CyberSecurity in the financial services sector:

threats and opportunities

kaspersky

CCHQ
Creative Cyber & Data Solutions

Foreword

The financial services industry is the biggest consumer of CyberSecurity products and services. Financial institutions are constantly targeted by threat actors, looking to monetise cyber attacks. Threat actors like Lazarus are exceptionally skilled at launching sophisticated cyber attacks targeting the financial services sector.

The current threat landscape has evolved considerably, and hackers are developing more sophisticated tools and techniques, leveraging artificial intelligence and automation. Yet, almost 30% of organisations surveyed across industries don't perform any adversarial assessment.

Developing a sense of the overall threat landscape and the threat actors' profiles targeting an organisation is essential to building appropriate and adapted cyber defensive mechanisms. Organisations should develop protective measures while understanding the threat actors likely to target them. Threat intelligence should go beyond mere informational purposes and provide actionable, contextual, and industry-specific insights and information on threat actors' activities as they relate to the industry and organisations within scope.

In the recent years, the financial services industry has experienced a paradigm shift from an operational and service delivery perspective. The ecosystem has considerably evolved with the advent of FinTech companies that provide financial services in a more agile way at more competitive prices relative to incumbent Banks. From an operational perspective, this paradigm shift presents numerous challenges and opportunities regarding digital transformation and IT security. New companies can be built natively for the cloud. On the other hand, incumbents still need to address the complexity and inefficiency of multi-layered legacy systems and operations, creating numerous potential security vulnerabilities. Closing all of the gaps all of the time would prove a daunting task. Organisations should instead take a proactive approach to prioritise security strategy to protect their most valuable and critical assets. Filter out the most relevant security events to minimise the impact and incident costs will contribute to building operational and infrastructure resilience.

Understanding your adversary will be vital to building solid and adapted protective measures and integrating the right technology to support security strategy and governance. A sound security strategy and framework will maintain business continuity, build operational resilience, and enable sustainable business growth.

Jean Lehmann
CEO, Cyber Capital HQ

From online banking and mobile payments to cloud solutions or artificial intelligence, digitalisation is advancing in the financial industry. However, the growth of complex, digital financial technologies also increases the attack surface for IT security threats; the high degree of networking makes the financial system particularly vulnerable.

In the wake of the pandemic this drive for digitisation has accelerated further, as people and companies have increasingly shifted their activities into the virtual space. At the same time, the financial sector is of great importance for public life in the United Kingdom and the FCA (Financial Conduct Authority) has encouraged financial services firms to **comply with operational resilience** ahead of the March 2025 deadline for the PS21/3 guidance. As a result, a sustainable and adequate CyberSecurity strategy and structure is essential for British financial companies.

But what is the current state of IT security in the UK financial services industry? What are the biggest threats facing the sector? How are budgets being distributed? What challenges do IT decision-makers face today, and what measures are they taking to ensure sustainable and effective protection against current and future cyber-threats?

A current Kaspersky survey on the British CyberSecurity landscape within financial services aims to provide answers to these questions. The results paint an overview of the most important threats currently from the perspective of those affected and show how IT security managers in the industry assess the current situation. In addition, it becomes clear how companies and institutions can effectively protect themselves against a constantly growing number of cyber threats.

Contents

Five key findings in the UK financial services sector 5
The current status of CyberSecurity in the financial sector 6
Voices from the industry: what CyberSecurity issues keep executives up at night? 7
Threats, opportunities and pitfalls – the role of CyberSecurity in the financial services sector 8
Consequences: what is the financial sector afraid of? 12
Measures against cyber-threats in the financial sector: combining people and technology is key 13

Methodology

The survey was conducted in January 2022 by Arlington Research on behalf of Kaspersky. It assessed the opinion on IT security from 200 IT decision-makers from the financial industry in the UK, of whom, 78.6% were senior or middle management. More than half (54%) of the sample work in companies with 50-499 employees, while 46% are at organisations with more than 1,000 workers.

Five key findings in the UK financial services sector

1. **A multi-layered CyberSecurity landscape: employee breaches and spear-phishing attacks reached a peak during the pandemic**
   98% of respondents from financial organisations experienced at least one CyberSecurity issue during the pandemic. Employees either intentionally or unintentionally disregarding security principles (49%) and spear-phishing attacks (35%) were the most common incidents, followed by generic malware attacks and targeted attacks (32%). Correspondingly, almost three quarters of respondents (74%) continue to rate the IT threat level for their company as "high". The C-Suite in particular has appeared to be more pessimistic in this regard, with 86% openly concerned.

2. **Organisations are worried about cyber-threats, yet they do not feel completely safe**
   Despite the majority of respondents in the financial sector believing that their company is sufficiently equipped to fend off cyberattacks, only 29% of respondents felt strongly about this, highlighting a degree of complacency. Surprisingly, the highest level of doubt is recorded amongst IT security professionals, with only 37% strongly agreeing that their CyberSecurity is adequate for the level or risk they anticipate. Almost half (48%) of respondents strongly agree they have a business continuity plan in the event of a cyberattack. However once again this is lower for IT security respondents (46.5%) with small financial institutions most likely to use these emergency mechanisms (63.2%) compared to large and very large organisations (50%).

3. **Lack of employee security awareness heightens the risk of non-compliance**
   On average, 70% of respondents agreed that non-compliance with regulations increase the risk of cyberattacks. In fact, a large number of respondents (44%) fear the financial impact of regulatory fines, rising to 53% for senior management (e.g. C-Suite). However, nearly half of (49%) state that IT security incidents during the pandemic were attributable to employees themselves, with remote working (13%) and ignoring company policies (16%) cited as the biggest vulnerabilities, compounded by the fact that many employees still lack basic CyberSecurity awareness. Although financial companies train their IT staff better than any other industry with regard to CyberSecurity, there is definitely room for improvement for regular training in other departments – only 37% said all IT professionals and 24% said all C-Level executives are regularly trained on CyberSecurity.

4. **The IT security budget paradox: compensating for the lack of expertise**
   Almost three-quarters of IT decision-makers at financial companies (74%) rate their cyber threat level as high. Although the majority of respondents (85%) think that their IT security budget is sufficient for the next two years, more than half (54%) believe that they do not have the necessary internal know-how to protect themselves comprehensively against cyber-threats, with over 30% of IT security professionals strongly agreeing with this statement. In fact, 85% want to work with external service providers - especially in small businesses with 50 to 249 employees (93% do so).

5. **Threat intelligence is being used, but not yet everywhere it's needed**
   Overall, according to our research, almost all (99.5%) financial institutions use at least one threat intelligence security service to protect themselves against the increasingly complex threat landscape. The most popular services are malware analysis (44%), APT reporting (43%) and targeted attack discovery (43%). However, not all companies use all the services they would like. More than a quarter, (26%) advocate that security assessments should be used in their company. Meanwhile, just over a third (34%) think "threat data feeds and threat lookup to help improve incident response" should be used in their organisation, when currently they are not.

The current status of CyberSecurity in the financial sector

Almost three-quarters (74%) of the decision-makers surveyed in the UK financial sector rate the current CyberSecurity threat situation in their company as "high", with 86% of the C-Suite in particular being more pessimistic, with 42% of those within very large organisations with 5,000-1,0000 employees agreeing.

Overall, the decision-makers surveyed reported multiple threats since the beginning of the pandemic. 98% say that their company has been affected by security incidents during this period. The types of attacks were as varied as they were complex: almost four in ten decision-makers (35%) surveyed reported spear-phishing attacks, more than a third (34%) had been affected by generic malware attacks and a similar level (33%) had been impacted by targeted attacks.

Almost a third (31%) of respondents have had to deal with spyware. However the biggest threat seems to be coming from the employees themselves – 16% think that the workforce is the greatest culprit for cyber-breaches, with almost 19% of IT security respondents agreeing. Almost one-in-three C-Suite executives experienced a cyberattack targeting "employees intentionally not following security protocols", whereas 40% experienced attacks targeting "employees who unintentionally disregarded CyberSecurity practices". This is followed by the 'bring your own device' trend (16%, jumping to 21% for IT respondents) and remote working (13%).

In our research, a C-Suite executive from a very large organisation (5,000 to 10,000 employees) also points to the dangers posed by untrained personnel, particularly "negligence within the company that has created a network risk, as some of the current staff training is not strong enough". Additionally, an IT security specialist at a medium-sized company (250 to 499 employees) also fears the "lack of understanding and cooperation when it comes to IT security".

Despite the many threats, seven in 10 respondents (75%) in the financial services sector believe their company is sufficiently equipped against cyberattacks. However, this differs depending on the size of the organisation and the role. For example, more than four in 10 (42%) very large organisations (5,000-10,000 employees) admit that the risk of cyberattacks is high; however just 21% strongly agree that they are suitably protected. **This figure doubles for medium organisations (500-999 employees), with 47% showing a high level of confidence. Rather concerning is the fact that less than one in three respondents strongly believe that their CyberSecurity measures are sufficient, followed by just 37% of IT security professionals, highlighting a degree of complacency.**

Almost half (48%) strongly agree they have a business continuity plan in the event of a cyberattack. This is slightly lower for IT security respondents (47%) with small financial institutions most likely to use these emergency mechanisms (63%) compared to large (41%) and very large organisations (40%).

Once again, the strongest sense of security prevails in medium-sized financial institutions with 500-999 employees – although a particularly high risk is found here. Four in five respondents (82%) believe that companies of this size are well protected against IT security threats. At 84%, they also use disaster recovery plans most frequently.

More than eight in 10 (86%) respondents from the financial sector would like to work with an external security partner. Among small companies, the approval rate is even higher (93%).

"Whether it's ransomware, phishing, targeted attacks or 'just' generic malware, the financial industry faces a diverse threat landscape. It is therefore not surprising that the IT decision-makers we surveyed rate the threat situation in the UK as high. Financial institutions see themselves as sufficiently equipped against cyberattacks because, among other things, they have emergency plans at hand. However, the complications brought by a highly regulated environment is prompting the sector to invest more in IT security. After all, a successful attack can lead to the loss of data, money and customers. We recommend a comprehensive, multi-layered CyberSecurity approach that covers all possible entry points."
Stuart Peters, Territory Manager, UK&I at Kaspersky.

Voices from the industry: what CyberSecurity issues keep executives up at night?

As part of the study, the research participants were also able to express themselves with open answers about their assessment of CyberSecurity in their companies and its related challenges. Reviewing their comments, it's clear that there is a fundamental awareness of IT security threats in the financial sector.

Statements from managers

For a senior manager (C-suite) of a smaller company with 50 to 249 employees, the main concern revolves around "integrating digitalisation and maintaining enhanced CyberSecurity". The senior manager (C-suite) of a large company (1,000 to 4,999 employees) also agrees with this statement: "The cost is continually increasing and so are the threats so it is difficult to see how we can keep ahead of the hackers". An IT employee from the middle management of a large company laments the "increased volume of attempted cyber and ransom ware attacks we see each week. At some point one will be successful based and the sheer number of attempts". A member of the C-suite of another large company gets more specific: he worries about the "disclosure of the company's secrets, which may lead to the company's bankruptcy" and an IT specialist at a large company also fears "malware, which may temporarily paralyse the system".

Overall, the management level is primarily concerned about the negative consequences of an IT security incident for the company and the loss of image if financial damage or the loss of sensitive data should occur.

Statements from IT experts

At the IT level, on the other hand, the respondents' thoughts largely revolve around the internal problem areas that could allow a cyberattack - or else the lack of preventive measures to prevent a security incident. An IT specialist from a very large company complains about the "internal use of non-standard security, because some staff training is not up to standard". Another expert from a large organisation fears "inappropriate use of the system by employees".

An IT security expert - also working for a large company - fears "[a] DDoS attack on us, because that would make our customers lose confidence", which appears to be a broader concern shared by many others. Another IT employee from middle management also expresses concerns around "the risk of DDoS attacks that might happen at any time", with others claiming "Ransomware attacks leading to huge financial losses". Another IT specialist from a large company worries about "the increased volume of attempted cyber and ransom ware attacks we see each week. At some point one will be successful based on the sheer number of attempts".

Threats, opportunities and pitfalls – the role of CyberSecurity in the financial services sector

Challenges for CyberSecurity in the financial sector

On the one hand, three-quarters of respondents in the financial industry feel well equipped against possible cyberattacks. At the same time, however, more than half (54%) of survey participants say they do not have the internal IT security expertise to be fully protected against threats, with less than one-in-four (24%) strongly agreeing with this. Here, the level of agreement is higher among IT professionals (55%) than among their IT security colleagues (51%).

A Senior Management employee at a medium-sized organisation with more than 500 employees sums it up in the Kaspersky study: "My main concern is that there are new vulnerabilities that we don't have a way to deal with."

Another Senior Manager from a large company (1,000 to 4,999 employees) agrees, outlining that a major worry is "the ever-expanding technical knowledge of cyber attackers and being able to keep up to date". Meanwhile, a partner at a large organisation also stressed "the main concern is the lack of security and the inability of the company to operate normally", showcasing the need for external dedicated expertise.

"The need for skilled workers in the UK - as in other European countries - is increasing in all sectors; several thousand experts are needed in the security sector alone. This affects small and large companies alike. We see a tendency for companies with a lack of resources to outsource their CyberSecurity department to a service provider in order to be comprehensively protected despite a shortage of skilled workers - and that is a good decision! Since companies in Europe that rely on external experts are better protected, they are confronted with almost 10% fewer cyber-incidents than companies that work entirely or predominantly with internal resources."

Stuart Peters,
Territory Manager, UK&I, Kaspersky

The respondents see another major challenge in the ever-increasing requirements: Thus, 59.3% state that the growing burden of rules and regulations increases the risk that they will not be complied with.

Risks to CyberSecurity in the financial sector

Employees as a gateway for cyberattacks

Are employees really a significant gateway into corporate networks? The findings of the current study point to this being the case. Both the results of the study and the statements of the decision-makers surveyed lead to the conclusion that the "human factor" is a significant sticking point when it comes to cyber-threats in the financial sector.

In fact, 49% of all respondents stated that IT security incidents during the pandemic were attributable to employees. Respondents see particular challenges with regard to IT security expertise and data protection: ignoring company policies (16%), remote working (13%) and shadow IT (16%) are named as the biggest weaknesses. "Remote working, collaboration platforms, data security and privacy" were listed as the major worries for the CEO of a large organisation (1000-4999 employees), a sentiment that was broadly echoed by both IT professionals and IT security specialists.

Many survey participants bang the same drum with their statements: "my main concern is our employees and lack of understanding and cooperation when it comes to IT security," says a respondent from the middle management of a medium-sized organisation. "Negligence within the company has created a network risk, as some of the current staff training is not strong enough", says a manager of a large company (1,000 to 4,999 employees). Other statements across all company sizes speak of "inappropriate use of the system by employees", or even "phishing attempts trying to catch our staff off guard for hackers to obtain valuable information".

The study's figures also show that many employees in the financial sector lack awareness of CyberSecurity - and that there is definitely still room for improvement in terms of training potential. Although in just over a third of organisations (37%) all IT employees are regularly trained on security topics and procedures, the situation is less reassuring in the remaining departments, such as executive assistants, marketing, analysts and traders, accounting: between 21% and 35% of the respondents state that in all other departments less than half of the employees are regularly trained. One IT staff member at a very large company (5,000- 10,000 employees) puts it succinctly: "internal personnel negligence leads to security risks".

"The convergence between the acceleration in digital transformation and increased regulations is incentivising the financial services sector to strengthen security and compliance safeguards. If security awareness among employees in all departments does not keep up pace, the risk of non-compliance is heightened. CyberSecurity awareness is an essential element to mitigate the very real threats due to a lack of compliance".

Jean Lehmann,
CEO, Cyber Capital HQ

The risks posed to the industry seem to be well-distributed, without major spikes in a particular vector or attack. Aside from the threats already experienced during COVID-19 (spear-phishing, targeted attacks and employees), respondents cited more common threats: ransomware attacks (27%), DDoS attacks (29%) and even supply-chain attacks (24%) were prevalent. A respondent in a large organisation stated that DDoS attacks "would make our customers lose confidence", whereas a director in a medium organisation said that such threats "will temporarily paralyze our system".

"Our study shows the financial industry sees its own employees as the biggest security risk to its organisation. It is important to bring your own workforce aboard the CyberSecurity boat. Education is key, alongside the use of strong technological solutions. An up-to-date security awareness programme can be customised from department to department and must be integrated into the daily work routine. Employees need to understand the possible attack vectors of cybercriminals, as well as the consequences of their own actions. A wrong click on a malicious attachment or link opens the door for cybercriminals to enter the company network. Education must address the entire workforce - from reception to management, to create a strong security culture throughout the organisation."

David Emm,
Principal Security Researcher, Kaspersky

The budget paradox

On the one hand, more than eight in 10 (86%) of the surveyed decision-makers in financial institutions assess the IT threat situation as "high". However, although 85% of these respondents believe that their IT security budget is sufficient for the next two years, only 34% strongly agree.

Respondents from very large companies (5,000-10,000 employees) show the greatest confidence here (42%). In senior management, on the other hand, 85% is convinced that the IT security budget is sufficient for the next two years. In the open-ended question included in the study, however, there were divergent opinions. One IT employee from a large company stated: "new threats always mean a budget challenge", whereas a senior manager at another large organisation stated that "we are pushing the board to increase the budget for this so we can increase our security".

Three-quarters of decision-makers (75%) said that current measures were sufficient to protect their organisation from cyberattacks. Respondents from large companies (1,000 to 4,999 employees) consider their IT security measures to be sufficient with 80% agreeing so. **Interestingly though, only 37% of IT security professionals strongly agree, compared to the average 29% from all respondents, highlighting a degree of complacency. The majority (86%) state that their company desired the support of external CyberSecurity experts, with smaller companies with 50 to 249 employees (95%) doing so in particular.**

"The added value of CyberSecurity is underestimated by IT decision-makers within the financial sector. Even if many see themselves as well protected, the financial sector in particular should not skimp on cyber defence, data protection and Threat Intelligence - because every (£) Pound invested in CyberSecurity in the coming years will pay off and is ultimately money well spent in the medium and long term."

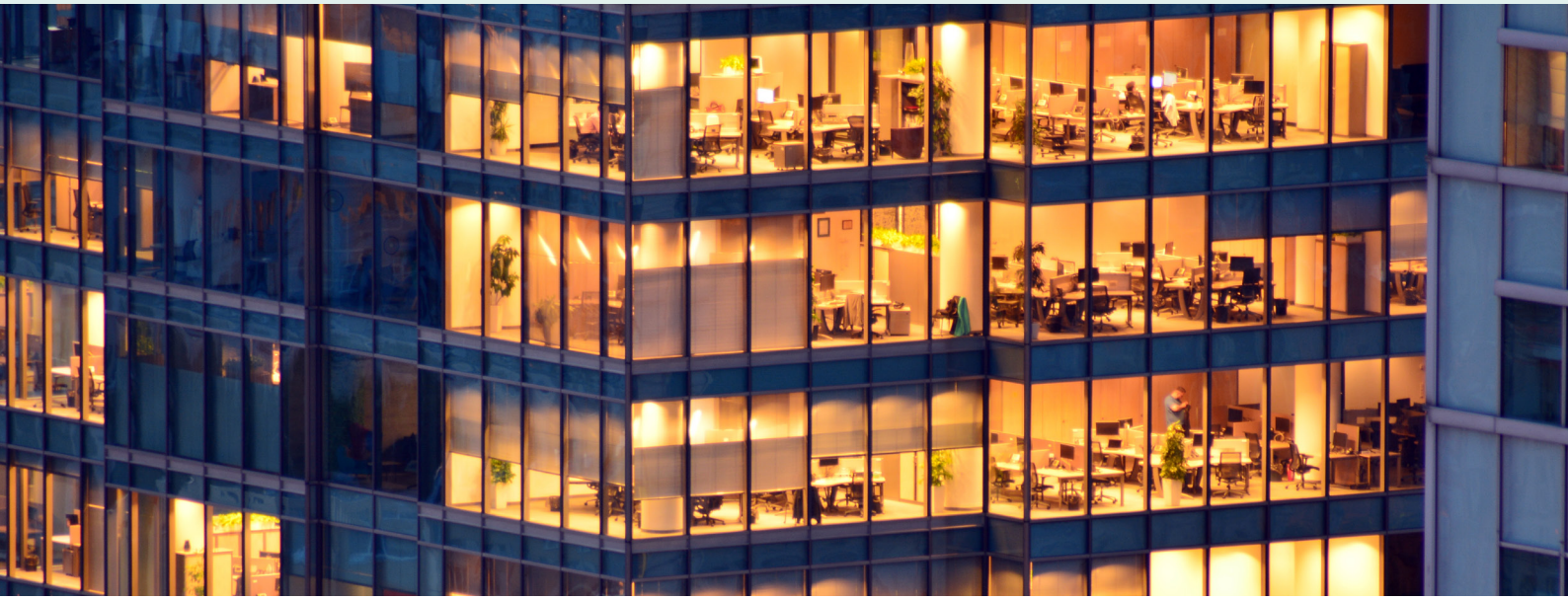
David Emm,
Principal Security Researcher,
Kaspersky

Consequences: what is the financial sector afraid of?

As part of the Kaspersky study, decision-makers in financial institutions were also asked what consequences of a possible cyberattack they most fear. The answers were complex: almost half (44%) fear the financial impact of regulatory fines or litigation. While 43% of decision-makers also fear the loss of customers for insufficient information security compliance, and others (41%) fear the damage to public image for insufficient information security compliance.

A similar picture emerges when looking at the statements from the open-ended question. An IT employee at a large company (1,000 to 4,999 employees) declared “the IT security I worry about most is in corporate software”. A large number of IT security employees and directors admitted that DDoS attacks and Trojans were experienced during the pandemic, having a direct impact on the availability of services to the public.

Mentioned again and again - across all company sizes - is the loss of sensitive data. A member of the C-Suite at a very large company (5,000 – 10,000 employees) says his biggest concern is "if customer data was taken, [we] would lose customers and business for years to come”. Another director in a medium-sized organisation stated that he is concerned about "all of our information being leaked”, with other organisations admitting they “would lose a lot” following an attack.



Measures against cyber-threats in the financial sector: combining people and technology is key

The financial sector in the UK is particularly vulnerable to cyber-threats. On the one hand, this is due to the high degree of digitalisation in the financial sector, which has become even stronger since the beginning of the pandemic. On the other hand, the financial sector is attractive for cybercriminals due to the monetary nature of the business as well as the amount of sensitive customer data managed by companies and institutions.

The study clearly shows that respondents in the financial sector are well aware of this special role. The majority of the study participants also know that comprehensive IT security requires a combination of technical solutions, threat intelligence services and general awareness of all employees.

Technical solutions as a foundation

The foundation of a comprehensive CyberSecurity strategy is a technical solution to defend against attacks. In fact, 44% state that their company is evaluating the current IT security solution and/or looking for a new solution. Furthermore, all respondents already rely on multi-layered technical solutions: a large amount of respondents (58%) have engaged external IT security service providers, including threat intelligence services, and more than half (58%) use preventive tools and expertise internally to detect and analyse cyber-threats.

Almost two thirds (65%) use dedicated security tools or services to protect cloud software and activities, whereas 54% work with network segmentation and 44% operate their own security operations centre (SOC). Just over half (54%) state that their company uses security information and event management (SIEM).

Employee training as a complement to CyberSecurity

A worrying percentage of respondents (70%) all agreed that increased regulation heightens the risk of non-compliance, making employees one of the weakest links in the security perimeter of the financial organisation. This view seems to be shared by IT professionals (81%) and the C-Suite (65%), followed by IT security professionals (56%). With high degrees of bureaucracy and compliance as part of the financial services sector, regular employee training seems to be an important complement to technological protection solutions.

However, this doesn't seem to resonate with our respondents: in just 24% of the organisations are all of the C-Suite are regularly trained on security topics and procedures. The IT department, on the other hand, seems to be doing slightly better, with 37% of organisations training the entire staff. In the remaining departments surveyed (for example, executive assistants, marketing, analysts and traders, accounting), results are less promising: just over one in 10 (between 15% and 10% depending on the function) state that their department is fully trained on CyberSecurity, therefore increasing the risk of incoming threats.

Threat intelligence rounds out the security approach

Companies in the financial sector almost universally use threat intelligence services, as the Kaspersky study shows. Almost all respondents (99%) use at least one such service. However, not all companies rely on the services they would like to use. For example, 43% of participants say that their company uses APT reports to keep up to date with the latest investigations, threat campaigns and techniques used by APT actors. A further 28% would like to see the use of such reports.

Over one-third (36%) use threat data feeds and threat data look-up to improve incident response, with a similar number (34% of those surveyed) saying they would like to use this tool in the future. Malware analyses are used by almost half (44%) of the financial institutions, 26% would like to use them. More than a third (39%) report that their organisation uses security assessments, for example via the TIBER framework (Threat Intelligence-based Ethical Red Teaming), as well as tools to detect targeted attacks (43%).

"Gartner defines threat intelligence as a key aspect of an enterprise security architecture that helps technical security and risk management professionals detect, segment and accurately investigate threats. Today, a reactive approach to CyberSecurity is simply not enough. Quality threat intelligence must include a number of features. These include - firstly - extensive context that creates actionable intelligence from data and adds value; and - secondly - support from a recognised team of experts with proven experience in uncovering complex threats. Thirdly, there needs to be a smooth integration of the services into a company's existing security processes. Good threat intelligence frees up internal CyberSecurity departments to focus on higher priority objectives."

David Emm,
Principal Security Researcher
Kaspersky