An NCC Group Publication

The Economics of Defensive Security 2020 Update

Prepared by:
Nick Dunn

Contents

Introduction	3
The role of risk acceptance	3
Limitations and disclaimers	4
The threat landscape and the data breach lifecycle	4
Value of stolen records	6
The breach lifecycle	6
Estimated cybercrime activity levels	8
Data breaches by sector	8
Gathering breach data	8
Data breaches in the UK	9
Breach cost data	9
Factors affecting breach costs	10
UK breach costs	10
UK breach costs by industry sector	10
An alternative view of breach costs	12
Potential fines under GDPR	13
Impact on share prices	13
Prevention and detection costs	14
Initial operational set-up costs	14
Annual operational costs	14
The SANS security costing model	15
Annual costs	15
Defence costs compared to breach costs	16
Other considerations	17
Conclusions	18
Statistics and statistical bias	18
Self-Selection bias	18
Reliability and validity	19
Theory vs. reality	20
Breach costs	20
Defence costs	20
GDPR	21
GDPR fines so far	21
Conclusions	21
Overall conclusion	21
References	22

Introduction

Since NCC Group's previous whitepaper on the economics of defensive security [1], there have been changes to the laws that can affect the cost of a data breach, in the form of potential fines under the General Data Protection Regulation (GDPR). In addition, more data on organisations' defence costs has become available, particularly in terms of cyber-defence spending by UK companies. In light of the significantly increased costs for data breaches and the more granular data on breaches and cyber-defence costs across different sectors, we have re-evaluated and updated our previous research by way of this whitepaper.

The principal changes are a drop in the annual number of data breaches and a drop in the average cost per record for a data breach. At the same time, there has been an increase in average breach costs for the healthcare and financial sectors as well as significant cost increases for any organisation which is found guilty of failing to comply with the requirements of data protection legislation in the context of the breach. As with the original whitepaper, the aim is to compare breach costs to defence costs and examine the arguments in favour of, or against, an increased security spend to defend critical assets.

The role of risk and acceptance

In some instances, there is no real choice of whether or not to implement cyber defences, as legislation or risk appetite drives a certain minimum level of defensive measures. 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 can have significant impacts, beside the monetary cost, 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.

Limitations and 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 that 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.

The threat landscape and the data breach lifecycle

Examination of data from Western Europe and North America had previously shown a rise in the number of attacks reported each year and a rise in the number of data breaches. However, the UK showed a decrease in reported attacks and breaches through 2018 and 2019, following the increases of the previous years.

Trends that have stayed the same since the previous report are the higher proportion of breaches for larger companies, compared to smaller organisations, and for specific sectors such as healthcare and finance. This would fit with the previous conclusion that the value of the data held by the finance and healthcare sectors is higher and that the attack surface is greater for a large organisation due to a greater number and a wider variety of resources exposed to the internet.

Singular catastrophic attacks, with considerable amounts of lost revenue, disclosure of personal data and disruption to systems and services, have continued to occur periodically. These large-scale breaches can be viewed as outliers in a number of ways, as they not only occur infrequently with much higher total costs, but also have a higher average cost per record that falls outside the regular average costs for smaller breaches[2].

The reasons for the drop in UK data breaches in the previous two years is not completely clear and there are a number of possible contributing factors. Firstly, the UK government and National Cyber Security Centre (NCSC) have made efforts to educate companies about the dangers of cyber attacks and to provide useful, practical information. While it's not possible to measure how many companies are influenced by the NCSC's campaigns or follow its recommendations, it does at the time of writing have ~74,000 Twitter followers, indicating some level of online influence.

In addition, UK government cyber security surveys from 2017 to 2019 indicated a slight increase in the number of businesses classing cyber security as a high priority and a significant increase in the number of charities classing cyber security as a high priority. Report extracts illustrating this change from 2017 to 2019 are shown below:

2017 - “In this context, three-quarters (74%) of UK businesses say that cyber security is a high priority for their senior management, with three in ten (31%) saying it is a very high priority. The proportion noting it as a very low priority is lower than in 2016 (down from 13% to just 7%) – a change mainly seen among the micro and small business population” [3]

2018 - “Three-quarters of businesses (74%) and over half of all charities (53%) say that cyber security is a high priority for their organisation’s senior management” [4]

2019 - “Around three-quarters of businesses (78%) and charities (75%) say that cyber security is a high priority for their organisation’s senior management. Four in ten businesses (40%) and around a third of charities (35%) say it is a very high priority” [2]

Interestingly, the total amounts spent on defence, for all companies within a sector, over the period of 2017 to 2019 have dropped for telecoms and communications firms, but increased for other sectors, most notably the financial sector. The high telecoms spending over that period may have been influenced by the TalkTalk breach that immediately preceded the point when gathering of that data began.

The 2019 spend on cybersecurity, compared to 2018, is up across all sectors combined, with the most significant increase (as a percentage of total spending) being for large businesses. Security spend alone may be viewed as a slightly misleading measurement and studies have measured cyber protection using a combined measure of security maturity and security spending [5].

Value of stolen records

In the previous report it was stated that studies in 2014 reported 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 [6]:

“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”

A McAfee study in 2017 gave the following values [7]:

- 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

The breach lifecycle

The concept of the breach lifecycle has become more widely used since the previous report. This concept describes the timeline from the point of a breach taking place, to its discovery, through to its containment and the post-breach clean-up.

The 2019 Ponemon report makes the following observation:

“The time between when a data breach incident occurred and when the breach was finally contained (also known as the breach lifecycle) grew noticeably between 2018 and 2019. The average time to identify a breach in 2019 was 206 days and the average time to contain a breach was 73 days, for a total of 279 days. This represents a 4.9 percent increase over the 2018 breach lifecycle of 266 days. However, the faster a data breach can be identified and contained, the lower the costs. Breaches with a lifecycle less than 200 days were on average $1.22 million less costly than breaches with a lifecycle of more than 200 days ($3.34 million vs. $4.56 million respectively), a difference of 37 percent.”

While this definition and its data may seem a little abstract, it is important to bear in mind that effective monitoring and incident response should assist in identifying and containing breaches more quickly, allowing a victim to directly affect and influence their own personal breach lifecycle, following an incident. Shortening the lifecycle of the breach has the result of reducing the theoretical cost and, hopefully, the practical cost. [9]

The Data Breach Lifecycle

Estimated cyber crime activity levels

Although there are limited estimates for the total number of attacks, a McAfee report [7] gives some figures for the total amount of cyber crime. These estimates are, in some cases, extrapolations based on detected or reported cyber crime. In other cases, such as malicious scans, they are the amounts of activity detected by a single organisation, or the amounts of activity within a single geographic area, which give a possible indication for the rest of the world. In the absence of any comprehensive listing, the table below, extracted from the McAfee report, will serve as a rough estimate for daily total attack likelihood.

Cybercrime Activity Type	Estimated Daily Activity
Malicious Scans	80,000,000,000
New Malware	300.000
Phishing	33,000
Ransomware	4,000
Records lost to hacking	780,000

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 previously, 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.

Gathering breach data

Information about worldwide data breaches is influenced by differing legal requirements for breach 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.

The Ponemon Institute provides an annual report [9] showing the average number of data breaches and average costs of data breaches around the world, which has been used to provide some of the numbers and costs in this report. Further cost data has been taken from the Department for Digital, Culture, Media and Sport Cyber Security Breaches Survey [4]. This is carried out each year and has data gathered from 1,566 companies within the UK.

For case studies of larger breaches, publicly available data has been used from the UK government and annual company reports.

Data breaches in the UK

As in the previous report, the UK was chosen for detailed investigation, as there is usable government data for the total 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.

Additionally, for the last 3 years, the UK government has produced an annual survey comparing security spend across sectors, number of cyber attacks and cost of dealing with a cyber attack.

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'.

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 – At its highest there is a possible fine of 4% of your global annual turnover or €20 million under the General Data Protection Regulation (GDPR), whichever is greater. See the discussion below on when this does and doesn't apply.

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 to their original state, fixing bugs or implementing additional security measures, associated testing, etc.

2. Reputational impact - Lost business, cancelled business and loss of both existing and potential customers.

3. Compensation - Companies can decide to pay compensation to people impacted by any breach and that would be dependent on their desire for good publicity or the nature of any existing contracts. In addition, the law says that any individual who have suffered material or non-material damage in a breach can claim compensation.

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.

Factors affecting breach costs

According to the Ponemon Institute report, the costs of a breach are related to the country in which the breach took place, the size of the affected organisation and the industry sector of the affected organisation.

In their 2019 study, the Ponemon Institute identified several global trends in the cost of data breaches:

“The average total cost of a data breach in the U.S. for the companies studied has grown from $3.54 million in 2006 to $8.19 million in 2019, a 130 percent increase over 14 years.

The average total cost of a data breach in the healthcare industry was $6.45 million, or 65 percent higher than the average total cost of a data breach.

Smaller organizations had higher costs relative to their size than larger organisations. The total cost for organisations with more than 25,000 employees averaged $204 per employee.

Organisations with between 500 and 1,000 employees had an average cost of $3,533 per employee.”

UK breach costs

Using the Ponemon Institute figures, it is possible to build a clearer picture of the costs of a breach in relation to the number of compromised records. The table below 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 figure for costs per breached record, a relatively small breach involving 2,000 compromised records would theoretically result in a cost of £232,000, whereas a large-scale breach involving 1 million compromised records would theoretically result in a cost of £116 million.

UK breach costs by industry sector

Ponemon Institute’s 2019 costs 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, the healthcare sector, as in previous reports, has the highest losses, and costs have increased more significantly than other sectors over the past few years.

While the average cost to an organisation per record has decreased, the average cost to an organisation for a single breach has increased.

Sector	Breach cost per record (£)
Healthcare	322
Financial	158
Technology	138
Service	134
Energy	124
Industrial	120
Education	107
Communications	99
Consumer	98
Transportation	98
Media	93
Hospitality	92
Retail	89
Research	88
Public	59
Average	**116**

This can be translated to an increasing scale of cost, dependent on the number of records and industry sector, as shown below:

Number of Records	Typical UK Breach Cost	HealthCare	Financial	Technology	Service	Energy	Industrial	Education	Communications	Public
1000	116000	322000	158000	138000	134000	124000	120000	107000	99000	59000
2000	232000	644000	316000	276000	268000	248000	240000	214000	198000	118000
4000	464000	1288000	632000	552000	536000	496000	480000	428000	396000	236000
5000	580000	1610000	790000	690000	670000	620000	600000	535000	495000	295000
8000	928000	2576000	1264000	1104000	1072000	992000	960000	856000	792000	472000
10000	1160000	3220000	1580000	1380000	1340000	1240000	1200000	1070000	990000	590000
12000	1392000	3864000	1896000	1656000	1608000	1488000	1440000	1284000	1188000	708000
14000	1624000	4508000	2212000	1932000	1876000	1736000	1680000	1498000	1386000	826000
16000	1856000	5152000	2528000	2208000	2144000	1984000	1920000	1712000	1584000	944000
18000	2088000	5796000	2844000	2484000	2412000	2232000	2160000	1926000	1782000	1062000
20000	2320000	6440000	3160000	2760000	2680000	2480000	2400000	2140000	1980000	1180000
22000	2552000	7084000	3476000	3036000	2948000	2728000	2640000	2354000	2178000	1298000
24000	2784000	7728000	3792000	3312000	3216000	2976000	2880000	2568000	2376000	1416000
26000	3016000	8372000	4108000	3588000	3484000	3224000	3120000	2782000	2574000	1534000
28000	3248000	9016000	4424000	3864000	3752000	3472000	3360000	2996000	2772000	1652000
30000	3480000	9660000	4740000	4140000	4020000	3720000	3600000	3210000	2970000	1770000
32000	3712000	10304000	5056000	4416000	4288000	3968000	3840000	3424000	3168000	1888000
34000	3944000	10948000	5372000	4692000	4556000	4216000	4080000	3638000	3366000	2006000
36000	4176000	11592000	5688000	4968000	4824000	4464000	4320000	3852000	3564000	2124000
38000	4408000	12236000	6004000	5244000	5092000	4712000	4560000	4066000	3762000	2242000
40000	4640000	12880000	6320000	5520000	5360000	4960000	4800000	4280000	3960000	2360000
42000	4872000	13524000	6636000	5796000	5628000	5208000	5040000	4494000	4158000	2478000
44000	5104000	14168000	6952000	6072000	5896000	5456000	5280000	4708000	4356000	2596000

Number of Records	Typical UK Breach Cost	HealthCare	Financial	Technology	Service	Energy	Industrial	Education	Communications	Public
46000	5336000	14812000	7268000	6348000	6164000	5704000	5520000	4922000	4554000	2714000
48000	5568000	15456000	7584000	6624000	6432000	5952000	5760000	5136000	4752000	2832000
50000	5800000	16100000	7900000	6900000	6700000	6200000	6000000	5350000	4950000	2950000
52000	6032000	16744000	8216000	7176000	6968000	6448000	6240000	5564000	5148000	3068000
54000	6264000	17388000	8532000	7452000	7236000	6696000	6480000	5778000	5346000	3186000
56000	6496000	18032000	8848000	7728000	7504000	6944000	6720000	5992000	5544000	3304000
58000	6728000	18676000	9164000	8004000	7772000	7192000	6960000	6206000	5742000	3422000
60000	6960000	19320000	9480000	8280000	8040000	7440000	7200000	6420000	5940000	3540000
62000	7192000	19964000	9796000	8556000	8308000	7688000	7440000	6634000	6138000	3658000
64000	7424000	20608000	10112000	8832000	8576000	7936000	7680000	6848000	6336000	3776000
66000	7656000	21252000	10428000	9108000	8844000	8184000	7920000	7062000	6534000	3894000
68000	7888000	21896000	10744000	9384000	9112000	8432000	8160000	7276000	6732000	4012000
70000	8120000	22540000	11060000	9660000	9380000	8680000	8400000	7490000	6930000	4130000
72000	8352000	23184000	11376000	9936000	9648000	8928000	8640000	7704000	7128000	4248000
74000	8584000	23828000	11692000	10212000	9916000	9176000	8880000	7918000	7326000	4366000
76000	8816000	24472000	12008000	10488000	10184000	9424000	9120000	8132000	7524000	4484000
78000	9048000	25116000	12324000	10764000	10452000	9672000	9360000	8346000	7722000	4602000
80000	9280000	25760000	12640000	11040000	10720000	9920000	9600000	8560000	7920000	4720000
100000	11600000	32200000	15800000	13800000	13400000	12400000	12000000	10700000	9900000	5900000
150000	17400000	48300000	23700000	20700000	20100000	18600000	18000000	16050000	14850000	8850000
200000	23200000	64400000	31600000	27600000	26800000	24800000	24000000	21400000	19800000	11800000
500000	58000000	161000000	79000000	69000000	67000000	62000000	60000000	53500000	49500000	29500000
1000000	116000000	322000000	158000000	138000000	134000000	124000000	120000000	107000000	99000000	59000000

An alternative view of breach costs

In 2017, Cisco gave a model for breach costs as equal to 20% of revenue [10]. Using a combination of this and the UK Office of National Statistics' figures for turnover of companies in 2019 [11] 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 (£££££'s)	0-49	50-99	100-249	250-499	500-999	1000-1999	2000-4999	5000-9999	10000-49999	50000+	**Total**
Number of new companies	247180	473350	641415	236155	152595	93510	67680	26285	23980	7610	1969760
Projected average loss at 20% (£££££'s)	5	15	35	75	150	300	700	1500	6000	10000	

To put the theoretical costs in perspective and to give some comparison of the differences between costing methods, The Ponemon Institute gives the average cost of a UK data breach as £2.91 million. Using the Cisco model for a business with a £1,000,000 turnover (the midpoint column) there is a theoretical breach cost of £300,000, using the 20% of revenue guideline. For a breach involving 25,575 records (the average number for a data breach according to the Ponemon study) multiplied by the Ponemon Institute's £2.91 per capita cost in the UK, we get a theoretical average loss of £74,423.25 (noting the wide variations between sectors).

A more recent Cisco publication gives a wide variance in breach costs, stating that "29% of midmarket companies say breaches cost them less than $100K. 20% say it costs $1,000,000-$2,499,999". We will compare theoretical costs with some examples of actual costs in a later section, but the important thing to note here is that theoretical costs can vary considerably, depending on the model used. As discussed in the second Cisco whitepaper mentioned above, the use of mean averages may be the cause of some of the distortion if breach costs are heavily dependent on company size or turnover.

Potential fines under GDPR

Since the introduction of the General Data Protection Regulation (GDPR), data protection regulators across the European Union are now able to impose significant fines on organisations following a cyber attack. Under GDPR the supervisory authorities have the power to issue monetary penalties for infringements of the law. There are two tiers of administrative fines, the lower being the greater of €10 million, or 2% of annual global turnover and the higher is the €20 million, or 4% of annual global turnover. GDPR provides guidance for regulators on the factors to take into consideration – mitigating and aggravating - when deciding on the amount to be fined. Some mitigating factors that could reasonably be expected to be taken into account would include the fact that an organisation was well prepared but fell victim to a sophisticated attacker or had an unknown vulnerability in a third party's software.

The reality is that the largest fines, even before GDPR came in, have been applied in situations where the company that suffered the breach demonstrably failed to apply good practice, such as using old unpatched third-party software. One of the most common failings cited by regulators is the lack of 'appropriate technical and organiational measures', a good catch all for poor security.

The most significant item to take into consideration here is that while our previous study showed the same resulting breach costs following a compromise, regardless of the investment in security by the victim organisation, the new costs show a significant difference. A breached organisation that cannot demonstrate that a reasonable level of care was taken in securing the records can suffer a significant additional fine, while an organisation that demonstrates that efforts were made to secure the data may escape the GDPR fine and only suffer any other ancillary costs.

Impact on share prices

A drop in share prices is a commonly stated result of a data breach. Available data does indicate an immediate short-term drop, but no impact in the longer term. A report by CompariTech on the effects of a data breach on share prices indicated a drop for the 14 days following a data breach, but a return to previous prices, or higher, in the following six months:

"Stock prices suffer following a breach, but perhaps not as much as one might assume. After 14 market days, or roughly three weeks, share prices drop -2.8% on average. After the first month, however, share prices recover, and the companies we examined actually performed better in the six months following a breach (+7.4%) than the six months prior (+4.1%)." [19]

Prevention and detection costs

Prevention of an attack cannot be guaranteed but effective defences can limit an attacker's chances of success and reduce the potential for damage in the event of a successful compromise. 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 attack to too, it will be disregarded here. This is partly in order to avoid unnecessary complexity, partly because it cannot be applied universally across the potential victims in the same manner as the operational costs.

Initial operational set-up 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.

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 tasks, and to budget for any additional staff as necessary.

The SANS security costing model

The SANS paper, Budgeting Critical Security Controls [13], 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 for small to medium IT estates and medium to large IT estates as shown below.

This has been reused in the absence of any further studies in the intervening period since the previous report.

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
Public Key Infrastructure*	$0	$0
Dynamic Host Configuration Protocol*	$0	$0
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.

Annual costs

The SANS paper proposes annual costs for the above solutions, as follows:

“Assuming a 21% annual maintenance fee will result in range of $184,800 to $493,500 in annual software support costs.”

In addition to the SANS implementation and annual costs discussed above, some further annual costs can be added 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 payscale.com and glassdoor.co.uk) [13]

Penetration Tester: £25000 to £65000 pa each
Systems Administrator: £20000 to £53000 pa each
Security Analyst: £20000 to £54000 pa each

Estimated staff time
Monitor IPS/logs: 1 man-day/month/system
Backing up: 1 man-day/month/system
Patching: 1 man-day/month
Configuration: 5 man-day/month/system

Testing DRP:
10 man-days - Quarterly or Annual (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 (£)
<10000	40000	N/A
10000-76000	40000	40000
76000-1000000	80000	40000

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 £1000 per day as a guideline.

Note that this is an estimate for infrastructure only. As discussed above, any software and web applications would require additional testing and maintenance.

Small	£5000 to £10000
Medium	£20000 to £40000
Large	£50000 to £100000*

*Upfront larger test, subsequent annual tests

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 figures 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.

In the initial study, the 2016 figures showed that each industry had a tipping point where the number of records that could be affected increased the theoretical costs of a breach to the point where it became more cost effective to put preventative measures in place, rather than suffer a breach. This, of course, assumed that the measures implemented would be effective and that the number of past breaches could be used as a predictor of the likelihood of future attacks.

This approach can no longer be viewed as realistic, following the introduction of GDPR and its requirement to apply "appropriate technical and organisational measures". An absence of policies, procedures, basic patching and updates or failing to follow policies that are in place, effectively becomes a gamble with a breach potentially costing an additional amount of €20 million or 4% of turnover (whichever is highest). [15]

In the previous report we took a view of defence costs vs breach costs which showed a cut-off point where the average theoretical cost of a single breach exceeded the cost of the first year's defence implementation, occurred between 5,000 and 6,000 records. Any organisation possessing 6,000 records or more could have been viewed as taking a risk of monetary losses if inadequate defences are implemented. A shortened version of the table from the previous report is shown below:

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
20,000	656,040	40,000	5,000	701,040	2,400,000
50,000	1,751,925	80,000	10,000	1,841,925	6,000,000
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

The GDPR penalty for failing to take proper measures and precautions has made this view more risky and no longer viable as an option for anyone with more than a minor risk of compromise. The higher a company's income and the more numerous its assets and records, the greater the potential consequences, with the breach cost in the table above being drastically overshadowed by the GDPR fine in any situation where inadequate security is in place.

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 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.

Finally, as discussed earlier, any failure to apply appropriate controls can result in a significant fine under GDPR. This introduces significant risk to the 'do nothing' option and some degree of risk when attempting to implement a bare minimum level of security.

Conclusions

In the previous report, data showed that the theoretical cost of a breach varies by sector and by the size of an entity's IT estate, regardless of whether we view estate size as proportional to turnover or proportional to number of records. This meant that previously a cut-off point existed that varied across sectors where it was theoretically cheaper to ignore security for an entity with a small number of records or small annual turnover. The potential cost of a fine under GDPR means that this cut off point no longer exists and that risks are drastically increased for any organisation that feels it may be at risk of a cyber attack but fails to implement at least some level of defence.

As stated elsewhere, the regulatory environment in sectors such as healthcare means that implementing defences is not optional and the question is what measures should be put in place and how?

Statistics and statistical bias

As for any study, different types of bias may be present in any data that has been used, and this bias may have been intentional or unintentional on the part of the entities gathering the data. This can result from the data gathering methods, the questions used, selection of targets and other factors, examined below.

Self-selection bias

Self-selection bias describes a situation where, in the words of Wikipedia, individuals select themselves into a group, causing a biased sample with nonprobability sampling. For the data we are looking at it is important to consider that a number of security surveys have been used. For these surveys, companies that are willing to take part are possibly those that have suffered frequent attacks or those that have already prioritised security. This can distort figures, giving biased values for the percentage of companies that have suffered breaches, the amounts spent on security, and percentage of companies prioritising security.

For the UK government survey, the sample size of 1,566 businesses may seem large, but it is less than 0.1% of the total 2,718,430 businesses in the UK at the time of the survey and may not be representative of UK business as a whole, due to the possibility of self-selection bias. It seems likely that the companies most likely to respond to a security survey are those who prioritise security or those that have suffered a security incident.

The percentage of companies reporting a breach varies according to the source of data that is used, giving further weight to any possibility of self-selection bias. The UK government and Ponemon surveys show 32% and 29.6% of companies suffering a breach, respectively. The UK Information Commissioner's Office gives a total of 2,386 compromises over 12 months, from a total number of tax-paying UK businesses of 2,718,430, giving a total of less than 0.1%. Although this ignores a number of cyber attack types, such as ransomware, recreational hacking and others, it is noticeably smaller than the percentages given in the voluntary surveys, which seems to lend credibility to the possibility of self-selection bias.

Reliability and validity

As mentioned in the introduction, there is no available detailed data for unsuccessful cyber attacks, undetected cyber attacks or cyber attacks which do not cause a data breach, although there are some estimates and conjectured figures. The seemingly odd statistic that the two sectors spending the most on cybersecurity suffer the highest and third-highest number of compromises are presumably a result of this lack of data, which leaves us with no way of calculating with any certainty the number of thwarted attacks in comparison to security spending.

The UK government survey offers some help as it reports both breaches and reported attacks, although it is down to organisations surveyed to volunteer this information:

"Around a third (32%) of businesses and two in ten charities (22%) report having cyber security breaches or attacks in the last 12 months. As in previous years, this is much higher specifically among medium-sized businesses (60%), large businesses (61%) and high-income charities (52%)."

This may seem helpful in showing the higher number of attacks (regardless of success or failure) against those sectors with a high defence spend, but there is no indication of how many attacks were successful or unsuccessful, or the even more useful data around detection and containment.

Again, we should treat these figures with some degree of caution. Although the sample size of 1,566 businesses may seem large, it is less than 0.1% of the total 2,718,430 businesses in the UK at the time of the survey and may not be representative of UK business as a whole.

Additionally, record breaches cannot be viewed as making up the entirety of all cyber attacks. A number of other types exist for which evidence cannot be reliably gathered for various reasons. In some cases attacks are just not reported, either because they do not succeed or because there is no readily identifiable benefit to the victim, in other cases they are prosecuted, but are not always readily identifiable from court records.

The offences are not always prosecuted under The Computer Misuse Act or Data Protection Act as prosecutors sometimes think the jury could have difficulty with the more technical laws.

Sometimes prosecutors have used Misconduct in a Public Office to prosecute a police officer who's performed a search for prosecutions against someone they have met in a non-work situation, and there have been instances of using The Theft Act to prosecute someone who has deployed ransomware (the act makes it an offence to withhold someone's property and demand money).

Theoretically it may be possible to find every prosecution that resulted from a cyber attack, but this would be a manual, or mostly manual, search to identify any use of computing in prosecutions for the offences below:

- Computer Misuse Act
- Police and Justice Act 2006
- Data Protection Act 1998
- Malicious Communications Act 1988
- Communications Act 2003
- European Convention of Human Rights
- Telecommunications Act 1984
- Misconduct in a Public Office
- The Theft Act
- GDPR

This process would, however, require a degree of manual oversight and of course would only offer a guide to attacks that have reached the prosecution stage.

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 real cases where the facts are known and where we can investigate the theoretical costs in comparison to the actual, known costs. In this respect, the infamous NHS WannaCry breach that took place in 2017 serves as a useful example as many of the direct and indirect losses involved have been disclosed. The breach took place in 2017 and took the form of a ransomware attack against unpatched Windows systems, whose support expired.

Breach costs

Using the Ponemon cost per record for the healthcare sector of £322 and the official NHS figure of 507,784 patients per year (in the absence of a figure for the exact number of records), we get a projected theoretical cost of £163,506,448 which is, thankfully, many times the actual costs discussed below. The Ponemon average £4.84 million per healthcare breach is, conversely, a fraction of the officially reported final cost to the NHS.

The NHS official cost estimates from a subsequent report indicated a total £92 million cost for the outage [16]. According to that report, this cost was estimated in order to avoid the burden (both work and cost) of attempting to work out the exact figure upon individual NHS trusts. Of the estimated £92 million, £72 million was the cost of restoring systems and data in the aftermath of the attack, £19.5 was the ‘cost’ of dealing with the attack itself and the lost time and appointments to the NHS.

Defence costs

Using an NHS report on planned, but not yet implemented, defence costs that could have prevented or mitigated the NHS breach it’s possible to get a comparison of defence costs vs breach costs. An initial report [17] stated that the financial impact was unknown, but gave details of money to be invested in cyber security after the attack (page 11). This indicated that an originally planned £50 million for cyber security had had an additional £21 million ‘reprioritised’, giving a £71 million cost for hardening the systems to guard against future compromises.

It’s unclear from the report whether the additional £21 million that was reprioritised was intended to cover the move from Windows XP to a more recent version of Windows, and it’s also a matter of speculation as to how effective these defences would have been against this particular attack. Assuming that these defences would have been effective, we have a cost of £92 million for the breach against a cost of £71 million for the defence.

GDPR - Appropriate technical and organisational measures

As discussed earlier, GDPR can result in a fine for a compromised organisation that has failed to apply "appropriate technical and organisational measures". No clear definition is given for what these measures might be, although we can assume that they would vary on a case-by-case basis.

GDPR - Fines so far

To add some perspective around the likelihood of a GDPR fine for a data breach (not all of which resulted directly from a cyber attack), figures from the European Data Protection Board give some clarity. According to the European Data Protection Board, 281,088 cases were logged by supervisory authorities in the first year of the GDPR's application. Of these cases, 144,376 related to complaints and 89,271 related to data breach notifications by data controllers.

By September 2019, the EU's supervisory authorities had issued, or announced their intention to issue, fines totalling approximately €372,120,990.50. (That figure is approximate owing to fluctuations in currency values.) [15]

Conclusions

Clearly, there is some disparity between theoretical costs and direct costs. The fact that costs for this real-life example are an order of magnitude less than or greater than the various theoretical costs, 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.

Additionally the costs for GDPR breaches, due to not implementing sufficient controls in the ICO's view, also resulted in significant increase to the breach cost. These may be viewed as special cases but do help to illustrate the level of risk to an organisation that might be seen to have not implemented what the ICO views as suitable controls.

Only when monetary penalties are finalised and announced with the description of the failings that led to them will we be able to factor in the cost of GDPR breaches with some degree of accuracy.

Overall conclusion

While there have only been small changes in the likelihood of a successful breach across sectors since our previous study, there have been greater changes in the risks and penalties for failing to implement cyber defences or failing to harden systems. The GDPR penalty associated with a failure to implement reasonable precautions or to keep systems updated means that the penalty for doing nothing at all is significantly increased, despite other costs around compromise and recovery outside the healthcare sector remaining very similar.

Shortening the breach lifecycle through the proactive measure of implementing systems for earlier detection and containment of a breach also offers advantages and there are indications that money spent on intrusion detection and proactive disaster recovery precautions can repay themselves.

References

[1] The Economics of Defensive Security
https://www.nccgroup.trust/uk/our-research/the-economics-of-defensive-security/?research=Whitepapers

[2] Department for Culture, Media & Sport – Cyber Security Breaches Survey 2019
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf

[3] Department for Culture, Media & Sport – Cyber Security Breaches Survey 2017
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf

[4] Department for Culture, Media & Sport – Cyber Security Breaches Survey 2018
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf

[5] Hit or Myth? Understanding the True Costs and Impact of Cybersecurity Programs
https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/hit-or-myth-understanding-the-true-costs-and-impact-of-cybersecurity-programs

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

[7] McAfee – Economic Impact of Cybercrime
https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf

[8] The Breach Lifecycle
https://blog.sensecy.com/2017/02/28/the-life-cycle-of-a-data-breach/

[9] Ponemon Report 2019
https://www.ibm.com/security/data-breach

[10] CBR – Cost of Data Breach Rises to 20%
https://www.cbronline.com/breaches/cost-of-a-data-breach-soars-20-revenue-hacking-goes-classic-corporate/

[11] UK Businesses by Turnover and Sector
https://www.ons.gov.uk/businessindustryandtrade/business/activitysizeandlocation/bulletins/ukbusinessactivitysizeandlocation/2019

[12] Cisco – Cybersecurity Special Report
https://www.cisco.com/c/dam/en/us/products/collateral/security/small-mighty-threat.pdf

References continued

[13] SANS – Budgeting Critical Security Controls
https://www.sans.org/reading-room/whitepapers/critical/budgeting-critical-security-controls-36652

[14] Security Staff Salaries
https://www.payscale.com/research/UK/Job=Penetration_Tester/Salary
https://www.glassdoor.co.uk/Salaries/systems-administrator-salary-SRCH_KO0,21.htm
https://www.payscale.com/research/UK/Job=Systems_Administrator/Salary
https://www.payscale.com/research/UK/Job=Cyber_Security_Analyst/Salary

[15] GDPR Penalties
https://www.itgovernance.co.uk/dpa-and-gdpr-penalties

[16] NHS WannaCry Breach
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747464/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf
https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/
https://tech.newstatesman.com/security/cost-wannacry-ransomware-attack-nhs

[17] UK Government NHS WannaCry Report
https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/787/787.pdf

Images

Front page: Shutterstock: Maksbart

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 15,000 clients worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate and respond to the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

For more information from NCC Group, please contact:

+44 (0) 161 209 5200 response@nccgroup.com www.nccgroup.com