Building a safer future in Finance

kaspersky BRING ON THE FUTURE

go.kaspersky.com/finance 2021

New trends – new threats

‘Follow the money’

$18.5 million

Accenture has estimated the average annualized cost associated with data breaches for Financial Services companies globally at $18.5 million

x300

A report by Boston Consulting Group indicates banking and financial institutions are 300 times more at risk of cyberattack than other companies.

According to the catchphrase beloved of investigative journalism, the solution to any criminal mystery can be unlocked by following the money trail back to its source.

So, before reviewing the new trends in Financial Services – and the new threats they attract – it is important to keep in mind cybercrime will always ‘follow the money’.

This includes not only attacks on financial institutions and their customers, but also any connected third-parties. Any organization that holds or controls funds of any kind will always be a top target for cybercriminals.

The question today is threefold: what happens when the industry changes; how do threat actors' tactics change; and how should Financial Services providers respond?

Eight trends in financial innovation and keeping customer trust

69%

69% of bank cyber executives say their organization has invested heavily in data security.

KPMG's Consumer Loss Barometer

The threat of losing customer trust constantly hangs over the Finance industry. Once earned, trust is more precious than the gold standard against which money used to be measured. As the 19th century Dutch saying goes: 'Trust arrives on foot and leaves on horseback'.

The Finance industry has understood that cyber trust is a number one priority. Inevitably this means investment in technology with the aim of making products and services more secure.

In this paper we will examine eight key trends in the Financial Services landscape in 2021. We will also identify how cyber risks connected with these new trends can potentially damage customer trust.

Cloud Compromise

Regulatory Challenges

The Internet of Things

Blockchain

FinTech

The Open Banking Revolution

Machine Learning and AI

Digital Transformation

Trend #1: FinTech

A vibrant and maturing market

For years, banks were able to tune out the sound of footsteps as technology made its approach. Banks were, by and large, slow to adapt until a few years ago. 2016 (or thereabouts) marked the Rubicon in the technological trajectory of Financial Services. Around the world, the era of Open Banking began to dawn. Each market saw that dawn according to its own unique rhythm and regulatory framework.

The sheer pressure that this change has brought to bear on banks hastened the development of a vibrant and maturing FinTech market, offering standalone services.

FinTech startups commonly found it easier than banks to attract the iconoclastic, visionary developer talent necessary for creating truly innovative services. But absent the strict and trusted regulatory framework of traditional Financial Services, and the FinTech market brought with it a new level of risk.

While high risk and volatility is common to all new technology, the absolute pre-eminence of trust when it comes to Financial Services renders risk even more acute. FinTech organizations are more dependent on cybersafety than all other digital platforms.

'Partially dissolving the traditional secure perimeter of retail banks and connecting innovative FinTech solutions to heritage infrastructures may inadvertently increase the opportunities for cyberattacks.'

98% vulnerable

Research by ImmuniWeb indicates 98% of the top 100 global FinTech startups are vulnerable to major cyberattacks.

$22.8 billion

CB Insights research revealed investment in FinTech was nearly $22.8 billion in investments from 614 deals in the first quarter of 2021.

70%

Keeper Security research showed 70% of Financial Services organizations reported experiencing a cyberattack in 2020 (up 20% on 2019).

FinTech threat spotlight: too young for Basel?

While traditional banks are by no means immune to cyberthreats, they are at least mature enough to have developed a robust procedure for ensuring compliance and preventing repeat mistakes.

The Basel Accords, a set of regulatory standards strengthening banks' minimum capital ratios and liquid asset holdings and funding stability, are the perfect example of how an industry's maturity can result in a tough protective framework.

Fast-forward to 2021 and banks rely heavily on (usually) much smaller third-party FinTechs to supply the innovative services that their customers (business and consumer alike) now expect.

Consequently, the risks have increased. The demand for innovative and fast financial services is growing constantly. Loosely regulated FinTech startups are launched without sufficient consideration of all aspects of their security framework. The post-pandemic work-from-home economy has exposed the vulnerability of organizations that transitioned fast to a remote working model, without implementing sufficient security or training employees on preventing cyber risk. Users accidentally reveal key data by mistake on unfamiliar FinTech platforms. Growing identity theft and online fraud exploit our increasing reliance on mobile devices for managing all personal financial matters.

As a consequence, more financial data breaches occurred in 2020 than any previous year.

On the bright side, the FinTech sphere, like all startup industries, does benefit from advanced technological literacy, and there is a huge drive among many operators to develop robust protections and cyber defense protocols.

13th century

In Venice bills of exchange were developed as a legal device to allow international trade without the need to carry gold.

1717

The Bank of England pioneered the use of printed slips with scrollworks at the left-hand edge. This could be cut through, leaving part on the cheque and part on the counterfoil.

1920

Credit cards introduced in the US by oil companies and hotel chains.

1959

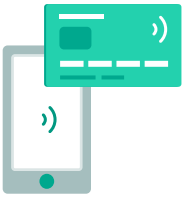
American Express cards switched to a plastic version.

1994

The first online purchase was carried out in the United States.

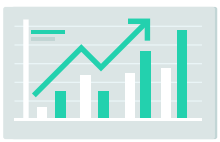
1997

First internet banking service introduced by Nationwide Building Society.



2007

First contactless payment takes place. A mobile phone with built-in contactless payment card technology piloted in London.



2022

The combined total of payments in the UK is expected to almost double **from 9.9 billion in 2012 to 17.3 billion GBP.**

Trend #2: The Open Banking revolution

The FinTech ecosystem: strength in numbers or a war on too many fronts?

A Forbes article - Open Banking Is Now Essential Banking concludes - 'The bottom line is that banks strengthen customer loyalty by offering APIs that integrate multiple external services with customer bank accounts. When businesses and people have all they want at their fingertips, they're less likely to seek out alternatives. The trend toward open banking is here to stay, and it's transforming into a full open finance system with each passing month and new API integration.'

The vision, articulated most clearly in a PwC paper is to foster a healthy FinTech ecosystem, in which Financial institutions, Governments and entrepreneurs act in perfect symbiosis to create value for customers, businesses and the wider economy. This plurality of players increases the overall energy of the system, creating the perfect conditions for ongoing transformation and innovation.

Like any ecosystem, however, an attack on one element can destabilize the whole. Each organization bears the responsibility not only for protecting itself from cyberattack, but for defending its entire connected ecosystem.

In the era of Open Banking, customers, whether business or consumer, are connected by a proliferation of devices adding to the number of fronts which must be defended from cyberattack. And as the number of connected parties increases, so too does the number of potential targets for cybercriminals.

The EU's Second Payment Services Directive (PSD2) came into force in January 2018, forcing consumer banks to open up their front end to third party developers, and implementing a range of rules designed to reduce new risks that might arise.

Even in markets (such as US) that do not have such regulation, all the major Financial Services providers are compelled by market demand to implement APIs of their own.

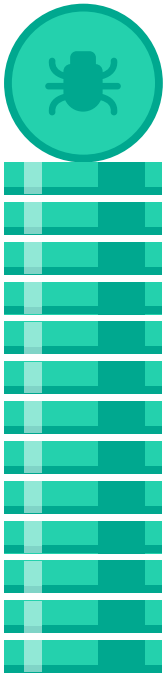
Lastly, regions such as Africa, which have traditionally taken a mobile-first approach to internet technology in general, are naturally poised to adopt Open Banking principles.

New technology – new threats

Financial Services providers are far from alone in turning to the use of third party provider services and suppliers to drive resource-efficiency, results and the bottom line. The cybercrime ecosystem is developing in parallel to the FinTech ecosystem and cybercriminals can be just as innovative as the technology they wish to attack.

The novelty of innovative FinTech technology is what gives it its power, yet novelty can also be an Achilles heel. Organizations that harness untried innovation can make themselves as vulnerable to cyberattack as a newborn baby is to infection.

Turning to the dark web for DIY malware or ransomware kits, flaw intelligence and other cybercrime products and services, criminals are assembling arsenals for launching targeted attacks that sting more than ever.



- **According to Experian, online payment services logins (such as PayPal) can sell on the dark web for as little as $20.**
- **Ransomware can be purchased on the dark web for a mere $1, with bespoke packages costing up to $3,000.**
- **Dark web ransomware samples and builders can be bought for $300 to $4,000. Ransomware-as-a-service rentals cost $120 to $1,900 per year.**

Open Banking threat spotlight: connectivity itself

There has been a significant increase in Open Banking fraud attempts. Threats on the rise include:

- Account takeover
- Authorised Push Payment (APP) scams
- Unauthorized third-party access to customer information resulting from impersonation of legitimate third-party providers
- Social engineering and phishing – gaining unauthorised access to financial data to authorize fraudulent payments
- Scam attacks utilizing customer data breaches

Open Banking services - dismantling the traditional security perimeter and connecting FinTech solutions to bank infrastructures - is gathering speed in 2021. However the complexity of the customer data supply chain in the context of Open Banking's compulsory sharing is a weak point in itself.

Devices are not the only entry points that multiply. The number of vulnerabilities explodes with the involvement of even greater numbers of the four traditional entry points for attack: removable media, internet, email and fixed connections.

Sharing financial data between more payment service providers inevitably offers cybercriminals a greater number of potential attack points to infiltrate and steal customer data. Global regulation remains inadequate. Cybercriminals can establish FinTechs with legitimate functionality and an additional covert task of removing data. End-users are vulnerable to phishing emails purporting to come from third-party providers. Cybercriminals can piece together data from related customer accounts to attempt identity theft and fraud.

Freedom, with limits

Returning again to the make-or-break-it power of trust, this new openness requires strict limits, providing for the security of stakeholders all along the value chain – from provider to customer.

Financial Services providers need to take a 360° approach to data security. Pushing forward with innovation, eyes firmly fixed on the profit horizon alone is not sufficient. Total vigilance is essential – all doors and entry points must be sealed before moving forward, and not a single step can be taken without first proving that the ground is solid and predator-free.

Trend #3: Cloud compromise

Security challenges of remote working

Whilst the Finance industry initially focused on the use of private cloud, it is now rapidly adopting public cloud platforms and infrastructures to manage cloud services. FinTechs are at the forefront of seeking to put in place applications in the cloud that deliver best customer experience. This in turn has forced banks and insurance organizations to accelerate their digital transformation. Up to 90% of banks' workloads globally could be hosted on public cloud or software-as-a-service in a decade, according to McKinsey & Company. The same is true for FinTech companies.

But cloud compromise, following the Covid-19 lockdowns and dramatic rise of work-from-home practices, is potentially the most significant cybersecurity issue facing the financial industry. Financial institutions have belatedly woken up to the fact that their data is inadequately protected against cloud-based and network-based attacks including data manipulation attempts and misconfigurations.

As cloud computing within banking grows, the prevalence of cyber breaches for cloud services is growing significantly as well. According to a Verizon study, 'the cloud is the cornerstone of threat actors' digital transformation strategies'.

'Today, 39% of all breaches are in the cloud and web-based applications. Cloud app adoption rates are continuing to accelerate in 2021, following a rush to get as many employee- and customer-facing systems into the cloud as possible in 2020.'

Digital transformation reliant on cloud-based technologies continues to accelerate. Gartner estimates worldwide cloud end user spending will grow 23.1% in 2021 to reach $332.3 billion, and will continue to be the number one target for bad actors.

Financial institutions' vulnerabilities when moving services to the cloud come from a number factors.

- They rely too much on cloud-service providers to provide failsafe cybersecurity checklists when it comes to third party risk management. Often the provider's security policies are neither adequate nor transparent.

Data breaches are an increasingly significant cost burden for the industry: Worldwide, financial firms that experienced a data breach reported estimated average losses of roughly $4.2 million per attack, with U.S. organizations hit hardest at $4.7 million in estimated losses.

The industry remains a popular target for cloud-based attacks: Over half of all organizations (54%) surveyed suffered a data breach in the last 12 months with 49% plagued by a cloud malware attack as well.

'The (2020) SolarWinds breach is an important reminder of the potential vulnerabilities of the financial services sector to cyber-attacks and outages via their reliance on third-party suppliers and service providers, over which they have little or no control when it comes to cyber security.'

- There is too much consolidation of financial data within too few cloud service providers, multiplying the potential return for cybercriminals if they can infiltrate that provider. According to the Bank of England, in 2020 the top two infrastructure-as-a-service providers had around two-thirds market share for banks.
- Financial institutions also fail to find out about potential configuration and technical limitations of their chosen provider which could potentially lead to a breach. And regulatory issues, due to the shared responsibility model of cloud infrastructure and platform, represent a growing burden.

Working-from-home issues include remote access enterprise systems lacking secure setup, inadequate end-user education against social engineering and lack of awareness of safe configuration practices.

The good news is the financial industry is making significant investments in upgrading cloud security infrastructure, turning to specialized cloud cybersecurity providers to protect against rapidly changing threats.

Trend #4: The Internet of Things

Welcome to a world where you can pay with your sneakers

$2,030 by 2023
The global IoT in the BFSI market is expected to grow to $2,030 million by 2023

There are currently more objects connected to the internet than there are people in the world. Yet the Internet of Things (IoT) is often misconstrued as an internet of physical objects alone. This is partly to do with the growing interconnectivity of the consumer's lived environment, with innovations such as Amazon's Alexa becoming increasingly popular.

A large part of the Financial Services industry's interest in the IoT is related to the payments sphere from payment cards (with chip and PIN technology) to smart watches, phones and mobile gadgets.

Wearables are increasingly used within the financial system to send alerts to users - e.g. about nearby bank branches, ATMs, localized sale offers, overspending and even loan approvals.

For careless operators, an IoT-connected device could lead to breaches bigger and more invasive than we've ever seen.

Naresh Persaud, Senior Director of Security at CA Technolohies:
The rapid growth of the Internet of Things (IoT) has raised a new set of cybersecurity risks in the financial services industry. New insecure interfaces increase the risk of unauthorized disclosure of critical data while attacks could bring services to a halt.
PwC

One example was the Berlin Metro's collaboration with Adidas on a pair of smart sneakers that serve a dual purpose – as subway passes.

Another key sphere is Usage Based Insurance – where IoT meets InsurTech with the use of tracker devices that track very specific usage indices and customer safety behaviors, enabling a more perfectly titrated and real-time risk assessment that both supplier and customer can profit from. Examples include healthcare insurance calculated from fitness profiling, and data and car insurance based upon driver behavior profiling and data.

However, when it comes to IoT, not all things are physical objects. Things include abstract entities, such as bank, or other financial, accounts.

Currently, the main opportunity that IoT offers banks is the power to generate hyper-personalized notifications, recommendations and suggestions.

These suggestions can be geographically localized when a customer's card use alerts the bank to their real-time location. While the number of (inter) connected things proliferate, so too does the number of devices and entry points vulnerable to cyberattack.

The question that banks and payment services providers need to ask is one that might not have been foreseen a decade ago: 'how do you secure a pair of sneakers against cyberattack?'

The Internet of Things threat spotlight: security beyond the traditional device perimeter

According to PwC, these are the key cybersecurity concerns that Financial Services providers need to focus on when using the IoT (summarized):

- Attack surface: entering a corporate network via an IoT device.
- Perimeter security: IoT relies on cloud-based services – how can these be secured?
- Privacy concerns: the risk of consumer privacy violations with breaches.
- Device management: how to maintain a security baseline as devices proliferate?
- Third party risk: how to identify exposure in an interconnected system?
- Regulatory compliance: failure to comply with legal implications of IoT usage.

When IoT meets the Open Banking revolution, the cybersecurity challenge is intensified and multiplied. How can Financial Services providers guarantee the protection of data that lies in a new array of connected devices? A major cyber risk is that when these connected devices were installed, IT security was not involved. In the post-Covid work-from-home environment, cybercriminals will concentrate on accessing smart devices in employees' homes to find a way into employers' networks.

In general, security issues come down to insufficient IoT device management. Securing IoT in Financial Services means knowing exactly how and where all the technology is used – at home, in the office and everywhere else.

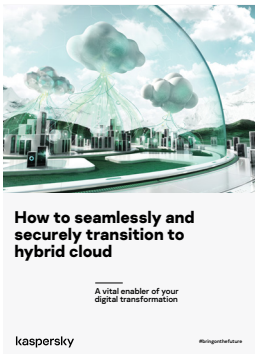
Trend #5: Digital transformation

The pressure to transform is universal

When it comes to the effect of technology on the financial sector, it is easy to focus on where the glamour lies – that is, the technological innovations that are adopted to increase revenue by delighting customers and enhancing user experience.

Yet the Open Banking, IoT, Blockchain and FinTech revolutions do not take place in isolation. Banking technology is not the only technology undergoing phenomenal paradigm-shifting changes. All of these innovations unfurl in the wider context of digital transformation – a revolution in and of itself. And, just as Financial Services providers will find themselves effectively out of the game if they fail to provide innovative services, so will they find it impossible to keep pace without undergoing the same digital transformation that leaders in every industry will undertake.

Read Kaspersky's whitepaper on hybrid clouds and digital transformation for detailed intelligence on the risk profile of digitally transformed organizations.



Threat spotlight: digital transformation

The good news is that one of the key threats related to digital transformation is actually easy to defend against. This threat is fear itself – and the cure for fear, as ever, is knowledge and informed action.

45%

A Cornerstone Advisors study revealed only 25% of banks and credit unions initiated a digital transformation strategy before 2019 and 45% still had not embarked on digital transformation by the start of 2021.

To (over) simplify, the broad FinTech revolution concerns customer-facing technology, while digital transformation describes what goes on behind closed doors. The latter is nothing less than a totally new approach and commitment to ongoing, permanent evolution; one in which an organization adapts constantly.

Combined, these twin revolutions significantly enlarge the scope of the 360° collaborative approach to data security that Financial Services providers must now adopt.

In 2020-21 the digitization of Financial Services has accelerated rapidly due to the dramatic increase in remote working practices, digital engagement, movement of data and a shift to technology deployed public cloud infrastructure. Globally, the financial industry is now scrambling to speed up digital transformation around a coherent strategy to satisfy the demands of its customers.

As a result, a constantly-increasing number of external endpoints interact with banking systems, and traditional security is no longer sufficient to protect them. Security breaches occur across a whole range of digital banking services – data leaks, unsecure mobile apps and targeted cyberattacks.

Only the proper implementation of future-driven, digital-first cybersecurity solutions can give banks and Financial Service organizations the confidence they need to continue to transform digitally and provide products and services that delight customers and bring profit.

Trend #6: Blockchain

It's a brave new decentralized world

People aren't just thinking about [Blockchain] technology as a method to promote efficiency and change some of their existing operations. It's also a way to bring about entirely new, creative revenue streams.
Grainne McNamara, Principal, Digital, PWC

Blockchain technology is still a relatively new technology. Due to the notoriety of Bitcoin, blockchain technology is commonly associated with cryptocurrency in the popular imagination. The truth is that cryptocurrency is only part of the story. For the Finance industry the applications of blockchain extend far beyond Bitcoin and the host of Alt-Coins that continue to pop up.

Blockchain will likely underpin the digital financial system. Blockchain distributed ledger technology stores categorized data in hierarchically managed blockchains enhancing data protection, minimizing security risk and protecting user privacy. As such it interacts perfectly with the Open Banking system.

33%

It is estimated that 33% of Bitcoin trading platforms have been hacked. Account takeovers can enable hackers to steal private keys and access and remove the currency. Bitcoin and other cryptocurrencies are untraceable making hacking of accounts and whole crypto platforms a very attractive target for cybercriminals.

$1.7 billion

In 2019 the Wall Street Journal reported that $1.7 billion in cryptocurrency had been stolen in recent years.

In the Finance sector blockchain technology enhances speed, transparency and security. Each of these benefits rest on the decentralized nature of blockchain and can be utilized to cut costs, reduce delays, minimize risk and speed up transactions.

Specifically blockchain technology facilitates international fund transfers such as the huge global market in remittances and trade finance. It solves the problem of online identity management - verifying customer identity. It optimizes record keeping recording transactions using unalterable blockchain digital ledgers. Other applications include share trading, smart contracts and loyalty and rewards.

However blockchain technologies are not free of risk. Deloitte identifies three types of risk: standard risks, value transfer risks and smart contract risk.

Specific cybersecurity risk has resulted in large scale thefts. Virtual savings accounts (wallets) containing cryptocurrency can be infiltrated. Many blockchain transactions are facilitated by third-party vendors with potentially weaker security. Cybercriminals can deploy routing attacks to intercept data during real-time transmission to internet service providers. Phishing attacks are a tested method of trying to obtain wallet key owners' credentials. Inadequate privacy protection can result in transaction leakage.

In conclusion: to implement and support blockchain applications, it is necessary to have an understanding of blockchain security vulnerabilities. An expert cybersecurity partner can assist financial organizations in minimizing risk.

Trend #7: Machine learning and AI

Man vs Machine 4.0

While Garry Kasparov's 1996 chess defeat at the 'hands' of Deep Blue was a shock, the machine's ability to learn the rules of the game held little more than a novelty factor to most onlookers.

Fast-forward a couple of decades, and machines are now outperforming humans on countless fronts, from robo-advisors to investment

Machine learning/AI algorithms are increasingly effective at preventing money laundering attempts. To benefit from ML/AI cyber-prevention innovation, Financial Services organizations are teaming up with expert partners who select relevant data collection criteria and define end goals to implement deep learning solutions.

But also the easy availability of machine learning frameworks inevitably boosts malicious AI usage.

algorithms, from chat-bots to 'sentiment analysis'. Unlike Deep Blue's victory over the chess master, the superiority of current common-or-garden machine learning technology over its human counterparts lies largely in its resource-efficiency, rather than intellectual or analytical superiority.

In 2021 the tech world is providing increasingly sophisticated AI solutions to the Finance industry mainly in the following areas: credit decisions, managing risk, quantitative trading, personalized banking and exposing cybersecurity fraud.

One example is the boom in robo-advisors for the consumer financial industry – particularly for mortgages and investments. This ML technology brings financial advice within affordable reach of a wider consumer market, cutting costs for provider and user alike.

However, robo-advisory, like other ML technology, does not render human insight redundant. In fact, when it comes to cybercrime, human oversight (and insight) becomes even more critical than ever.

The exploitation of even a single flaw in the ML system can lead to vulnerability on multiple fronts, potentially extending to the totality of customer accounts. Leaks and cyberattacks are always an enormous reputational risk – across industry. Yet for Financial Services, reputation really is everything.

While the resource-efficiency of ML Financial Services might lower the bar for consumer entry points into hitherto cost prohibitive fields such as investment, the appetite for risk remains low. One breach could force the end of even the most popular provider.

Machine learning threat spotlight

IDG has identified six key ways that hackers will employ ML technology to launch cyberattacks, by developing (Source: IDG):

- Increasingly evasive malware.
- Smart botnets for scalable attacks.
- Advanced spear phishing emails.
- Disruptions to threat intelligence (including 'false positives').
- Unauthorized access.
- Poisoning the ML engine itself.

Trend #8: Regulatory challenges

Laws beyond the border

Governments and financial regulators globally are responding to this proliferation in new technology with a succession of new laws, which vary enormously according to the attitude, experience and political climate native to each respective market.

And, along with players in just about every single industry on the planet, Financial Services providers do not operate in nation-state or market-specific bubbles. Even if cross-border business is restricted to software use or customer services outsourcing, the regulatory picture still becomes ever more complicated.

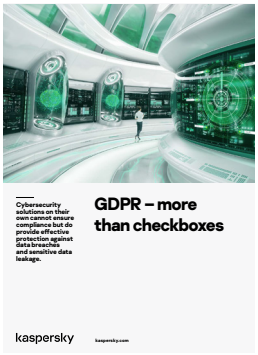
The EU's General Data Protection Regulation, which came into effect in May 2018, is a case in point. While in theory the GDPR's jurisdiction is restricted to the borders of the EU itself, in reality Financial Services providers outside the EU have to comply with the GDPR if they wish to do business (whether buying, selling or prospecting/marketing) within EU markets.

From the EU's perspective, the GDPR was the essential counterpoint to the apparent freedom of Open Banking. Markets which took a more laissez-faire approach to Open Banking might not have seen the need for such stringent data protection regulation, but the GDPR was a call to action that banks and other Financial Services providers could not afford to ignore – wherever they are.

The GDPR is just one example of the impact that huge regulatory changes can have on Financial Services providers. Another is the PSD2 Payment Services Directive which came into effect in January 2018 with a deadline to comply by September 2019.

PSD2 includes a set of rules for payment services, and incorporates stringent customer authentication regulatory standards to reduce fraud and assure safe user authentication. The aim is to make international finance transfers EU-wide more secure and easier. The directive is also designed to promote competition and encourage innovation - opening the door for greater market participation by FinTechs.

Read our whitepaper on GDPR



4% fine

Companies that contravene the GDPR face fines of up to 20 million euros, or 4% of turnover, whichever is greater. The top five GDPR fines in 2021 were:

- Notebooksbilliger.de - €10.4m fine
- Vodafone España - €8.15m fine
- Caixabank SA - €6m fine
- Fastweb SpA – €4.5m fine
- EDP Energía - €1.5m fine

Threat spotlight: regulatory challenges

To a large extent, regulation such as the GDPR is a strong reminder to businesses of something that's plain common sense: treat customer data with respect. Lock it up, defend it against cyberthreats and don't share it without permission. Breaking these golden rules has always had costly impacts on reputation.

Put simply, the penalties for improperly protecting customer data are heavier than ever before. Breaches and leaks now threaten to destroy even the most robust blue-chip.

Regulatory actions also substantially raise the risk of litigation. The 2019 Capital One bank breach, which attracted a regulatory fine of $80m, was also a catalyst for lawsuits from customers.

Regulators also plan to do more than simply react after a breach. They see their role as preventative. The proposed Digital Operational Resilience Act (DORA) plans to implement an EU-wide regulatory framework to manage Financial Services firms' third-party risk and boost resilience. The UK Financial Conduct Authority (FCA) will require organizations (from March 31, 2022) to address disruption to business services, including from cyberattacks.

Regulatory challenges and balkanization

The effect of regulatory changes on the Financial Services industry is further proof that the balkanization of the internet is harmful and dangerous. We are connected across borders and money can flow as freely as ideas. The same is true of malware, ransomware, crypto-miners, viruses and every other cyberattack to come.

A separatist mentality no longer serves as a viable defense. In a context where cyberattacks show no respect for international borders, the response must be equally borderless. It is in this context that Financial Services providers must now look to cybersecurity providers combining a clear vision across borders, with in-depth local knowledge about the adoption of new technology (and its attendant threats) and the effect of regulatory challenges, market by market.

Summary

All the trends outlined above point to the following: the future of the financial industry is borderless, flexible and changing at bewildering speed. The need both to adopt new technology and to protect that technology has never been greater. The consequence of failing to secure new technology sufficiently can destroy an organization. That is why having a truly global security partner with relevant experience in all relevant emerging technologies is an essential support, assisting organizations to navigate the future of Finance.

Choose what fits best to protect your business

Kaspersky helps the Finance industry adopt proven security strategies in today's volatile and challenging environment. Our perfectly engineered, tailored solutions and services – assisted by world-leading security intelligence - protect data and business continuity 24/7 against advanced threats and targeted attacks – mitigating risks, detecting attacks earlier, dealing effectively with live attacks and fortifying future protection.

Step-by-step cybersecurity approach for future-proof protection

Our step-by-step cybersecurity approach is designed to clarify which level of security as well as which specific solutions suit your organization best. The frameworks provide a set of easily managed threat protection measures coordinating seamlessly with one another to meet the needs of each individual organization, and offer a cybersecurity roadmap assuring smooth transition from one IT security maturity level to another when the time comes.

Kaspersky's step-by-step cybersecurity approach

1

Kaspersky Security Foundations – essential core of cloud-based, automated protection for all devices, VDI and hybrid server infrastructures, before organizations advance seamlessly to ...

2

Kaspersky Optimum Security - for organizations requiring more specialized security against new and evasive threats, before effortlessly implementing our third

3

Kaspersky Expert Security – for organizations with established mature IT security teams combatting the most complex targeted attacks.

Cybersecurity maturity level	Solution
IT Smaller businesses without a specialized IT security team	**What** Kaspersky Security Foundations **How** Implement fundamental security for organizations of any size and infrastructure complexity delivering cloud-managed automatic prevention of commodity cyberthreats on any devices, VDI and hybrid server infrastructures. ▸ **Endpoints:** Protect every endpoint in your organization with Kaspersky Endpoint Security for Business; Kaspersky Embedded System Security ▸ **Cloud:** Benefit from borderless security with Kaspersky Hybrid Cloud Security ▸ **Network:** Secure your perimeter with Kaspersky Security for Mail Server; Kaspersky Security for Internet Gateway ▸ **Data:** Safeguard valuable and sensitive data with Kaspersky Security for Storage ▸ **Security Management:** Access expertise with Kaspersky Premium Support; Kaspersky Professional Services
IT security Organizations in need of advanced defenses, but with limited specialist IT security resources	**What** Kaspersky Optimum Security **How** Combat evasive threats with effective endpoint detection and response and continuous security monitoring – but without prohibitive costs or complexity ▸ **Advanced detection:** Boost ML behavior analysis, sandboxing, threat intelligence and automated threat hunting* with Kaspersky Sandbox, Kaspersky Threat Intelligence Portal and Kaspersky Managed Detection and Response Optimum ▸ **Analysis and investigation:** Enhance threat visibility and simplified investigation process with Kaspersky Endpoint Detection and Response Optimum ▸ **Rapid response:** Deploy automated in-product response options, as well as guided and managed response scenarios* with Kaspersky Endpoint Detection and Response Optimum and Kaspersky Managed Detection and Response Optimum ▸ **Security awareness:** Equip employees with automated tools at all levels with cybersecurity skills with Kaspersky Security Awareness Training *Supported by Kaspersky experts

Mature and fully formed IT security team and/or dedicated SOC

- Have a complex and distributed IT environment
- Are a highly likely target for complex and APT-like attacks
- Have a low risk appetite due to high costs of security incidents and data breaches
- Are concerned about regulatory compliance

What

Kaspersky Expert Security

How

Complete mastery over the most complex and targeted cyberattacks

- **Equipped:** Equip your in-house experts to address complex cybersecurity incidents. Benefit from a unified cybersecurity solution. **Kaspersky Anti Targeted Attack Platform with Kaspersky EDR** at its core empowers your team with XDR capabilities.

- **Informed:** Enrich your knowledge pool with threat intelligence and upskill your experts to deal with complex incidents:
  - Integrate actionable, immediate threat intelligence into your security program. **Kaspersky Threat Intelligence** gives you instant access to technical, tactical, operational and strategic threat Intelligence.
  - Develop your in-house team's practical skills, including working with digital evidence, analyzing and detecting malicious software, and adopting best practices for incident response, with **Kaspersky Cybersecurity Training.**

- **Reinforced:** Call upon external experts for security assessment, immediate support and back-up:
  - Take advantage of immediate support from the **Kaspersky Incident Response** team of highly experienced analysts and investigators to fully resolve your cyber-incident, fast and effectively.
  - Bring in a second opinion and managed threat hunting expertise from a trusted partner with **Kaspersky Managed Detection and Response**, so your in-house IT security experts have more time to spend reacting to the critical outcomes requiring their attention.
  - Understand just how effective your defenses would really be against potential cyberthreats, and whether you're already the unwitting target of a long-term stealth attack, through **Kaspersky Security Assessment**.

Targeted Solutions

What	How
 **Kaspersky Fraud Prevention**	Advanced Authentication allows for frictionless and continuous authentication, cutting the costs of second factor processes for legitimate users, while keeping fraud detection rates high in real time. Automated Fraud Analytics thoroughly analyzes events that occur during the entire session, transforming them into valuable pieces of data. Protects the external perimeter of any business, ensuring safety and protection for clients.
 **Kaspersky DDoS Protection**	Covers a bandwidth of up to 2Gbps, with extensive service coverage, including attack analysis reports and anti-DDoS capability assessments. Optional automatic always-on DDoS mitigation, fortified by Kaspersky engineers running parallel checks to optimize defense according to the nature of each DDoS attack.
 **Kaspersky Payment System Security Assessment**	Uncovers any vulnerabilities in your ATM/POS infrastructure that are exploitable by different forms of attack, outlines the possible consequences of exploitation, evaluates the effectiveness of your existing security measures, and helps you plan further actions to fix detected flaws and improve your security.
 **Kaspersky Threat Attribution Engine**	A malware analysis tool deployed on your network, “on premise”, that incorporates 22 years of Kaspersky’s database of APT malware samples. Delivers automated analysis of the “genetics” and “genotypes” of malware for code similarity with previously investigated APT samples to rapidly link new attacks to known APT malware, actors, campaigns and previous targeted attacks.
 **Kaspersky Research Sandbox**	Emulates company-specific systems in an isolated environment, performing automated, behavioral malware analysis, and enabling safe detonation and detection of advanced and previously unseen threats.

Cyberthreats News: www.securelist.com

IT Security News: www.kaspersky.com/blog

Threat Intelligence Portal: opentip.kaspersky.com

Technologies at a glance: www.kaspersky.com/TechnoWiki

Awards and recognitions: media.kaspersky.com/en/awards

Interactive Portfolio Tool: kaspersky.com/int_portfolio

kaspersky BRING ON THE FUTURE