Changing The Cyber Crime Ecosystem via Systemic Cyber Risk Ownership

By Calvin Liu

The digital revolution which has transformed business is now in the process of transforming much of the infrastructure in the United States. The aggregate increase in business productivity from 1980 to 2007 represents an 84% increase of total output from the pre 1980 or post 2007 productivity growth rates. This business productivity increase due to the adoption of digital technology represents potential infrastructure impact, but is accompanied by the risk of cyber attack.

PPD 21 is intended to address this issue with critical infrastructure in the United States. Above and beyond the dollar value of potential loss, interruption of this infrastructure would entail loss of life as well as permanent damage to the American way of life going forward.

A look at the cyber loss problem is no more encouraging. Europol has termed cyber crime to be more profitable than the illegal drug business worldwide,[1] and even calls "technology at the root of almost all serious crime."[2]

Europol's view is supported by a more recent study which calculates annual cyber crime revenues at over $1.5 trillion.[3]

Cyber crime and cyber attack are societal scale threats due to several factors:

1) Like the digital revolution, cyber crime is at internet scale.
2) Unlike common non-digital crime and even violent crime, cyber does not require physical proximity. It is difficult even to understand if a cyber attack is occurring and who is attacking.
3) Equally unlike many traditional threats posed to critical infrastructure, the source of the threat is not a natural disaster but profit seeking or ideologically motivated individuals and groups.

The wave of cyber related loss being experienced by private sector business is an indication of how difficult it is to stop the profit oriented cyber criminal: despite a $90 billion cyber security industry in 2017,[4] losses continue to grow in scope and severity.

Nation-state and terrorist attackers could only be expected to have greater motivation and potentially sovereign resources such as

[1] Detlef, Robert. "How cyber attacks became more profitable than the drug trade." *Fortune*, May 1, 2015. http://fortune.com/2015/05/01/how-cyber-attacks-became-more-profitable-than-the-drug-trade/.
[2] Colville, Waverly. "Technology is now at root of almost all serious crime: Europol." *Reuters*, March 9, 2017. https://www.reuters.com/article/us-crime-europol/technology-is-now-at-root-of-almost-all-serious-crime-europol-idUSKBN16G1XN.
[3] McGuire, Michael. "Hyper-Connected Web of Profit Emerges, As Global Cybercriminal Revenues Hit $1.5 Trillion Annually." *GlobeNewswire*, April 20, 2018. https://globenewswire.com/news-release/2018/04/20/1482411/0/en/Hyper-Connected-Web-of-Profit-Emerges-As-Global-Cybercriminal-Revenues-Hit-1-5-Trillion-Annually.html.
[4] Muresan, Razvan. "Cyber security spending to reach $90 million in 2017, Gartner says." *Bitdefender*, March 15, 2017. https://businessinsights.bitdefender.com/cyber-security-spending-2017.

the Shadow Crew release of NSA tools in 2017.[5]

The complex web of modern life encompasses a wide range of critical infrastructure ranging from traditional fixed installations such as dams, bridges, power plants and so forth to modern infrastructure capabilities such as banking and finance, telecommunications and the internet.

The Problem

While banking, finance and telecommunications have long employed the Internet in their internal as well as public facing operations, the advent of SCADA systems introduces cyber risk to areas traditionally threatened only by physical damage: utilities, transportation and public works.

It is this confluence of infrastructure capability into the digital realm which is so dangerous. Despite hundreds of billions of dollars in cumulative losses worldwide, the banking and finance industry continue to be plagued by profit motivated cyber crime.

Factors behind this include:

1) Cyber security companies continually deploy technology, but ultimately do not share in their customer's cyber risk
2) Cyber insurance companies offer financial risk pooling, but do not actually improve systemic cyber loss profiles either through direct customer interaction (inspections) or even systematic root cause analysis
3) Digital product and services companies are in no way motivated to focus on cyber security, because cyber security is not a profit maker nor is there civil or criminal liability for insecure products. Even for those companies who do exert an effort to create secure products, cyber security ranks a distinct second priority vs. their primary product and services focus

Another potential factor is law enforcement. While law enforcement (and military defense) are both chartered with prosecution of criminality and defense against attack, respectively, neither vertical is enabled to actually change the business and consumer behaviors which enable cyber crime and cyber vulnerability.

Research has shown that 44% of successful cyber attacks employed vulnerabilities that were known for 2-4 years or more,[6] with 7 of the top 10 exploits being more than 2 years old.[7] Many of the hacks being seen are thus not "Mission Impossible" type expert attacks but rather the use of well known weaknesses packaged into criminal easy to use software. Monitoring compliance against cyber security vulnerabilities amounts to taking over significant portions of IT functionality for the entire private sector – not something which law enforcement and other

[5] Lawler, Richard. "Shadow Brokers' dump of NSA tools includes new Windows exploits (updated)." *Endgadget*, April 4, 2017. https://www.engadget.com/2017/04/14/shadow-brokers-dump-windows-zero-day/.

[6] Martin, Alan. "Top 10 breaches of 2014 attacked 'old vulnerabilities', says HP." *WeLiveSecurity*, February 25, 2015. https://www.welivesecurity.com/2015/02/25/top-10-breaches-2014-attacked-old-vulnerabilities-says-hp/.

[7] Hewlett-Packard Development Company, L.P. "HP Security Research Cyber Risk Report 2015." *HP.com*, March 12, 2015. http://whp-hou9.cold.extweb.hp.com/pub/msc/B9302434-70B4-45CE-AEB7-29F6EAD6E2FE.pdf.

government organizations are well suited for, particularly in an area as dynamic as IT. Even were such to be undertaken, the cost for such an effort would dwarf existing efforts including the creation of the US Department of Homeland Security, post 9/11, since the IT sector grosses well over $1.5 trillion in annual revenue worldwide,[8] over $3.7 trillion by some estimates.[9]

This same lack of focus on cyber security demonstrated by digital product and services vendors is shared by businesses and consumers.

This situation is understandable. Patching and other security behaviors, much less actual security organizations, are very expensive and do not generate a clear ROI. Security products and technology are equally murky in terms of value for expenditure: Even 3 decade old technology like anti-virus (AV) does not show clear differentiation between no AV, good AV or bad AV from an ROI perspective.

Furthermore, the present ecosystem is such that cyber security is effectively too expensive for an SMB (small or medium sized business). While an enterprise can devote tenths of a percent to revenue and project a strong cyber security posture via a multi-million dollar budget, the minimum cost for a modern cyber security department is certainly a six digit cost and likely much more. NIST Special Publication 800-17 lists 14 different areas for its minimum cyber security standards,[10] each area requires some form of expertise which in turn is also costly due to the shortage of skilled personnel.[11] Few SMBs can afford a 6 or 7 digit cyber security spend, and as a result 62% of attacks are conducted against SMBs,[12] often by individuals with no particular skills at cyber attack. This creates an enormous population of cyber criminal "plankton" which can make a living from cyber attacks, and which in turn some proportion will gain in skills and interest to form the cyber criminal "whales" which prey on the enterprise scale companies and governments.

How many plankton are there? Actual numbers are impossible to gather, but there are credible reports of as many as 5 million hackers worldwide.[13] Contrast this with 600 technical FBI agents, a similar order of US military and trained police personnel, and the

[8] "Global revenue generated by the IT industry from 2005 to 2016 (in billion euro)." *Statista*, last accessed April 20, 2018, https://www.statista.com/statistics/273257/worldwide-revenue-made-by-the-it-industry-since-2005/.

[9] CompTIA. "IT Industry Outlook 2016." *CompTIA*, January 27, 2016. https://www.comptia.org/resources/it-industry-outlook-2016-final.

[10] Keller, Sharon et al. "Modes of Operation Validation System (MOVS): Requirements and Procedures Computer Security." *US Government Printing Office (Washington)*, February 1998. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-17.pdf.

[11] Loeb, Matt. "Cybersecurity talent: Worse than a skills shortage, it's a critical gap." *The Hill*, April 17, 2015. http://thehill.com/blogs/congress-blog/technology/239113-cybersecurity-talent-worse-than-a-skills-shortage-its-a.

[12] Miller, Gary. "60% of small companies that suffer a cyber attack are out of business within six months." *The Denver Post*, October 23, 2016. https://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/.

[13] Lew, Yon. "Revisiting Security Part II – How many hackers?." *LinkedIn Pulse*, April 21, 2015. https://www.linkedin.com/pulse/revisiting-security-part-ii-how-many-hackers-yon-lew/.

750,000 employed in private cyber security;[14] the situation looks quite grim. A shift in ecosystem away from criminally reaped rewards to commensurate rewards for systemic risk hunting and mitigation would swing the balance back to a more reasonable ratio.

The cyber loss paradigm is thus not a simple technology issue. Non-cyber security OEMs are not strongly economically incentivized to build secure products. SMBs are not able to afford strong cyber security. Enterprises have clearly struggled to execute strong cyber security despite having the economic capability.

However, the biggest missing component to the ecosystem is a systemic cyber risk owner (SCRO).

Systemic Cyber Risk Owner

A systemic cyber risk owner would be a 3rd party entity that takes on the full cyber risk for its members in return for a services payment. Members would additionally have to abide by policy declarations by the systemic risk owner or be excluded and/or pay significantly higher premiums.

Why is a SCRO important?

First, there is an enormous information gap. Consumers and businesses that are attacked are negatively incentivized to report their losses. There are no positive benefits except in a very general sense and many negative ones such as reputation loss, lawsuits and becoming a target for further attack. Laws which require notification will be complied with, but no law can compel a full and complete accounting for root causes, security overviews of the victim, serious attribution of the attacker or even evaluation of the performance of whatever security technology and personnel were involved.

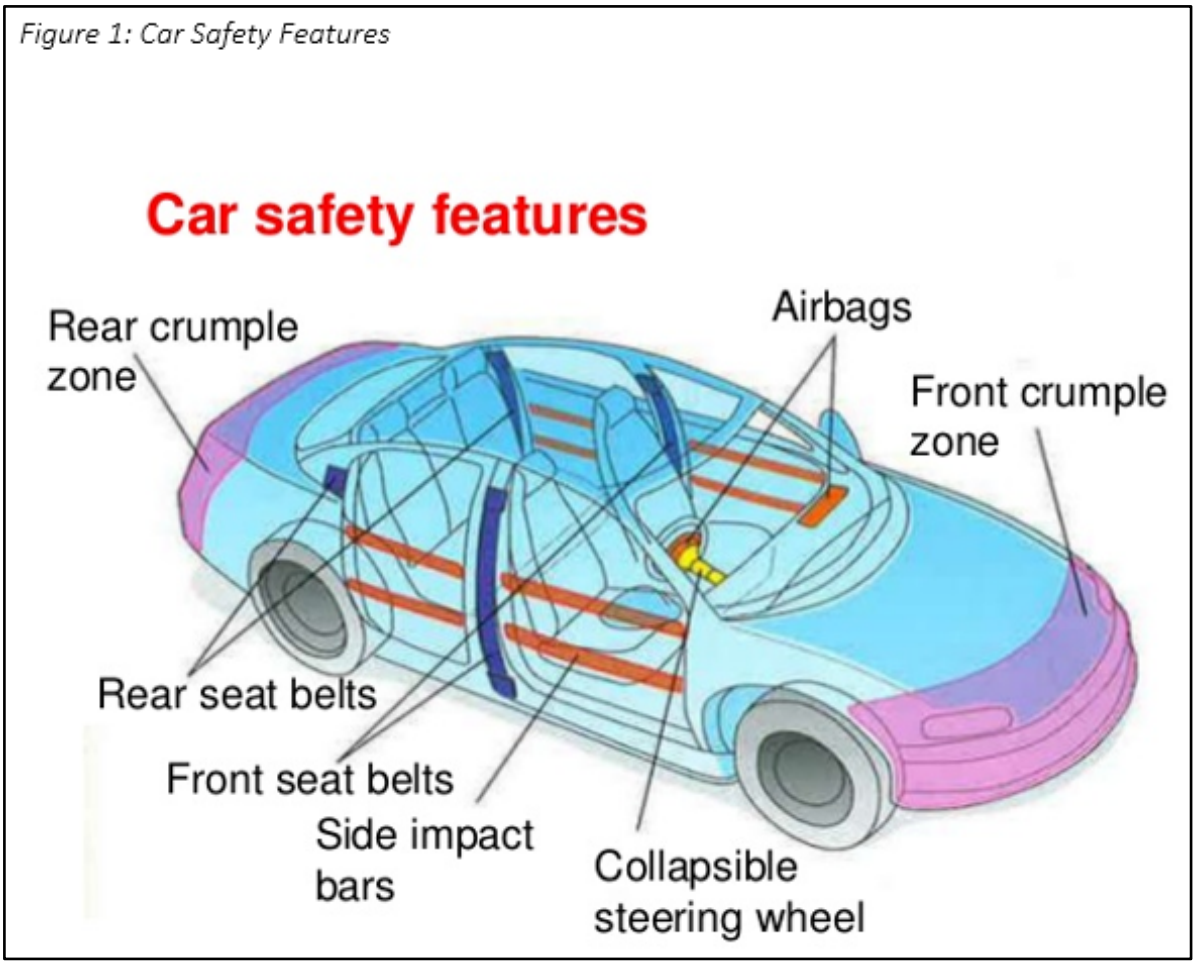
The SCRO, on contrast, would have both the full cooperation of victims and the charter to understanding the true sources of cyber loss as well as the true performance of actual defenses against cyber loss. Victims would report whatever is desired in order to be reimbursed, supplemented by the SCRO's additional work needed to gather information desired.

Second, the acceptance of systemic cyber risk means that the SCRO is incentivized to reduce overall cyber loss as opposed to sell technology or financial services. As noted above, reduction of even 2 year old vulnerabilities could reduce overall losses by 44%. The means to reduce systemic loss is very different than the technology of cyber security or the financial loss pooling of cyber insurance –it would encompass whatever technology and practices are deemed effective by the SCRO as any losses directly impact this organization. A good example of this different approach can be seen with automobile safety and accident losses. Present day automobiles have dozens of systems intended to reduce deaths compared to accident prevention systems. Driver or passenger deaths are the single largest potential losses in an automobile accident. [15]

[14] "Cybersecurity Supply/Demand Heat Map," *Cyber Seek*, last accessed June 6, 2018, http://cyberseek.org/heatmap.html.

[15] Bishop, Steve. "P2.2 car design & safety." *SlideShare.net*, September 9, 2014.

Figure 1: Car Safety Features



Contrast these standardized systems with the still-in-progress field of accident avoidance depicted in Figure 2.[16]

Accident prevention is far more difficult - there are numerous additional variables ranging from the driver's own capability and focus to environment conditions to other driver behavior. It is harder than loss reduction, which is why the loss reduction technologies are widespread while accident prevention technology is still in development.

It is very likely that a similar scenario exists for cyber security: the technology and practices to reduce losses is far simpler to deploy than what is necessary to prevent cyber attack.

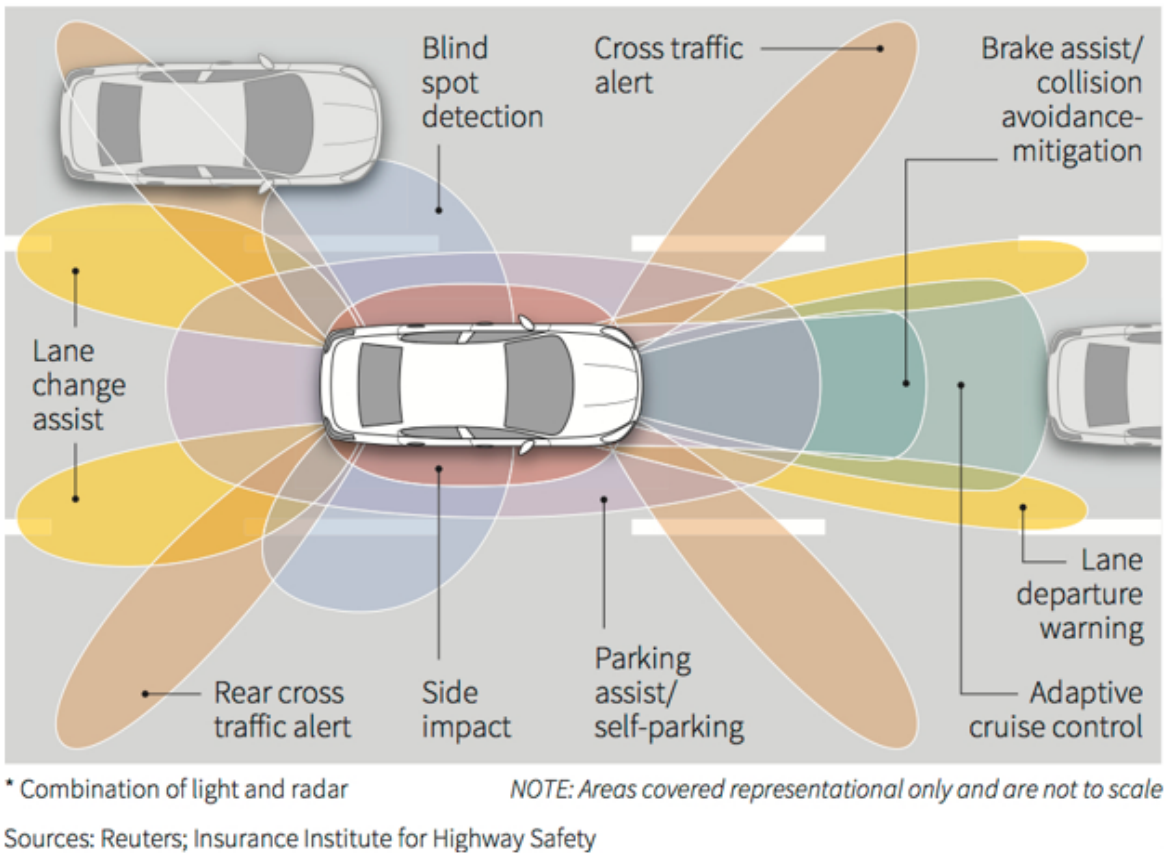
Either way, an SCRO will examine all of the ways to reduce systemic cyber losses including loss reduction techniques as well as loss prevention techniques.

Third, the SCRO thus would also provide valuable, objective performance criteria for

https://www.slideshare.net/sbishop2/p22-car-design-safety.

[16] Baumgartner, Greg. "How Accident Prevention Technologies Increase Road Safety." *LERA blog*, August 30, 2015. https://lerablog.org/technology/how-accident-prevention-technologies-increase-road-safety/.

Figure 2: Accident Prevention Technology



the entire system, not just its participants. Overall reduction of the profits, hence motivation fed into the cyber criminal ecosystem directly benefits everyone including the SCRO.

Fourth and lastly, an SCRO is able to do what no other entity can: change the economic incentives in the cybersecurity ecosystem. At present, the financial rewards for "positive" behavior are far outweighed by the rewards from cyber crime. One example: In May 2016, a technical exploit was published called ImageTragick.[17] This involved a 1980s era open source library called ImageMagick which is used by nearly every social media, blog, CMS and similar media web site in existence because it allows users to crop and resize uploaded photographs. ImageTragick showed that certain types of uploaded photos, specifically the .svg variety, could have program code embedded which the ImageMagick library would then execute directly on whatever server said photo and library were hosted on. It is a hot needle

[17] Ermishkin, Nikolay. "ImageMagick 7.0.1-0 / 6.9.3-9 – 'ImageTragick' Multiple Vulnerabilities." *Exploit Database*, May 4, 2016. https://www.exploit-db.com/exploits/39767/.

through every conceivable layer of security wax.

Fast forward 9 months: in January of 2017, Facebook paid $40,000 to the person who reported ImageTragick functioned on Facebook.[18] While $40,000 is a lot of money, the value of being able to directly access Facebook server content militates a dark web value of well over $500,000. The original reporter of ImageTragick gained nothing from this reward. Even the researcher who proved the problem at Facebook - if Facebook cannot compete with the dark web in terms of "security researcher" compensation, it is impossible for anyone else to nor does Facebook's bounty do anything for the hundreds, thousands, possibly tens of thousands of other potentially affected organizations.

An SCRO as representative of its customers is the best entity to make use of economic scale to equalize the financial incentives between "good" and "bad" cyber behavior. Changing the criminal/defender ratio closer to equality through more equal financial rewards would fundamentally change the human potential dynamic in cyber security.

Obstacles to a Systemic Cyber Risk Owner

Likely objections to an SCRO include:

Scale of risk. Some would argue that situations like Target make it impossible to create an SCRO with sufficient scale. Target experienced a massive cyber breach in 2013.[19] Despite a $100 million dollar cyber insurance policy which paid out $90 million dollars, Target suffered $262 million of cumulative additional losses to date.

In actuality, the cyber insurance industry has managed a 30%+ gross margin despite the ever increasing reports of breaches and losses. Even in 2015 when the bulk of the $90 million Target cyber insurance payout was made, the overall cyber insurance industry had a loss ratio of 65.2% (34.8% gross profit margin).[20] Clearly even the existing financial dynamic can withstand very large losses, much less one where the actual losses are reduced through a new focus on loss reduction.

Ability to propagate systemic change. Since massive aggregate losses, technology, cyber insurance and even government regulation do not seem to have made an impact on escalating cyber losses, will the presence of an SCRO affect systemic change? There are clear precedents across all other risk pools that systemic change is achievable. Some examples include: smoking and health care, seat belts and auto collision related losses, building codes and fire/earthquake losses. Many forms of property and casualty insurance deploy "property management" practices to reduce losses. One example is

[18] Kovacs, Eduard. "Facebook Awards $40,000 Bounty for ImageTragick Hack." *Security Week*, January 18, 2017. http://www.securityweek.com/facebook-awards-40000-bounty-imagetragick-hack.

[19] Finkle, Jim et al. "Target cyber breach hits 40 million payment cards at holiday peak." *Reuters*, December 18, 2013. https://www.reuters.com/article/us-target-breach/target-cyber-breach-hits-40-million-payment-cards-at-holiday-peak-idUSBRE9BH1GX20131219.

[20] Business Wire. "Fitch: U.S. Cyber Insurance Premiums Total $1B Per New Supplemental Filing." *Business Wire (Chicago)*, August 24, 2016. https://www.businesswire.com/news/home/20160824005973/en/Fitch-U.S.-Cyber-Insurance-Premiums-Total-1B.

fire insurance companies inspecting buildings for adequate numbers of fire extinguishers, fire alarms and exits/exit plans.

More importantly is that there are also technology capabilities, which can be leveraged by an SCRO to reduce losses. The fundamental problem with cyber risk and vulnerabilities, beyond focus, is that they are often juxtaposed with fully depreciated and irreplaceable IT assets. The banking sector is still largely dependent on generation old COBOL back end systems, for example.[21] The SMB (small and medium business) equivalent is Quickbooks accounting software running on Windows XP – an operating system released in 2001 which was end of lifed by Microsoft in 2010.[22] In other words, billions of dollars of potential cyber risk losses are hinging on decade plus systems.

The reason for these systems is perfectly valid from a certain standpoint: they are fully depreciated and usage is already enshrined as common practice. However, from a cyber risk standpoint, these are magnets for cyber loss.

It is actually not necessary to choose between a tried and true system vs cyber security. Modern IT practices have enshrined the use of Virtual Machines (VMs) – these are software packages that take advantage of the ever increasing computing and storage power of modern systems to emulate, via software, the operating systems of old. Thus there is no need to combine a 10+ year old PC with Windows XP and Quickbooks – which combines enormous cyber risk with familiarity and convenience. Instead, a modern hardware chromebook with Linux could run a Windows XP virtual machine which permits the Quickbooks and XP environment the user desires.

The second technology development which can be leveraged by the SCRO is Virtual Desktop Infrastructure (VDI). This is an IT practice where the operating system, application software and other user facing capabilities are packaged into a single image to be loaded onto new machines. This is much more efficient than loading an operating system, then laboriously installing software and uploading user preferences. However, VDI can also be used to synchronize operating systems against those vulnerabilities and attacks deemed by the SCRO to be targets to reduce systemic losses.

VMs for customer facing applications, VDI for the underlying public facing interfaces and infrastructure, and digital twins echoing all of an existing IT infrastructure on the cloud are just a few of the examples of loss reduction methods that an SCRO would deploy in its own interest (and to its customers' benefit).

Conclusion

This paper only examines, at the highest level, some the benefits provided by a Systemic Cyber Risk Owner.

The ultimate goal for the creation of an SCRO is to change the ecosystem by which cyber losses are continuing to escalate. This

[21] Colvey, Scott. "Cobol hits 50 and keeps counting." *The Guardian*, April 8, 2009. https://www.theguardian.com/technology/2009/apr/09/cobol-internet-programming

[22] "Windows XP," Wikipedia, last accessed June 6, 2018, https://en.wikipedia.org/wiki/Windows_XP.

present ecosystem is heavily prejudiced to the benefit of the attacker, because the attacker can pick and choose wherever and whenever to conduct operations. The primary counter to this dynamic is the scale of the defense: there are trillions of dollars collectively available in the victim base which can be used to change the ecosystem for the better. Similarly, collection of data and propagation of "loss reduction" mechanisms favors the defender. Preventing the first attack is extremely difficult but is the only choice available for the customer today. Preventing the 2nd, 5th, 100th, or 1000th attack but pooling the loss for the few successful initial attacks is how the systemic problem is addressed.

Failure to change the ecosystem dynamic via the creation of one or more SCROs will only lead to continuing escalation of losses. It is a tribute to the honor and professionalism of the existing cyber security community that worse has not yet occurred, but only a Systemic Cyber Risk Owner can change the cyber risk ecosystem and thus change the course of cyber risk for all.