INVISIBLE TECH REAL IMPACT.

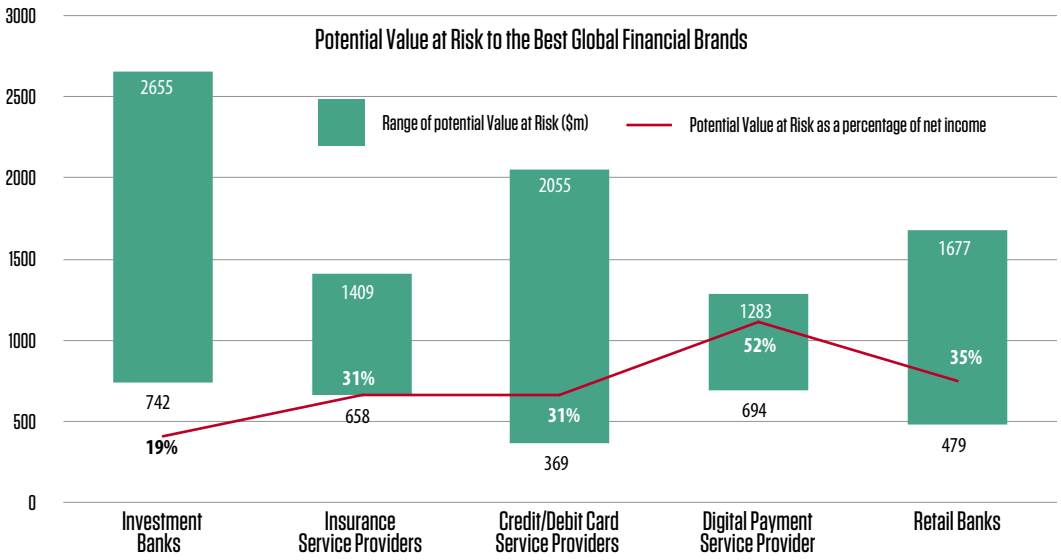
The Industry View.

Infosys®
Navigate your next

Interbrand

1

Financial Services



The global financial sector has been a primary target for cyberattacks because of the tremendous value of the information to which these organizations often have access.

Financial institutions have loads of PII – personal identification information, including cryptocurrency portfolios. Cybercriminals often perform attacks like phishing to compromise account credentials and gain unauthorized access.

In fact, according to the Boston Consulting Group, financial services firms are hit by cyberattacks a staggering 300 times more frequently than businesses in other industries.

In a survey by Clearswift, an information security firm, the leading cause of most incidents was the employees' failure to follow the security protocol.

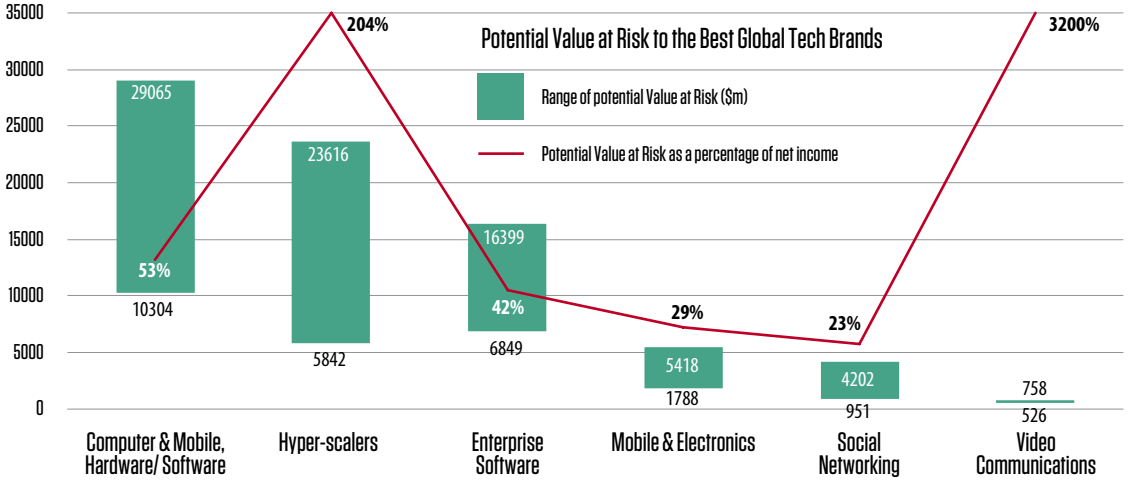
Another reason, according to the same study, was the introduction of BYOD (bring your device) which contributed to 32% of the attacks, allowing file and image downloads which contributed to 25% of them, and sharing of data by the employees unintentionally which contributed to 24% of the attacks[1].

Security is at the core of any financial services brand's proposition. It is therefore, no surprise that these brands have a very high value at risk. Indeed, monetary loss in addition to a loss in trust can cause irreparable damage to a financial services brand. In fact, the cumulative value at risk due to a cybersecurity breach for financial services brands can be as high as 2.6$b.

Traditional bank brands that handle large amounts of customers' wealth might see up to 16-17% of their brand value at risk. For insurance brands, this value at risk is somewhat lower at 11-12%. For a digital-first brand, the value at risk might be as high as 52% of their net income, even though it represents 11-12% of the overall brand value. With "digital-first" quickly becoming the norm for even traditional financial services brands, the quantum of this value at risk can only go higher.

2

Technology



The recent times have seen a number of new technologies become a part of our lives and businesses – 5G and IoT to Artificial Intelligence, Cloud technology, and Machine Learning.

While these technologies create efficiencies, save time, reduce costs, they have also led to an increase in the amount of data we create and share online. New technologies mean vulnerabilities are lesser known and easier to exploit.

In fact, in a recent survey by Raconteur, 94% of the telecom operators and industry experts agreed that security challenges would escalate with the advent of 5G technologies[2].

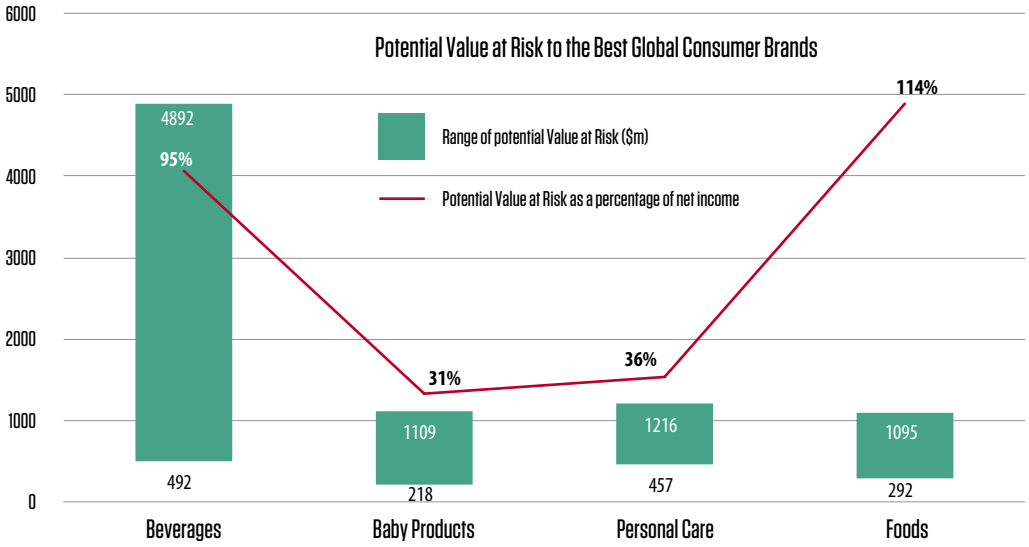
It is no wonder then, that the absolute Value at Risk for the technology brands is the highest across industries. In fact, the cumulative value at risk that tech brands have in the event of a breach could be as high as 29$b. This represents up to 53% of their total cumulative brand value.

This is of course, commensurate with the overall value of technology brands. But more importantly, it is reflective of the value that technology (and, by extension, technology brands) play in our lives. Whether it is hailing a cab, making an appointment at the dentist, paying bills or transferring money – technology is at the center of most of our tasks and daily chores. The corollary is that we willingly share large amounts of personal data with these brands. The value at risk then, is also reflective of the importance of safeguarding this personal information.

As tech plays a deeper role in our lives (also credibly offering financial products now), issues like security and privacy are expected to become even more important in driving brand choice.

3

Consumer Goods



While most consumer product brands still operate in the physical realm, they are also highly dependent on manufacturing. And that is where the risk to these brands emanates from.

In many – if not most – cases, the manufacturing facilities can not afford to be down for extended periods of time. Cybercriminals take advantage of this fact and target these companies with ransomware attacks.

But manufacturing facilities are only one part of the story. Most consumer product brands also depend on a complex and highly inter-connected supply chain that has a web of suppliers, production lines, multinational sites, and logistics. With the increasing complexity, comes increased vulnerability to attacks.

According to Darktrace, a leading cybersecurity company, cyberattacks against manufacturers increased seven times between January and April 2020. 26% percent of companies Darktrace surveyed didn't have a division overseeing security at factory management systems[3].

For consumer product brands, this translates into a potential value at risk of up to 4.3$b. In some cases, this might be as high as 114% of the net income of the brand.

As these brands increasingly adopt digital means of engaging with their consumers and creating personalized experiences for them, this potential value at risk might only go higher.

4

Automotive

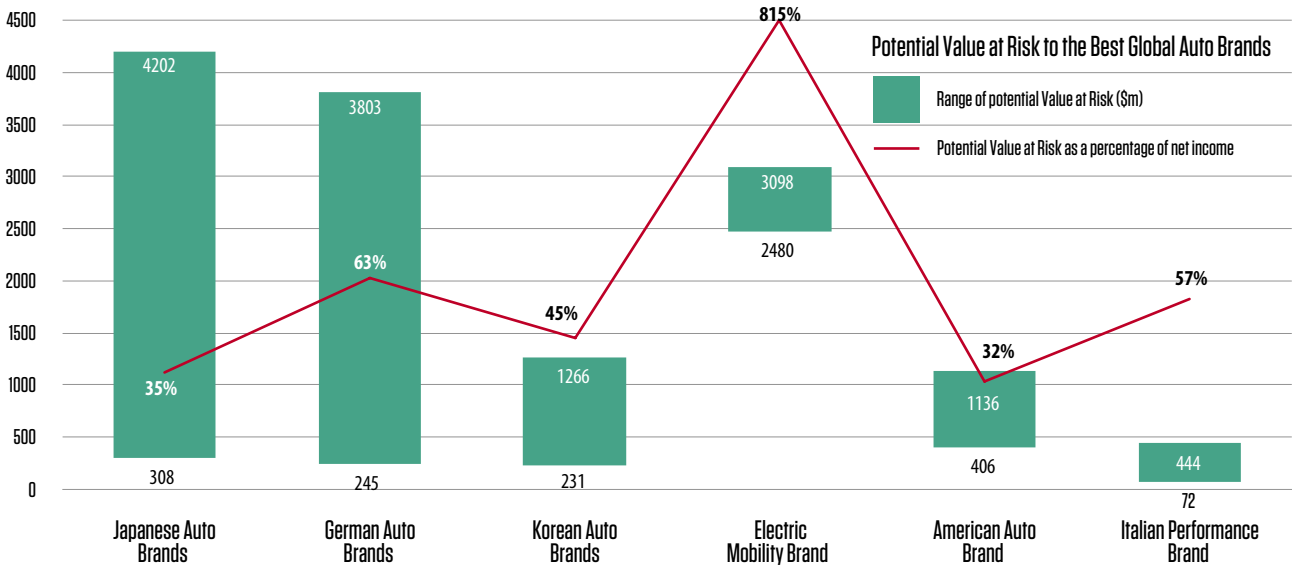
Since the large majority of automotive brands still operate in the "real" world, one would assume that these brands are relatively lower at risk.

That might be partly true, since the risk to 'traditional' auto brands might come primarily from reputational risk. In percentage terms, this might translate to 8-9% of their total brand value.

However, the automotive industry is changing at a blazingly fast pace. Indeed, much of the innovation in the industry is driven by software. Whether it is on-board telematics, connected cars or fully autonomous cars, the world of auto is transforming into a world of mobility. Each of these innovations bring with them, an increased risk of a breach.

Of course, the car itself is just one element that is at risk, and car and passenger safety are of prime importance to focus on, in the event of a breach. However, the breach can potentially affect the larger ecosystem – from disrupting factories to financing operations, to even loss of customer data. A leading global automaker for example, experienced a cyber attack in June 2020. The company confirmed that work at the UK plant had been halted alongside a suspension of other operations in North America, Turkey, Italy and Japan[4].

As traditional auto shifts to "mobility solutions", digital is expected to become increasingly more important to their experience. With this, the value at risk even for 'traditional brands' can only go up.

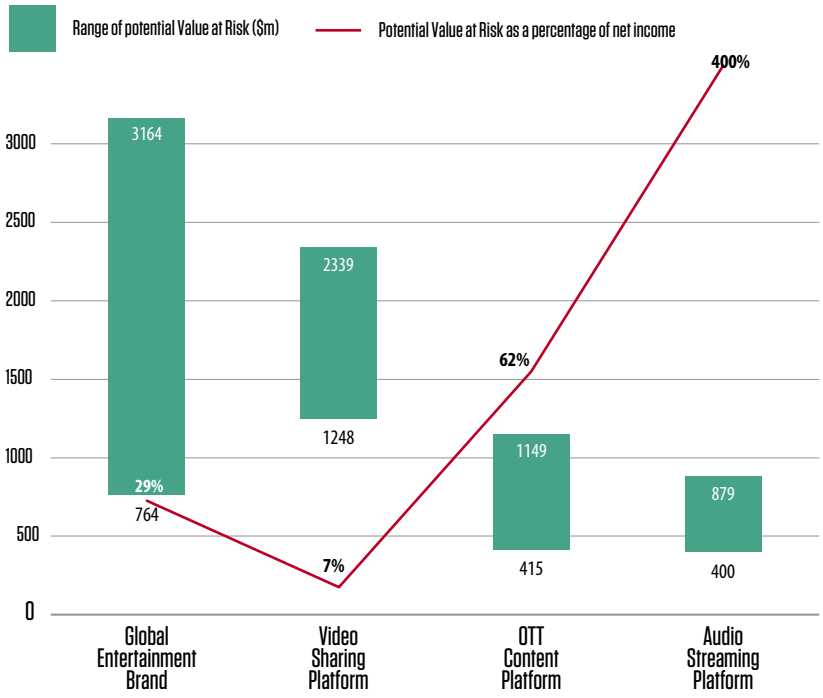


5

Media

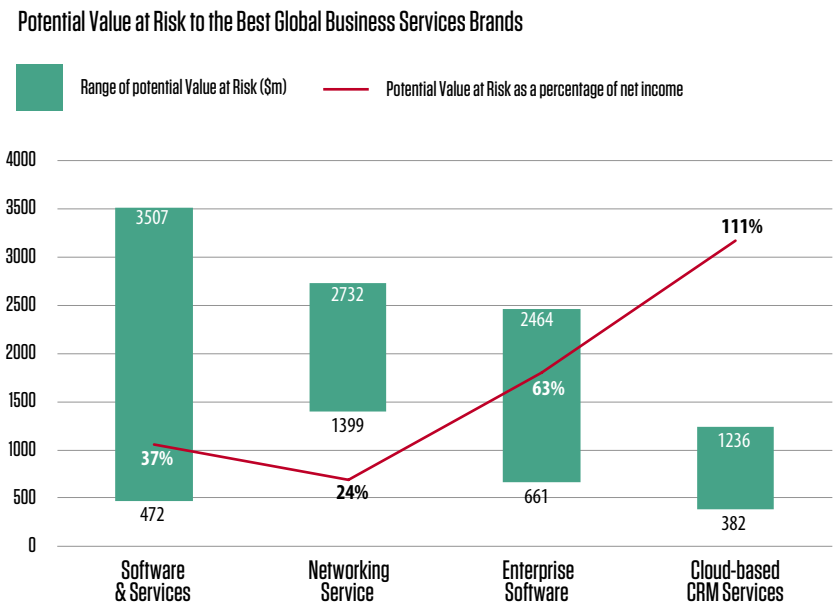
Media as an industry is also undergoing fundamental changes in the way the consumer interacts with it. Indeed, as digital and online become the primary channels of media consumption, the exposure to cyber threats increases manifold. What makes online media brands especially vulnerable is the large number of consumers that they interact with. This makes them a potential entry point for launching attacks onto individual customers. This of course, is in addition to the risk that these brands inherently face in terms of disruption of service (and the resultant dent in customer experience) and the risk of compromising customer data.

Potential Value at Risk to the Best Global Media Brands



6

Business Services



Business services handle a vast amount of corporate data, which is one of the primary sources of risk for these brands. The cumulative value at risk for these brands could be as high as 3.5$b. Expressed as a percentage of net income, the value at risk could be as high as 111% in some cases.

The changing nature of worklife in a post-pandemic world presents newer complications. WFH became the norm during the pandemic and chances are, it will still dominate a large part of our working lives in the years to come. That in turn implies that organizations provide their employees with resources that ensure they remain productive – and connected.

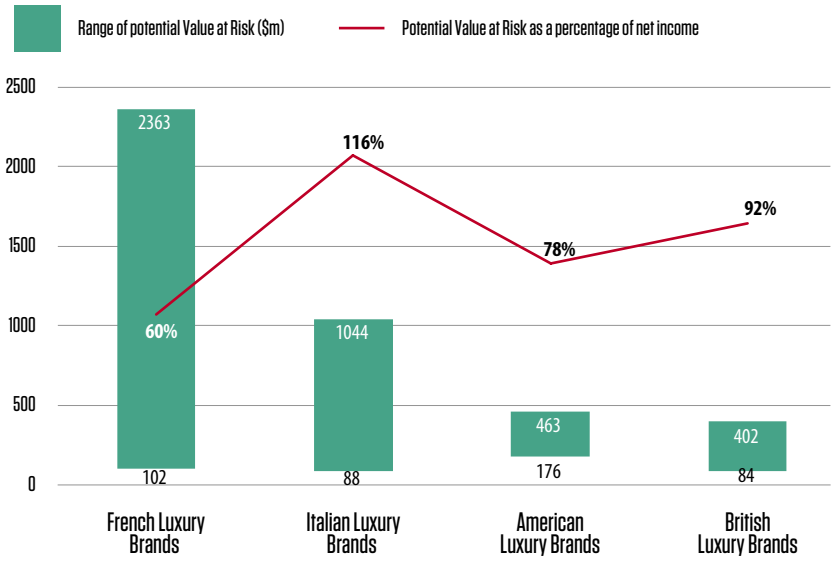
A survey conducted by Malwarebytes, a cybersecurity firm concluded that since the start of the pandemic, remote workers had caused a breach in 20% of the organizations[5]. The same survey found that business email compromise and a quick shift to cloud services in response to the pandemic, contributed to the emerging issue.

For business services brands, this directly impacts the reputation of the brand, and ultimately, their brand value at risk.

7

Luxury

Potential Value at Risk to the Best Global Luxury Brands



Luxury as a category relies on creating an exclusive, "otherworldly" experience for their customers. These experiences are still primarily delivered in the physical world, making the value at risk relatively lower in percentage terms.

In absolute terms, however, these brands still have up to 2.4$b at risk. This is largely due to the sheer value of luxury as a category, thanks to their highly premium offering.

There is of course, another aspect of risk that luxury brands face – the loss of reputation and the resultant loss in brand value. Luxury brands have a clientele that is largely comprised of high net worth individuals, and a breach in their systems can put these individuals at risk. In April 2018, it was announced that the JokerStash hacking group, also known as Fin7, walked off with an astounding 5 million credit and debit card numbers from Saks Fifth Avenue, Saks Off 5th, and Lord & Taylor. It was also one of the more significant credit card heists in history[6].

The other source of reputational risk is spoofing. Criminals use variants of a luxury brand's name to create fake URLs that lure shoppers with astounding 'offers'. The fake sites then steal money from the clients.

For luxury brands, this translates into an impact on both, online commerce as well as reputation.

In fact, it is estimated that the spoofing industry could be as big as 460$b globally. For comparison, the value of of the online luxury goods market is estimated to be 264$b[7].

As luxury brands target a younger customer set, digital and online interfaces would be increasingly more important in creating that unique experience. That in turn translates into higher value at risk in the future.

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. Clearswift; *https://www.clearswift.com/about-us/pr/press-releases/70-percent-companies-suffered-cyber-security-incident-in-last-12-months*
2. Raconteur; *https://www.raconteur.net/technology/5g/5g-security/*
3. Tech Republic; *https://www.techrepublic.com/article/top-5-business-sectors-targeted-by-ransomware/*
4. BBC; *https://www.bbc.com/news/technology-52982427*
5. ZDNet; *https://www.zdnet.com/article/working-from-home-trend-causes-surge-in-cybersecurity-costs-security-breaches/*
6. CPO Magazine; *https://www.cpomagazine.com/cyber-security/asus-supply-chain-attack-highlights-new-security-vulnerability-for-tech-giants/*
7. TMC Net; *https://www.tmcnet.com/topics/articles/2018/05/20/438191-luxury-brands-cyber-security-a-big-deal.htm*

For more information, contact askus@infosys.com

Infosys®
Navigate your next

Infosys.com | NYSE: INFY

Stay Connected