CAPCO

a wipro company

THE CAPCO INSTITUTE

JOURNAL

OF FINANCIAL TRANSFORMATION

FINANCIAL

Managing the uncertainties of cybersecurity

MARTIJN DEKKER

CRISIS MANAGEMENT

#57 APRIL 2023

THE CAPCO INSTITUTE

JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

CONTENTS

FINANCIAL

REGULATION

ESG

DEAR READER,

Recent events in the U.S. banking sector, and broader concerns around instability and contagion within the global financial services industry, have meant that crisis management is once more front of mind for many institutions.

In addition, the world of business and finance is facing broader geopolitical and socioeconomic challenges, ranging from conflict, climate change, inflationary pressures, and precarious energy resources. Factor in heightened regulatory and competitive pressures, and it becomes clear that financial institutions must prioritize risk management, within their own organizations and with their counterparties.

The papers in this edition of the Journal address the theme of crisis management through various lenses, including regulatory compliance and traditional risk management, as well ESG, the low carbon economy, and sustainable finance. Our authors also explore topics such as the impact of social change on the world of finance, the rise of artificial intelligence and virtual reality technologies, and cybersecurity.

Contributions in this edition come from a range of world-class experts across industry and academia, and showcase some of the very best expertise, independent thinking, and strategic insights within the financial services sector.

As ever, I hope that you find the latest edition of the Capco Journal to be engaging and informative. Thank you to all our contributors, and thank you for reading.

Lance Levy, **Capco CEO**

MANAGING THE UNCERTAINTIES OF CYBERSECURITY[1]

MARTIJN DEKKER | Visiting Professor of Information Security, University of Amsterdam,
Global Chief Information Security Officer, ABN AMRO Bank N.V.

ABSTRACT

Companies and organizations need, more than ever, to control their digitalization efforts. This is due to the increasing importance of digitalization to their business models and due to the increased IT spend levels. In the current threat landscape, digitalization can also lead to significant operational risk events. Managing these events requires an approach that incorporates the growing uncertainty in the probability and impact of these events. This article highlights how corporate and information security executives can improve the way they communicate with each other in order to manage these events.

1. INTRODUCTION

As digitalization has become a top priority for almost all industries nowadays, it has led to information security also becoming one of the top concerns for companies, their boards, and their stakeholders. The European Union is tracking the level of digitalization on a yearly basis[2] and although there are differences between countries, a steady increase in digitalization is obvious. This holds true for larger enterprises as well as smaller companies consisting of only 10 people or more. In those smaller companies, technology is usually used via managed services or cloud providers. This shows that technology is increasingly becoming essential for the daily operations of any company.

There are three important reasons why digitalization is a priority for decision-makers. First, business leaders should pay attention to technology, and in particular the use of data, because it is creating both new opportunities and new, sometimes disrupting, business models. This makes digitalization clearly of strategic importance.

To illustrate the operational relevance of IT to companies, we can look at IT spend. In the Flexera state of tech 2022 report,[3] the results of their survey amongst 501 companies worldwide concerning IT spend and priorities are published. One of the conclusions is that IT spend is on average 8 percent of the total revenue of companies. A vast majority of the respondents (71 percent) expect that their IT budgets will increase next year. This financial view is the second reason why executives should be paying attention to it.

Finally, the third reason that technology is a priority that requires board level attention is the fact that it gives rise to significant and even existential operational risks. We will discuss the implications of the need to manage those risks and, in particular, information security risks.

2. UNDERSTANDING INFORMATION SECURITY RISK

Managing risks is what boards and leaders are used to doing. Having to decide between scenarios without perfect information is also something executives are used to. Yet,

[1] This article is based on earlier blogs by the author and reflects solely the views of the author, not necessarily those of ABN AMRO Bank N.V.
[2] Eurostat, "How digitalised are the EU's enterprises?" August, https://bit.ly/3kKNhVc
[3] Flexera, 2022, "Flexera state of tech 2022," https://bit.ly/3lAkgDl

managing information security risks requires knowledge and skills that many boards are not yet familiar with. Given the role of technology in businesses, and its implications for operational risks, it becomes imperative for boards to become used to managing technology and information security risks.

Risks[4] are potential events that can occur with a probability p and with an impact i. The magnitude of the risk is usually expressed as $R = p \times i$. Risk management is then about estimating the p and i to implement controls that reduce the risk to a level that is deemed to be acceptable. Risks become uncertainties when the p or the i are unknown or not well understood.

This seems a rather straightforward task, but assessing these probabilities and impacts is increasingly difficult in the complex world that businesses now need to navigate. In the technology domain, this is compounded by two additional factors.

The first factor is the complexity of the technology landscape. In large enterprises, that landscape can consists of hundreds or even thousands of applications and services, hosted in multiple data centers and by multiple (cloud) providers. This can also be spread over multiple countries and jurisdictions, adding legal and regulatory complexities. In smaller companies, the technology is usually outsourced to multiple providers, which is complex too. In general, we see a lengthening of supply chains in all industries, which has inherent operational risks. These risks manifested themselves, for example, during the COVID-19 pandemic and subsequent lockdown measures across the world that impacted those supply chains. These impacts were often unexpected. Hence, to assess impacts, one needs to consider not only sources of risk within one's own data center or in-house managed IT landscape, but also sources of risk within supply chains, value chains, or technology chains. The complexity of the technology landscape supporting the business makes it hard to determine the impact (i) of a potential event.

A striking example of this was the vulnerability discovered in the widely used Citrix software. On December 17, 2019, Citrix published on their website the discovery of a vulnerability in some of their software products. The vulnerability would allow hackers to intrude networks. Although Citrix provided guidance on how to deal with this issue, a solution was not immediately available and in January 2020, the Dutch National Cyber Security Center issued an urgent advice to the general public and Dutch corporations to switch off their Citrix installations. This shows how a software vulnerability in a third-party developed and maintained piece of software translated into an unavailability risk for thousands of companies worldwide (some sources estimated that 80,000 companies were affected).[5] Depending on the usage of the software within a company, this risk can be high and even critical. It turned out that many companies were not able to assess the risks arising from this vulnerability and, therefore, had to simply turn it off, often causing business continuity issues. For example, their employees could no longer access their systems to do their work.

The second factor is the fact that the threat landscape has become extremely volatile, with many highly connected and motivated threat actors. Some information security risks happen by accident and can be modeled by pretty well-known probabilities and impacts, for example, the risk of a server shutting down because of a hardware failure. But there is a growing category of information security risks caused by motivated adversaries. The behavior of these actors is not random but targeted, organized, and hard to predict. The fact that adversaries change their attack patterns based on the defensive controls they encounter in a particular target, impacts the defender's ability to assess the probability. This human behavior creates uncertainty in the probability distribution (the p) of a risk. A more extensive description of this inherent uncertainty in the domain of information security can be found in Dekker (2022).[6]

As stated, uncertainty and risk (p times i) are different notions. Any risk is an uncertainty, but an uncertainty is a potential event with probabilities or impacts that are unknown or are uncertain. The extension of the domain of risk management to also include uncertainties is a relative new development. It started with a new definition of risk in ISO31000:2009. In that framework, a risk is defined as the "effect of uncertainty on business outcomes." Although this would imply that risks and uncertainties are related, only in ISO27000:2018 this more general definition of risk was adopted in the cybersecurity context.[7] Currently, many risk assessment methodologies that are in actual use still apply the "$p \times i$" model as an approximation of risk.

[4] In this article we will always define "risk" in this strict sense, even though in ISO31000 a more general definition is used. This will help us better distinguish uncertainties from risks.
[5] Townsend, K., 2019, "Citrix vulnerability leaves 80,000 companies at risk," Security Week, December 23, https://bit.ly/3kDm5l1
[6] Dekker, M., 2022, "Managing information security if managing uncertainty," March 19, https://bit.ly/3y1n9sj
[7] ISO/IEC 27000:2018, https://bit.ly/3SET1fS

In the cybersecurity domain, the level of uncertainty (lack of calculability) in both the p and the i is growing. We believe, therefore, that distinguishing between uncertainty (events with an unknown probability distribution and hard-to-predict impacts) and risks ($p \times i$) matters in cybersecurity. It matters as it leads to different strategies for managing cybersecurity. One of the reasons is the fact that we tend to treat risks and uncertainties differently when making decisions, as is illustrated by the Ellsberg paradox.

The Ellsberg paradox, popularized by Daniel Ellsberg in 1961, is described as a paradox in which people's decisions are inconsistent with subjective expected utility theory.[8] It is generally taken to be evidence of ambiguity aversion, in which a person tends to prefer choices with quantifiable risks over those with unknown, incalculable risks.

Ellsberg's findings indicate that choices with an underlying level of risk are favored in instances where the probability of risk is clear, rather than instances in which the probability of risk is unknown. A decision-maker will overwhelmingly favor a choice with a transparent probability of risk, even in instances where the unknown alternative will likely produce greater utility. When offered choices with varying risks, people prefer choices with calculable risks, even when they have less utility.

Hence, we see that the amount of uncertainty influences decision-making and, as we have argued, the domain of cybersecurity has inherent high levels of uncertainty due to the interplay between defenders and attackers and because of the non-randomness of attacker behavior. There are two other sources of uncertainty that we will now briefly discuss. The first is the agency problem that arises from the highly specialized knowledge involved in the cybersecurity domain. This information needs to be understood by non-technical decision-makers and stakeholders. The second source of uncertainty stems from the different rates of change, for example, between regulation (and other mandatory requirements) and technological developments. Another example is the slow process of control testing compared to the fast changes in the threat landscape. These create pacing problems, which complicate decision-making.

3. AGENCY PROBLEMS AND PACING PROBLEMS

As already mentioned, executive leaders are increasingly required to consider cybersecurity as an element of their business decision-making. Whether it is about business decisions like opening a branch in another country, moving data into the cloud, or launching a new product, security and data protection need to be reviewed and assessed and properly managed. In addition, daily operations and business continuity are increasingly impacted by cybersecurity and many stakeholders (not only customers but also shareholders and others) are demanding more transparency about the cybersecurity posture of a company. Business leaders are, therefore, spending more time on reviewing their security setup. As a result, more security leaders are requested to inform their managing boards about the status of security on a regular basis.

Due to the very technical nature of the topic, information security reports are often hard to understand for the non-technical reader. This is compounded by the sheer volume of management information available. In any larger IT estate, the number of security controls implemented can easily be dozens or more. All these controls need to be tested regularly for operational effectiveness. The resulting reports of the hundreds of instances of controls, their operational effectiveness, and the value of the assets they are supporting, need to be evaluated to enable risk-based decision-making. This is complex, but it is even more complex because some of the controls can compensate others, which is hard to consider without a deep understanding of the control objectives. But even more importantly, one should compare the operational effectiveness to the current threat level. If there is currently no threat that would exploit a failing control, the resulting risk can be low. This brings in the threat perspective, which is as hard as the control perspective. This creates an agency problem between the security specialists and the decision-makers and other stakeholders.[9] Security leaders are facing the challenge of presenting a security posture to the decision-makers that is comprehensible in order to ensure that the business leaders do not overestimate the risk (because they do not understand it) or underestimate it (because they, for example, simply trust the security department to do it right).

[8] Ellberg's paradox, https://bit.ly/3INDZ34; Ellsberg, D., 1961, "Risk, ambiguity, and the Savage Axioms," Quarterly Journal of Economics 75:4, 643-669
[9] Kiesow Cortez, E., and M. Dekker, 2022, "A corporate governance approach to cybersecurity risk disclosure," European Journal of Risk Regulation 13:3, 443-463

One of the compounding problems is the fact that it takes time to test all the security controls. Companies that are doing this on a quarterly basis are doing it fast; many companies are slower. This means that the situational awareness derived from periodic control testing is often at least three to six months old. Given the high volatility of the threat landscape, this creates a pacing problem. Pacing problems arise when two processes of very different rates of change interact. The notion of a pacing problem was first introduced in Downes (2009)[10] in the context of regulations lagging technology developments. In information security there are many pacing problems, for example, the difference in pacing of discovery of vulnerabilities and implementation of patches, fast growing needs for employees and the slow training of new talent, etc. Another important pacing problem is the one arising from the relatively slow policymaking process and the relatively fast developments of technology. This creates regulatory uncertainty for decision-makers, which is particularly relevant in the cybersecurity domain as regulations in this domain often include liability for executives. As argued above, adopting new technologies for new or updated business models is high on the agenda of many managing boards, but the slower regulatory developments and the liabilities associated with regulations can cause boards to adopt a cautious strategy, as it can be unclear what regulatory risks are or will be.

To summarize, we have increased IT complexity due to interconnectedness and growing supply and technology chains. We see a highly dynamic cyber-threat landscape with diverse groups of adversaries with very differing motivations. This uncertainty is now inherent in information security management. It increases the gap between uncertainty management and risk management. Next to that, we have a growing number of security controls being implemented, each producing operational data and data on operational effectiveness. All this data needs to be reconciled into a concise security posture for business leaders to make informed decisions on strategy, resource allocations, or investments, etc. This is complex and hence creates agency problems. Slow control testing in a volatile threat landscape plus regulatory risks arising from the regulation pacing problem adds even more uncertainty.

> *"Executive leaders are increasingly required to consider cybersecurity as an element of their business decision-making."*

4. A WAY FORWARD

Currently, there is no easy solution to this situation. However, there are relevant developments that could provide a way forward. In general, strategies to cope with uncertainty include activities to gather new information as soon as possible and the ability to quickly course-correct earlier decisions and directions.

In the information security domain, this calls for a shift in thinking. Historically, information security started out with a focus on preventative controls and being compliant. When things got more complicated, the field moved towards a risk-based approach. And now that the uncertainty is growing, the field should move to a threat-based approach. A key element of this approach is a good security foundation. This means that the overall security framework is operating above a certain operational effectiveness level. And on top of that, specific controls and specific assets have stronger security controls in place. The decision about which controls and which assets need enhanced attention is threat-based. The volatility of the threat landscape implies that the organization must be able to make timely shifts in prioritization and have the ability to quickly respond to new information.

Consequently, a threat-based security strategy requires, like any security strategy, a mature security baseline, including a complete overview of the assets that need to be protected, and an up-to-date knowledge of the threat landscape. Threat intelligence gathering is, therefore, a key capability. This is also why information sharing is a top priority for security leaders and a central notion in almost all cybersecurity regulations.

[10] Downes, L., 2009, The laws of disruption, Basic Books

Addressing the inherent uncertainty can also be done via Bayes' theorem and threat intel driven approaches allow for actions that reduce uncertainty. This is also the very essence of Bayes' formula: it allows us to adjust probability distributions when new information comes in. In that sense, Bayes' formula makes uncertainty reduction very precise (Dekker and Alevizos (2023)[11] provide a more detailed description of how this can work).

Seiersen (2022) provides a data driven approach to information security that is very well suited to a threat-based security approach.[12] His BOOM framework provides five baselines for managing information security. BOOM is his abbreviation for "Baseline Objectives and Optimization Measurements". These are baselines of metrics that, in our view, allow security professionals to define measurable goals for their security strategies without resorting to $p \times i$ approximations. The metrics also help with communicating with non-technical decision-makers about how well the security strategy is performing. This can help address the agency problem.

To illustrate how cybersecurity status and progress can be measured and discussed with business leaders, we will summarize the BOOM framework. The BOOM framework consists of the following five baselines: survival analysis, burn-down metrics, arrival rates, wait times, and escape rates. These baselines require some maturity in organizational and technical setups. They often articulate security agility and ability to absorb new information. These are, as we argued above, important elements of a security strategy that is aimed at uncertainty reduction.

4.1 Survival analysis

The first baseline is about measuring the survival time of events. By understanding how long events (like vulnerabilities or other risk causes) survive in your environment, and how that depends on the type or severity of events, you are reducing the uncertainty about your risk exposure. An example of this baseline is: "50 percent of critical vulnerabilities live for 48 hours or longer." You need to avoid using averages over clusters of types of events and gather as much fine-grained data as possible.

4.2 Burn-down metrics

The second baseline is concerned with the ratio of removed risks (in a certain timeframe) against the total number of new risks that are out there. It measures whether you are mitigating risk faster or slower than the growth of risk. For example: if in the last month you had 100 new vulnerabilities, and your team was able to remove 60, the burn-down rate is 60 percent. Although this is lower than 100 percent, and hence risk is increasing, if the burn-down rate was 50 percent the month before, you still know you are improving. This is a very useful performance metric that developer teams can use to measure their own performance. CISOs can also use them to compare teams to decide on which team to focus on to make the biggest impact on security in the coming period.

4.3 Arrival rates

Burn-down metrics measure how fast you are removing risks, the third baseline is measuring the rate at which risks emerge. Predicting what will happen tomorrow is difficult, but by leveraging intel-feeds and historical data (for your environment) you can build probability curves that show the chances of a vulnerability for one of your technology stacks being reported on in the coming month. Of course, you need to constantly update those probability curves. Arrival rates are useful to know because the arrival of a new vulnerability defines work for your team. This baseline, therefore, helps you make decisions on resource allocation.

4.4 Wait times

The fourth baseline, wait times, is a well-known measurement in operations management. It is measuring the time between arrivals of risk causes, like vulnerabilities. Knowing this metric helps you optimize your security operations teams. However, it should also be used as a leading indicator for risk: if wait times are decreasing, risk is increasing.

4.5 Escape rates

The last baseline is measuring how risks migrate across your environment. In particular, it measures the rate at which risk-causes move from an environment with one state of control to an environment with a lesser state of control. For example,

[11] Dekker, M., and L. Alevizos, "A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision making," arXiv.org, February 25, https://bit.ly/3kGomCs

[12] Seiersen, R., 2022, The metrics manifesto, Wiley

it measures the rate at which risks are moving from your development environment to the production environment. In other words, the rate at which those risks "escape". Modern software development teams are increasing their release velocity. This would increase the escape rate too, unless your security program is able to reduce escape rates without reducing release velocity.

These baselines are relatively easy to explain, do not require deep technical knowledge, and hence facilitate a meaningful conversation with executives and business leaders. It also provides five easy questions business leaders should ask their security teams to find out about their security strategy and progress towards set goals. The nature of these baselines fit the volatility of the threat landscape and incorporate the resulting uncertainty in risk calculations.

5. CONCLUSION

Information security is a highly complex and technical domain. Given the growing role of IT and digitalization in companies and organizations, decision-makers are required to consider the opportunities of IT for the business strategy, the financial risks of the increased IT spend, and the operational risks arising from cybersecurity. Together with the leadership in their company, information security leaders need to overcome the agency and pacing problems and have a meaningful conversation in order to agree and monitor the execution of a security strategy that is aimed at uncertainty reduction. By adopting a threat-based approach combined with metrics that measure security agility they can navigate the volatile environment, reduce uncertainty, and improve the quality of information security decision-making. This helps in moving beyond a risk-based approach towards an uncertainty-based approach in information security decision-making.

ABOUT CAPCO

Capco, a Wipro company, is a global technology and management consultancy focused in the financial services industry. Capco operates at the intersection of business and technology by combining innovative thinking with unrivalled industry knowledge to fast-track digital initiatives for banking and payments, capital markets, wealth and asset management, insurance, and the energy sector. Capco's cutting-edge ingenuity is brought to life through its award-winning Be Yourself At Work culture and diverse talent.

To learn more, visit www.capco.com or follow us on Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Dubai
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO
a wipro company