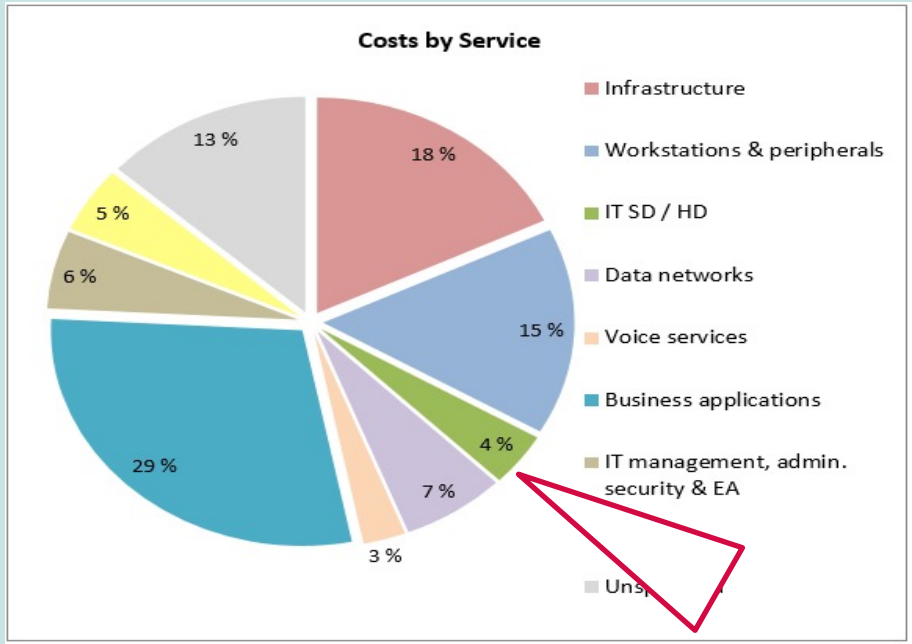
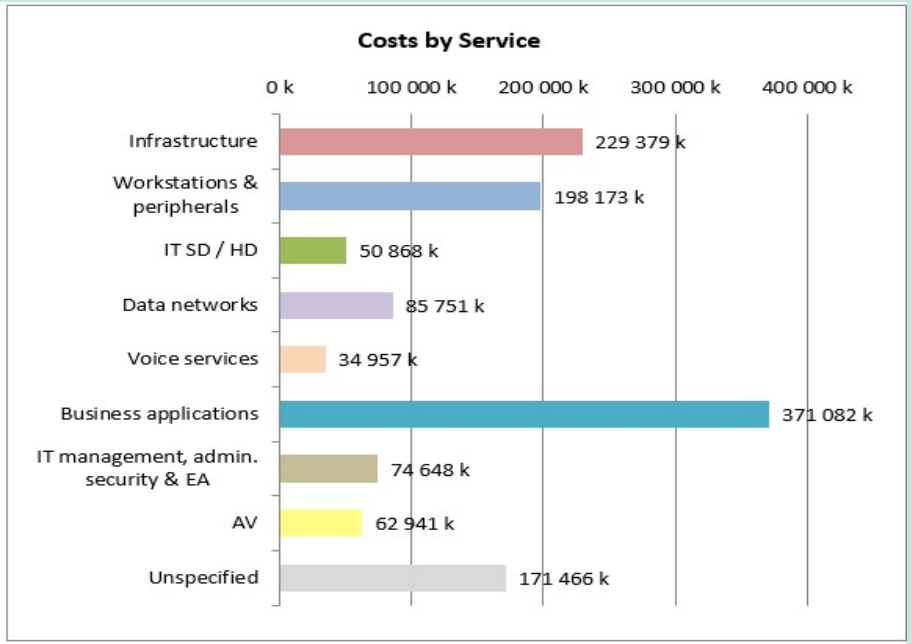
Using Bencheit for cybersecurity economics





CIO Kurt Gammelgaard Nielsen

Erhvervsakademi og Professionshøjskole

Economics of cybersecurity

- **Incentives and market failures**: HEI use 18% of their Business Application spending on Teaching, alas students and academic staff use a lot of ”free software”. Is ”free” secure? And who pays for security breach?
- **The power of incentives**: Who is buying a Business Application and who is responsible for IT-security
- **Asymmetric information**: Firms have insight in level of security and flaws in their products, HEI and students have not.
- **Externalities**. One HEI’s cybersecurity investment can affect other HEI. If uni X have unsecure services and user behavior, these can negative effect other HEI.

3 variables: security costs, security level and security benefits

- Cost of security appears to be the most straightforward variable to measure.
- Direct costs include purchasing, installing, and administering security measures. Think of acquiring products such as firewalls and antivirus software, but also of user training, awareness campaigns or staffing an incident response team.
- Indirect costs: implementing a strong password policy can affect system employee morale.
- Security level: User awereness, phished credentials
- Security benefits: possible research, funding req. and trust from community

Security as a function of the economic activity in the core business.

- HEI have fixed costs which are independent of the core business activity, for instance, acquiring new firewalls.
- HEI have variable costs; these grow proportionality to the activity, like the cost of distributing security tokens or number of students on LMS
- ISPs are not obliged to act on notifications that their customers are infected with malware

Gordon-Loeb Model*

- (1) Estimate the value/ the potential loss for each information set in the organization; eg the institutions mailsystem.
- (2) to estimate the probability that an information set will be breached based on the information set's vulnerability; (user lured by spearphishing)
- (3) to create a grid of all possible combinations of steps 1 and 2 above
- (4) to derive the level of cybersecurity investment by allocating funds to protect the information sets, subject to the constraint that the incremental benefits from additional investments exceed (or are at least equal to) the incremental costs of the investment.

*Gordon, L.A. and Loeb, M.P. (2002) The Economics of Information Security Investment. ACM Transactions on Information and System Security, 5, 438-457

1 Estimate value from cost of Buisness applications

Service	Sub Service	Organisation Level	Help texts	Grand total	Hardware (EURO)	Software (EURO)	Staff (EURO)	Facilities (EURO)	Outsourcing (EURO)	Other acc. group (EURO)	Staff FTE
				62.739.084	**16.901.341**	**8.190.124**	**18.448.350**	**1.530.042**	**8.191.682**	**9.477.544**	**277,6**
		Other centralised	planning, ERP, travel costs management etc.)	303.280		106.312			109.911	87.058	
		Distributed		15.625		817	13.875	933			0,2
		Unspecified org.level									
	Human resources		Human resources IT systems. (Payroll systems, skills & training related systems, e-recruiting etc.)	**605.552**	15.826	69.001	165.418	10.732	215.714	128.860	2,3
		IT Center		453.705	14		159.248	10.265	215.714	68.463	2,2
		Other centralised		145.210	15.812	69.001				60.397	
		Distributed		6.636			6.170	467			0,1
		Unspecified org.level									
	Facilities		Housing and facilities management systems (house & room rents, room reservation systems, house planning systems etc.)	**641.298**	8.197	436.756	131.380	9.332	9.434	46.199	2,0
		IT Center		363.658	3.703	206.937	131.380	9.332		12.306	2,0
		Other centralised		232.331	4.494	184.509			9.434	33.893	
		Distributed		45.309		45.309					
		Unspecified org.level									
	Communications		Communication systems such as e-mail, instant messaging, Wiki, groupware etc.	**1.795.346**	34.049	429.348	922.212	62.526	413.375	-66.164	13,4
		IT Center		1.468.235	34.049	234.718	860.515	57.860	412.109	-131.016	12,4
		Other centralised		233.869		194.321				39.547	
		Distributed		93.243		309	61.697	4.666	1.265	25.305	1,0
		Unspecified org.level									
	Student administration systems		Student administration systems / student record management systems (incl. also e.g. student application systems)	**2.971.157**		298.446	593.921	41.995	931.047	1.105.749	9,0
		IT Center		2.635.098		274.294	303.944	20.064	931.047	1.105.749	4,3
		Other centralised		190.060		24.152	154.243	11.665			2,5
		Distributed		145.999			135.734	10.265			2,2
		Unspecified org.level									
	Teaching		Systems related to teaching such as e-learning platforms, specially designed classrooms for distance learning etc.	**5.182.029**	54.050	1.522.629	1.256.438	89.589	1.032.849	1.226.474	19,2
		IT Center		3.389.022	52.363	644.097	732.013	49.927	975.428	935.194	10,7
		Other centralised		958.861	1.661	388.815	431.880	32.663	55.862	47.981	7,0

Erhvervsakademi og Professionshøjskole

2 Estimate propability of breach/ level of security

- In the Nordic region 11 of 70 HEI in 2020/1 was attacked by TA047 (Silent Libarian): 15 % risk

8	login.ezproxy.bib.hh.se.ezpro.xyz	19-02-2020	libguides.hh.se/	Halmstad University
13	login.ki.se.iftl.tk	27-10-2020	login.ki.se	Karolinska Institute
18	login.e.bibl.liu.se.ctit.tk	29-10-2020	liu.se	Linköping University
28	innsida.ntnu.snnu.me	31-10-2020	ntnu.no/ub	NTNU Norwegian University of Science and Technology
66	login.proxy3-bib.sdu.dk.ezlogin.info	02-03-2020	alvis-bib.sdu.dk	University of Southern Denmark

2021 IOC

87	ezproxy.vid.no.liblog.info	11-06-2021	vid.no	VID Specialized University
88	login1.ep.bib.mdh.se.liblog.inf	30-08-2021	mdh.se	Malardalen university
89	ezproxy2.hkr.se.liblog.info	02-09-2021	login.hkr.se	Kristanstad University
90	idp.it.su.se.mosc.me	15-09-2021	sub.su.se	Stockholm University
91	login.ki.se.ersta.me	16-10-2021	login.ki.se	Karolinske Institute

End-to-end mapping of a spear-phishing attack on Higher Education Institution in EU
https://doi.org/10.29007/53wk

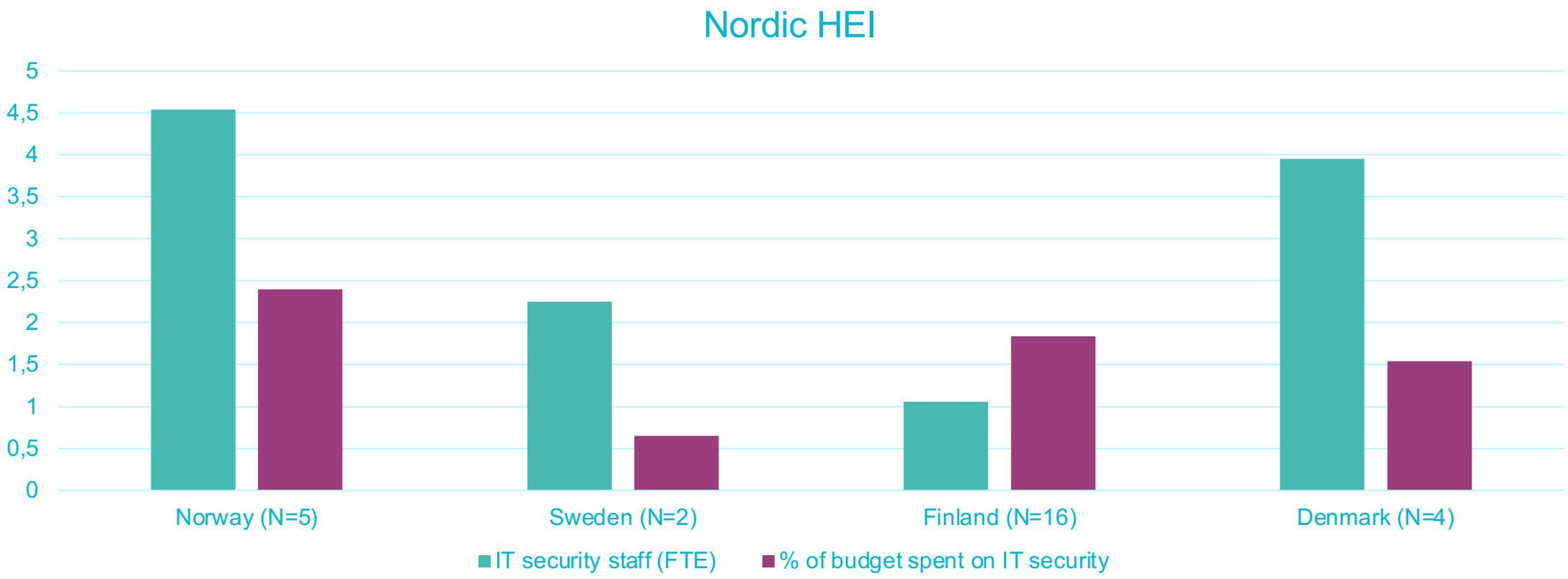
Create a grid for possible outcomes for 1 & 2

Value of information sets in mill. euro

High Medium Low	Low		Medium		High
	10	20	30	40	50
20%	2	4	6	8	10
40%	4	8	12	16	20
60%	6	12	18	24	30
80%	8	16	24	32	40

- GL rule that the optimum investment is less than 37% of the expected loss. If the potential loss for your HEI is 50 mill euro for your mailsystem is hacked, do not spend more then 40 mill. You will overspend on this item.

4 Derive the level of cybersecurity investment by allocating funds. Bencheit: Subservice IT security



Erhvervsakademi og Professionshøjskole

The security level

- Security level can have deterministic and stochastic indicators.
- Stochastic indicators are able to capture uncertainty produced by the attacker behavior, while deterministic don’t. For example, deterministic indicators include patch level, existence of intrusion detection systems, whether virus scanners are in place, etc.
- Stochastic indicators are the incidents reported by intrusion detection systems or phishinattack
- Within Benchheit we can find these numbers on security level

Do you have a ISO/IEC 27001 Information security management implemented (ISMS) in your organisation?		
Yes	14	38 %
No	23	62 %

Benefits of security.

- We can estimate the security benefits as the reduction of losses that would have been incurred in the absence of security. However, this reduction could be due to a change in the attacker's behavior rather than due to the deployed security measures.
- Will TA47change, many swedich HEI are attacked, but no Finish. Is this due to spending on IT security in finish HEI and security level?
- There is no correlation on this from Bencheit. Further investigation is needed
- Immediate financial impact of compromise mailsystem due to TA047 attack can be hard due to the random nature of losses and the same time raise some questions like "What are the right security measures to implement?"

UCL: 2020-2017

2020			Grand total	Hardware (DKK)	Software (DKK)	Staff (DKK)	Facilities (DKK)	Outsourcing (DKK)	Other acc. group (DKK)	Staff FTE
0		Grand tota	47.613.180	6.328.000	8.434.500	22.562.000	0	9.685.680	603.000	42,5
Service	Sub Servic	Organisati								
Infrastructure			**7.022.000**	**1.650.000**	**730.000**	**4.642.000**	**0**	**0**	**0**	**8,0**
	Workstations		**9.650.000**	3.372.000	5.728.000	550.000	0	0	0	1,0
IT Service Desk / Helpdesk (incl			**4.802.000**	**5.000**	**0**	**4.797.000**	**0**	**0**	**0**	**13,0**
Business applications			**16.546.180**	**0**	**504.500**	**7.057.000**	**0**	**8.984.680**	**0**	**12,0**
	Teaching		**6.733.500**	0	77.000	5.452.000	0	1.204.500	0	9,0
		IT Center	6.733.500		77.000	5.452.000		1.204.500		9,0
		Other cen	0							
		Distribute	0							
		Unspecifie	0							
IT management, administratio			**4.846.000**	**0**	**200.000**	**4.646.000**	**0**	**0**	**0**	**7,0**
	IT management etc.		**3.573.000**	0	0	3.573.000	0	0	0	5,0
		IT Center	3.573.000			3.573.000				5,0
		Other cen	0							
		Distribute	0							
		Unspecifie	0							
	IT Security		**1.273.000**	0	200.000	1.073.000	0	0	0	2,0
		IT Center	1.273.000		200.000	1.073.000				2,0
Incidents			8							
	Medium		6							
	High		2							
Comply wit IT security standar			In progress with ISO27001, in progres with complay with national IT-security standards, GDPR, check of all subcontracters							

2017			Grand total	Hardware (DKK)	Software (DKK)	Staff (DKK)	Facilities (DKK)	Outsourcing (DKK)	Other acc. group (DKK)	Staff FTE
0		Grand tota	28.251.059	8.230.000	1.995.500	13.647.559	0	4.428.000	0	23,5
Service	Sub Servic	Organisati								
Infrastructure			**15.361.500**	**6.630.000**	**1.695.500**	**3.158.000**	**0**	**3.878.000**	**0**	**6,0**
	Workstations		**2.400.000**	1.600.000	300.000	500.000	0	0	0	1,0
IT Service Desk / Helpdesk (incl			**3.950.000**	**0**	**0**	**3.950.000**	**0**	**0**	**0**	**7,0**
Business applications			**3.539.559**			**3.039.559**		**550.000**		**5,5**
	Teaching					2.500.000		550.000		4,5
		IT Center				2.500.000		550.000		4,5
		Other cen								
		Distribute								
		Unspecifie								
IT management, administratio			**3.000.000**	**0**	**0**	**3.000.000**	**0**	**0**	**0**	**4,0**
	IT management etc.					3.000.000				4,0
		IT Center								4,0
		Other cen								
		Distribute								
		Unspecifie								
	IT Security									
		IT Center								0,0
			13							
			2							
			8							
NO										

Erhvervsakademi og Professionshøjskole