Global

CRQ Network

Quantifying Systemic Cyber Risk

Report on the "Connectedness in Cyber Risk" Workshop

Global Cyber Risk Quantification Network[1]

San Diego, California
2018

[1] Includes representatives from 4A Security, AIG, Aon, Beecher Carlson, Deloitte, Drexel University, FAIR Institute, FICO, Philips, Risk Lens, Stanford University, The Hartford, University of Michigan, Verisk Analytics and Willis Towers Watson.

Table of Contents

Background

The World Economic Forum recognizes that the risks, rewards and governance of the networked economy are core issues of the global agenda and fundamental for sustainable growth and stability. Additionally, it recognizes that only a coordinated approach will ensure that new opportunities for growth are fully leveraged and risks managed.[2]

Related to the networked economy, the Forum has placed emphasis on investigating cybersecurity in this connected world. At the 2015 World Economic Forum meeting, there was a discussion about quantifying the risk around cybersecurity in order to understand the exposure to the global economy if a cyberattack occurs.

The Global Cyber Risk Quantification Network (GCRQN), an extension of the Partnering for Cyber Resilience work group, was formed to further investigate the quantification of cyber risk. The GCRQN consists of representatives from government, academia and industry. At the second annual meeting held on May 11–12, 2017, the GCRQN focused on the topic of connectedness in cyber risk. The group shared experiences and insights on the latest in risk quantification methodology as it relates to economics, policy making, risk management and society. This report summarizes the perspectives shared by the GCRQN participants.

[2] Partnering for Cyber Resilience, World Economic Forum, September 2012

Connectedness in cyber risk

As a global society, we have realized tremendous economic benefit by connecting technologies into cyberspace. Unfortunately, as our connectedness increases, so does our risk of attack. By transcending our geo-political boundaries, we are now exposed to nefarious activities such as crime, espionage and cyber warfare. Some recent examples include:

- In August 2016, the Mirai botnet infected poorly protected internet devices by identifying those that were still using their factory default username and password. This malware turned networked household devices into remotely controlled "bots" that were used for large-scale network attacks.
- In May 2017, the WannaCry worldwide cyberattack targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments. The ransomware spread itself rapidly across 300,000 unpatched systems, crippling organizations in its wake.
- In June 2017, the NotPetya cyber weapon was deployed globally, primarily affecting the Ukraine where more than 80 companies were attacked, including the National Bank of Ukraine.

In addition, democratic processes around the globe have been perturbed by hacks and the spread of fake news. Attacks on critical infrastructure, such as the central bank in Bangladesh and the electricity grid in the Ukraine, have led to global scares over the possibility that such attacks might debilitate our post-geo-political cyber society.

We are all connected—not just for the benefit of cyberspace, but also in making cyberspace safe. This is no simple task. Several questions come to mind: What are reasonable levels of safety in cyberspace? What efforts should be made to accomplish this? Who should take responsibility for those efforts? How can we ensure these efforts are continuously maintained to be both effective and economical?

Quantifying cyber risk

The quantification of cyber risk is no longer the exclusive domain of (cyber) insurance companies and academia. Utility companies, banks, corporations and governments are increasingly using quantification approaches as part of their business and/or risk management. Across the globe, more and more organizations are reaping the benefits of these cyber risk quantification approaches to efficiently limit their cyber risk exposure. In some cases, such as insurance, this primarily concerns third-party cyber risk. In other cases, such as large banks, this concerns the management of cyber risk within the organization. For multinational companies, it concerns a combination of both.

A number of different methodologies and tools are now available that range from sophisticated cyber risk benchmarks to management-oriented approaches. The uses range from threat and technology oriented approaches to business value oriented approaches.[4] From our experience, all known approaches have one thing in common: They do not (yet) have efficient and reliable tools to take correlations, dependencies or systemic risk into account. There are four interrelated challenges that cause this limitation:

1. **Priority** – Paradoxically, the urgency of cybersecurity on the level of individual organizations limits the amount of attention devoted to systemic risk.
2. **Change** – Innovations involving connected technologies and cyber threats develop increasingly rapidly, making it difficult to keep up with evolving risks.
3. **Complexity** – The huge number of interacting and changing elements requires innovative approaches.
4. **Data** – Companies are not collecting relevant data because it isn't clear which data is needed. In addition, there is a reluctance to sharing data that is available.

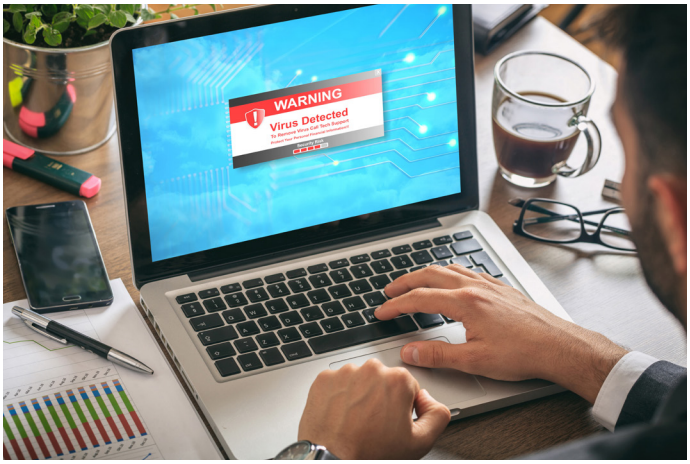
The result of these challenges is that the predominant cybersecurity effort is aimed at the level of individual organizations. We see that larger organizations typically have better cybersecurity than smaller ones, given the high costs involved with obtaining cybersecurity capabilities. There are many interesting parallels with physical security. Historically, investments in physical security were made at individual and local levels. This essentially left individuals to fend for themselves, leading to "Wild West" conditions for public safety and security. Over the centuries, society has learned that it is economically stimulating and more efficient to publicly organize safety and security.

Systemic nature of cyber risks

Cyber risks are widely perceived to be intrinsically systemic and there is no question that this is true. A survey by AIG to a global group of experts[5] indicated that more than 90% believe that cyber risk is systemic. Approximately 60% saw a 50% or greater chance of a multi-company event in the subsequent 12 months, with over half noting a 10% or greater chance of an event impacting 50–100 companies. In fact, with the benefit of hindsight, it appears that the experts may have underestimated the potential for a systemic event.

On May 12, 2017, during the second day of the GCRQN workshop, it was reported that the self-replicating ransomware WannaCry was disrupting a large mobile operator in Spain as well as hospitals across the UK. Fortunately, a "kill switch" was discovered the same day, limiting the spread of the attack to "only" 300,000 computers across the globe in a matter of days. No one knows what would have happened if such a switch had not been found, but the direct and indirect impact would certainly have been much worse. Shortly thereafter, the NotPetya attack demonstrated the potential for more significant disruption. These kinds of attacks illustrate the challenge for governments and insurance companies grappling with the potential for systemic risk.

Additional examples include the intensified and widespread attention for cyber risk management in banks that followed the cyber theft of $81 million from the Central Bank of Bangladesh in March 2016. There have been similar attempts at other banks since that occurrence. Utility companies are also on alert following the emergence of worryingly versatile malware aimed at seizing control of industrial systems. On a more microscopic level, failure of cybersecurity has been related to third-party risks on a number of occasions ranging from breaches at the United States National Security Administration (NSA) to security problems at Target retail stores.



We have observed four types of systemic cyber risk scenarios:

1. **Common vulnerabilities** – Widespread vulnerabilities lead to the risk of rapidly spreading malware infections and associated abuse (such as the Mirai, WannaCry and NotPetya attacks).
2. **Infrastructure failure cascade** – A cyberattack that causes the failure of a single organization or infrastructure service provider may have a cascading impact on many other organizations that rely on that infrastructure (such as the Ukrainian power grid, Dyn DNS services, Amazon S3 outages and CloudFlare CDN vulnerabilities).
3. **Trust-base** – A loss of integrity undermines trust-based value systems, e.g., financial, news media or democratic systems (such as the SWIFT-related attack on the Central Bank of Bangladesh).
4. **Indirect attacks** – Attacks that exploit third and even fourth parties to reach large, higher-value targets imply an unmanageably large attack surface (such as the fallout from NotPetya for Maersk, the attack on the relatively small HVAC supplier that led to the Target breach, and the compromised vendor credentials used to exploit Equifax's vendor portal that led to massive data breaches).

Each of these types of systemic cyber risk needs to be addressed differently. However, they all require a community-wide approach to preserve the common good of cyberspace.

Tragedy of the commons

In the 2015 report, *Towards Quantification of Cyber Threats*[6] , it was stated that "A tragedy of the commons scenario is emerging surrounding proliferating digital access in an unstable ecosystem, which lacks concerted controls and safeguards." Since then, the outbreak of the Mirai botnet as well as the WannaCry and NotPetya worms have had an impact on a macroscopic level due to insufficient cybersecurity at the microscopic level.

[5] AIG, "Is Cyber Risk Systemic?," 2017

[6] World Economic Forum, "Towards Quantification of Cyber Threats," 2015

Another example is the wave of cyber-based interference with democratic processes around the globe. This interference is a clear case of negative externalities where the cost of investment in cybersecurity is considered too high by most individuals. However, as a consequence, the security of the overall system is so low that it increases exposure to even well secured entities. In short, the confidentiality, integrity and availability of cyberspace has become a global resource that is insufficiently secure. Given the myriad applications being developed whose value is predicated on this resource, and the massive economic benefits that are expected to result, we had better pay close attention.

At the heart of the problem is a lack of organization. Governing a global resource such as cyberspace requires a coordinated effort. Currently, its security is almost exclusively a private matter with only limited coordination that is predominantly focused on the exchange of threat intelligence between large organizations. Given that cybercriminals are hard to track, let alone bring to justice across the geo-political boundaries, they get to explore cyberspace freely in search of victims who are unable to sufficiently protect themselves.

By continuing to embed connected technologies into almost every corner of our lives, this problem will likely be exacerbated. And since most larger organizations have made significant investments in cybersecurity, the victims of cyberattacks are typically the small to mid-sized organizations and individuals who cannot economically afford cybersecurity.[7] Combined with the added risk of default for such smaller organizations, the risk of significant loss to the global economy is increasing and we urgently need to assess the magnitude of this risk in order to identify the required level of coordination that would reduce the cyber exposure to within acceptable levels.

Governing the cyber commons

The tragedy of the commons has historically been associated with the need for supervision through governmental policies and regulations. However, as the research by the Nobel prize–winning Elinor Ostrom has demonstrated,[8] communities are very capable of jointly governing common resources, provided that there is mutual trust and regular communication.

Arguably, such communities are already forming around large corporations that intensively manage their third-party risk around cybersecurity (managed) services providers, cyber insurance firms and threat intelligence sharing communities such as Information Sharing and Analysis Centers (ISACs). In the near future, smart cities are likely to emerge as natural cyber communities, given that physical vicinity breeds trust in human relations. The clear common need for a safe and secure cyberspace is intricately linked to physical safety and security. The scale of such security-oriented cyber communities has been somewhat limited, most likely due to the difficulty in realizing the required trust and communication on larger scales.

Individual governments have several limitations in effectively governing the cyber commons. The first limitation is that direct control over cyberspace is not economically feasible given its global scale and trans-jurisdictional nature. Another limitation is that government regulation is slow, typically requiring several years to pass legislation and even longer to make an impact. Meanwhile, the pace of technical innovation continues to accelerate with several disruptive changes impacting cyberspace each year.

The economic burden of such regulations can be significant due to high implementation cost and potential productivity loss, as well as other undesirable side effects. Despite increased government regulation and enforcement, it is not uncommon for organizations to be years late in responding to new regulations, given limited resources and know-how as well as competing risk and investment prioritization.

An important step for a government to take to give systemic cyber risk the priority it deserves is to form or support a specialized, independent "Systemic Cyber Risk Council" tasked with the development of a common framework for the governance of systemic cyber risk. This council could develop a set of harmonized guidelines aimed at limiting systemic risk across sectors in reference to a systemic cyber risk model and associated metrics. This council could also enable various cyber communities to build trust and communication around systemic cyber risk. A qualified council requires expertise on the analysis of cyber systemic risk as well as on the conditions that make communities successful. By aggregating the data relevant for systemic cyber risk, the council can identify sensible mitigation strategies and measure their impact.

[7] Deloittte, "Cyber Value at Risk in The Netherlands 2017," 2017

[8] E. Ostrom, Governing the commons, Cambridge University Press, 1990

The role of cyber insurance

Most governments have high expectations for cyber insurance. This naturally emerging, free market based, and economically incentivized form of risk transfer could lead to risk reduction during the underwriting process. In practice, however, there are challenges. First, cyber insurance premiums are small relative to the cost of a cyber risk assessment. When combined with competitive pressure, this may limit the amount of information provided by clients to insurance carriers. In addition, loss trends are rapidly evolving due to the fast-changing cyber threat landscape. And finally, the size of systemic risk (with the potential to trigger significant insurance claims) must be carefully analyzed and managed.

A rapid influx of new participants in the cyber insurance market has led to competitive pressure, depressing premiums and expanding the types of coverage available. While this benefits the cyber insurance client, it is important for the industry to maintain discipline in assessing and managing its total exposure. Insurance carriers could benefit from additional quantitative data on systemic cyber risk.

Cyber insurers may also play an important role in driving improved risk mitigation and supporting the emergence of cyber communities. Similar to the history of fire insurance, many insurers are partnering with cybersecurity firms to provide value-added mitigation services and cyber assessments as well as post-breach incident response. In addition, we see the emergence of collaboration among cybersecurity providers regarding appropriate cybersecurity standards and the sharing of cyber risk management best practices. As additional data is collected over time, cyber insurers will be uniquely positioned to assist clients in assessing, addressing and controlling their risk.

Cyber risk self-regulation

Organizations have strong intrinsic motivation to limit their own cyber risk. As a traditional means of risk management, some have resorted to tools such as benchmarks, assessments, certifications and norms to obtain insight into their own cyber risk posture and where to improve. However, most such approaches quickly become outdated due to the tremendous rate of change in the threat landscape. The only way to deal with this rapid change is to build the assumption of change into the framework by going to a higher level of abstraction. Unavoidably with this approach, there will always be room for interpretation, meaning that the application and interpretation will vary widely from one organization to another, leading to varying levels as well as diversification of cybersecurity.

Problems with cybersecurity have become all-pervasive because of the connectedness of technologies. As a result, more and more companies are including third-party risk management as an important part of their cyber risk strategy. In response to this need, and in response to the actuarial needs of cyber insurance underwriters, enterprise cybersecurity ratings systems have emerged in recent years. Similar to the FICO® Score for consumer credit risk, such ratings systems, including FICO® Enterprise Security Scores, aim to provide a numerical score that captures the cybersecurity posture of an organization. These systems typically use a combination of data points collected or purchased from public and private sources and proprietary algorithms to articulate a rated company's security effectiveness into a quantifiable measure or score. While the efficacy of a security program cannot be solely reduced to a single number, security ratings based on accurate and relevant information are useful tools in evaluating risks. And as security rating technology continues to mature, more organizations in the public and private sectors will leverage these scores for making business and risk decisions.

A ratings system plays two very important roles. Like a consumer credit rating, an enterprise security rating introduces a potentially standard and normalized way of inspecting the security posture of a third party or a peer. In addition, it can serve as a way for an enterprise to self-evaluate and self-regulate. For instance, it could be used to gauge the effectiveness of resource allocation strategies in cybersecurity within an organization. Against the backdrop of the high degree of connectedness of cybersecurity, we believe these ratings systems are critical to the cybersecurity ecosystem as a tool to assess the security conditions of those connected to each other.

As rating technology matures, we believe it is important that rating companies work toward standardization and transparency of these rating systems. Both can help various stakeholders in the ecosystem reach a common understanding of the meaning of cybersecurity ratings and common practices for how they are used in areas such as vendor validation and underwriting.

Cyber communities of trust enabling defense in depth

Better coordination on systemic cyber risk is needed, but how can this be realized in practice? We introduce the concept of "cyber communities of trust" as any collective of organizations (or cyber communities) that jointly operates or utilizes cybersecurity capabilities in alignment with a shared level of trust. With this scalability, smaller organizations benefit by being able to attain cybersecurity levels on par with larger organizations. The level of trust naturally tends to decrease as the size of a community increases, so cyber communities will have an optimal size that balances trust with the benefits of scale. Such communities will not be mutually exclusive, but will be part of multiple communities—in effect, creating a network of communities that will have a natural distribution of knowledge and a built-in resilience.

To a certain extent, cyber communities are already forming naturally. Examples of cyber communities include: IT and cybersecurity providers and their customers, cyber insurers, brokers and their customers, large corporations that structurally manage their third-party cyber risk, smart cities and ports, participating members of any ISAC, regulators and the institutions they regulate, and cloud providers and their user base. Some of these communities will prove more successful than others when it comes to building the trust needed to build communal defense in depth. Based on experience, we can expect that geographical distance, anonymity, cultural differences, power asymmetries and other such barriers will limit the success of such communities in dealing with systemic cyber risk. Therefore, stimulus to forming cyber communities for organizations with common interests and backgrounds on a local level will be welcome.

We have identified the following domains in which stimulus would help reduce systemic cyber risk:

1. **Cyber architecture** – Structuring cyberspace to facilitate utility while limiting abuse.
2. **Threat intelligence** – Exchanging knowledge and understanding of known threat activity.
3. **Cyber risk measurement** – identification and reporting on metrics around the dependency of value(s) on connected technologies and linking this to Threat Intelligence.
4. **Cybersecurity** – Offering efficient and compatible cybersecurity solutions and services.
5. **Secure connectivity standards** – Providing objective, standardized testing and measurement of security performance of devices and services (through a security standards company such as Underwriters Laboratory).
6. **Incident response** – Sharing capabilities that are needed only in case of a cybersecurity breach.
7. **Risk transfer** – Agreeing on standards for cybersecurity implementation associated with third parties.
8. **Coordination** – Harmonizing standards, approaches, metrics and methods in cybersecurity.
9. **Regulation** – Especially where the potential impact outsizes the organization or individual community level, identifying and limiting systemic cyber risk through security standards combined with measurement and reporting of cyber risks.

For each of the perspectives listed above, we provide a set of proposed improvements that can be implemented at every scale. These improvements are mutually reinforcing:

1. **Cyber architecture:** Similar to cybersecurity best practices employed by large organizations, a "defense in depth" architecture limits many of the dependencies on cyber infrastructure that lead to systemic risk. This could be realized by groups of organizations collectively creating cyber communities and then joining several such cyber communities into larger cyber communities. The desired result would be a more secure, shared cyber infrastructure with multiple layers of protection from threats commonly found in the rest of cyberspace. It should enable relatively open channels for information exchange between trusted sources. There should be more protected channels in case such trust has not yet been established and restrained channels in case of illicit activity. Providers of internet and security services are well positioned to originate such cyber communities.

2. **Threat intelligence:** Rapid distribution of threat intelligence to trusted parties according to common standards enables effective response against emerging malicious activity. Well-structured and well-implemented threat intelligence within cyber communities of trust (following the defense in-depth strategy above), has the potential to either stop illicit activity or, in case of insider threats, to limit it. Cyber communities would also enable better quality threat intelligence according to the agreed level of trust. Threat intelligence providers and ISACs should lead the opportunity in facilitating such threat intelligence sharing arrangements.

3. **Cyber risk measurement:** The impact from (potential) cyber incidents on value systems ranging from the monetary and economic systems that drive businesses to values as trust and democracy can be tangible as well as intangible. Understanding this impact is key to identifying the overall exposure. For this, third-party and other stakeholder dependencies will have to critically be included in the analysis, measurement and reporting. By combining this understanding of impact and exposure with threat intelligence, the priorities in mitigating systemic cyber risk can be identified.

4. **Cybersecurity:** On the level of cybersecurity, it would be beneficial to improve the integration with (standardized) threat intelligence sources, the mutual compatibility of security solutions and the overall IT infrastructure. Efficient cybersecurity operations on the level of cyber communities would benefit from open-source security platforms and services that enable such efficient implementation and operation. Vendors are in a unique position to (jointly) develop these security platform(s) and services and would benefit from taking a leading role.

5. **Secure connectivity standards:** Today there is no industry-wide standard for measuring the performance of cybersecurity features on consumer software and devices, nor do such standards exist for cybersecurity tools themselves. As such, there is no security warranty provided by the vendors of such products and little or no accountability for security failures. And yet, when consumers buy a lightbulb or a toaster, it has been tested and approved by a security standards company, so it is expected that these products, under normal use, will not burn down your

house. As more devices are networked and become part of the Internet of Things (IoT), and as autonomous vehicles take to the streets, such cybersecurity testing, along with the establishment of minimum standards and performance warranties, must become embedded in the cyber product lifecycle and cybersecurity supply chain.

6. **Incident response:** Similar to the fire department, incident response units should rarely be needed. Only a few units would be needed for each cyber community and it's possible to pool these units across cyber communities in case of major events. Such units will require regular training with each of the organizations in the cyber communities and they will play a pivotal role in developing the robust crisis management plans with these organizations so that impact upon a cyber incident is minimized. By exchanging best practices and protocols between cyber communities, lessons learned can be optimally leveraged across cyberspace.

7. **Risk transfer:** Given improved levels of security through the effective and widespread implementation of defense in depth, each individual organization within the larger pool of a cyber community will be at lower risk, thereby facilitating risk transfer. This can be further enhanced by agreeing on auditable standards for the implementation and continuous maintenance and testing of cybersecurity levels, either by third parties or the community itself. For insurance companies, sharing exposure to larger cyber communities with other insurers, while also diversifying across cyber communities, will improve diversification and enable access to better cyber insurance coverage at lower premium levels.

8. **Coordination:** Many benefits can come from early harmonization between emerging cyber communities in terms of their capabilities, methods, standards and information exchange. Stronger cybersecurity can be derived from joining cyber communities in a (partially) nested fashion to form a larger cyber community. To enable this, sufficient coordination between cyber communities would be considered crucial. All parties associated with cyber communities have a role in continuously seeking such coordination and supporting the emergence of other cyber communities. As needed, government can also play an important role in stimulating this process.

9. **Regulation:** In principle, much of the regulation required to limit cyber risk exposure from exceeding too far beyond the boundaries of any individual organization is already in place. However, regulation can be significantly improved by ensuring better training of and alignment between such regulatory bodies on the intricacies of cyber risk in general and systemic cyber risk in particular. The bill on IoT recently proposed in the US is another step in the right direction. More regulation may eventually be required, though it will likely remain slow to implement relative to the rate of changes in cyberspace itself. Regulation and policy drawing on well-established methodologies for setting standards, conducting testing and providing certification of the Underwriters Laboratory can provide a model for developing and achieving similar measurable levels of security performance and minimum cybersecurity standards for a wide range of connected products, services and cybersecurity devices, along with warranties and accountability.

Quantifying systemic cyber risk

Communities will be key in securing cyberspace, and this is also the natural place to start collecting the data needed for commencing quantification of systemic cyber risk. Rather than building the high level of trust needed to directly exchange such data, quantification models may act as an intermediary of such trust and may serve to accumulate insight from the lowest operational levels of individual organizations to the level of communities, communities of communities, and eventually on the level of nation states and global regions.

In the years to come, more and more accurate models will likely be developed that will leverage techniques such as machine learning and artificial intelligence. Already, some models have been developed by several stakeholders to help quantify systemic cyber risk. In this report, we focus on the specific needs such models will have as related to the systemic component of cyber risk. At a high level, all models that aim to completely quantify cyber risk will have three key components: attack activity, combined cyber risk control, and cyber abuse impact.

Ideally, the model used for exchange of information is aligned over a large group so that very little is lost in translation between models. Even when various models are in use, it will be possible to some extent to exchange information between models based on their logical mathematical commonalities in reference to the (implied) underlying data models they refer to. For the conceptual model that can be used in quantifying systemic cyber risk, alignment benefits the overall quantification community. We have identified the following dependency mechanisms that give rise to systemic cyber risk:

1. **Attack-related dependencies** (several organizations suffering the same attack)
   a. Attack innovation (e.g., combining existing attacks)
   b. Attacker scaling (e.g., through network worms, cloud or IoT)
   c. Attacker alignment (e.g., herding, copy-cat behavior)
2. **Controls-related dependencies**
   a. Common vulnerabilities (e.g., critical software)
   b. Common controls (e.g., through cloud or security services provider)
   c. Cascading effects in controls (e.g., due to controls interdependencies)
3. **Impact-related dependencies**
   a. Cascading effects in impact (e.g., related to trust)
   b. Value-chain dependencies (e.g., critical infrastructure)
   c. Alignment effects (e.g., ISP, CA and bank simultaneously hacked)
4. **Higher order dependencies**
   a. Between attacks and controls (e.g., attackers attracted to common vulnerabilities)
   b. Between attacks and impact (e.g., attackers jointly aiming at a similar impact)
   c. Between impact and controls (e.g., an attack whose impact leads to failure of controls)

In practice, the quantification of such dependencies will amount to defining and measuring against metrics that are logically linked to the above elements. Harmonizing such definitions and metrics will greatly enable communities to sensibly exchange information leading to quantitative insights on the systemic component of cyber risk. Such metrics can both be defined at a high level (e.g., new types of malware observed in the last 90 days) or on a more granular level (e.g., number of mutations discovered of a strain of malware as a time-series). The art in this is to set granularity for metrics that can be maintained across the entire range of subcomponents, because the uncertainty of the most granular subcomponent will simply be the leading factor in the overall uncertainty (thus risk) of the model outcome.

Coming full circle to the role of cyber communities in quantifying as well as managing systemic cyber risk, there is no fundamental limitation to obtaining the data needed. Because, by its nature, the cyber domain allows for accurate and extensive metrics, more than any system ever before. The challenge is to make cyber communities recognize the added value of investing in the collection, monitoring and use of such metrics. If they do so, they can expect scaling benefits in their cybersecurity as a consequence. Threat intelligence sharing in communities is a good start, but it's also important that controls, impact, and all the interdependencies above are measured and exchanged within communities.

By the non-exclusive nature of cyber communities, however, sharing within one community implies sharing with other communities. This effect may erode trust and it is therefore key to transfer information in relation to a given model that allows for aggregation of data against information received from others. Aggregation will enable the confidential data of any organization to be incorporated with the information of the other organizations, effectively obfuscating, if not de-identifying, the confidential data and thus sustaining trust. As a group of experts in this field, we are fully aware that such a model does not yet exist and the above merely serves as a conceptual starting point. Nevertheless, this group also has the ambition to take on this challenge and we invite those who want to contribute to join in.

Next steps

Understanding the concepts mentioned in this paper, the Global Cyber Risk Quantification Network has identified next steps to seek out and develop a cyber community to further develop the conceptual model into an operational model. The next challenge that this community will take up is the identification of fundamental risk scenarios associated with this model. From there, we will identify appropriate metrics to put in place and feed back into the common model for the purpose of improved cyber risk management leading to reduced systemic cyber risk. The holy grail is to collect evidence that this approach will demonstrably reduce the common, as well as systemic, cyber risks to the benefit of that community as well as the larger community. To facilitate this process as well as the development of quantification of systemic cyber risk for the benefit of society, we will start a non-governmental organization (NGO) that can independently define, maintain and drive this agenda as well as to seek out, stimulate and support cyber communities around the globe.

1

Start an NGO that initiates a consortium.

- File the legal documents to establish the NGO.
- The NGO shall target small companies with a passion for the greater good and improving security.
- The NGO shall be an independent organization that provides guidance to improve security.

2

Create an agenda.

- The agenda shall include discussion topics and action items on a quarterly or annual basis.

3

Reach out to the networks to attract early adopters and obtain support from organizations and the government.

- Identify 1 or 2 Smart Cities with non-monolithic population and diversity in economy to be early adopters.
- The group identified possible candidates: Atlanta and San Diego.
- Maarten van Wieren will reach out to Global Economic Forumn to get support.
- Mark Silvestri will reach out to contacts from DHS.

4

Expand globally.

- The group agreed that the consortium should have branches in Asia, Europe and Africa.
- **Asia:** The group identified Singapore, Japan and Australia as countires that are interested in joining consortia.
- **Europe:** Maarten van Wieren is reaching out to his contacts in Europe.
- **Africa:** South Africa was mentioned in the group discussion as a potential due to the large impact of cybercrimes in the region.

Workshop participants

San Diego, CA, May 2017

Doug Clare	FICO
Jim Coggeshall	FICO
Cherie Dawson	AIG
Mark Fernandes	Deloitte
Ben Goodman	4A Security / Drexel University
Jeff Gutman	Willis Towers Watson
Todd Higginson	FICO
Jack Jones	FAIR institute / Risk Lens
Christopher Keegan	Beecher Carlson
Keira Li	Deloitte
Mingyan Liu	FICO / University of Michigan
Kim Manibusan	FICO
Jack McNeil	Philips
Prashant Pai	Verisk Analytics
Mark Silvestri	The Hartford
Camelia Simoiu	Stanford University
Maarten van Wieren	Aon
Brian Warszona	Willis Towers Watson
Scott Zoldi	FICO

Contacts

Maarten van Wieren
Managing Director – Aon Cyber Solutions
Tel.: +31 6 82 01 92 25
E-mail: maarten.van.wieren@aon.nl

Ming-yan Liu
Director of Analytic Science – FICO
Tel.: +1 734 764 9546
E-mail: mingyanliu@fico.com

Ben Goodman
President, 4A Security & Compliance, and
Drexel University, LeBow School of Business
Tel.: +1 484 858 0427
E-mail: goodmanb@4asecurity.com

4606WP_EN 09/18 PDF