KASPERSKY lab

GLOBAL IT SECURITY RISKS 2014 – ONLINE FINANCIAL FRAUD PREVENTION

Table of contents

THE MAIN FINDINGS

- **Businesses place high importance on guarding Financial/Transaction info:** 34% of businesses claim that the protection of sensitive information (including financial information) is a top priority of their IT department. Our findings show that 45% of businesses feel they need to take improved measures to protect financial transactions. Surprisingly, E-Commerce/Online Retail organizations were the least likely to keep their existing anti-fraud measures up-to-date. They also reported only a slightly above-average interest in taking improved measures to protect financial transactions.

- **Financial companies are not immune to cyber threats:** 48% of E-Commerce/Online Retail businesses and 41% of Financial Services organizations have reported losing some type of finance-related information to cybercriminal activities within the past 12 months.

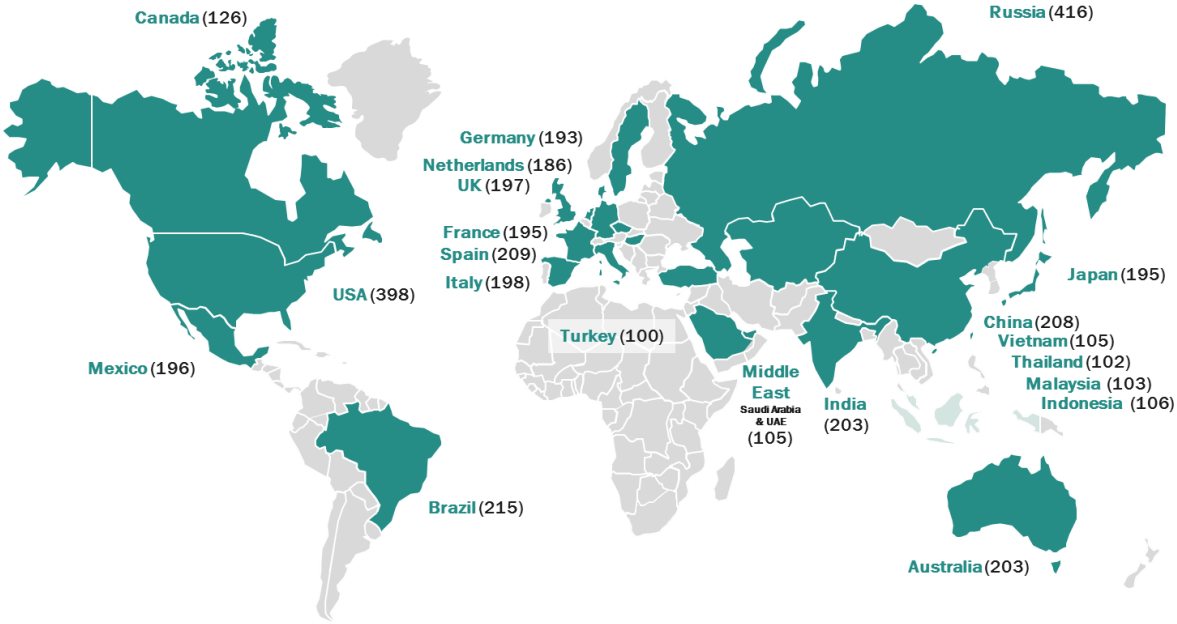
- **Businesses take a pragmatic view towards losses incurred by cybercrime:** roughly one out of every four businesses – 27% – is willing to suffer losses incurred by cybercrime, because they believe the cost of protection will outweigh the cost of dealing with the losses. Moreover, 52% of Financial Service businesses have a policy of reimbursing customers' losses caused by cybercrime without investigation. Given this and the data we discovered on the true cost of financial data lost ($66,000–$938,000, depending on the size of the company), this attitude is risky.

- **The security reputation of financial institutions plays a critical part in businesses' propensity to do business with them:** 82% would consider leaving an institution that suffered a breach. Moreover, businesses are more open to the idea of investing in premium software solutions to protect financial transactions: 53% prefer to pay more for the best security solution for transaction protection.

- **Businesses do have a relatively broad view about who is ultimately responsible for the risks of financial transactions:** only 35% of survey respondents think banks are primarily responsible, whereas financial institutions in this survey believe 85% of the burden is being placed upon them. Unsurprisingly, smaller businesses rely more heavily on financial institutions to take responsibility for the safeguarding of their transactions and data. However, even amongst larger business, only one in five feels it is the responsibility of their security department.

- **Banks and online services providers have quite a lot of room to adopt more and more sophisticated security measures for their clients:** a surprising 4% of businesses operating some kind of online service admitted they took NO specific measures to protect their customers/clients from online financial fraud.

METHODOLOGY



A total of 3,900 respondents from 27 countries - including representatives from companies of all sizes - took part in this year's survey. Compared to the previous year, the survey grew both in total size and global scope (the 2013 survey included 2,900 respondents in 24 countries). More than 54% of the participants were mid-sized, large and very large companies. Approximately 17% of the respondents were corporations in the Large Enterprise segment (with anywhere from 5,000 to 50,000 employees), while 12% of the survey participants fit into the Large-Medium category (1,500 to 5,000 employees). About 25% of the survey participants were companies with anywhere from 250 to 1,500 employees, and the remaining respondents represented small and very small businesses.

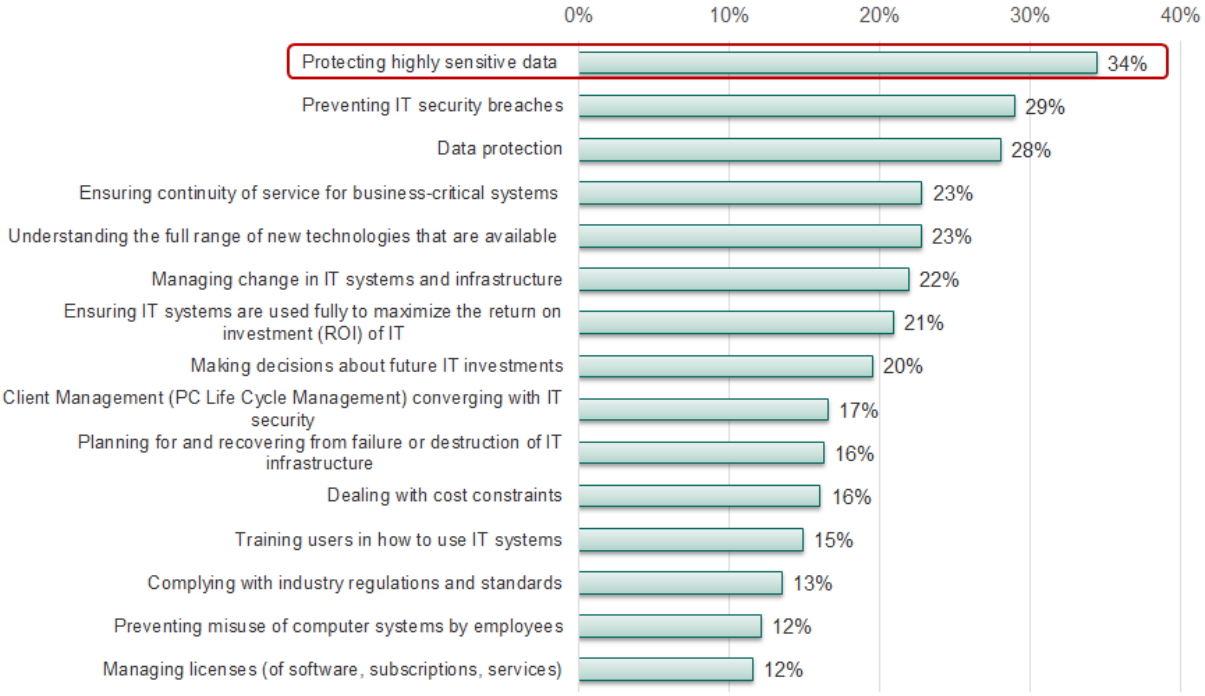
All of the companies that took part in the survey answered dozens of questions concerning the main obstacles that both the company's general management and IT management face, specifically when building and maintaining a reliable, smooth-running IT infrastructure. Additionally, respondents also answered questions about the resources allocated by their companies for tackling IT problems, including data security problems. The survey questions asked respondents about business conditions within a period of the previous 12 months, from April 2013 through May 2014.

SECTION 1: ATTITUDES TOWARDS SENSITIVE DATA BY REGION AND BUSINESS SECTOR

We began the survey by measuring businesses attitudes towards IT security in general, as well as their attitudes towards their existing and planned anti-fraud protection plans. It should come as no surprise that security concerns ranked highly when respondents were asked to list their top IT department concerns. A full 34% responded that "protecting highly sensitive data" (which includes financial information) was a priority, making it the most commonly-cited concern. It's also noteworthy that security-related concerns were the top four highest IT priorities.

TOP CONCERNS OF THE IT FUNCTION

DATA PROTECTION ISSUES AND ANTI-DDOS ARE AMONGST THE TOP CONCERNS FOR THE IT FUNCTION



Q19. Taking into account all the issues that need to be considered by IT personnel, what are the top 3 concerns of the IT function at the moment?

Base: 4,438
All Respondents

Drilling a more deeply into concerns specifically around financially-sensitive data, we found respondents were equally enthusiastic when asked about their anti-fraud practices. "Making every effort to ensure our anti-fraud measures are up-to-date" was by far the most widely agreed-upon response, with 62% of respondents agreeing. This demonstrates that businesses are placing a high priority on securing their financial data, which is most popular target of fraud attempts.

Having established the perceived importance of anti-fraud protection, we asked a question to gauge respondents' opinions about whether they believed their existing measures for protecting financial transactions were sufficient, or if new measures should be added.

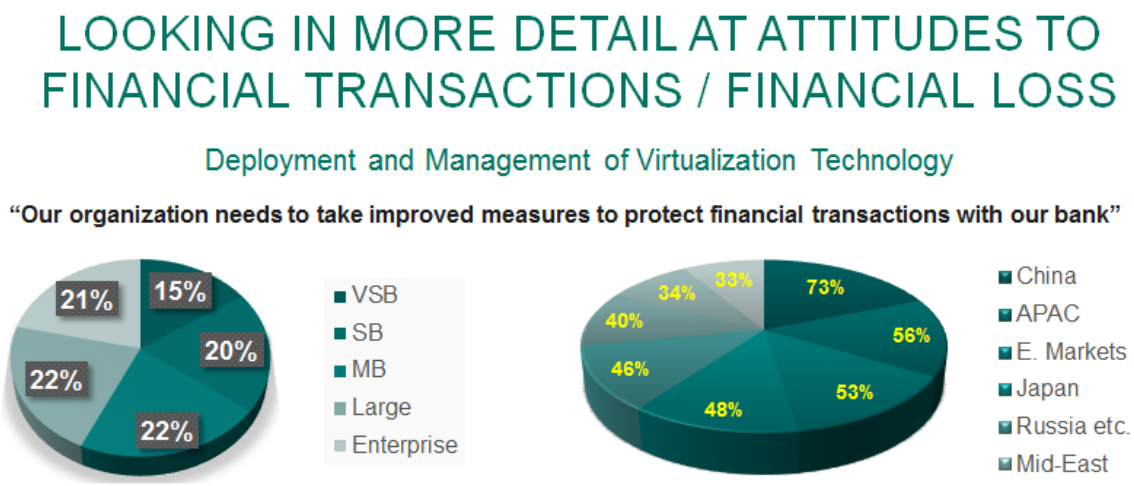
GENERAL ATTITUDES TOWARDS IT SECURITY

43% OF ORGANIZATIONS FELT THAT THEIR CURRENT MEASURES TO PROTECT THEIR FINANCIAL TRANSACTIONS WERE NOT GOOD ENOUGH

You can see a notable drop in agreement when asked if "our organization needs to take improved measures to protect financial transactions," which was reported by 45% of respondents, compared to the previous question where 62% "make every effort to keep our anti-fraud measures up-to-date."

This would suggest that businesses believe they have an adequate amount of anti-fraud protection in place, and only need to keep these measures operating rather than invest in new solutions. It is also possible that businesses feel their own anti-fraud investment is adequate, and instead hope to see improved anti-fraud measures implemented by their financial service providers and institutions.

Here are the same regional and vertical-industry responses to this question, which were also measured for the previous question:



There was a similarly-sized variation of responses between VSBs (very small businesses with fewer than 25 employees) and their larger business counterparts. But we see a much more consistent level of response amongst businesses with 26–5,000 employees, and even a slight drop at the Enterprise level.

At the regional level, China remains very willing to take additional measures, a rate nearly identical to the previous question. Russia, however, dropped from 73% "ensuring their current measures are up-to-date" to only 46% agreeing that they need "irmproved measures." North American support for this statement also dropped virtually in half, from 66% to 34%, with Western Europe reporting a similar decline. While support for this question was lower on average across all regions, we found the steep drop in support from businesses in these three highly-modernized regions to be unexpected and noteworthy.

By itself, this last group of regional-focused data suggests that North American and Western Europe could be highly-satistifed with their existing fraud prevention measures, and thus see no reason to change. It could also mean they are least-aware of fraud prevention solutions that may be available to them.

Again, we reference the responses to the following two statements for comparison:

(1) "*We make every effort to ensure our anti-fraud measures are up-to-date*" (62% overall).

	Manufacturing	IT/ Software Etc.	Financial Services	Business Services	Construction/ Engineering	Government /Defence	Education	Healthcare /Services	Consumer Services	Other	Transportation /Logistics	Telecoms	Real-Estate	Utilities & Energy	Media /Design	Non-Profit /Charitable	E-commerce /Online Retail
Base	724	613	328	305	294	292	279	199	535	187	140	116	99	95	93	71	68
We make every effort to ensure our anti-fraud measures are up-to-date	62%	63%	64%	67%	62%	62%	64%	64%	59%	63%	65%	59%	65%	59%	61%	54%	53%

Clearly, the most surprising statistic here is from E-Commerce/Online Retail businesses reporting the *lowest* rate of agreement regarding the upkeep of their anti-fraud systems. This seems highly counter-intuitive, since their entire business model is based on processing online payments.

(2) "*Our organization needs to take improved measures to protect financial transactions*" (45% overall).

	Manufacturing	IT/ Software Etc.	Financial Services	Business Services	Construction/ Engineering	Government /Defence	Education	Healthcare /Services	Consumer Services	Other	Transportation /Logistics	Telecoms	Real-Estate	Utilities & Energy	Media /Design	Non-Profit /Charitable	E-commerce /Online Retail
Base	724	613	328	305	294	292	279	199	535	187	140	116	99	95	93	71	68
We need to take improved measures to protect financial transactions	49%	43%	52%	40%	47%	37%	47%	45%	43%	35%	56%	36%	47%	41%	39%	35%	46%

Here, the three vertical markets that agreed the least with this statement are Non-Profit/Charitable, Telcom, and Government/Defense. Transportation/Logistics and Financial Services were the highest at 56% and 52%, respectively.

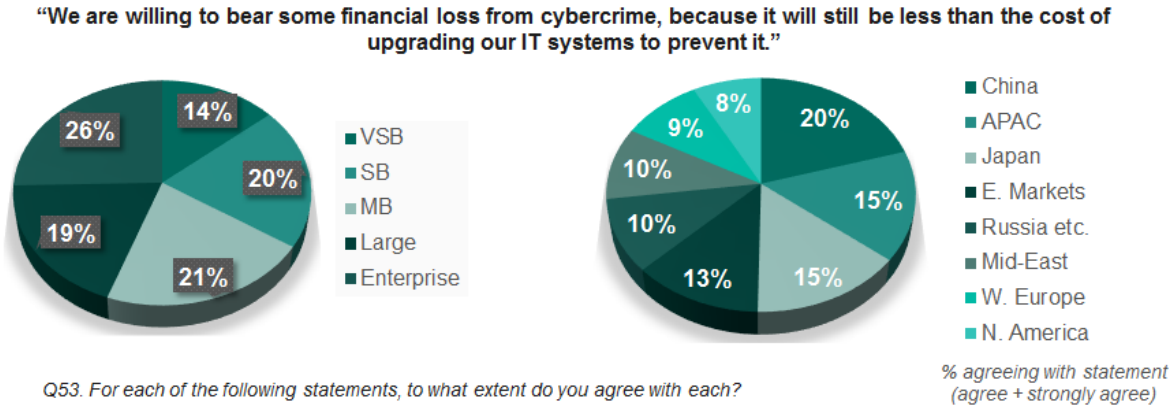
From these groups of market-segment data, we see that:

- E-Commerce/Online Retail has a surprisingly low rate of agreement with both statements, which is strange taking into account that this is one of the industries that suffered mostly from loss of financial data.
- Financial Services is another critical business segment when discussing online fraud, so it is encouraging to see 52% (second-highest overall) report their desire to implement new technologies to protect financial transactions.
- Business Services, another key segment for handling financial transactions, reported the highest response rate (67%) for "ensuring our anti-fraud measures are up-to-date," but also generated the greatest overall rate of variance, with only 40% reporting that "they need to take improved measures to protect financial transactions."

Kaspersky Lab believes the growing onslaught of malware and cybercriminal campaigns focused on hijacking financial transactions will reach levels in the coming years that will make dedicated financial transaction security software a necessity.

Much like a person on a treadmill, businesses combating financial fraud will have to "run just to stay in the same place." This means that (1) "commitment to ensuring anti-fraud measures are up-to-date," and (2) "taking improved measures to protect financial transactions" will both be key attitudes for businesses in all countries and business sectors.

SECTION 2: BUSINESS ATTITUDES TOWARDS CYBERCRIME



Here we see some interesting data that forms the core of any risk-management strategy – the cost of protection versus the cost of cybercrime. Across the spectrum of business sizes, from VSB to Enterprise, an average of 27% of businesses reported that they were willing to suffer some financial losses from cybercrime because it was more cost-effective than upgrading their IT systems/security to prevent the losses. This attitude was most prevalent within Enterprises at 35%, and relatively consistent across Small Businesses through Large Businesses. *(Note: if you remove VSBs - under 25 employees and unlikely to have sophisticated IT networks - the average climbs to 31%)*

When measuring this attitude by country/region, we see that China is once again at the top. It is interesting that from previous questions, we know that China is most willing to take measures to prevent fraud, and it appears they are also the most willing to accept a certain amount of loss as "the cost of doing business." North America and Western Europe rate the lowest in this category. If you recall, North America and Western Europe also rated the lowest in their response to the statement "our organization needs to take improved measures to protect financial transactions." It is interesting to see that both regions are equally unwilling to accept losses from cybercrime, and unwilling to consider improving their financial transaction security measures.

We asked organizations that had experienced data loss within the past 12 months to indicate the most serious type of cyberintrusion or malicious activity they encountered – the one event most responsible for the majority of their data loss. Once again, the E-Commerce/Online Retail category had the most interesting response.

MOST SERIOUS THREAT EXPERIENCED

	Manufacturing	IT/ Software Etc.	Financial Services	Business Services	Construction/ Engineering	Government /Defence	Education	Healthcare /Services	Consumer Services	Other	Transportation /Logistics	Telecoms	Real-Estate	Utilities & Energy	Media /Design	Non-Profit /Charitable	E-commerce /Online Retail
Network intrusion / hacking	8%	12%	8%	5%	6%	4%	10%	5%	6%	4%	6%	7%	8%	6%	9%	8%	30%

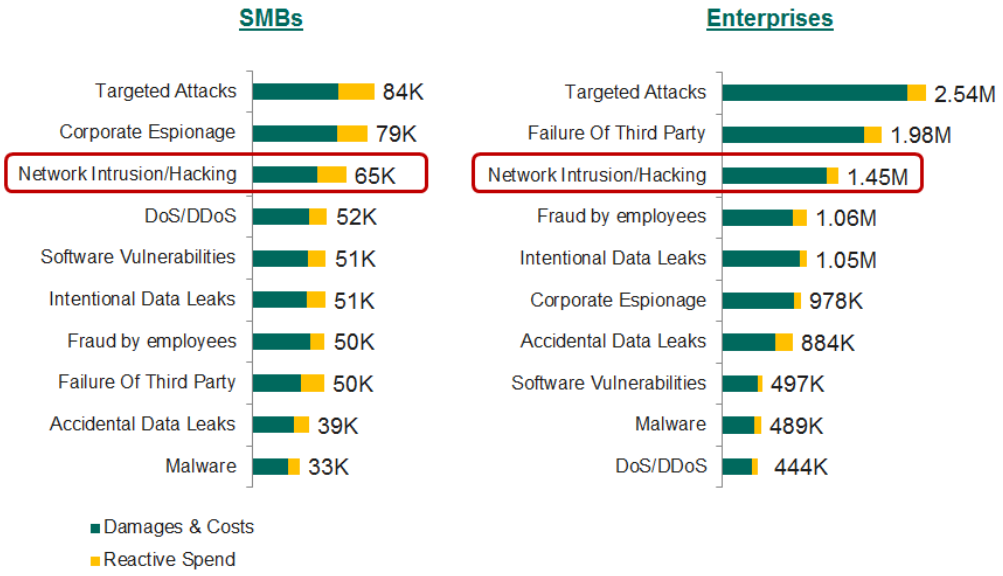
As you can see, intrusion into the network of E-Commerce/Online Retailers was reported at a rate of 30%, far exceeding any other market segment. Once again, recall that E-Commerce/Online Retail was the segment *least likely* to maintain their anti-fraud measures, although they are clearly be targeted by cybercriminals. This revelation is even more surprising due to the high rate of online attacks these businesses face: in the last 12 month, 93% of financial services providers and 90% of E-commerce/Online Retailers encountered various cyberthreats.

A separate question asked what type of data loss was associated with each type of cyber-incident. Our research shows that **32% of all financial data stolen in the past 12 months was the result of a Network Intrusion/Hacking incident. In fact, Network Intrusion/Hacking was the top source of all stolen financial information.**

To offer perspective on how much money a Network Intrusion/Hacking incident can cost a business, the data below accounts for the cost of immediate cleanup as well as the cost of installing new software, hiring consults, etc., to prevent future incidents. Depending on the size of the E-Commerce/Online Retail business, a Network Intrusion/Hacking Incident can cost anywhere from $65,000 to $1.45M.

AVERAGE IMPACT OF DATA SECURITY BREACHES BY TYPE

AGGREGATED W3 & W4



So far, the research shows that E-Commerce/Online Retailers are being disproportionately targeted by the type of attack that steals the most financial information. Now let's examine some other business segments to see what else is being stolen and see if what businesses worry about the most is actually aligned with what is occurring.

As this graph shows, financial information is the number two "most feared" category of information to lose, second only to customer/client information. Interestingly, this graph shows that internal operational information and customer client information are the two types of data most often stolen (42% and 32%, respectively). However, if you take the data loss from the entire "financial-related data" group – which includes financial information, payment information and corporate bank account credentials), we see that a total of **33% of businesses had experienced a loss of this data within the past 12 months.** Since 32% of respondents felt this was the worst possible type of data to lose, it appears their fears are justified.

Once again, we took a closer look at what types of data were being lost most often across all business sectors. This graph shows the type of data lost in the past 12 months.

DATA TYPES BEING LOST

	Manufacturing	IT/ Software Etc.	Financial Services	Business Services	Construction/ Engineering	Government /Defence	Education	Healthcare /Services	Consumer Services	Other	Transportation /Logistics	Telecoms	Real-Estate	Utilities & Energy	Media/Design	Non-Profit /Charitable	E-commerce /Online Retail
Base	882	651	340	222	373	327	299	208	495	140	152	156	78	93	95	58	29
Financial information	24%	26%	32%	19%	26%	19%	16%	23%	26%	19%	27%	21%	21%	24%	18%	24%	31%
Payment Information	11%	10%	11%	8%	11%	6%	9%	10%	11%	9%	12%	12%	15%	6%	11%	14%	10%
Corporate bank account access credentials / log-ins	4%	6%	4%	3%	5%	4%	4%	4%	3%	3%	5%	4%	3%	9%	0%	5%	10%
Any Financial/Payment/Bank Information	32%	34%	41%	26%	32%	26%	24%	31%	34%	25%	33%	30%	33%	30%	23%	34%	48%

Here, we see that E-Commerce/Online Retail is the number two source of stolen financial information at 31%, and alarmingly, the Financial Services sector is number one, with 32%. The bottom row shows the aggregated amount of "financial-related data": here, **48% E-Commerce/Online Retail reported losing this data within the past 12 months, while 41% of Financial Services organizations reported the same.**

To better illustrate the costs associated with these data breaches, we asked businesses about the costs of responding to data loss incidents. This included the costs of professional service providers to help manage the immediate problem (e.g., hiring securing consultants, lawyers, auditors, etc.), as well as the cost of lost business opportunities (e.g., the loss of the ability to trade, damage to company reputation, etc.), and investment in services and solutions to prevent additional incidents (e.g., extra security training). When all these costs were totaled, the actual cost of a business losing financial data ranged anywhere from $66,000 to $938,000, depending on the size of the company.

The rate of stolen financial data from E-Commerce/Online Retail continues to be alarming. But this is surprising news for the Financial Services sector, which in the previous section of this report had indicated high rates of commitment to maintaining their anti-fraud solutions, as well as willingness to adopt new anti-fraud measures. This is also surprising due to the fact that only 8% of Financial Services reported "Network Intrusion/Hacking" as their most serious cyber incident, compared to the 30% reported by E-Commerce/Online Retail. (Remember, "Network Intrusion/Hacking" is the type of incident most likely to result in stolen financial information.)

It's clear that both Financial Services and E-Commerce/Online Retail are big sources of stolen financial information. But there appears to be a notable difference in terms of how these two business sectors prioritize the security of this data.

DATA TYPES COMPANIES FEAR LOSING
BY INDUSTRY VERTICAL (W3 & W4):

	Manufacturing	IT/ Software Etc.	Financial Services	Business Services	Construction/ Engineering	Government /Defence	Education	Healthcare /Services	Consumer Services	Other	Transportation /Logistics	Telecoms	Real-Estate	Utilities & Energy	Media /Design	Non-Profit /Charitable	E-commerce /Online Retail
Base	813	595	312	195	344	288	260	185	454	123	136	139	73	78	87	51	28
Customer/Client Information	17%	24%	29%	30%	23%	19%	21%	30%	21%	21%	21%	24%	19%	18%	28%	41%	21%
Financial information	18%	17%	24%	16%	23%	17%	21%	18%	24%	24%	26%	17%	21%	18%	16%	12%	7%
Internal Operational Information (details of processes, e-mails etc.)	19%	16%	11%	9%	16%	20%	14%	15%	17%	16%	20%	16%	19%	19%	20%	14%	11%
Intellectual Property	17%	14%	7%	16%	14%	13%	17%	12%	11%	13%	12%	12%	10%	5%	16%	16%	21%
Market Intelligence / Competitive Intelligence	11%	10%	9%	12%	11%	7%	6%	7%	9%	7%	7%	11%	10%	18%	11%	4%	18%
Payment Information (e.g. customer credit card data)	7%	8%	9%	9%	5%	8%	8%	5%	8%	7%	4%	12%	7%	9%	2%	6%	11%
HR/Personnel Information	7%	9%	8%	6%	5%	13%	9%	8%	7%	6%	5%	4%	11%	8%	3%	8%	7%
Corporate bank account access credentials / log-ins	4%	2%	4%	2%	3%	2%	3%	3%	3%	4%	4%	4%	3%	5%	3%	0%	4%
Other	0%	0%	0%	1%	0%	1%	1%	2%	0%	2%	1%	1%	1%	0%	0%	0%	0%
Any Financial/Payment/Bank Information	29%	27%	37%	27%	31%	27%	32%	26%	35%	35%	35%	33%	30%	32%	22%	18%	21%

Table Shows % Of All Respondents Who Lost Data, Who Most Fear The Loss Of This Data Type

W3N21. Which type of data would you say was most crucial or potentially damaging to your company?

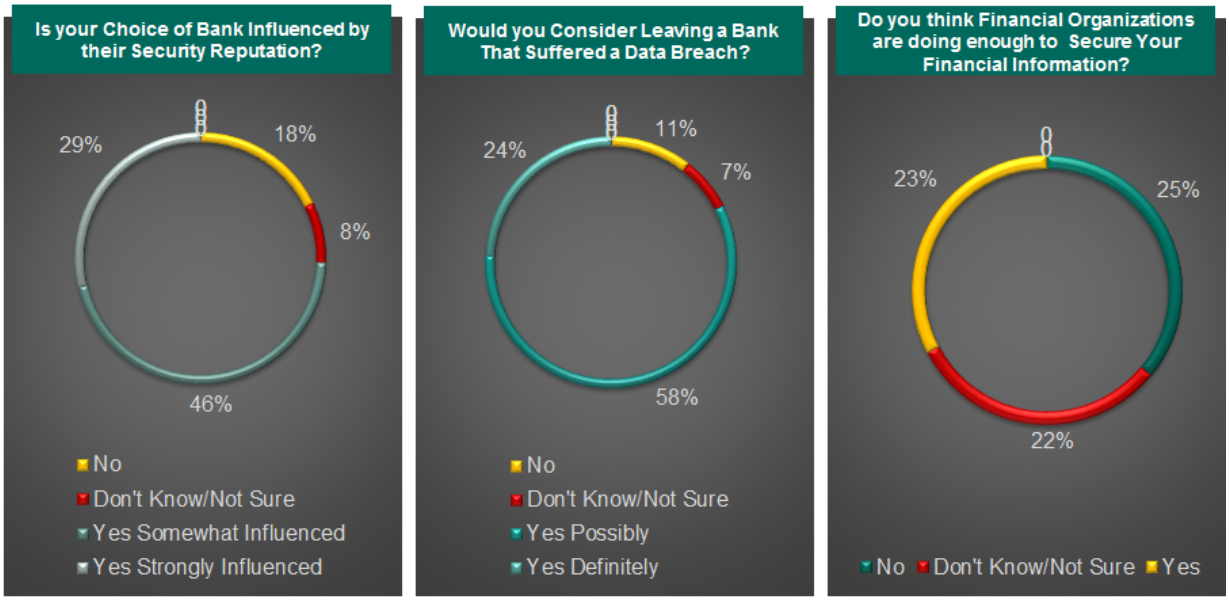
Here, we see an interesting breakdown of what types of data business fear losing the most. Notice that Financial Services show the highest rate of fear (37%) associated with losing "financial-related data." E-Commerce/Online Retailers are nearly the lowest at 21%, behind only Non-Profit/Charity organizations.

In the next section, we will examine attitudes that specifically relate to fraud prevention, with a focus on Financial Service providers and E-Commerce/Online Retailers. From this data, we can draw some conclusions about what drives a business's opinions about online fraud and financial data theft, and we can show how these attitudes translate to actions and real-world business consequences.

SECTION 3: ATTITUDES TOWARDS ONLINE PAYMENT FRAUD PREVENTION

Let's begin with what shapes businesses' attitude regarding the banks and financial service providers with which they choose to partner.

THE IMPORTANCE OF TRUST IN FINANCIAL SERVICE PROVIDERS



- **74%** of businesses surveyed considered the strength of the bank's security reputation when choosing who to work with
- **82%** also stated that they would at least consider switching banks if the bank suffered a data breach
- Most shockingly, **only 53% of businesses** felt that financial organizations did enough to protect their financial information

W4N4. Is your company's decision to continue working with your current bank influenced by the strength of their security reputation?
W4N5. Would you consider terminating business relations with a bank that suffered a data breach?
W4N6. Do you think the banking and financial services industry is doing enough to secure your organizations financial information?

Base: 4,438 All Respondents

To summarize:

- **74%** of businesses surveyed considered the strength of the bank's security reputation when choosing which one to work with.
- **82%** also stated that they would at least consider switching banks if the bank suffered a data breach.
- **25% don't think banks are doing enough to secure their financial information.**
- Most shockingly, **only 53% of businesses** felt that financial organizations did enough to protect their financial information.

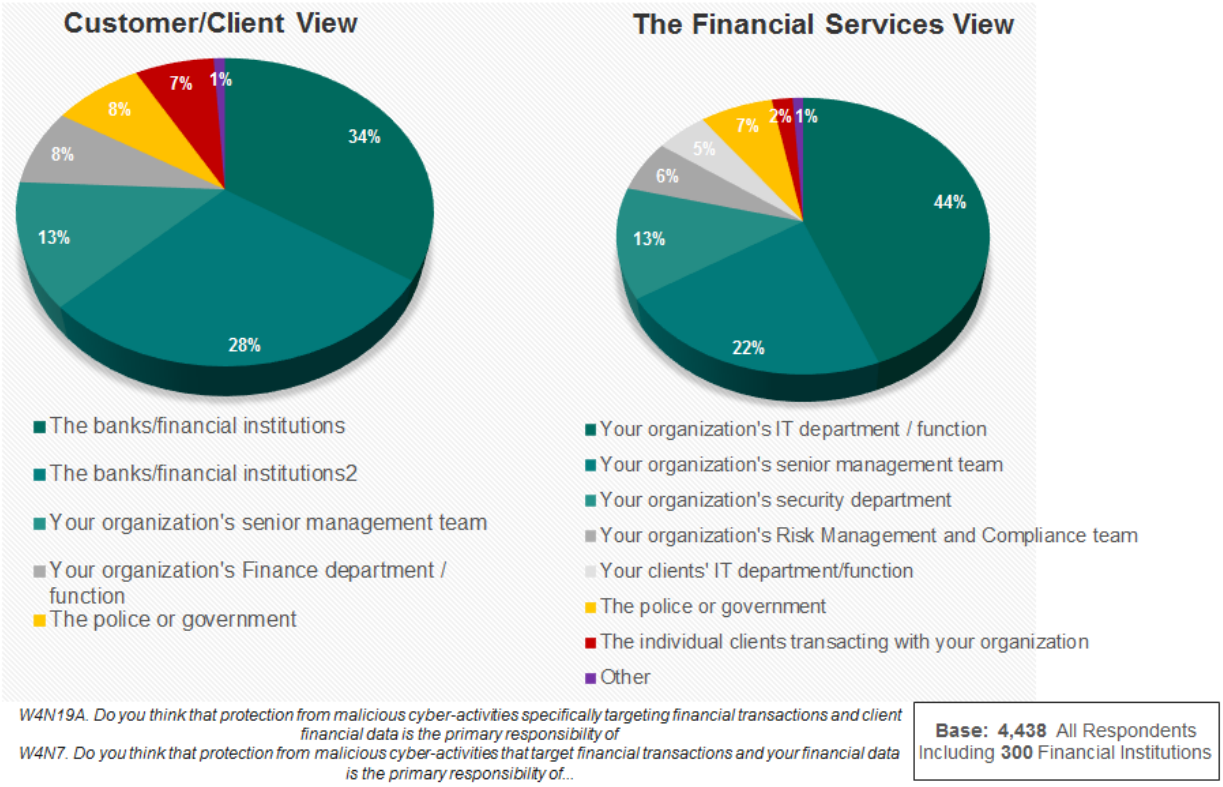
Our survey found another interesting point on the topic of trust and reputation. We asked all business sectors to name their top most-feared consequences of a data breach. **In the Financial Services sector, the most highly-rated "worst consequence of a data breach" was "the loss of credibility/damage to company reputation," listed by 47% of Financial Services**

organizations. This fear appears to be justified, as the data above shows clients are very willing to walk away from financial instructions that they don't fully trust.

Lastly, the Financial Services sector is not alone in their fear about damage to their reputation. **Loss of credibility/damage to company reputation was the top response across 13 of the 17 business segments we surveyed, and in the remaining 4 sectors, it was the number two answer.** Clearly, businesses everywhere realize that trust and reputation are everything.

Now that we have established the importance of trust, let's turn our attention to how businesses and financial organizations perceive themselves to be responsible for securing financial transactions.

WHERE DOES THE FINANCIAL SECURITY BUCK STOP



W4N19A. Do you think that protection from malicious cyber-activities specifically targeting financial transactions and client financial data is the primary responsibility of
W4N7. Do you think that protection from malicious cyber-activities that target financial transactions and your financial data is the primary responsibility of...

Base: 4,438 All Respondents
Including **300** Financial Institutions

From this graph, we see the biggest disparity lies in the perceived responsibility of the IT departments of the client organization. 28% of the clients themselves believe their own IT department is responsible for securing financial transactions with their financial service provider, and only 5% of financial service providers agree that this responsibility resides on the client-side of the transaction.

In fact, financial service organizations are much more likely to believe that it is their own responsibility to provide a secure transaction for their client. When all the internal components of a financial services organization – including the IT department, internal security, senior management, etc. were added up – 80% of financial service providers felt they were responsible

for security. This attitude aligns with the data discovered in the previous section regarding what types of data loss these organizations fear the most – financial services organizations are much more likely than any other business sector to rate securing financial transactions as their number one.

For more detail on how business perceive this balance of responsibility, we examined how this attitude may change based on the size of the business. **On average, 34% of businesses feel it is the financial institution's responsibility.** It's probably not surprising to learn that smaller businesses rely more heavily on financial institutions to take responsibility for safeguarding transactions and data. According to 48% of VSBs, it is the responsibility of the financial institution, and even within Enterprises with more than 5,000 employees and large amounts of IT resources, a full 25% still expect the financial institution to take responsibility for a safe transaction. However, it is worth noting that within Medium Businesses, Large Businesses and Enterprises, all three respondents feel their own combined internal IT and Security departments hold at least an equal share of the security responsibility.

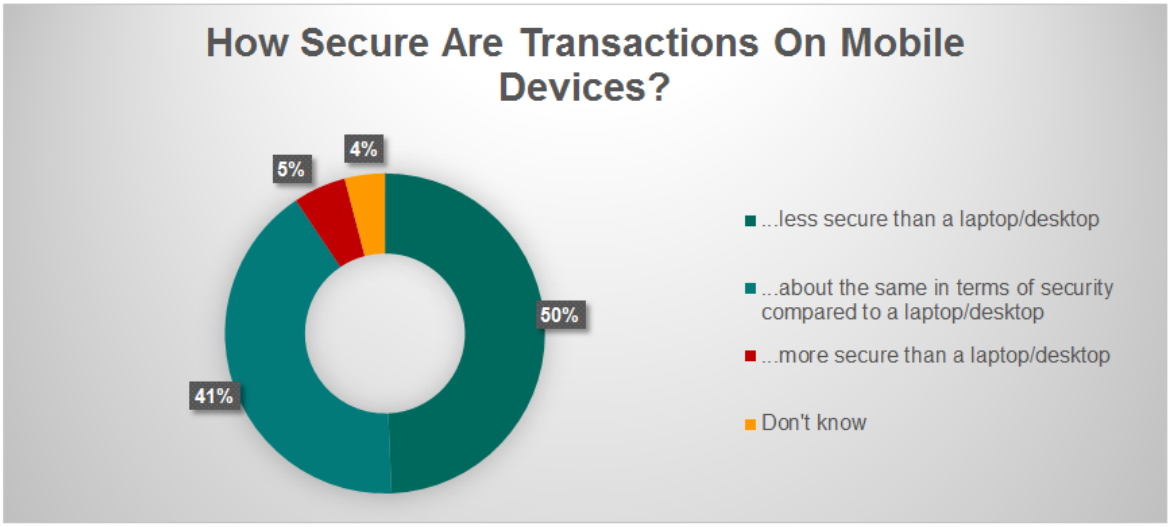
Before moving on to specific attitudes regarding the value of anti-fraud solutions, we asked our respondents about their attitudes towards banking transactions conducted from mobile devices (smartphones and tablets).

Overall, 43% of businesses claimed to conduct sensitive transactions on mobile devices, including transactions with financial services organizations. Smaller businesses were least likely to use mobile devices for these sorts of transactions, with 35% of VSBs admitting to this behavior – that's one out of every three businesses with fewer than 25 employees connecting to their bank on phones and tablets. Not surprisingly, the rate was higher with enterprises, with 51% claiming this sort of activity.

Kaspersky Lab approaches everything from a security perspective, while businesses are primarily focused on productivity and efficiency, and we suspected that businesses might not understand the reduced levels of security often associated with mobile devices.

USAGE AND ATTITUDES TOWARDS MOBILE TRANSACTIONS

How Secure Are Transactions On Mobile Devices?



W4N8. Does your business conduct any sensitive or confidential transactions from mobile devices ?
W4N8A. How do you feel the level of security of such transactions on mobile devices compares to those conducted on a conventional laptop or desktop computer? I think these transactions from mobile devices are

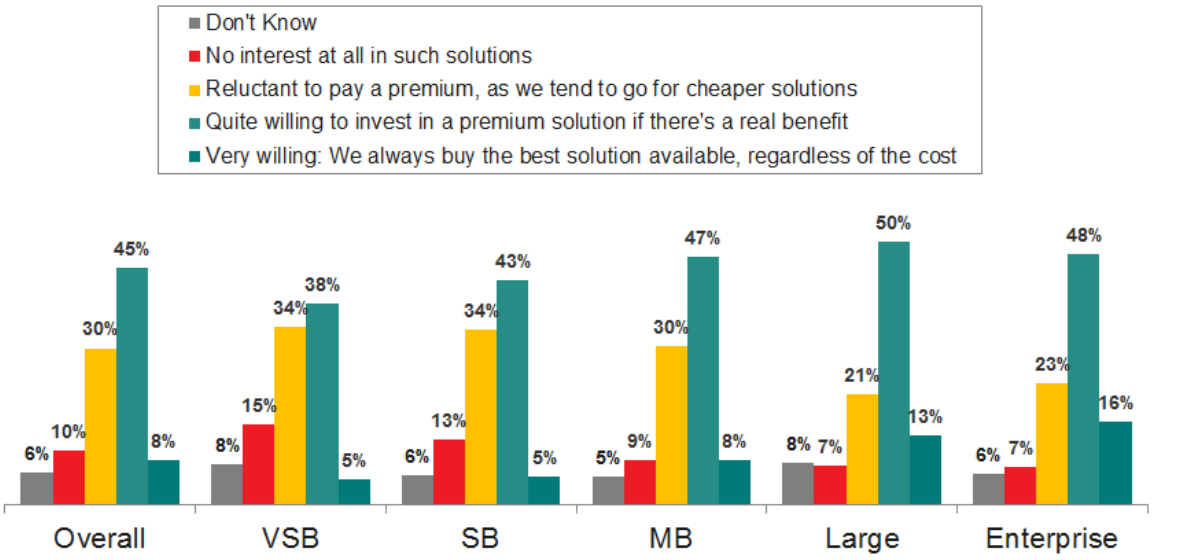
Base: 4,438 All Respondents

When we asked businesses about their attitudes towards mobile device security, our suspicions were confirmed: only 49% acknowledged that mobile devices were less secure than a laptop or desktop computer, while 41% believed them to be about the same in terms of security. Given the willingness of businesses of all sizes to use mobile devices to conduct sensitive transactions, special attention should be paid to ensure these devices are included within any specialized financial security solution.

Here, we see a more direct measurement of businesses' willingness to invest in software specifically designed to protect financial transactions. **Overall, 53% of businesses are "very willing" or "quite willing" to invest in such a solution.**

WILLINGNESS TO INVEST IN FINANCIAL TRANSACTION PROTECTION SOFTWARE

LARGER BUSINESSES WERE SIGNIFICANTLY MORE OPEN TO THE IDEA OF INVESTING IN PREMIUM SOFTWARE SOLUTIONS TO PROTECT FINANCIAL TRANSACTIONS



W4N9. Is your organisation willing to invest in software that would provide superior protection for financial and confidential transactions that are performed in your company (both on mobile and/or PCs)?

Base: 4,438 All Respondents

As has been the case throughout this survey, we see that smaller businesses are least likely to invest in fraud prevention software, and larger businesses are much more likely.

When applying this question to our vertical markets, we found that the **Telecom sector had the largest percentage of "very willing" respondents (17%), making Telecom the most enthusiastic at the prospect of fraud prevention software.** Combined with their 38% of "quite willing" respondents, Telecom produced a total of 55% of respondents who were "willing to invest."

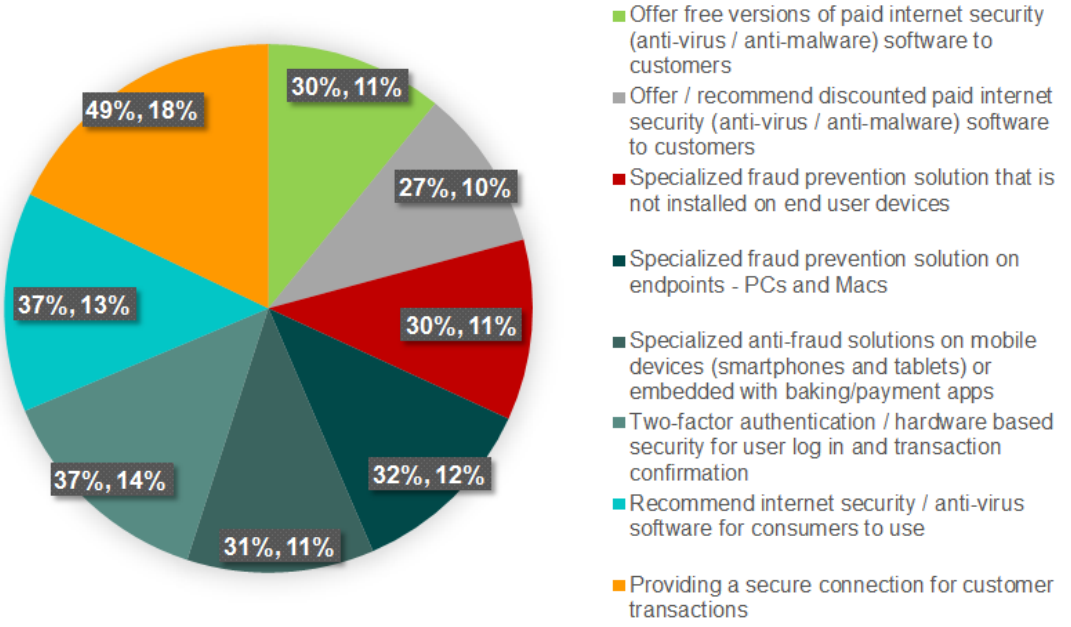
The Financial Services sector was not far behind, with 13% of respondents "very willing" and a whopping 51% being "quite willing." **This means Financial Services showed the greatest overall interest (64%),** even though Telecoms were most likely to install a transaction security solution.

Our respondents from the **E-Commerce/Online Retail sector once again lagged behind,** with only 6% of respondents being "very willing" and 32% being "quite willing," bringing their total "willing to invest" rate to 38%. Interestingly, E-Commerce/Online Retail also had the highest rate of respondents who indicated they were "reluctant to pay a premium, as we tend to go for cheaper solutions" – 38% supported this statement. Does this indicate E-Commerce/Online Retail are mostly concerned about the cost/ROI of such a solution? This is a reasonable theory, given the tight profit margins that most E-Commerce/Online Retailers operate with. But the data shows that these companies are actually willing to pay for these additional anti-fraud services if

they are provided by their financial institutions, and would prefer to have this service provided to them rather than investing in their own infrastructure, which they would have to manage.

Throughout the survey, we have established that the "heavy transaction" sectors of Financial Services and E-Commerce/Online Retail have very different attitudes towards the value of financial transaction security software. For the final portion of our survey, we took a closer look at the anti-fraud measures currently being used by both sectors.

ANTI-FRAUD MEASURES EMPLOYED BY FINANCIAL SERVICES PROVIDERS & E-COMMERCE OPERATORS



4% of businesses operating an online transactional service admitted they took **none of these actions** to protect their customers/clients

W4N20. Do you currently take any of the following steps to protect your customers from online transaction fraud when using your services

Base: 2,680 All Respondents In Financial Services Or Operating Online, Public Facing Services (Not Asked In Select APAC Countries)

As you can see, "providing a secure connection for customer transactions" is by far the most common measure of transaction protection provided, with 49% reporting it to be a built-in part of the transaction process, and another 36% reporting it to be "optional/not yet fully implemented."

With regard to encouraging clients to use internet security/anti-virus software, businesses from these sectors were much more likely to recommend a particular type of software (37%) rather than provide that software at a discount or free of charge (27% and 30% respectively).

We also see that these businesses are almost equally likely to install part of their anti-fraud solution onto their customers' devices (31% for mobile devices, 32% for PCs and Macs), as they were to have an anti-fraud solution operating on their own back-end system (30%).

Seeing that the limited usage of E-Commerce/Online Retailers may skew the statistics, we separated the two segments to compare usage statistics. The Business Services sector is also provided below for comparison.

ANTI-FRAUD MEASURES EMPLOYED

BY INDUSTRY VERTICAL: 2014

	Manufacturing	IT/ Software Etc.	Financial Services	Business Services	Construction/ Engineering	Government /Defence	Education	Healthcare /Services	Consumer Services	Other	Transportation /Logistics	Telecoms	Real-Estate	Utilities & Energy	Media /Design	Non-Profit /Charitable	E-commerce /Online Retail
Base	**429**	**396**	**302**	**149**	**133**	**174**	**141**	**117**	**344**	**83**	**93**	**86**	**58**	**64**	**56**	**33**	**55**
Providing secure connections for customer transactions	87%	90%	88%	79%	79%	84%	86%	90%	82%	78%	91%	88%	81%	83%	84%	76%	78%
Recommend internet security / anti-virus software	80%	84%	80%	77%	79%	66%	79%	80%	72%	64%	80%	85%	86%	75%	71%	61%	71%
Two-factor authentication / hardware based security	80%	84%	85%	73%	77%	75%	74%	76%	66%	67%	83%	81%	81%	83%	68%	61%	69%
Specialized anti-fraud solutions for mobile devices	77%	82%	75%	68%	81%	60%	66%	74%	66%	59%	69%	76%	81%	69%	70%	58%	56%
Specialized fraud prevention endpoint solution	73%	76%	71%	68%	70%	60%	67%	78%	65%	65%	74%	71%	76%	75%	57%	64%	62%
Specialized fraud prevention solution that is not installed on end user devices	75%	76%	74%	70%	74%	58%	67%	77%	61%	63%	75%	73%	67%	72%	59%	61%	56%
Discounted paid internet software for customers	70%	76%	66%	65%	76%	49%	61%	68%	59%	53%	71%	78%	74%	63%	54%	55%	60%
Free versions of paid internet security software for customers	72%	74%	61%	60%	76%	54%	67%	63%	57%	48%	72%	77%	69%	59%	55%	52%	60%

Table Shows % Of Organizations Who Experienced Some Data Loss For Whom This Was The Most Serious Event Within The Last 12 Months

W4N20. Do you currently take any of the following steps to protect your customers from online transaction fraud when using your services

Base: 2,680 All Respondents In Financial Services Or Operating Online, Public Facing Services

The areas where we see the largest amount of divergence between Financial Services and E-Commerce/Online Retail include the use of two-factor authentication, anti-fraud solutions for mobile devices and specialized fraud prevention software installed on back-end IT systems of the business itself. For comparison, the Business Services sector appears to be more likely to implement these measures than the E-Commerce/Online Retail sector.

Lastly, we asked Financial Service providers only about (1) their usage of real-time transaction monitoring, and (2) their policy of reimbursing customers in the event of lost funds. The answers regarding real-time transaction monitoring were polarizing: 52% responded that they did use this technology, while 38% responded that they did not. A similar number of Financial Service providers (52%) reported that customer funds are replaced either immediately or within a few weeks, and are replaced prior to any internal or criminal investigation. This propensity to quickly incur the cost of missing funds on behalf of their customers likely explains their fear of losing these funds in the first place, as well as their higher-than-average rate of anti-fraud adoption.

Given that customer endpoints are the mostly likely route for cybercriminals to compromise a financial transaction, and businesses are often liable to replace stolen funds, offering endpoint security programs to strengthen their customers' endpoints seems like a cost-effective

investment for these businesses. Also, given the fast and stealthy nature of online transaction fraud, it seems clear that the lack of real-time transaction monitoring services reported by more than one-third of these companies could create a scenario in which large amounts of money are lost before the Financial Service provider realizes there's a problem. Since the majority of these providers are expected to pay back their customers immediately, and given the long and difficult process of investigating and prosecuting the criminal perpetrators, this type of incident will certainly result in higher insurance premiums for the Financial Service provider or an immediate financial crisis for the business.

CONCLUSIONS AND RECOMMENDATIONS

When businesses deal with financial institutions, the importance of trust and reputation cannot be overestimated. Businesses are happy to take their accounts somewhere else if their financial institution suffers a data breach, or somehow loses the trust of their clients. Financial institutions, and most business in general, seem to understand the importance of protecting their own and their customers' financial information. We did observe a notable deviation from this pattern exhibited by E-Commerce/Online Retail organizations, which appear to be less likely to adopt new technologies that would further secure the online financial transactions of their customers. This attitude could be driven by financial concerns, such as the cost of protection not equaling the cost of the money they lose to cybercrime.

In recent years, Kaspersky Lab's researchers have observed a notable increase in cybercriminal efforts focused on stealing money, including sophisticated malware, phishing attacks that impersonate financial institutions and a variety of threats targeting mobile banking activities. To read more about this research, please read our Financial Cyber Threats in 2013 report.

Kaspersky Lab believes that this growth in financially-motived malware must be countered by dedicated security software that protects financial transactions. Our research shows that customers expect banks and financial institutions to provide this enhanced level of security, and therefore these businesses should consider investing in new technology to prevent tomorrow's threats. Kaspersky Lab offers a suite of technologies to accomplish this task through the Kaspersky Fraud Prevention platform for financial and e-commerce companies. This platform is a combination of security technologies and security services providing:

- Endpoint protection to secure all the devices used by the customers of financial services companies – regardless of whether the customer uses a Windows, Mac, iOS or Android-based device.
- Anti-fraud monitoring within the financial services company's infrastructure to detect any suspicious activity.
- A software development kit enabling financial services companies to develop their own secure mobile apps.
- Specialist monitoring, reporting and educational services to provide the latest intelligence on the global threat landscape – and enable knowledge transfer from Kaspersky Lab's anti-fraud security experts to the company's security team.

Additional information:

Banking Threats Report

Online Financial Fraud Infographic

Kaspersky Fraud Prevention Solution Overview