The Value of Data

A CHEAP COMMODITY OR A PRICELESS ASSET?

Trustwave®

The Value of Data

Executive Summary

Trustwave commissioned industry analyst firm Quocirca to conduct a study into the Value of Data between May and September 2017. It included a survey of 500 senior IT managers in the Australia, Canada, Japan, U.K. and U.S.

This project was conceived to examine the relative value placed on data from the perspective of different stakeholders: be they enterprise security professionals, regulators, insurers or cybercriminals. An integral part of this process is determining what that data is worth. The report attempts to answer this question and to provide guidance that can be used to help evaluate the cost of data breaches. It also looks at what data risk vigilance measures organizations have in place.

Data types: The report focuses on four basic data types: personally identifiable information (PII), payment card data (PC data), intellectual property (IP), and corporate email. It also looks at how the value of PII varies by data subject, using per capita values (PCV).

Evaluator groups: Value is not just looked at from the perspective of the data controllers that own data, but other interest groups: the criminals that steal data, those who regulate the way data is used and the insurers which underwrite it.

Data risk vigilance: The report concludes by looking at the effort put in to protecting data using a data risk vigilance score.

Key takeaways from this study include:

- U.S. security professionals value their PII data more than twice as much as their U.K. counterparts: The average PCV of PII in the U.S. is $1,820 versus $843 in the U.K. and $1,025, $1,186 and $1,040 respectively in Canada, Australia and Japan.
- Dramatic differences exist between values placed on PII data by attackers, senior IT managers, insurers and regulators. The mean PCV placed on a PII record by cyber criminals is $39 compared to $1,198 by senior IT managers, $3,211 for insurers and $8,118 for regulators.
- Different levels of priority are attributed to different data types such as PII, IP, PC data and email. PII is given a higher priority than IP data and corporate email comes last.
- Industry sector influences the type of data that is given highest priority. Healthcare and hospitality prioritize PII data, while industrial and IT/communications companies rank IP as most important.
- Shareholder data and patient data are the most valuable data subjects. Shareholder data is most highly valued by businesses at more than $1,700 per record, followed by patient records with a mean value of more than $1,500 and consumers at just over $1,000 per record. Lowest ranked are contractors at just under $600 per record.
- Patient data is the most rigorously risk assessed. Nearly 80% of organizations seeing patients as their prime data subject said they had carried out a comprehensive risk assessment, more than for any other data subject. In the U.K., where health care is largely controlled by the government through the National Health Service (NHS), this rose to 90% and in the U.S., where requirements are tightly governed through the Health Insurance Portability and Accountability Act (HIPAA), to 85%.
- Certain types of PII are much less rigorously risk assessed: Contractors and supplier PII data is less likely to be assessed than patient data. Forty five percent of companies holding contractor's private data and 42% holding supplier's data failed to conduct comprehensive risk assessments.
- Corporate security and risk professionals over-estimate the value of PII data for sale on the black market. Overall criminal resale values for PII are less than 5% of the value that senior IT manager estimate them to be worth. For a payment card record, senior IT managers over-estimate by 60 times the actual criminal values of data for sale on the black market. For a single banking record, it is 2,000 times.
- "Data risk vigilance" is highest among Canadian firms and lowest among Australian businesses with the U.K. in the middle. Financial companies and IT/communications companies were the highest scoring verticals and hospitality and retail the lowest.

The Data Value Stakeholders

The value of data varies widely depending on the evaluator group:

Data controllers (the organizations that own and have responsibility for data) must find a value that both reflects the profit data can bring to their business and covers the risk of its compromise. Both vary depending on the type of data.

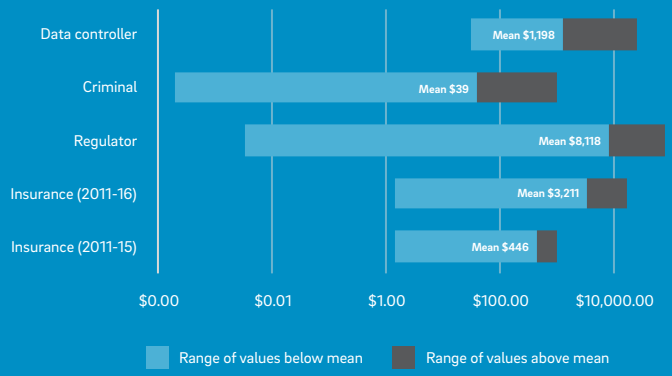
Those that steal data – be they **criminals** who hunt down PII or unscrupulous nation states and other businesses that steal IP – must see a benefit that makes their effort and risk worthwhile. The return needed is often very little, as the risk taken is small.

Regulators must protect the interests of data subjects (the likes of you and me) about which data is stored, while not imposing fines that undermine the productivity of the markets they govern.

Insurers must offer premiums that are attractive to buy while covering the shared risk of policy holders.

Figure 1 shows the value ranges for PII for these evaluator groups using per capita value of a unit for comparison (see next page, **Valuing PII**).

Figure 1: Estimating per capita value ranges for PII by evaluator group (see valuing PII)



Data Types and Units of Value

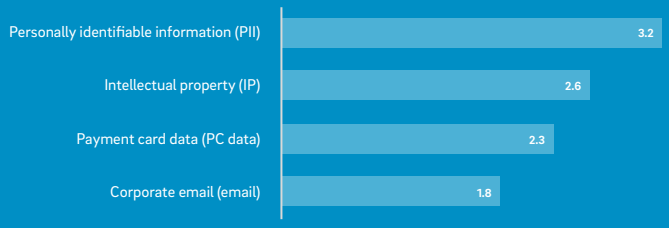
Different types of data may be involved in any given data breach. For example, the targeting of a point-of-sales device may involve exclusively PC data, whereas the theft of a laptop may involve PII, email and IP.

Respondents were asked to rate four basic data types in order of priority. Each data type could then be assigned an overall average priority score (Figure 2). PII was ranked highest, followed by IP, PC data and email. All organizations store PII and IP of some sort and all must deal with email, although email is given the lowest priority. However, only a subset deal with PC data.

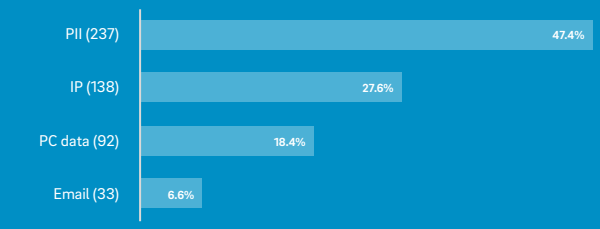
The data type ranked first by each organization has been termed its **prime data type**. 47.4% selected PII, 27.6% IP, 18.4% PC data, and 6.6% email (Figure 2). Different data types matter more in certain industries: PII is given the highest priority in health care (3.5) and hospitality (3.4) and least in industrial (2.9), while IP was given the highest priority in industrial (3.0) and IT and comms (2.9) IP was lowest in hospitality (2.4) and financial services (2.4).

Among the different countries, scoring was closer (Figure 3). Japan rated PII highest priority (3.4) and the U.K. and Canada ranked it lowest (both 3.1). Japan also rated IP highest (2.9), Australia and the U.S. ranked IP lowest (both 2.4). Japan can only place highest priority on both PII and IP, as it gives such a low priority to PC data (1.8) compared to the overall average of 2.3 (see box).

Figure 2: Ranking of main data types
All 500 respondents



Priority Score: each respondent ranked four basic data types from highest to lowest priority for their organization. The mean score for each is out of 4. If all respondents had ranked PII highest it would have scored 4, if all had ranked email lowest it would have scored 1.



Prime data type: Percent ranking a given data type as highest priority for their organization

Payment Card Data

PC data took third place when it came to the priority given to the four main data types. However, whereas all organizations deal with PII, IP and email, not all organizations deal with PC data. Japan gives PC data the lowest priority, perhaps reflecting that is has its own payments brand (JCB) and a language that is harder for criminals to penetrate than English (the primary language of the other markets surveyed).

PC data is highly controlled via the Payment Card Industry Data Security Standard (PCI DSS), and many organizations choose to outsource processing to payment service providers to avoid direct responsibility. Those that keep PC data in house, have the highest data risk vigilance score (see below **Data risk vigilance**).

Valuing PII

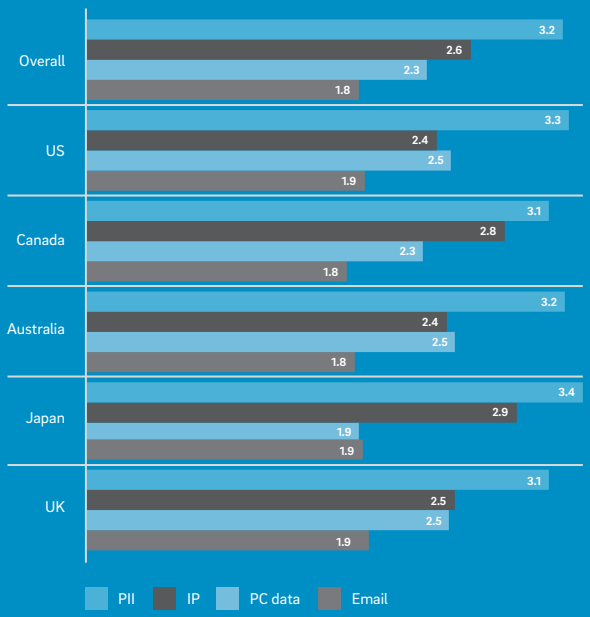
The challenge with the comparative valuing of data is to establish a unit of value. For PII, there is an established approach termed **per capita value** (PCV) [Ref 1].

A top-down approach to PCV takes the overall value of a set of records and divides that value by the number of records. For example, if the social media details of 10,000 people are sold by a criminal for $500, then the PCV is $500/10,000 or five cents per record.

The value of data varies depending on the evaluator. Figure 1 summarizes the range of PCVs for PII uncovered for this report from the perspective of the four evaluator groups. More detail on these follows, however, it is clear criminals consider PII a cheap tradable commodity compared to the higher values placed on it by data controllers, regulators and insurers.

> *"Criminals consider PII a cheap tradable commodity"*

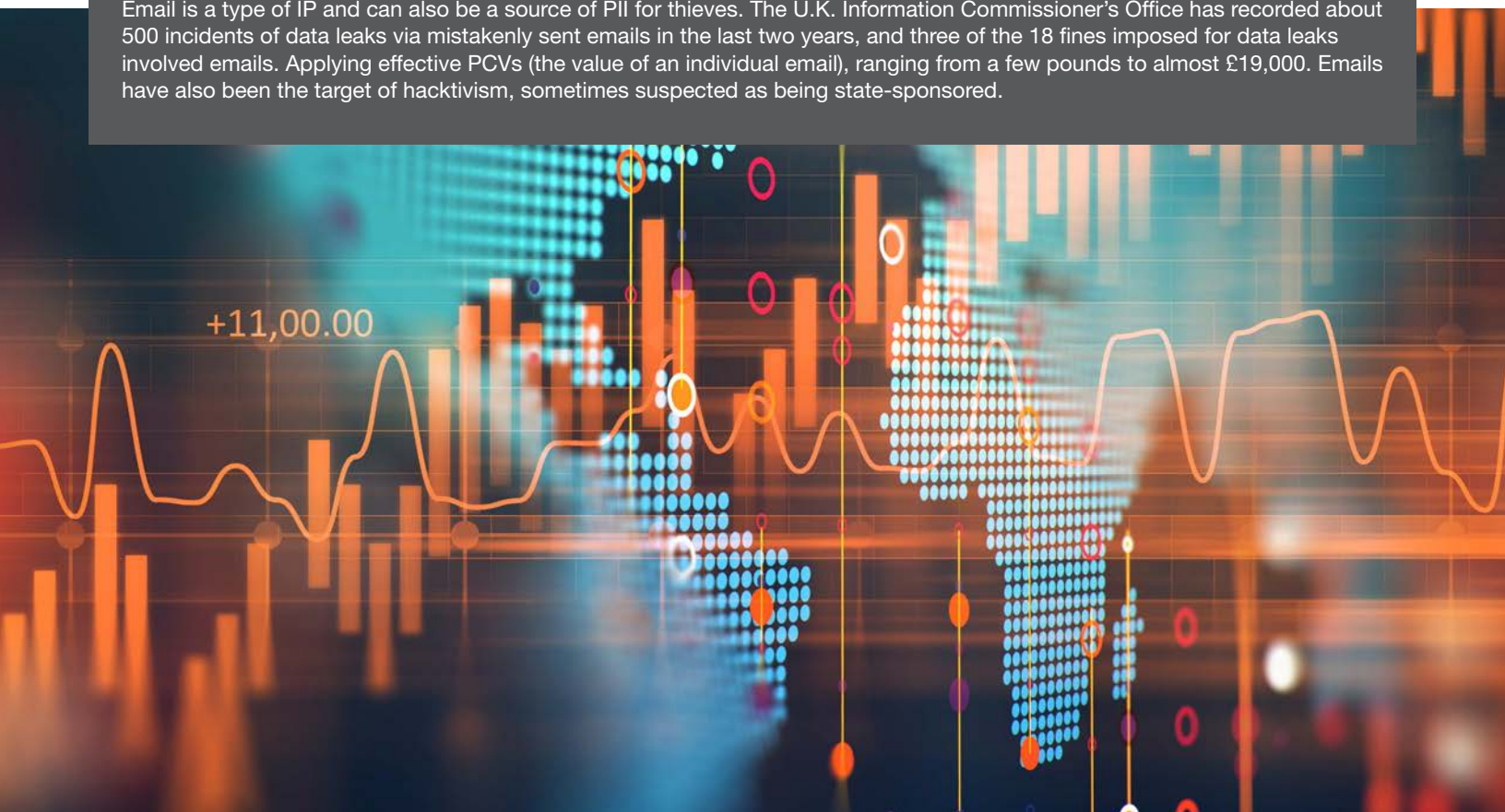
Figure 3: Ranking of main data types by country



Corporate Email

Email is given the lowest priority, despite its high profile in many data leaks. Perhaps – because email is so ubiquitous and hard to control – organizations have almost given up.

Email is a type of IP and can also be a source of PII for thieves. The U.K. Information Commissioner's Office has recorded about 500 incidents of data leaks via mistakenly sent emails in the last two years, and three of the 18 fines imposed for data leaks involved emails. Applying effective PCVs (the value of an individual email), ranging from a few pounds to almost £19,000. Emails have also been the target of hacktivism, sometimes suspected as being state-sponsored.



The Value Data Controllers Place on Data

Figure 4 shows the range of estimated values for PII provided by data controllers. In the U.S., both the highest and lowest PCVs were placed on PII. This may reflect two things about the U.S: the global scale of some of its companies, which store data on so many data subjects that the value placed on an individual is bound to be low. Conversely, the high values may reflect the potential legal costs of data compromise, which will drive PCV estimates up when data volumes are low.

There is a lot of variety within the PII data category. This is best understood by looking at the data subjects for which PII is stored. All organizations hold PII on at least one type of data subject (Figure 5). Employees are the most common data subject stored by 80% of organizations.

> *"The days when the privacy of any data subject can be ignored are numbered"*

It is perhaps surprising that 20% of respondents say they do not store data about employees. This is likely attributable to the use of outsourced human resources services. However, the ultimate responsibility for PII lies with data controllers and not the data processors to which they outsource.

You might expect that risk assessments were carried out to address this responsibility. Too often this is not the case (Figure 6). Only 70% of organizations that store employee PII have carried out a comprehensive risk assessment. This rises to 79% for patients and consumers, but drops to 55% for contractors. All are protected under regulations such as the EU GDPR, which even considers IP addresses and telephone numbers as PII. The days when the privacy of any data subject can be ignored are numbered.

Figure 4: Ranges of estimated per capita values of PII by country

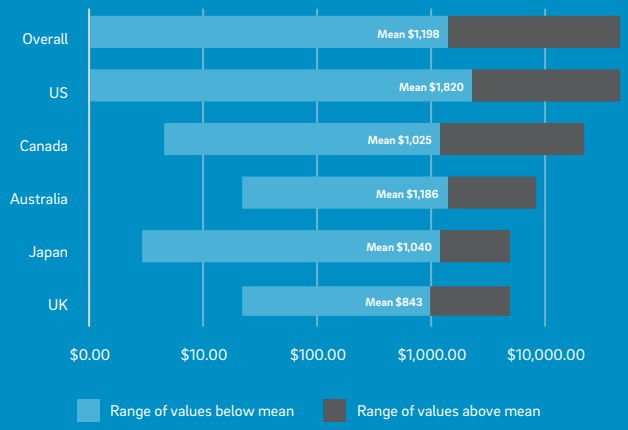


Figure 5: Percentage storing data on data subjects All 500 respondents

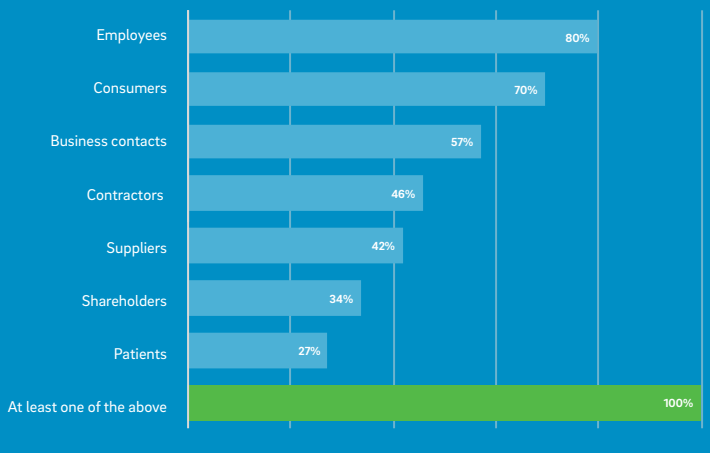


Figure 6: Percent storing data on a given data subject that have conducted a comprehensive risk assessment

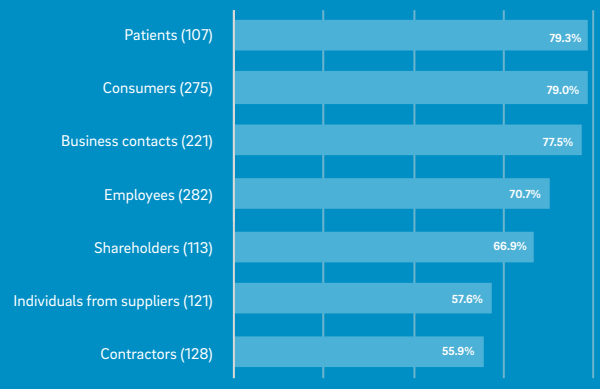
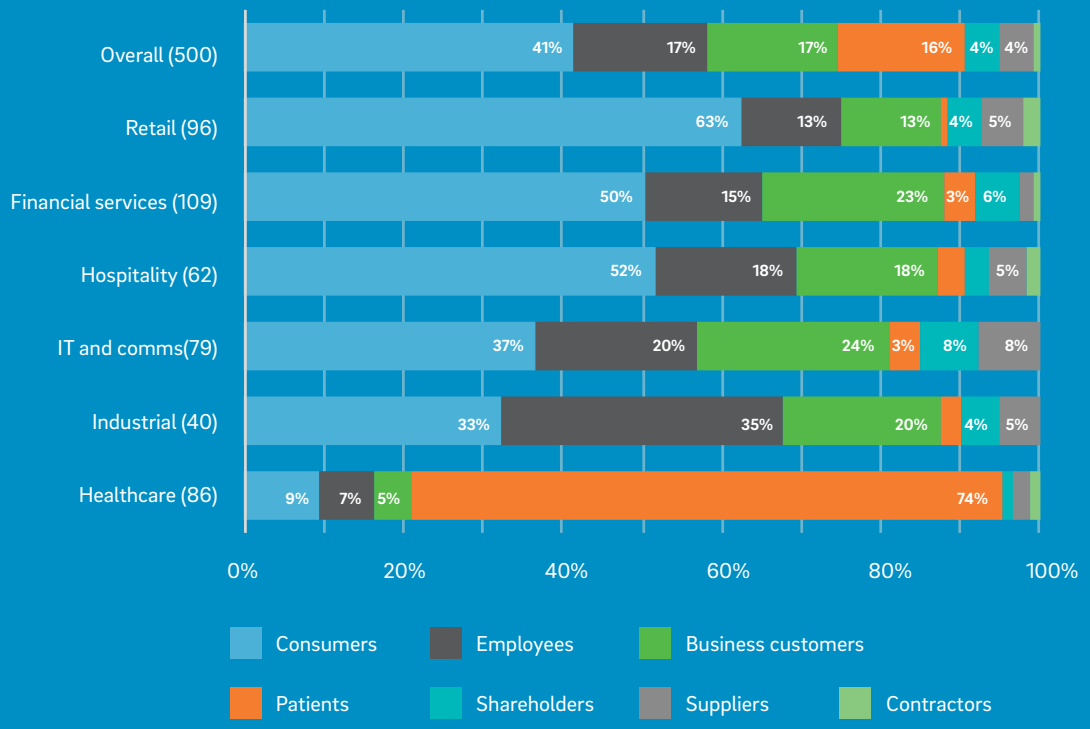


Figure 7: Prime data subjects, those of greatest concern reguarding business damage caused if their data was stolen

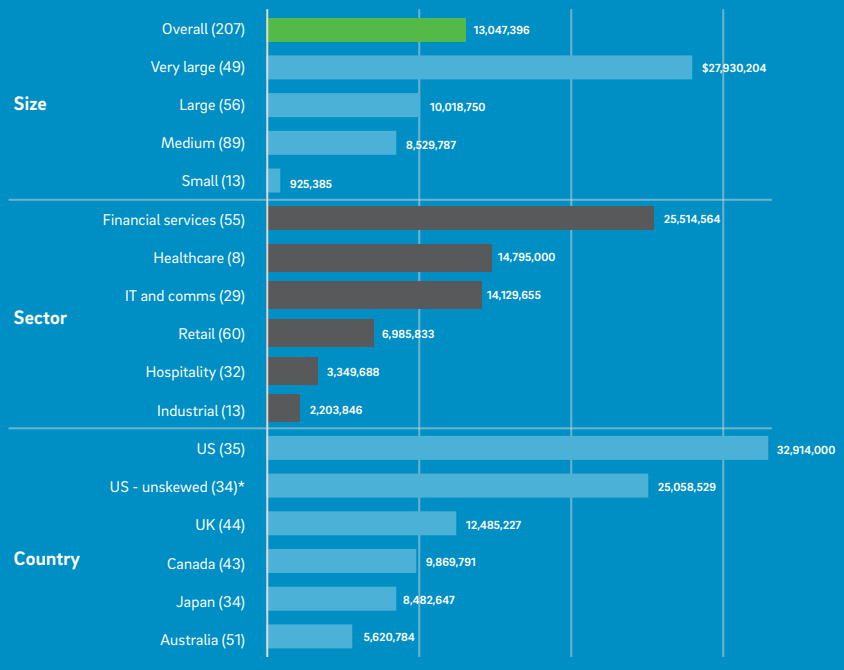


Each respondent was asked to select the data subject about which it had greatest concern regarding the damage that would be caused if PII of the data subject was leaked. This is termed its **prime data subject** (Figure 7). Consumers are the most common prime data subject (41%). This was also the case in most of the main sectors covered: retail, financial services, IT and comms. In health care, patients dominate (see box). Just 1% selected contractors as their prime data subject.

The volume of consumer PII data stored by country varies dramatically. U.S. organizations store twice as much as any other country, even higher if one extreme value is not eliminated (Figure 8). This will be partly down to the scale of the U.S. market (the data does not cover China and India, the most populous countries), but also due the global scale at which some U.S. organizations operate, especially in areas such as social media and online retail.

The size, and therefore value, of data sets is not just a function of the number of records, but the information each contains. A data subject record consists of attributes: family name, date-of-birth, Social Security number, mother's maiden name are all examples. An average of 49 attributes are held for each prime data subject (Figure 9). This rises to 74 for patients and drops to 18 for contractors.

Figure 8: Mean number of consumer PII records held where prime data subject is consumers



*A large US financial services organization had data for 300 million consumers. If this is taken out (unskewed), US organizations still have the most consumer data.

This richness of information is part of the reason patient records are considered some of the most valuable, being assigned an estimated mean PCV of $1,546 (Figure 10). This is just behind shareholders, which come highest at $1,725, and ahead of consumers at $1,054. Lowest ranked are contractors at $596, although the small sample size of just five must be noted.

Considering all prime data subjects together, the U.S. estimates a far higher mean PCV than other countries (Figure 10). The U.K. has the lowest mean value although, as the data is reported in U.S. dollars, using mid-2017 exchange rates, U.K. data may be reflecting the 20% devaluation of the pound during the preceding 12 months.

If the variation in the value of PII varies depending on the data subjects involved, this is nothing compared to the range of values assigned to items of IP, which are stored by all organizations in one form or another (Figure 11). As with employee data in the PII category, it may be surprising that only 66% of organizations say they store email. However, the management of email is also commonly outsourced.

> *"U.S. estimates a far higher mean value per record than other countries"*

Health Care and Patients as Data Subjects

Unsurprisingly, patients are the prime data subjects for health care organizations (Figure 7). However, patients are also the prime data subjects for some in financial services (e.g. companies that sell medical insurance), retail (e.g. pharmacies), hospitality (e.g. care homes and private healthcare) and industrial (e.g. clinical trials of medical equipment). Patient data is seen as a good source of PII, as so many attributes are stored (Figure 9) and the data is more likely to be accurate (people are less likely to lie about things, such as their date of birth, to a health care provider then they are, for instance, to a social media company).

Seventy-nine percent of organizations seeing patients as their prime data subject said they had carried out a comprehensive risk assessment (Figure 6), more than for any other data subject. In the U.K., where health care is largely controlled by the government through the National Health Service (NHS), this rose to 90% and in the U.S., where regulation is tight via HIPAA, to 85%.

Figure 9: Mean number of attributes held for each individual for an organization's prime data subject

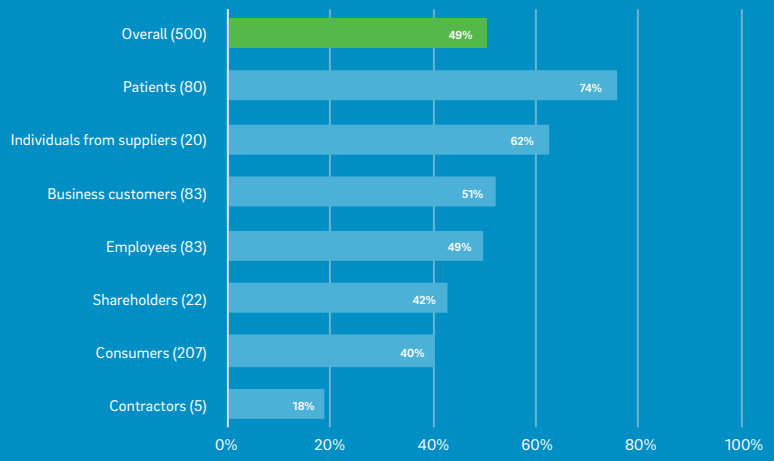
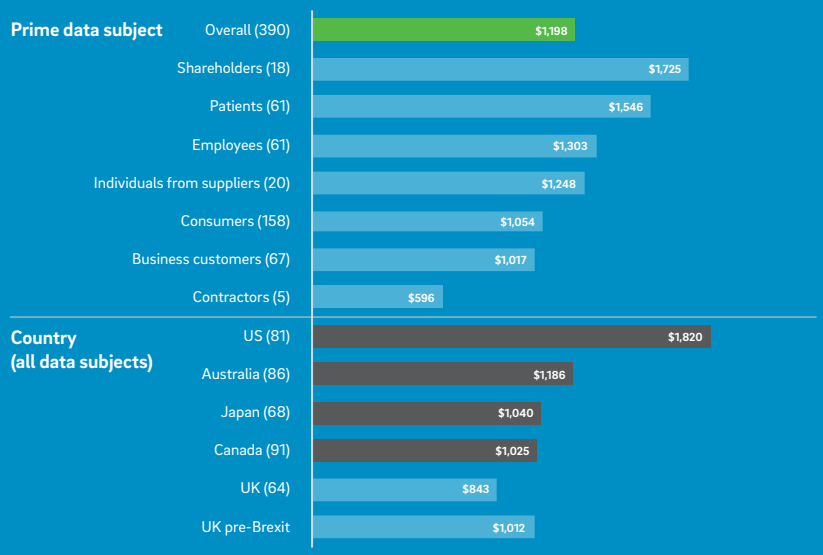


Figure 10: Mean value estimates for prime data subject records 110/500 respondents were unable to estimate a value



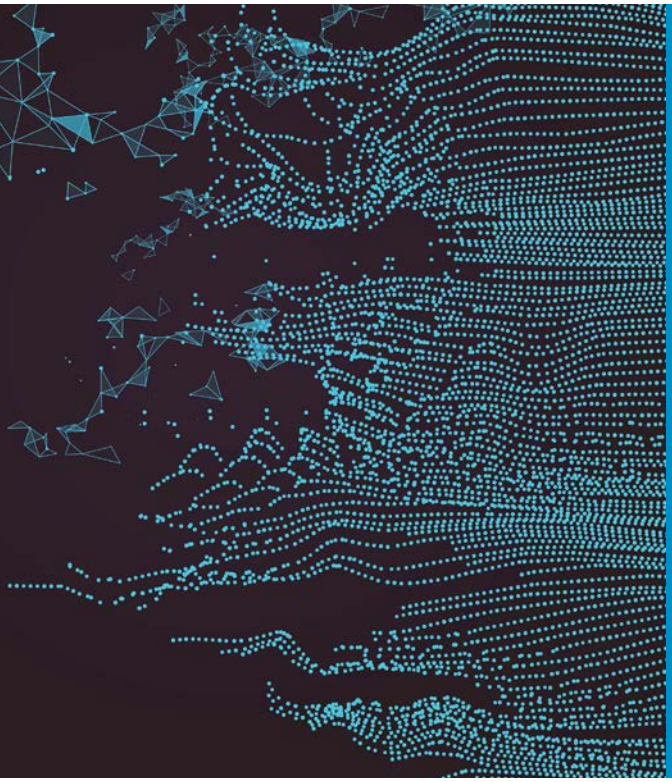
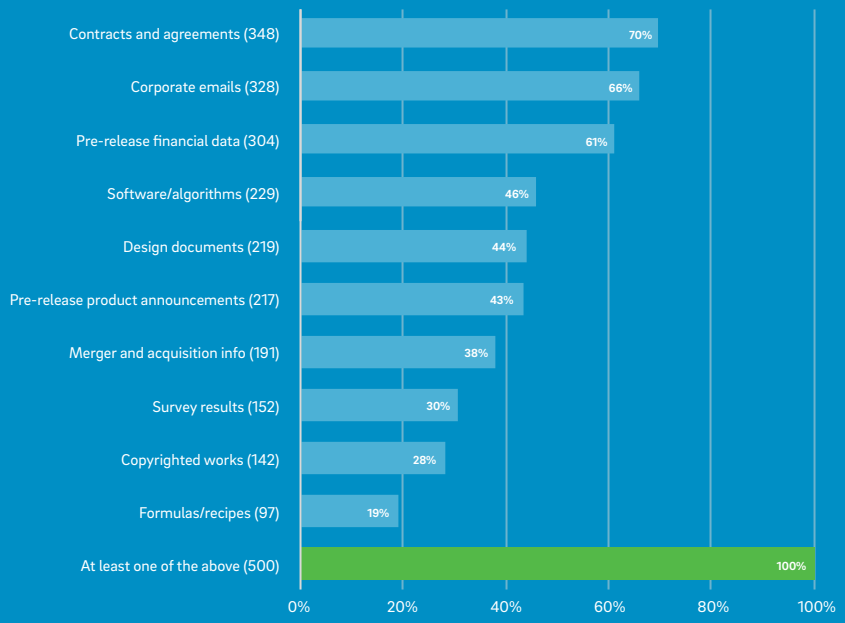


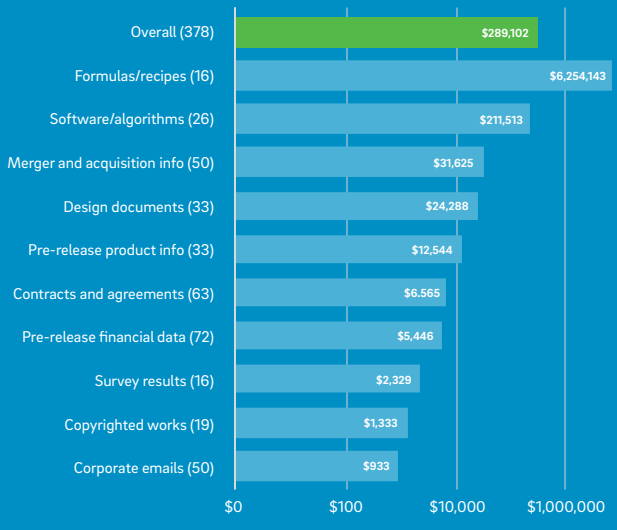
Figure 11: Percent saying they hold a given category of intellectual property



Each respondent was asked to select the one type of IP stored by their organization that would cause more damage than any other if it was compromised. This was termed their prime IP type, for which they were asked to estimate the value of an individual item. The values assigned to prime IP types may reflect that of an individual file or email, or of an unreleased song or film or secret formula. However, many copies of each of the latter are stored (the compromise of one copy compromising all).

Seventy-six percent of respondents felt they could provide estimates for the value of an item of their organization's prime IP type (Figure 12). Five percent gave extreme values of more than $5,000 per item, including a U.S. private health care company valuing a formula at $100 million and, in financial services, a U.S. company valuing an algorithm at $5 million, and a U.K. company valuing merger and acquisition information at $1.2 million. These figures reflect the views of the senior IT professionals interviewed. They may be underestimating the value of IP to their business. Some estimates suggest that, from the data controller's perspective, the value of IP can be up to 80% of any given business [Ref 2].

Figure 12: Mean values for items of prime IP type
378 out of 500 respondents were able to estimate values



Criminal Value of Data

The values assigned to PII by data controllers are always going to be estimates. However, when it comes to value placed on data in criminal circles, absolute value ranges can be ascertained by visiting the markets where the data is traded. These can be found on both the hidden dark web and the public internet (see appendix 1).

Sale values range widely (Figure 13). For example, for PC data, one of the most widely sought data types, criminal PCVs range between five cents and $18. This reflects both the quality and volume. An old file containing millions of out-of-date payment card details will be much cheaper than a small set of up-to-date and validated records. In line with earlier findings, health care records attract some of the highest prices, with PCVs ranging from $5 to almost $1,000, the highest values could be for the health record of a targeted individual.

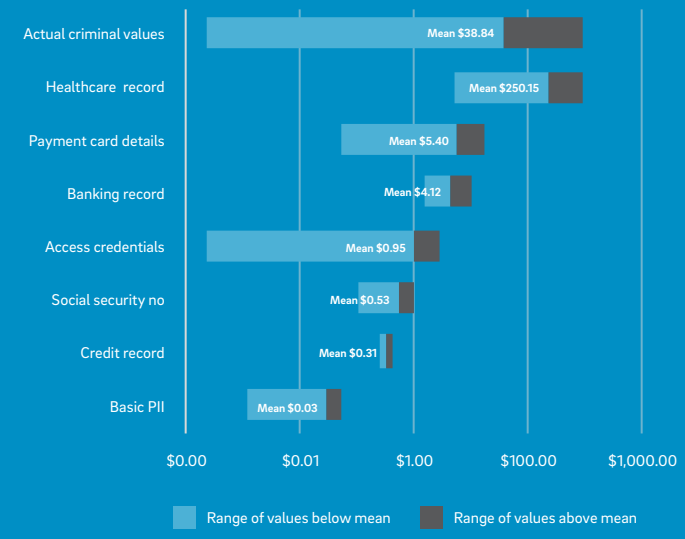
What is clear from this data, and those presented in Figure 1, is that overall criminal resale values for PII are less than 5% of the value data controllers place on their own data. Furthermore, data controllers have little idea their PII records are being sold so cheaply. Their own estimates of criminal resale values are much closer to their own valuations than reality (Figure 14). For a payment card record, data controller estimates averaged out at around 60 times the actual criminal values. For a single banking record, it is 2,000 times.

The motives and aims of those who steal IP are often different to the short-term financial gain sought by those that steal PII and PC data, although certain copyrighted materials, such as music, video and software may be stolen to sell black market copies.

Other IP thieves have longer-term or non-financial objectives. Nation-states steal IP to advance their technological prowess. Companies steal each other's IP (industrial espionage) to better their competitive position. Hacktivists steal IP to undermine the ongoing business of targets. This variety of motives makes it hard to place an objective value on a single item of IP.

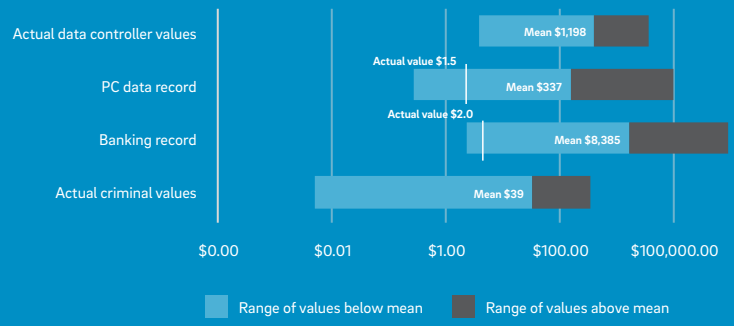
The cost to the organizations targeted can be huge. For example, new drug formulas or machine designs, with years of time and millions of dollars invested in them, may end up in the hands of competitors in a few seconds. A mining organization may have spent years developing a natural resource, only to be outbid by an unscrupulous competitor with stolen copies of bids. One author has described IP theft as "the greatest transfer of information in history" [Ref 3].

Figure 13: Actual black market per capita value ranges for selected PII data types



> *"Health care records attract some of the highest prices"*

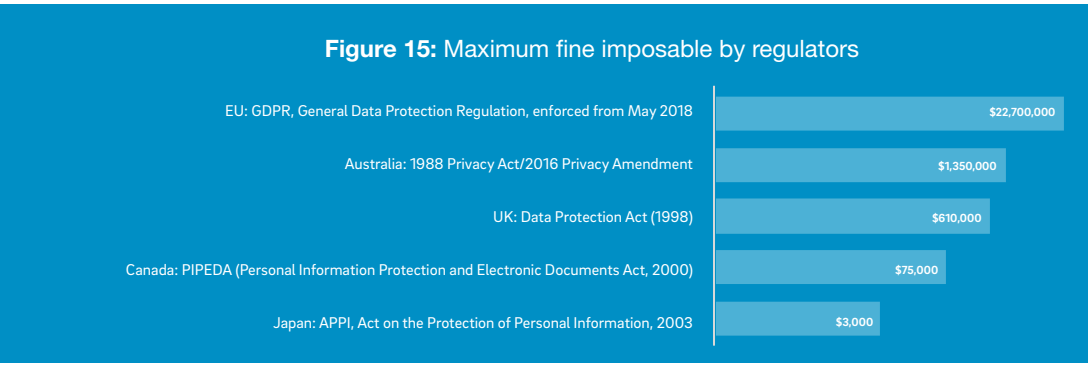
Figure 14: Estimated per capita value of data on black market



Regulator Value of Data

Regulators focus primarily on PII rather than IP, although there are times when the latter does concern them. The standard for PII regulation is being set in the European Union (EU), where a new regulation, the General Data Protection Regulation (GDPR), is set to be enforced in May 2018. GDPR applies to any organization processing and storing data regarding EU citizens, even if it is situated outside the EU. GDPR will have the highest fines by far (Figure 15). Looked at through maximum fines, the EU is placing a value on PII thousands of times higher than Japan.

Figure 15: Maximum fine imposable by regulators



> *"The standard for PII regulation is being set in the EU"*

The U.S. is not included in Figure 15 because it has multiple existing data protection regimes. Federal and state privacy regulations are enforced by a network of federal agencies, federal prosecutors, state regulators and private plaintiffs. Compensation for impacted data subjects following privacy violations is often settled by state attorneys general cooperating in joint enforcement actions. Some of the estimates for the total of settlements reached for cases to date have been substantial.

The Office of the Australian Information Commissioner (OAIC) implements the 1988 Privacy Act, recently modified by the Privacy Amendment (Notifiable Data Breaches) Bill 2016. The maximum penalty of 1,800,000 AUD that can now be imposed on businesses makes Australia potentially one of the most expensive places after the EU to sustain a data breach. That said, the highest fine for an incident to date has been 23,000 AUD [Ref 4], and many of the cases brought by OAIC have been on behalf of individuals. Plus, the total numbers impacted are often not on record, making it hard to calculate PCVs.

> *"The average fine imposed by the U.K. ICO for a data leak in the last two years was £114,000"*

In Canada, enforcement is conducted via the Personal Information Protection and Electronic Documents Act, 2000 (PIPEDA), and private sector legislation in British Columbia and Alberta. The maximum fine imposable on a business is Canadian $100,000. Quebec has separate legislation, with a maximum fine of Canadian $50,000. There have been 598 investigations into businesses for the handling of PII since 2001 [Ref 5].

In Japan, the Personal Information Protection Commission (PPC) enforces the Act on the Protection of Personal Information, 2003 (APPI). Business operators are subject to a maximum fine of just Yen 300,000.

Of the countries covered in this report, the U.K. is of interest for two reasons. First the U.K. Information Commissioner's Office (ICO) publishes all the fines it has imposed, often with the number of data subjects impacted, allowing PCVs to be calculated [Ref 6]. Secondly, the U.K. will be subject to GDPR, as the government is implementing the regulation despite the U.K.'s pending departure from the EU. The ICO's enforcement of the current U.K. Data Protection Act, 1998 (DPA), which is based on the existing EU Data Protection Directive, 1995, provides precedents for GDPR enforcement. The U.K. ICO also enforces the Privacy in Electronic Communications Regulations (PECR), 2003, based on the EU Privacy and Electronic Communications Directive, 2002.

The U.K. ICO can issue enforcement notices, undertakings and monetary penalties, and bring prosecutions against individuals. Since June 2015, the ICO has had about 4,000 leaks reported to it, but only taken a little over 215 enforcement actions, 95 of which involved fines. More than half of the fines were issued under PECR for unsolicited communications. Others were for misuse of data, and only around 18 fines are clearly associated with data leaks.

The average fine imposed by the U.K. ICO for a data leak in the last two years was £114,000, 23% of the maximum fine of £500,000. The biggest fine was £400,000 to a telecoms provider for the leak of 156,959 customer records stolen, implying a PCV of £2.55. However, the range of regulatory PCVs for all the leaks imposed so far ranges from £2.28 to £64,000, the high fine being the serious compromise of a single individual's privacy. The ICO is influenced more by the sensitive nature or the records leaked than the volume of data or any other criteria.

IP is regulated in certain circumstances, and in others its compromise may attract legal actions. For public companies, in the U.S. pre-release financial data could be used to manipulate stock trades and is regulated by bodies such as the Securities and Exchange Commission (SEC). As evidenced, merger and acquisition data can be sensitive, and a deal compromised by a leak could lead to legal action by an aggrieved party. Governments are also acting to protect business from the onslaught of IP theft with legislation such as the U.S. Defend Trade Secrets Act and European Union's Trade Secrets Directive.

Insurer Value of Data

Insurance companies do not go out of their way to publicize the premiums they charge. An application process is required, and the payments they make are not published. However, there is a detailed 2016 report based on 183 reported claims (mainly in U.S.) from cyber risk management firm NetDiligence [Ref 7], which looks at insurance payouts for incidents involving PII.

The mean PCV paid for claims in 2016 was more than $17,000, while the median was just under $40. This difference is due to some very high compensation in 2016 for breaches involving just a few data subjects. In the previous years, the mean value for pay-outs was less than $1,000, which is why there are two lines for insurance on Figure 1, the first pre-2016 and second including 2016.

Data Risk Vigilance

The more value that is placed on something, the more it might be expected that vigilance would be put in to caring for it. The final part of this report looks at data risk vigilance, the measures organizations put in place to care for their data.

Respondents assessed their organization's data risk vigilance across ten factors – four relating directly to risk, four to data value assessments and two to the impact of data theft (Figure 16). The most attention is paid to the value of data. Organizations are least likely to have an in-depth understanding of issues relating to external agencies, such as who might steal their data, the value of data to would-be thieves and the cost of cyber insurance. Rather than looking at all 10 factors separately, it is convenient to combine them to create data risk vigilance scores.

Figure 16: Assessment of ten factors to prime data type (all 500 respondents)

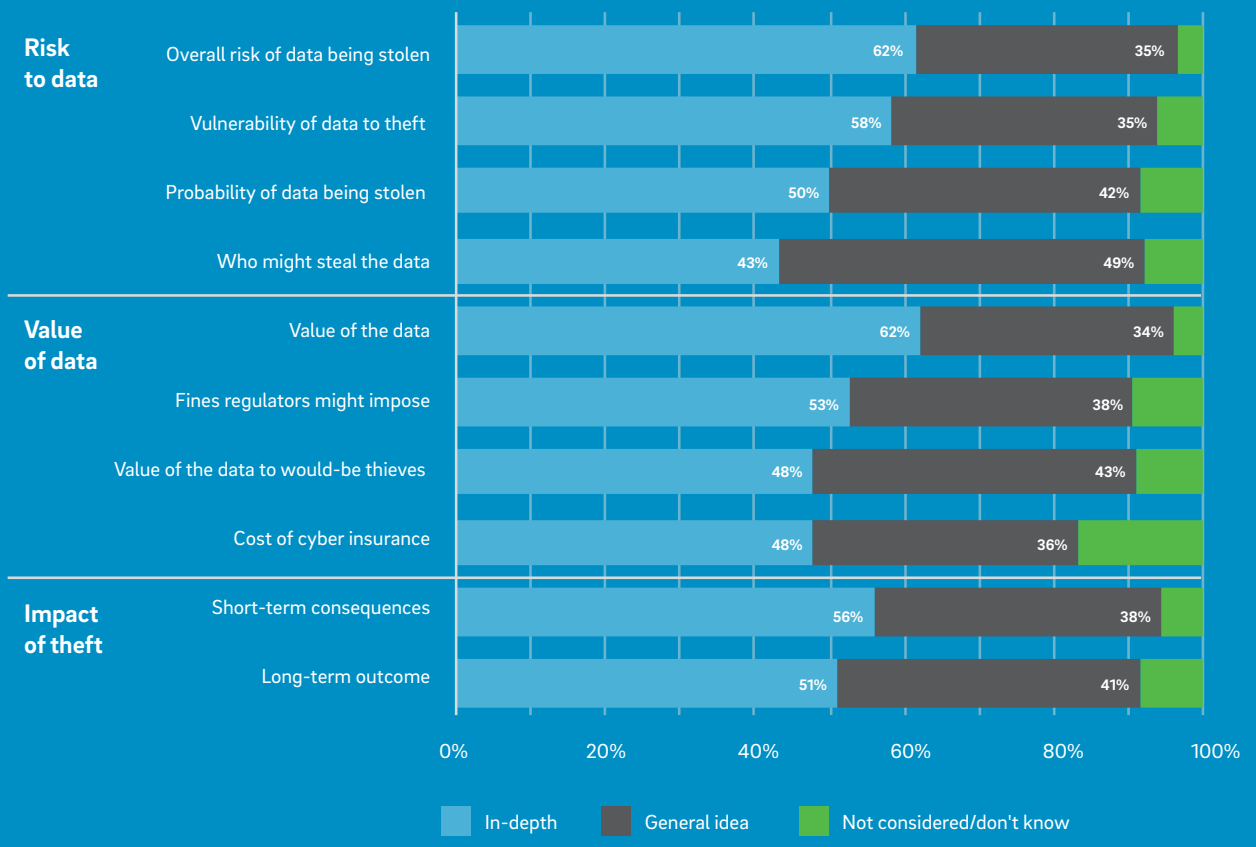


Figure 17 shows the average data risk vigilance scores. For prime data types, PC data had the highest score (14.8), just ahead of PII (14.7) and IP (14.4). Email was relatively neglected with a score of 13.0. It may well be that the 6.6% of organizations that see email as their prime data type are not very data-focussed in the first place, so email defaults as their prime data type in the absence of any other and, as such, their data risk vigilance is generally poor.

> *"Organizations are least likely to have an in-depth understanding of issues relating to external agencies, such as who might steal their data, the value of data to would be thieves and the cost of cyber insurance"*

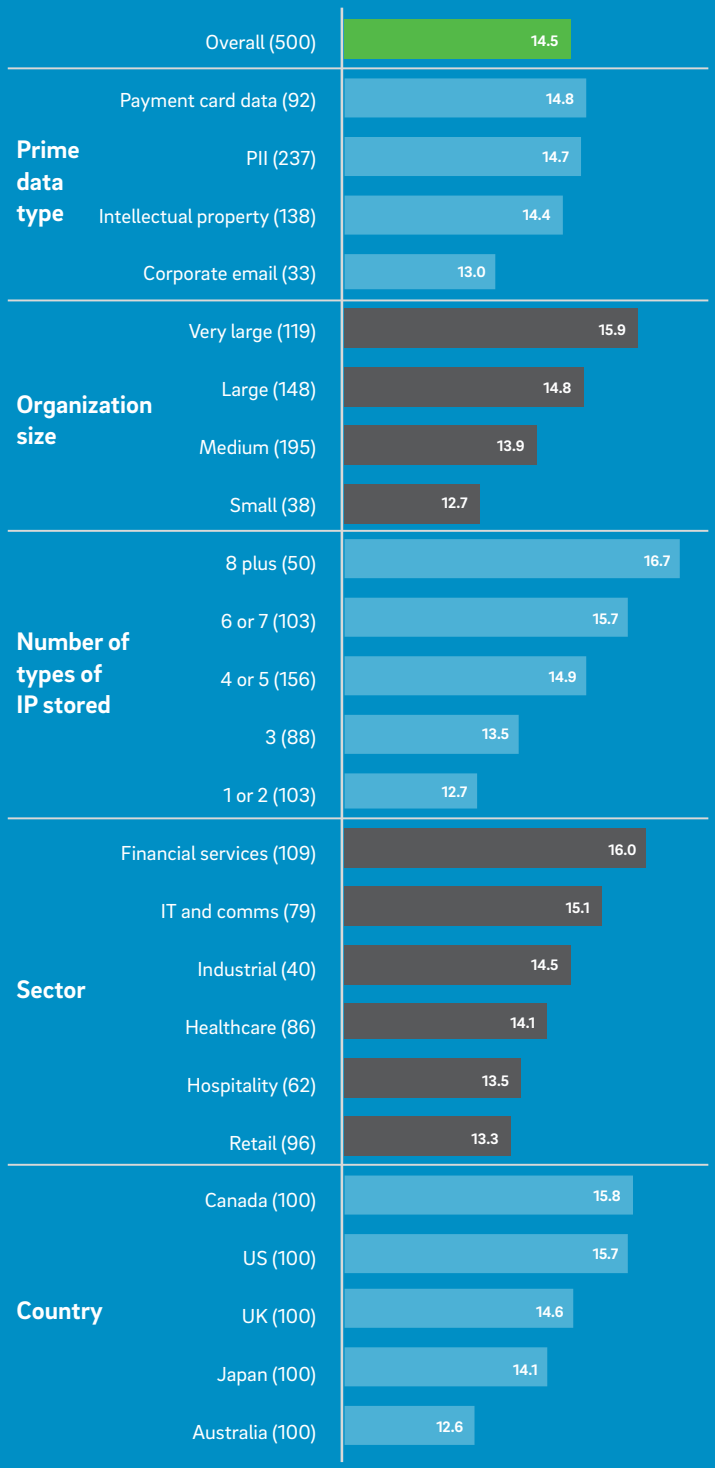
Large organizations are more vigilant than their smaller counterparts, as they are more attractive targets for criminals, face more regulation and, perhaps, are more likely to be investigated. They will also be more likely to receive press scrutiny when incidents occur and less likely to get a sympathetic hearing from regulators. All this, along with bigger budgets and more resources, lead to greater investment in data protection measures.

> *"Those dealing with eight or more types of IP were considerably more vigilant than those dealing with just a few"*

It also seems that the more complex the data stored by an organization, the more vigilant it is. Those dealing with eight or more types of IP were more vigilant than those dealing with just a few – which will be mainly the email and contracts that all organizations must handle.

Retail and hospitality had the lowest data risk vigilance score compared to other sectors, which is worrying given the amount of consumer data they handle and store. Financial services had the highest scores, which is gratifying given the sensitive nature of the data they process. The U.S. and Canada had higher scores than other countries, and Australia and Japan earned the lowest (although in both samples there were a disproportionate number of small companies).

Figure 17: Data risk vigilance scores



Data risk vigilance score: each respondent was asked to gauge their assessment of the risk posed in their organization's data for each of ten factors. Scoring 2 for an in-depth assessment, 1 for a general idea and 0 for not considered or don't know enables the calculation of a data risk vigilance score. The maximum score is 20 (10 times 2) and minimum score is 0.

Conclusion

Data is transforming businesses in the early 21st century in the same way electricity did at the start of the 20th. For nearly all businesses, PII and IP are essential assets that are enticing targets for criminals, but those storing PC data are the most tempting target of all.

Data subjects are becoming more aware of the value their data has to the businesses they deal with and are less forgiving when things go wrong. Meanwhile, even as one data breach is eclipsed by another in the eye of the press, regulators continue to investigate serious incidents as they are invested with more powers and the clout to issue ever greater fines.

As businesses in Europe confront the prospect of complying with more rigorous data privacy laws with the EU General Data Protection Regulation coming into force in May 2018, many businesses are being obliged to take stock of the personal data they are responsible for and assess how to manage the risk associated with it. What is only too apparent is that no organization can afford to neglect its data. All need to keep improving their levels of data risk vigilance to stay ahead in the data value race.

> *"For nearly all businesses their PII and IP are essential assets that are enticing targets for criminals"*

Recommendations

The following are Trustwave's key takeaways and recommendations to consider in the context of assessing data risk and protecting against compromise:

- Establishing a risk baseline for all data residing within your organization is an essential first step because you can't defend against what you don't know. As the cybersecurity landscape continues to rapidly evolve in terms of attack sophistication, as well as new regulations and compliance standards, a preliminary risk assessment will give you a comprehensive picture on the likelihood of an incident. This assessment should also include factors such as third-party vendor access to internal systems and prevalence of bring-your-own-device (BYOD).
- Make email protection a priority. Email remains a primary channel to wage ransomware, phishing and other malicious campaigns that can quickly cripple an organization. In addition, valuable intel such as contracts, vendor records, confidential conversations and access to corporate social accounts can all be gleaned through email and are attractive to cybercriminals. All email should be protected bidirectionally through secure email gateways complete with the latest signatures to block malicious attempts.
- Continuous testing is paramount. Security is not a "set it and forget it" affair. It is ongoing and fluid. Organizations must rigorously test their networks, applications and repositories of sensitive or confidential information for vulnerabilities that could result in loss of data or a failure to meet compliance objectives.
- Managed security services can help fill the gap. Organizations should consider leveraging the benefits of managed security to augment the responsiveness and remediation capabilities of their internal security teams. Having on-demand access to the latest threat intelligence, coupled with the ability to dynamically scale resources when needed, is both practical and cost effective.
- Create a cybersecurity culture. Your weakest link to protecting data and intellectual property will always be the user. The latest in cutting-edge firewalls or intrusion detection systems are no match against an employee easily duped into giving out passwords or clicking on a malicious link. Creating a cybersecurity-minded culture should be high priority for all organizations and driven from the top-down, starting with CEO. Established processes and procedures paired with annual training can help prevent a great percentage of breaches and substantially reduce overall organizational risk in the process.

Appendix 1 – References

References for secondary sources used in the report:

1. IBM/Ponemon, Cost of Data Breach Study, 2017
   https://www.ibm.com/security/data-breach/
2. Lexicology.com
   https://www.lexology.com/library/detail.aspx?g=6f7dd161-e101-4809-9cb6-af37b853aae8
3. Corera, Gordon. Intercept: The Secret History of Computers and Spies, Orion, 2015
4. OAIC.gov.au
   https://www.oaic.gov.au/privacy-law/determinations/
5. priv.gc.ca
   https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/
6. ico.org. U.K.
   https://ico.org.uk/action-weve-taken/enforcement/
7. Net Diligence, 2016, Cyber Claims Study
   https://netdiligence.com/wp-content/uploads/2016/10/P02_NetDiligence-2016-Cyber-Claims-Study-ONLINE.pdf

Sources of criminal data values

- Various sources were used for the criminal value of data
- Cambridge Centre for Risk Studies, Managing Cyber Insurance Accumulation, Feb 2016 (page 30)
  http://forms2.rms.com/Managing-Cyber-Insurance-Accumulation-Risk.html?utm_CName=Cyber_2016_Managing-Cyber-Insurance-Accumulation-Risk&utm_CContent=Managing-Cyber-Insurance-Accumulation-Risk&utm_LSource=web
- Keeper Security – How Hackers Make Money
  https://keepersecurity.com/assets/pdf/Infographic-how-hackers-make-money.pdf
- Bestvalid.cc – website selling payment card details
- Other dark web sources researched by Quocirca

Appendix 2 – Demographics

Of the 500 respondents surveyed overall, 471 were senior IT managers, 29 were senior managers in the risk, fraud, compliance, and/or governance area. The breakdown by country, company size, and sector is shown below. The fieldwork was conducted by Quocirca's research partner Vanson Bourne.

Figure 18: Countries surveyed by business size (number of employees)

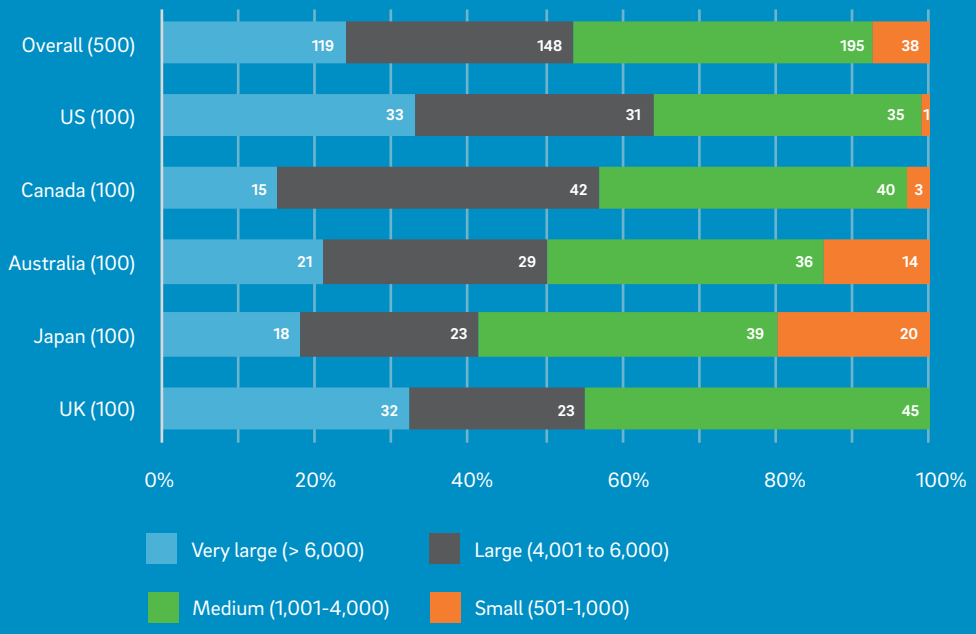


Figure 19: Sectors surveyed by business size

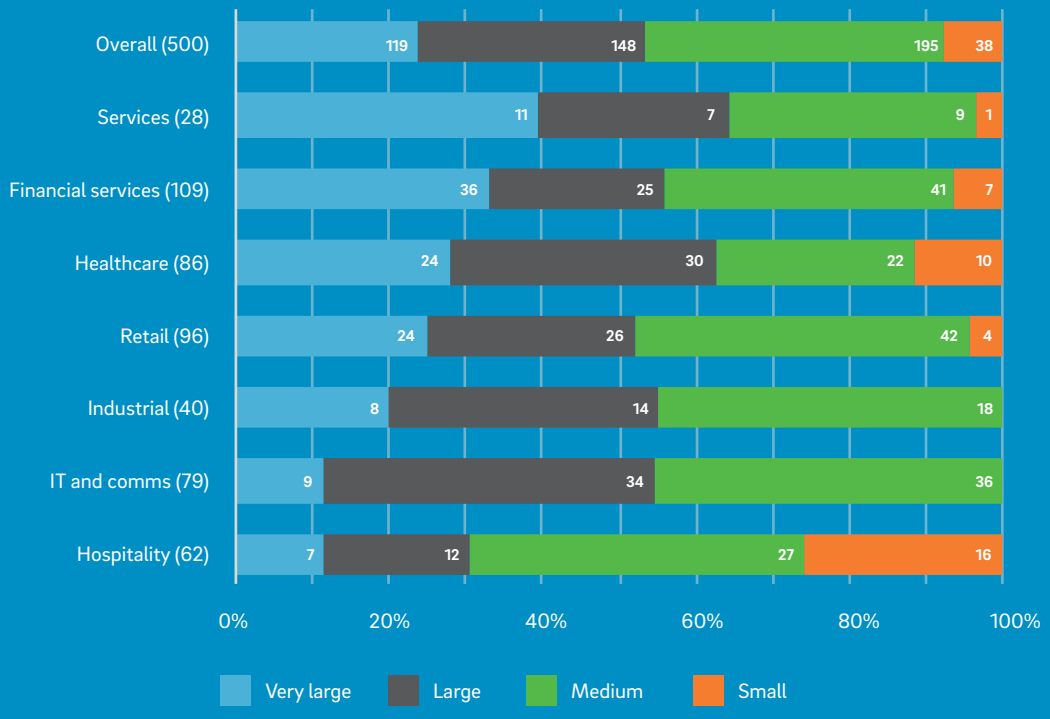
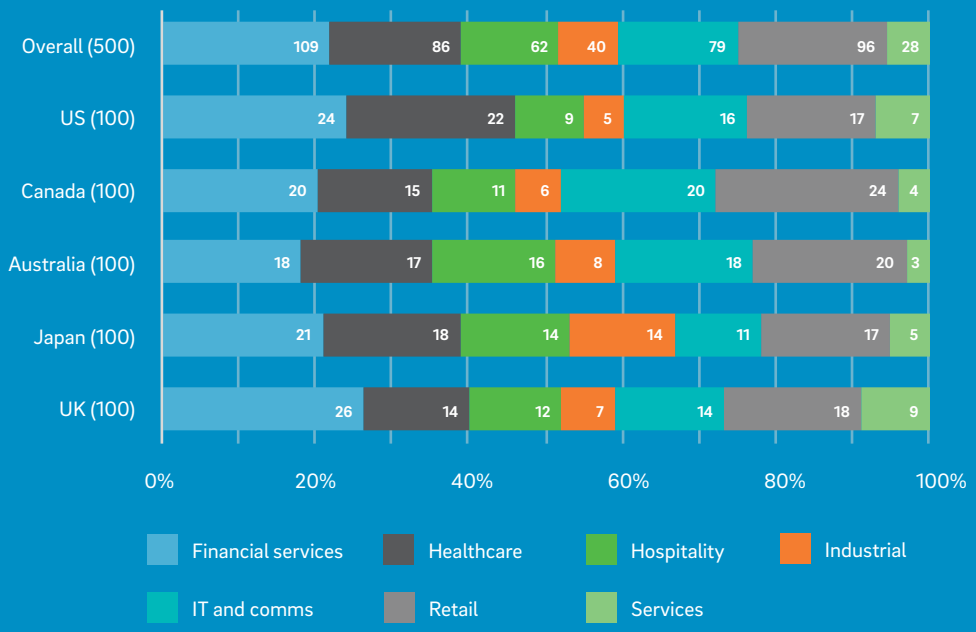


Figure 20: Countries surveyed by sector



Appendix 3 – Data calculations and exchange rates

Calculation of data controller estimates and exchange rates

Respondents were asked the value of a single record pertaining to both their prime data subject and their prime IP type, using the ranges shown below. The mid-value of each range was taken and used to calculate the weighted averages for data controller estimated value of PII and IP shown in the report:

- Less than $10 (please specify)
- $10-$50
- $50-$100
- $100-$200
- $200-$500
- $500-$1,000
- $1,000-$2,000
- $2,000-$5,000
- More than $5,000 (please specify)
- Don't know

The same ranges and calculation were used when the respondents were asked to estimate the criminal value of a payment card and banking records.

For purposes of comparison, all monetary values reported are in U.S. dollars (U.S. $). However, the research was conducted in local currency and converted using the following mid-2017 exchange rates:

1 U.S. $ =

- Japanese Yen 110.58
- Australia $1.33
- Canadian $1.33
- U.K. £0.82
- Euro €0.88 (no countries using the Euro were surveyed but some sources used for data values were quoted in Euro)

Appendix 4 – Definitions

Per capita value (PCV) for PII data is the value that can be placed on a single record.

Prime data type is the data type that was given most priority by respondents (in the new research) when considering data value by a given organization, based on one of four basic types:

- Personally identifiable information (PII)
- Intellectual property (IP)
- Payment card data (PC data)
- Corporate email (email)

Prime data subject is the type of data subject (consumers, patients, employees etc.) a respondent considered would cause the most damage to their organization if PII concerning that data subject was compromised.

Prime IP type is the type of intellectual property considered of greatest value to an organization.

Data risk vigilance is a value derived from 10 questions asked of respondents about the attention they pay to the value of their data.

About Trustwave

Trustwave helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. More than three million businesses are enrolled in the Trustwave TrustKeeper® cloud platform, through which Trustwave delivers automated, efficient, and cost-effective threat, vulnerability, and compliance management. Trustwave is headquartered in Chicago, with customers in 96 countries. For more information about Trustwave, visit https://www.trustwave.com.

About Quocirca

Quocirca is a U.K.-based research and analysis company. Quocirca produces free-to-market content aimed at IT decision makers and those that influence. Much of the content Quocirca produces is based on primary research across Europe, the Americas, and Asia, sponsored by a broad spectrum of IT industry organizations. Quocirca content is written from an independent standpoint and addresses the use of IT within the context of an organization, rather than specific products. Through its close relationships with the media, Quocirca articles and reports reach millions of influencers and decision makers: www.quocirca.com.

Trustwave®

For more information: www.trustwave.com