The Need for National Cyber Insurance – A Lesson to be Relearned

John T. Harvey

Securing a nation's cyber borders requires a high degree of coordination and openness among the relevant units, including real-time information sharing and threat assessment. Unfortunately, however, not only is there little incentive for private sector entities to voluntarily offer the necessary level of cooperation, but policy makers in free societies are reluctant to force such measures on them. Even more unfortunate is the fact that the threats are real, substantial, and have the capacity to have an adverse impact far beyond the initial point of incursion. This raises the question as to whether or not there exist yet-to-be learned lessons that could point us toward a means of motivating businesses and other institutions to accept what would otherwise be unwelcome intrusion and expense.

Defending in Cyberspace

This paper answers with a resounding yes and explains why the nation's cyber defense would greatly benefit from a study of the highly successful historical precedent set by the Federal Deposit Insurance Corporation (FDIC). The problem in that era was that the incentives created by the profit motive were not conducive to systemic stability. Particularly during expansions, individual banks tended to follow portfolio management practices that made them increasingly vulnerable to shocks. Greater risk carries the potential for greater return, and during an upturn, economic agents are inclined downplay risk (Minsky 1986). Competitive pressures may lead others to follow suit, and when and if trouble does emerge, those at the center can be expected to hide the details for as long as possible. Even if this behavior is confined to a minority of institutions, the fact that the financial system is an interconnected web of obligations means that a ripple in one sector has the potential to become a tsunami elsewhere. The situation in cyber security is very similar. Lax security practices—like risky assets—promise greater short-run returns; and, so long as they

John T. Harvey is Professor and Chair of the Department of Economics at Texas Christian University, where he has been employed since 1987. His areas of specialty include international economics, macroeconomics, and contemporary schools of thought. He has served as Executive Director of the International Confederation of Associations for Pluralism in Economics, a member of the board of directors of the Association for Evolutionary Economics, a member of the editorial boards of the American Economist, American Review of Political Economy, the Critique of Political Economy, the Encyclopedia of Political Economy, the Forum for Social Economics, the Journal of Economics Issues, and the Social Science Journal, and was the lead editor of World Economic Review. John has won several teaching and research awards at his institution.

While he has two publications in Military Cyber Affairs, John is first and foremost an economist. His interest in cyber conflict is a function of his long-time fascination with international relations, conventional warfare, and wargaming.

are successful, competition may force others into similar cost-cutting measures. If a successful attack does occur, it is in the best interest of the victim to cover this up—even if there is the potential that it is affecting others as well and the consequences may become much more serious. In both cases, the individual incentives created by the profit motive can contribute to systemic instability. And again, in both cases, it behooves us to develop policies that tie system stability to individual profitability.

The FDIC and Financial Stability

As suggested above, the financial sector is inherently unstable. This is a problem because we need banks and other financial institutions to be on a sound financial footing so that they can provide the credit needed to fund consumer and business spending. A financial market failure can be crippling. Unfortunately, risk and return are inversely correlated and during an economic upturn, banks, etc., show a strong tendency to steer away from safer assets to more profitable but riskier options. This means that throughout the expansion, they are creating increasingly fragile portfolios. Hence, when the next downturn arrives, it is all the more severe, and recovery will be all the more difficult.[1]

This boom-bust cycle is precisely what was witnessed during the 1920s and 1930s. The 1920s demonstrated high rates of growth and low unemployment, the latter as low as 1.9% in 1926 and 3.2% in 1929, just before the recession hit. As expected, banks took on more risk (Calomiris and Wilson 2004: 422). So long as the expansion continued, there appeared to be no need for caution, and there was lots of money to be made. As we know, however, the expansion did not continue, with the economy peaking in late summer of 1929. Throughout the entire decade of 1920s, there had been roughly 6000 bank failures, generally among smaller, rural institutions, already considered to be less stable (FDIC 1984: 33). By contrast, in just the first four years of the

1 See https://scholarcommons.usf.edu/mca/vol3/iss1/4/ for an explanation of the business cycle.

Depression, not only were there over 9000, but these were spread over what had been considered much more secure enterprises (Martens and Martens 2021). There is little question that this historic collapse contributed substantially to the severity of the Depression, and that banks' fragile portfolios were a significant contributor (Benmelech, Frydman, and Papanikolaou 2019).

Because those failures had consequences well beyond the solvency of the individual institutions in question, the government became involved. Though not without controversy, the Banking Act of 1933 was eventually passed, and it included the creation of the FDIC (FDIC 1984: 40). The final version (based on the Banking Act of 1935) included, first, an admission audit for new banks. Those banks then had to agree to additional monitoring above and beyond existing state and federal requirements. The FDIC assessed "the adequacy of the bank's capital, its future earnings prospects, the quality of its management and its usefulness in serving the convenience and needs of the community." (FDIC 1984: 52). And, of course, there was a subscription to be paid.

Bank failures fell from over 4000 in 1933 to just 370 from 1934 through 1941.[2] This was not solely due to the introduction of the FDIC, but the presence of the FDIC was a major factor. And, despite a subscription fee and the requirement of an admission audit and monitoring thereafter, banks—though initially reluctant—eagerly joined once they saw how successful the program had proved (FDIC 1984: 50). Indeed, FDIC insurance became a competitive advantage, with telltale advertising stickers on the door that advertised to the public that their deposits would be safe. Meanwhile, the event against which banks were insuring themselves became far less frequent—which of course was the real goal of the program. The financial system was the intended beneficiary, not the individual banks.

It has not always been clear sailing since then, of course. The deep recession of the early 1980s saw bank failures rise to a peak of 119 (1982), during the Savings and Loan Crisis (1986 through 1995) they averaged over 200 per year, and after the Financial Crisis over 400 banks failed (2008 through 2011). In addition, adjustments have been made to the original regulations. But it is difficult to argue that it has not been a success. Indeed, just a year into the program, the banking industry dropped its "fierce opposition" "in the face of the success of deposit insurance" (FDIC 1984: 50).

Elements of a Federal Cyber Insurance Corporation (FCIC)

A similar achievement is possible in the context of US cybersecurity. The situation is analogous: there exists a critical vulnerability in a key element of our national infrastructure, one that can be mitigated if agents followed more prudent policies and permitted a third party to monitor their activities (possibly in real time). It cannot be ignored because the consequences could be dire, and they go well beyond those directly involved. Unfortunately, individually they have still little incentive to cooperate to grow the program to the scale necessary to make it

2 Data from FDIC: https://banks.data.fdic.gov/explore/failures.

nationally effective. For each agent or enterprise, participation would include surrendering more autonomy and privacy than would be necessary if they simply signed up with a private insurer. If we are reluctant to use a stick however, then we can use a carrot: insurance.

The principles underlying an FCIC would include:

- An overriding goal of securing US cyber borders, achieved by inducing private entities to follow expert-specified protocols and allow real-time information monitoring and sharing and crisis response. *Other features (e.g., the insurance program itself) are merely a means to this end.*
- Within that context, while it will be necessary to devise a schedule of pay outs for various event categories, *the FCIC is not an attempt to solve the puzzle of creating an economically efficient means to price cyber risk*. Again, federally sponsored insurance is but a means to an end. Indeed, private-sector options already exist, however their ability to address systemic problems is limited. They have no incentive to forward information to a central authority capable of determining the possibility of wider attacks, no incentive to reach out to possible targets who are not already customers, and limited financial ability to payout losses (not to mention the difficulty in pricing that they face).
- Given the degree of intrusion by federal authorities that would be required, insurance coverage pricing would have to be quite low to induce robust participation. However, it is important to remember that banks, at first reluctant, embraced the FDIC once it became successful.
- Since the program, unlike the FDIC, would not be self-financing, a working FCIC must be funded entirely by the federal, not state or local governments, because the federal government alone is free of a budget constraint.
- As with the FDIC, the expectation is that even if there is a monetary cost to the program, it would be a net gain for the US with a discernable decline in frequency and severity of costly events.
- Private-sector cyber insurance could be negatively impacted, but this is often true when the national interests are paramount, as here, where added security has become essential.

The outline below further reflects on these essential elements.

Securing the US Cyberspace as Overarching Goal

Cybercrime, cyber espionage, and cyber warfare are serious issues. The frequency and severity of attacks continue to increase, with one projected cost to the world's economy pegged at $10.5 trillion by 2025 (Morgan 2020). And while there is a tendency to monetize and aggregate costs into a single number, the reality is far more complex. How does one really put a price on the lost schematics of a weapon system or the infiltration of a power grid? Nor does anyone need to be convinced that the US is vulnerable.

Eliminating all threats is not feasible, but there are means of limiting them. While non-democratic nations can limit freedoms and resources in order to combat threats, the U.S. must entice private sector cooperation. This is where federally sponsored insurance can play a role. A basic element of an effective program would be well-defined best practices that all insured must follow to qualify. The FCIC would depend critically on this work. Most authorities agree that the overwhelming majority of breaches result from human error, with some projecting this cause as high as 95%, and techniques themselves may be far less important than continuous training and monitoring (The Coyle Group 2019). But federal agencies could easily provide, indeed require, the training (and do now in some cases), and monitoring should be added to their duties, as a vital component of any successful defense.

Pricing is no doubt the greatest challenge, and the primary reason we do not already have a vibrant private sector market for cyber insurance. It has thus far proven impossible to create actuarially reliable estimates of the cost and likelihood of the relevant events (Kshetri 2018). This is not to say that there has not been some promising growth, but in any event the FCIC's goal would not be to develop an ideal means of evaluating risk, but to induce firms to adopt policies that enhance system-wide resilience. Fortunately, one key advantage of public sector insurance is that there is no need to earn a profit. This means that creating reliable forecasts of the likelihood of specific events, with margins of error small enough to ensure the financial viability of the insurance provider, is not an issue. If there is a cyber event, the cost is evaluated–something we already do–and payment is made. It would be necessary to establish how the latter is calculated, but *a priori* risk assessment–normally an expensive component of insurance–is unnecessary. Ironically, public sector insurance could potentially contribute to the data set necessary to determine various probabilities and thus help create an industry for those who would like to offer supplemental or alternative insurance.

If these calculations are not being made, then one might fairly wonder how financing would be determined. For the FDIC, it is via subscriptions. The same could be done with the FCIC, but it is important to recall that while FDIC was initially very unpopular with the banking industry, it became law due largely to its immense popularity with the general public. Cyber insurance is unlikely to command mass appeal, so its passage may depend much more heavily on making it financially attractive to those desiring insurance. Funding via subscriptions would create an obstacle to this goal. If a subscription is to be charged, it could be a token amount based on the firm's annual revenues or profits. Or it could be entirely free: firms are covered by the cyber insurance if they adopt the practices outlined by the FCIC and they permit random audits and real-time monitoring. I suspect that this would be necessary.

Assuming no subscription fee, then data from 2016 suggest that payouts would add around 3% to the federal government's budget (based on the high-end estimate of the cost of cybercrime that year of $109 billion and a federal budget of $3.9 trillion; Chalfant 2018). This is with no reduction in the frequency and severity of the breaches, disruptions, etc., which is of course the primary goal of the program.[3] Where do we get the extra money? The same place we found

3 This also does not count any administrative costs, which would be somewhat mitigated by the fact that existing agencies could either take on the tasks or supply the data necessary to pursue them.

the $2 trillion for the CARES Act in 2020 and the funding for World War II: we simply create it. In neither instance did we borrow dollars from another country or from our own people (who, in both instances, were still reeling from an economic shock: unemployment averaged 8.1% in 2020 and 9.9% in 1941). Resources are scarce, but money is not and it is impossible for the US to default in debt denominated in dollars (Kelton 2020). This has been more openly acknowledged by recent Federal Reserve chairs and is referenced here in a Federal Reserve Bank of Kansas City publication: "As the sole manufacturer of dollars, whose debt is denominated in dollars, the US government can never become insolvent, i.e., unable to pay its bills" (Fawley and Juvenal 2011: 5). Inflation is a potential problem if we continue to stimulate the economy via deficit spending when it is already at full employment, as we did in World War II (when unemployment fell to 1.2% and wage and price controls became necessary). Otherwise, there is no reason to expect inflation to be any more of an issue than it was after the Financial Crisis when in the ten years following the $840 billion American Recovery and Reinvestment Act of 2009, average annual price increases were 1.76%–the lowest of any decade since World War Two.

Another reason why the federal government should help absorb the cost makes sense is that "the US government is likely to end up footing the bill should a catastrophic cyber incident occur" (Knake 2016: 1). Because an ounce of prevention is worth a pound of cure, we should not wait for the disaster to occur but instead act today. As an analogy, consider the impact of Hurricane Katrina. In the end, the federal government financed $114 billion of the recovery (total damage was estimated to be $161 billion; KPRC 2018). Meanwhile, the cost of repairing the levees around New Orleans is estimated to be $200 million, or 0.18% of the amount contributed by Washington (Perlstein 2019). This is not to suggest that the levees alone would have prevented all the damage, but the difference in cost is staggering. And just because the federal government is not budget constrained does not mean that there is not a real savings here. Those dollars were used to activate resources, and many fewer would have been necessary to limit the damage done than were employed to clean up after it. The same is true in cyber.

An essential element of any successful FCIC would be conditioning pay outs on the insured fulfilling membership requirements. These could include the following (based on top cost mitigating factors identified in Ponemon 2020: 42):

1) Forming an FCIC-trained incident response team.
2) Adhering to FCIC-monitored incident response testing.
3) FCIC-approved artificial intelligence platforms and automated breach orchestration.
4) FCIC and Insured Red Team testing.
5) FCIC-supervised employee training.

Also critically important is real-time sharing of data and monitoring by FCIC and periodic audits, with payout discounts whenever, post-incident, there are findings that protocols were not followed.

One issue deserving consideration is the impact on private industry. It has been raised as a concern that a government program could end up crowding out the private sector (Knake 2016 and Woods and Simpson 2017). I do not think that there is any doubt that this would be the case. However, the same is true when we consider the impact of public police protection on private security firms, public libraries on bookstores, public schools on private schools, and so on. This is always the case when we determine that the volume of a good or service forthcoming because of the profit motive falls short of that we believe is in the public interest. Firms would still be free to purchase supplemental insurance and the data collected by the FCIC could be freely shared with private insurers so that they could more accurately price various risks. But in any event, the impact on private insurance should not be a reason not to pursue this avenue.

Lessons not Learned

This essay is not the first place where such a solution has been suggested. Knake (2016) and Woods and Simpson (2017) offer excellent analyses of the costs and benefits of public-sector insurance and describe other governmental efforts to induce industry to adopt safer standards. Despite this and the obvious example of the FDIC, however this lesson has not been learned. No one should expect it to be a panacea or a cure-all, but it would nevertheless put us in a much better position to defend our cyber borders. And, as the massive attacks of 2020-21 have demonstrated, time is now to act (Schneier 2020).

Our national infrastructure and our underlying cyberspace substrate is vulnerable to disruption and collapse and our intellectual property to sabotage and theft. If followed, fast- and ever-evolving best practices and guidelines exist that, will greatly reduce vulnerability, but they cost money. As in 1933, the cyber threat presents us with a range of choices today to include (a) private sector coverage that is partial or substantially complete, (b) public sector coverage that is wholly or partially subsidized, and (c) no coverage (i.e., self-insured.) Accompanying these alternatives again is a range of policies that would include mandated government audits and access to monitor compliance. As is true in the banking industry, some institutions are FDIC-insured, which requires compliance with certain mandated standards, and others are uninsured. If that could be accomplished, then offering insurance against losses from cyber-attack would have a similar effect on cyber resilience that the FDIC had on financial stability. And, just as with the FDIC, the insurance is secondary; the policy is about the system, not the individuals therein.

Thus far, applying this nationwide solution to national cyber security has received very little attention and, where it has, it has been unfairly discounted. This chapter will argue that this is a lesson not learned in the US in particular. We do not have the ability to eliminate cyber risk any more than we can banish bankruptcies, but we can absolutely learn from the FDIC how a Federal Cyber Insurance Corporation (FCIC) might reduce their frequency and severity.

NOTES

E. Benmelech, C. Frydman, and D. Papanikolaou, 2019, "Financial frictions and employment during the great depression," *Journal of Financial Economics*, 133(3), 541-563.

C.W. Calomiris and B. Wilson, 2004, "Bank capital and portfolio management: The 1930s "capital crunch" and the scramble to shed risk," The Journal of Business, 77(3), 421-455.

M. Chalfant, 2018, "Cyber crime costs global economy $600B annually, experts estimate," The Hill, Feb 21, 2018, accessed February 19, 2021, https://thehill.com/policy/cybersecurity/374854-cybercrime-costs-global-economy-600-billion-annually-experts-estimate.

The Coyle Group, 2019. "95% Of Data Breaches Are Caused By Human Error." The Coyle Group Risk Management Blog, December 30, 2019, accessed February 18, 2021, https://thecoylegroup.com/95-of-data-breaches-are-caused-by-human-error/

B.W. Fawley and L. Juvenal, 2011, "Why health care matters and the current debt does not," The Regional Economist, Federal Reserve Bank of St. Louis, 19(4), 4-5, accessed February 19, 2021, https://www.stlouisfed.org/publications/regional-economist/october-2011/why-health-care-matters-and-the-current-debt-does-not.

Federal Deposit Insurance Corporation (FDIC), 1984, Federal Deposit Insurance Corporation: The First Fifty Years: a History of the FDIC, 1933-1983, Washington, D.C.: Federal Deposit Insurance Corporation.

J.T. Harvey, 2018, "An Economics Primer for Cyber Security Analysts," Military Cyber Affairs, 3(1), article 4, 1-44, https://scholarcommons.usf.edu/mca/vol3/iss1/4/.

S. Kelton, 2020, The Deficit Myth: Modern Monetary Theory and the Birth of the People's Economy, New York: Public Affairs.

R.K. Knake, 2016, "Creating a Federally Sponsored Cyber Insurance Program," Council on Foreign Relations, Cyber Brief, November 2016, accessed February 19, 2021, https://cdn.cfr.org/sites/default/files/pdf/2016/11/CyberBrief_Knake_Cyber-Insurance_OR.pdf.

KPRC, 2018, "How much money has federal government paid to cover hurricane damage?" KPRC-TV, Houston, accessed February 19, 2021, https://www.click2houston.com/weather/2018/01/29/how-much-money-has-federal-government-paid-to-cover-hurricane-damage/.

N. Kshetri, 2018, "The Economics of Cyber-Insurance," IT Professional, 20(6), 9-14.

H.P. Minsky, 1986, Stabilizing an Unstable Economy, New Haven: Yale University Press.

P. Martens and R. Martens, 2021, "Wall Street's Casino Banks, Taking Deposits from Savers, in 1929 and Today," Wall Street On Parade, January 4, 2021, accessed February 11, 2021, https://wallstreetonparade.com/2021/01/wall-streets-casino-banks-taking-deposits-from-savers-in-1929-and-today/.

S. Morgan, 2020, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," *Cybercrime Magazine*, November 13, 2020, accessed February 18, 2021, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

M. Perlstein, 2019, "New Orleans' levees won't be up to standard as early as 2023; Louisiana will need $200 million to fix them." WWL-TV, New Orleans, LA, accessed: February 19, 2021, https://www.wwltv.com/article/news/investigations/new-orleans-levees-wont-be-up-to-standard-as-early-as-2023-louisiana-will-need-200-million-to-fix-them/289-97215927-1d99-4383-a1b9-9f1e1494430e.

Ponemon Institute, 2020, "Cost of a Data Breach Study: Global Overview," Benchmark research sponsored by IBM Security independently conducted by Ponemon Institute LLC, accessed February 19, 2021, https://www.ibm.com/security/data-breach.

Bruce Schneier, 2020, "The US has suffered a massive cyberbreach. It's hard to overstate how bad it is," The Guardian, December 23, 2020, accessed February 19, 2021, https://www.theguardian.com/commentisfree/2020/dec/23/cyber-attack-us-security-protocols.

D. Woods and A. Simpson, 2017, "Policy measures and cyber insurance: A framework." *Journal of Cyber Policy,* 2 (2), 209-226.