Annex B. Experts Knowledge Verification Results

This annexe presents the questionnaire used for expert knowledge verification and results calculated by the expert calibration tool Excalibur.

Table B.1. Seed questions for expert knowledge verification (Created by author)

No.	Questions	Value
1	Percentage of remote code execution attacks associated with crypto mining.	90%
2	Percentage of malware is delivered by email.	92%
3	Percentage of IT decision makers defined targeted phishing attacks as their top security threat.	56%
4	Percentage of fileless compromised attacks .	77%
5	Average ransomware attack costs for the company in millions.	5M
6	How long in average it takes for organizations to identify data breaches.	191 days
7	Percentage of companies see compliance mandates driving spending.	69%
8	Percentage of companies spent more than $1 million on preparing for the GDPR.	88%
9	Percentage of organizations have a standalone security department.	25%
10	Percentage of companies experienced an industrial control system security incident	54%
11	Percentage of organizations have experienced an IoT security incident	61%
12	The proportion of data breaches caused by external attackers	75%
13	The average cost of a data breach in 2017	3,6M
14	Percentage of enterprises that say they require up to 50% more budget for cybersecurity	87%
15	Percentage of organizations that would likely increase the resources available for cybersecurity following a breach that causes significant damage	76%
16	Total number of publicly disclosed data breaches in 2017	1579

End of the Table B.1

No.	Questions	Value
17	Percentage of attacks in 2017 were due to weak or stolen passwords, many of which could have been prevented by the use of multifactor authentication.	81
18	Percentage of businesses reported having an information security strategy in place.	56
19	Percentage of cyber attacks target small business	43
20	Percentage of cybersecurity breaches are due to human error	95%
21	Percentage of all files are not protected in any way.	21%
22	Amount of security areas covered by ISO 27001:2013 standard	14
23	Amount of high-level requirements defined by PCI DSS 3.2.1: 2018	12
24	Amount of Risk assessment process steps defined by the NIST Guide for Conducting Risk Assessment (800-30)	4
25	Provide the year when General Data Protection Regulation comes into the force?	2018

To acquire the expert assessment on the topic, a set of 7 experts, has been presented with the questions, provided in Annex B Table B.1. The assessment results of each expert are provided in Annex B Table B.2. In this table, experts are identified by providing an identification code, consisting of the letter E and the sequence number. The cell values are the expert assigned probabilities for the occurrence of the previously expressed phenomena.

Table B.2. Results of expert assessment of the seed (Created by author)

Question	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5	Expert 6	Expert 7
1	85	68	75	70	65	95	81
2	90	96	90	95	95	98	74
3	75	45	75	45	35	42	55
4	75	62	56	56	65	58	79
5	7.5	6	7.5	6.1	4.5	4.5	3.2

End of the Table B.2

Question	Expert 1	Expert 2	Expert 3	Expert 4	Expert 5	Expert 6	Expert 7
6	45	90	720	250	150	365	180
7	69	45	75	75	55	71	59
8	75	80	95	75	75	72	75
9	20	26	33	45	33	48	33
10	53	51	45	33	70	74	51
11	54	70	35	60	55	81	74
12	70	83	55	65	83	86	83
13	2.5	2.5	1	0.5	4.1	1.8	2.8
14	80	81	95	95	98	95	93
15	86	70	85	89	81	82	81
16	2200	1500	2000	2000	2500	1200	1000
17	81	75	57	40	79	91	89
18	78	45	45	25	65	65	67
19	30	65	67	65	61	61	50
20	91	70	80	85	75	87	94
21	19	54	35	45	45	41	40
22	14	14	14	14	14	14	14
23	12	12	12	12	12	12	12
24	4	4	4	4	4	4	4
25	2018	2016	2018	2018	2018	2018	2018