InsuranceFramework

Youngetal.proposedaquantitativecyber-insuranceframeworkthatintegratedfourdistin ct models: (1) threat likelihood and severity model, (2) reduction of threat likelihood model, which incorporated (3) Gordon and Loeb's class II security breach investment function, and (4) an insurance premium discount model. This research extended the Young et al. frameworkbyincorporatingtheinsurancecom ponentsofcoinsuranceanddeductiblesnot previouslyconsidered.Eachofthesemodelshas beenupdatedtofittheanalyzeddataused for this research as described below. Table 1 provides an overview of the variables used in theframework.

Table 1. Variables used in cyber insurance framework.

Variable	Definition
Λ	Annual loss severity calculated using self-reported power industry data
T	Probability of an attempted breach
V	Vulnerability of the system
Λvt	The expected loss conditioned on no new additional security investment
Z	Monetary investment in additional security
S(z,v)	Securitybreachprobabilityfunctionexpressingtheprobabilitythat securitywillbebreachedgivenamonetaryinvestmentinsecurityz
A	Effectiveness of security investment

Operationalizing the Framework

To begin, we construct the wealth of a company in a loss scenario. Equation (1) represents this conceptualization, where the wealth in a loss event, W, was reduced by the sum of the insurance premium, P; security investment, z; the minimum of deductible, DExp or loss; coinsurance expenses, CExp; and unforeseen losses above the insurance coverage, ε. This equation will be the foundation of the optimization utilized in this research.

$$Wealth=W-(P+z+min[D_{Exp},S(z,v)\lambda t]+C_{Exp}+\varepsilon)$$

Eq. 1. Wealth post loss event equation

Threat Likelihood Model

Thethreat-likelihoodmodelusesanannualrateofoccurrenceandtheexpectedprobability of a successful cyber attack to derive the impact of a single event from the cost of annual losses. [16] Reliability data reported by the power industry was used to develop the annual losseverity,λ.Whenmultipliedbyvulnerability,v,andthreat,t,thesinglelossexpectancy (SLE) is derived for use as part of the measured risk ratio. The equation for SLE is provided in Equation(2).

$$SLE=\lambda * v * t$$

Table 2. Insurance premium discount model.

Variable	Definition	Derivation
D	Deductible percentage	Model recommendation
C	Coinsurance percentage	Model recommendation
D^*	Amount of loss assumed by insured	$D^*=(\lambda^*D)$
C^*	Amount of loss assumed by insured	$C^*= ((\lambda- D^*)^*C)$
P_0	Base rate insurance premium	$P_0=\lambda- D^*- C^*)^*8\ \%$
r	Rate of discount for investment in security	$50\ \%$
δ	Attained insurance discount	$\delta=r(1- S(zv))$
P	Total insurance premium	$P=P_0(1- \delta)$

Cost Sharing

The cost-sharing mechanisms of deductible and coinsurance generate premium discounts thatprovidetheprimaryincentiveelementthatdifferentiatesthismodelfromitspredecessor. These elements position the insured to assume partial responsibility for incurred losses, increasing their risk while reducing the risk of the insurer. The result of the additional risk assumed by the insured is that they are not expected to pay as much for coverage, but are alsoincentivizedtotakeadditionalactionstoreducelossesinordertopreservetheirwealth.

Inpractice,deductiblesareconsideredfirstwhenmakingaclaim,wheretheinsuredwillpay the minimum of the entirety of the deductible or loss amount prior to the insurer making anypayments.Coinsuranceisthencalculatedontheremainingclaimandsplitbetweentheinsurerandinsuredasdictatedbythepolicy.Table2showstheimpactofcostsharingonthecalculation of insurancepremiums.

Security Rate of Discount

The insurance offeror establishes the security investment discount, r. Policy premium discounts, r%, are determined on the vulnerability reduction as a direct result of security investments. In this model, the security discount offered by an insurance company is assumed to be 50% of the reduction in losses.

Model Confirmation

To ensure that the proposed extension to the Young et al. base model functions correctly, the authors implement a scenario from their published work. We set the extended model's deductible and coinsurance coefficients to zero and repeated the scenario 35 times. We usedtheresultstoestablisha95%confidenceinterval(CI).The95%CIfellentirelywithintheYoungetal.publishedresults.Thisprovidessufficientevidencethattheextendedframework model isstable.

Notes

1 StamatisKarnouskos, “StuxnetWorm Impact on Industrial Cyber-physical System Security,” in IECON Proceedings – 37th Annual Conference on IEEE Industrial Electronics Society, 2011, pp. 4490–4494, doi: 10.1109/IECON.2011.6120048; R. M. Lee, M. J. Assante, and T. Conway, “Analysis of the Cyber Attack on the Ukrainian Power Grid,” Washington, DC, 2016,https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

2 DepartmentofHomelandSecurity,“FiscalYears2014-2018StrategicPlan,”Washington,DC,2014,h

ttps:// www.dhs.gov/sites/default/files/publications/FY14-18%20Strategic%20Plan.PDF.

3 Department of Energy, "Energy Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan," 2010,https://www.dhs.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf.

4 DerekHarpandBengtGregory-Brown,"TheStateofSecurityinControlSystemsToday,"Bethesda,MD, 2015,https://pdfs.semanticscholar.org/4ab7/f69cbf6c8bf72b7d2d24e880cb5fabbf5b50.pdf.

5 OxanaAndreeva et al., "Industrial Control Systems Vulnerabilities Statistics," Woburn, MA, 2016; ICS-CERT, "Environmental Systems Corporation Data Controllers Vulnerabilities (Update B),"2016.

6 National Protection and Programs Directorate, "Insurance Industry Working Session Readout Report," Washington, DC, 2014, https://www.dhs.gov/sites/default/files/publications/July%202014%20Insurance%20 Industry%20Working%20Session_1.pdf.

7 Ibid.

8 Cyber Incident Data and Analysis Working Group, "Enhancing Resilience through Cyber Incident Data Sharing and Analysis: Overcoming Perceived Obstacles to Sharing into a Cyber Incident Data Repository," 2015, https://www.dhs.gov/sites/default/files/publications/Overcoming%20Perceived%20Obstacles%20White%20Paper_1.pdf; Cyber Incident Data and Analysis Working Group, "Enhancing Resilience through Cyber Incident Data Sharing and Analysis: The Value Proposition for a Cyber Incident Data Repository," 2015, https:// www.dhs.gov/sites/default/files/publications/dhs-value-proposition-white-paper-2015_v2.pdf; Cyber Incident Data and Analysis Working Group, "Enhancing Resilience through Cyber Incident Data Sharing and Analysis: Establishing Community-Relevant Data Categories in Support of a Cyber Incident Data Repository," 2015,https://www.dhs.gov/sites/default/files/publications/Data%20Categories%20White%20Paper%20FINAL_v3b.pdf https://www.dhs.gov/sites/default/files/publications/Data%20Categories%20White%20Paper%20FINAL_v3b.pdf.

9 Chris Currie, "Critical InfrasturctureProtection," Washington, DC, 2016, https://www.gao.gov/ assets/690/682547.pdf.

10 Ibid.

11 DepartmentofHomelandSecurity,"FiscalYears2014-2018StrategicPlan,"Washington,DC,2014,https:// www.dhs.gov/sites/default/files/publications/FY14-18%20Strategic%20Plan.PDF.