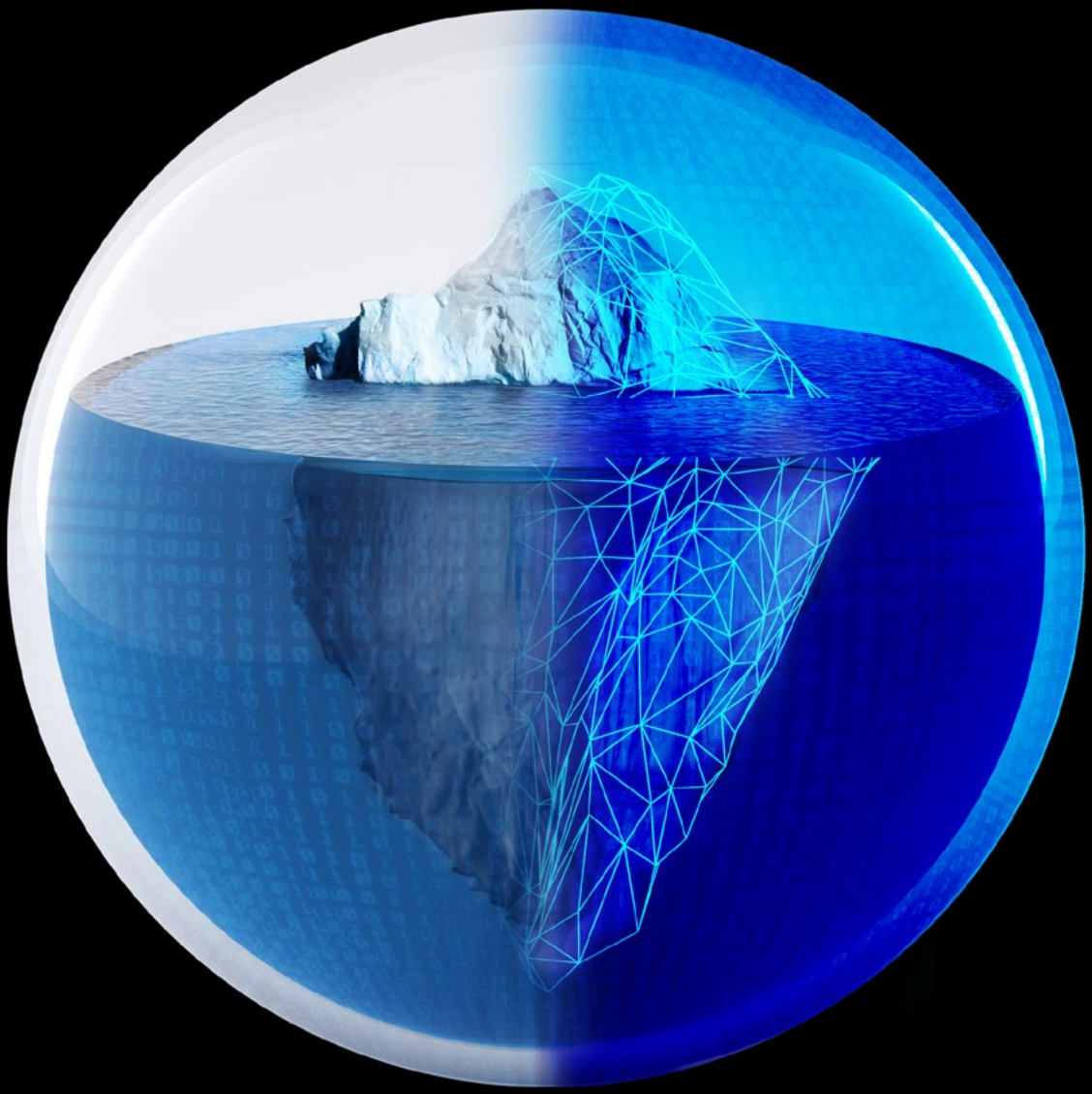
Deloitte.



Beneath the surface of a cyberattack: Collision avoidance

The business application of cyber risk quantification

Figure 1.

Fourteen cyber breach impact factors

Foreword

In 2016, Deloitte published a study titled "Beneath the surface of a cyberattack," which discussed, in financial terms, the broader business impacts a cyberattack may have—from incident discovery through the longer-term recovery process.[2] Applying financial modeling methods, 14 cyber breach impact factors were identified and analyzed, including both direct and intangible costs, as they played out in phases over time (figure 1). A 15th impact factor, national security and economic impact, was later added to better describe mission impact within public sector organizations. The study showed that behind the scenes, organizations often discover the rippling aftereffects of a cyberattack are broader and deeper than planned—particularly when it's more destructive than a common data breach, illuminating the need for precise risk quantification techniques.

More recently, in February 2018, the Securities and Exchange Commission (SEC) compelled "public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyberattack."[3] This imperative highlighted the increasing need to develop more proactive risk assessments and protocols to quantify risks.

Today, organizations face an era of "cyber everywhere," of hyper-connected, unparalleled data and device connectivity, with Internet of Things (IoT) and other technologies contributing to expanded attack surfaces. "As the world becomes smaller, cyber is getting bigger, and it's moving in multiple dimensions across multiple disciplines—beyond an organization's walls and IT environments and into the products it creates, the factories where it makes them, the spaces where its employees conceive them and where its customers use them."[4] These cyber risk landscape shifts have solidified the need to avoid the symbolic "icebergs beneath the surface" and to use cyber risk quantification (CRQ) for both overarching risk assessments and more granular, specific business use cases (such as digital transformation projects and mergers and acquisitions).

This study is written as collision avoidance for a host of leaders who face challenging business decisions every day to navigate risks, known and unknown. We hope this discussion will:

- Help leaders shine a spotlight on the financial risks associated with increasing the organization's technology footprint into the cyberspace domain
- Facilitate a deeper understanding of methods to enhance and align broader risk "buydown" investments across the organization
- Expand the application of CRQ as a means to provide data-driven and defendable insights into business decisions and other large transactions that could otherwise be fraught with risk

Recent advances in artificial intelligence (AI) and information theory practices by both individual organizations and industry associations are quickly paving the way for the use of advanced modeling techniques for quantifying cyber risk. Careful application of these modeling techniques can help reduce the ever-growing business risks that organizations are facing in today's increasingly hostile cyber environment.

Deborah Golden
US Cyber & Strategic Risk Leader, Principal
Deloitte & Touche LLP

Jeffrey Kennedy
US Valuation and Modeling Services Leader, Principal
Deloitte Transactions and Business Analytics LLP

Safely navigating cyber risk

Safe navigation is the process of using available sensors and data to ensure that navigators have the most relevant information to fully understand all the risks so that the best possible decisions are made to mitigate those risks before they can cause harm. It's a process that mirrors how C-suite executives are looking to improve the value of investment in cyber tools and capabilities while removing what may be ineffective or excessive in terms of people, process, and/or technology. A variety of tools have emerged to help categorize and manage cyber risk, such as scorecards or dashboards (for example, red, amber, and green "lollipop" charts). While these can be helpful, chief information officers (CIOs), chief data officers (CDOs), and chief information security officers (CISOs) face increasing pressure from executive leadership to quantify cyber exposure in dollar or mission terms, not just the overall "color" health of a particular business process or function (figure 2). These stakeholders seek hard data relevant to business value, to understand risks with the greatest impact, and the overall "cost" to resolve the risks (in part or in whole). The factor analysis of information risk (FAIR) method is emerging as a popular ontology for determining value at risk (VaR). However, tailoring the FAIR taxonomy is often needed to meet the specific requirements of an organization.

Figure 2. Emerging questions in the spectrum of stakeholders

CRQ provides a repeatable model for insights in the context of individual use cases

When navigating the high seas, a **360-degree collision avoidance system** senses threats and hazards, calculates risk, and recommends preemptive action to avoid and mitigate potential accidents. For cyber risk, we use CRQ: cyber risk quantification.

Despite CRQ's inherent advantages to inform fiscal decisions, many organizations have been slow to adopt its principles. According to Deloitte's 2019 Future of Cyber Survey, only half of the C-level executives who responded use any form of quantitative risk-evaluation tools (including financial loss models). The other half still rely largely on the experience of their cyber experts, maturity assessments, or other qualitative measures to gain an understanding of their cyber risks.[4] One reason may be that many methods do not provide leaders with tailored actionable insights parsed in the context of their individual roles and responsibilities. For example, while a chief financial officer (CFO) can better relate to cyber risks placed in the context of impact on large financial transactions, the chief risk officer (CRO) might prefer a view of cyber risks parsed and correlated against broader enterprise risks.

Figure 3.
360-degree collision avoidance: Foundational elements of the CRQ framework

Cyber quantification models estimate the probability and impact of potential security events in order to calculate financial and mission risk metrics such as value at risk (VaR) or expected loss.

50%

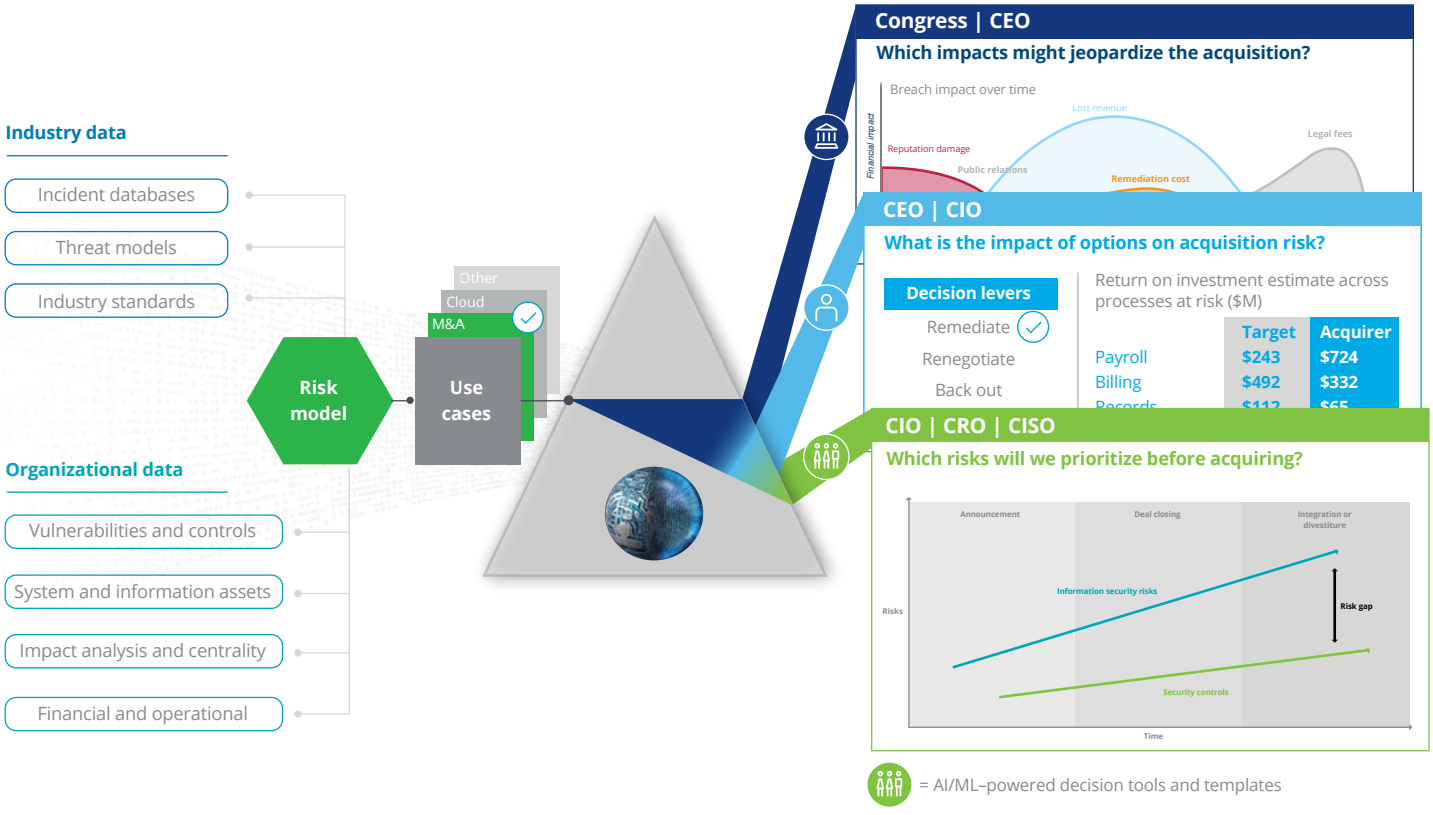
of participating C-level executives employ risk quantification tools to track and evaluate their cybersecurity investment decisions

Source: Deloitte Future of Cyber Survey 2019

A well-designed model can be applied to specific use cases to estimate impacts and loss probabilities using a combination of data-driven statistical mathematics, scenario analysis, expert judgment, and financial analysis. Combined, they can help determine a loss distribution, which is used to calculate dollar loss metrics such as value at risk (VaR) (figure 3).

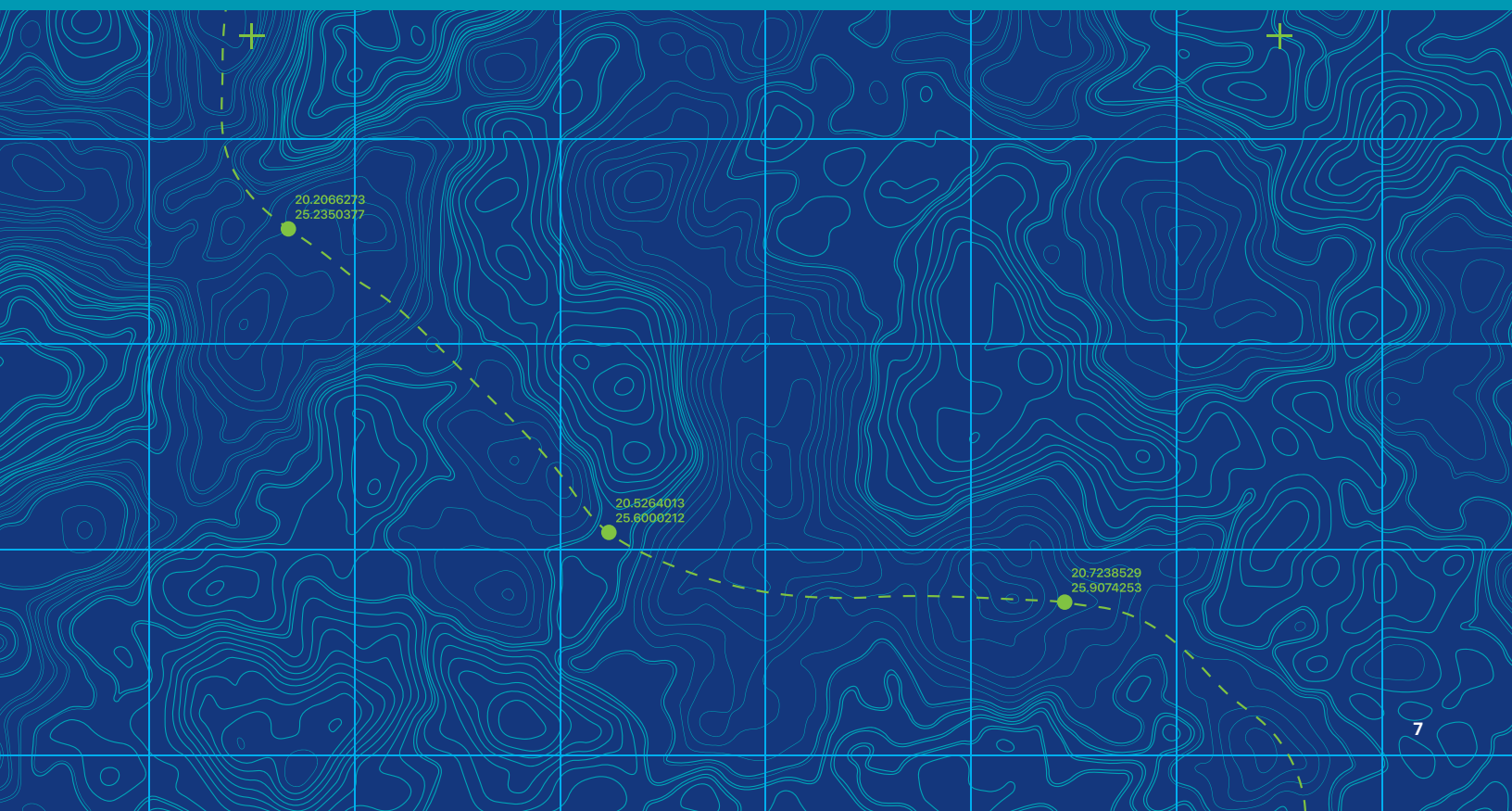
While enterprise-level CRQ is useful, decision-makers and implementers need a consistent model to quantify risks through a prism tailored to their own business scenarios and priorities. Just as a dispersive prism can be used to break up light into its constituent spectral colors, this same science can describe how a risk quantification model can disperse information to specific stakeholders. For example, Deloitte's Risk Quantification Prism™ (figure 4) provides the ability to aggregate, normalize, and enrich data inputs, run these data sets through a tailored modeling methodology, and then automate the distribution outputs through the lens of specific business scenarios and use cases.

Figure 4. Risk quantification should tailor insights to stakeholders (illustrative M&A use case)



Safe navigation: CRQ in action

There are many data sources to assist the mariner. These include charts; advisories; and electronic aids like GPS, radar, and radio. Individually, they cannot confirm the ship is safe, but when brought together, they aid in making the right decisions to avoid miscalculations. To demonstrate how CRQ can help organizations navigate potential hazards, we offer two scenarios to illustrate how the Risk Quantification Prism™ supports risk decisions. Use case 1 features a private organization—a health care system—and use case 2 simulates CRQ for a public service organization—a tax administrator. The organizations and the situations are fictitious, but highlight how CRQ can be applied to support a variety of strategic business decisions.



USE CASE 1

Health care system merger and acquisition (M&A):

Understanding value (and risks) before you buy

M&A continues to be a favored corporate growth tool of executive teams, and the trend is growing. Today, many organizations tend to combine for several strategic reasons, including market expansion and scale efficiencies.

However, in the complexities that often characterize an M&A transaction, there are many balls in the air that deal teams must juggle during the due diligence process. One of the heaviest activities, and one that is often glossed over, is cybersecurity. At each stage of the M&A process—strategy, screening, due diligence, transaction execution, and integration—there is heightened risk for cyber threats and vulnerabilities that, if not discovered and/or mitigated in advance of a merger, can harm both the acquirer and target organization or potentially scuttle the deal altogether.[5]

Throughout the M&A life cycle, cyber risk exposure can increase, from the announcement of the transaction (for example, outside adversaries seeking to understand revenue projections) to the integration or divestiture process (such as insider risks from disgruntled, soon-to-be-separated employees). As risks increase, however, the impact of not having the appropriate security controls is often not fully understood or may not keep pace with the acquisition decisions being made (figure 5). If realized, these impacts could include:

- Improper pricing that doesn't reflect potential loss scenarios uncovered in a broad assessment of the target organization
- Poorly formed financial agreements that do not accurately portray the distribution of responsibilities of either (or both) the

About the organization

Leading provider health care system serving 30 counties in the Midwest. Includes a 698-bed hospital; hub of health care system. Specialties include typical areas such as:

- Emergency care
- Intensive care
- Pediatrics
- Neurosurgery
- Cancer care

Number of employees: 7,500
60 specialties; 990 physicians
Revenue: Approximately $800 million
Assets: Approximately $3.1 billion

target and acquiring organizations or the cyber risk mitigation capabilities that will be needed in the newly formed entity

- Unwittingly exposing the acquirer's or target's systems to threats during integration

These are just a few of the potential traps that could ensnare an M&A transaction. But a step that organizations can take to mitigate these potential risks is to form a cyber risk management team prior to initiating a M&A process that leverages a risk quantification methodology. Such a team can provide strategic input alongside other variables at the onset of the deal to help guide decision makers in understanding the cyber risks, in financial terms, so that decisions are better informed.

Approach: The M&A quantification model

To illustrate the practical application of CRQ in an M&A use case, we will present an example of a leading national health care system as it entered into an agreement to acquire a midsize not-for-profit (for context, a health care system serving around 60 specialties with about $800 million in annual patient revenues).

To begin, the acquiring organization built a foundational cyber risk model in the initial due diligence process that quantified the impact of a variety of likely scenarios, but specifically focusing on the loss of personally identifiable information (PII) or protected health information (PHI), which were considered to be the most financially impactful.

The acquiring organization applied the principles of CRQ to the target health care information systems environment, focusing on the critical business service(s) that hold PII or PHI (such as application, data, infrastructure, and associated security controls). The analysis specifically sought to quantify the liability a data loss scenario might introduce within the combined organization. The model was used by

Figure 5. The M&A risk gap increases over the life cycle of the deal

Source: Deloitte & Touche LLP, 2016

the acquiring organization to conduct a comparison of the risk posed by applications and data owned by the target organization and the financial risks they pose, considering the combined business value, assets, maturity assessments (target), threat profile, and other available modeling inputs.

The organization created a tailored risk quantification model (applying the techniques described in Deloitte's "Beneath the surface" paper)[2] to estimate the potential financial losses of a data breach scenario. The output in this case illuminated financial losses associated with a decrease in brand reliability, potential negative adjustments to contracted rates from key payors, capital expenditures to enhance information security, increases in cyber insurance premiums, regulatory actions and legal costs from attorneys, and litigation from affected patients. Further, for illustrative purposes, the probability of loss is largely attributed to security control gaps in the target's access management, data protection, and recovery programs.

Output: The M&A quantification model empowers negotiations

The multifaceted picture of the CRQ model provided deeper clarity when the CEO presented the acquisition business case to the board for a formal go or no-go decision. The model identified losses associated with specific security control flaws in the target organization, exposing potentially large financial risks.

The CRQ model was able to illuminate the financial implications associated with bringing these two separate security organizations, IT, and associated security controls together. CRQ impacts supplemented the broader due diligence financial model (including accounting and operations), with the resulting profit and loss (P&L) presented to the organization's board of directors. In this case, the CEO presented trade-offs and potential negotiation levers to help navigate the next steps in the M&A process, whether that be to escrow the liability, require the target to remediate some (or all) of the security controls, reduce and/or negotiate the overall purchase price, or decide to scuttle the deal altogether. This methodology becomes a repeatable model also tailored to joint ventures and divestitures.

Trade-offs and potential negotiation levers help navigate the next steps in the M&A process

Figure 6. Quantification models inform M&A decisions levers

USE CASE 2

Tax administrator cloud migration:

Quantifying trade-offs and mitigating impacts

Today, many organizations are focused on cloud migration as an important strategy in their quest to move toward digital; enhance the customer experience; and increase flexibility while improving resilience, availability, and security. As indicated in Deloitte's 2019 Future of Cyber survey, 60 percent of responding organizations are prioritizing activities related to digital transformation, such as cloud, artificial intelligence (AI), and Internet of Things (IoT). According to our survey, however, respondents view digital transformation as one of the most difficult aspects of cyber risk management, with the CSO (35 percent) and CIO (34 percent) respondents ranking digital transformation as most challenging.[4]

Cloud migration is at the forefront of digital transformation, with organizations increasingly leveraging the cloud for many of their critical business needs. However, while the cloud has both enabled business innovation and created opportunities to mitigate an ever-expanding set of cyber risks, the foundational scenario and model that follows identifies specific CRQ approaches organizations can leverage when prioritizing investments in a major cloud transformation program.

Approach: The cloud migration security quantification model

In this example, an organization which administers taxes in the public sector assessed two of its most likely—and costly—scenarios. The first scenario was an internal actor that could cripple its ability to receive tax payments (or require a switch to manual processing), the second a nation-state stealing financial profiles of high-net-worth individuals and those occupying senior executive or national security positions as part of a cyber fraud campaign.

About the organization

Large tax administrator. The organization faces a number of potential loss scenarios, including business disruption and the loss of personal identifiable and health information (PII/PHI) across its business processes of:

- Tax payments
- Tax refunds
- Information returns
- Notices

Number of employees: 6,500
Taxes collected: $135.2 billion
Budget: Approximately $800 million
Assets: Approximately $1.1 billion

35%

of CSOs and CIOs believe cyber transformation is the most challenging aspect of cyber management

Source: Deloitte Future of Cyber Survey 2019

The organization conducted in-depth analysis on these scenarios through activities such as estimating the change in risk exposure over time, quantifying root causes of impacts, and identifying trends. As part of the overall risk quantification planning, the organization tailored a pool of repeatable templates to address situations and decisions they anticipated and down selected to the most relevant interpretations and views. For example, they knew cloud migration would be a major priority over the next several years but couldn't tell what or when exact decisions had to be made. So they prioritized creating collaborative spaces (decision support environments) with already curated data relevant around cloud risk decisions so they would be ready as those situations arised.

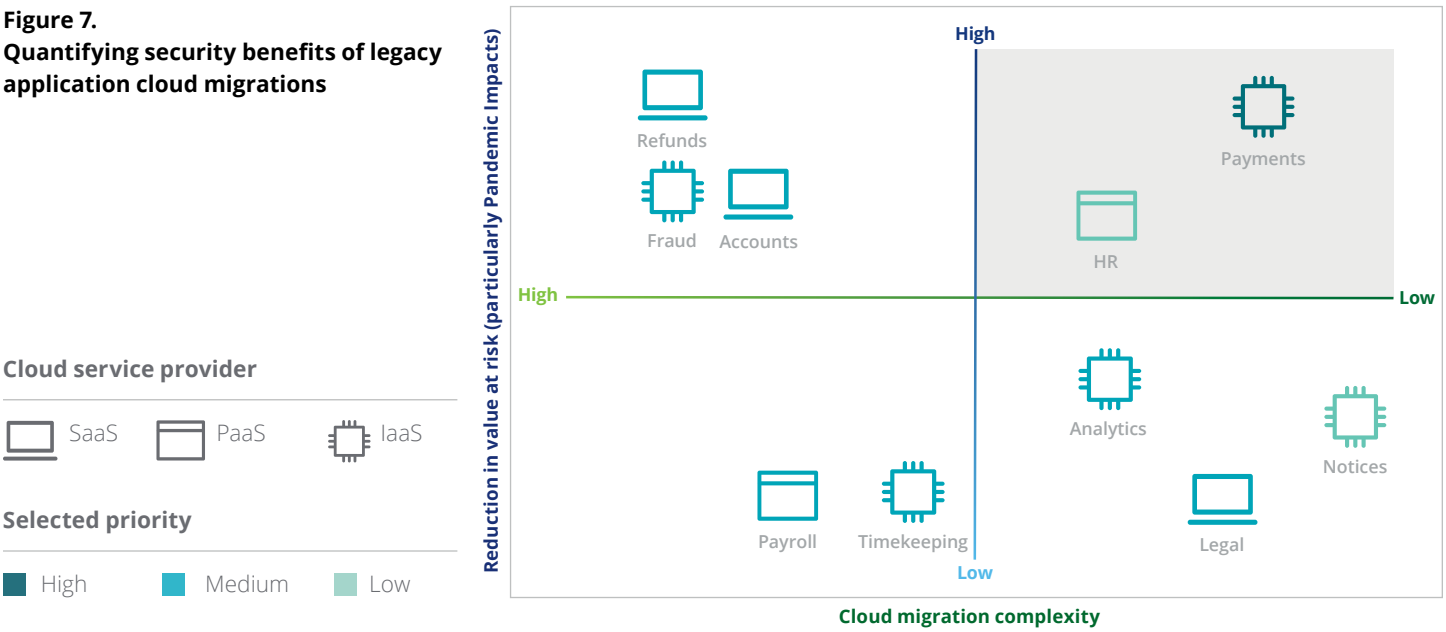
Output: Cloud security quantification model to prioritize legacy application migrations and roles

One of the first templates selected was a security decision aid to assist in deciding which legacy systems to migrate into a cloud environment (those reducing overall value at risk—see figure 7). This view confirmed that the cloud service provider demonstrated more robust security capabilities at a specific tier (such as software-as-a-solution (SaaS) or platform-as-a-service (PaaS)) than the legacy application. Of note, robust cyber security hygiene is still appropriate in both cloud and legacy scenarios.

Steps to applying CRQ in this context involved comparing the current VaR to the VaR after the cloud migration application (with Pandemic impacts given greater weights) while still considering the complexity of application migration. Just because an application migration may lower risk doesn't mean it is the easiest application to migrate. This "with and without" analysis consisted of three primary steps:

1. **Determine current value at risk.** The process started with a baseline understanding of the total VaR. These estimated impacts not only compared the likelihood of cyberattacks affecting the organization from a variety of technical and nontechnical sources, but also evaluated in what tier the risks existed to help determine potential solutions.
2. **Simulate change in value at risk and complexity for alternative cloud migration scenarios.** The organization

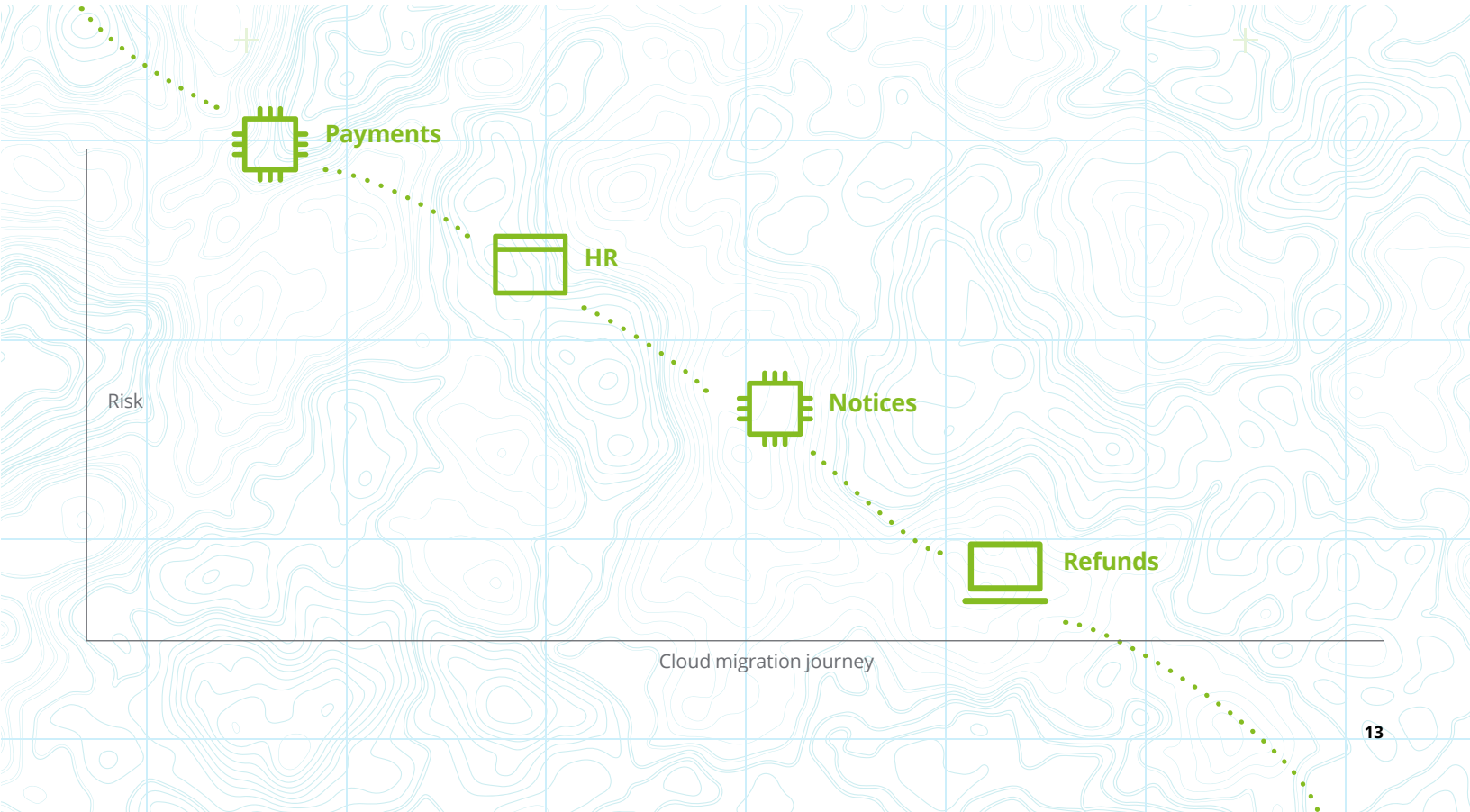
Figure 7.
Quantifying security benefits of legacy application cloud migrations

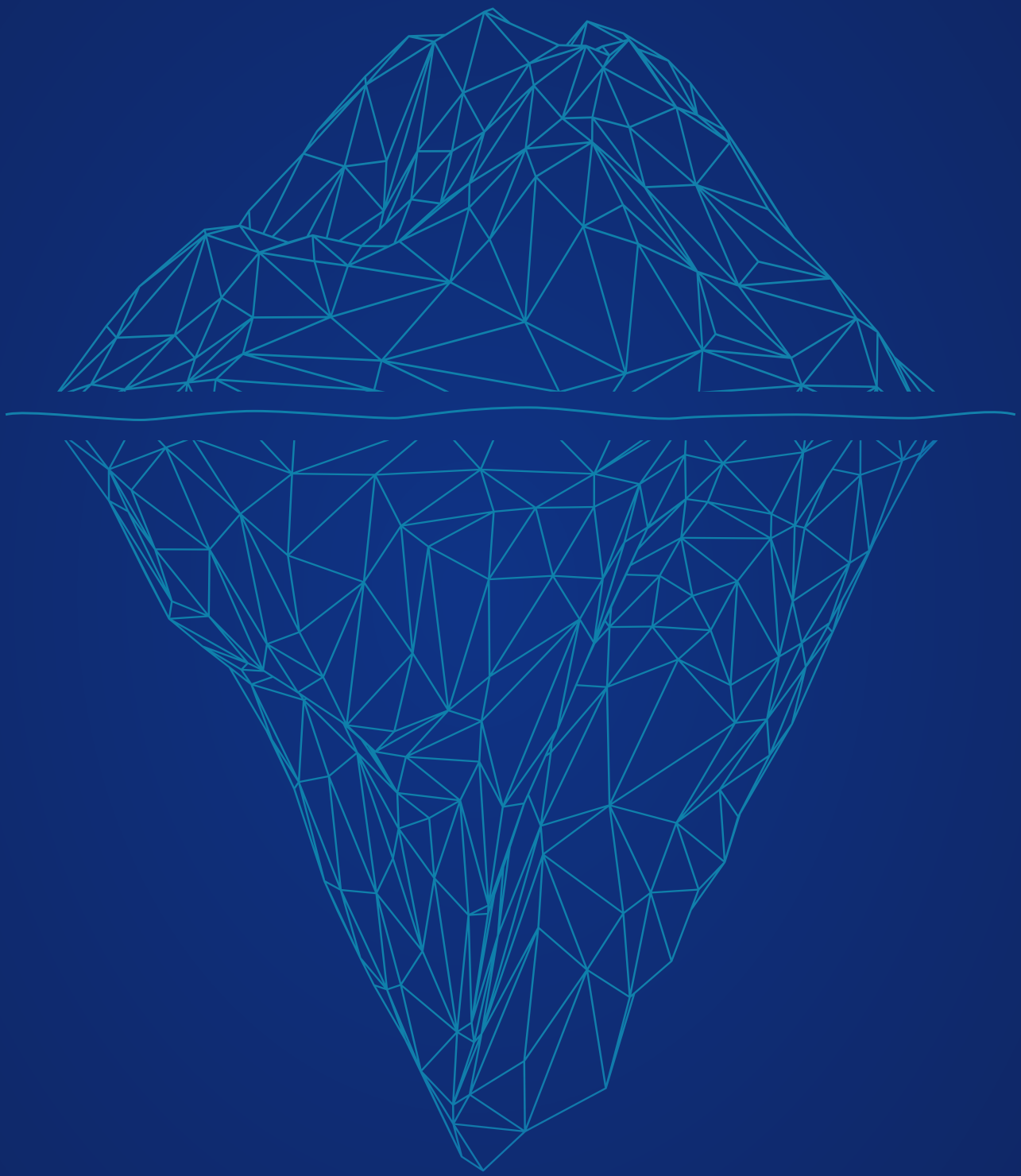


modeled the track records of potential cloud service providers (CSPs) to evaluate the security benefits of transitioning specific applications to those CSPs. However, transitioning applications to higher tiers (such as SaaS) can also have a greater amount of complexity, because more business processes will need to be redesigned. Simulating these design trade-offs helps the organization make clear-eyed decisions.

3. **Prioritize specific applications and tiers to migrate.** The organization used its tailored CRQ model to identify the specific legacy applications to migrate and which tiers to transition (for example, operating system, platform, or application). For example, for concentrations of security risks existing at the application code tier, the organization prioritized adopting SaaS, assuming complexity was also low; whereas, where operating system risks were more prevalent, priority was given to migrations that provided continual patches and upgrades.
4. **Distribute decisions throughout the organization.** Machine-learning logic was used to steer relevant data, metrics, and information to decision-makers needing to understanding specific risks and their financial impact. The output provided the CISO with not just a security voice, but also a fiscal voice that didn't exist previously. Instead of only presenting the risk to cloud assets in general terms, the CISO shared insights that directly quantified the specific financial losses with the CFO in order to better prescribe the investments necessary to mitigate potential losses. Specifically, to not only view that the organization had the right technology migration priorities in place, but also identify opportunities to accelerate risk buydown.

Figure 8. Risk quantification models help navigate the cloud migration journey





Outcomes and opportunities: Collision avoidance in cyber risk navigation

Visibility is an important aspect of avoiding collisions, and a mariner who is more aware of their surroundings is less likely to be involved in an accident. Tracking systems that collect, model, and present information help provide visibility well beyond that which the human eye can see, improving safety across whole operations. The parallel exists for organizations working to prevent and reduce the impact from a cyberattack. As the rate of attacks and attack surfaces increase, so too must organizations' ability to identify the risks on the horizon and correctly correlate the level of investment necessary to mitigate, remediate, or even capitalize on such risks. In the use cases presented, executives can extrapolate ways CRQ can help provide a common taxonomy regarding risk management.

In the M&A use case provided, CRQ aided in uncovering the potential level of cyber risk exposure that the acquiring organization may take on as a result of the acquisition of the target organization. The process provided a baseline, a point of discussion around the likely cyber investments necessary should a final decision to purchase the target organization be made. In the event the risk exposure dollar values are too high or beyond the monetary thresholds established, this defendable supporting data could provide justification to scuttle the deal altogether or be leveraged as a bargaining tool to affect the purchase price of the target, therefore enhancing the overall anticipated rate of return.

In the cloud migration use case for the tax administrator, CRQ was leveraged to better understand the relationship between complexity and the overall return on investment of migrating critical business processes to the cloud. The process enabled the organization to better prioritize migration at the earliest stages of projects

providing data necessary to calculate risk buydown—essentially "baking in" cybersecurity up front.

While the use cases discussed above are hypothetical, CRQ is emerging as a leading decision aid in helping to manage risk. As organizations consider the application of CRQ within their own environments, a few leading practices should be considered. These include:

Internal and external data helps validate assumptions. Regardless of the use case, an effective quantification framework should consider both industry and internal data. Industry data is useful, as it can capture extreme "tail risk" events. On the other hand, internal enterprise data provides valuable information on the specific risk characteristics of an organization and may also be useful for assessing real-time threat information. In addition, characteristics such as industry, size of balance sheet, and number of employees influence an organization's overall exposure to cyber risk and should be considered when calibrating a quantification model that leverages industry data. What should not be diminished in the CRQ process, however, is the role judgment plays to help validate or enrich these models. Subject-matter expertise is essential to better understand threats, help shape the most likely threat scenarios, confirm "weighting" schemes, and—most importantly—validate modeling assumptions.

Scaling the distribution of the model drives adoption. Organizations may experience challenges scaling the CRQ model beyond a few scenarios without the technical capabilities to aggregate, normalize, and enrich data across a variety of sources. Automation, through the use of AI and machine learning (ML), can not only help create efficiencies and repeatable, improved risk insights, but also begin to distribute these insights at speeds that can potentially outpace the threat.

CRQ should enrich, but not replace, other risk management processes. While CRQ provides a business-focused methodology to model risk, organizations should not consider modeling as stand-alone. Other tools, while not new, help to paint a more complete picture of an organization's potential exposure. These include independent cybersecurity assessments, external cyber reconnaissance, automated breach simulations, wargaming, and internal IT audits. In fact, today, Deloitte is transforming the traditional way cybersecurity assessments are conducted through innovative thinking and continuous application of data-driven approaches to inform decision-makers in real time, not just on a periodic basis. In aggregate, these assessment tools can not only aid in providing a broad view of the cyber risks an organization faces, but can also be used to challenge the assumptions and outputs of each other, creating a healthy friction to help ensure the most accurate representation of risks and remediation recommendations is presented to executive leadership.

Develop a repeatable CRQ capability to help navigate the pace of change. Given the pace of change, organizations can begin to apply CRQ to quantify cyber risks more broadly around many strategic business decisions (big and small). These might include using CRQ to help determine the dollar value the organization should consider transferring to a cyber insurance provider or to help measure the growing financial risks associated with reliance on third-party vendor support for critical business functions. Regardless, to keep pace with burgeoning cyber threats and ensure organizational dollars are spent wisely, organizations should consider implementing repeatable modeling processes to allocate funding efficiently, measure investment effectiveness, and forecast future risk and budget needs.

During maritime operations, collision avoidance works because it collects from multiple data sources, predicts risk based on current conditions, and recommends preemptive action to avoid and mitigate accidents. Just like maritime operations, CRQ can help serve as collision avoidance in your organization. A mature CRQ approach can provide a structured way for organizations to collect and report cyber risk in dollar terms, in a way that both technical and nontechnical stakeholders can understand. Without such efforts, organizations may find it increasingly more difficult to navigate the rough seas of cyber risk on the horizon.

Endnotes

1. 15th impact factor added in the Federal version of the paper. Deloitte, *Beneath the surface of a cyberattack: A deeper look at Federal Sector impacts*, 2017
2. Deloitte, *Beneath the surface of a cyberattack: A deeper look at business impact*, 2016.
3. US Securities and Exchange Commission, *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, Release Nos. 33-10459; 34-82746, February 26, 2018.
4. Deloitte, *Future of Cyber Survey: Cyber everywhere, succeed anywhere*, 2019.
5. Deloitte M&A Institute, "Don't drop the ball: Identify and reduce cyber risks during M&A," 2016.

Authors

John Gelinne
Managing Director
Commercial
Cyber Quantification Leader
Deloitte & Touche LLP
+1 410 649 4775
jgelinne@deloitte.com

Kelly Miller Smith
Principal
Government & Public Services
Cyber Data Leader
Deloitte & Touche LLP
+1 571 814 6804
kellysmith@deloitte.com

Hector Calzada
Managing Director
Commercial
Valuation Leader
Deloitte Transactions and Business Analytics LLP
+1 404 631 3015
hcalzada@deloitte.com

Contributors

Andrew Morrison
Timothy Li
Steve Livingston
Michele Sipes
Nicole Hockin
Dovid Adler
Emily Johns
Madhavi Karkala
Dan Sadler
Samir Khakimov
Halle Hagan
Danielle Restaino

Deloitte.