Kaspersky Lab Report 2017

NEW TECHNOLOGIES, NEW CYBERTHREATS

Analyzing the state of IT Security in financial sector

Introduction

Cybercrimes are posing an increasing threat to businesses of all shapes and sizes. However, when it comes to cybersecurity, financial institutions have a difficult and unique task on their hands. This sector – including banks and other financial organizations – is a desirable target for cybercriminals looking to make money out of sensitive customer data, bank details, financial records and more.

Financial institutions therefore find themselves facing an increasing number of threats from targeted attacks to DDoS, and from phishing to POS and ATM security issues. And the stakes are high for these organizations. Those that get it wrong can suffer from monetary loss and even damage to their brand reputation. The financial retail industry is also finding itself in a unique situation, where it suffers from attacks both on its own infrastructure and on its customers.

There are steps financial institutions can – and should – be taking to protect themselves and their customers against attack. They need to establish which department within their business is responsible for IT security. They should understand the difference between compliance and security and they should exchange intelligence about threats within their sector. But are they taking these steps, and what more can be done? To find out, Kaspersky Lab together with B2B International has conducted a global study of **841** business representatives from financial services businesses in **15** countries.

The results of the study demonstrate that cybersecurity is a real concern for financial institutions but that there is much more they can do to share intelligence. There is, after all, safety in numbers.

A unique sector

The financial industry finds itself in an unusual position in terms of cybersecurity. As a sector it faces unique challenges in terms of infrastructure and customer demands, yet there is no let-up on the type of threats and losses these companies and their clients can be exposed to by cybercriminals.

Highly complex infrastructure

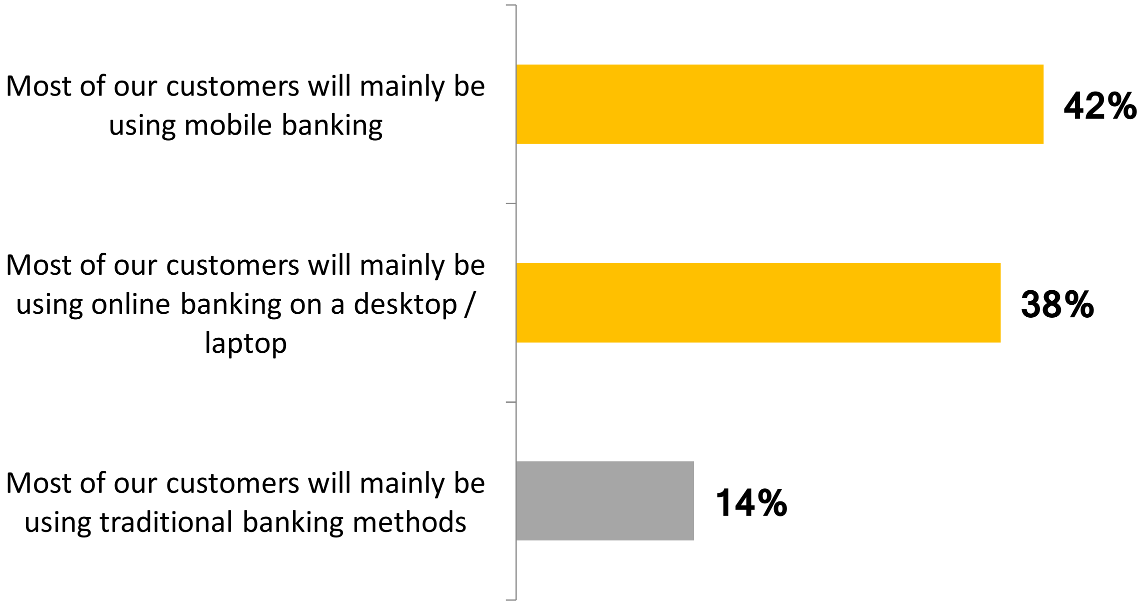
Financial institutions manage a highly complex array of infrastructure. The average number of end user devices in these companies is testament to this, with financial services firms having an average **9.9k** end user devices per company. These devices, of course, all need to be managed and provided with adequate protection in order to secure the business from cyber threats.

Banks have the largest number of devices to manage of any industry overall, with an average **12.2k** end user devices per bank. Only defense, telecoms, professional services and government get close to these figures by comparison.

Adding further complexity to protecting financial services companies from cybercriminals is their complex array of infrastructure and their use of hybrid cloud. Around **a third (31%)** of financial institutions use a combination of on premise and cloud-hosted VDI infrastructure, compared to just **a quarter (24%)** of non-financial institutions.

The growth of mobile banking

As well as having complex systems to protect, there is pressure on financial institutions to provide customers with access to mobile and online banking. On average **around half (47%)** of banking customers currently use mobile banking, and this is expected to increase, meaning that banks need to be in a position to protect a greater number of mobile users. **Around half** of banks also expect there to be a **20%** or greater increase in mobile banking use in the next three years, with **two-fifths (42%)** of banks expecting mobile banking to be the main form of customer interaction for servicing accounts in three years' time.



Most likely scenario for customer accounts servicing in three years' time

But mobile banking is not without its concerns for banks. Almost **four-in-five** (**78%**) are worried about the security implications of mobile and online banking growth and **one-in-ten** (**10%**) have serious security concerns. Among banks citing concerns, the top three worries include customers being frequently subjected to phishing or social engineering attacks (**46%**), customers being careless with their online behavior (**41%**) and the difficulty in balancing customer convenience with the need to prevent fraud (**38%**).

Customers are frequently subjected to **phishing / social engineering attacks**	**46%**
Customers are **too careless** in their online behavior	**41%**
Difficult to balance customer convenience with the need to prevent fraud	**38%**
The Internet connections used by **customers** are unsecure	**37%**
Customers' devices are often **infected with malware**	**31%**
It is **difficult to verify the identity** of those logging into online banking	**24%**
Development of banking websites and apps is **slow due to the need to consider security**	**22%**
DDoS attacks make it difficult to maintain a **high-availability service**	**21%**

Specific concerns – among banks citing concerns with online/mobile banking

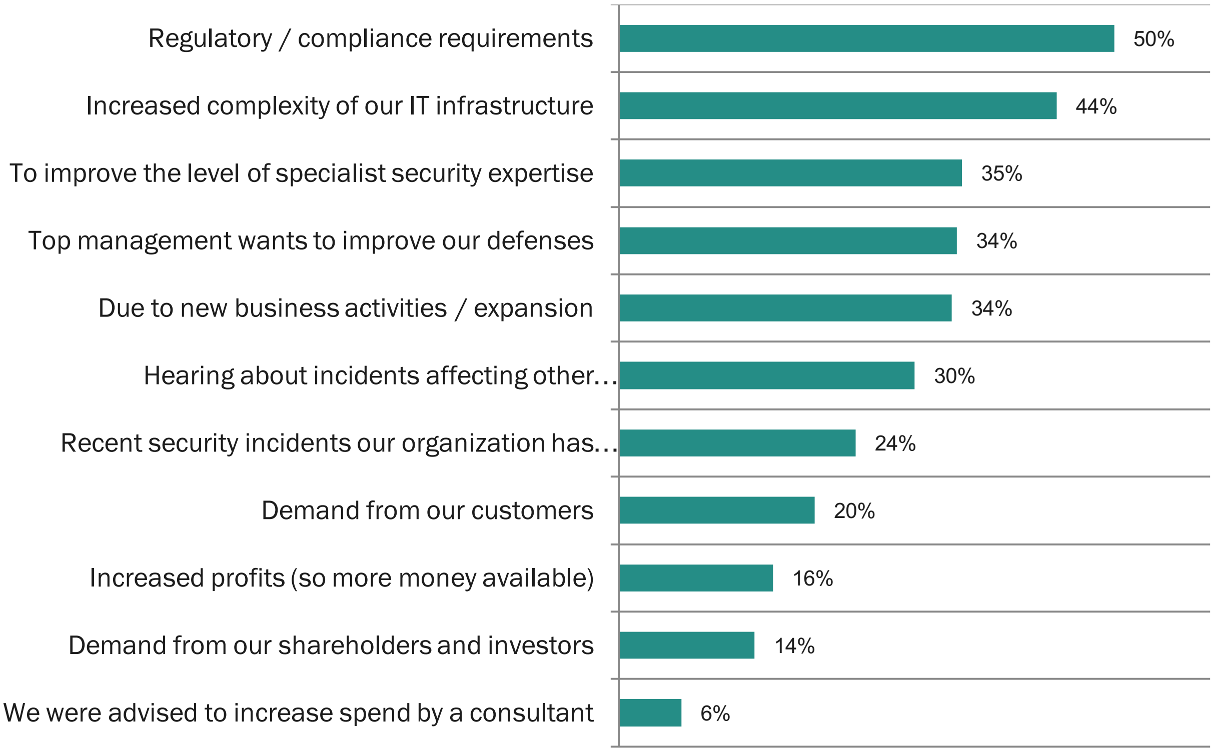
High spend on IT security

Banks uniquely spend more on IT security than any other sector, spending three times as much as comparably sized non-financial institutions. On average, a bank's IT budget reaches **$253m**, with **a quarter** of that (**23%**) being spent on IT security.

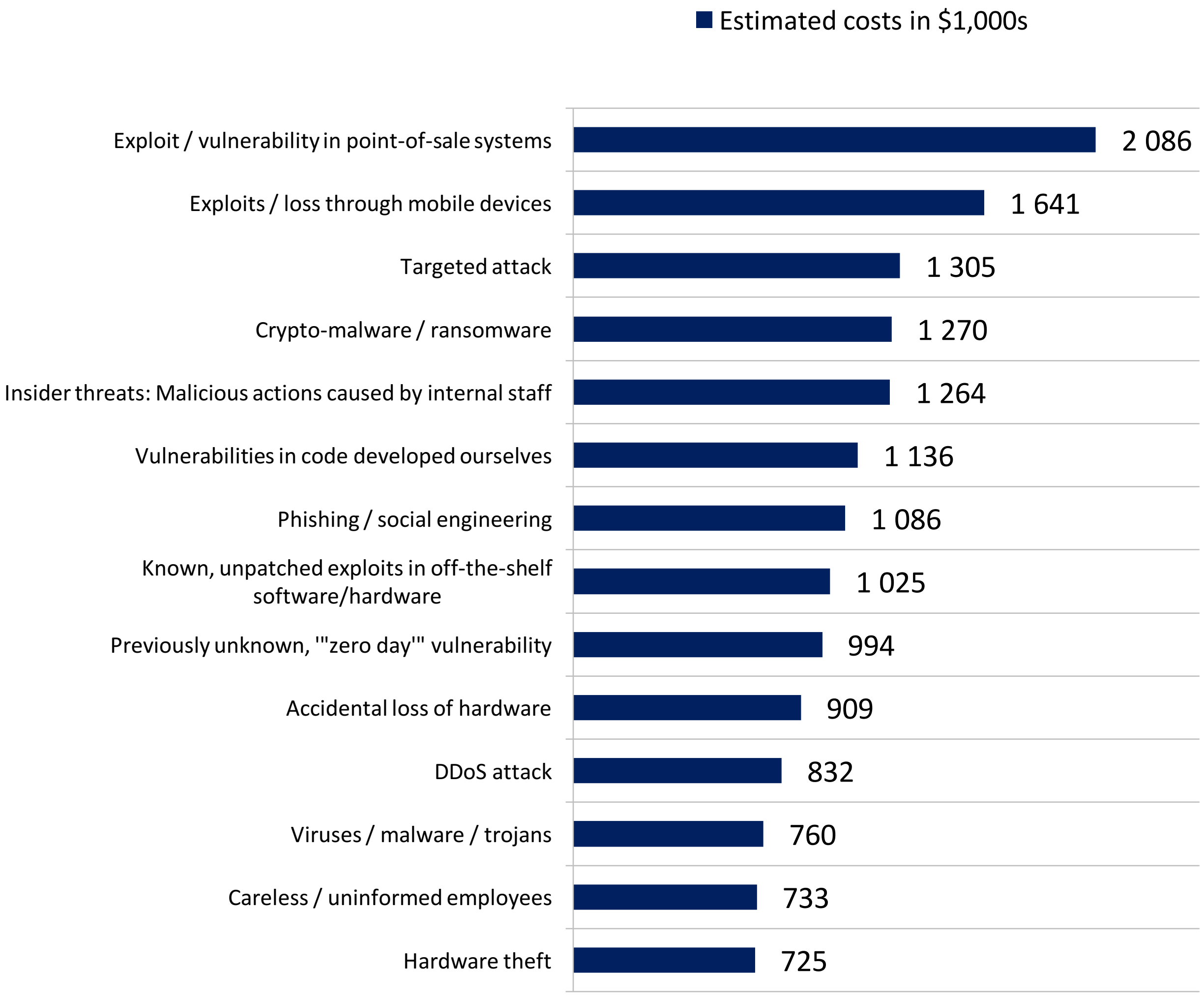
Yet despite the huge amount spent on IT security within the financial sector, cost control is not generally a priority for these companies. Financial institutions are driven by the need to protect their assets, comply with industry regulations and maintain their brand reputations. They are most likely to prioritize protecting the assets they manage – **26%** rank this as their number one concern, compared to just **one-in-ten (9%)**, which said that improving security without increasing costs was an influential factor.

83% Of Financial Institutions expect to increase their spend on IT security in the next 2 years

Drivers below…



This high spend on IT security should be put into context of the financial impact of a serious cyber security incident. The average cost per serious incident is **$988K** for banks and **$926K** for financial firms in general. That's **50%** higher than the cost of recovering from a data breach for other, similar sized firms. These costs include paying for additional internal staff wages, employing external professionals, lost business, the need to employ extra PR to repair brand damage, damage to credit/ insurance premiums and compensation payouts to customers. Following a breach, these businesses must also spend money on preventing future breaches – including covering the costs of new staff, training and software and infrastructure improvements.

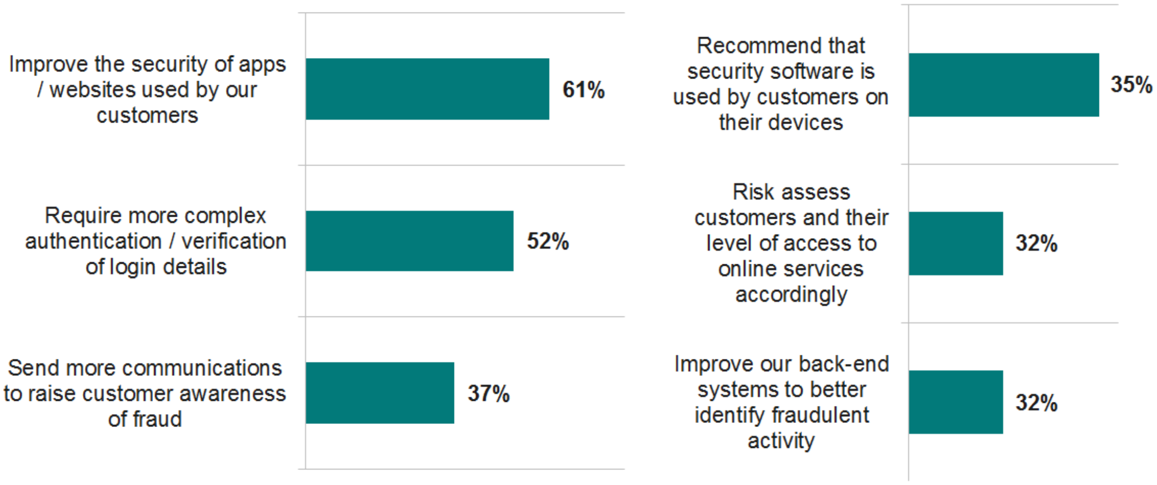


Cost of events involving different attack vectors

Patterns in the strategies banks adopt to fight fraud

Fraud too, is an expensive and worryingly common threat for banks. As many as **7-in-10** banks have been affected by financial fraud and when it strikes, fraud is costly. The average loss per incident for a consumer customer suffering from financial fraud is **$1,446**, rising to **$10,312** for business customers. And it doesn't stop there. Overall, **59%** of banks expect financial fraud losses to increase over the next three years, demonstrating the need for more robust and effective security solutions to be put in place.

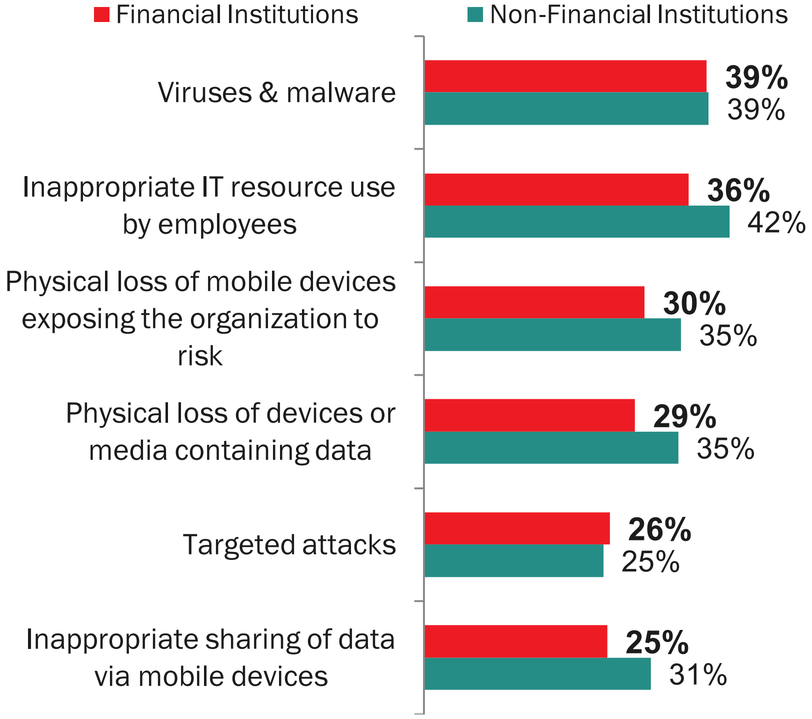
Recognizing that customers could be the weakest link in their IT security (**63%** of banks believe this), banks understand the importance of communication with customers to prevent online fraud. **35%** of banks plan to encourage customers to use security software on their devices and **a third (32%)** plan to risk-assess their customers.



Strategies banks will adopt to combat online financial fraud in the next three years

Protecting themselves from cyber threats

Although most financial institutions report fewer security events than non-financial institutions of a similar size, they are nonetheless subject to a range of cyber threats, from malware to inappropriate IT resource use and physical device loss.



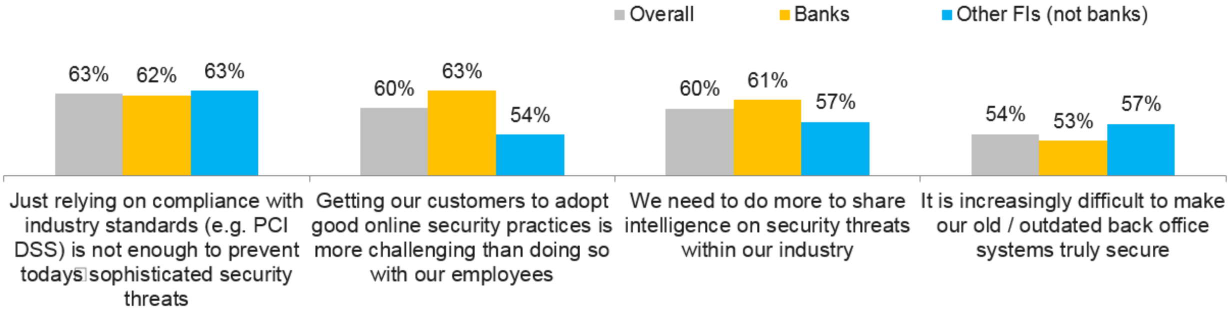
Security events experienced by financial and non-financial organizations

What's more, these security incidents, when they happen, are expensive to rectify. The study shows us that exploits in point-of-sale items are particularly expensive, costing an average **$2,086**. Exploits through the loss of mobile devices (**$1641**) and targeted attacks (**$1305**) are the next most expensive threats to recover from.

Understanding the difference between compliance and security

The need to comply is still the biggest driver for financial organizations to increase their IT security budgets - as many as **50%** of financial institutions are driven by the need to comply, compared to just **32%** of non-financial institutions.

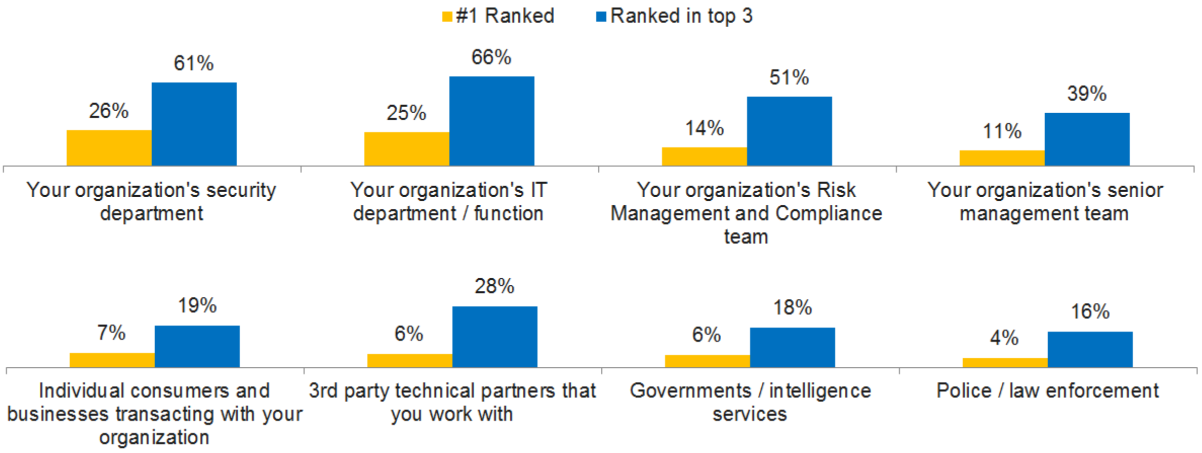
There is also a growing awareness that being compliant is no longer enough, but there is still room for improvement here. Many financial institutions (**63%**) see standard compliance frameworks, such as PCI DSS, as merely a 'starting point' when putting together their security strategy, knowing that this alone cannot protect them from today's sophisticated security threats.



Agreement with statements regarding the financial services industry

Knowing where the responsibility lies

Financial organizations need to better understand where the responsibility lies for IT security within their own businesses in order to better combat threats. Although **26%** ranked their firm's security department as the department with top responsibility for preventing IT security events, **39%** also ranked senior management amongst the top three responsible entities. Many financial institutions see the responsibility as being shared by other parties such as customers, third parties and government/ law enforcement.



Entities seen as responsible for preventing IT security incidents

Banks and financial firms, by design, often have this responsibility shared across multiple teams, which may present them with additional challenges when dealing with cyber threats.

Accepting outside assistance and intelligence

Financial institutions appear to be more reluctant to accept outside assistance when it comes to cybersecurity. Only **45%** of these organizations agree that they need external consultants to conduct an IT security audit of their organization, compared to **52%** of non-financial institutions. Financial organizations are also less willing to accept that their knowledge of the security threats targeting their business is less than ideal (**42%** compared to **48%** of non-financial institutions).

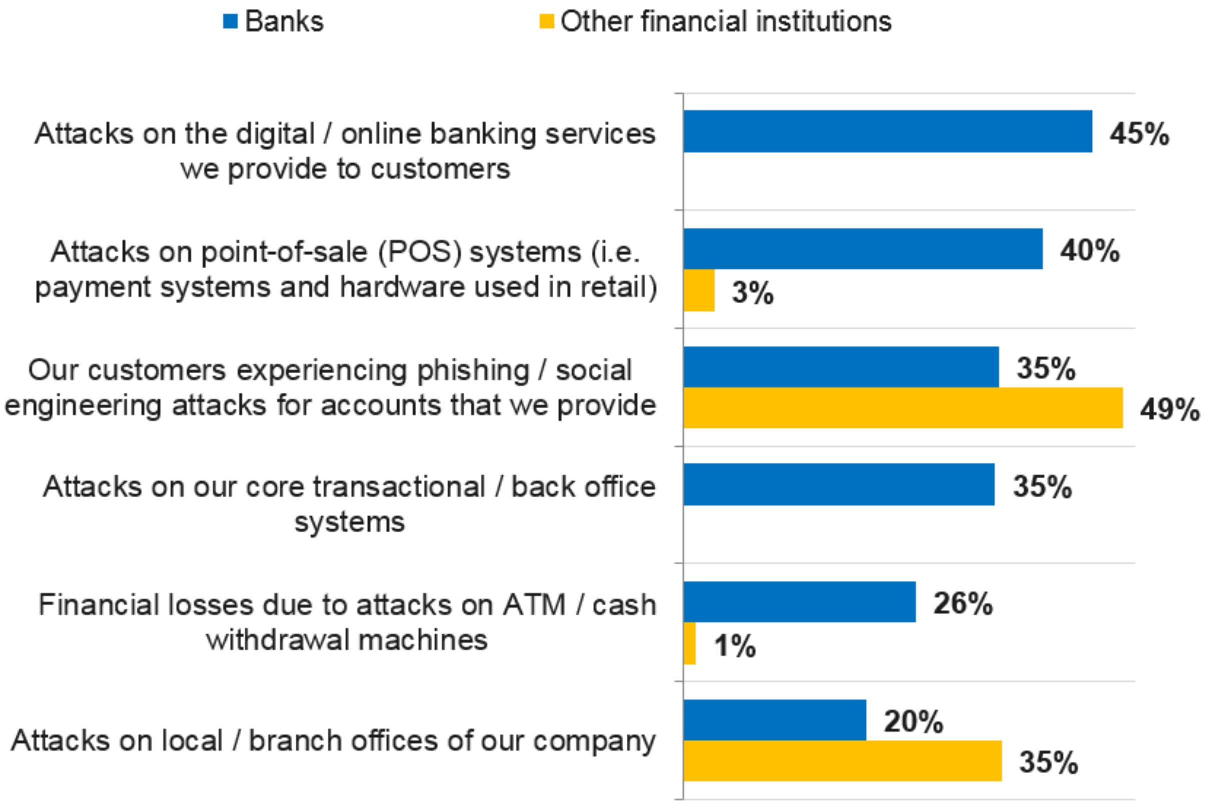
The study suggests that financial organizations are aware that this attitude is potentially putting them at risk and as a result, **a third (31%)** plans to seek external help and security intelligence in the next 12 months.

Current and future threats for the financial sector

Financial organizations have to navigate a complex threat landscape and there are a number of specific threats that businesses in this sector have to address, for example by putting anti-fraud measures in place, to mitigate the risk of DDoS, and from protecting POS technologies from exploitation to ensuring the security of ATMs.

Potential weak spots

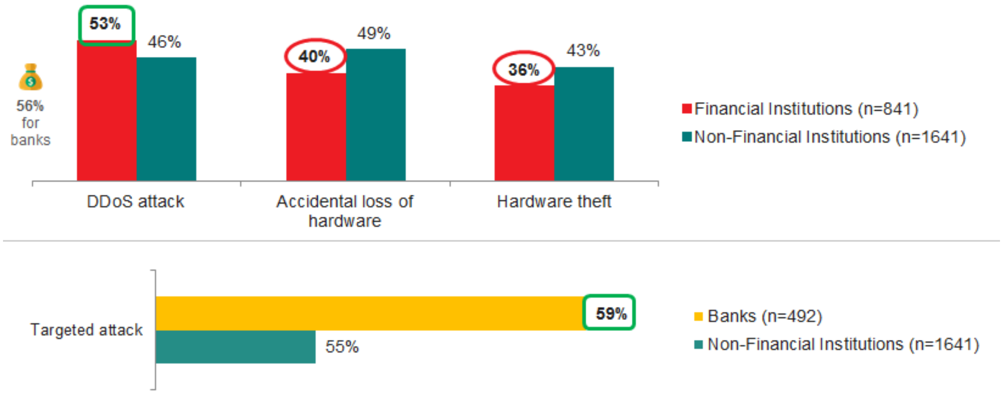
Alongside the concerns already discussed in this report, almost half of all banks questioned in the study cited potential attacks on their POS or digital banking services as a major security concern and over a third are now fearful of attacks moving into their core transactional systems. The top five major concerns can be seen in the table below.



The top cybersecurity challenges to financial institutions

Taking a closer look at the top three general IT security concerns in the sector highlights a disproportionate fear of DDoS attacks (**53%**) among financial institutions, with the accidental loss or theft of hardware cited as a key IT security challenges for **two-fifths** of financial institutions. Banks meanwhile are particularly fearful of targeted attack (**59%**).

With DDoS such a concern, financial institutions need to put measures in place to protect themselves from this threat effectively. But as many as **36%** of financial institutions admit they are not sure of the most effective strategy to combat threats like targeted attacks and DDoS.



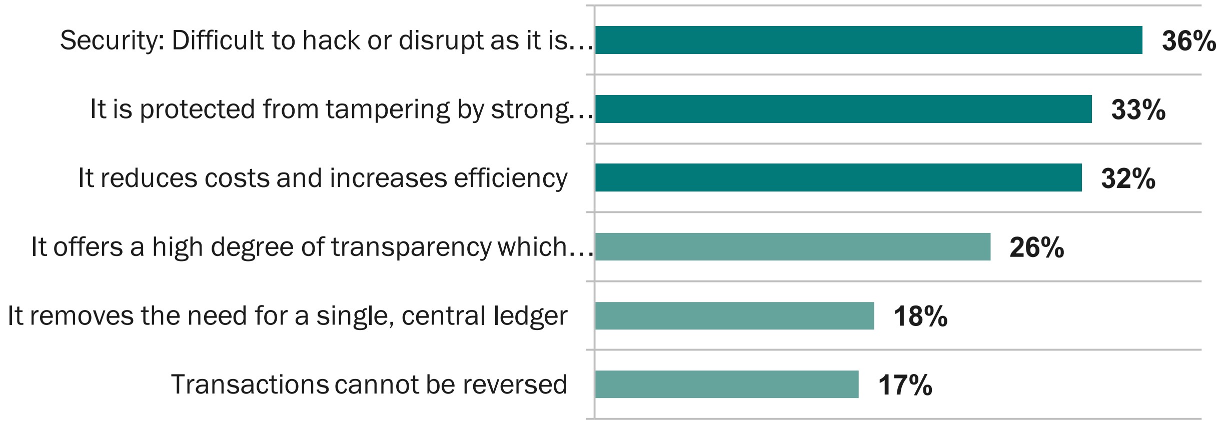
The most worrying attack vectors for financial institutions

Targeted attacks also make financial organizations feel vulnerable, with **38%** of financial institutions being specifically targeted in this way. Businesses in this sector are much more conscious of targeted attacks and their impact on data loss than their non-financial counterparts (**53%** compared to **45%**) and perhaps that's no surprise considering a single targeted attack costs a financial institution **$1305** on average.

Expecting the blockchain

With the threat landscape evidently causing banks and financial institutions concern, it is understandable that banks are exploring the latest technologies to help them mitigate risks. Indeed, **51%** agree that innovation can have a meaningful impact on the security of transactions.

Blockchain is one example of such a technology because it is difficult to hack and is protected from tampering by strong encryption techniques. Very few companies are currently using blockchain in live production projects (**4%**) but **40%** of banks are planning to use the technology for test and trial projects and just **one-in-ten** banks are not considering blockchain technologies at all. However, despite its planned adoption for testing purposes, only **one-in-five** see blockchain completely replacing traditional back office systems, even in ten years' time.

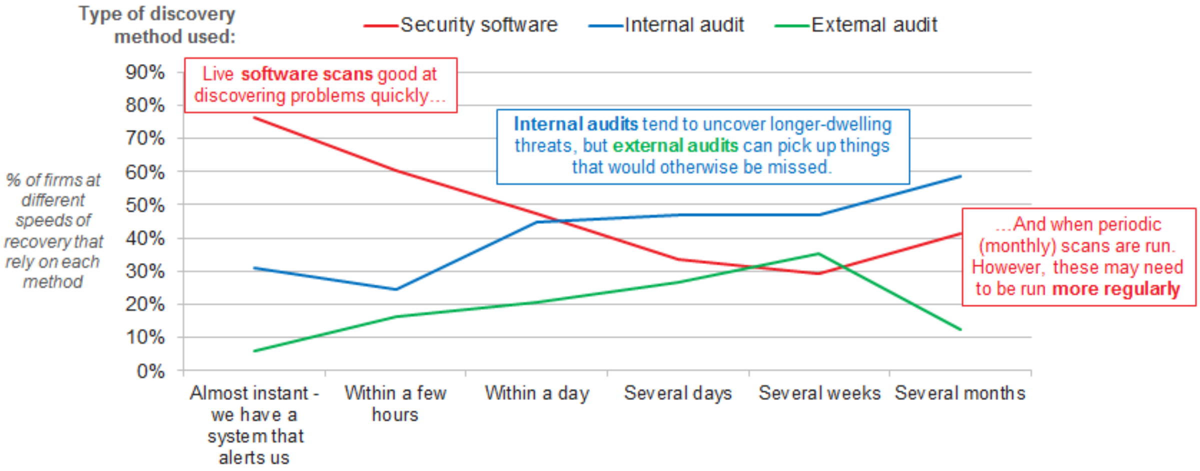


Key perceived drivers towards blockchain adoption

A similar pattern can be seen for contactless payment technologies and SWIFT technologies, with roughly half of banks thinking these present significant security risks.

A way forward: tailored security solutions plus intelligence sharing

The study tells us that in general, financial institutions have better security systems in place to detect attacks, than other organizations. Nonetheless, for **a quarter (24%)** of banks that have a security incident, it is the customers that end up noticing the problem, suggesting that there is a need to go beyond prevention technologies to protect these organizations effectively.



Live **software scans** good at discovering problems quickly…

Internal audits tend to uncover longer-dwelling threats, but **external audits** can pick up things that would otherwise be missed.

…And when periodic (monthly) scans are run. However, these may need to be run **more regularly**

Responses required for discovering long-standing attacks

Conclusion: The need for advanced technologies and security intelligence

The financial industry has found itself in a unique situation when it comes to cybersecurity. Attacks on these companies' core infrastructures are as frequent as attacks on their customers. We have found that customer losses, as a result of a cybersecurity incident, are typically thousands of dollars. And what's more, when there is a large number of such incidents - which is often the reality - this can also lead to significant financial losses for the bank involved. Unlike complex and targeted attacks at the banks' core infrastructure, this challenge can be addressed using existing protection methods. With banks concerns over threats such as phishing being the highest, fraud prevention methods need to be applied more actively, and modern approaches should be applied - such as the behavior-based detection of irregular activity with intelligent algorithms.

The study shows us well-known prevention techniques are very efficient for detecting widespread attacks. Expanded security measures meanwhile, tend to uncover longer-dwelling threats. At the same time, the security of financial transactions may be significantly improved in the future using modern technologies such as blockchain. Before this happens, though, the need for modern, intelligent solutions to detect complex and targeted attacks is high. Prevalence of complex attacks is also the argument for intelligence sharing within the financial services sector.

Although intelligence sharing has obvious benefits, the study shows us that as many as **6-in-10** financial organizations are yet to subscribe to third-party threat intelligence, and the same number admit that more must be done to share intelligence on security threats within the financial services industry. The financial industry, like no other, depends on new, customized security technologies to better protect existing infrastructure and financial applications, from ATMs to core data centers. It also needs security intelligence to efficiently respond to new cyberthreats and to predict the evolution of the threat landscape for the near future.