Community of Trust™

Reprivata, Corp.

Cybersecurity Insurance

A major defect preventing the development of accessible and efficiently priced cybersecurity insurance is the absence of a standard contract structure that would enable the "Principle of Equivalence" to be used to calculate risk. Due to the complexities of the systemic risks involved in cybersecurity, underwriters safety load the policy premiums to contend with the theory that it is virtually impossible to perform a reasonable assessment of risk. This practice in and of itself is an accumulating hazard for underwriters. This practice is preventing underwriters from creating the precise velocity that is required to generate premiums and thus stagnates the development of accessible and efficiently priced cybersecurity insurance. Further, we assert here that the defect is the absence of a standard contract structure that would enable the syndication of risk to natural financial counterparties. While there is no doubt that risk complexities require a *significant premium*, the absence of standardized contracts prevents the development of an efficient pricing mechanism to determine the *significance of that premium* as viewed by a diverse group of market participants.

To begin to solve this problem we have developed a suite of standardized contracts for the insured that will enable cybersecurity insurance providers to begin to uniformly mitigate risks in the underwriting process. By enabling the Principle of Equivalence to be more objectively applied and creating liquidity by virtue of the standard contract structure, Community of Trust enables broad syndication of risk.

Benefits for Insurers

- Community of Trust standard contracts enable fungibility and frictionless, systematic syndication of risk.

- Community of Trust standard contracts enable the creation of tradeable financial instruments enabling intermediation of risk by traditional financial market participants.

- Community of Trust requirements for interconnection/counterparty compliance enables underwriting velocity, creating accelerated portfolio/premium acquisition.

Community of Trust Overview

The implementation of Community of Trust provides the Chief Executive Officer or Director of an organization with a simple Cyber Risk Management tool similar to tools currently used to manage the financial condition of an organization or enterprise. Master Agreements similar to those used in financial settlement mechanisms are implemented to manage all aspects of the organization's cyber risks. This standardized contract structure also enables cyber insurance underwriters to price risk more effectively and efficiently enabling enterprises or organizations to obtain efficiently priced cyber insurance. Community of Trust also enables uniform interoperability between communities that enables the interconnection to or with other Communities of Trust using the NIST Cyber Security Framework as a governance mechanism.

2017 Master Agreements Community of Trust requires that an organization become a member to obtain access to the Master Agreements that constitute and enable an independent Community of Trust instance. These agreements are comprised of a 2017 Master Membership Agreement that requires members to organize and deploy their independent Communities of Trust using a process that will facilitate the reliable implementation of security policy and technical interoperability between independent Communities of Trusts and interconnected entities. The 2017 Master Interconnection Agreement, similar to a financial settlement mechanism, requires that the Community of Trust Owner and all interconnected entities enter into an agreement that requires a minimum threshold of Cyber Insurance and that each party be named as an additional insured in the policy. It also requires the counterparty to be U.S. Cybersecurity Framework (CSF) Tier 3 compliant. The 2017 Master End User Agreement enables an organization to provide a standardized agreement with customers that mitigates risk and creates a trusted (PII) relationship between customers and the Community of Trust owner. The 2017 Master Employee Agreement enables an organization to provide a standardized agreement with employees that mitigates risk and creates a trusted (PII) relationship and remove ambiguity in the relationship with the employer and/or the Community of Trust owner. The 2017 Master Member Agreement with a Service Provider Addendum enables an organization to contract with a third party to implement the Community of Trust policy and technical layer.

Community of Trust also obtained the first Underwriter's Laboratory (UL) 2900 certification for our secure network transmission software and hardware product. This product is integrated into our service. Reprivata provides this technology certified by Underwriter's Laboratory ("UL") Cyber Assurance Program 2900 to all Community of Trust participants that enables even small

interconnected counterparties to cost effectively connect securely and this capability enables monitoring of interconnection threats in real-time. Reprivata's secure transport technology is the only technology to date that has been certified by Underwriter's Laboratory ("UL") Cyber Assurance Program 2900.

The Industrial Internet of Things is enabling more sophisticated capabilities through network-connected products and systems. As a result, industrial control systems are becoming more interconnected, connectable and networkable. The security, performance and financial risks impacting industrial control systems globally are the key drivers to develop new safeguards in an ever-changing security threat landscape faced with growing risks. The new UL CAP was developed with input from major stakeholders representing the U.S. Federal government, academia and industry to elevate the security measures deployed in the critical infrastructure supply chain. The White House recently released the Cybersecurity National Action Plan (CNAP), designed to enhance cybersecurity capabilities within the US government and across the country. UL's CAP services and software security efforts were recognized within the CNAP as a way to test and certify network-connectable devices within the Internet of Things supply chain and ecosystems especially relevant in critical infrastructures.
