How ISACA can unleash a Digital Trust revolution

An editorial response to ISACA's white paper on digital trust

Thomas Lee, PhD, Chief Executive Officer of VivoSecurity

Have you ever wondered if there could be a silver bullet for cybersecurity? I argue that there can be, and it might not be what you think: I believe the silver bullet is a process.

Recently, ISACA published a white paper on the importance of digital trust[1] to which, cybersecurity is a foundation. The article called digital trust an imperative, but did not offer any real solutions for business. I argue below that the silver bullet is third-party risk management (**TPRM**) and that ISACA can pull the trigger.

A problem with achieving digital trust is that business leaders must decide how much money to allocate for cybersecurity, but cybersecurity practitioners are unable to credibly present risk in business-material terms. Risk is the product of impact and probability, and while impact might be understood, cybersecurity practitioners do not calculate probability. As a result, risk is presented as green-yellow-red, or as maturity scores or other subjective measures.

What business leaders want to know is the likelihood and ex-ante models are an effective way to calculate and convey likelihood. Business leaders are comfortable with such models and most MBA programs teach methods such as regression modeling.

The most effective use of ex-ante models is managing the vexing blind-spot which is third-party risk[2]. There are two reasons. The first is that data breaches are rare, generally. The frequency for an individual company might be once in 50-years, which is not a concern for management. But ten-vendors, each with a once in 50-year frequency becomes once in 5-years for a third-party data breach–which is a concern for management. So, a level of security and subsequent breach-frequency that would seem acceptable for an individual company becomes unacceptable when viewed across a collection of vendors.

The second reason is that by managing third-party risk with ex-ante models, companies can increase outsourcing. This is important because vendors bring new technologies and efficiencies to the business, so limiting the use of vendors can limit a company's ability to be competitive and to grow. To see this, consider that instead of a monetary budget, there is a risk budget, which is set by the company's risk tolerance. Perhaps this risk budget is 2% or a tolerance for a third-party data breach once in 50-years. Because risk accumulates with each vendor, each vendor takes a piece of this budget. For example, 10-vendors, each with a 0.1%-probability would use up half of this risk budget. Some vendors hog a larger piece due to a weaker security and limit what is left for more vendors. For example, a vendor with a 1%-probability, by itself, would use half of this risk budget. Avoiding these highest risk vendors can often double or triple the number of vendors that a company can use while still staying within their risk tolerance.

So the silver bullet is using ex-ante models to measure third-party data breach risk. The driver is not a desire for better security, but for more outsourcing and ex-ante models provide clarity on how to achieve it. Businesses will favor vendors with better security primarily because it allows more outsourcing. Vendors will accept the better level of security as the cost of being competitive and understand it allows their customers to leverage more third-parties. The result of this effect will be cascading, creating competition among vendors for better security and improving digital trust generally.

ISACA is in a unique position to advance the use of ex-ante models since they provide an important certification for **Internal Audit**. Internal Audit reports to the board-of-directors and this connection is important since it is the business that must recognize this double-risk: the risk of third-party data breach and the risk of limiting outsourcing.

ISACA can shepherd this change by creating standards and training for the use of ex-ante models to manage cumulative vendor risk. They can adopt and teach the Federal Reserve standard for model risk management: SR 11-7[3]. They can train auditors how to present cumulative vendor risk to the board, how to work with TPRM teams to decide evaluation criteria and management strategies for reducing cumulative vendor risk. ISACA is also replete with members that have statistics skills, with many having degrees in statistics, economics, mathematics, engineering and physics. ISACA could leverage these skills to develop the standards and training.

ISACA can do more than simply call digital trust an imperative–they can make it happen.

---

[1] Digital Trust: A Modern-Day Imperative, ISACA 2022

[2] Assessing the Effectiveness of Third-Party Risk Management using Quantitative Models, VivoSecurity 2022

[3] Guidance on Model Risk Management, Federal Reserve and Office of the Comptroller of the Currency, 2011