WHITE PAPER
December 2015
For professional investors

ROBECO
The Investment Engineers

Vaulting financial technology

Security in the financial sector

Jeroen van Oerle
Frank van der Spek
Patrick Lemmens

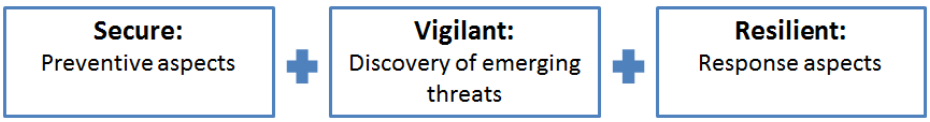
TABLE OF CONTENTS

Executive summary

The introduction of new technologies in our everyday lives is increasing exponentially. In the financial sector this is no exception. Customers expect to get service anywhere, any time and on any device. In order for people to use these new technologies they must be trustworthy. In order to be trustworthy, one of the conditions is to be secure. The financial sector is most often targeted by criminals, loses most when breached, but underinvests in security. We believe this will change quickly, which creates investment opportunities.

Focus is on being secure, vigilant and resilient

In this paper we discuss the trends that are currently shaping developments in terms of security in the financial sector. In order for a financial institute to be well positioned it must have a strategy to be secure, vigilant and resilient with regard to security.



Investment implications

Although developments in some parts of security (especially on the cyber side) are still in an early stage, valuations of companies in this area have already peaked. Many companies with exposure to the theme have rich valuations, as shown by the characteristics of security ETFs like HACK US or CIBR US. Currently it is hard to pinpoint clear winners.

In this paper we provide a corporate governance checklist to assess how far financial institutions are in becoming secure, vigilant and resilient. Several financials have already started to implement security solutions such as biometrics, advanced persistence threat detection and cybersecurity insurance. Although progress has been made, we see challenges for companies that are lagging behind, especially due to new regulations.

Another way of looking at the theme from an investment perspective is to search for companies that are best positioned to supply financial institutions with the required security solutions. Within the preventive aspect it is important to have scale because of the commodity-like nature of the product offering. Within vigilance it is important to have a top-of-class product or service and price is less relevant, but there are no clear winners. Resilience is a new market with a feedback loop into the other two areas. We see interesting developments here, but no pure-play investment opportunities, yet.

Secure				Vigilant		Resilient	
Authentication	**Secure element**	**Basic cyber security**	**Endpoint security**	**Advanced cyber security**	**Data analytics**	**Managed Security Service Providers**	**Insurance**
• Safenet • EMC • Gemalto • Symantec • Vasco Data Security	• NXP • Gemalto • Oberthur • Giesecke &Devrient	• McAfee • Sophos • Palo Alto • HP • IBM • Checkpoint	• Symantec • MacAfee • Sophos • Kaspersky • Trend micro	• Palo Alto • Checkpoint • Fortinet • Imperva • Splunk • Fireeye	• IBM • SAS • KNIME • Rapid Miner • Relx	• IBM • Dell SecureWorks • AT&T • Verizon • Symantec	• Munich re • Swiss re • Hannover re • Beazley • Travelers • Scor

Source: Robeco. This table is intended to facilitate analysis and should not be construed as an investment advice in any way.

Introduction

During the past year we have written[1] about the fast adoption of new technologies in the financial sector. There is, however, also a dark side to this story which is called security. Financial institutions need to find a balance between security and the level of convenience. Too little security will restrain the adoption of technology due to mistrust, while an excessive level of security will have the same effect due to the level of inconvenience in terms of usage.

Although the speed of adopting technology within the financial sector might be in line with other sectors, the level of security breaches is not. The financial sector has been the largest target for organized crime. The level of sophistication within organized crime increases fast. By continuously searching for weaknesses in security (both physical and cyber) there is a constant risk of major breaches. As an indication of frequency it would be fair to state that by listing the latest major breaches in the financial sector, this report would be outdated within a couple of months. The financial sector is not yet prepared to deal effectively with this topic. Security breaches are costly (USD 65k per day on average in direct costs[2]), and they also undermine trust. The number one reason for not using a mobile phone to make financial transactions is security[3]. Once this hurdle is taken we expect adoption levels of financial technology to increase very fast.

It will get worse before it gets better

Security in the financial sector is still in its early stages and it is not being addressed systematically. Intrusions via third party providers (like mobile wallets or customer loyalty administration) are spreading fast. 2015 Marked a record year in terms of confirmed breaches. Few senior executives have enough technical background to understand the underlying dynamics of security risks, and there is a more general lack of qualified personnel. Big structural changes are required, but as with many changes, it first needs to get worse before there is a feeling of urge to change.

This whitepaper will first describe the security landscape within the financial sector, after which we will dive deeper into security trends. We specify three drivers, namely being secure, vigilant and resilient to deal with security. Within these three drivers we see different trends. At the end of this paper we list the best positioned companies that can benefit from these trends.

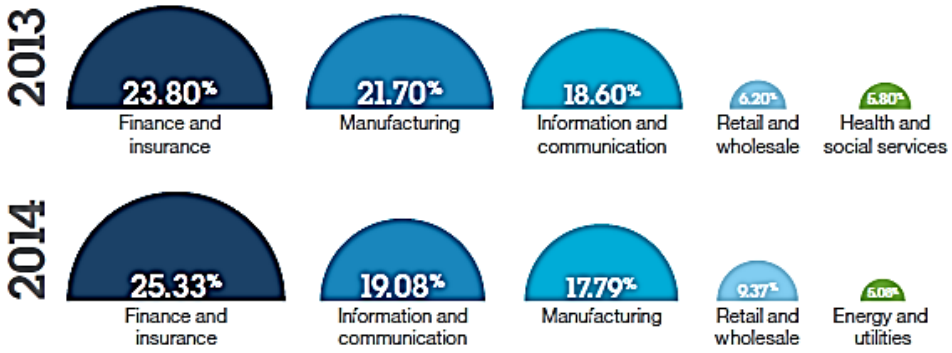
[1] Robeco white papers: Van Oerle, Getting old and staying wealthy, March 2015; Lemmens and Van Oerle, Fintech. The Robin Hood of payments?, August 2015; Aloko, Lemmens and Van Oerle, Mobile payments in emerging markets, October 2015.
[2] Ponemon, 2015
[3] Deloitte, 2014

Security in the financial sector

The financial industry is most often targeted by criminals…

As can be seen in figure 1, 25 percent of all reported incidents related to criminal activity can be traced back to the financial industry. There are two main reasons for this. First of all there is a lot of money to be made from criminal activity in the financial sector. This is not only done through direct monetary theft, but also in the form of false insurance claims. The second reason why the financial sector scores high in terms of reported breach incidents is that regulation is strict, which enforces public reporting. In many other sectors there is a reluctance to publicly announce a breach. Still, we believe public data severely underestimates real underlying threats.

Figure 1: Reported incident rates across industries



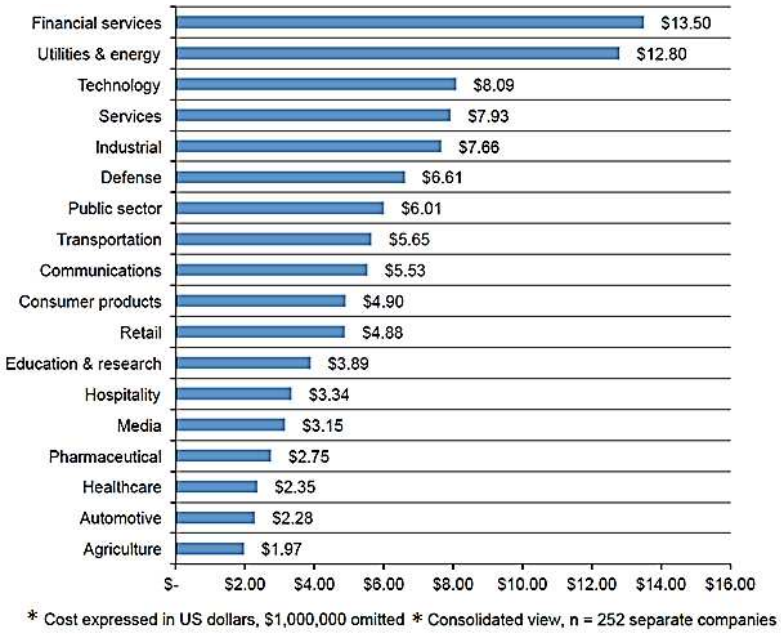
Source: IBM, 2015

…has the highest average costs related to cybercrime….

Not only is the financial sector most often targeted by criminals, the average cost of cybercrime is also highest of all industries. On average, the costs of data breaches in the financial sector are 13.5 million dollars. In total (across sectors) an amount of approximately 575 billion[4] dollars was lost as a result of cybercrime in 2014. Juniper estimates this amount to reach 2,100 billion dollars by 2019. Figure 2 looks at direct costs of confirmed cybercrime. It does not take into account indirect costs of breaches such as reputational damage or physical theft. Given the fact that the financial services sector depends on trust, the costs when including theft and loss of confidence are likely much higher.

[4] McAfee, 2014

Figure 2: Average annualized costs of cybercrime by industry or sector



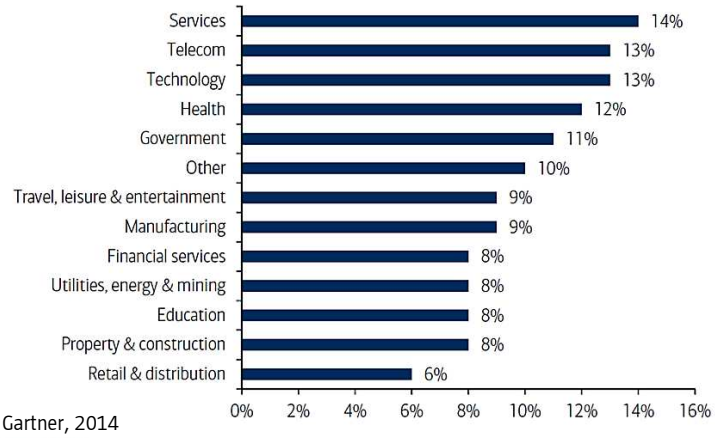
Source: Ponemon Institute, October 2015

...but invests least in security

When looking at the previous two figures, one would argue that financial service companies have most incentive to optimize security. However, the average budget that is available for security within the financial sector is one of the lowest when compared with other industries, as can be seen in figure 3. Overall IT spending in financial services is higher in terms of sales (6% versus a cross-sector average of 4%[5]), but we would expect security to follow that trend.

What is often still the case in financials is that security is thought out at the end of the design phase. A good example is mobile payments. A lot of banks offer mobile wallets, but the security of those mobile wallets (and mobile endpoints) only became a topic of consideration after some large breaches made the headlines. Regulators force financial institutes to open up to third party providers and to share customer information. Breaches often take place within this interaction. In the end, we believe financial institutions should determine the required level of security.

Figure 3: Percentage of IT budget spend on cyber security



[5] Gartner, 2014

Source: BIS, PwC

Security trends that shape the financial sector

Given that the financial sector is targeted most, has a lot to lose from breaches but underinvests in security, it is clear the market opportunities are large. Current cyber security spending across sectors is about USD 70bn (versus USD 1.2tn spending in IT)[6], growing at an estimated 6.5% per year. On the physical side current spending is about USD 30bn, representing card- and point-of-sale security. What we found interesting is that about a third of financial institutions does not have a specified security budget and rather determines its security spending on an ad-hoc basis. This observation can also be made when looking at spending in relation to breaches. Due to the reactive characteristics of security spending, we expect major breaches to be catalysts for security spending and only in the long run do we expect security spending to be a more constant, pre-budgeted factor.

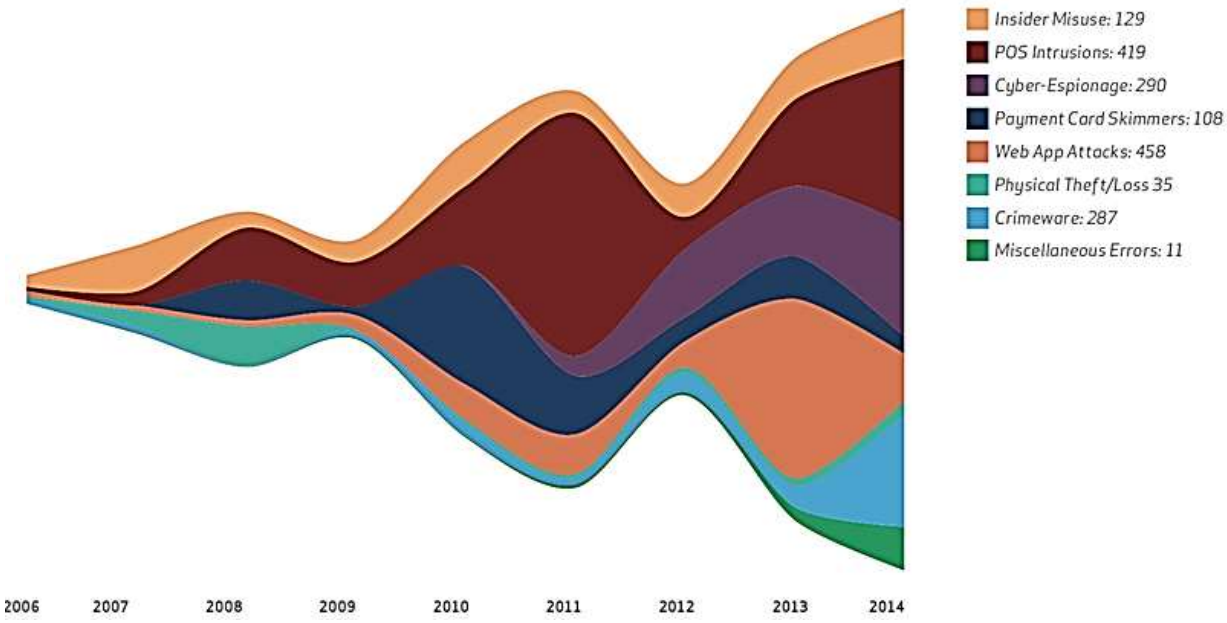
Criminals search for the weakest link...

The behavior of criminals in the financial sector is opportunistic, as can clearly be seen in figure 4. Criminals are constantly searching for the weakest link. After the introduction of the EMV (chip and pin) standard in Europe for instance, a lot of fraud simply moved to the US where magnetic stripes were being used. Now that the liability shift in the US is pushing the adoption of EMV, threats will move again to another area, most likely cyber.

Two important conclusions can be drawn from figure 4. First of all, the total number of incidents is increasing (and these are only the known/confirmed breaches!). Secondly, it is a relative game. POS intrusion is a clear example of this latter phenomenon. In 2011 most of the data breaches focused on POS intrusion, while in 2012 this was one of the least important areas. The underlying message is that there is a continuous requirement to update the complete product/service offering instead of focusing on a sub-part. Otherwise criminal activity will quickly try to exploit new relative weaknesses.

[6] Gartner, 2014

Figure 4: Count of incident classification patterns with confirmed data breaches



Source: Verizon, 2015

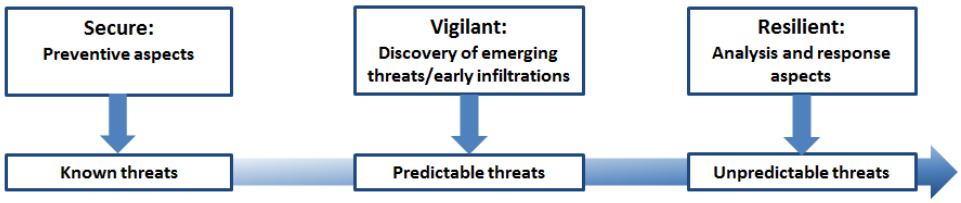
...and employees are your fastest way in

The most advanced security solutions will not work if the person who works with it is careless or ill-trained. Internal employees are most often quoted as main source of successful breaches. Research by SANS institute (2015) provides the following five causes of successful breaches in the financial sector: internal employees (46%), spearfishing emails (42%), exploits on unpatched or misconfigured systems (27%), lost devices (27%) and compromised endpoints (26%). Within internal employees, most fraud is committed by junior employees, followed by middle management. This clearly shows the need for security planning in terms of restricted access, document encryption and staff training throughout the organization.

Secure, vigilant and resilient

In order to optimize security, financial institutes must have a clear roadmap. This can be accomplished by defining the task of management to create a secure, vigilant and resilient strategy for security. Secure refers to reacting to currently known threats and making sure that the underlying application- and system security are up to date. Being vigilant implies being able to react quickly to new threats and continuously search for unfound breaches. The focus of resilience is to minimize damage once a breach has occurred and to develop a clear roadmap on how to respond to security issues. On the back of these three elements we discuss trends that are shaping, or will shape, security in the financial sector.

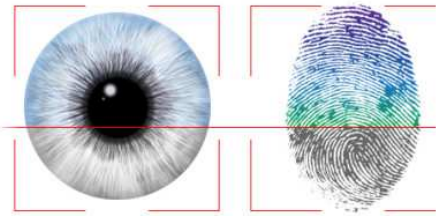
Figure 5: Three dimensions to manage security effectively



Source: Deloitte Center for Financial Services analysis, Robeco

1. Secure

Secure refers to the capacity to protect infrastructure against known threats. Being secure is in and of itself not sufficient to manage all security related threats, but it forms the foundation of the security roadmap. There are three dominant trends that shape this area, namely user authentication, preventive cyber security and end-point protection.



Biometric authentication becomes more important for device security

In order to prevent the bulk of fraud on the physical side, it is important to authenticate a user. In order to do so there are three options available. The first is authentication through something that only the user knows, such as a PIN or a password. The second method is to identify the user by means of something that only the user has, such as tokens or proximity cards. The third method is identification by something that only the user is characterized by, such as biometrics. The latter area is relatively new and growing fast.

Biometrics differs from the other two authentication methods in that a binary element (correct or wrong pin) is replaced by a probabilistic approximation of correct or wrong. This technology can mostly be found back in mobile applications, but within the financial sector it also has use cases for point of sale terminals and payment cards. All three methods of identification have their pros and cons, but we think biometrics will have the largest impact. Within biometrics there are many alternatives and it is too early to tell which method will prevail. It is likely that we will see a combination of biometric identification methods being used in different situations. Appendix B shows the main pros and cons of selected biometric authentication methods.

Device authentication through secure elements

Another important trend within physical security is the installation of the so called secure element. At the moment there are two forms of secure elements. They can either be installed on the device itself, such as Apple does with iPhone 6 and newer, or on the SIM card, which is the Samsung approach in cooperation with Oberthur. Although there are alternatives to physical secure elements (like host card emulation), we believe secure elements will become more important to endpoint security and will be used in combination with online/soft security instead of being replaced by it.

Preventive cyber security is the basis of online security

Technology enabled a large part of business interactions to move online. This is also the case within the financial services industry. Instead of having to walk into a physical branch, more and more can be done online. This brings along new challenges in terms of security. Financial institutions have to make sure that the hardware layers are well protected.

Firewalls and anti-virus scanning form the basis of being secure in an online environment. This layer has become more commoditized over the years. Due to this characteristic it is important for the suppliers of these products and services to have scale. As discussed before, basic cyber security products and services form the foundation of security from an online perspective. The need to constantly keep up to date implies these products cannot be disregarded, which forms an attractive recurring business potential.

Endpoint security forms the bridge between being secure online as well as offline

Bring your own device (BYOD) is a clear trend and within the financial sector this is no different. Not only do more employees use their own devices to work (mostly for checking emails at home), the mobile phone is also being used to perform a multitude of functions like scanning or making payments (half of e-commerce payments are done through the mobile phone[7]). Currently many of these own devices are not well protected.

One of the most striking trends in terms of cyber-attacks is the focus on mobile endpoints. In terms of being secure, endpoint security requires a combination of online and offline elements. Secure elements and user authentication form the physical side of security, while virus- and malware scanning form the online side of security. We think that in its current stage too much attention goes to prevention of endpoint breaches, while we would argue threat analysis should become a future focal point.

2. Vigilant

Being secure is not enough, but many organizations still believe it stops there. Installing firewalls and buying anti-virus scanning software will indeed protect against known threats and it is important to continue to protect against them. Referring back to figure 4, the opportunistic behavior of criminals would otherwise allow for old vulnerabilities to be re-used. Instead of only preparing for the known threats, a financial institution also needs to be prepared for emerging threats, most of which are found online. Within vigilance the main trends are the need to move up the cyber security stack and changing regulation.

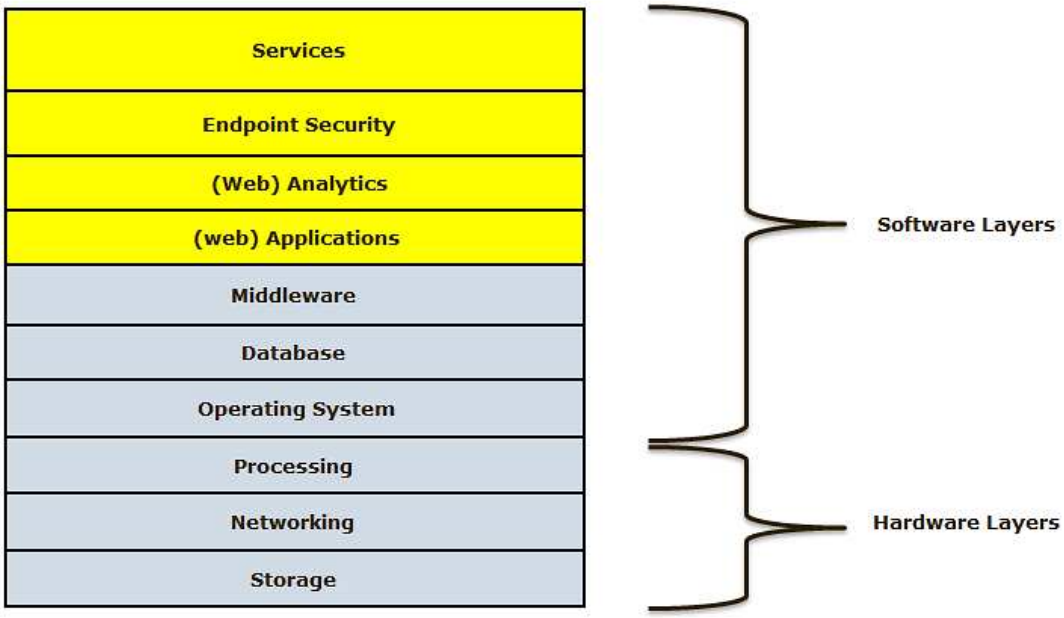
Cyber security is the name of a complex multi-layered game

Figure 6 introduces the so called technology 'stack'. The first focus of security was on the hardware layers. Currently more applications have migrated online and there is a more general move towards (private) cloud services which diminishes the need for self-owned hardware. This implies it is not enough to protect only the hardware layers, because the software layers on top have become directly accessible. In the lower part of the stack the more commoditized products are offered. Firewalls, anti-virus and DDOS (distributed denial of service) can be found here.

Being vigilant implies constantly scanning all layers for intrusions in order to react as soon as possible to breaches. Many companies in the financial sector still have difficulties to behave vigilantly. It takes too long in order to find exploits (205 days on average[8]) and to fix those exploits (30 days on average). The layers are currently too connected which implies an exploit can travel fast, with 75% of the total breached devices being reached within one day[9]. We expect the layers to become more separated in terms of security and we think specialized security products per layer will become an important differentiator for security companies. Examples are solutions for email scanning and sandboxing in order to counter advanced persistence threats and anti-DDOS solutions.

[7] Iovation, 2015
[8] The Economist, November 2015
[9] Ponemon, 2015

Figure 6: The technology stack



Source: Robeco internal resources

Moving up the stack

A trend that is clearly shaping this area is the need to move up the technology stack. An example is the trend for more and more banks to migrate parts of their business to the cloud, which allows them to react more quickly to changing demand. Payment processors for instance have peak moments around Christmas and in May. In order to facilitate this demand, they exceed capacity by 40%, which implies that on average days more than half of their computing power sits idle. They now seek the solution in the cloud business.

We expect to see banks move non-critical processes (HR, CRM etc.) to the cloud, but keep crown jewels in-house for now. This implies security will also need to migrate to the cloud and up the stack. As a result we see many companies coming to market with specialized layer solutions. Especially within web applications we think security will become a more dominant theme. Developers of web applications used to spend little time and money on security because they only gain when new products are quickly launched. Security is often seen as a cost and an obstacle to first mover advantages. Changing regulatory conditions are likely to change this. We believe more resources will be allocated to security within the web applications layer.

Very fragmented market

Gartner has introduced the 'magic quadrant' in which a certain solution is split between challengers, leaders, niche players and visionaries. The framework lays out more than 200 categories of technology providers, of which about half represent solutions for cyber security. Appendix A lists the biggest cyber security threats for the financial industry. Most attention currently goes to forensics and real time detection. Being vigilant is also about being able to discover new threats in a timely manner. We see demand for these services increase fast and expect forensics and detection to become essential parts of the security product range. Especially within the financial sector we believe that regulatory changes drive demand for these specific products given the fact that undiscovered breaches can be fined if too little effort is made to detect and analyze it.

New regulation will shape vigilance

Perhaps one of the strongest catalysts for security spending in the financial sector is provided by new cyber security regulation. Traditionally, legislation has not been able to keep up with developments in the cybercrime space, but that is changing. One of the biggest regulatory impacts will be the installation of dedicated security employees. Once companies are required to have dedicated security employees, security spending will also become more sophisticated.

USA and EU drift apart in terms of regulatory enforcement

In the US, regulation mainly focuses on sharing breach information. The response of Google to the 'Aurora' attack in December 2009 completely changed the landscape. Google went public with the breach, which had not been done before for fear of reputational damage. Besides sharing the insights from the breach, Google also publicly pointed to the source of the attack (China) and got government protection in return. Other commercial companies realized there was value in their data and they had to protect it too. New regulation in the US is now building upon the actions of Google to go public with the breach information. The Cyber Information Sharing Act (CISA) was passed by US congress in October 2015. This bill allows companies to share personal information in order to detect, prevent and mitigate cyber threats and vulnerabilities. Clearly, centralized data analytics becomes a more important industry as a direct result of this bill.

Within the European Union, the tone of voice is much stricter than in the US. Via the introduction of the General Data Protection Regulation (GDPR), the European Union tries to create a united approach to battling cybercrime. This is not a directive, but a regulation, which implies all member states have to comply and implement the new laws within the coming two years. It is expected that at the end of 2015 an agreement will be reached on this law, which implies that from December 2017 onwards the GDPR becomes effective.

Although the exact details are not yet fully clear, the law goes much further than in the US. If a company has not complied with the regulation on protecting data against criminal activities, it can be fined up to 5% of annual worldwide revenue, with a maximum amount of 100 million euros. Next to the GDPR there is also a directive in the making that focuses more on financial institutions. The Network and Information Security (NIS) directive is set to come into force in 2017, specifying that companies that have experienced a breach are required to report to a data protection authority. This authority is allowed to disclose details to peers or to the public if this is deemed necessary. Sanctions for insufficiently securing systems are also part of this directive, but the details are not yet known.

3. Resilient

After being secure and vigilant, the final step is to be resilient. The realization that there is no way to completely protect against breaches (on the physical side as well as on the cyber side) is an important one. It opens up for incident analysis and the formulation of a proper response procedure. Trends that shape resilience are the organization of corporate governance structures, outsourcing and insurance.

Organizing corporate governance will drive security spending

Based on Ponemon research as well as internal sources, we prepared eight corporate governance questions in order to assess the level of sophistication concerning cyber security governance. According to Morgan Stanley research, based on insights from FireEye, only 36 percent of EU companies are positioned well enough to meet the security standards under the new set of regulations, which come down to being secure, vigilant and resilient. Although information on this topic is not readily available in many cases, we believe it is important to ask the questions in figure 7 to assess the downside risk from security breaches.

Figure 7: Corporate governance questions on security

Does the company…

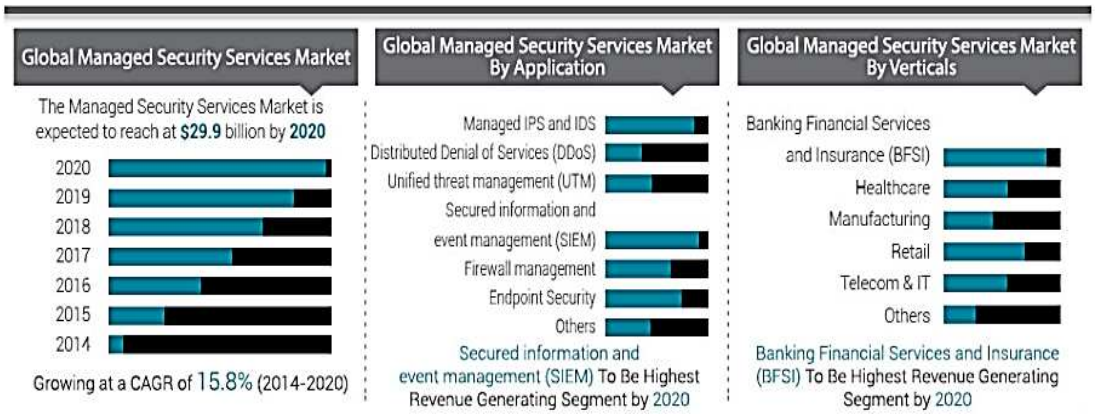
…comply with audited industry leading certifications (e.g. the PCI DSS or ISO27000 series)
…have a clear action plan with clearly defined crown jewel data and backup systems?
…provide training and awareness activities internally as well as to external partners?
…have a high level security leader with a clear connection to top management?
…install a senior level Security Council or presence in the supervisory board?
…use security metrics to benchmark against peers and best practices?
…have a sufficient budget that is separate from the IT budget?
…employ certified/expert security personnel?

If it becomes too much to handle; outsource it

Most cyber security products are being sold through resellers. Smaller financial institutions that lack resources to have a dedicated security department are often advised by these resellers in terms of products and services to buy. This model will, in our view, become more dominant. We think managed security service providers (MSSPs) will benefit. This will be especially the case in Europe where regulatory pressure is likely to increase demand for outsourcing services.

Next to regulation, the complexity of the security landscape changes fast which implies that companies with limited resources can have difficulty keeping up with developments. Another important implication of this driver is that large security companies that offer solutions on many different parts of the security chain become more interesting to customers. These companies devote a lot of time in order to advise their clients on the products they need and are then able to select those products from their own product range. This makes it more difficult for smaller niche players to make their entrance. On the other hand side, MSSPs are able to combine many small niche players into one solution, without bothering the end-client with the exact technical details. In that way the end-customer is not tied to one supplier and neither does he have to make complex decisions per security layer. An important side note is that the customer will always be responsible for security in the end.

Figure 8: The global Managed Security Service (MSSP) market



Source: Allied market research, 2013

If you can't beat them, insure yourself

The final trend we see is the offering of insurance products that cover damage in case of breaches. 2014 Was the year in which this trend saw a significant jump in both the number of insurance solutions offered and the number of firms buying coverage. Over fifty insurance providers currently offer products. Demand for insurance has risen by 20 percent per year since 2012, with financial institutions representing the biggest increase in coverage buying. Of US companies with USD100 million or more in annual revenues, 85 percent purchased cyber or data privacy insurance and of that group, 44 percent filed a claim as a result of a breach[10].

Insurance coverage differs per provider, but usually the direct cost of a security breach or hack is covered (up to a certain amount). Common direct costs are: regulatory fines and penalties, notification costs and public relations expenses, forensic investigation of the breach, and legal defense expenses. Other costs like reputational damage or loss of future revenues are most often not covered by insurance.

EU will follow the US cyber insurance market

Most buying takes place in the US at the moment, but we expect to see the same in Europe when regulation changes. The current market size is 2 billion dollars and is expected to increase to 10 billion dollars[11] in 2020. An interesting discussion within cyber insurance is also the link between insurers and security product offerings. One model would be that the insurance company only pays out in case the insured party has used pre-specified security products. We think this is an interesting area to keep a close eye on, although not yet investible given the fact that these insurance products still represent only a small part of the product portfolio to many insurers.

[10] Wells Fargo, 2015

[11] Morgan Stanley, 2015

Well positioned companies

There are two ways to translate the trends described above into investment implications. The first angle concerns the financial service companies themselves, and how they are positioned in this changing landscape. Especially the corporate governance framework that we described in figure 7 is of help here. It goes without saying that financial companies that are well positioned have a clear strategy for being secure, vigilant and resilient. Another angle would be to specify companies that are able to help financial institutes to move into the right direction by offering security products and services.

Different trends, different investment dynamics

Companies able to fulfill the requirements of being secure benefit from having scale. The products and services that are being offered are reasonably similar and price is the biggest differentiator. Companies we list below have this scale advantage. The product offering within being vigilant is far less price sensitive. Offering unique solutions to deal with advanced threats is at the core of the companies we list below. Solutions for being resilient are still early stage. Companies that offer products and services to become resilient to security risks are no pure-plays. We list investment opportunities with an as high as possible exposure to the theme. By specifying the underlying dynamics, we think it becomes clear that the security theme is broad and there is not just one correct way of approaching investment opportunities.

Limited investment opportunities with a clear focus on the financial industry

Many of the companies we identified have exposure to almost all industries. Within the financial sector a lot of the basic infrastrucure to be installed is the same as in other industries, but there are also parts of the industry that require a more specialized approach. It is important to have a good understanding of the specific underlying mechanisms and risks, especially within payments. Companies that stand out from this perspective are Vasco Data Security, Oberthur and Imperva. These companies have their largest customer base within the financial industry and are able to tailormake products for their customers.

Figure 9: Well positioned companies to benefit from cyber security trends

Secure				Vigilant		Resilient	
Authentication	**Secure element**	**Basic cyber security**	**Endpoint security**	**Advanced cyber security**	**Data analytics**	**Managed Security Service Providers**	**Insurance**
• Safenet • EMC • Gemalto • Symantec • Vasco Data Security	• NXP • Gemalto • Oberthur • Giesecke &Devrient	• McAfee • Sophos • Palo Alto • HP • IBM • Checkpoint	• Symantec • MacAfee • Sophos • Kaspersky • Trend micro	• Palo Alto • Checkpoint • Fortinet • Imperva • Splunk • Fireeye	• IBM • SAS • KNIME • Rapid Miner • Relx	• IBM • Dell SecureWorks • AT&T • Verizon • Symantec	• Munich re • Swiss re • Hannover re • Beazley • Travelers • Scor

Source: Robeco. This table is intended to facilitate analysis and should not be construed as an investment advice in any way.

Appendix A: biggest cybercrime challenges in the financial sector

1. **Advanced Persistent Threats (APT).** APTs use undetected, continuous computer hacking processes to gain access to a high-value organization's network. Phishing emails or other tricks to fool employees into downloading malware are a common practice. When the unauthorized person gains access, they often go undetected for a long period of time—quietly stealing data, committing fraud, destroying an institution's economic stability or undermining its reputation.
2. **Insider and Internal Threats.** Any employee, contractor, supplier, or business partner who has authorized yet uncontrolled access to systems and/or sensitive information all have the opportunity to do irrevocable harm to a company. This threat has grown more substantial by the increased use of personal devices in the workplace, personal email, and cloud-based and USB storage devices. Intentionally or unintentionally, insiders can undermine systems, open them to malicious intrusion, and engage in fraud, theft, or market manipulation.
3. **Denial of Service Attacks.** These threats are defined as "any attack intended to compromise the availability of networks and systems" and are of concern to financial corporations operating consumer-facing websites or trading systems. Such attacks flood a network with phony connection requests, making it unavailable to process legitimate user requests.
4. **Account Takeovers.** Cyber criminals have quickly discovered how to exploit financial and market systems that interface with the Internet, such as the Automated Clearing House (ACH) systems, card payments, and market trades. Exploiting system users, rather than the systems themselves, earn criminals access to existing bank or credit card accounts or financial systems, and allow them to carry out unauthorized transactions. A recent report on cybersecurity in the banking sector identified that almost half (46 percent) of institutions reported account takeovers as the most frequent cyber intrusion activity they experience.[5]
5. **Securities and Market Trading Breaches.** Financial institutions in the securities and brokerage business, as well as their customers, are frequently targeted by cyber criminals. According to the FBI, market manipulation and unauthorized stock trading are common risks faced by traders and the exchanges they are sold on.[6]
6. **Third-Party-Payment Processor Breaches.** Sophisticated cyber criminals are also targeting the computer networks of large payment processors, resulting in the loss of millions of dollars and the compromise of personal information of millions of individuals.
7. **Supply Chain Infiltration.** In recent years, trusted suppliers of technical, computer and security equipment, software and hardware have been targeted by cyber criminals seeking to gain physical and technical access to financial institutions. Cyber criminals are continuously devising new ways to infiltrate financial institutions, from posing as vendor employees to delivering infected equipment. Some recent attacks involved hardware installed in bank branch systems to enable transactions to be manipulated via mobile networks.[7]
8. **Mobile Banking Breaches.** Meeting customer demands for greater mobile banking capability, has opened financial institutions up to another cyber threat. Cyber criminals have quickly figured out how to exploit the vulnerabilities in mobile technology by using malicious websites, text messages, or mobile applications to gain access to a user's credentials and account information.
9. **Payment Card Skimming.** A skimmer fitted to the outside or inside of an ATM or gas station pumps enables a criminal to collect card numbers and personal identification number (PIN) codes. The stolen data is usually sold or used to make fake cards to withdraw money from the compromised accounts. As companies continue to roll out—and consumers embrace—new electronic, wireless payment systems, criminals are quickly adapting. Hackers have already designed Bluetooth-enabled wireless skimmers to instantly download data when in range of the wireless network.

Source: Lockheed Martin, 2015

Appendix B: Selection of biometric identification methods

Technology characteristic	Fingerprint	Iris	Facial	Hand
How it works	Captures and compares fingertip patterns	Captures and compares iris patterns	Captures and compares facial patterns	Measures and compares dimensions of hand and fingers
Cost of device	Low	High	Moderate	Moderate
Enrollment time	About 3 minutes, 30 seconds	2 minutes, 15 seconds	About 3 minutes	About 1 minute
Transaction time[a]	9 to 19 seconds	12 seconds	10 seconds	6 to 10 seconds
False nonmatch rate[b]	.2%–36%	1.9%–6%	3.3%–70%	0%–5%
False match rate (FMR)[c]	0%–8%	Less than 1%	0.3%–5%	0%–2.1%
User acceptance issues	Associated with law enforcement, hygiene concerns	User resistance, usage difficulty	Potential for privacy misuse	Hygiene concerns
Factors affecting performance[d]	Dirty, dry, or worn fingertips	Poor eyesight, glare, or reflections	Lighting, orientation of face, and sunglasses	Hand injuries, arthritis, swelling
Demonstrated vulnerability[e]	Artificial fingers, reactivated latent prints	High-resolution picture of iris	Notebook computer with digital photographs	None
Variability with ages[f]	Stable	Stable	Affected by aging	Stable
Commercial availability since	1970s	1997	1990s	1970s

[a]Amount of time it takes to verify machine-read biometric versus stored biometric.

[b]The probability that individuals who should be matched are not matched by a biometrics system.

[c]The probability of an erroneous match in a single template comparison.

[d]Human characteristics or measurement condition circumstances that could adversely affect accuracy of biometric systems.

[e]Demonstrated methods of beating biometric systems that have been employed in tests.

[f]Effects of age, if any, of individual on his or her biometric identifiers.

Source: globalsecurity.org, 2015

Jeroen van Oerle
Trend analyst at Robeco
Trends Investing

Patrick Lemmens
Portfolio Manager Robeco
New World Financials

Frank van der Spek
Group Security & Continuity
Manager at Robeco

Important information

This document has been carefully prepared by Robeco Institutional Asset Management B.V. (Robeco).
It is intended to provide the reader with information on Robeco's specific capabilities, but does not constitute a recommendation to buy or sell certain securities or investment products.
Any investment is always subject to risk. Investment decisions should therefore only be based on the relevant prospectus and on thorough financial, fiscal and legal advice.
The information contained in this document is solely intended for professional investors under the Dutch Act on the Financial Supervision (Wet financieel toezicht) or persons who are authorized to receive such information under any other applicable laws.
The content of this document is based upon sources of information believed to be reliable, but no warranty or declaration, either explicit or implicit, is given as to their accuracy or completeness.
This document is not intended for distribution to or use by any person or entity in any jurisdiction or country where such distribution or use would be contrary to local law or regulation.

The information contained in this publication is not intended for users from other countries, such as US citizens and residents, where the offering of foreign financial services is not permitted, or where Robeco's services are not available.
Robeco Institutional Asset Management B.V. (trade register number: 24123167) has a license of the Netherlands Authority for the Financial Markets in Amsterdam.