Future-driven cybersecurity

Predicting the future, eliminating financial risks

kaspersky

#bringonthefuture

New trends – new threats

‘Follow the money’

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.

Indeed, the relationship between crime and money is as old as crime itself, stretching back long before Babbage and Pascal's earliest dreams of the computer.

And so, before reviewing the new trends in Financial Services – and the new threats they attract – it is important to remember this one glaring and enduring fact:

#1

The Financial Services industry is the number one target for cyber criminals everywhere.

This includes attacks on financial institutions themselves, as well as attacks on their customers.

While the motivations behind cyber attacks may vary, there is one constant – the motivation of financial gain. Any organization that holds or controls funds of any kind will always be a top target for cyber criminals.

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

60%

As per the IBM Cyber Security Intelligence index, over 60% of all security events happened in just a single industry – Financial Services.

8 trends and the challenges they bring

In this paper we will examine 8 key trends to analyze the lay of the Financial Services landscape in 2018 and understand just how different the industry is from former years. We will also identify some of the key cyber risks incurred by each in turn:

FinTech

Trust

The Open Banking Revolution

The Internet of Things

Digital Transformation

Blockchain

Machine Learning and Artificial Intelligence

Regulatory Challenges

Trend #1: FinTech

Young Turks challenge the ancien régime

For years, banks were able to tune out the sound of footsteps as technology made its approach. While concessions were made to its inevitable encroachment, in the form of limited online banking and mobile applications, these were often 'side salads' and not the main dish.

Banks were, by and large, slow to adapt. That was the case until very recently, when everything changed.

2016 (or thereabouts) marked a 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. Common to all was one eternal fact: playing the ostrich in the face of inevitable change is never an option.

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

Deloitte

The sheer pressure that this change has brought to bear on banks has hastened the birth of a maturing and vibrant FinTech market, offering standalone services **(including mobile-first banks like N26)** as well as Third Party Providers, or TPPs s (such as **Bud**, which built services for HSBC).

Banks now often rely on these (usually) smaller third-party entities to supply the innovative services that their customers (business and consumer alike) now expect.

FinTech startups commonly find it easier than banks to attract the iconoclastic, visionary developer talent necessary for creating truly innovative services.

The result has been something of a culture clash (though not entirely negative), where suited bankers meet sneakered FinTech visionaries at conferences held by governments and institutions across the globe – anxious not to miss out on the chance to ride this new profitable wave.

Absent the strict and trusted regulatory framework of traditional Financial Services, the FinTech market brings with it a level of risk (both real and imaginary).

While high risk and volatility is common to all new technology, the absolute, unequivocal pre-eminence of trust when it comes to Financial Services renders the risk even more acute.

Institutions have responded with guidelines and frameworks to mitigate this new rippling risk scenario; one example is **Open Banking's How-to Consent guide.**

FinTech threat spotlight: too young for Basel?

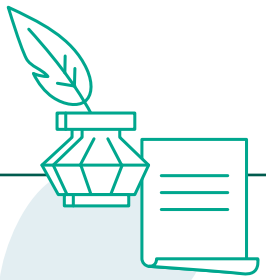
While traditional banks are by no means immune to cyber threats, they are at least mature enough to have developed a robust procedure for ensuring compliance and preventing repeat mistakes.

The Basel Accords are the perfect example of how an industry's maturity can result in a tough protective framework.

The FinTech sphere, like all startup industries, does however benefit from advanced technological literacy, and there is a huge drive among many operators to develop robust protections and cyber defense protocols. Nevertheless, as with any highly innovative industry, its very newness can put it at increased risk of cyber threats.

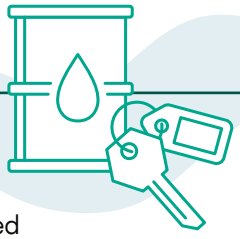
13th Century

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 forms. The printed slips had scrollwork at the left-hand edge which 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 introduces 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.

Trend #2: Trust is everything

You can bank on that

Loss of trust causes bank runs, and market collapses. This rule is universal, and applies the world over. Usually when we speak of trust in Financial Services, the main concern is the trust that customers need to be able to place in their providers.

However, in the age of FinTech, it is banks and Financial Services providers themselves who also need to be able to trust the third parties they rely on to provide the innovative services their customers demand.

If banks are not able to trust third party FinTech providers, then they simply will not be able to satisfy growing market demands for new mobile and online services.

Credit

Trust is built into the very lexicon of financial services: the Latin word credere (to believe) is the root of the word 'credit.'

x3

According to EY, 'Customers who have complete trust in their bank indicated that they were 'very likely to recommend' the bank three times more than customers who had only moderate levels of trust.'

Threat spotlight: trust (or the lack thereof)

The threat of losing customer trust constantly hangs over the Financial Services industry. Once earned, trust is more precious than the very gold standard against which money itself used to be measured.

In fact, EY specifically pinpoints cybersecurity improvement as one of the key six actions that banks must take right to preserve trust now, recommending that Financial Services providers. **'Proactively protect customer data like it's your own — and defend against cybersecurity threats.'**

Source: EY Report: 'Customer trust – without it you're just another bank.'

Trend #3: The open banking revolution

No man is an island

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

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 party bears the responsibility not only for protecting themselves from cyber attack, but for defending the entire ecosystem. And as the number of parties increases, so too does the number of potential targets for cyber criminals.

With Open Banking, financial institutions allow the use of open APIs so that third parties can build applications and services around their services. Adoption varies worldwide, with some governments enforcing Open Banking, and others taking a more market-led (or laissez-faire) approach.

The number of players (and potential targets) in the FinTech ecosystem is made even more complicated in the new era of Open Banking. Customers, whether business or consumer, become players too (however peripheral), and the proliferation of devices and (inter) connected Things (in the IoT) adds to the number of fronts which must be defended from cyber attack.

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 by market demand for 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.

No man is an island entire of itself; every man is a piece of the continent, a part of the main; if a clod be washed away by the sea, Europe is the less.

John Donne (English Poet), 1624
The same could be said of the FinTech ecosystem in the age of Open Banking.

Crime as a service: cyber criminals use third parties, too

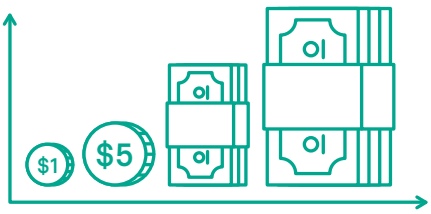
Sadly, Financial Services providers are far from alone in turning to the use of third provider services and suppliers to drive resource-efficiency, results and even the bottom line.

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

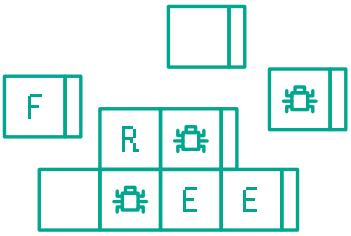
The cyber crime ecosystem develops in parallel to the FinTech ecosystem, just like the antigenic shift and drift of the influenza virus as it seeks to continue infecting its human targets.

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.



Shockingly, the dark web ransomware economy is said to be growing at a rate of 2,500%.



DDoS scripts (initially for minecraft servers) can even be downloaded for free from GitHub – while these may sound relatively innocuous, the Mirai botnet, which very nearly 'brought down the internet', had its origins in a minecraft DDoS scam.

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.

The role of the Compliance function within Financial Services is forced to work more closely than ever with the IT department, as its realm of concern expands from the purely financial to the technological. Collaboration and expertise-sharing is essential.

New technology – new threats

Naturally, cyber criminals can be just as innovative as the technology they wish to attack. Their approaches mutate to meet the evolving technology of their prey.

The novelty of innovative technology is what gives it its power, yet novelty can also be an Achilles heel.

In this sense, organizations that harness the power of innovation can make themselves as vulnerable to cyber attack as a newborn baby is to infection.

The result is a threat environment in which 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.

What do cyber-criminals want?

Motivations for cyber attacks on Financial Services providers include:

- **Financial gain from ransom payments.**
- **Financial gain from fraudulent transactions.**
- **Information theft (for market intelligence and insider trading).**
- **Malicious service disruption.**
- **Data deletion or manipulation to influence stock prices.**
- **Damage to competitors' reputation.**
- **DDoS attacks on competitors.**

Open banking threat spotlight: connectivity itself

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 entrypoints that multiply. The number of vulnerabilities explodes with the involvement of even greater numbers of the four traditional entrypoints for attack: removable media, Internet, email and fixed connections.

In an attack on Bangladesh Bank, hackers stole some $81 million, by exploiting the banking system's very complexity. These same criminals are now thought to have been responsible for the notorious WannaCry ransomware attack.

The North Korean collective, Lazarus, compromised the bank with spear phishing emails and then proceeded to attack the terminals that connected to the SWIFT (Society for Worldwide Interbank Financial Telecommunication) system, sending fraudulently authenticated messages authorizing the illegal transfer of funds.

The hackers went even further, employing malware in an attempt to erase records of the theft.

Trend #4: The Internet of Things

Welcome to a world where you can pay with your sneakers

There are currently more objects connected to the Internet than there are people in the world. Yet the Internet of Things 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.

x30

Gartner Estimates a 30-fold growth in IoT-capable devices by 2020.

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 Technologies

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

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 now wearables.

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

The other 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 might profit from.

It is still early days, but EY estimates that UBI market penetration in Europe, Asia and America will reach 15% by 2020.

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 even 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 cyber attack.

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 cyber attack?'

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 not only in the hands of third party FinTech providers, but also now in a new array of connected devices? How can they not?

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.

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.

59%

Companies everywhere are delaying digital transformation because of the fear of new cyber threats – and this delay is costing them greatly.

According to a Microsoft report, 'cybersecurity incidents are undermining Asia Pacific organizations' ability to capture future opportunities in today's digital economy, with 59% respondents stating that their enterprise has put off digital transformation efforts due to the fear of cyber-risks.'

The Financial Services industry is no more immune to the threat of fear than any other, and the same rules still apply. Only the proper implementation of future-driven, digital-first cybersecurity solutions can give companies the confidence they need to continue to transform digitally and provide products and services that delight customers and bring profit.

Read our White Paper on hybrid clouds and digital transformation contains detailed intelligence on the unique risk profile of digitally transformed organizations.

To (over) simplify, the broad FinTech revolution concerns customer-facing technology, while Digital Transformation describes what goes on behind closed doors. The latter, rather than being a one off project that can be ticked to a corporate to-do list, is nothing less than a totally new approach and commitment to ongoing, permanent evolution; one in which an organization adapts and responds constantly, with a firm eye fixed on the future.

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

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 such a new technology that a developer with a mere five years' experience might be seen as a veteran expert. At times, simply the act of throwing around a few choice words from the Blockchain glossary is enough to mystify – and even frighten – uninitiated onlookers.

Due to the early notoriety of Bitcoin, Blockchain technology is commonly associated with currency in the popular imagination. The truth is that crypto-currency is only part of the story. For Financial Services Providers, the applications of Blockchain extend far beyond Bitcoin and the host of new Alt-Coins that continue to pop up.

New

Rakhini is the supreme example of a cyber threat that has evolved specifically to take advantage of the exact same technology that Financial Services providers are harnessing in order to grow.

The blockhain-savvy malware recently added a cryptocurrency mining module to its arsenal.

Read more from Kaspersky

There remains some uncertainty about which of Blockchain's promised innovations will bear enduring fruit. However, according to **Deloitte**, these are the top five use cases for Blockchain technology in Financial Services:

- Speeding up and simplifying cross-border payments.
- The future of share trading.
- The benefits of smart contracts.
- Improving online identity management.
- Loyalty and rewards.

Underlying each of these are two key benefits – speed and security. Each of these benefits rest on the decentralized nature of Blockchain.

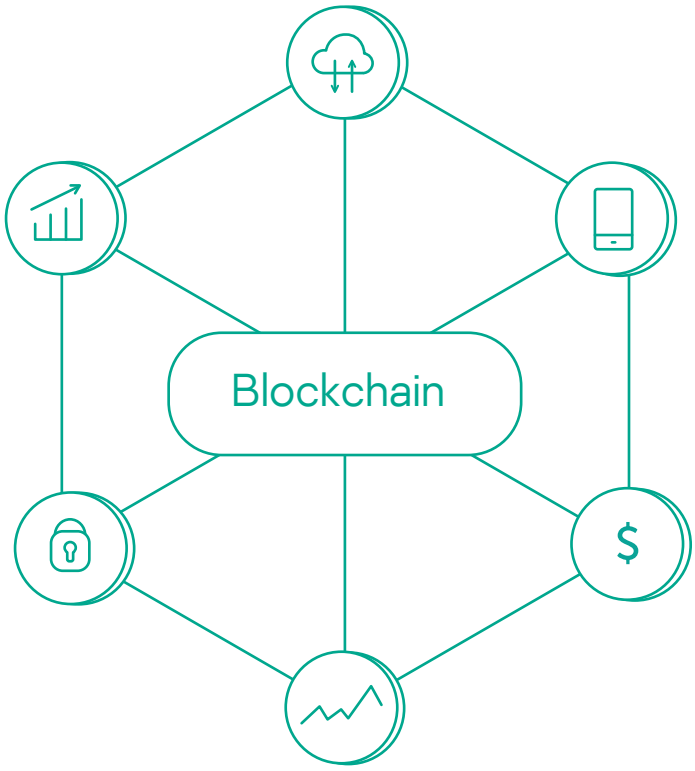
Consumers and businesses alike are increasingly impatient when it comes to financial transactions. While consumers can expect to transfer money instantly between friends and family (often for free), businesses are now demanding the same, unwilling to wait days, hours, or even minutes, for funds to cross entities, and now borders.

The march of the crypto-miners

Returning to Blockchain's traditional image as a crypto-currency technology; hunger for new tokens has led to the birth of a new genre of cyber attack – the crypto miner.

In fact, we recently found that crypto-miners have replaced ransomware as the main threat in 2018.

The use of Blockchain technology can make it easier for Financial Services providers to offer faster and more secure payment methods or fund management facilities, but at the same time, the implementation of such technology does bring unique risks of its own.



Financial Services providers need to be able to balance Blockchain's promise with its risk if they are to thrive into the next era.

Blockchain threat spotlight: the dao attack

The Decentralized Autonomous Organization set the record for the largest crowdfunding campaign in history **(2016)**. The excitement around this new stateless venture-capital fund was phenomenal.

Built on the Ethereum platform, the DAO promised to embody and prove the potential of Blockchain technology to bring about a paradigm shift in financial technology, crossing borders and defying neat definition.

Sadly, almost as soon as this new age began to dawn, a shadow was cast over the DAO's dream of leading the decentralized cryptocurrency revolution.

Just about a month after its launch, hackers began to exploit a weakness in its code, and siphoned off a full third of its funds – with the $50 million worth of Ether being stolen.

Far beyond the financial loss of this specific cybercrime, the DAO attack cast a shadow over the whole cryptocurrency and Blockchain sphere. While Blockchain still promises new heights of security through distributed ledgers and smart contract technology, there is also an enormous level of distrust.

Trend #7: Machine learning and AI

Man vs Machine 4.0

What's good for the goose is good for the gander

Cyber criminals innovate just as hungrily as Financial Services providers, making use of the very same ML technology that is driving so much growth in the industry.

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 out-performing humans on countless fronts, from robo-advisors to investment 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.

An 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. Examples in Europe include Moneyfarm, Habito and Nutmeg.

However, robo-advisory, like other ML technology, does not render human insight redundant. In fact, when it comes to cyber-crime, 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 cyber attacks 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 point for consumer entry 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 cyber attacks, 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

All over the world, governments and financial regulators 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 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. Recent regulations such as the EU's General Data Protection Regulations are a case in point. While in theory the GDPR's jurisdiction was restricted to the borders of the EU itself, providers across the globe could not avoid the ripples of its aftershocks.

The call was simple – Financial Services providers outside the EU had to comply with the GDPR if they wished to do business (whether buying, selling or prospecting/ marketing) within EU markets.

From the EU's perspective, the GDPR was the essential belt-and-suspenders 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 no afford to ignore – wherever they are.

In the run-up to its implementation, the Financial Services industry was awash with concern and a degree of panic about the GDPR.

How would banks, venture capital firms, FinTechs continue to grow if their ability to share data was so tightly controlled?

How would cross-border players continue to scale and grow, taking on new markets?

While the GDPR is just one very recent example of the impact that huge regulatory changes can have on Financial Services providers, it is extremely unlikely to be the last.

Threat spotlight: regulatory challenges

4% fine

Now companies can add a direct financial impact in addition to the reputational risk – in the form of hefty fines. Companies that contravene the GDPR can face fines of up to 20 million Euros, or 4 % of turnover, whichever is greater.

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

As an indication of how strictly the authorities might adhere to this fine scheme, it is worth remembering that even before the GDPR came int ect, two companies were fined a total of £83,000 by the UK's Information Commissioner's Office. The shocking thing is that one of these companies – Honda – was actually fined £13,000 not for sending marketing emails, but for sending emails that it thought were going to help it comply with data protection law.
Put simply, the penalties for improperly protecting customer data are now heavier than ever before – breaches and leaks now threaten to destroy even the most robust bluechip.

Regulatory challenges and balkanization

The ect of regulatory changes on the Financial Services industry is further proof that the **balkanization** of the Internet is harmful and dangerous.

From now on, no industry can remain an island. We are connected across borders and now – both sadly and happily – money can flow as freely as ideas. The same, alas, is true ofmalware, ransomware, crypto-miners, viruses and every other cyber attack to come.

A laager mentality – protectionist, particularistic and balkanized – no longer serves as a viable defense. In a context where cyber attacks show no respect for international borders, the response should be equally borderless.

This attitude should persist, even where regulatory challenges appear to place obstacles in the path of Financial Services providers' attempts to protect precious data (or funds) once these have crossed the safe boundariesof a particular market.

It is in this context that Financial Services providers must now look to cybersecurity providers with an international outlook. What is needed, now more than ever, is clear vision across borders, with in-depth local knowledge about the adoption of new technology (and its attendant threats) just as much as about regulatory challenges, market by market.

How to protect your business - choose what fits your needs best

Kaspersky solutions protect businesses in all sectors, including financial services, against cyber attack.

For financial services organizations operating in today's extremely volatile and challenging environment, Kaspersky has the perfect solution to protect your data - and your business continuity.

Choose the one that suits your company best.

Solution	Good	Better	Best
 **Kaspersky Hybrid Cloud Security**	**What** Kaspersky Hybrid Cloud Security **How** — Comprehensive range of security layers, with a unique tech stack for VDI protection. — Additional security boosting functionality via APIs for VMware platforms.	**What** Kaspersky Hybrid Cloud Security, Kaspersky Security for Storage **How** — Additional anti-ransomware defenses to prevent system compromise and guard against access denial and destruction. — Specialized defense for connected storage, and dedicated protection against remotely running cryptors.	**What** Kaspersky Hybrid Cloud Security Enterprise, Kaspersky Security for Storage **How** — Integrity monitoring, extra system hardening technologies and advanced network IDS. — Built to support the large-scale, branching infrastructures characteristic of national and international banks.

Solution	Good	Better	Best
 **Kaspersky Endpoint Security**	**What** Kaspersky Endpoint Security for Business + Kaspersky Maintenance Service Agreement **How** — Defends the full range of endpoint platforms, with no impact on user productivity. — Extended and premium support programs. — Security infrastructure covered for up to 12 incidents per year – with a guaranteed response time of 6 business hours.	**What** Kaspersky Business + Kaspersky CyberSafety Kaspersky Maintenance Service Agreement Business + Kaspersky Private Security Network **How** — Defends the full range of endpoint platforms, with no impact on user productivity. — Secures key data protection and compliance targets, including GDPR, thanks to FIPS 140.2 certified encryption functions and OS-embedded encryption management. — Interactive staff work shops, extended and premium support programs.	**What** Kaspersky Endpoint Security for Business + Kaspersky CyberSafety Management Games + Kaspersky Maintenance Service Agreement Business + Kaspersky Private Security Network **How** — Defends the full range of endpoint platforms, with no impact on user productivity. — Rapid response protection with no unsecured time gaps. — Secures key data protection and compliance targets, including GDPR, thanks to FIPS 140.2 certified encryption functions and OS-embedded encryption management. — Interactive staff work shops, extended and premium support programs.
 **Kaspersky Threat Management and Defense**	**What** Kaspersky Endpoint Detection and Response **How** — Integrated Endpoint Protection under a single agent. — Advanced threat detection as well as industry-leading KES detections. — Single unified console for KEDR and KES, for threat investigation and response. — Automated (scheduled) IoC search capabilities. — KEDR as a standalone agent working alongside 3rd party EPP.	**What** Kaspersky Anti Targeted Attack Platform, Kaspersky Endpoint Detection and Response Standard, Kaspersky Secure Mail Gateway, Kaspersky Security for Internet Gateway, Kaspersky Security Training **How** — Highly responsive and adaptive, with enhanced network layer protection; actively discovers even hidden threats via Proxy, Web, Email and Endpoint activities. — Advanced threat detection with fully	**What** Threat Management and Defense, Kaspersky Anti Targeted Attack Platform, Kaspersky Endpoint Detection and Response, Kaspersky Incident Response, Kaspersky Security Training, Threat Intelligence Portal **How** — Full circle advanced threat discovery, analysis and reaction for SOC. — Centralized web interface gives a panoramic picture of security events across the IT

Solution	Good	Better	Best
		automated data collection, analysis and correlation. — Single unified console identifies compromised systems, locating communication between local and external systems and data sets, and pinpointing identities affected or compromised during the attack. — Advanced Threat Prevention with KSIG and KWTS.	infrastructure, with automated data collection, aggregation, and detection of complex threats. — Access to global Threat Intelligence Portal for insights from cybersecurity experts. — Isolated on-premise implementation for better control, regulation and privacy. — Regular trainings and optional subscriptions to industry-specific intelligence sources.
 **Kaspersky DDoS Protection**	**What** Kaspersky DDoS Protection Standard on-demand **How** — Secures ATMs, online banking, POS and other Internet-dependent services against DDoS attacks.	**What** Kaspersky DDoS Protection Ultimate on-demand **How** — Gives businesses the option to keep critical traffic in-house, with full control to configure parameters for redirection (DNS tables or BGP prefixes). — Uses on-demand BGP redirection - faster than the DNS redirection of KDP Standard. — Covers a bandwidth of up to 300Mbps.	**What** Kaspersky DDoS Protection Ultimate Plus with on-demand traffic redirection OR Kaspersky DDoS Protection Connect with always-on traffic redirection **How** — 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 the nature of each DDoS attack.

Solution	Good	Better	Best
 **Kaspersky IoT Security**	**What** Kaspersky Embedded Systems Security **How** — Provides mandatory protection even for devices with weak or legacy hardware, and old software, making it easier to satisfy international compliance requirements.	**What** Kaspersky Embedded Systems Security **How** — Provides mandatory protection even for devices with weak or legacy hardware, and old software, making it easier to satisfy international compliance requirements.	**What** Kaspersky Embedded Systems Security **How** — Provides mandatory protection even for devices with weak or legacy hardware, and old software, making it easier to satisfy international compliance requirements.
 **Kaspersky Cybersecurity Services**	**What** Threat Data Feeds, Payment Systems Security Assessment Customer-specific Threat Intelligence Reporting, Incident Response Training **How** — Threat Data Feeds integrated with existing security controls enable SOC to effectively prioritize and classify security alerts. — Customer-specific Threat Intelligence Reporting delivers clarity about risks across the totality of the organization's digital footprint, including insider threats and more. — Instant insight into exploitable flaws in payment processing applications, owned ATMs and POS devices, delivering remediation guidance to prevent costly breaches. — Staff Incident Response training builds internal IR capability, significantly reducing potential damage.	**What** Threat Data Feeds, Payment Systems Security Assessment Customer-specific Threat Intelligence Reporting, Incident Response Training + Threat Lookup, cloud Sandbox, Financial Threat Intelligence Reporting, Incident Response retainer **How** — Financial Threat Intelligence Reporting - up-to-date finance industry-specific intelligence on current threats, tactics and tools in use by cybercriminals worldwide allowing SOC teams to detect and proactively hunt for the associated threats in their environments. — Threat Lookup and Cloud Sandbox - access to Kaspersky's comprehensive threat intelligence repository to lookup information on files' behaviour, indicators of compromise	**What** Threat Data Feeds, Payment Systems Security Assessment Customer-specific Threat Intelligence Reporting, Incident Response Training + Threat Lookup, cloud Sandbox, Financial Threat Intelligence Reporting, Incident Response retainer + APT Intelligence Reporting, Digital Forensics Training, Malware Analysis and Reverse Engineering Training, Penetration Testing **How** — APT Intelligence Reporting gives SOC teams an accurate understanding of attacks with cross-industry targeting, and helps to develop use cases for early detection, scanning the whole network for the presence of previously undiscovered threats. — Penetration Testing allows for prophylactic repair and accurate prevention of catastrophic incidents.

Solution	Good	Better	Best
		and various relationships between them boosting incident investigations and response. — Incident Response retainer supplies immediate help and support from a qualified IT security partner, guaranteeing successful complex incident resolution.	— Staff training in Incident Response, and Malware Analysis and Digital Forensics helps to build internal IR capability.
 **Kaspersky Fraud Prevention**	**What** Kaspersky Fraud Prevention **How** — Protects the external perimeter of any business, ensuring safety and protection for clients. — Events and incidents provided allow for accurate and timely decisions and uncover even the most complicated fraud cases. — Ultra-efficient fraud prevention reduces the operational cost of anti-fraud measures.	**What** Kaspersky Fraud Prevention **How** — True machine learning with advanced forensic capabilities ensures smooth running of digital accounts. — Constant access to valuable session and behavioral data in real-time. — True machine learning with advanced forensic capabilities ensures smooth running of digital accounts. — Protects the external perimeter of any business, ensuring safety and protection for clients. — Events and incidents provided allow for accurate and timely decisions and uncover even the most complicated fraud cases.	**What** Kaspersky Fraud Prevention **How** — 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. — True machine learning with advanced forensic capabilities ensures smooth running of digital accounts. — Protects the external perimeter of any business, ensuring safety and protection for clients. — Constant access to valuable session and behavioral data in real-time. — Events and incidents provided allow for accurate and timely decisions and uncover even the most complicated fraud cases.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com

www.kaspersky.com

kaspersky **BRING ON THE FUTURE**