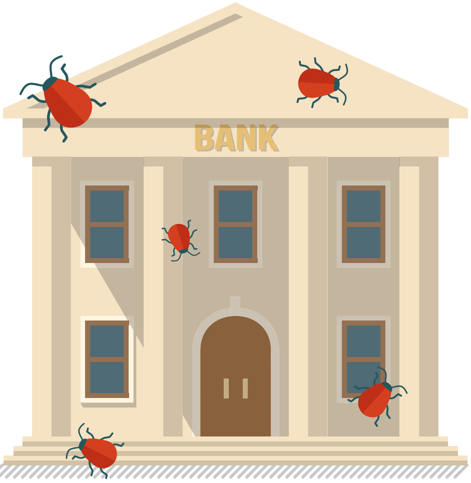
SECURITY SNAPSHOT

Locking the Safe:

Protecting Banks and Financial Services Firms from the Most Advanced Threats

KASPERSKY lab

$1,165,000	Cost of a cybersecurity incident to a financial institution in the U.S.
$2,086,000	Cost of an attack on a financial organization's point-of-sale (POS) system
$1,641,000	Cost of an attack on mobile devices that serve financial institutions
$1,305,000	Cost of a targeted attack on a financial institution[1]



Financial Services: Facing Unique Challenges

In the world of cybersecurity, the financial industry finds itself in a unique position, working to balance customer demands with infrastructure needs. While cybercriminals never let up in their quest to infiltrate their systems, IT professionals must work to fulfill cybersecurity needs as well as meet the customer demands of the market. It's a fine line to walk between functionality and data security.

Externally, both mobile and online banking place continual demands on IT security. Approximately 47% of banking customers use mobile banking—a number that is expected to grow by 20% in the next three years. With costs of a mobile banking security incident averaging at more than $1.6 million, it's no wonder that 78% of banks cite worries about the security implications around the growth of mobile and online banking.[2]

Internally, financial institutions manage a highly complex infrastructure with an average of 9,900 end user devices per company. Banks have the highest number of devices to manage at 12,200 end user devices per bank.

For all financial organizations, the three most costly incidents are breaches to point-of-sale (POS) systems at $2,086,000, breaches to mobile devices at $1,641,000, and targeted attacks that cost an average of $1,305,000. Banks and financial institutions are aware of the seriousness of the issue. In fact, out of the average bank budget of $253 million, nearly one-quarter (23%) is spent on IT security. But there is always room for improvement. How can financial organizations ensure that they are allocating the right amount to ensure protection against these very costly breaches? We'll take a closer look at the threat landscape and how to bridge it.

[1, 2] Kaspersky Lab's *New Technologies, New Cyberthreats: Analyzing the state of IT Security in the financial sector*

Understanding the Threat Landscape for Financial

With the cost of a cybersecurity incident at a financial institution going as high as $1,165,000, banks and financial institutions are right to invest in IT security with a robust, multi-layered system. The costs to banking customers add up, too. Business customers of these institutions see average losses of $20,625 for cyberincidents, while consumers see losses of $2,062. In order to avoid the unwelcome scenario of passing costs along to customers, it's important to understand exactly what threats plague financial institutions.

Phishing

One of the most pernicious threats to financial institutions is phishing and social engineering. According to a survey of financial services firms by Kaspersky Lab and B2B International, 46% say that customers are frequently subjected to phishing or social engineering attacks, and that they cost, on average, $1,086,000 due to staff downtime and damage to company reputation, credit ratings, and insurance premiums.

In 2016, the share of financial phishing increased 13.14 percentage points to 47.48% of all phishing detections. This figure is an all-time high for Kaspersky Lab statistics for financial phishing caught on Windows-based machines.

Banking Malware

In 2016, the number of users attacked with banking Trojans increased by 30.55% to reach 1,088,900. The estimated cost of a malware attack is $760,000, including all mitigation costs incurred to recover from the attack.

Android Banking Malware

In 2016, the number of users who encountered Android malware increased 430% to reach 305,000 people worldwide. Most of this activity can be attributed to one Trojan that has been exploiting a single security flaw in a popular mobile browser. Even so, just three banking malware families accounted for attacks on 81% of users.

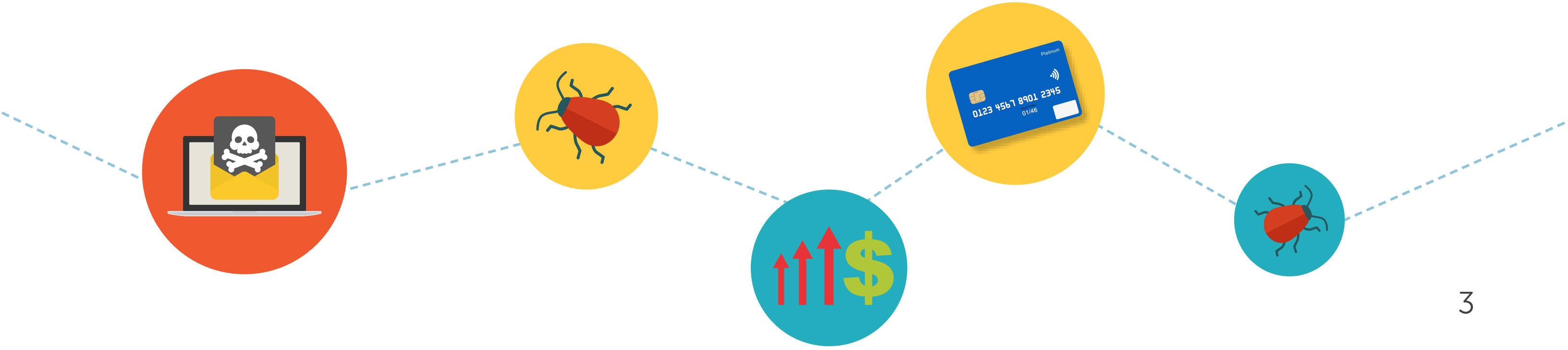
Point of Sale (POS)

40% of banks cite attacks on their point-of-sale (POS) systems as a major concern for their IT security, according to our survey. Along with attacks on their digital or online banking services, POS are yet another portal for cybercriminals to gain access to your data.

Advanced Persistent Threats (APTs)

Advance Persistent Threats—or APTs—are among the most expensive attacks a financial institution can face, costing an average of $1.3 million in mitigation costs, including public relations, brand damage, internal staff time, and the cost to hire external consultants.

In a targeted attack, a bank or financial institution is specifically targeted by cybercriminals for financial gain, and many of these attacks are quite persistent. Law enforcement personnel note that cybercriminals have become increasingly sophisticated in getting financial institutions to transfer large sums of money. With a multi-layered security solution, an IT staff to install and maintain the solution, and the training and knowledge of your own



10 Tips to Safeguard Your Firm

The average cost per serious cybersecurity incident is $988K for banks and $926K for financial firms. That's 50% higher than the cost of recovering from a data breach for other, similar sized firms. Avoiding costly mistakes such as these is in your hands if you follow a few key security practices.

1. Protect against targeted attacks by protecting against the easiest points of entry.

TAKEAWAY:
Targeted attacks are likely to be executed through third parties or contractors. These service providers typically have weak protection or no protection at all that can be used as an entry point. It's easy to target these organizations with phishing emails that can download malware that can then be used against your firm. Make sure that your contractors and vendors can explain their security practices.

2. Be aware of the simple techniques cybercriminals are using. Less sophisticated attacks are on the rise.

TAKEAWAY:
Cybercriminals have learned that they don't have to bother crafting complex malware when they can buy something off-the-shelf or use social engineering or phishing and get the same result. Cybercriminals are looking for attacks that cost less and require less effort.

3. Compliance alone isn't enough.

TAKEAWAY:
In order to be truly protected, you have to go beyond just meeting regulatory requirements. While many companies cite compliance as the main reason for investing more in cybersecurity, it is important not to just meet this minimum threshold, but to take a more thorough approach by looking at your firm's specific vulnerabilities and instituting measures to protect them.

4. Regular penetration testing is key.

TAKEAWAY:
It is not a question of *if* your firm will be attacked but *when*. In order to understand where your vulnerabilities lie, it's important to test them through regularly scheduled penetration testing. If you know where the holes are, you can patch them up.

5. Insider threats are real.

TAKEAWAY:
Even well-intentioned employees can be exploited by cybercriminals, which is why it is important to protect beyond the perimeter and implement techniques to detect suspicious activity inside of it. There are still marketplaces on the dark web where third parties can hire insiders to become a company's employee with a hidden agenda, or where employees can sell access to the company that they work for. Don't be caught off guard. Not all threats are from the outside.

6. There is always a new freshman class of cybercriminals. Know what new threats are out there.

TAKEAWAY:
Entering the world of cybercrime has never been easier. With turnkey tools, cybercriminals are always looking for new ways to expand their businesses—and new people to recruit to help them. Understanding the threat landscape is an important way to protect your business.

7. Take action now to ensure protection.

TAKEAWAY:
Once you understand the threat landscape, it's important to take action. An organization may not have had any incidents over the previous year, but that does not mean that the risks are not there. For example, banks know that the threat of mobile malware is there, so it's important not to wait until a problem emerges. Act now to protect your firm.

8. Money is just one type of loss.

TAKEAWAY:
Public relations issues, damage to company reputation and staff downtime all contribute to the total costs of a cybersecurity incident. Not all losses can be immediately measured in dollar signs, but the costs do add up.

9. Security is a shared responsibility.

TAKEAWAY:
Since security challenges are constantly growing and becoming more complex, collaboration across your organization and coordination of efforts across departments is vital. When each department knows what their responsibility is, you can shorten your response time to threats and ensure that you are better protected.

10. Understand the security weaknesses of new technologies and take steps to protect your firm.

TAKEAWAY:
With new technologies come new vulnerabilities. Digital financial technologies are growing fast, and it's important to stay ahead of the threats so that you can protect your organization. Ask questions and dig for answers when purchasing a new technology.

True Cybersecurity

Kaspersky Lab's True Cybersecurity approach combines multi-layered security with cloud-assisted threat intelligence and machine learning to protect against the threats your business faces. True Cybersecurity not only prevents attacks, but also predicts, detects and responds to them quickly, while also ensuring business continuity for your organization.

Try Kaspersky Lab >

Join the conversation

Like us on Facebook

Follow us on Twitter

Join us on LinkedIn

Watch us on YouTube

Review Our Blog

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 usa.kaspersky.com.

Contact Kaspersky Lab today to learn more about Kaspersky Endpoint Security for Business and our other IT security solutions and services:

usa.kaspersky.com/business-security

(866) 563-3099

corporatesales@kaspersky.com

KASPERSKY lab

THE POWER
OF PROTECTION