The economics of defensive security

Prepared by:

Nick Dunn, Managing Security Consultant

Table of contents

1. Executive summary

Defensive security - balancing costs against risks & potential losses

This paper examines the costs of cyber defence in comparison to the costs and likelihood of a data breach. Varying breach costs and attack probabilities for different industry sectors are used to indicate the likely cost-effectiveness or overspend for different sectors and estate sizes in order to determine the cost or cost benefits of effective cyber defence.

The key highlights are:

1. The cost of a breach varies by sector and the number of breached records
2. The likelihood of a successful breach varies by sector
3. There is a cut-off point that varies across sectors where it is *theoretically* cheaper to ignore security for an entity with sufficiently low revenues and small numbers of records
4. The risks of not securing the IT estate in some sectors is so great that it cannot be ignored

The risks of not securing the IT estate in some sectors is so great that it cannot be ignored

2. Introduction

While there are many claims that cyber security is an indispensable necessary cost, there is also a body of opinion that cyber security does not always justify its costs and the costs of a breach are frequently either exaggerated or unclear. As a result, this whitepaper aims to compare breach costs to defence costs and examine the arguments in favour of, or against, an increased security spend to defend critical assets.

2.2 The role of risk acceptance

In some instances, there is no real choice of whether or not to implement cyber defences, as legislation or risk appetite demands a certain minimum level of precaution. For example, the healthcare, defence and financial industries are subjected to legislation or regulation to varying degrees in almost every country and the choice of not spending on cyber defences is not available.

In other cases, a breach has no monetary cost but may still have significant impacts, such as the effect on a nation's defences resulting from a compromise of military resources or the effects on individual patients resulting from the compromise of a healthcare provider.

The sectors discussed above have a much more limited choice with regards to defence implementation and are obliged to maintain some level of defence. We will focus on the costs of defence and breaches in purely commercial terms, mainly for organisations which have a greater freedom of choice as to how much or how little they spend on defences.

2.3 Limitations & disclaimers

There is, clearly, no reliable way to measure unreported or undetected breaches. The information relating to data breach occurrences has been gathered from public sources, usually from organisations operating in countries which have laws enforcing disclosure of data breaches. Consequently, the disclosure figures relate almost entirely to breaches or compromises where legal disclosure is compulsory - usually a loss or theft of personal data.

A small number of other breaches come to the public notice either because of services going offline for an extended period or because they are reported directly by a successful attacker wishing to cause embarrassment to the victim, to demonstrate their skills and achievements, or both. In these cases, data may be available from the news media and victim companies' annual reports.

Finally, it must be assumed that there are other types of breaches that go unreported, either due to a desire to avoid bad publicity and the associated loss of revenue that invariably accompanies adverse publicity, or because of other concerns such as the necessary privacy concerns of defence and government organisations. There is, of course, no way to obtain data for any unknown breaches.

3. The evolving threat landscape

Examination of data from Western Europe and North America shows a rise in the number of reported attacks reported each year and a rise in the number of data breaches. This would appear to be driven to some extent by a rise in the value of certain types of data and an increase in the attack surface of the typical organisation as larger numbers and a wider variety of resources are exposed to the internet.

For example, in the UK, the Office for National Statistics reported an increase in breaches per quarter throughout 2016 and the number of breaches in the first quarter of 2017 (678) was approximately 50% higher than in the first quarter of 2016 (448).

Over recent years the comparative values of different record types has varied, with studies in 2014 reporting medical records to be worth 10 to 20 times as much as financial records, while a 2017 study reported the opposite, giving financial accounts a much higher value than medical records.

A Reuters report in 2014 gives the following comparison [1]:

“Stolen health credentials can go for $10 each, about 10 or 20 times the value of a U.S. credit card number, according to Don Jackson, director of threat intelligence at PhishLabs”

While a McAfee study in 2017 gives the following values [2]:

- McAfee Labs finds stolen medical records available for sale from $0.03 to $2.42 per record.
- Comparable stolen financial account records available for $14.00 to $25.00.
- Credit and debit card account data available for $4.00 to $5.00 per account record.
- Most lucrative cybercrime targeting health care industry data is pharmaceutical, biotech intellectual property.
- Cyber crime-as-a-service economy is developing specifically around healthcare industry data.
- Concerted effort by cybercriminals to recruit health care industry insiders as accomplices.

There appears to be a recent, growing type of theft where attackers attempt to steal computing resources, principally processing power, in order to mine cryptocurrencies [3]. Interesting as this is, there is not a great deal of public data that can be used to add to our discussion at the time of writing. While a successful attack of this nature does not necessitate a breach disclosure (one of the reasons for a lack of data) and may not result in any direct loss or theft of data, it can result in indirect costs from incident response and in increased resource usage.

4. Data breaches by sector

When looking at the impact of data breaches, the industry sector plays a prominent part in the likelihood of attack. As discussed above, this is partly driven by the value of data emanating from different sectors and partly by variations in the attack surface for different sectors.

An additional factor is the sociological or political aspect, whereby a sector may be targeted because it is viewed negatively by hacktivist groups, such as the targeting of religious groups, political organisations, banking or governments by activists who oppose the current political position (or perceived political position) of their targets.

4.1 Gathering breach data

Information about worldwide data breaches is affected by differing legal requirements for disclosure around the world and so any figures should be viewed as a guideline rather than a fact. The trends for certain types of breach can be viewed as reasonably accurate for North America and Western Europe where laws exist enforcing disclosure for an unauthorised compromise of personal data.

Ponemon Institute provides an annual report showing the average number of data breaches and average costs of data breaches around the world, which has been used to provide numbers and costs in this report [4].

4.2 Data breaches in the UK

The UK was chosen for detailed investigation, as there is usable government data for the number of companies and organisations, along with their turnover, broken down into market sectors available from the UK Government and the Office for National Statistics. In addition, detailed information is available from the Information Commissioner's Office for the number of reportable breaches (chiefly those involving personal data), again broken down into market sector [5].

The UK also occupies a convenient median position in Ponemon Institute's data, being the middle-ranking country for ‘average number of records breached’ and for ‘average organisational cost of breach’ [6].

4.3 Factors affecting the accuracy of figures

It should be noted that the likelihood of an attack for government organisations can be viewed as more likely than illustrated by the officially disclosed data breach figures. Government assets in the UK and in other states are attacked on a regular basis by nation state actors and other groups whose attacks would not be listed. They are also not always disclosed either because of national security or because such organisations are not bound by the same rules obliging disclosure.

In addition, we are forced to some degree to assume that governments suffer breaches from nation state actors which remain undisclosed, either because they are not discovered or for national security reasons.

As a result of these considerations, some caution should be exercised when dealing with the costs and probabilities in the document. They should be viewed as a guideline rather than fixed rules.

4.4 UK businesses by sector

According to UK Government figures, there are 2,555,000 businesses in the UK registered for VAT and/or PAYE (UK taxation schemes applying to businesses above a certain turnover). [7]

These businesses can be broadly broken down as follows:

- Sole proprietors and partnerships: 27.4%
- Companies and public corporations: 68.8%
- The largest sector is professional, scientific and technical: 18%

These figures, as shown below, can be used in conjunction with breach data per sector in order to give a clearer picture of the likelihood of a breach for each sector.

Number of VAT and/or PAYE businesses by broad industrial grouping: UK, 2014 to 2016 [7]

Count (to nearest thousand)						
	2014	%	2015	%	2016	%
Agriculture, forestry & fishing	146	6.2	147	6.0	148	5.8
Production	140	5.9	142	5.8	146	5.7
Mining, quarrying & utilities	11	0.5	12	0.5	13	0.5
Manufacturing	129	5.5	130	5.3	133	5.2
Construction	274	11.6	284	11.6	302	11.8
Wholesale & retail; repair of motor vehicles	372	15.7	369	15.0	370	14.5
Motor trades	71	3.0	72	2.9	73	2.9
Wholesale	105	4.4	104	4.3	104	4.1
Retail	196	8.3	192	7.9	192	7.5
Transport & storage (inc. postal)	74	3.1	83	3.4	93	3.6
Accommodation & food services	145	6.2	146	6.0	148	5.8
Information & communication	181	7.6	193	7.9	207	8.1
Finance & insurance	45	1.9	49	2.0	52	2.1
Property	85	3.6	88	3.6	91	3.6
Professional, scientific & technical	409	17.3	436	17.8	459	18.0
Business administration & support services	181	7.7	194	7.9	208	8.2
Public administration & defence	7	0.3	7	0.3	7	0.3
Education	39	1.6	40	1.7	42	1.6
Health	99	4.2	106	4.3	113	4.4
Arts, entertainment, recreation & other services	164	6.9	166	6.8	168	6.6
TOTAL	2,361	100	2,449	100	2,555	100

4.5 UK data breaches – The numbers

The figures for UK data breaches in 2016 give a total of 2168 reportable breaches. It is notable that reportable data breaches, in the UK and worldwide, have continued to increase. In the UK, there was a rise in incidents per quarter throughout 2016 and Q1 of 2017 was 50% up on Q1 of 2016 [5]:

Q1 2016:	448
Q1 2017:	678

Over the same period, according to ID Theft Centre, data breaches were up 40% in the USA, with 1091 reported breaches in 2016 as compared to 780 in 2015 [8].

By combining the figures from the UK data breach regulatory authority and the UK tax authorities, we get the following table, showing data breaches per market sector compared to the number of organisations in each sector. Some totals have been left blank for situations where it is difficult to assess the exact number of organisations from UK tax department figures or other official figures, such as ‘religious’ or ‘other’.

It is important to note that we are looking at the number of successful attacks, not the total number of attempted attacks and so this can only act as a guideline to the probability of attack. This also explains the low figure in the financial sector. While it is accepted that cyber attacks take place against all major banking and financial organisations, these organisations are also well-defended, with a good security posture helping to reduce the number of successful attacks and to minimise the number of successful compromises.

Total breaches	**Central government**	**Charitable and voluntary**	**Education**	**Finance, insurance & credit**	**General business**	**Health**	**Justice**	**Land or property services**	**Legal**	**Local government**	**Marketing**	**Media**	**Membership association**	**Online technology and telecoms**	**Political**	**Regulators**	**Religious**	**Retail and manufacture**	**Social care**	**Transport and leisure**	**Utilities**	**Other**
Q1: 448	9	23	36	25	36	184	18	17	25	43	0	3	1	5	1	3	0	5	7	6	0	1
Q2: 545	12	29	34	34	53	232	22	10	14	62	0	3	4	4	2	4	2	6	8	4	2	4
Q3: 598	10	35	40	40	56	239	27	7	20	62	1	4	7	18	0	9	0	5	2	3	3	10
Q4: 577	12	33	56	37	52	221	39	5	11	49	0	0	7	13	0	6	1	8	4	2	2	19
Total: 2168	**43**	**120**	**166**	**136**	**199**	**876**	**106**	**39**	**70**	**216**	**1**	**10**	**19**	**40**	**3**	**22**	**3**	**24**	**22**	**15**	**7**	**34**
Total companies in sector	**426 [9]**	**167,109 [10]**	**42,000**	**52,000**	**280,000**	**113,000**		**91,000**		**353 [11]**	**25,000 [12]**	**168,000**		**207,000**	**16, 442 or 517 [13]**			**325,000**		**93,000**	**40 [14]**	

Defining the ‘political’ group

When determining probability of attack for a ‘political’ organisation the total number of targets is dependent upon which groups are included:

426 govt depts

75 'high profile groups'

16 political parties

Using the available figures for total number of data breaches and organisations, we can gauge a rough probability of a successful attack, at least for the more clearly defined sectors.

Notably the number of successful attacks in proportion to target organisations for government and local government are significantly higher than other sectors. The possible explanations for this are there being a greater number of attacks, weaker defences or some combination of the two.

Of the non-government breaches, the utilities sector had the largest proportion of successful compromises, with seven reportable breaches throughout 2016, in a sector with 40 organisations (17.5% likelihood of compromise).

5. Data breach costs

5.1 Measuring breach cost data

The costs of a data breach can be broken down into direct and indirect costs. The direct costs are both obvious and immediate. They include any fines resulting from the breach, lost revenue from any downtime during and after the breach and any additional staffing costs directly related to the breach, such as call-outs and overtime for incident response.

Direct costs can be summarised as follows:

1. Fines: Current maximum of £500,000, increasing to either 4% of your global annual turnover or €20 million following General Data Protection Regulation (GDPR) (whichever is greater)
2. Any theft of credit or resources
3. System downtime and associated revenue losses such as staff call-out costs for incident response

The indirect costs include the results of reputational damage, which can include an ongoing loss of revenue from both the loss of existing customers and a failure to attract new customers. Further indirect costs can result from the use of external consultancies and contractors for digital forensics, for hardening of systems and for other additional testing, redevelopment or reconfiguration of systems. The indirect costs are, by their nature, more difficult to quantify and are sometimes a matter of conjecture. Some of the indirect costs referred to in subsequent sections are implied via a reduction in profits, reduction in revenue or shrinking customer base, rather than being based on an outright statement by the breach victim(s).

Indirect costs can be summarised as follows:

1. Staff costs: Any extra payments, overtime, etc. involved in restoring systems from backups, associated testing, etc.
2. Reputational impact: Lost business, cancelled business and loss of both existing and potential customers.
3. Compensation: Something of a special case. This depends on legal obligations, the desire for good publicity and the nature of any existing contracts.
4. Reduction in company value: As an extreme example, Verizon was able to get a $350 million price cut when buying Yahoo after they had suffered a breach.

5.2 Available breach cost data

Studies carried out by Ponemon Institute and IBM Security are completed annually and have been chosen to give a guideline for breach costs in this study. The 2017 edition [4] covered 419 companies in 13 countries or regions. As the numbers are split by industry sector, they can be used in conjunction with the figures for UK industry data breaches and data on UK companies in different sectors.

In the past, measurements have also used a cost per customer or percentage of revenue as a rough calculation of potential breach costs. The 2015 Ponemon Institute [15] study gave $200 per customer as the typical cost of a data breach. Cisco calculates cost as typically around 20% of revenue for more than one third of breached companies [16].

In their 2016 study [6], Ponemon Institute identified seven global trends in the cost of data breaches:

“Over the many years studying the data breach experience of 2,013 organisations in every industry, the research has revealed the following seven megatrends.

1. Since first conducting this research, the cost of a data breach has not fluctuated significantly. This suggests that it is a permanent cost organisations need to be prepared to deal with and incorporate in their data protection strategies.

2. The biggest financial consequence to organisations that experienced a data breach is lost business. Following a data breach, organisations need to take steps to retain customers' trust to reduce the long-term financial impact.

3. Most data breaches continue to be caused by criminal and malicious attacks. These breaches also take the most time to detect and contain. As a result, they have the highest cost per record.

4. Organisations recognise that the longer it takes to detect and contain a data breach the more costly it becomes to resolve. Over the years, detection and escalation costs in our research have increased. This suggests investments are being made in technologies and in-house expertise to reduce the time to detect and contain.

5. Regulated industries, such as healthcare and financial services, have the most costly data breaches because of fines and the higher than average rate of lost business and customers.

6. Improvements in data governance programs will reduce the cost of data breach. Incident response plans, appointment of a Chief Information Security Officer (CISO,) employee training and awareness programs and a business continuity management strategy continue to result in cost savings.

7. Investments in certain data loss prevention controls and activities such as encryption and endpoint security solutions are important for preventing data breaches. This year's study revealed a reduction in the cost when companies participated in threat sharing and deployed data loss prevention technologies."

For our purposes the following headline from the report is of interest as this invites comparison with our other figures, covering the number of breaches per sector and likelihood of breaches per sector:

"The cost of data breach varies by industry. The average global cost of data breach per lost or stolen record was $158. However, healthcare organisations had an average cost of $355 and in education the average cost was $246. Transportation ($129), research ($112) and public sector ($80) had the lowest average cost per lost or stolen record."

5.3 UK breach costs

Using the Ponemon Institute [4] figures, it is possible to build a clearer picture of the costs of a breach in relation to the number of compromised records. The following table outlines average costs across all sectors and shows costs for the public sector, which, as discussed earlier, is generally subjected to tighter regulation and has limited freedom of choice regarding defence implementation (or at least the choice to not defend is largely absent).

The theoretical cost of impact as compared to the number of breached records is also worthy of note and shows the impact of increased estate size upon any potential losses. Using the average Ponemon Institute [4] figure for costs per breached record, a relatively small breach involving 2,000 compromised records would theoretically result in a cost of £240,000, whereas a large-scale breach involving 1 million compromised records would theoretically result in a cost of £120 million.

Number of records	**Average cost (all sectors) (£)**	**Public sector cost (£)**
1,000	120,000	60,000
2,000	240,000	120,000
4,000	480,000	240,000
6,000	720,000	360,000
8,000	960,000	480,000
10,000	1,200,000	600,000
12,000	1,440,000	720,000
14,000	1,680,000	840,000
16,000	1,920,000	960,000
18,000	2,160,000	1,080,000
20,000	2,400,000	1,200,000
30,000	3,600,000	1,800,000
40,000	4,800,000	2,400,000
50,000	6,000,000	3,000,000
60,000	7,200,000	3,600,000
80,000	9,600,000	4,800,000
100,000	12,000,000	6,000,000
150,000	18,000,000	9,000,000
200,000	24,000,000	12,000,000
500,000	60,000,000	30,000,000
1,000,000	120,000,000	60,000,000

5.4 An alternative view of breach costs

Using Cisco's model for breach costs as equal to 20% of revenue [16], in combination with the UK Office of National Statistics' figures for turnover of companies in 2016 [7] we have the following theoretical breach costs. Breach costs have been calculated as the midpoint of the range. For example in the £250,000 - £499,000 range, costs have been calculated with £375,000 to give a loss of £75,000.

Companies by turnover

Turnover size band (thousands £):	0-49	50-99	100-249	250-499	500-999	1,000-1,999	2,000-4,999	5,000-9,999	10,000-49,999	50,000+	Total
Number of companies	433,115	604,100	795,665	309,745	181,145	103,920	69,925	26,620	22,825	7,450	2,554,510
Projected average loss at 20% (thousands £)	5	15	35	75	150	300	700	1,500	6,000	10,000	

To put the costs in perspective and to give some comparison of the differences between costing methods, for a business with a £1,000,000 turnover (the midpoint column) there is a theoretical breach cost of £200,000 using the 20% guideline. For a breach involving 22,759 records (the average number for a data breach) multiplied by the Ponemon Institute's £125 per capita cost in the UK [4], we get a theoretical average loss of £2,844,875 (noting the wide variations between sectors).

5.5 UK breach costs by industry sector

Ponemon Institute's 2017 costs [4] for a breached record in each industry sector are shown below, using a conversion rate of $1 = £0.75. As discussed above, the public sector impact is roughly half the average financial impact across all sectors.

Interestingly, healthcare and education are the sectors with the highest losses, just ahead of the less surprising financial sector.

Sector	**Breach cost per record (£)**
Healthcare	267
Education	185
Financial	166
Service	156
Life science	147
Retail	129
Communications	123
Industrial	117
Energy	111
Technology	109
Hospitality	105
Consumer	100
Media	99
Transportation	97
Research	84
Public	60
Average	120

Using Ponemon Institute's costings for different industry sectors in the UK [4], it is possible to gain the following figures for breach costs in relation to sector and number of records. This can provide an interesting, if theoretical, guide to rising costs for numbers of breached records and varying costs across sectors. Both of these factors will come into play when we compare breach costs to defence costs.

Figures in the following table have been placed with sector multipliers in descending order of cost, from left to right. As discussed, Healthcare on the extreme left is the sector which incurs the greatest breach costs.

Number of records	**Healthcare (£)**	**Education (£)**	**Financial (£)**	**Service (£)**	**Life science (£)**	**Retail (£)**	**Communications (£)**	**Industrial (£)**	**Energy (£)**	**Technology (£)**	**Hospitality (£)**	**Consumer (£)**	**Media (£)**	**Transportation (£)**	**Research (£)**
1,000	267,000	185,000	166,000	156,000	147,000	129,000	123,000	117,000	111,000	109,000	105,000	100,000	9,9000	97,000	84,000
2,000	534,000	370,000	332,000	312,000	294,000	258,000	246,000	234,000	222,000	218,000	210,000	200,000	198,000	194,000	168,000
4,000	1,068,000	740,000	664,000	624,000	588,000	516,000	492,000	468,000	444,000	436,000	420,000	400,000	396,000	388,000	336,000
6,000	1,602,000	1,110,000	996,000	936,000	882,000	774,000	738,000	702,000	666,000	654,000	630,000	600,000	594,000	582,000	504,000
8,000	2,136,000	1,480,000	1,328,000	1,248,000	1,176,000	1,032,000	984,000	936,000	888,000	872,000	840,000	800,000	792,000	776,000	672,000
10,000	2,670,000	1,850,000	1,660,000	1,560,000	1,470,000	1,290,000	1,230,000	1,170,000	1,110,000	1,090,000	1,050,000	1,000,000	990,000	970,000	840,000
12,000	3,204,000	2,220,000	1,992,000	1,872,000	1,764,000	1,548,000	1,476,000	1,404,000	1,332,000	1,308,000	1,260,000	1,200,000	1,188,000	1,164,000	1,008,000
14,000	3,738,000	2,590,000	2,324,000	2,184,000	2,058,000	1,806,000	1,722,000	1,638,000	1,554,000	1,526,000	1,470,000	1,400,000	1,386,000	1,358,000	1,176,000
16,000	4,272,000	2,960,000	2,656,000	2,496,000	2,352,000	2,064,000	1,968,000	1,872,000	1,776,000	1,744,000	1,680,000	1,600,000	1,584,000	1,552,000	1,344,000
18,000	4,806,000	3,330,000	2,988,000	2,808,000	2,646,000	2,322,000	2,214,000	2,106,000	1,998,000	1,962,000	1,890,000	1,800,000	1,782,000	1,746,000	1,512,000
20,000	5,340,000	3,700,000	3,320,000	3,120,000	2,940,000	2,580,000	2,460,000	2,340,000	2,220,000	2,180,000	2,100,000	2,000,000	1,980,000	1,940,000	1,680,000
22,000	5,874,000	4,070,000	3,652,000	3,432,000	3,234,000	2,838,000	2,706,000	2,574,000	2,442,000	2,398,000	2,310,000	2,200,000	2,178,000	2,134,000	1,848,000
24,000	6,408,000	4,440,000	3,984,000	3,744,000	3,528,000	3,096,000	2,952,000	2,808,000	2,664,000	2,616,000	2,520,000	2,400,000	2,376,000	2,328,000	2,016,000
26,000	6,942,000	4,810,000	4,316,000	4,056,000	3,822,000	3,354,000	3,198,000	3,042,000	2,886,000	2,834,000	2,730,000	2,600,000	2,574,000	2,522,000	2,184,000
28,000	7,476,000	5,180,000	4,648,000	4,368,000	4,116,000	3,612,000	3,444,000	3,276,000	3,108,000	3,052,000	2,940,000	2,800,000	2,772,000	2,716,000	2,352,000
30,000	8,010,000	5,550,000	4,980,000	4,680,000	4,410,000	3,870,000	3,690,000	3,510,000	3,330,000	3,270,000	3,150,000	3,000,000	2,970,000	2,910,000	2,520,000
32,000	8,544,000	5,920,000	5,312,000	4,992,000	4,704,000	4,128,000	3,936,000	3,744,000	3,552,000	3,488,000	3,360,000	3,200,000	3,168,000	3,104,000	2,688,000
34,000	9,078,000	6,290,000	5,644,000	5,304,000	4,998,000	4,386,000	4,182,000	3,978,000	3,774,000	3,706,000	3,570,000	3,400,000	3,366,000	3,298,000	2,856,000
36,000	9,612,000	6,660,000	5,976,000	5,616,000	5,292,000	4,644,000	4,428,000	4,212,000	3,996,000	3,924,000	3,780,000	3,600,000	3,564,000	3,492,000	3,024,000
38,000	10,146,000	7,030,000	6,308,000	5,928,000	5,586,000	4,902,000	4,674,000	4,446,000	4,218,000	4,142,000	3,990,000	3,800,000	3,762,000	3,686,000	3,192,000

40,000	10,680,000	7,400,000	6,640,000	6,240,000	5,880,000	5,160,000	4,920,000	4,680,000	4,440,000	4,360,000	4,200,000	4,000,000	3,960,000	3,880,000	3,360,000
42,000	11,214,000	7,770,000	6,972,000	6,552,000	6,174,000	5,418,000	5,166,000	4,914,000	4,662,000	4,578,000	4,410,000	4,200,000	4,158,000	4,074,000	3,528,000
44,000	11,748,000	8,140,000	7,304,000	6,864,000	6,468,000	5,676,000	5,412,000	5,148,000	4,884,000	4,796,000	4,620,000	4,400,000	4,356,000	4,268,000	3,696,000
46,000	12,282,000	8,510,000	7,636,000	7,176,000	6,762,000	5,934,000	5,658,000	5,382,000	5,106,000	5,014,000	4,830,000	4,600,000	4,554,000	4,462,000	3,864,000
48,000	12,816,000	8,880,000	7,968,000	7,488,000	7,056,000	6,192,000	5,904,000	5,616,000	5,328,000	5,232,000	5,040,000	4,800,000	4,752,000	4,656,000	4,032,000
50,000	13,350,000	9,250,000	8,300,000	7,800,000	7,350,000	6,450,000	6,150,000	5,850,000	5,550,000	5,450,000	5,250,000	5,000,000	4,950,000	4,850,000	4,200,000
52,000	13,884,000	9,620,000	8,632,000	8,112,000	7,644,000	6,708,000	6396,000	6,084,000	5,772,000	5,668,000	5,460,000	5,200,000	5,148,000	5,044,000	4,368,000
54,000	14,418,000	9,990,000	8,964,000	8,424,000	7,938,000	6,966,000	6,642,000	6,318,000	5,994,000	5,886,000	5,670,000	5,400,000	5,346,000	5,238,000	4,536,000
56,000	14,952,000	10,360,000	9,296,000	8,736,000	8,232,000	7,224,000	6,888,000	6,552,000	6,216,000	6,104,000	5,880,000	5,600,000	5,544,000	5,432,000	4,704,000
58,000	15,486,000	10,730,000	9,628,000	9,048,000	8,526,000	7,482,000	7,134,000	6,786,000	6,438,000	6,322,000	6,090,000	5,800,000	5,742,000	5,626,000	4,872,000
60,000	16,020,000	11,100,000	9,960,000	9,360,000	8,820,000	7,740,000	7,380,000	7,020,000	6,660,000	6,540,000	6,300,000	6,000,000	5,940,000	5,820,000	5,040,000
62,000	16,554,000	11,470,000	10,292,000	9,672,000	9,114,000	7,998,000	7,626,000	7,254,000	6,882,000	6,758,000	6,510,000	6,200,000	6,138,000	6,014,000	5,208,000
64,000	17,088,000	11,840,000	10,624,000	9,984,000	9,408,000	8,256,000	7,872,000	7,488,000	7,104,000	6,976,000	6,720,000	6,400,000	6,336,000	6,208,000	5,376,000
66,000	17,622,000	12,210,000	10956,000	10,296,000	9,702,000	8,514,000	8,118,000	7,722,000	7,326,000	7,194,000	6,930,000	6,600,000	6,534,000	6,402,000	5,544,000
68,000	18,156,000	12,580,000	11,288,000	10,608,000	9,996,000	8,772,000	8,364,000	7,956,000	7,548,000	7,412,000	7,140,000	6,800,000	6,732,000	6,596,000	5,712,000
70,000	18,690,000	12,950,000	11,620,000	10,920,000	10,290,000	9,030,000	8,610,000	8,190,000	7,770,000	7,630,000	7,350,000	7,000,000	6,930,000	6,790,000	5,880,000
72,000	19,224,000	13,320,000	11,952,000	11,232,000	10,584,000	9,288,000	8,856,000	8,424,000	7,992,000	7,848,000	7,560,000	7,200,000	7,128,000	6,984,000	6,048,000
74,000	19,758,000	13,690,000	12,284,000	11,544,000	10,878,000	9,546,000	9,102,000	8,658,000	8,214,000	8,066,000	7,770,000	7,400,000	7,326,000	7,178,000	6,216,000
76,000	20,292,000	14,060,000	12,616,000	11,,856,000	11,172,000	9,804,000	9,348,000	8,892,000	8,436,000	8,284,000	7,980,000	7,600,000	7,524,000	7,372,000	6,384,000
78,000	20,826,000	14,430,000	12,948,000	12,168,000	11,466,000	10,062,000	9,594,000	9,126,000	8,658,000	8,502,000	8,190,000	7,800,000	7,722,000	7,566,000	6,552,000
80,000	21,360,000	14,800,000	13,280,000	12,480,000	11,760,000	10,320,000	9,840,000	9,360,000	8,880,000	8,720,000	8,400,000	8,000,000	7,920,000	7,760,000	6,720,000
100,000	26,700,000	18,500,000	16,600,000	15,600,000	14,700,000	12,900,000	12,300,000	11,700,000	11,100,000	10,900,000	10,500,000	10,000,000	9,900,000	9,700,000	8,400,000

6. Prevention & defence costs

Prevention of an attack cannot be guaranteed but is clearly much more likely when effective defences are in place. Effective defences, of course, require an investment of both time and money. For our purposes the expression ‘monetary costs’ can be freely exchanged with the expression ‘resources’, and includes extra staffing, security software and, where necessary, additional devices such as firewalls and servers, as explained below.

The defence costs can be primarily viewed under two broad categories; operational costs and development costs. In this context, operational costs encompasses the following:

1. Asset tracking, whereby an organisation must list both the data assets to be protected and the software which interacts with the data and must consequently be patched or updated.
2. The costs of various security-related hardware and software such as firewalls, anti-virus, etc.
3. The costs of any additional staffing to handle the increased workload of updating software, operating security-related software, responding to incidents, etc.

Development costs would only apply to an organisation developing its own software and would vary considerably, depending on the number and size of applications being developed and maintained. As the cost of secure development also takes us into the arena of whether applications are being used by external entities and clients, thus exposing them to attacks too, it will be disregarded here. This is partly in order to avoid unnecessary complexity and partly because it cannot be applied universally across the potential victims in the same manner as the operational costs.

6.1 Initial operational setup costs

Initial setup costs cover software licences and the resources needed to implement operational systems and procedures. This includes people-hours spent installing and setting up any new defensive hardware and software such as firewalls and people-hours spent on configuration. Configuration activities would include ensuring a secure build for all operating systems used by the organisation and ensuring that patch-management systems are in place to keep software updated.

6.2 Annual operational costs

Maintaining secure IT operations incurs an annual cost, mainly from software support licences and additional people-hours. The man-hours spent on software support includes patching of normal business systems and the patching and maintenance of defence systems. Additional people-hours are needed for incident response and daily monitoring activities such as reviewing application logs.

One way to project staff costs is to look at the tasks needed in order to maintain the operational security systems and to budget for any additional staff as necessary.

6.3 The SANS security costing model

A paper from SANS institute, Budgeting Critical Security Controls [17], provides a cost model for implementing operational security, assuming the use of standard Microsoft functionality inherent with the existing Microsoft Active Directory environment. It provides two cost ranges; one for small to medium IT estates and another for medium to large IT estates, as shown below.

Technology solution budget ranges

Solution	Low range	High range
Asset inventory database	$30,000	$150,000
Device scanners	$50,000	$300,000
Network access control	$500,000	$1,200,000
Logging/alerting/analytics	$300,000	$700,000
Total	$880,000	$2,350,000

Using a conversion rate of 0.75 US Dollars to 1 GBP we get a low range figure of £660,000 and a high range figure of £1,762,500.

6.4 Annual costs

In addition to the SANS implementation costs discussed above, some annual costs have been included to take account of the costs of staffing and consultancy. These are based on the following guidelines or assumptions:

Estimated UK IT staff costings (average figures using job postings)

Penetration tester:	£50,000 to £75,000 pa each
Systems administrator:	£40,000 to £60,000 pa each
Security analyst:	£40,000 pa each

Estimated staff time

Monitor IPS/logs:	1 person-day/month/system
Backing up:	1 person-day/month/system
Patching:	1 person-day/month
Configuration:	5 person-day/month/system
Testing disaster recovery plan (DRP):	10 man-days - quarterly or annually (depending on size of estate and risk appetite)

Estimated annual staff costs in relation to number of records

Number of records	System administrator costs (£)	Security analyst costs (£)
<10,000	40,000	N/A
10,000-76,000	40,000	40,000
76,000-1,000,000	80,000	40,000

Estimated external consultancy time

Annual penetration testing estimated costs for small, medium and large infrastructure are broken down roughly as follows. These have been incorporated into annual costs in the following section using £1,000 per day as a typical guideline cost for penetration testing and assuming five to ten days for a small organisation, and a larger numbers of days for larger organisations. Clearly this is a guideline only as the costs of a penetration test would vary according not only to the number of assets, but also the complexity, types and variety of systems.

Small	£5,000 to £10,000
Medium	£20,000 to £40,000
Large	£50,000 to £100,000*

*This is a figure for a single upfront larger test (or group of tests) of anything from 15 days upwards (reaching high numbers for large multinationals), followed by smaller subsequent annual tests of 5 to 15 days. For very large organisations this figure could vary further dependent on the amount of specialist software that has been written internally, size of IT estate, etc.

7. Defence costs compared to breach costs

The above discussion about the monetary costs of security gives cause for consideration of the value obtained from a cyber security implementation. At what point, if any, does a security programme fail to justify its costs? Utilising the Ponemon Institute figures [4] for breach costs and the defence cost figures discussed in the preceding section it becomes possible to compare defence costs to breach costs in order to provide a quantitative justification for implementing cyber defences.

The defence costs are chiefly influenced by the size of the IT estate; mainly the presence of internet-facing hosts, and the size of any internal estate. It has been assumed that an increase in the number of records held by an organisation will be accompanied by a corresponding increase in the size of the organisation's IT estate. This assumption underpins the estimated defence costs which increase broadly in line with the number of records.

As can be seen from the table below, each industry has a tipping point where the number of records that could be affected increases the theoretical costs of a breach to the point where it becomes cheaper to put preventative measures in place, rather than suffer a breach. This does, of course assume that the measures which are implemented will be effective and that the number of past breaches can be used as a predictor of the likelihood of future attacks.

7.1 Other considerations

Although each individual case is different, the figures could be viewed as a justification for reduced security spending in some sectors where an entity has a small number of records and low theoretical cost per record. If tempted by this idea, it's important to bear in mind that these figures show past numbers of breaches which means they are not necessarily a guide to future breaches and that they only show successful attacks, not the total number of attacks.

In addition, it may be tempting to view the small number of reportable breaches in the marketing and media sectors as validating a lower spend on cyber defence. It is important to bear in mind that there is a possibility of high indirect costs in these sectors, particularly if exceptionally litigious clients have been affected.

As we can see below, there is a cut-off point where the average theoretical cost of a single breach exceeds the cost of the first year's defence implementation, occurring between 5,000 and 6,000 records. Any organisation possessing 6,000 records or more could be viewed as taking a risk of monetary losses if inadequate defences are implemented.

Number of records	Initial defence costs	Annual defence staffing costs	Annual consultancy costs	Total 1st year cost	Average breach cost
1,000	656,040	40,000	1,000	697,040	120,000
2,000	656,040	40,000	1,000	697,040	240,000
4,000	656,040	40,000	1,000	697,040	480,000
5,000	656,040	40,000	1,000	697,040	600,000
6,000	656,040	40,000	1,000	697,040	720,000
8,000	656,040	40,000	1,000	697,040	960,000
10,000	656,040	40,000	5,000	701,040	1,200,000
12,000	656,040	40,000	5,000	701,040	1,440,000
14,000	656,040	40,000	5,000	701,040	1,680,000
16,000	656,040	40,000	5,000	701,040	1,920,000
18,000	656,040	40,000	5,000	701,040	2,160,000
20,000	656,040	40,000	5,000	701,040	2,400,000
22,000	656,040	40,000	5,000	701,040	2,640,000
30,000	656,040	40,000	5,000	701,040	3,600,000
40,000	656,040	80,000	5,000	741,040	4,800,000
50,000	1,751,925	80,000	10,000	1,841,925	6,000,000
60,000	1,751,925	80,000	10,000	1,841,925	7,200,000
70,000	1,751,925	80,000	10,000	1,841,925	8,400,000
80,000	1,751,925	120,000	10,000	1,881,925	9,600,000
100,000	1,751,925	120,000	10,000	1,881,925	12,000,000
150,000	1,751,925	120,000	10,000	1,881,925	18,000,000
200,000	1,751,925	160,000	10,000	1,921,925	24,000,000
500,000	1,751,925	160,000	15,000	1,926,925	60,000,000
1,000,000	1,751,925	160,000	15,000	1,926,925	120,000,000

7.2 Summary

In summary, it can be seen that the theoretical cost of a breach varies by sector and by the size of an entities’ IT estate, regardless of whether we view estate size as proportional to turnover or proportional to number of records. This means that a cut-off point exists that varies across sectors where it is *theoretically* cheaper to ignore security for an entity with a small number of records or small annual turnover.

8. Theory vs reality

“In theory there’s no difference between theory and practice, but in practice there is” – Yogi Berra

Although the previous discussions have used average or theoretical costings and theoretical likelihoods of attack, it is helpful to discuss a real case where the facts are known and where we can investigate the theoretical costs in comparison to the actual, known costs. In this respect, the notorious TalkTalk breach that took place in 2015 serves as a useful example as many of the direct and indirect losses involved have been disclosed. The breach took place in October 2015 and took the form of a SQL injection attack which resulted in a compromise of 157,000 records [18].

8.1 Breach costs

Using Ponemon Institute’s per capita multiplier for communications companies of £123 and the official TalkTalk figure of 157,000 records we get a projected theoretical cost of £19,311,000. When comparing this to the costs taken from TalkTalk’s annual report [19], we get an actual cost of £60,000,000 [20].

The firm was fined £400,000, which was a record at the time, although the upcoming introduction of heavier fines under General Data Protection Regulation (GDPR) could have seen a much larger financial impact were the same incident to take place at some point in the post-GDPR future.

In addition, further indirect costs can be implied from a loss of 100,000 customers [21] over the following year and a drop in share prices [22].

8.2 Defence costs

Unlike the breach costs, the size of the TalkTalk IT infrastructure is more a matter of speculation and we cannot discuss defence costs with the same degree of accuracy as the breach costs. However, for a telecommunications company with 3.97 million customers at the time of the attack it is safe to assume a very large IT estate.

We can also assume, at the very least, an initial set up cost equal to the high end of the SANS estimate of £1,751,925. For such a large estate, it is probably safe to assume one additional security manager in the region of £120,000 pa, plus ten additional security-based system administrators at a total of £400,000 pa and ten security analysts at a total of £400,000 pa.

An additional security consultancy programme of 50 days to cover infrastructure and application assessments would cost a further £50,000 per year.

This gives a total of £2,721,925 for operational security costs. While it ignores any costs associated with secure software development and penetration testing of the web site, it is significantly less than the actual losses suffered, which emphasises the danger of relying on a theoretical cost and the potential pitfalls of providing inadequate resources for defence.

9. Conclusion

As we have seen, the risks of not implementing defences vary across sectors and greatly increase for larger numbers of records. While a theoretical cut-off point appears to exist where it may appear to be cheaper to not implement defences, this should be treated with caution. Comparisons of theoretical costs to actual costs indicate that this theoretical cut-off point may exist for a far smaller total number of records than indicated by the figures in this report. An attempt to gamble with the likelihood and cost in this way may have far more serious consequences than expected.

The disparities in this single example earlier in the document, between theoretical costs and direct costs showed costs for this real-life example to be three times the theoretical cost. This emphasises that all figures for projected costs and losses in this document should be treated with caution and not used as a definitive set of rules.

As stated elsewhere, the regulatory environment in sectors such as healthcare means that implementing defences is not optional and the only genuine consideration is how to effectively defend resources.

10. References

[1] https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924

[2] https://www.mcafee.com/uk/about/news/2016/q4/20161026-01.aspx

[3] https://bitcoinmagazine.com/articles/cryptomining-malware-fuels-most-remote-code-execution-attacks-study/

[4] https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&

[5] https://ico.org.uk/action-weve-taken/data-security-incident-trends/

[6] https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN

[7] https://www.ons.gov.uk/businessindustryandtrade/business/activitysizeandlocation/bulletins/ukbusinessactivitysizeandlocation/2016

[8] http://www.idtheftcenter.org/2016databreaches.html

[9] https://www.gov.uk/government/organisations

[10] https://www.gov.uk/government/publications/charity-register-statistics/recent-charity-register-statistics-charity-commission

[11] http://www.lgiu.org.uk/local-government-facts-and-figures/

[12] http://www.marketingquotes.co.uk/marketing-pr-agency/uk-marketing-companies/

[13] https://www.gov.uk/government/organisations
https://en.wikipedia.org/wiki/List_of_political_parties_in_the_United_Kingdom

[14] https://switch.which.co.uk/energy-suppliers/suppliers-atoz.html

[15] https://www-03.ibm.com/press/us/en/pressrelease/47022.wss

[16] https://www.cbronline.com/news/cybersecurity/breaches/cost-of-a-data-breach-soars-20-revenue-hacking-goes-classic-corporate/

[17] https://www.sans.org/reading-room/whitepapers/critical/budgeting-critical-security-controls-36652

[18] https://www.theguardian.com/business/2015/nov/06/nearly-157000-had-data-breached-in-talktalk-cyber-attack

[19] https://www.talktalkgroup.com/articles/talktalkgroup/2016/Annual-Report-2016

[20] https://www.theregister.co.uk/2016/02/02/talktalk_hack_cost_60m_lost_100k_customers/

[21] https://www.theguardian.com/business/2016/feb/02/talktalk-cyberattack-costs-customers-leave

[22] http://www.cityam.com/228714/talktalk-share-price-plunges-twice-as-deep-as-sony-carphone-warehouse-barclays-and-ebay-after-cyber-attacks

About NCC Group

NCC Group is a global expert in cyber security and risk mitigation, working with businesses to protect their brand, value and reputation against the ever-evolving threat landscape.

With our knowledge, experience and global footprint, we are best placed to help businesses identify, assess, mitigate & respond to the risks they face.

We are passionate about making the Internet safer and revolutionising the way in which organisations think about cyber security.

Headquartered in Manchester, UK, with over 35 offices across the world, NCC Group employs more than 2,000 people and is a trusted advisor to 15,000 clients worldwide.