ISSA DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

The Future of IT Risk Management WILL BE QUANTIFIED

By Jack Freund – ISSA Senior Member, Charlotte Metro Chapter

This article discusses the evolution of IT risk measurement from ordinal scale, verbal risk labels to more rigorous, actuarial-inspired cyber risk quantification methods for ascribing financial losses to IT security incidents.

Abstract

IT risk has matured as a discipline, and in the next decade we can expect the pace to accelerate, driven in large part by regulatory, insurance, and customer requirements. This article discusses the evolution of IT risk measurement from ordinal scale, verbal risk labels to more rigorous, actuarial-inspired methods for ascribing financial losses to IT security incidents. These methods are being called cyber risk quantification (CRQ) and are quickly becoming a major component of an organization’s integrated risk management strategy.

Our profession’s risk management capabilities have devolved over the previous decades. Silicon Valley entrepreneurs have created a discipline and an appetite for new technologies that push the limits of what is possible at both the hardware and software levels. Perhaps because or in spite of this, we’ve been conditioned to reject old methods in favor of a brave new world of computational exemplification of everything in our lives. And such a thing has, on the whole, been good for humanity. But it has also created such a unique new environment that we have no idea how impactful this will be for our everyday lives. This layering of complexity has created often unknown subtleties in system interdependence as well as emergent behavior that belies expectation. This kind of futuristic prevarication can lead us to believe we live in a world that makes quantification troublesome. Indeed, with so much complexity and so many new technologies, how could we even begin to think about all the risk associated with our endeavors?

To date these problems spaces have been solved using quick and easy methods such as ordinal scale measures, heat maps, and direct application of verbal risk labels. In essence, the expected result of a risk assessment is the assignment of a high, medium, or low label, so such methods give you the permission to select them directly, or at least derive them from two also easy-to-evaluate variables (such as probability and impact). Classic examples of this approach include the NIST 800-30, NIST CSF, and ISO 27001. These standards allow for the application of more rigorous, quantified methodologies, but do very little to describe what and how to accomplish this beyond saying that such approaches are compatible with these standards. NIST CSF includes some specific references

to a cyber risk quantification (CRQ) methodology that will be addressed later.⁴

However, a series of techniques, standards, and research has begun creating a phase shift away from devolving cyber risk management capabilities and applying CRQ methods. CRQ is an emerging trend in the industry and the term itself is somewhat autological. A general working definition of CRQ for this article is the application of actuarial methods to quantify cyber risk using dollars (or other currency). This includes the application of statistical methods due to a paucity of data and the need to forecast future events. CRQ is a critical component of what Gartner has dubbed integrated risk management (IRM),⁵ which is a hallmark of highly mature risk management programs. In essence, this allows risk from various sources in an organization to be mapped and tracked using a single dashboard. This gives organizations the ability to compare severity of risk scenarios across their organization and make well-informed decisions about remediation and potential losses. This proclamation by Gartner in 2018 comes at the end of more than a decade of work in developing and testing CRQ methods in academia, industry, and standards organizations.

A brief history of modern CRQ methods

Statistician and measurement expert Douglas Hubbard has studied difficult-to-measure problems, especially business intangibles, and the approach by many to apply ordinal scale methods to the problem space in a 2010 paper on the topic.⁶ Hubbard also published a series of books on the topic starting with How to Measure Anything in 2007.⁷ This book was not intended to be a book for the IT world but quickly found a foothold there, especially in the realm of IT risk management. This spawned his second book on the topic, The Failure of Risk Management in 2009,⁸ a seminal work that describes how devolved our risk management capabilities have become over time. Indeed, this work shows that IT risk is far from the beautiful unique snowflake that we think we are and that other disciplines have been dealing with difficult (yet not impossible) things that need to be measured for several decades.

The concept of catastrophic risk has been around for a long time, and the methods in use to measure risk there can be helpful in understanding how we can do so in information security and IT risk. One of the best techniques for understanding how to do this is to change your expectation of what “measurement” really is. As Hubbard specifies, a measurement is really a reduction in uncertainty, not necessarily a precise measure of something. It’s the difference between ordering a dozen cupcakes at a bakery and trying to decide if one of your cousins is taller than the other. The level of precision necessary is really dependent upon what you plan to do with the decision that follows (i.e., only a useful level of precision is necessary).

One example of a difficult-to-measure problem in the insurance space is the Olympics, which requires that the host city

---

The Future of IT Risk Management Will Be Quantified

Jack Freund

purchase event cancellation insurance. These kinds of policies pay out if the Olympics are canceled. Similar in some ways to information security breaches, we do not find many examples of canceled Olympics from which to crib together a precise measure of frequency (if you look, it’s only ever been canceled a handful of times due to world wars). And yet, it is still possible to find several firms willing to underwrite this kind of coverage.

There are many such examples of difficult-to-measure problems that are actively being managed, and the lesson for information security is that we cannot postpone making a decision due to a lack of data. We need to move forward with the data we have and provide our decision makers with a solution set that helps them make the best decisions with the right amount of data. Its difficult sometimes for those in the IT community to be comfortable with the amount of uncertainty that this affords. However, the world will continue to make these decisions regardless of any equivocating we may do in the meantime.

The other facet of measurement is that when applied to the future we simply cannot be precise in the way we talk about measurement. And risk is always about creating future-looking views of what risk may or may not be over time. To expect (or represent) precision in such measures is madness. One of the key techniques that Hubbard uses to help reduce uncertainty around a measurement without falling prey to precision is to express it using ranges. These ranges inherently represent uncertainty. Anyone who has experience with project management will be familiar with the concept of performance evaluation and review technique (PERT) that helps to represent time and costs estimates using a three point estimation system: best case, worst case, and most likely. When substituted for min, mode, and max values, these can allow us to build a bell curve distribution of values that is perfect for risk management decision making.

Factor Analysis of Information Risk

In 2009, the OpenGroup published standards based on the Factor Analysis of Information Risk (FAIR) methodology, which they branded as OpenFAIR. This was approximately six years after the creation of what today is the primary CRQ methodology in use. FAIR is a widely adopted methodology for providing actuarially sound statements of how much cyber value-at-risk (Cyber VaR) a firm has. The OpenGroup began with two standards covering risk analysis and risk taxonomy and later published standards on the application of FAIR in other risk assessment frameworks, including the FAIR ISO Cookbook in 2010 and the FAIR - NIST CSF Cookbook in 2016.

Additionally in 2014, a foundational guide to understanding and applying FAIR was published. This book covers conceptual risk principals as well as understanding how to apply FAIR to conduct risk analyses in organizations. These publications cover the basics of the language of CRQ including important definitions for risk that facilitate quantification. For example, FAIR purposefully uses frequency in place of probability to allow for the analyses of events occurring.


ring more than once per year. Further, FAIR separates loss analysis into two phases with another frequency variable to allow for proper modeling of high dollar, low frequency events like class action lawsuits and customer desertion. Variables for deriving frequency are developed using a comparison of preventative control strength and attempts by threat communities to generate a loss event.

These techniques, along with Monte Carlo simulation\textsuperscript{16} are necessary for establishing true Cyber VaR modeling.\textsuperscript{17} Such models are important for understanding the amount of potential (future) losses associated with cyber operations at an organization along with an estimated time frame. This allows organizations to gain an understanding of the value of loss at risk as a result of a particular set of operational conditions. For instance, a firm that is looking to move from a bricks and mortar operation to an online storefront would need to understand the potential losses associated with fraudulent transactions as well as breach scenarios and what that loss could represent to the organization.

Regulator views of CRQ

In 2016, the Office of the Comptroller of the Currency (OCC), the Federal Reserve System, and the Federal Deposit Insur-

\textsuperscript{16} Monte Carlo methods are computational algorithms that utilize repeated random sampling from ranges to compute a numeric value.


30 percent of the Fortune 100 in the summer of 2018. The FAIR Institute now holds annual conferences with hundreds of attendees and grants awards for those that exemplify and promote cyber risk quantification.

**Future of CRQ**

One of the key drivers for the next decade of IT/cyber risk management will be the application of risk-based capital. Mature financial services firms have long since been required to maintain a strong discipline around setting money aside for a rainy day. These rainy day funds allow a bank to weather bad financial markets and keep insurance companies from going under during terrible catastrophic losses such as those that occur when a major hurricane blows through and obligates major payouts. Insurance companies leverage reinsurance firms to help spread the risk around, but even these firms have contractual requirements to ensure capital adequacy in the case of major fallouts. Such reserve requirements were codified by the Basel Committee on Banking Supervision (BCBS) in 2004 with the second Basel Accord (Basel II). Some firms implemented these prior to 2008, but the global financial crisis of that year brought these guidelines into sharp focus, with many countries’ banking regulators making specific rules around capital reserve adequacy and conducting bank-stress testing.

These tests, while focused on the financial risk firms faced, also covered a significant segment of operational risk activities. These leveraged the well-known Basel II event categories:

1. Internal fraud
2. External fraud
3. Employment practices and workplace safety
4. Clients, products, and business practices
5. Damage to physical assets
6. Business disruption and systems failures
7. Execution, delivery, and process management

Information security professionals will obviously see the connection to their work in numbers 1, 2, 3 and probably others as well. So too did those in the operational risk professions and more importantly regulators who began asking that firms account for operational losses associated with their IT operations and cybersecurity. As a result, many of the risk practices, good and bad, from the operational risk field are making their way into the IT security field. This includes, curiously, the divergent approaches of using ordinal scale, verbal risk labels as well as mature capital modeling techniques sometimes referred to as potential capital at risk or PCaR. Such stress testing models incorporate scenario analysis and will sound very familiar to those discussed above.

This approach involves developing a series of fictitious, yet plausible, loss scenarios for an organization and accounting for all the costs and business losses associated with that scenario. Every activity within the scenario should be accounted for and costs/losses assigned. The sum of the fallout from a realized series of losses would generate a figure that can be used to better understand how much capital reserve a firm needs to have in order to weather a bad incident, or during cascading risk scenarios, several of them simultaneous.


ously. These practices have taken root in financial services, but will undoubtedly make their way into other industries although they may require less rigor.

Non-financial organizations without regulatory pressure to adopt CRQ will also see their IT risk management practices change as a result of the adoption of these methods. Many organizations are looking to gain a better understanding of what cyber loss looks like to them, often in response to press coverage of mega breaches. When company leadership hears of multimillion dollar losses, they will invariably wonder how that would affect them. CRQ methods, such as FAIR, are purpose-built to provide non-IT security executives insight into why investing in IT security should be a priority. Indeed, CRQ will be a critical tool in organizational budget-setting activities around cybersecurity. When every dollar invested in the department results in risk reduction of some kind, no other approach but CRQ can provide company leadership with implicit risk acceptance (i.e., fund this tool/program or accept increased loss exposure).

Additionally, organizations interested in purchasing cyber insurance will need measures to help them anticipate how much coverage they will need. Indeed, the insurance industry will provide proxies for this such as record count, similar to how assumptions are made about repair costs based on the make and model of vehicle you are insuring. But organizational validation for such a large purchase will be necessary to provide management with purchase satisfaction and to better understand what expenses will and will not be covered. Reading the exclusions on these policies is critical and many substantial losses, such as customer desertion, are often not covered.

Customer and industry pressure in general will also be a driving force in adoption. When such practices become de rigueur and third-party risk questionnaires routinely ask not whether or not you employ CRQ but which methodology you use as an indirect measure of IT risk management maturity, the influence this will have over widespread adoption will be substantial. Lastly, organizations doing business with your company may ask you to post bonds (if you don’t currently have a cyber insurance policy) to help ensure the proper care and handling of the data they have entrusted to your organization. Such bonds and associated losses will need to be rationalized using CRQ.

Risk appetite in a CRQ future

At present many organizations operate as if they believe that cyber incidents are not inevitable. Indeed, they make mention of using best practices and proclaim that they take the security of their customer’s data very seriously. Yet very few organizations have best-in-class security programs and/or are able to keep pace with complex security hygiene routines. Underneath it all, we know that a breach will be inevitable and losses will occur. This is implicitly expressed at security conferences with popular phrases such as “not if, when” and “assume breach.” However, such reality is missing from corporate risk appetite statements (when there is one at all).

Instead we see risk appetite statements that discuss obliquely that while no organization can prevent all bad things from occurring, they don’t accept any high-risk scenarios. Undoubtedly, all these organizations are living with at least one control deficiency that would allow the realization of losses associated with a high-risk scenario. Regardless of the sentiment, risk appetite statements that do not incorporate CRQ methods and show the verbal risk label only make it hard to better understand what is and isn’t allowable in an organization’s IT operations. With the further adoption of CRQ methods, organizations will be able to more confidently assert and draw evidence that their IT risk appetite is $1.5 million per incident (for example) and that they expect that this will not occur more than once in a five year period. Such a declarative statement gives organizations the ability to sock away money in their rainy day fund in case something bad really does happen, and drives much better prioritization within firms to understand where their serious control deficiencies are and how to best prioritize budgetary dollars to remediate them.

This alone would be an amazing advancement in the ability of information security organizations to develop prioritization routines and develop multi-year strategies aligned with organizational appetite and tolerances. However, it can also contribute to a firm’s ability to offer a competitive advantage over other organizations. We in information security have long since talked about using security as a marketplace differentiator; however, with CRQ methods an organization could boldly proclaim the specifics of their differentiation. Instead of appearing better simply by comparison (they were breached and we were not), an organization could post a public, truth-in-lending style proclamation about their expected

---

**Infosec Book Reviews**

Have you read an excellent information security book of value to ISSA members? You are invited to share your thoughts in the ISSA Journal.

- Summarize contents
- Evaluate interesting or useful information
- Describe the value to information security professionals
- Address any criticisms, omissions, or areas that need further development

Review should be 500-800 words, including short bio, photo, and contact email. Submit your review to editor@issa.org.
time line for a breach. For instance, a bank might indicate that based on their security controls they expect a security incident about once every five years. A more mature bank might be able to forecast such a loss out to seven or ten years. Such an approach was recently proposed on the FAIR Institute blog.\footnote{Freund, J., "Cyber Risk Prospectuses," The FAIR Institute – https://www.fairinstitute.org/blog (accepted for publication).} As it stands right now, bank customers that experience a breach have to choose whether to stay with their current bank or pick another one. There are significant problems in this decision as they suffer from asymmetric information; to wit, they know very little about the true state of security at competing banks outside of public, lawyer-sanitized statements around best practices and taking security seriously—the same level of information they know about their current bank that just experienced a breach.

Consumers could then choose from banks with a more well-informed set of guidelines than currently available, in a way that is similar to their choosing a mortgage rate or an investment product. It makes real the well-know financial principle that past performance is not an indicator of future performance, and indeed, on a long enough time line the survival rate for everyone drops to zero.

Conclusion

The progression of IT risk from qualitative measures to cyber risk quantification is clearly going to continue in the coming decade. We will see more regulators requiring quantified statements of cyber risk. Further, they will require such statements to be backed up by capital reserves sufficient to protect the firm and its customers from the fallout of such incidents. This will continue for highly regulated industries, especially financial services, but will also make its way into others, probably through cyber insurance policy underwriting similar to the way that fire insurance has driven better practices into commercial and residential buildings via local code specifications.

Organizations not required to take on CRQ either through regulatory or insurance underwriting requirements may find themselves at the mercy of customers asking them to post bonds to assure that their data is secure while in their care and the amount of that bond will need to be rationalized, undoubtedly by CRQ methods. Avant-garde organizations will have the opportunity to lead the marketplace by making public statements about their IT risk management practices using quantified, time-bound statements to give customers assurance over their operational due diligence and cyber risk hygiene. Irrespective of origin, however, the next decade of IT risk will be quantified.

About the Author

Dr. Jack Freund, CISSP, CISA, CISM, CRISC, CIPP, PMP, is a leading voice in cyber risk measurement and management. He is currently serving as Director, Cyber Risk for TIAA. Jack has been named an IAPP Fellow of Information Privacy and ISACA’s 2018 recipient of John W. Lainhart IV Common Body of Knowledge Award. Jack’s book, Measuring and Managing Information Risk: A FAIR Approach, was inducted into the Cybersecurity Canon in 2016. All of Jack’s writing and work is available at riskdr.com and he can be reached at jfreund@gmail.com.