FINANCIAL INDUSTRY AT RISK: THE PRICE OF DATA LOSS

WHY CYBERSECURITY IS REQUIRED FOR THE WORLD OF FINANCE?

The financial services permanently suffer from activity of cyber criminals and malicious insiders. These firms are 300 times as likely as other companies to be targeted by a cyberattack, the Boston Consulting Group confirmed.

Top 6 threats

business email compromise

phishing

ransomware

malware

human error

malicious insider threat

Big banks and pension funds usually have enough resources for cybersecurity solutions. According to a forecast by research firm IDC, banks will invest in it more than any other industry – $151.2 billion by 2023 when combined with manufacturing and governments, the other top spenders. Whilst small and medium-sized companies as venture capital firms, private equity funds, fintech companies, family offices and hedge funds lack resources for cybersecurity needs.

SEARCHINFORM

RISK AND COMPLIANCE MANAGEMENT

Another challenge for SMB is high cost of recruiting, hiring and retaining in-house security staff. This problem can be fixed by outsourcing when the professionals come as a part of service. It is worthy of note that the percentage of the total IT budget being spent on outsourcing increased from 9.4% in 2018 to 12.7% in 2019 (a Computer Economics report).

48%

In accord with that research, 48% of companies are ready to increase the amount of security work that they outsource.

SearchInform services instead of hiring extra staff:

- risk management;
- corporate fraud and data loss prevention;
- in-depth investigation;
- profiling;
- data-at-rest monitoring;
- hardware and software audit.

Learn more

CYBERSECURITY BUDGET

Many organisations set the budget on the basis that of either company size or compliance and regulatory spending. But, the primary element of the formula is value of the data collected, used and shared by the company. The formula for cyber security costs in financial industry has to include value of Personally Identifiable Information, Quantitative Research, Alternative Data, Intellectual Property and so on.

Malicious insiders attacks

the most expensive type of issues in 2019

which cost **$243.101**

A data valuation model is more precise and realistic than the other based on the size of an organisation's IT infrastructure. For example, a model when the company spends on cybersecurity 10% of its total IT costs does not have regard to the cyber risks the company encounter.

In 2019, attacks of malicious insiders became the most expensive type of issues to resolve for financial services. It costs an average of $243.101 (Cost of Cybercrime Study in Financial Services: 2019 Report by Accenture).

PERSONALLY IDENTIFIABLE INFORMATION (PII)

PII, Personally Identifiable Information is any data that can be used to identify a particular person. At the most basic level it includes:

- residential and commercial addresses;
- email address;
- date of birth;
- passport details;
- phone numbers.

And also:

- IP addresses;
- login IDs;
- digital images;
- geolocation, biometric, and behavioral data.

Venture capital firms, private equity firms, and hedge funds hold much more amount of PII than family offices. All the companies usually split PII into records and keep it on databases and CRM platforms. And each record has a value.

As an example, in the dark web one record now costs about $12. The tech giants of Facebook, Google and LinkedIn put the value of a record at $20. Moreover, the current average cost of a data breach is $140 per record. It allows calculating the final cost of potential PII breach according to a quantity of the records.

$140 per record is an average cost of a data breach

Hedge and private equity funds with $100 million under management have about 1 000 PII records for every $100 000.

Here are approximate values of PII data for hedge funds and private equity funds:

Type of a company	Assets under management	PII value
Hedge fund	> $100 000 000	$116 000
Hedge fund	> $ 1 BN	$1 100 000
PE fund	> $100 000 000	$ 155 000
PE fund	> $ 500 000 000	$ 775 000

Fintech companies collect two types of data – for the running of company and on the platform for customers. They as usual have one PII record for every $100 000 of company valuation, and firms that are more successful have one PII record for every $1000 of valuation.

Thus, the value of PII data for Fintechs can be approximated as:

Type of data	Company valuation	PII value
Not including platform	> $ 100 000 000	$ 60 000
On the platform	> $ 100 000 000	$ 600 000

In family offices a number of collected PII records is similar to hedge funds, as it is one PII record per $100 000 of fund valuation. Besides, these data are not transferable and often incomplete. Therefore, an average cost of one record is $20 (normal rate).
So the value of PII data for family offices can be approximated as $20 000 for > $100 000 000 valuation.

QUANTITATIVE RESEARCH, ALTERNATIVE DATA, INTELLECTUAL PROPERTY

All the financial companies create, manage and hold a big number of quantitative research, alternative data and some intellectual property.

Quantitative Research are used for forecasting of investment opportunities on the base of complicated mathematical models. It is precious information that has an impact on the company future revenue.

Alternative data is the sort of second hand information, which financial services get from such suppliers as Bloomberg, Thomson Reuters etc. For example, annual financial reports which the company can use at corporative paperwork.

Intellectual property at financial industry is the data, which used to construct a fund manager's strategy, and thus requires protection.

SEARCHINFORM
RISK AND COMPLIANCE MANAGEMENT

Therefore, the value of the data as detailed above can be approximated as:

Type of a company	Assets under management / company valuation	Data value
Hedge fund	> $100 000 000	$ 490 000
PE fund	> $100 000 000	$ 560 000
Family offices	> $100 000 000	$ 330 000
Fintech	> $100 000 000	$ 645 000

The total value of data can be approximated as:

Type of a company	Assets under management / company valuation	Total data value
Hedge fund	> $100 000 000	$ 600 000
PE fund	> $100 000 000	$ 710 000
Family offices	> $100 000 000	$ 350 000
Fintech	> $100 000 000	$ 1 290 000

All the numbers above are average, because each company has different threats, different vulnerabilities and different risks. However, this approach when the data value is the key variable is the first step to understanding exactly what to spend on cybersecurity.

In additional, cybersecurity spending must also focus on encryption, personnel training, regulatory attestation, as it can mitigate the impact and reduce the cost of a leakage.

HOW TO CALCULATE CYBERSECURITY BUDGET?

When you know the total value of your data, the next step is to calculate what percentage of that value is the correct cost to spend annually to protect it. The appropriate way is to look at how cyber insurance works.

Cyber insurance companies offer coverage for network security and privacy liability, Public Relations, forensics investigations, credit monitoring, regulatory defense, penalties and fines, and much more. **The normal level of premium is 1.75% of the payout.**

Even so, **the cure** is **3 times more expensive than prevention** of an incident.

5.25%

Experts suggest that 5.25% of the value of the data is the correct amount to spend on an annual basis.

Thus, the annual cyber security spend (CSS) should be:

Type of a company	Assets under management / company valuation	Total data value
Hedge fund	> $100 000 000	$ 31 800
PE fund	> $100 000 000	$ 37 500
Family offices	> $100 000 000	$ 18 300
Fintech	> $100 000 000	$ 67 600