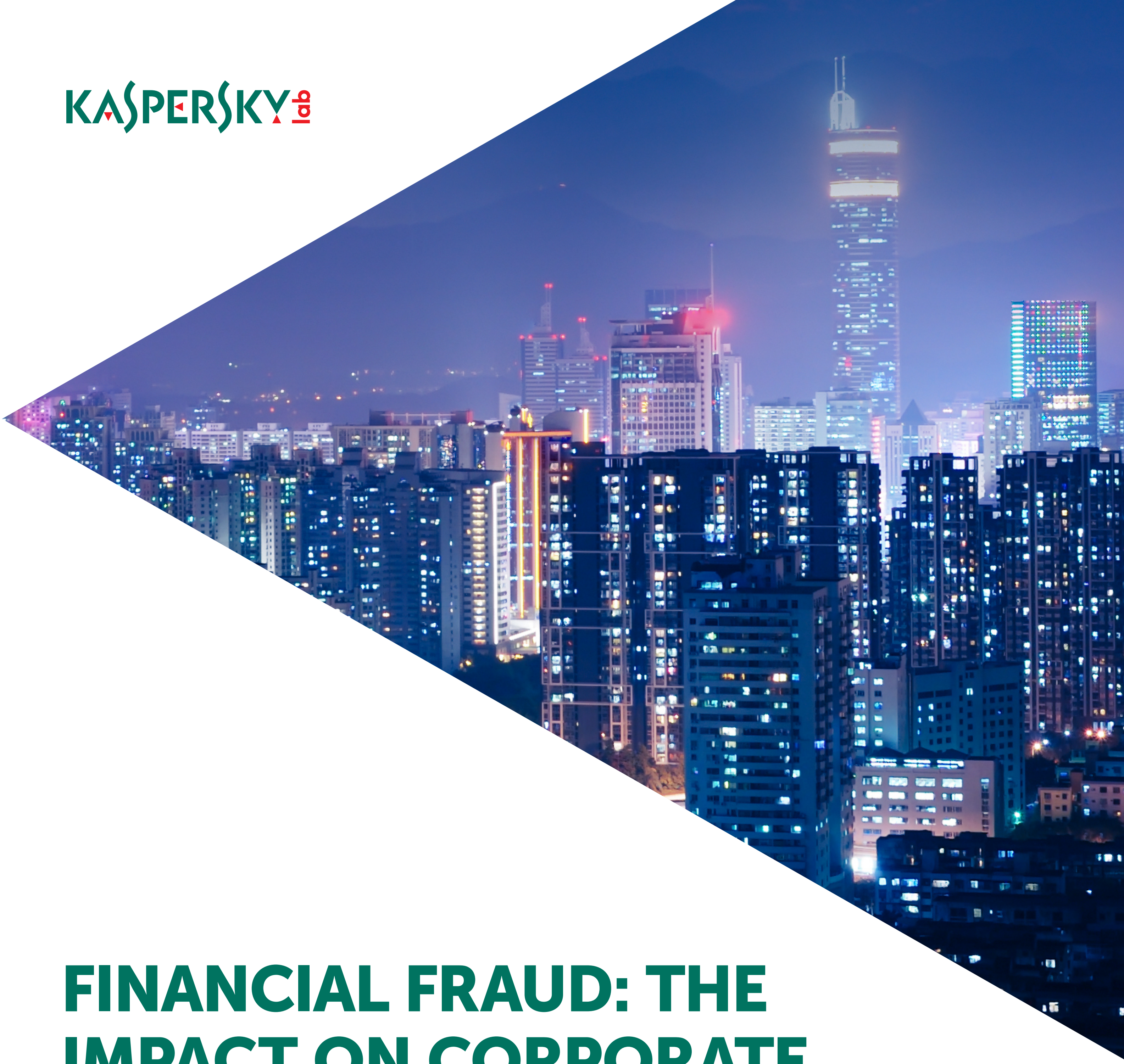


FINANCIAL FRAUD: THE IMPACT ON CORPORATE SPEND

IT SECURITY RISKS SPECIAL REPORT SERIES

Kaspersky Lab

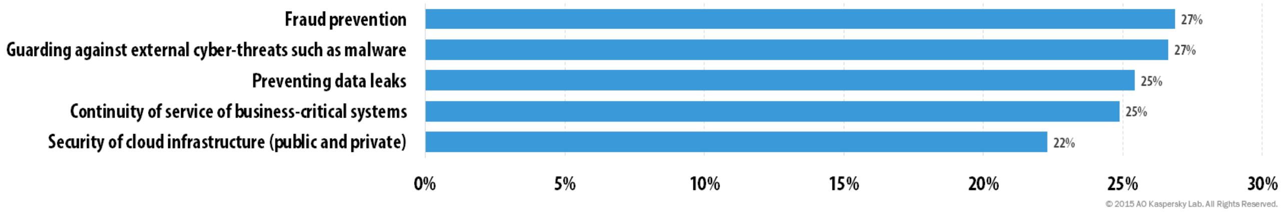
Corporate IT Security Risks Survey details:

- More than 5,500 companies in 26 countries around the world took part.
- Top managers and IT professionals answered a series of questions about security, IT threats and infrastructure.
- We specifically asked them about their attitudes towards the security of financial transactions.

What we found:

Importance of protection against fraud

- Prevention of any type of fraudulent activity is one of the top 3 priorities for **27%** of businesses, in addition to protection from cyber threats (**27%**) and data leakage prevention (**25%**).



Major security priorities for businesses in the next 12 months

- Verticals that specifically require protection from financial fraud report a higher-than-average level of concern: financial services (**40%**), e-commerce (**33%**), consumer services (**29%**).
- **47%** of businesses feel they specifically need to improve protection of financial transactions.
- **54%** of companies have fully implemented some form of financial transaction protection solution – provided either internally and/or by their bank.
  - There is no distinct preference between an in-house solution for financial transactions protection (41% of businesses have technology fully implemented) and a solution provided by a bank (45%).

Fraud-related threats faced by businesses

- **35%** of businesses have experienced a phishing attack.
- **5%** of businesses offering consumer services have experienced an incident involving POS intrusion.
- **10%** of financial services companies reported a targeted attack. **9%** for e-commerce, **4%** for consumer services.

How they perform financial transactions

- **31%** of businesses use mobile devices for their financial transactions. **59%** use a device with a WiFi connection.
- Access to financial transactions is usually handled by dedicated personnel and/or top management. **14%** of businesses grant access to such transactions to a broader range of employees.

Financial fraud: diverse, complex, universal threat

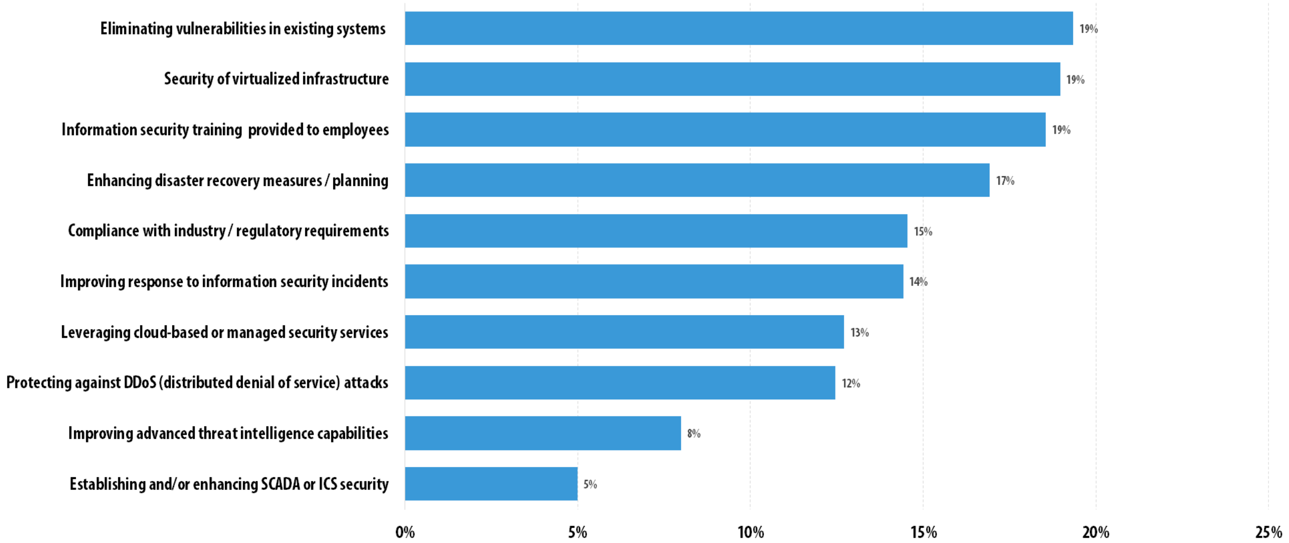
It is hard to completely avoid electronic transactions of any kind: even the most determined of individuals would find it difficult to operate solely using cash. For businesses it is absolutely impossible, largely due to technical reasons and, in many countries, the legislature and established practices. E-payments of all sorts have become so ubiquitous, that before we proceed to the statistics from our regular Global IT Security Risks survey, we have to define what transactions are being attacked and need to be protected. There are three major types of financial fraud affecting businesses today, all being actively exploited by cybercriminals:

- Attacks on B2B transactions: transfer of funds using specialized software, usually with higher-than-average security measures.
- Attacks on consumerized corporate spend: business transactions using widespread instruments like credit cards, consumer online banking, etc.
- Attacks on B2C transactions affecting businesses: the most obvious example is the bank taking responsibility for safety of its clients' online transactions.

Obviously, there are numerous points of vulnerability which can lead to the theft of money, and sometimes it is simply impossible to trace the attack to its original point of entry. To paint the complete picture of businesses' attitudes towards financial fraud, we asked questions across three major topics: perception of the threat, actual threats faced by businesses, which can lead to financial fraud, and their attitudes towards protection of financial transactions.

Perception: fraud as the top priority in IT security

Of all threats in the field of cyber security, businesses appear to perceive fraud as one the most sensitive topics. When we asked companies to select their three most important IT security priorities, fraud prevention came at the top of the list, perceived to be equally important as protection of cyber-threats in general. Other priorities, also regarded as important, such as data leaks prevention, were not mentioned as frequently.



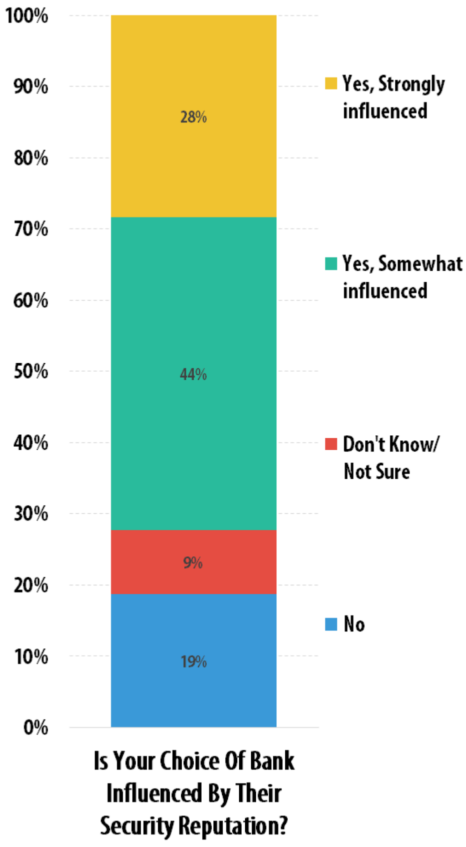
There is a simple explanation: businesses don't like it when someone tries to steal their money, inventory or hardware. It's a fact that theft of data – a simple sequence of bits – can destroy a company as quickly as theft of money from a bank account. Still, people (and businesses alike) make a much better effort trying to protect their wallet, rather than their e-mail account. The perception of money is much closer to that of physical objects, but this perception has to change: as in most cases today money is represented as a sequence of bits, like any other "virtual" data.

A number of industries appear to be more concerned about fraud in general: examples of those are financial services (**40%** of businesses name fraud prevention to be one of the top three priorities), e-commerce (**33%**) and companies offering consumer services (**29%**).

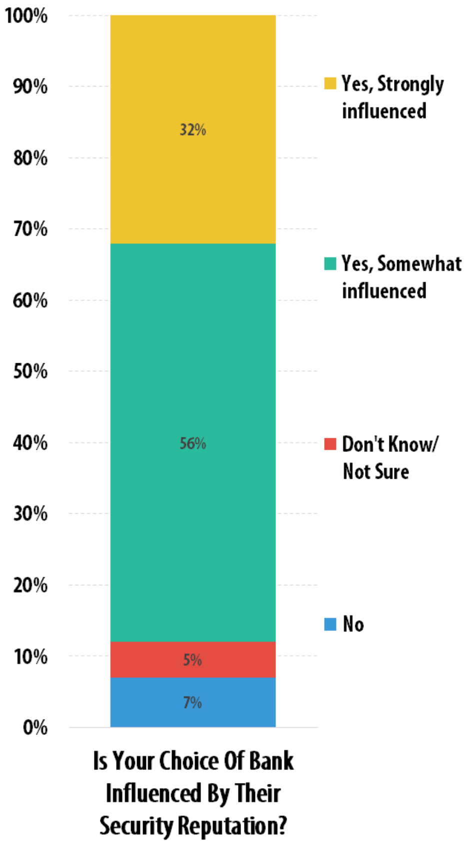
Are they ready to face the threat of financial fraud? Not all of them, certainly. **63%** of businesses admitted that they take every major effort to make sure their security measures against fraud are up-to-date. Surprisingly, the industry with the most confidence in their online fraud security is not financial organizations – they are number three with **67%**.The industry with the highest percentage of companies feeling that they are doing everything possible to protect against online fraud is telecoms with **70%**. We suggest that this indicates telecom companies have a certain advantage through being more experienced in IT and IT security matters. But confidence aside, the real situation is far from perfect in almost half of businesses. **47%** think that their protection of financial transactions has to be improved.

Security affects the choice of financial services provider

Given the importance of securing financial transactions in particular, and fraud prevention in general, it is no surprise that a bank's reputation when it comes to security, strongly affects businesses' choice. **72%** of companies agree that a bank with a stronger reputation in this area will have more chance of becoming their next banking provider. Moreover, **88%** of businesses are happy to spend more on financial services, provided that this additional spend guarantees better security.



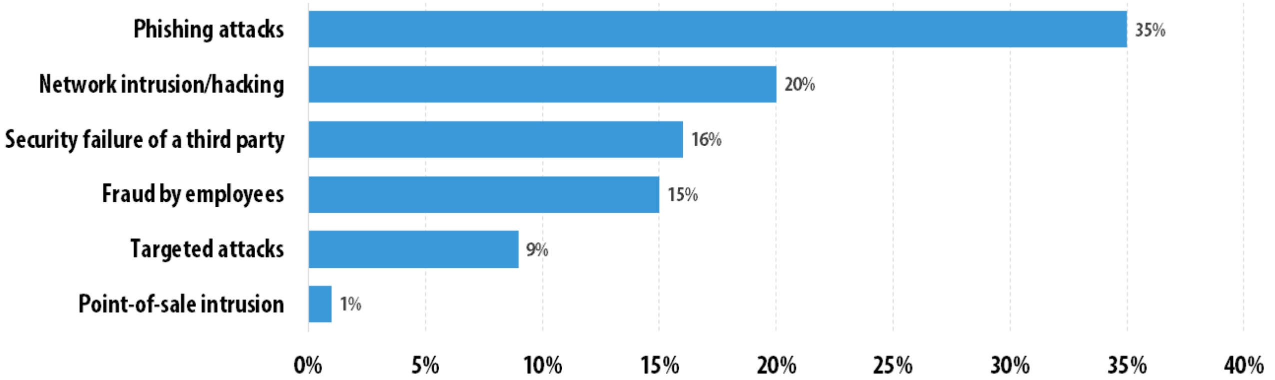
© 2015 AO Kaspersky Lab. All Rights Reserved.



© 2015 AO Kaspersky Lab. All Rights Reserved.

Experience of IT security threats related to fraud

There are many internal and external security threats that may be connected to the general problem of financial fraud. External threats include phishing attacks, network intrusion, targeted attacks, attacks to specialized infrastructure such as Point-of-Sale terminals and ATMs. Internal threats such as direct fraud by employees and security failure by a third party, may also result in loss of funds, or used as a key stage of a successful financial cyber attack. By analyzing the frequency of these types of attacks, we can estimate the likelihood of a company becoming a victim of financial fraud. Let's take a look at the numbers:



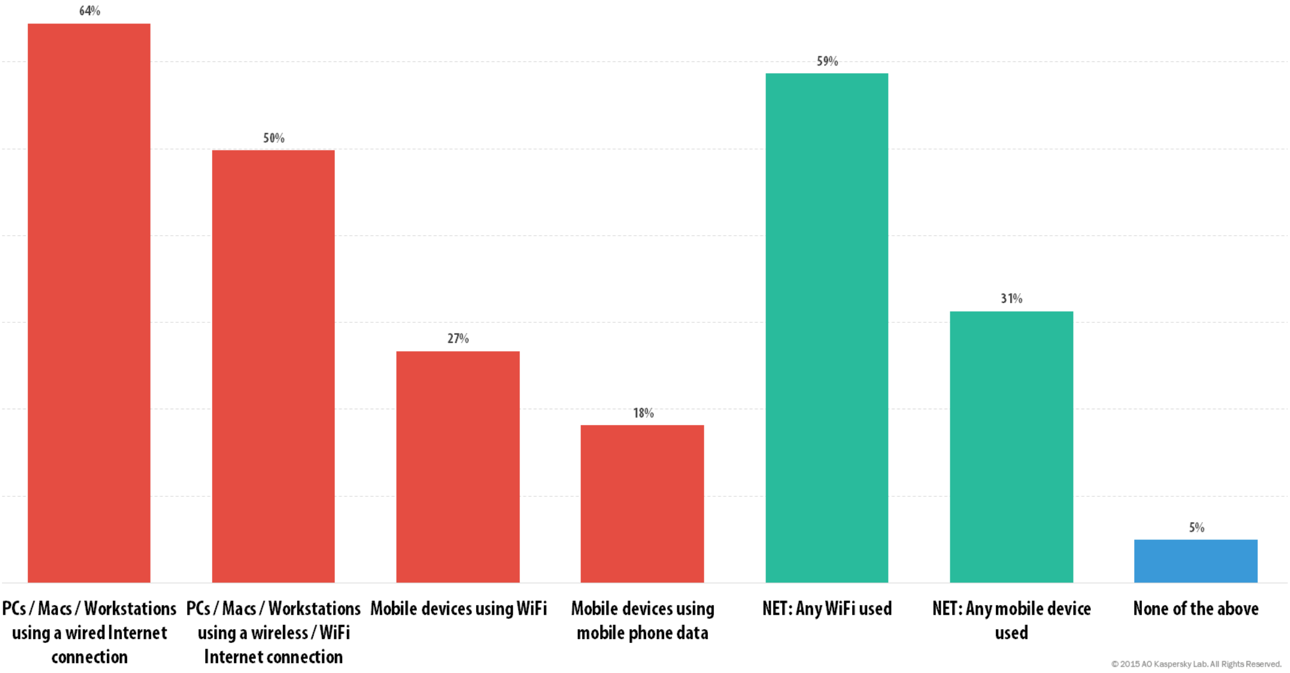
© 2015 AO Kaspersky Lab. All Rights Reserved.

The most widespread fraud-related IT security incident is the phishing attack, which was experienced by **35%** of businesses. Point-of-sale intrusion is rare, although the consequences of even a single attack of this type may be devastating. If we single out companies offering services to consumers, **5%** of them reported at least one attack on their PoS infrastructure. Targeted attacks were experience by **10%** of financial services companies, **9%** e-commerce organizations and **4%** of companies working in the consumer services industry. Overall, **60%** of businesses experienced at least one attack of any aforementioned type which can potentially become an important step towards a successful theft of funds.

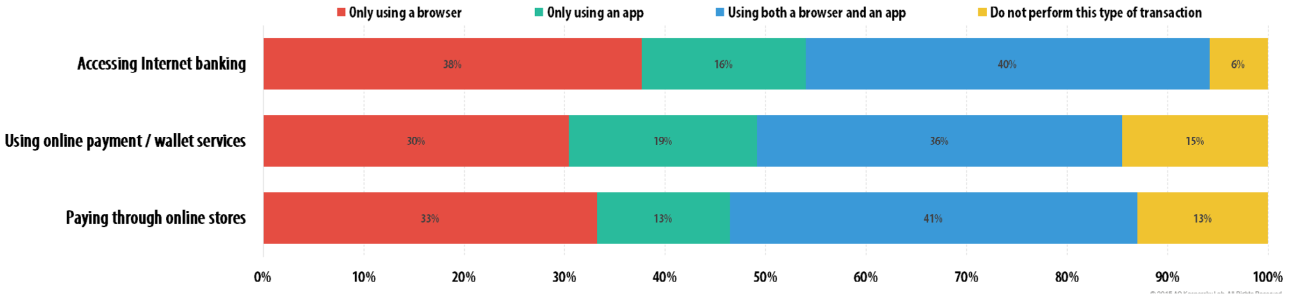
Handling financial transactions

Although a targeted or phishing attack always puts companies in danger of money loss, it can't be successful if financial transactions are properly secured. The third stage of our survey was to find out, how exactly businesses protect their online transactions, how do they handle them in general, and is this way of handling them secure. Let's start with protection.

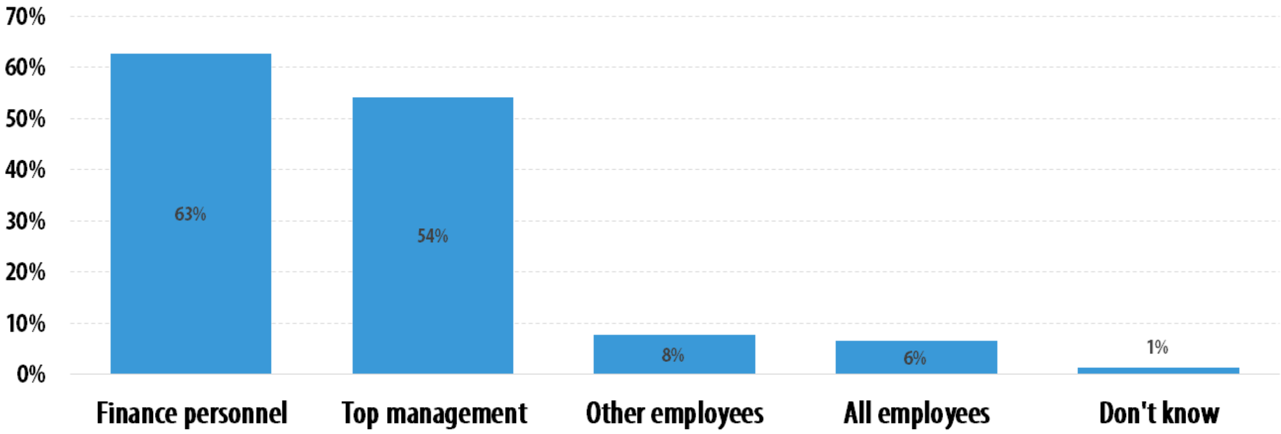
Slightly more than a half of businesses are actually ready to protect their financial transactions using some form of security solution. **54%** of businesses have fully deployed either an internal solution, or the one provided by their financial services provider. If we dig into the details, we see that **41%** of businesses have implemented an in-house solution and **45%** rely on a third-party solution from their bank. **32%** of businesses obviously take no chances and use a combination of these approaches, but still, **46%** of companies have either partially implemented a protection solution against financial fraud or have not implemented it at all. Among financial organizations themselves, a dedicated anti-fraud security solution is implemented in only **57%** of cases. Let us put a stress on the "only": although financial companies show a higher penetration rate, in our view the truly satisfying result would be 100% and no less.



Two findings deserve particular attention here. **59%** of businesses are conducting financial transactions using any type of device connected via a wireless network. While this alone does not necessarily impact the security, it increases the complexity of the chain of communication between a company and a bank. Complexity, in turn, results in a much wider attack surface, which, in the case of highly sensitive operations such as money transfers, has to be avoided. **27%** of businesses admitted carrying out financial transactions via a mobile device. Behind this number is the inevitable consumerization of corporate spend: even if a business secures B2B transactions with all necessary measures, its employees may still have access to corporate funds using their mobile phone – by managing a company-issued credit card, for example. This is particularly true for banks themselves and retail: they try to offer payment services to their customers in the most simple and user-friendly way, while at the same time struggling to maintain a proper level of protection against malware and phishing attacks.



Let's explore the "consumerized" part of corporate financial transactions. When corporate spend goes online, it appears to be no different from consumer behavior. For example, only **38%** of companies access Internet banking using a browser – a scenario in which additional security measures are easy to implement (like having a dedicated computer for financial operations). In other cases, such activity may be done via an application on a mobile device, which is highly convenient, but, again, badly affects the attack surface. In the third quarter of 2015 Kaspersky Lab discovered close to 300,000 new mobile malware samples, and, among them, 630 new banking Trojans, directly aimed at users' wallets. The same is true for online payment and online retail services, when used by corporations.

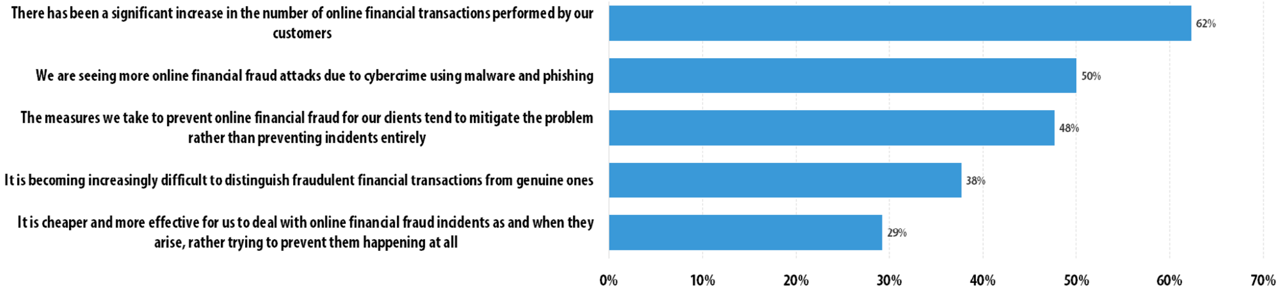


© 2015 AO Kaspersky Lab. All Rights Reserved.

The majority of corporate financial transactions are still handled by dedicated personnel and/or top management of the company. Still, **8%** of companies give the privilege (or a burden) of spending money to other employees, and **6%** of businesses provide such access to all employees, which is most likely is due to specifics of a particular business process.

Security of online financial transactions: a view from a bank

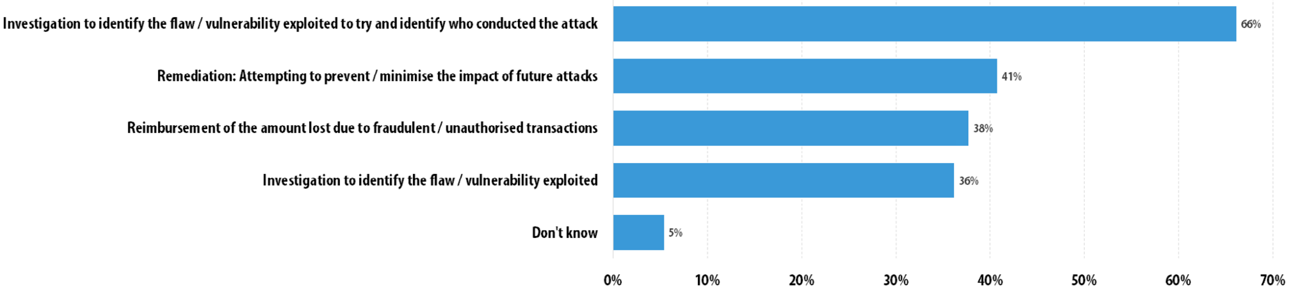
To conclude our report, let's look how banks themselves perceive the threat of online fraud. We specifically surveyed 130 banks around the world, and here's what they think:



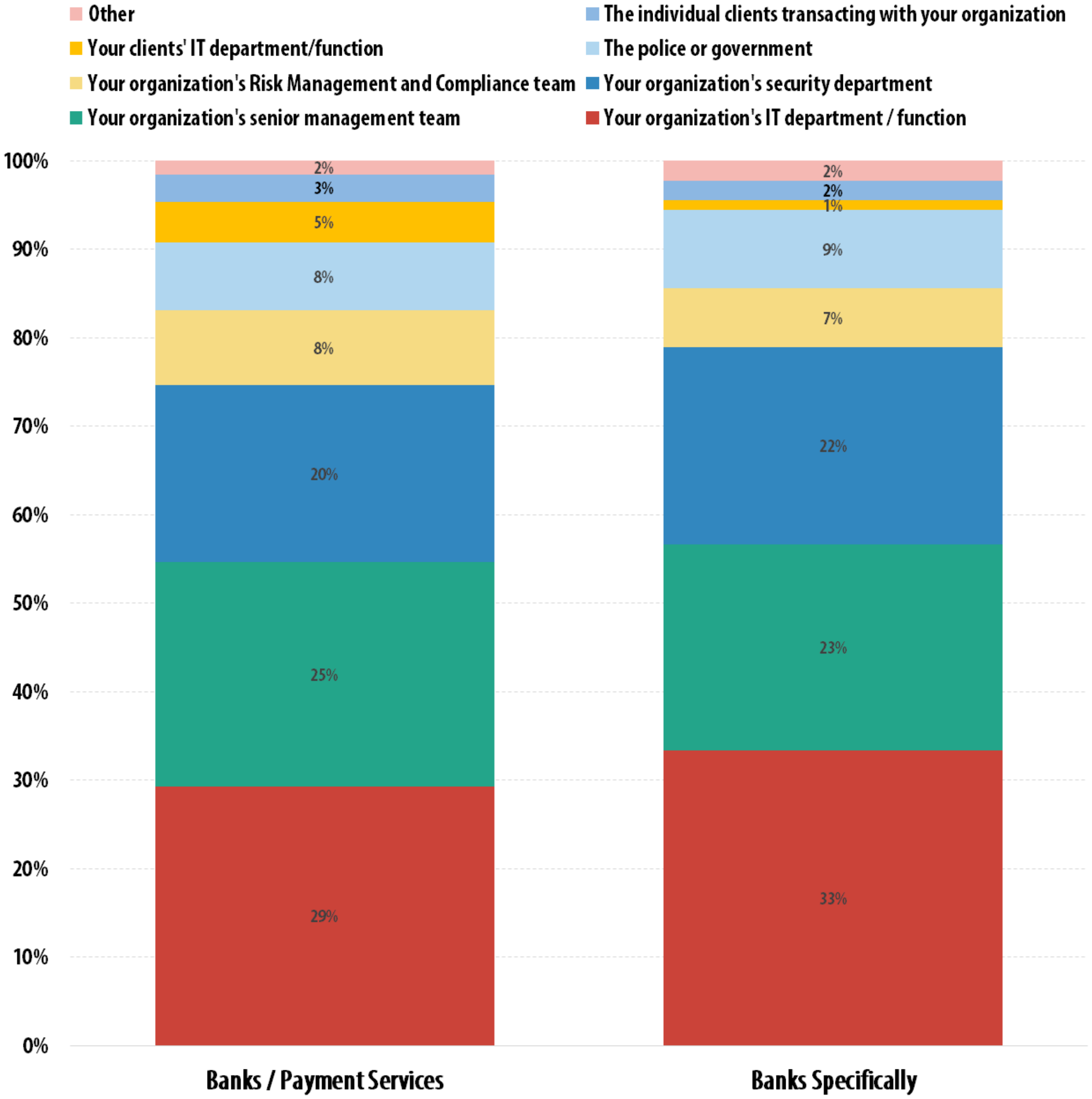
© 2015 AO Kaspersky Lab. All Rights Reserved.

Financial organizations confirm that the number of online transactions is growing steadily, and so too are the number of online fraud attacks. **48%** of banks admitted that what they do to address the problem can be described as "mitigation" rather than "prevention". Although it is important to invest in procedures designed to recover from an attack, we believe that, security-wise, it is important to pursue both goals: prevent as many attacks as possible from happening at all, and effectively mitigating those few that managed to bypass security measures for any reason.

Another significant concern for banks is distinguishing an attack from a normal customer activity: **38%** of financial organizations agree it's a problem. As we discussed at the beginning of the report, circumstantial data shows that banks still don't have enough experience in IT and IT security that is necessary to protect their customers from online fraud.



We found further proof of that when we asked banks who is actually responsible for keeping the number of successful online fraudulent attacks low. The answers show us that there is no uniform opinion among the banks. However for a security strategy to be effective, it requires not only the best technology, but also a coordinated effort within the organization.



Conclusion: The next big thing in online financial security

Our survey confirms that online financial fraud is one of the most sensitive topics for businesses. Other types of cybersecurity breaches, even the most dangerous such as cyberespionage, may still provide enough time to mitigate risk. Loss of money affects operations and reputation almost immediately. At the same time we observed that the perception of online fraud is sometimes far from realistic or as uniform as we would like it to be. Businesses are yet to decide upon who has ultimate responsibility for the prevention of such attacks. The scope of solutions aimed at securing financial transactions of any type is also not well defined: some companies rely on banks, some use third-party solutions in-house or develop their own routines, and some haven’t yet fully implemented a fraud prevention solution at all.

While the most feared and frequently used method of online fraud attacks remains the ‘good old’ phishing and malware, our experts see financial cyberattacks evolving into sophisticated state-of-the-art campaigns, for example, Carbanak. Security of many other entities has to be taken into account, such as mobile devices, WiFi networks and channels used for money transfers outside of the corporate perimeter. When complexity meets a lack of well-defined protection strategy, loss becomes inevitable. Businesses need to have a clear understanding of the threat, the strategy to prevent it, and the procedure and tools to mitigate it. The role of the security industry is therefore not only to provide new technology designed to prevent online fraud, but to share intelligence to help businesses define their strategy and shape the appropriate mitigation and response.

About Kaspersky Lab

Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest that is privately-owned. The company is ranked among the world's top four vendors of security solutions for endpoint users (IDC, 2014). Since 1997 Kaspersky Lab has been an innovator in cybersecurity and provides effective digital security solutions and threat intelligence for large enterprises, SMBs and consumers. Kaspersky Lab is an international company, operating in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide.

Learn more at www.kaspersky.com.

Securelist the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Kaspersky Lab B2B Blog

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab security news service

Kaspersky Lab Academy