PwC Cybersecurity & Privacy Day 2022

Out of the shadows: CISOs & DPOs in the spotlight

It's a wrap for another year (almost - there is still the Cybersecurity Week Luxembourg gala dinner!). Another successful edition of PwC's Cybersecurity and Privacy Day ended on Thursday October 13, 2022.

PwC Luxembourg, CLUSIL (Club de la Sécurité de l'Information – Luxembourg) as well as the CNPD (Commission Nationale pour la Protection des Données) collaborated to create the first edition of the only survey dedicated to CISOs, ISOs, DPOs and privacy experts in Luxembourg, which was presented at the the annual event. This year was a return-to-form with a live event only, and with over 250 attendees it was brimming with great speakers who shared their expertise on cybersecurity and privacy matters.

This year's main focus was on Critical Infrastructure Protection which could not be a more timely topic as cyber threats become more sophisticated and increasingly target operators of critical infrastructure, industries and organisations. These must urgently assess and uplift their cyber resilience.

Closing the event, Koen Maris, Advisory Partner and Cybersecurity Leader PwC Luxembourg, thanked all the participants and organisers for "giving him a full day of their time" and emphasised that, "Critical infrastructure suffers the same cyber issues as other organisations, but with one significant difference, if it fails society gets hit."

2022 CISO's and DPO's role and responsibilities survey

A worthy addition to this year's agenda was the exclusive presentation to attendees of the first edition of the only survey dedicated to CISOs, ISOs, DPOs and privacy experts in Luxembourg.

The session was hosted by Alain Herrmann, Data Protection Commissioner, CNPD (Commission Nationale pour la Protection des Données), Antonin Jakubse, Privacy Senior Manager, PwC Luxembourg, Marc Lemmer, Data Protection Commis-sioner, CNPD (Commission Nationale pour la Protection des Données), Cédric Mauny, President, CLUSIL and Maxime Pallez, Cybersecurity Senior Manager, PwC Luxembourg.

With the growing importance of the CISO in mind (incl. Information Security Officer/ ISO) and DPO (incl. data privacy professionals), the team collected 90 responses from CISOs (41%) and DPOs (47%) within Luxembourg (the remaining 12% represent respondents with both roles).

Home-based working, companies transitioning to digital workspaces or public cloud, an escalating number of cyberattacks and the growing complexity of information systems, evolving legislation and enforcement, better informed data subjects—these and many other factors have further increased the importance of the roles of Chief Information Security Officers (CISOs) and Data Protection Officers (DPOs) in the last few years.

Antonin Jakubse, Privacy Senior Manager, PwC Luxembourg says of the survey, "Privacy without cybersecurity doesn't work. The collaboration of CISOs and DPOs is paramount in order to protect data and ensure privacy".

As always, participants heard from internationally renowned speakers, who shed much light on challenges we are facing in today's sophisticated digital world and with the topic of critical infrastructure in mind.

Speakers highlights included:
- Paul Rhein, from the Governmental Computer Emergency Response Team Luxembourg (GOVCERT.LU), ministère d'État Luxembourg, which oversees the management of cybersecurity incidents compromising Luxembourg, its citizens or its economy and is responsible for receiving, reviewing and responding to reports of such. He emphasised strongly that there is a need to cooperate and collaborate. "We can't solve issues as a single organisation, we need to do it together."
- Eric Kalajzic, Belgian Defence, gave a sobering talk on critical infrastructure in an interconnected world, concluding that infrastructure is a top target for intelligence services, Human beings are the most fragile link (a theme that was repeated over the course of the day), permanent risk assessment and checks are necessary on a regular basis and legal frameworks are key in our democracies.
- Christian D'Cunha, DG CONNECT, European Commission, posed the question, "Can you have privacy without cybersecurity?" and concluded the answer is no. When you are in the cyberworld you are interfering with personal data, hence privacy is affected.
- Dalia Khader, Swiss Life & Donia El Kateb, EIB, gave a fantastic presentation using famous examples of cyberhacks and security breaches, taking the audience on a journey from the past to the present with lessons learned that could be applied to the future. Of their list of key takeaways, they also concluded that what is still missing as we all actively participate in cyberspace is a security culture and awareness, meaning once again, humans are the weakest link.
- Jean de Chillou, CSSF, gave a riveting presentation on how the CSSF and the BCL have adopted the "Threat intelligence-based ethical red teaming" (Tiber) framework last November. This European system makes it possible to launch real-fake cyberattacks against financial or banking institutions, to test their resilience.

Full report:
https://www.pwc.lu/en/advisory/digital-tech-impact/cyber-security/out-of-the-shadows-ciso-and-dpo-in-the-spotlight-2022.html

On elicitation techniques for cyber risk audits

Risk Management is typically based on statistics and risk measures that go with them. If we consider quantitative risk measurement it is typically Value at Risk and/or Expected Shortfall. Apart from questions relating to the coherency of risk measures, different measurement (econometric) methods could be used. Those statistical techniques, however, presume some kind of stationarity of the dataset and more importantly depend on the past.

For most econometricians the past is a good way to learn about the future. This, however, is an assumption and in many cases carefully analysed individual and/or aggregate expectations may provide better information. It turns out that recent research papers address this kind of issues under the term elicitation of beliefs.

The distinction between statistical approaches using the past and elicited probabilities from framed choices go to the heart of conceptual definitions of probability. For most statisticians and economists, probabilities are determined from historical frequencies of events. Some risks such as geopolitical risks and cyber risks, however, are more difficult to evaluate as there do not exist any statistics to evaluate expectations.

This type of uncertainty is more radical and also known in economics literature as ambiguity. This new literature is extensively developed in Marinacci (2015). Note also, as he highlights, that information and uncertainty are twin notions and uncertainty is thus epistemic. There is thus a strong link with information theoretic concepts such as entropy, already extensively used in Rational Inattention models (Mackowiak et al. (2022)).

A way to address decision-making problems when no statistics are available, was originally analysed by de Finetti and Ramsey in the 20's and 30's. In this approach, probabilities are beliefs that are measured through decision-makers' willingness to bet on events. Such epistemic beliefs quantify degrees of belief that can be assigned to any event whether it is repeatable or not. A recent literature has developed elicitation approaches that enable, under some conditions to truthfully extract information about expected events and/or values. The general mechanism is based on the idea that talk is "cheap" but bets on events makes individuals reveal their beliefs.

If we think about Audit and Risk Management, the idea is to extract information about risk distributions and expectations within organizations through decision makers' choices. If we think about a centre, a government for instance, the aim could be to extract informal information about cyber risks by aggregating elicited beliefs extracted from decision makers across institutions.

Let's focus a bit on this new elicitation literature. Cvitanic et al. (2019) propose a new incentive-compatible approach called choice matching. The idea is to link multiple choice questions with an auxiliary question that reveals individual's beliefs (types, in technical terms). The auxiliary task consists in predicting other individual's predictions (answers to potential outcomes). To incentivize the individuals to reveal their beliefs about potential outcomes, a compensation is paid.

This compensation will be based on a score. If such a scoring rule is proper, the beliefs are correctly revealed. Researchers have analysed different elicitation approaches, from incentive compatible rules (Schotter and Trevino (2014)) to un-incentivized elicitation (Trautmann and van de Kuilen (2015)).

Different scoring rules exist and in case individuals are risk neutral it is easy to develop a proper scoring rule such as quadratic scoring rules. The problem arises when individuals are risk averse and/or distort probabilities as documented in the empirical decision making literature. An exhaustive overview is provided by Wakker (2010).

A scoring rule typically defines payments contingent on whether certain events occur. An individual thus faces a prospect whose payoffs will depend on his reported beliefs about those events. The scoring rule is proper when a risk neutral individual is incentivized to report his beliefs truthfully. Offerman et al. (2009) analyse biases when decision makers are not risk neutral and exhibit probability weighting, within the quantitative scoring rule framework.

Calibration exercises show that when the utility function and/or the weighting function are not linear, the reported probability differs from the true probability assessment. One way to solve this issue is to use calibrated versions of utility functions and probability weighting functions such as the one used in Prelec (1998). Another approach is to check for alternative elicitation procedures that are independent from utility and weighting functions.

Schlag and van der Weele (2013) suggest that stochastic payments may overcome the issue of non-linear utility function and probability weighting. Karni (2009) suggested to use auction type mechanisms to reveal probabilities but those approaches can only be used in binary settings. Hossain and Okui (2013) introduce the Binarized Scoring Rule (BSR) which is a stochastic scoring rule that provides either a smaller or a bigger reward. If individuals maximize the probability of getting the biggest reward it leads to truthful revelation. It can be used to elicit any probabilistic value of interest. For instance, the probability that a random variable exceeds a cut-off level, which is the definition of Value at Risk.

Danz, Vesterlund and Wilson (2022) analyse incentive compatibility and its consistency with broader sets of behaviours. They compare different methods with the Binary Scoring Rule developed in Hossain and Okui (2013). The fundamental issue is whether the incentives that are offered lead to truthful revelation. It turns out that apart from incentives, the degree of information provided about the potential lotteries (prizes) and the incentive structure play a key role in the truthful belief revelation. Strangely, too much information and details about the incentive mechanisms leads to stronger biases in reported beliefs.

Paradoxically, by reducing the provided incentive information to the minimum and informing subjects that truthful reporting maximizes the chance of winning, truthful reporting is maximized. Interestingly, the biases that occur with too much details on incentive mechanisms are strongest the farthest away from centered probabilities, which might be linked to likelihood insensitivity for mid-range probabilities as documented in behavioural economics.

The development of those elicitation techniques is an active field of research and very powerful to extract information. Even though those elicitation approaches seem to be adapted for at least some kind of risk audits, it seems that such potential approaches have not really been explored. Especially, the growing interest in cyber risk management seems a promising area for applications, given limited statistical data and its eventual stationarity issues.

Dr. Michel VERLAINE
ICN Business School
Michel.verlaine@icn-artem.com

References

Cvitanic, J., Prelec, D., Riley, B. and Terick, B. (2019) "Honesty via Choice-Matching", *AER Insights I(2): 179-192*.
Danz, D., Vesterlund, L. and Wilson, A. (2022) "Belief Elicitation and Behavioral Incentive Compatility", *American Economic Review 112(9)*: 2851-2883.
Hossain, T. and Okiu, Ryo (2013) "The Binarized Scoring Rule", *Review of Economic Studies* 80(3): 984-1001.
Offerman, T., Sonnemans, J., Van de Kuilen G. and Wakker, P. (2009) " A truth serum for non-Bayesians : correcting proper scoring rules for risk attitudes ", *Review of Economic Studies* 76, 1461-89.
Mackowiak, B., Matejka, F. and Wiederholt, M. (2022) "Rational Inattention: A Review", *Journal of Economic Literature forthcoming*.
Prelec, D. (1998) "The Probability Weighting Function." *Econometrica* 66: 497-527.
Schotter, A. and Trevino, I. (2014) "Belief Elicitation in the Laboratory", *Annual Review of Economics* 6 (1): 103-128.
Trautmann, S. and Van de Kuilen, G. (2015) "Belief Elicitation: A Horse Race Among Truth Serums", *Economic Journal 125* (589): 2116-35.
Wakker, P. (2010) Prospect Theory for Risk and Ambiguity, Cambridge University Press.