VALUING CYBER RISK

Estimating the long-term cost of data breaches to brands and businesses today.

Infosys®
Navigate your next

Interbrand

Introduction

The world we live in

Cybersecurity has been a hot topic of discussion, especially in the current times that we live in. Indeed, what was once an arcane subject that only the most seasoned of IT professionals would understand, has now spilled over into the lexicon of laypeople as well. Terms like

Vishing, Phishing, Data Security and Privacy Policy

are becoming an increasingly common part of our daily conversations.

Much of this reflects the world that we live in. As we transform into a data-rich, but time-poor society, we are increasingly relying on technology to ease some of the pressure on our time. Why, for instance, take the trouble of walking down a street to hail a cab when Alexa or Siri can do your bidding just as easily? The way we interact with the outside world has fundamentally changed. It is no longer a purely “real” world that we interact with, it is a mix of physical and digital experiences. And new tech like AI and AR are only blurring those lines more.

For brands, these shifts imply the need to re-evaluate even ‘hygiene’ aspects of their experience, like cybersecurity.

Brand value (and why it matters)

Over the years, intangible assets (of which brands form a significant proportion) have become increasingly important to business success and valuation. In fact, as of July 2019, tangible assets accounted for just 29.5% of the value of the average US company! This is far lower than 15 years ago, where about 33% of the value was represented by tangible assets[2].

Clearly, brand value positively impacts enterprise value and along with it, shareholder value.

The most important assets of any business are intangible. These assets, which comprise brand equity, are a primary source of competitive advantage and future earnings, contends David Aaker, the global authority on branding.1

Brands create real economic value for their owners by creating value in the minds of the consumers.

They're able to do this in three ways –

First, by ensuring recognition. Indeed, identity is the most fundamental utility of a brand. In a large supermarket for example, a consumer is more likely to choose a brand that they are more familiar with. In business terms, this translates into topline sales growth.

Second, brands engender trust in the minds of the consumers. Trust and credibility are important for a business to be able to charge a premium. Nike, for example, is a brand that has 'running' in its history and its very origins. It's no wonder then, that their median prices are, on an average, 15% higher than comparable brands of running shoes[3].

Finally, a strong brand creates emotional connections with customers. That translates into loyalty which, in business terms, means a lower risk to future earnings. Apple's success as a brand, for example, reflects its ability to create a strong engagement among its customers with its ecosystem of apps.

The Annual revenue of Apple stands unmatched at

274.5$b

(July 2019-June 2020)[4],

ranking it first among its top 10 competitors;
the average revenue of its top 10 competitors is

57.6$b

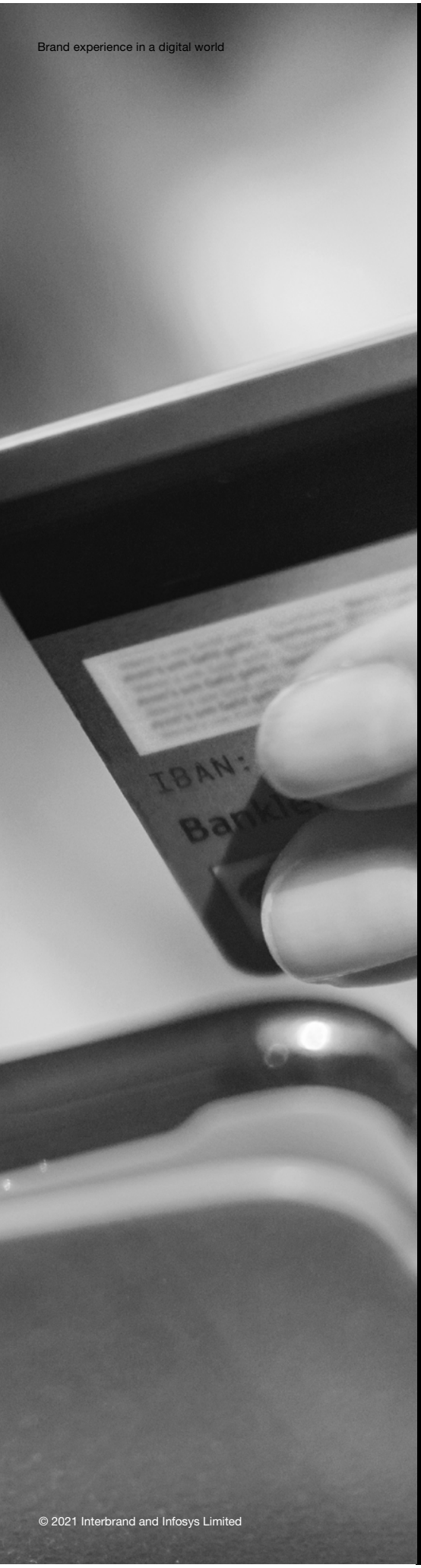
Our view of brands is that they are economic assets whose value represents the lifetime (branded) earnings of the business. Any fundamental change to the way consumers interact with brands therefore, impacts this value; a key aspect that other measures like market capitalization (that are primarily sales-focused) do not fully evaluate.

(A full explanation of Interbrand's ISO-certified valuation methodology can be seen in the appendix)

Brand experience in a digital world

In a time-poor world where attention spans are getting progressively shorter, brands rely on creating unique experiences to attract and retain customers. In fact, a unique brand experience is one of the reasons why customers are willing to pay a premium for the brand and stay loyal to it. It's why a customer may choose a $4-cappuccino at Starbucks instead of a perfectly good $2-coffee at the neighborhood coffee shop

As a large part of our day (and indeed, our life) moves online, brands are responding by relying more and more on digital technologies to deliver a unique experience to their customers.



This has two implications:
First, on the part of the customer, it implies a quid pro quo – sharing personal information with the brand for a personalized experience in return. Much of the experience that brands strive to deliver relies on massive amounts of data that their customers willingly or unwillingly share with them. And as brands chase the next level of personalization, the depth and width of this data only increases – not just name, age and demographic details but even details of the websites they frequent, their children's favorite restaurant, their partner's favorite cafe, and more. Since customers willingly share these details with brands, they also implicitly trust that the brand will not misuse that data.

Second, on the part of the brands, it means that the real and the virtual have to coexist in creating this unique experience. As a large part of our day (and indeed, our life) moves online, brands are responding by relying more and more on digital technologies to deliver a unique experience to their customers. This is true not just for purely "digital" brands like Google or Amazon, but also for brands who hitherto always relied on the "real" to deliver their experience. Hotel chains, for example, are beginning to meld the digital with the real to deliver a unique and personalized experience to their guests.

The COVID pandemic has only hastened this process. With 'contactless' becoming the norm in the post-pandemic world, the 'high touch' are rapidly morphing into 'high tech' to deliver the experience. Not surprisingly, the amount of data shared over the internet will only explode – and along with it, the vulnerabilities too.

It is estimated that the amount of data shared online at the beginning of 2020 was a staggering

44 Zettabytes

(1 Zettabyte is a trillion Gigabytes).

Of this

Google, Amazon, Facebook and Microsoft alone handled

1,200 Petabytes of data

(1 Petabyte = 1 million Gigabytes).

By 2025 in fact, the amount of data expected to be generated and shared daily is

463 Exabytes5

(an Exabyte is equal to a billion Gigabytes)

Security – no more just hygiene

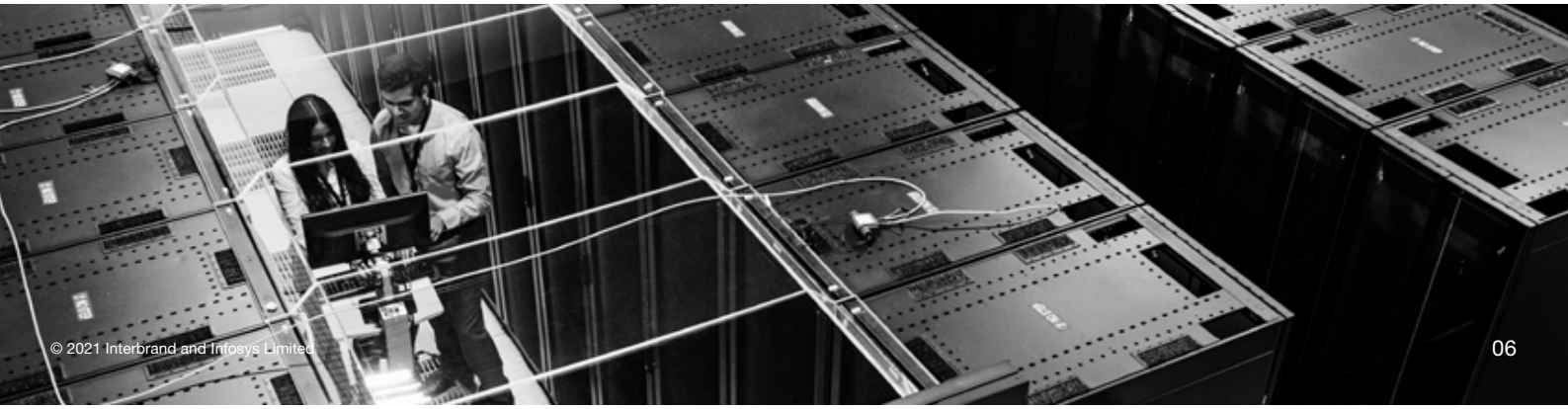
With such staggering amounts of data being shared by customers, older concerns once relegated to oblivion are re-emerging in a newer garb.

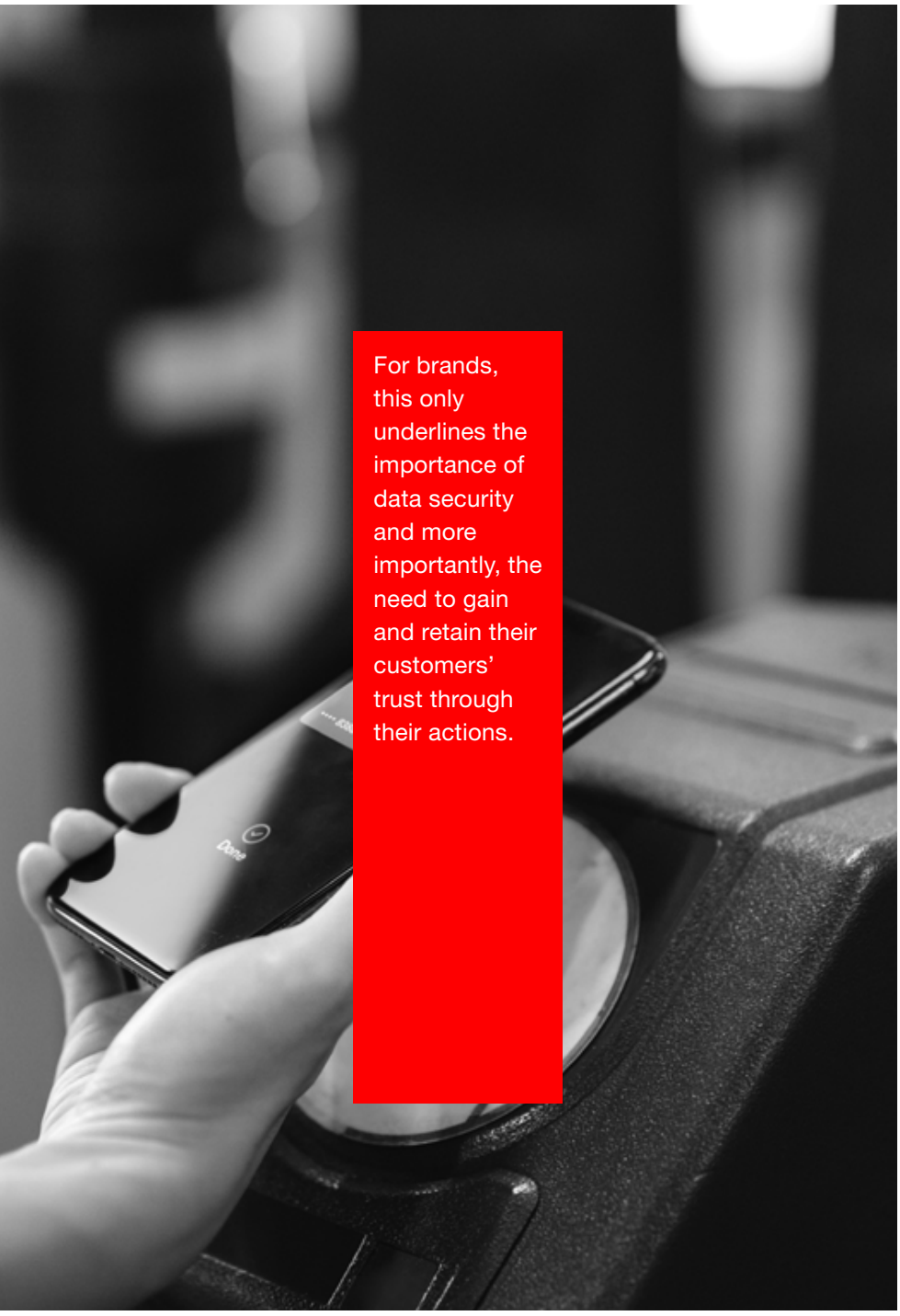
There are two aspects to this. To begin with, ‘security’ as a driver of choice is more relevant in today’s world. Security has largely been seen as a hygiene factor both, by businesses as well as consumers. So, the presence of a robust cybersecurity system in itself has never been reason enough for a consumer to trust that brand or organization, but the absence of it is enough to drive customers away. In real-world terms, much of what cybersecurity stands for has been reduced to customers looking for the “https://” or the green lock in their browser windows. But, with the increasing frequency with which customers are being hacked or cheated, these so-called hygiene factors are becoming more relevant.

Secondly, the definition of security itself has expanded. Until recently, the biggest risk that consumers faced in the event of a data breach was financial loss. So, cybersecurity as a term was something to be associated with banks and other financial brands. But in the recent years, and especially because consumers are willing to readily share their personal data with brands, that risk has expanded to include personal data as well. As a result, while on the one hand, customers readily share their data with brands, on the other, they constantly worry what the brands will do with that data. New conveniences like “sign in with Apple” or “sign in with Facebook” or “sign in with Google” make the case for sharing data. But incidents like the iCloud hack or the Facebook-Cambridge Analytica scandal keep bringing data security front and center in the customers’ relationship with the the brands that they love.

There is of course, a third aspect to this vulnerability that consumers might not even be aware of – businesses that interact with other business, but have consumer data at the center of it. The 2017 data breach of Equifax is a case in point. In 2017, hackers gained access to Equifax systems and exfiltrated hundreds of millions of customer records6. These records contained data that consumers had shared with their respective banks and financial intitutions, but not explicitly with Equifax.

In real-world terms, much of what cybersecurity stands for has been reduced to customers looking for the “https://” or the green lock in their browser windows





For brands, this only underlines the importance of data security and more importantly, the need to gain and retain their customers' trust through their actions.

Some reports estimate that 143 million customers – about 40% of the entire population of the United States – were affected by the breach6.

This was of course, unbeknownst to the end customer who had trusted their bank with data like their Social Security Number, but in many ways, it highlights their vulnerability in today's highly connected world. Ultimately, the breach resulted in significant declines in the stock price.

For brands, this only underlines the importance of data security and more importantly, the need to gain and retain their customers' trust through their actions. This is true not just for brands that directly interface with end customers, but also for the "B2B" brands that interface with other companies that might have access to customer data.

The cost of a breach runs beyond the immediate and the obvious

Most studies on a data breach have tended to focus on the immediate costs to a business. They have, for example, estimated the cost of each stolen record (including the costs of plugging the leak, rebuilding the business, damage to reputation and negative PR). On the other hand, the first casualties of a breach are often the topline sales or a drop in the market capitalization of the brand. The Equifax stock, for example, declined by as much as 35% following the 2017 breach6.

But, customer memory is short, and with time, the breach is forgotten. Sales often bounce back to pre-breach levels within 2 years at most and with it, the stock prices.

There's ample evidence of this – well-known brands like Target, eBay and JP Morgan Chase all saw their toplines returning to **'normal'** levels within 2-3 years after a data breach. Volkswagen's **'Dieselgate'** scandal, though not a data breach in the strictest sense, also illustrates this. In the years following Dieselgate, while VW sales quickly returned to normal, this was on the back of discounts (up to 18,000,000 Won on some models in South Korea, for example)[15]. Therefore, indicators like drop in revenues or stock prices might not always reveal the entire picture.

The real cost of a data breach might run much deeper because it fundamentally affects the way customers think of their relationship with the brand.

In fact, there have been studies published that demonstrate that 65% of consumers lose trust in a business in the event of a data breach and 85% of them “don’t want to deal with that business again”7.

In 2013, after a major US retailer faced a breach, the costs were astronomical. Aside from the immediate costs of the breach – **18.5$m** in fines and **61$m** to rebuild the systems – **12%** of the local customers said they’d stop shopping at the store, **36%** of them said they’d shop less frequently and **26%** of the returning customers said they’d spend less at the store8. Three years after the breach, their stock was still underperforming its peers9.

Data breaches impact a brand's relative strength

Brand Strength is Interbrand's primary brand management and measurement framework. It is the main platform through which we can diagnose issues and identify the actions required to grow a brand and business. An important component of Interbrand's brand valuation framework, Brand Strength measures the relative strength or weakness of a brand as compared to competition, across ten factors. Four of these factors are internal to the organization while six of them bring out the market and consumer perspective (see details about Interbrand's brand strength framework in the appendix).

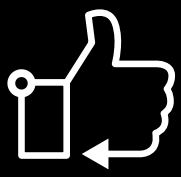
While a data breach might affect a brand and its perceptions holistically, we believe there are three factors of particular interest that a breach directly impacts, which together have an impact on the relevance the brand creates in its customers' lives.

Presence:

At the most basic level, a data breach instantly creates negative news about the brand. In the age of social media, this can quickly spiral out of control to create an overall negative perception about the company and brand.

In Target's case, for example, consumer perception dipped 54.6% in the year following the data breach (2014). And, while it had a steady uptick post that, it still didn't reach the pre-breach levels till end of 2018. This was also the period where the brand for the first time had more negative perception than positive perception among customers10.

This is consistent with a dip in scores for 'Presence' as a brand strength factor. In fact, we believe that the presence score is dented for every brand – regardless of whether it is a digital-first brand or a 'physical' brand – between 0.5 and 1 points.



Affinity:

The second significant impact that a breach has is on Affinity. As news of a data breach spreads, customers might either stop engaging with brands completely, or continue to do so at a significantly lower level.

For example, TSB, a 200-year-old British bank, lost 80,000 customers in the 12 months immediately following a breach in 2018.

Loss of affinity led to customers parting ways with the brand and earned the bank the dubious distinction of being among the most 'complained about' companies for that period11.

Admittedly, the impact of a breach on Affinity varies and is dependent on the degree to which customers feel a positive connection with the brand, based on their sense of having shared values. So, brands that primarily engage in the digital domain (Apple, Google, SAP, Netflix et al) might show a higher dent in Affinity scores than brands that might be more 'real world' (Nescafe, Pampers, Starbucks, for example). In our estimation, a breach might impact Affinity scores between 0.5 points to 2 points, depending on the extent to which consumers engage with them digitally.

Trust:

But, perhaps the most significant impact that a data breach has is on a brand's Trust. Indeed, trust is at the heart of any strong relationship, and the relationship between a brand and its customers is no different.
In today's world, where most – if not all – engagement between a brand and its customers is in the digital space, this assumes even greater significance.

Facebook for instance, saw users' trust in the brand plummet by as much as 66% in the wake of the Cambridge Analytica scandal 12.

Of course, the loss of trust in a brand is not limited to digital-first brands alone. In the wake of Dieselgate, VW lost 12.5b$, or 9% of its brand value, slipping four places in Interbrand's Best Global Brands league table13.

While 'Trust' is a much wider concept, we can infer that the impact on trust of a data breach is likely to be higher for digital-first brands (Apple, Google etc.) as compared to brands that engage with customers primarily in the real world (Gucci, Louis Vuitton, Pampers, Coca Cola, for example).

Still, the impact of a breach on a brand's strength can range between 0.5 and 2 points.

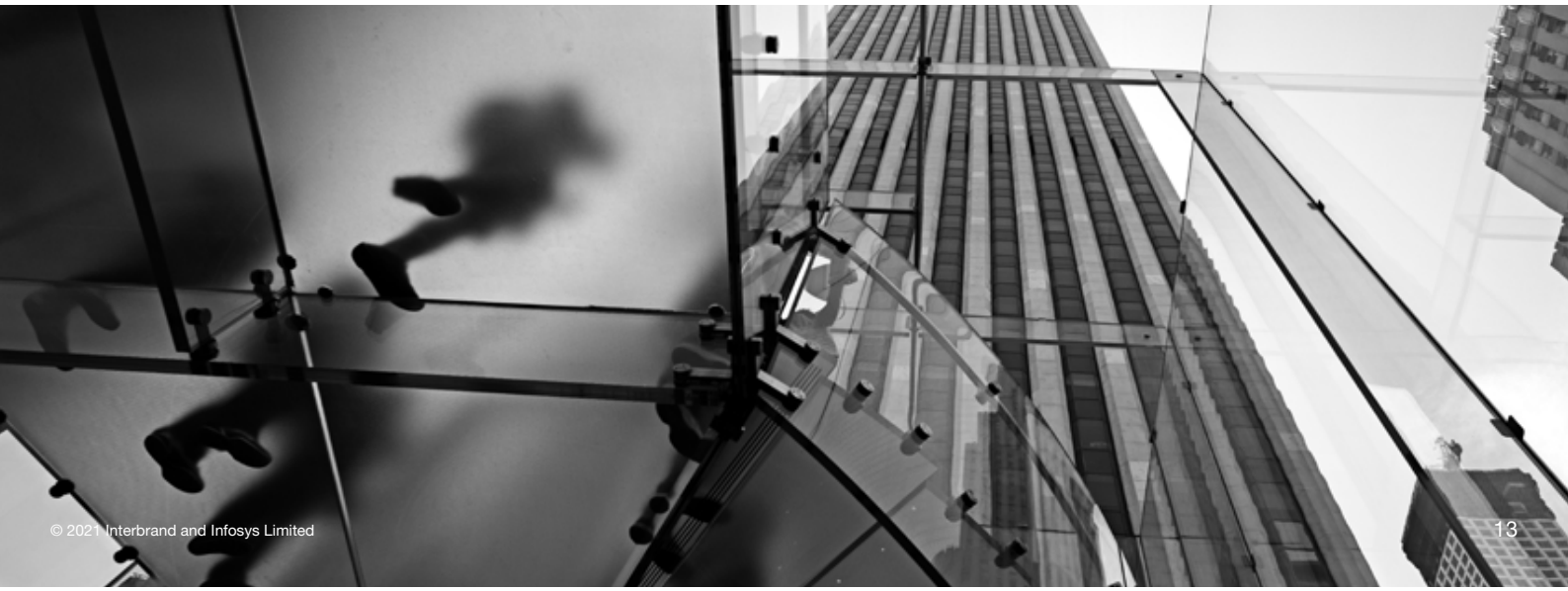
The bottom line – up to 223b$ Value at Risk

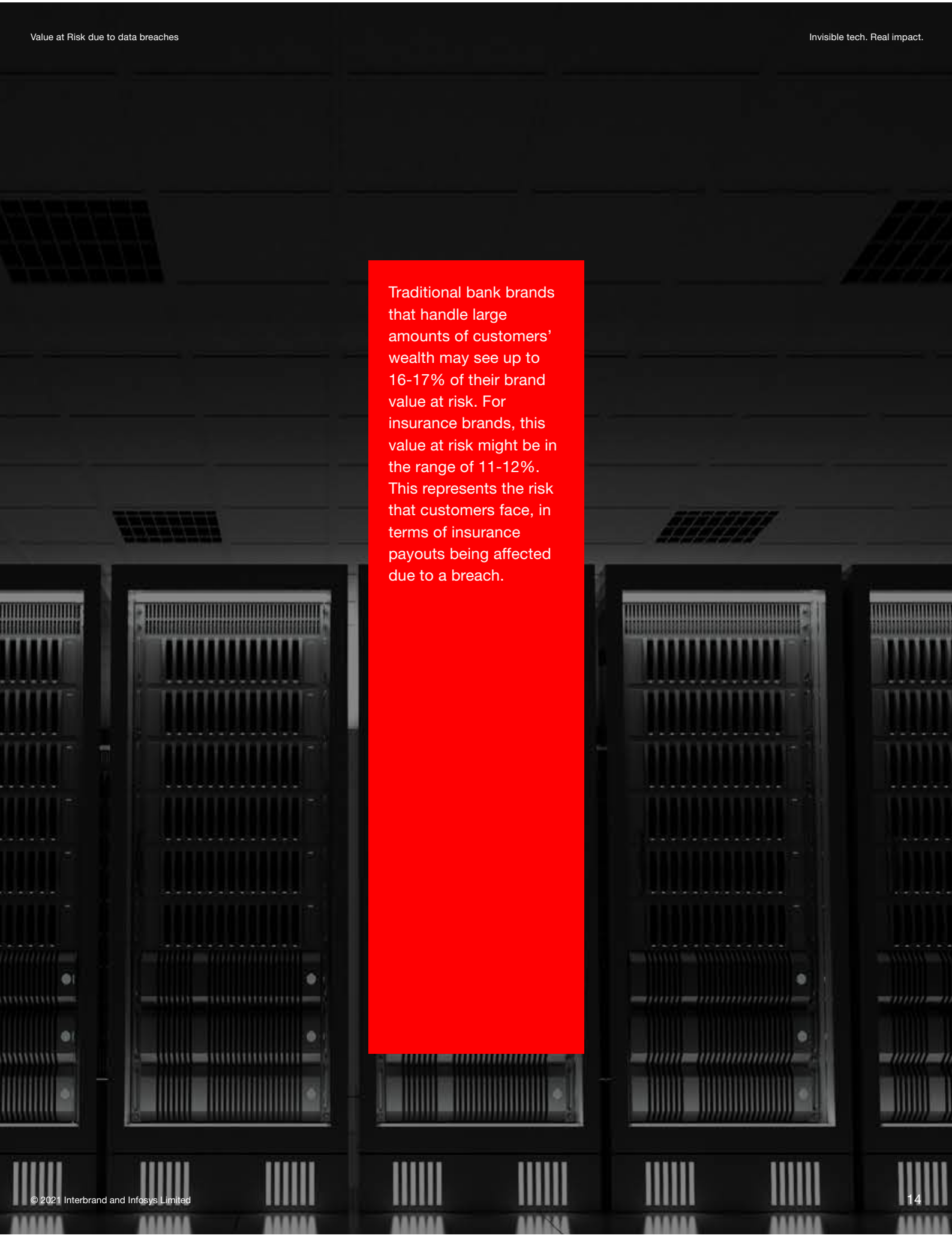
In value terms, the impact of a data breach is staggering. If, by some quirk of fate, the world's 100 most valuable brands were to experience a data breach, we estimate that the collective value that they might lose could be between **93$b** on the lower end, and **223$b** on the higher end. This represents between **4%** and **9.6%** of their cumulative value.

To put that figure in perspective, consider this – the total investments by VC funds in the United States in 2019, were estimated to be **135$b**[14] .

(see "How we did it" for more details on methodology).

Of course, the magnitude of the value at risk varies, depending on the industry that the brand operates in, and its relative brand strength. Financial Services brands are understandably, higher at risk. This is not surprising, considering that trust and security form the core offering of a financial service brand.





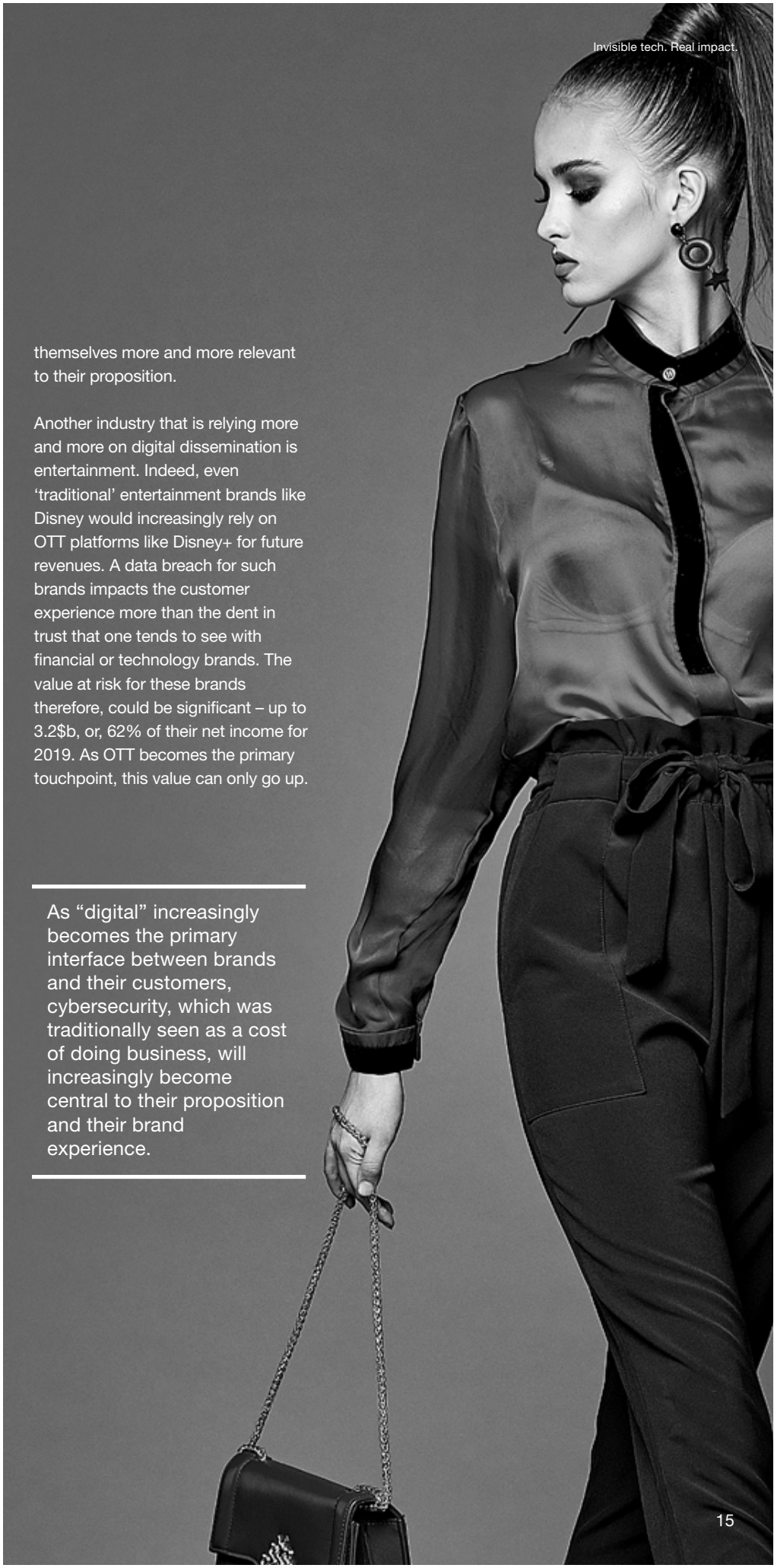
Traditional bank brands that handle large amounts of customers' wealth may see up to 16-17% of their brand value at risk. For insurance brands, this value at risk might be in the range of 11-12%. This represents the risk that customers face, in terms of insurance payouts being affected due to a breach.

New age financial brands on the other hand, face a different challenge. While a brand like PayPal might see about 12% of its brand value at risk, that still represents ~52% of its net income. This is logical, since these brands engage with their customers almost exclusively in the digital domain. As more and more traditional financial brands adopt a digital- and mobile-first strategy, the relevance of a robust cybersecurity strategy at the center of their value proposition can't be overemphasized.

Technology brands also have between 9 and 12% of their brand value at risk. However, in terms of the absolute number, this value at risk is the highest across industries. The largest of tech brands, for instance, might have up to 29$b of its value at risk in the event of a breach (Facebook, in fact, lost almost 12% of its brand value in the wake of bad press and regulatory pressures). This in many ways represents the ubiquity of these brands in our everyday lives, with customers willingly sharing vast amounts of personal data with them. That ubiquity is also the reason these brands have such astronomical brand values. In fact, technology as a sector accounts for the lion's share of the cumulative value of the top 100 brands. As these FAANG* brands play an ever-increasing role in our lives, their customers continue to put greater trust in them. It is this trust that makes it possible for these brands to credibly offer financial products like the Apple Card or Amazon Pay to their customers. For the brands, issues like security and privacy would increasingly find themselves more and more relevant to their proposition.

Another industry that is relying more and more on digital dissemination is entertainment. Indeed, even 'traditional' entertainment brands like Disney would increasingly rely on OTT platforms like Disney+ for future revenues. A data breach for such brands impacts the customer experience more than the dent in trust that one tends to see with financial or technology brands. The value at risk for these brands therefore, could be significant – up to 3.2$b, or, 62% of their net income for 2019. As OTT becomes the primary touchpoint, this value can only go up.

> As "digital" increasingly becomes the primary interface between brands and their customers, cybersecurity, which was traditionally seen as a cost of doing business, will increasingly become central to their proposition and their brand experience.



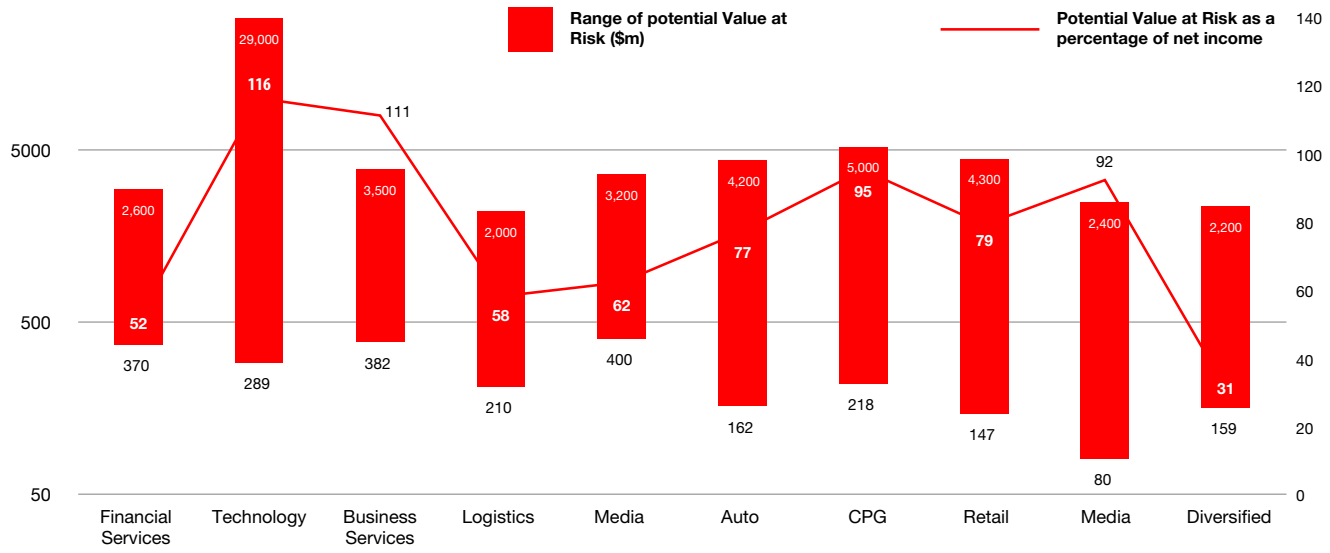
** Facebook, Apple, Amazon, Netflix, Google*

Traditional B2B brands, though not directly interfacing with the end customer, are equally at risk. Business Services brands collectively have between 382$m and 3.5$b at risk. That represents, on an average, 9-11% of their brand value, and could be as high as 63% of their 2019 net income. For new-age brands that have been born in the digital-age, the value at risk can be as high as 111% of their 2019 net income. The primary reason for such high values at risk is the extent of customer data that these brands handle. A breach in their systems might thus not only impact the experience that their customers' customers have, it could also compromise end customer data. With the pandemic and the resultant shift in working habits of the world, the risk to these brands will only go higher.

Are there any brands that are relatively insulated? One might tend to think that brands that rely on the 'real world' for their experience are relatively safer. So, luxury brands like LV or Gucci, personal care brands like Pampers, Gillette et al, or retail brands like McDonald's, Starbucks, IKEA or Nike might be relatively protected. But, that reality is changing rapidly, as the example of automotive brands shows. The risk to a traditional auto brand is primarily in terms of the bad press and the dent in its reputation. And so, they may only lose 8-9% of their brand value in the event of a breach. However, a 'digital native' brand may have up to 24% of its value at risk and, while that might not be a very large number in absolute terms, it could represent up to 800% of their net income for 2019.

For brands, the writing is on the wall – as "digital" increasingly becomes the primary interface between them and their customers, cybersecurity, which was traditionally seen as a cost of doing business, will increasingly become central to their proposition and their brand experience.

With the pandemic and the resultant shift in working habits of the world, the Value at Risk for Business Services these brands may only grow.



And we all fall down
From Technology to Media, Logistics to a Luxury – a data breach can have catastrophic consequences for brand value both, in absolute terms as well as as a percentage of net income.

Seven steps to a future-ready Cybersecurity strategy

For brands to continue enjoying the trust that their customers have placed in them, they need to implement a well-defined, evolving cybersecurity strategy to maintain constant vigil and protect applications, data, networks and systems from the ever-present cyberthreat landscape. While there are no set “rules” to build the framework and no system can possibly guarantee protection against 100% of threats, there are guidelines that experts believe are important, to build a robust strategy:

1

It all starts with the culture

Whilst it is the most difficult thing to achieve, a truly robust strategy begins by inculcating a “culture of security” within the organization. That can be followed up by putting in place a robust organizational foundation for it. Very often, this begins by placing the Chief Information Security Officer at the center of the organization. To the rest of the organization, this signals the strategic importance of cybersecurity within. This also ensures business ownership of the cybersecurity agenda, besides clarifying the roles and responsibilities of people within the wider organization. Building the culture and foundation makes security everyone’s responsibility, and not just that of the “IT team”.

2

Independence and Empowerment

The second building block is ensuring independence and empowerment of the CISO. To the wider employees, this signals the seriousness that the organization places on IT security (as opposed to making it a part of the CIO’s remit). Independence and empowerment of the CISO also ensures that critical security-related changes within the organization can be driven effectively and efficiently.

3

Backing the strategy with the right investments

Strategy without the right investments to translate it into action can be sub-optimal. Estimating investments into cybersecurity initiatives largely depends on the profile of the specific company, its customers, the kind of (customer) data it handles and its sensitivity. A realistic estimation of the risk profile is essential to ensure that the investments in people, processes and technology stay ahead of the cyber-threat landscape. The fact that investments in cybersecurity spends have gone up to ~8-10% of the overall IT budget from ~4-5% a decade ago points to the commitment that organizations are making to it.

4

Staying ahead of the curve

Given the ever-changing nature of the cyber threat landscape, it is important to ensure a proactive cybersecurity strategy that anticipates threats, and stays ahead of them. Undertaking a peer benchmarking study to ascertain the target state is only the beginning. This should be backed up by investing in robust threat intelligence platforms, threat hunting capabilities and other emerging technologies. Building a robust cyber resilience program (to ensure that the organization 'bounces back' from an attack quickly) and making cyber insurance a part of the overall cybersecurity strategy are other ways to build a proactive strategy.

5

Engaging the board and building a robust governance system

A robust cybersecurity system must also ensure the continuance and building of initiatives that are taken. This is often achieved by creating an Information Security Council that has participation from the leadership and various other parts of the organization. Setting up processes like regular meets of the council, and exchanges between the council and the board, ensures commitment to the cause and consistent outcomes across various parts of the organization.

6

Cyber Risk Management

Integrating cyber risk management into the overall risk management framework of the company ensures a more holistic view of the various risks that the organization might face, and the risk-mitigation actions that it could take. Doing this involves understanding the cyber threats to business, undertaking a risk assessment that is signed off by the Information Security Council and the CISO and integrating the cyber risk management framework with the operational risk management framework.

7

Don’t forget the supply chain

But, in today’s connected world, the biggest risk to the organization might often lie outside it. Supply chains are often the most vulnerable, since there is limited control that an organization may exert on vendors and partners. Assessing risks in the supply chain, tightening supply chain security and integrating the governance of cyber risks due to the supply chain with the corporate governance function ensures a higher level of protection to the organization, as well as better visibility and tracking.

How we did it

For the purposes of this exercise, we elected to simulate the Value at Risk for a brand, in the event of a data breach. Desk research and initial discussions with both, customers and cybersecurity experts helped us determine that the three major ways a brand might be impacted was through negative perceptions about the brand, a loss in trust and a lowered sense of positive connection with the brand in future. We determined that these corresponded to Presence, Trust and Affinity in terms of Interbrand's brand strength factors, that have a direct impact on the relevance of the brand in its customers' lives.

We then ran a poll amongst valuation experts across Interbrand's global offices, to get a 'consensus estimate' for the specific impact on each brand strength factor, in points. The brand value for each brand was then calculated using these impaired brand strength scores to estimate the "best case" brand value, i.e. the value at risk assuming that the brand's revenue was unchanged.

To obtain the "worst case" scenario, it was important to simulate a dip in revenues that a breach might result in. To arrive at an average, we studied the revenue drop that some of the brands that faced a breach, showed in the years after the breach (Target, Adobe, JP Morgan, TSB, Playstation, Starbucks). Calculating the brand value with the dip in revenues and the dented brand strength scores gave us the upper end of the Value at Risk.

15	**Interbrand offices**
45	**Valuation experts**
100	**Best Global Brands**

An example

This example for a hypothetical luxury brand shows the above methodology in action. The Financial Analysis provides the Economic Profit, and the basis for brand valuation.

€ millions	2016 (act.)	2017 (act.)	2018 (act.)	2019 (act.)	2020 (act.)	2021 (ff.)	2022 (ff.)	2023 (ff.)	2024 (ff.)	2025 (ff.)
Revenues	1,347	1,801	2,069	2,516	2,934	3,827	4,990	6,508	8,487	11,068
Revenue growth %	15%	34%	15%	22%	30%	30%	30%	30%	30%	30%
EBIT	226	322	401	577	805	843	1,098	1,432	1,867	2,435
EBIT margin %	16.7%	17.9%	19.4%	22.9%	27.4%	19.1%	19.2%	21.1%	24.7%	24.7%
Tax	59	84	104	150	185	219	285	372	485	633
NOPAT[1]	167	238	297	427	620	623	812	1,059	1,382	1,802
Operating Assets	357	375	593	683	1,137	1,086	1,416	1,847	2,409	3,141
WACC[2]					8.36%					
Capital Charge	46	49	77	89	70	92	120	157	205	267
Economic Profit	**121**	**189**	**220**	**338**	**550**	**531**	**692**	**903**	**1,177**	**1,535**

1. Net Operating Profit After Tax
2. Weighted Average Cost of Capital

Applying the Role of Brand to Economic Profit then yields the Branded Earnings. For this luxury brand, we assumed a Role of Brand Index of 62%. Branded Earnings are estimated for the forecast period.

€ millions	2020 (act.)	2021 (ff.)	2022 (ff.)	2023 (ff.)	2024 (ff.)	2025 (ff.)
Economic Profit	550	531	692	903	1,177	1,535
Role of Brand Index	**62%**	**62%**	**62%**	**62%**	**62%**	**62%**
Branded Earnings	**341**	**329**	**429**	**560**	**730**	**952**

Finally, the Brand Strength Score (68, in this case), translates into a discount rate of 11.1%.

Brand Strength Score		Implied Discount Rate
68	>	11.1%

Combining Economic Profit, Role of Brand, and Brand Strength into a time value formula yields the financial value of the Brand

Brand Value through Year 4

BV Through Year 4 € millions	2021 (ff.)	2022 (ff.)	2023 (ff.)	2024 (ff.)	2025 (ff.)
Branded Earnings	329	429	560	730	952
Discount Rate	11.1%	11.1%	11.1%	11.1%	11.1%
Discount Factor	1.05	1.17	1.30	1.44	1.60
Discounted Br. Earnings	**312**	**+ 367**	**+ 431**	**+ 506**	**+ 594** = 2,209

Perpetuity Value

Year 5 Value	594
	X
1+ Growth Rate	1.065
	÷
Discount Rate	4.60%
–Growth Rate	=
Residual Brand Value	**13,984**

€16,103m

Accounting for the breach (BSS of 64.5translating to a discount rate of 11.3%) lets us simulate the impaired brand value

Brand Value through Year 4 – Post Breach

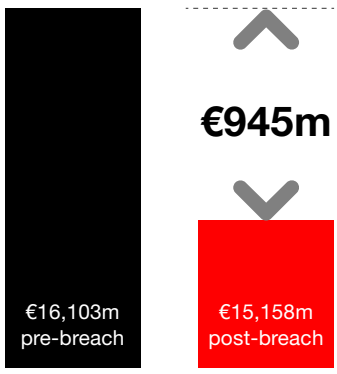
BV Through Year 4 € millions	2021 (ff.)	2022 (ff.)	2023 (ff.)	2024 (ff.)	2025 (ff.)
Branded Earnings	329	429	560	730	952
Discount Rate	11.3%	11.3%	11.3%	11.3%	11.3%
Discount Factor	1.06	1.17	1.31	1.46	1.62
Discounted Br. Earnings	**312**	**+ 365**	**+ 428**	**+ 501**	**+ 587** = 2,194t

Perpetuity Value – Post Breach

Year 5 Value	587
	X
1+ Growth Rate	1.065
	÷
Discount Rate	4.80%
–Growth Rate	=
Residual Brand Value	**12,964**

€15,158m

Simulated Value at Risk



Interbrand's ISO-certified Brand Valuation Methodology

Interbrand's brand valuation methodology seeks to provide a rich and insightful analysis of brands, providing a clear picture of how the 'brand' is contributing to the business growth today, together with a road map of activities to ensure that it is delivering even further growth tomorrow.

Having pioneered brand valuation in 1988, we have a deep understanding of the impact a strong brand has on the growth of business. Strong brands influence customer choice and create loyalty; and even attract, retain, and motivate talent; as well as lower the cost of financing. Our brand valuation methodology has been specifically designed to take all of these factors into account.

Interbrand was the first company to have its methodology certified as compliant with the requirements of ISO 10668 (requirements for monetary brand valuation) and played a key role in the development of the standard itself.
There are three key components to our valuations: an analysis of the financial performance of the branded products or services, of the role the brand plays in purchase decisions, and of the brand's competitive strength.

Financial Analysis:

This is the measure of the overall financial return to an organization's investors, or its economic profit. Economic profit is the after-tax operating profit of the brand, minus a charge for the capital used to generate the brand's revenue and margins.

Role of Brand:

This measures the portion of the purchase decision attributable to the brand as opposed to other factors (for example, drivers of purchase like price, convenience, or product features). .

Brand Strength:

Brand Strength analysis is based on an evaluation across 10 factors that Interbrand believes constitute a strong brand. Our 10 Brand Strength factors are based on both internal and external dimensions:.

Internal Factors: Leadership

Direction:

The degree to which there is a clear purpose and ambition for the brand, a plan to deliver on them over time, and a defined culture and values to guide how those plans should be executed.

Alignment:

The degree to which the whole organization is pulling in the same direction, committed to the brand strategy and empowered by systems to execute it across the business

Empathy:

The degree to which the organization is in tune with customers and wider stakeholders, actively listening to and anticipating their evolving needs, beliefs and desires, and responding effectively and appropriately.

Agility:

The speed to market that a company demonstrates in the face of opportunity or challenge, enabling it to get ahead and stay ahead of expectations.

External Factors: Engagement

Distinctiveness

The existence of uniquely ownable signature assets and experiences that are recognized and remembered by customers and difficult to replicate.

Coherence:

The degree to which customer interactions, whilst varying depending on channel and context, remain authentic to the brand's narrative and feel.

Participation:

The degree to which the brand has the ability to draw in customers and partners, create a sense of dialogue and encourage involvement and collaboration.

External Factors: Relevance

Presence:

The degree to which a brand feels omnipresent to relevant audiences, is talked about positively, and is easily recalled when a customer has a need in the brand's category.

Trust:

The extent to which a brand is seen to deliver against the (high) expectations that customers have of it, is perceived to act with integrity and with customers' interests in mind.

Affinity:

The degree to which customers feel a positive connection with the brand, based on the functional and/ or emotional benefits provided, and/or a sense of having shared values

Contributors

Akifumi Ito
Ameya Kapnadak
Apeksha Lohia
Armen Soorenian
Arnita Chakravorty
Arsene Oka
Ashish Mishra
Ashmita Kannan
Atsuko Sakamoto
Balaji Sampath
Beatriz Diego
Bosco Torres
Calin Hertioga
Charlie Sturr
Chris Kwon
Constanza Gabelich
Cristobal Pohle Vazquez
Declan O'Callaghan
Francisco Castanos
Gaia Pedinelli
Hiromitsu Hatakeyama
Isabel Mossato
Jay Myers
Jennifer Zuo
Jordan Siff
Josh Ezickson
Jungwon You
Kartik Mani
Kayoko Kurashige
Lajja Marjadi
Lea Nolting
Magnus Marwege
Mariana Sun
Matteo Corbellino
Megan Skeats
Meike Papenfuss
Michael Kim
Mike Rocha
Mythreya Reddy Kota
Patrick Fuller
Patrick Lopez
Philip Bae
Rahul Bansal
Rodrigo Marques
Sachin Mistry
Silvia Venturini
Steven Lee
Sumit Virmani
Valentina Suligoj
Vanessa Esquivel
Vishal Salvi

References

1. David Aaker, "Managing Brand Equity"
2. Jonathan Knowles; https://www.linkedin.com/pulse/intangible-assets-represent-80-value-sp-500-jonathan-knowles/
3. Statista; https://www.statista.com/statistics/828403/median-price-of-popular-sneaker-brands-worldwide/
4. Owler; https://www.owler.com/company/apple
5. World Economic Forum; https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/
   Science Focus; https://www.sciencefocus.com/future-technology/how-much-data-is-on-the-internet/
6. CSO India; https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html
7. Varonis; https://www.varonis.com/blog/company-reputation-after-a-data-breach/
   PWC; https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/cybersecurity-protect-me.html
8. Interactions- Retail's Reality: "Shopping Behavior after a breach"
9. The Motley Fool, July 15, 2016; https://www.fool.com/investing/2016/07/15/target-stock-history-what-you-need-to-know.aspx
10. Varonis; https://www.varonis.com/blog/company-reputation-after-a-data-breach/
11. BBC; https://www.bbc.com/news/business-47085474
    The Telegraph; https://www.telegraph.co.uk/money/consumer-affairs/consumers-win-9-10-tsb-complaints-summer-shame/
12. NBC News; https://www.nbcnews.com/business/consumer/trust-facebook-has-dropped-51-percent-cambridge-analytica-scandal-n867011
13. Interbrand's Best Global Brands 2014 and 2015; https://www.interbrand.com/best-brands/
14. KPMG; https://home.kpmg/us/en/home/media/press-releases/2020/01/venture-capital-investment-in-us-in-2019-hits-136-5-billion-second-highest-on-record-kpmg-report.htm
15. WSJ.com; https://www.wsj.com/articles/volkswagen-sales-in-south-korea-make-sharp-upturn-1449203756

Infosys®
Navigate your next

Interbrand

Stay Connected