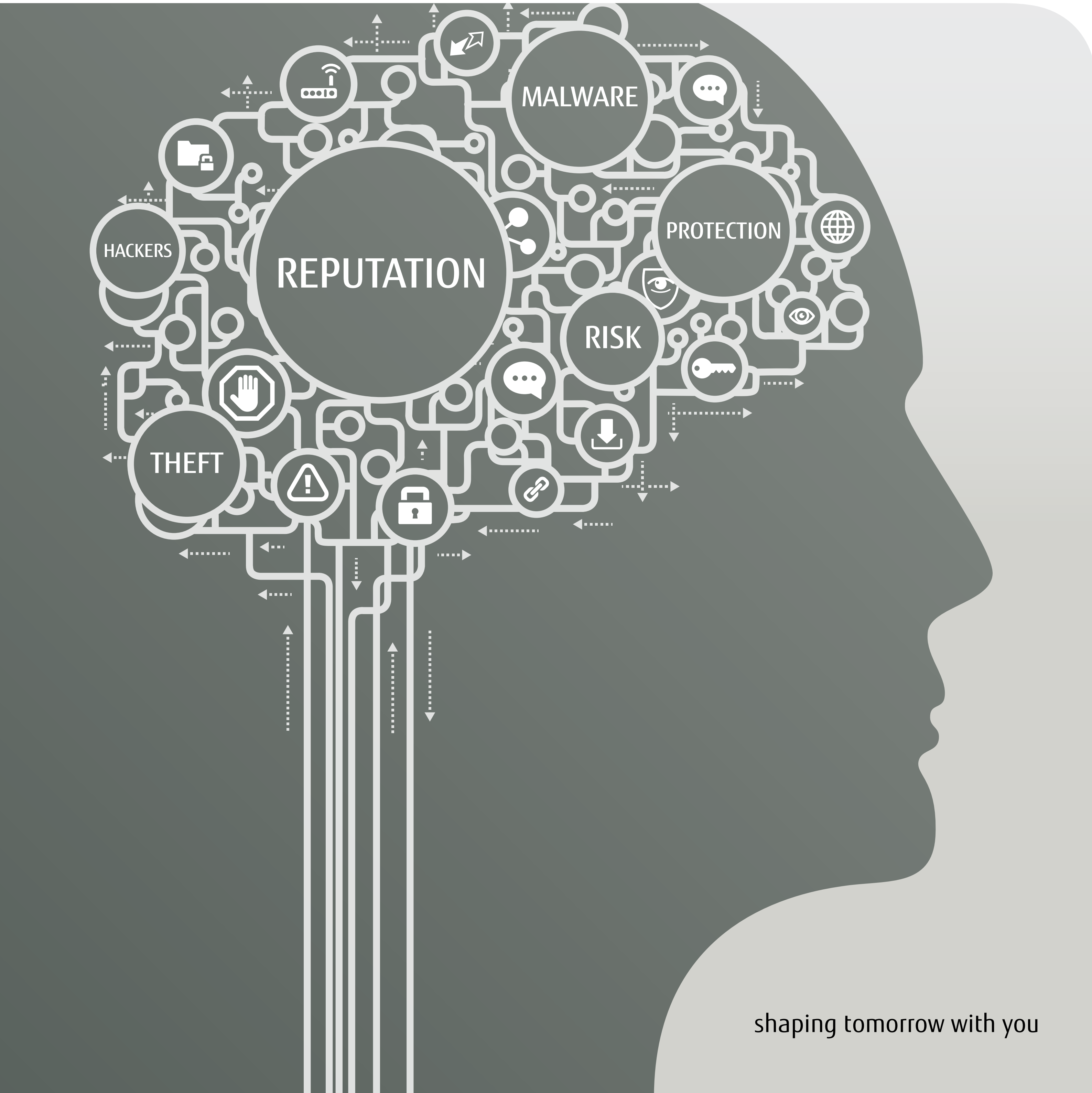
FUJITSU

Secure Thinking

Bigger Data. Bigger risk?



shaping tomorrow with you

There has always been data.

What is different now is the scale and speed of data growth. Every day we create 2.5 quintillion bytes of data and 90% of today's data was created in just the last two years. By the time you read this these figures will seem trivial.

Despite the opportunity to use new forms of information to improve products or services to consumers and citizens, this rapid explosion in data brings clear risks.

The costs associated with data losses – particularly high profile or confidential information – can be significant. Meanwhile, headlines about data security breaches often result in a dip in consumer confidence, erode share prices and can negatively impact the reputation of an organisation for many years.

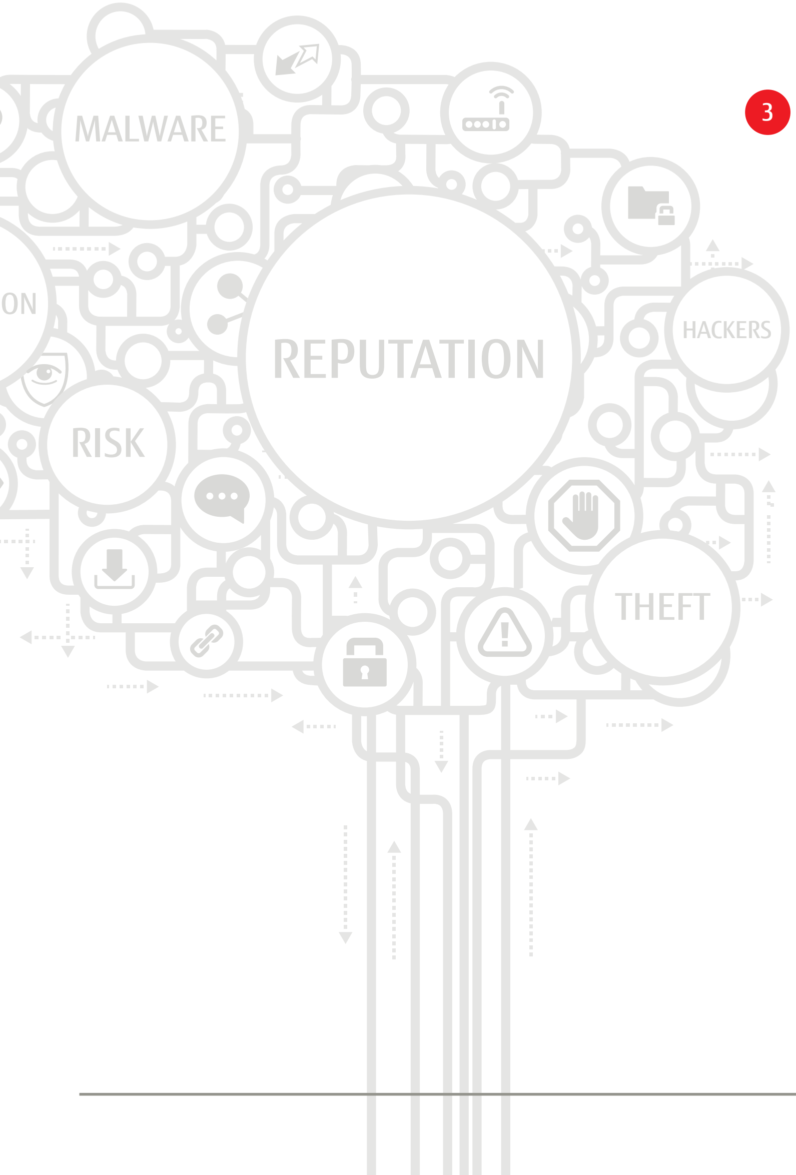
Serious security breaches

Between July 2011 and July 2012, the United Kingdom's National Health Service experienced several data breaches that exposed nearly 1.8 million patient records. A global payment processing company was hacked in June 2012, with over 1.5 million payment card details stolen. In the same year, €36 million was taken from more than 30,000 bank customers in what was dubbed the 'Eurograbber Attack'. And perhaps most worryingly of all, according to the Check Point 2013 Security Report, 54% of organisations have experienced at least one potential data loss incident.

The evidence suggests that the traditional security systems employed by enterprises – designed to deal with smaller-scale, static data – are no longer fit-for-purpose in the era of Big Data.

As streaming data adds a new, mobile dimension to data collation, storage and retrieval, there is an even greater need for flexible, ultra-responsive security systems that can meet the Big Data risks each individual organisation faces.

Where is the risk coming from?



Three key challenges stand out in the world of Big Data:

1 Organisations are not prepared for current or future data security requirements.

Old or out-dated security tools not only fail to protect one of the most valuable assets but also present their own challenges in terms of IT management. Recent lack of investment in security systems – due to economic conditions, a lack of foresight or inertia – has meant many organisations will need to modernise rapidly to catch up.

2 There are now greater threats and more opportunities for invasion of privacy. This is particularly important for organisations, from Local Government to Finance, that rely on confidentiality to deliver high-quality services. As increasing numbers of companies make a business out of mining information about individuals and their technology becomes ever more intelligent, protecting databases becomes an ongoing challenge.

3 The greater the volume of data collected, the greater the opportunity for security breaches. The amount of corporate information stored in datacentres, servers, PCs and mobile phones is growing at an exponential rate and with so many more platforms there are now multiple entry points for a cyber attack. Far from getting shorter, the list of security threats is growing and with increasing sophistication.

» Hackers' techniques are constantly changing. As these nefarious assaults become more advanced and sophisticated, security challenges are raised to new heights.«

Check Point Security Report,2013

What is the risk in my market?

The risks associated with Big Data impact every sector, every type of organisation and every element of the IT infrastructure.

In **Financial Services**, for example, firms have always collected vast amounts of market and customer data. However, with new compliance legislation and increasing sources of information, firms need to modernise systems and improve data tracking to ensure the security of large, complex datasets. Much of this must be addressed at the application layer – a field in which few firms have the requisite expertise.

For **telecommunications and media** companies, consumer confidence is everything. The bundling of broadband, mobile, internet and cable TV is leading consumers to the cloud. With cloud computing and virtual storage comes the need for better management of third party datacentre hosts.

Case in point

The impact of not protecting consumer data while it resides in storage systems was demonstrated by the hacking of 77 million Sony Playstation accounts in 2011. Sony said at the time that it lost millions, while its online gaming site was down for over a month while the company tried to recover its reputation.

In **Utilities**, the big challenge is protecting data on the move. An increasingly mobile workforce is spending less time in the office, making it essential that the applications used 'in the field' are impenetrable if devices are lost or stolen.

For **manufacturers**, the availability of low-cost data storage has opened up new holes in operational security. The vast amount of data used in design and engineering processes has facilitated the recent switch to tools such as auto-tiering. These tools do not track where data is stored, making it harder to identify if information has gone missing and affecting competitiveness.

Meanwhile, **retailers** are at risk of breaching privacy laws despite recognising the benefits Big Data can bring to their business. One estimate puts the potential increase in operating margin of the full use of Big Data at 60%[1]. However, unprotected data can have an even bigger impact on revenue if, as in the case of TK Maxx in 2006, the details of millions of customer credit card are hacked.

The **public sector** is not immune either. In the UK, the Government has already identified the need to raise the bar in IT security following high profile breaches.

Case in point

Fujitsu manages IT security for one of the UK's largest government departments. As more people use its online services, this area put the wider organisation at risk. Cyber threats occur daily, so Fujitsu's approach is to provide a layered, end-to-end security service that focuses on operational risk. The team advises on existing security needs and emerging threats from new developments such as G-Cloud. Using specialist technology partners, Fujitsu manages a security system that has become a 'business-enabler' – balancing the cost of protection against the cost of an attack.

[1] http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation

What is the technical risk?

Fujitsu and other vendors have identified the top five Big Data Vulnerability Classes. These highlight the technical challenges facing IT departments across the public and private sectors. Importantly, these five areas indicate that organisations must focus on multiple areas of the IT infrastructure – not just data storage or data inputting via devices.

Top 5 Big Data Vulnerability Classes[2]:

1. Unsecure computation

Unprotected computer programmes can offer hackers a route into accessing sensitive data, such as personal profiles or credit card details. They can also directly impact the data, corrupting mission-critical information or invoke a Denial of Service, leading to significant financial losses by blocking access to products.

2. Input validation / data filtering

Big Data is collected from an increasing number of sources and this presents organisations with two challenges:

1. Input validation: Is the data from a trustworthy source and what are the sources of untrusted data?
2. Data filtering: How can the organisation filter out rogue or malicious data?

3. Granular access control

Existing solutions for Big Data are designed for high performance and scalability with little concern for security. While traditional relational databases had comprehensive security features - in terms of access control – many Big Data solutions have not evolved to these standards.

4. Privacy preserving data mining and analytics

Big Data is typically stored at various nodes. Encryption, authorisation and authentication at each node require multi-layered security protocols. Auto-tiering – or partitioning – can reduce the costs associated with Big Data storage but queries of distributed data will require multiple entry points in a database, opening up new routes of attack.

5. Privacy preserving data mining and analytics

Using Big Data to its full capacity generally involves data mining and analytics capabilities. As soon as this data is offered up for analysis, the anonymity of the data - and potentially its source(s) - is immediately comprised. When AOL released anonymised search logs for academic purposes users were easily identified by researchers. Netflix faced a similar problem when users of their anonymised data set were identified by correlating their Netflix movie scores with IMDb scores.

[2] Source: Expanded Top Ten Big Data Security and Privacy Challenges, Cloud Security Alliance, April 2013

So how do I minimise my risk?

The bigger risks associated with Big Data require a new way of thinking. Instead of relying on previous protocols or technologies, organisations must face up to the reality of a flexible, multi-layered and ongoing approach to IT security.

There are big benefits to this approach. By analysing every aspect of Big Data, organisations will be empowered to only protect what they need to. Some systems will remain secure, some will not. Without investigating the impact of Big Data across the organisation there will always be the threat of attack.

With the ability to track, compartmentalise and evaluate everything from online purchases to the latest Twitter trending topics, Big Data offers massive opportunities for real-time intelligence through analytics and can optimise decision-making. That is why it is important to look at every layer of the organisation's Big Data solution, not just the entry or storage points. The most effective form of IT security is that which is adaptive to every layer of the IT environment.

Perhaps most important of all, recognising that standing still is no longer an option requires a change of mind-set. Once this has been achieved organisations can set about utilising technology that will actually keep pace with changes to risks in Big Data. Understanding that the cyber war should be fought on many battlegrounds and that threats are ongoing and relentless means organisations will be better placed to deal with them.

Contact us on:
Tel: +44 (0) 870 242 7998
Email: askfujitsu@uk.fujitsu.com
Web: uk.fujitsu.com