White Paper

Bitdefender®

Top Security Challenges for the Financial Services Industry in 2018

Author: Luana PASCU

Key Findings

- **Lack of specialists, tools, budget and knowledge are the main roadblocks for financial sector**, shows a Bitdefender survey over 118 companies. 118 IT security purchase professionals from large companies in the US and Europe, are providing worrying details of how difficult it is to cover security of operations.
- 47.5% of financial institutions were breached in the past year
- 58.5% of financial institutions have experienced an advanced attack or seen signs of suspicious behavior in their infrastructure.
- 83.9% of surveyed execs think **EDR-like tools are a solid solution in preventing attacks**.

How Well Is the Financial Services Industry Doing on Security?

Healthcare, manufacturing and financial services have one thing in common: they are the three most-targeted industries in 2018. Not only do they provide access to reams of data, but the sectors are also critical to society. So, if hackers want to seriously do harm, they can go after either of these sectors to succeed. Companies in the financial services sector manage money, covering banking, offshore financial operations, stock brokers, credit card vendors, insurance companies and investment funds. For a clear example of the mayhem a data breach in this area can lead to, let's just say it will take a while before anyone forgets the notorious Equifax breach from 2017.

To ensure success, hackers have developed attack strategies to target particular companies in the financial services industry. In fact, research shows that the number of **security incidents in this sector has tripled in the past five years**, and the containment cost has increased by 9.6 percent. Denial of service, social engineering, drive-by downloads and phishing to disseminate banking Trojans, and malicious insiders remain the most prevalent attack strategies, the study says.

Malware authors often resort to social engineering to inject financial malware to ultimately empty accounts, and they use businesses to reach the end user. By showing how easy it is to go after their customers, hackers reveal the dire need for security in the financial services sector. Financial malware, developed to pilfer financial information, usually flies under the radar, operating undetected until it's too late. Multiple sophisticated malware variants mainly target banks, but that doesn't mean other businesses in this field should rest on their laurels. Besides making off with money, hackers can do so much more with the data stolen. For example, they can sell the data on the dark web.

This is not a new threat, as sophisticated banking Trojans go back to even 2007 when Zeus was first detected. Zeus was already a tough, complex malware exploit kit and, when the code somehow leaked, it was further developed into other sophisticated banking Trojans such as Terdot, Atmos and Citadel. "Even if Terdot is technically a Banker Trojan, its capabilities go way beyond its primary purpose: it can also eavesdrop on and modify traffic on most social media and email platforms," say Bitdefender researchers Bogdan Botezatu and Eduard Budaca. "Its automatic update capabilities allow it to download and execute any files when requested by its operator, meaning it can develop new capabilities." Terdot, a sophisticated threat that went after financial institutions in the UK, Germany, US, Australia and Canada, was detected by Bitdefender. The full technical analysis can be read on Bitdefender Labs.

If, in the past, financial companies thought they could get away with mediocre security strategies or even without properly investing in cybersecurity, recent bank stings have proven them wrong. Banking Trojan malware schemes have been in the spotlight in the past because they were large-scale campaigns that drained accounts worth millions of dollars. Whether they use keylogging to steal bank account credentials and payment information or inject code to corrupt baking sites for man-in-the-middle attacks, cybercriminals actively use targeted attacks to go after financial institutions.

Much of the trade media has focused on Lazarus, the state-sponsored cybercriminal gang allegedly from North Korea. Some researchers believe they are responsible for the **illegal SWIFT transactions that transferred $13.5 million** from an Indian 112 year-old bank to other accounts in Hong Kong, as part of a two stage heist in August 2017. This is however only speculation and too early to determine.

And banking malware keeps on spreading. Earlier this year, researchers from IBM detected the BlackSwap banking malware that targeted Polish and Spanish banks, and is believed to be a test campaign preparing for a large-scale attack in Q4 of 2018. Similarly, CamuBot malware that went after Brazilian banks is also believed to be a small piece of a larger puzzle, while Mexican banks were also actively targeted earlier this year, losing $15.4 million in illicit transfers to fraudulent accounts and cash withdrawals.

Bitdefender has investigated a number of advanced spear phishing attacks targeting employees of financial institutions in Eastern Europe and Russia. Bitdefender researchers found evidence that may link this activity to the Carbanak cybercriminal gang that has targeted over 100 institutions from more than 40 countries in the past five years. The group deployed fileless attack techniques and has generated a financial loss of over EUR 1 billion.

Third-Party Risks are the Main Cause of Data Breaches in the Financial Sector

Financial crimes are still as popular as in the Wild West, when robbers limited themselves to the good-old fashioned bank. But, in today's climate, businesses are struggling to fight off sophisticated attacks launched by cybercriminals who constantly improve their techniques. DDoS, social engineering, spear-phishing, ransomware and insider threats are among the most widespread techniques used against not only traditional banking infrastructures, but also digital banks, cryptocurrency exchanges, credit reporting agencies and venture capital, and others.

Cybercriminal gangs going after the financial services industry have developed sophisticated schemes such as ATM malware, card fraud and bank domain hijacking to drain accounts or shut down operations. Their schemes don't resort to tricking customers into using fake platforms that would infect them with malware or giving away their personal data. Nation-state sponsored actors such as North Korean Lazarus group have actively targeted SWIFT systems since 2015 by exploiting bank vulnerabilities.

SWIFT banking attacks have grown in complexity over the years and led to the theft of millions of dollars. They have operated by deploying malware to bypass security and steal genuine SWIFT credentials. They used them to manipulate banks to transfer funds to the group's accounts. Their first victims were a Vietnamese bank and the central bank of Bangladesh, the latter losing $101 million in the heist. And that was only their warmup. Ecuador's Banco del Austro followed and hackers made off with $12 million. In the past three years, Lazarus deployed the same operation mode and robbed banks from a number of countries in Europe, Asia, Latin America and Oceania.

The notorious hacking group The Shadow Brokers leaked NSA hacking tools and exploits, including "a working directory of an NSA analyst breaking into the SWIFT banking network" dating from 2013. "The SWIFT documents are records of an NSA operation, and the other posted files demonstrate that the NSA is hoarding vulnerabilities for attack rather than helping fix them and improve all of our security," wrote The Atlantic in early 2017, associating the attacks with state-sponsored operations.

Fintech in areas such as cryptocurrency, Revolut and banking transactions via Facebook Messenger or WhatsApp, has been gaining popularity, especially in developing countries, creating a new threat landscape. Fintech integration raises many security concerns, because the firms in the sector are third parties that operate with sensitive customer data on a daily basis. At any given time, if their infrastructures have exploitable vulnerabilities and are not secured properly, they could leak millions of customer records – not only payment card data, but also addresses, emails and social security numbers.

Financial institutions in the UK, for example, are in the dark when it comes to third-party risks of open banking. Open banking allows developers access to the company's network to create applications that may have security vulnerabilities. Research shows that 72 percent of financial services companies in the UK were hacked in the past year, possibly due to third-party vulnerabilities, while 69 percent blamed them on insider threats.

Third parties, such as vendors, pose serious risks for financial services, even though researchers found that 48 percent of respondents say they have complete faith in the third-party vendors they work with.

Internal security is not enough, and unfortunately too many CISOs forget external factors they can't control. Many data breaches are caused by third-party risks and, for the financial services sector, any security gap is critical, especially if it involves point-of-

sale or payment operations. Distrust in company, business disruption and customer data on sale on the dark web are among damages caused by vulnerable third parties. The financial sector works with sensitive information daily, and is currently working on integration with fintech, such as open banking, digital banks and mobile payments, posing a risk if their security is poor. Because they have access to the computer systems and customer information, they automatically facilitate hacker access.

Similarly to the Bangladesh Bank heist of 2016 when hackers manipulated the SWIFT system, third-party risks are what led in 2018 to a wave of cyberattacks launched against five Mexican financial groups. Cybercriminals also abused Mexico's SPEI (Interbank Electronic Payment System) – a local version of SWIFT – and made unauthorized transfers of funds to fake accounts by manipulating the (third-party) system that connected the financial groups to the payment system. They got away with $15.33 million from three banks, a broker and a credit union. After the heist, financial authorities in Mexico issued an alert urging financial groups to strengthen security.

The Cost of a Security Breach and How Financial Services Deal with Attacks

What is the actual cost of breaches in this sector and what kind of measures do CISOs leading financial services institutions take to ensure proper cyber defense, data security and prevent business disruption?

Data breaches are nothing to joke about, especially when hackers actively target critical industries and infrastructures. Some of the most targeted organizations are those in the financial sector. As stated in a report by Generali Global Assistance (GGA) and Identity Theft Resource Center (ITRC), **8.5 percent of the total of 1,579 data breaches in 2017 in the US affected financial services** businesses such as credit unions, banks and pension funds. In 2017, data breaches increased by 44.7 percent, while "**financial services firms fall victim to cybersecurity attacks 300 times more frequently than businesses in other industries**," states the report.

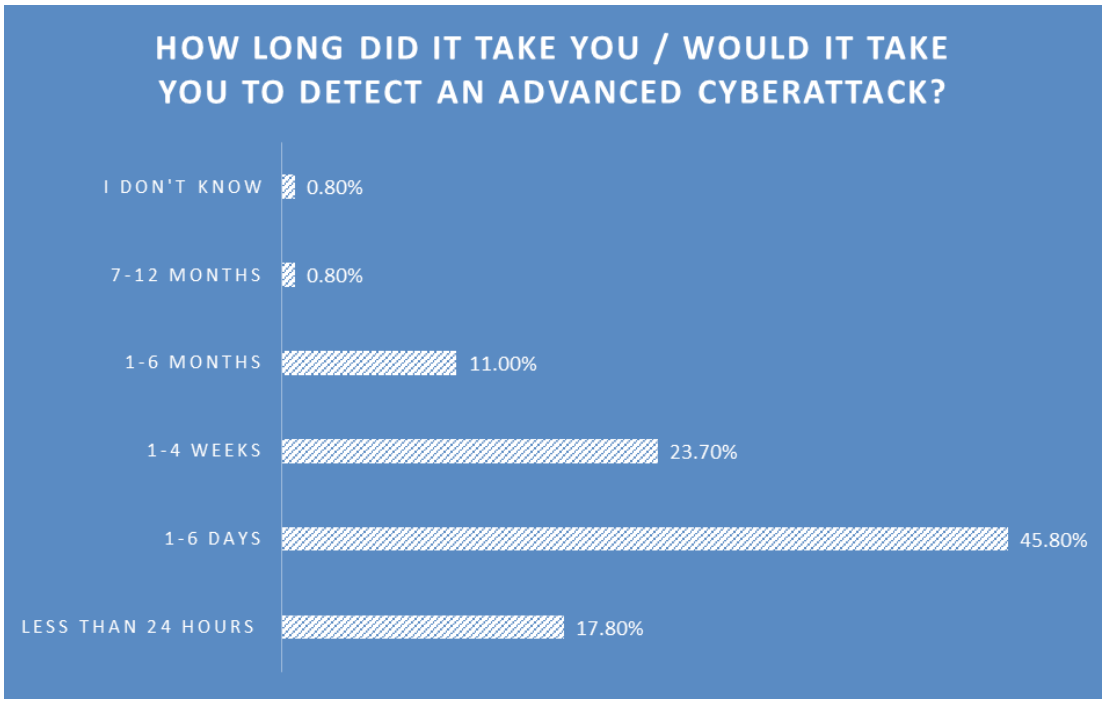
The financial services sector currently spends as much as 40 percent more on breach containment and detection than it did three years ago, Accenture found, making it easily "the highest cost of cybercrime" in comparison with other industries. Financial services companies are severely impacted by business disruption and information loss, which end up draining the mitigation budget.

Financial services firms deal with high volumes of critical data. Cybercriminals move fast, knowing that access to this information is a gold mine, as they can sell it to the highest bidder on the dark web, or even use it themselves for fraud and other illegal endeavors. Naturally, this raises mitigation costs. The **data breach recovery cost is higher for financial institutions**, and considering **all-industry US companies spent $7.35 million per breach last year** according to the global overview report from IBM and the Ponemon Institute, these organizations are in for some dramatic numbers.

Enterprises that can successfully contain breaches in less than a month could save significantly, especially in the healthcare and financial services sector. The longer it takes to contain a breach, the more a company has to lose in terms of revenue, reputation and customer trust.

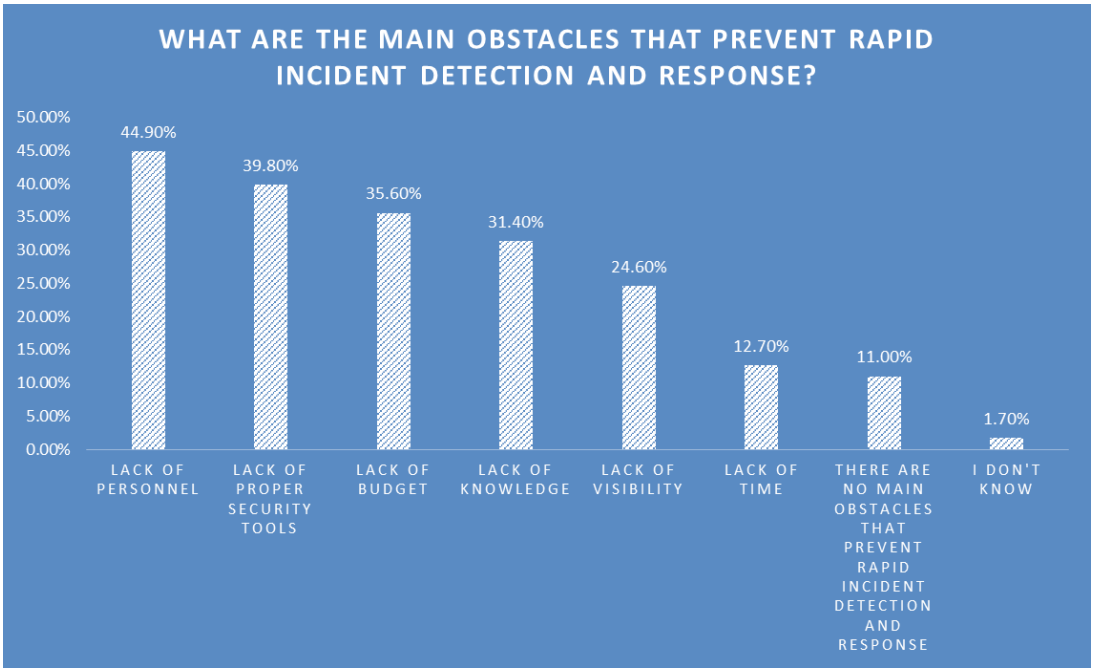
According to a Bitdefender survey of financial institutions in February and March 2018, **17.8 percent of respondents say it takes them less than 24 hours to detect an advanced cyberattack**. Most companies, **45.8 percent, say their company detects an attack in 1 to 6 days**, while 23.7 percent said they need about 1 to 4 weeks, 11 percent take about 1 to 6 months and 0.8 percent take between 7 to 12 months to detect an advanced cyberattack.

Figure 1: Advanced cyberattack detection time



Among **main obstacles that prevent rapid incident detection and response** are the **lack of: personnel** (44.9%), **proper security tools** (39.8%), **budget** (35.6%), **knowledge** (31.4%), **visibility** (24.6%) and **time** (12.7%). 11 percent of CISOs say there are no main obstacles that prevent rapid incident detection and response.

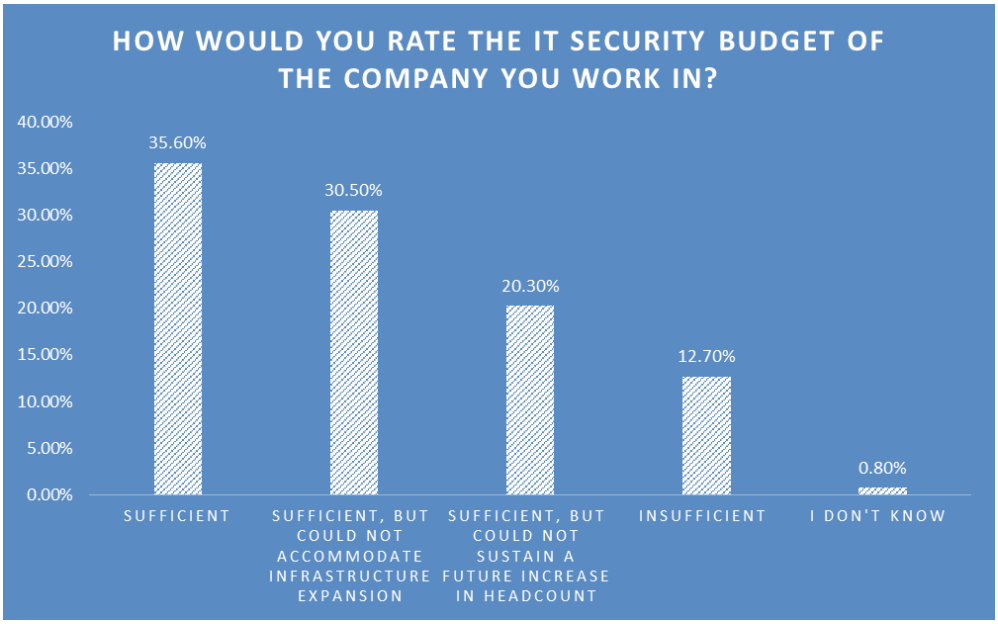
Figure 2: Main detection and response obstacles



In spite of shortcomings, CISOs are **struggling to develop a proper risk mitigation strategy** to block unauthorized activity in their infrastructure. Security experts have been encouraging critical industries, such as the finance sector, to increase budgets to make urgent investments in cybersecurity strategies that concentrate on emerging threats and vulnerabilities, and to purchase cybersecurity insurance and deploy multi-level security.

In spite of this, businesses in the financial sector still do not invest heavily in IT security and are comfortable with current funding levels, found Bitdefender. As many as **35.6 percent of CISOs say the IT security budget of the company they work for is sufficient**, while 30.5 percent consider it enough, but mention that it could not accommodate infrastructure expansion. 20.3 percent say their IT security budget is sufficient, but can't sustain a future increase in headcount. Only 12.7 percent consider their budget insufficient.

Figure 3: Security budget rate



Critical industries still fall victim to ransomware and social engineering schemes, the oldest tricks in the book. Considering how fast the threat landscape is evolving, it might be difficult to actually address all threats and prevent breaches 100%, but **some companies are breached more than once a year because they don't properly document previous attack methods and hackers regularly step up their game.**

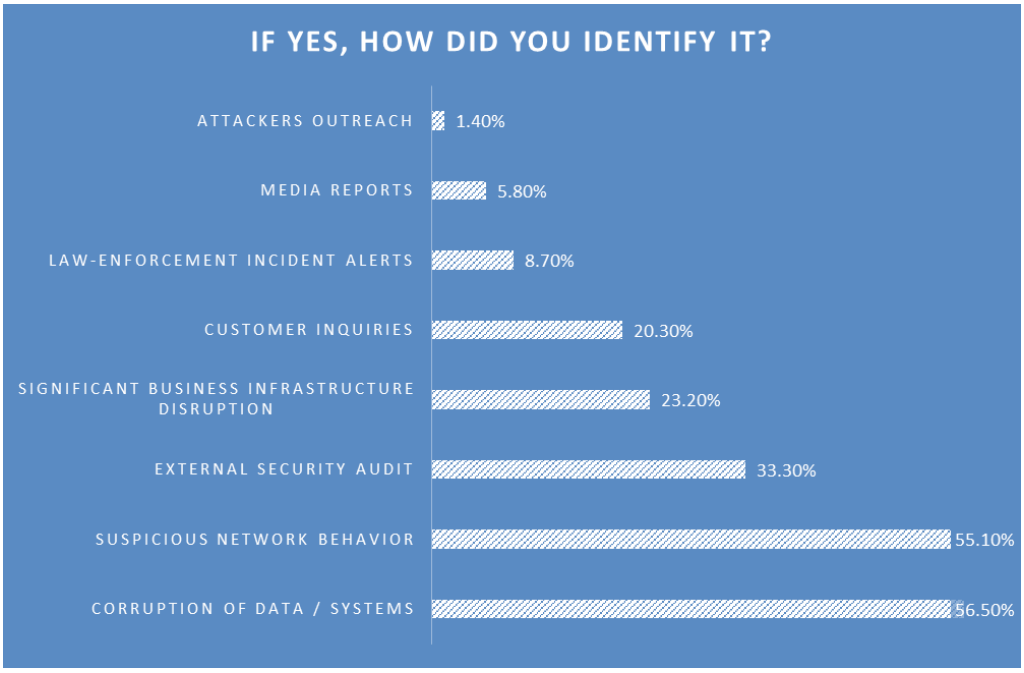
According to Bitdefender, **47.5 percent of financial institutions confirm they were breached in the past year**, while 50 percent say they did not experience a security breach, and 2.5 percent don't know. On a positive note, **94.6 percent of the companies that were hacked know why this happened**.

Figure 4: Company breaches per country

	UK	US	Germany	France	Italy	Sweden	Denmark
No	48%	76.90%	41.20%	47.80%	36.40%	9.10%	80%
Yes	48%	19.20%	58.80%	52.20%	63.60%	81.80%	20%
Don't know	4%	3.80%	0	0	0	9.10%	0

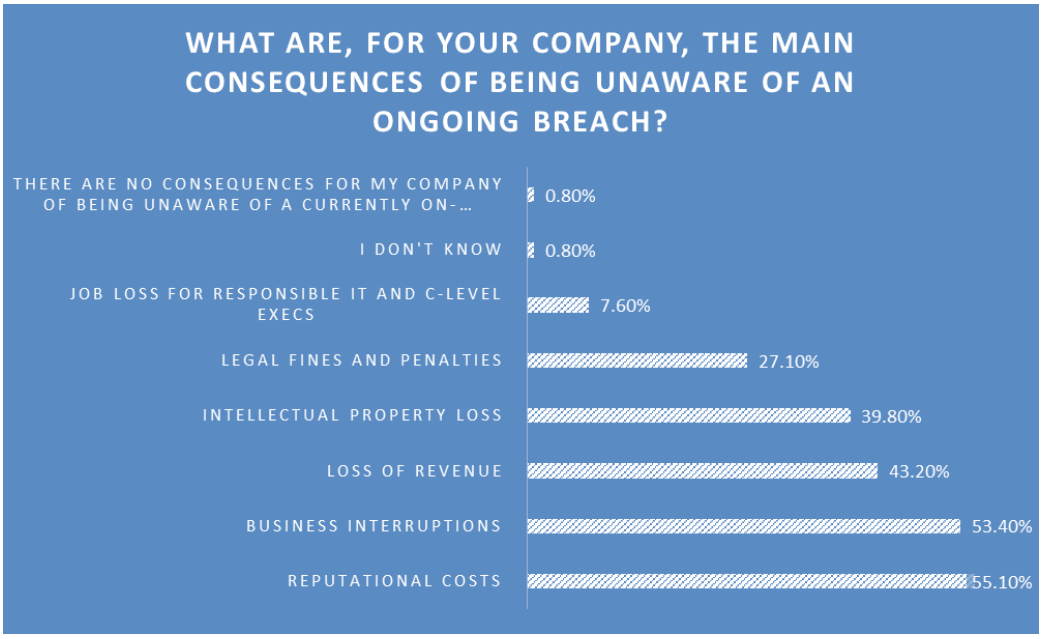
58.5 percent of financial institutions have experienced an advanced attack or malware outbreak, or have seen signs of suspicious behavior. The financial institutions that experienced an advanced attack or malware outbreak, or have seen signs of suspicious behavior, detected it by noticing a **corruption of data/systems** (56.5%), **suspicious network behavior** (55.2%), **through an external security audit** (33.3%), **significant business infrastructure disruption** (23.2%), **customer inquiries** (20.3%), **law enforcement incident alerts** (8.7%), **media reports** (5.8%) and **attackers' outreach** (1.4%).

Figure 5: Advanced attack or malware outbreak detection



The main consequences of not knowing that a breach is taking place are **reputational costs** (55.1%), **business interruptions** (53.4%), **revenue loss** (43.2%), **intellectual property loss** (39.8%), **legal fines and penalties** (27.1%) and **job loss for responsible IT and C-level execs** (7.6%).

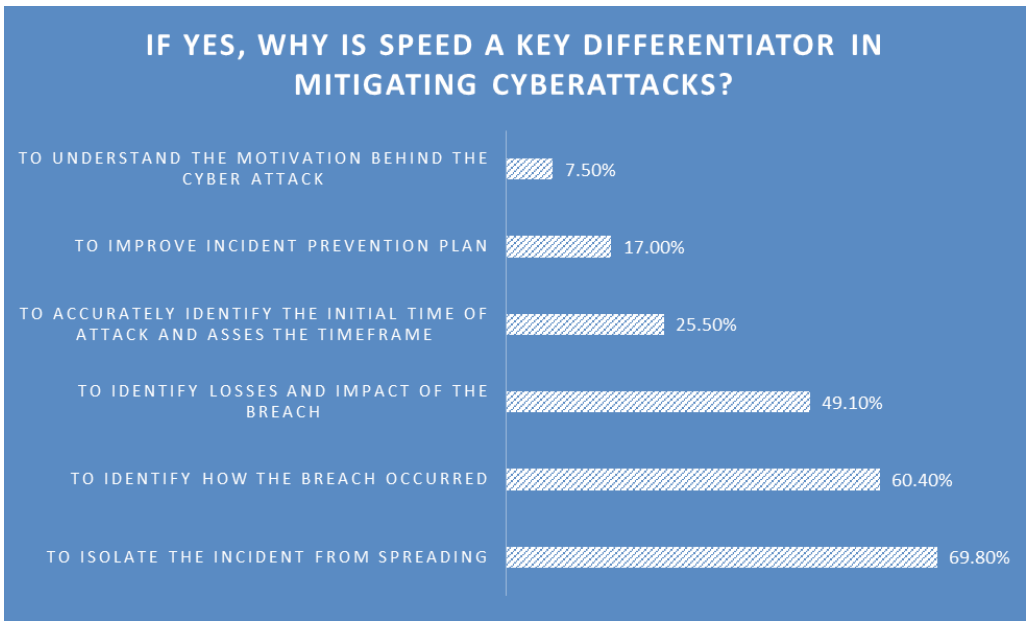
Figure 6: Consequences of unknown ongoing breaches



Overall, **70.3 percent of executives in the financial services sector have a dedicated IT security budget for incident investigation and forensic (EDR)**, and 89.8 percent believe **reaction time** is a key differentiator in mitigating cyberattacks.

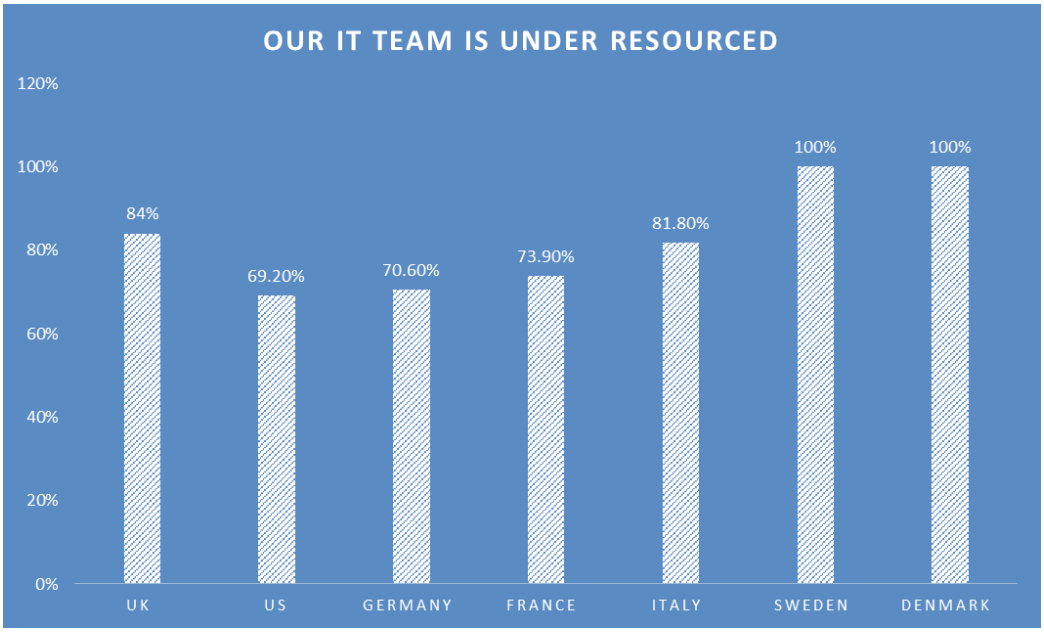
Speed is another key differentiator in mitigating cyberattacks because it's important to isolate the incident from spreading (69.8%), to **identify how the breach occurred** (60.4%), to **identify losses and impact** of the breach (49.1%), to accurately **identify the initial time of attack and asses the timeframe** (25.5%), to **improve incident prevention plan** (17%) and to **understand the motivation behind the cyberattack** (7.5%).

Figure 7: Speed as a key differentiator in attack mitigation



The **cybersecurity skill shortage** affects CISOs' plans to develop a proper containment and mitigation strategy, Bitdefender found. **78.8 percent of IT executives say their IT security team is majorly under resourced**. The **countries where insufficient resources are a top struggle include Sweden (100%) and Denmark (100%)**, followed by the UK, where 84 percent said they are dealing with an under-resourced team, then Italy (81.8%), France (73.9%), Germany (70.6%) and the US (69.2%).

Figure 8: Insufficient resources per country

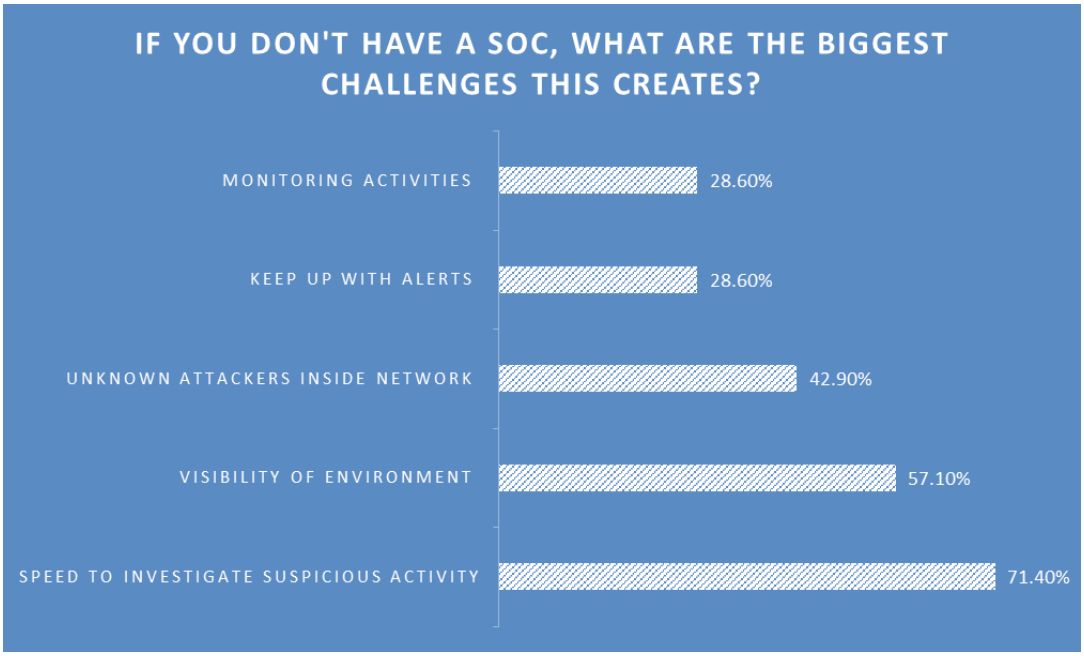


When asked about the **global cyber skills deficit**, as many as 72.9 percent say their company is **affected in a negative way**, while only 25.4 percent believe their business has not been affected.

Security Operations Centers (SOC) are teams of IT security specialists that deal with security incidents. Fortunately, **94.1 percent of respondents confirmed having a SOC**, while only 5.9 percent have not yet created such a team. All respondents from Germany, Italy and Sweden have Security Operations Centers in place.

For respondents who **don't have a SOC,** some of the **biggest challenges** are speed to investigate suspicious activity (71.4%), visibility of environment (57.1%), unknown attackers inside network (42.9%), keeping up with alerts (28.6%) and monitoring activities (28.6%).

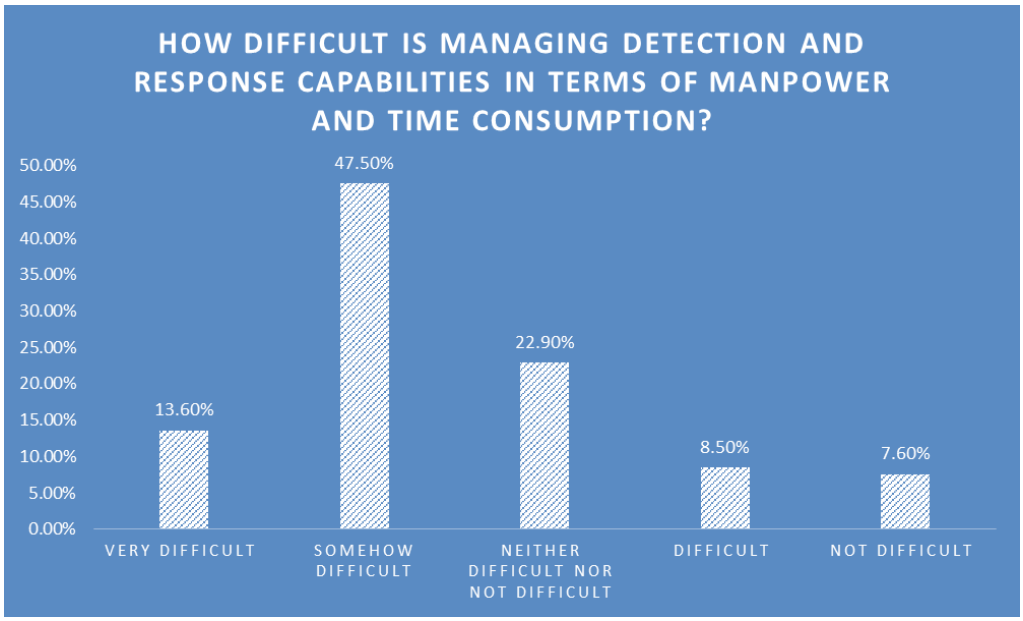
Figure 9: Lack of SOC challenges



Managing detection and response capabilities in terms of manpower and time consumption is considered very difficult by 13.6 percent of respondents, while 47.5 percent find it somehow difficult, 22.9 percent say it is neither difficult nor not difficult, and 8.5

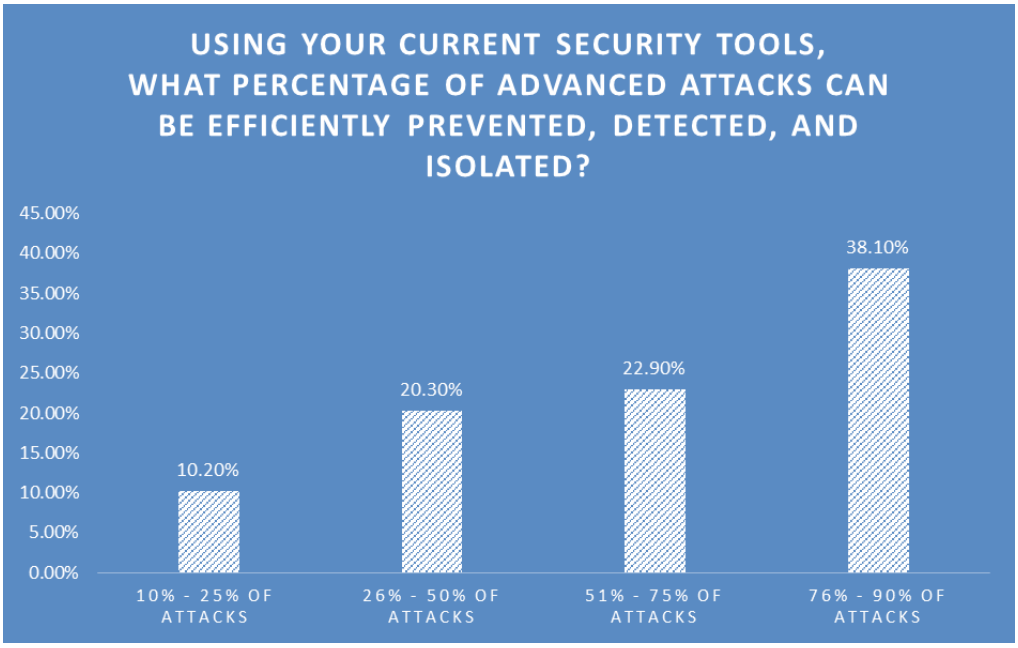
percent say it is difficult. Only 7.6 percent don't think it's difficult.

Figure 10: Difficulty level of detection management and response capabilities



38.1 percent **trust their current security tools** with which they can **efficiently prevent, detect and isolate between 76% and 90% of advanced attacks**.

Figure 11: Detection percentage of current security tools

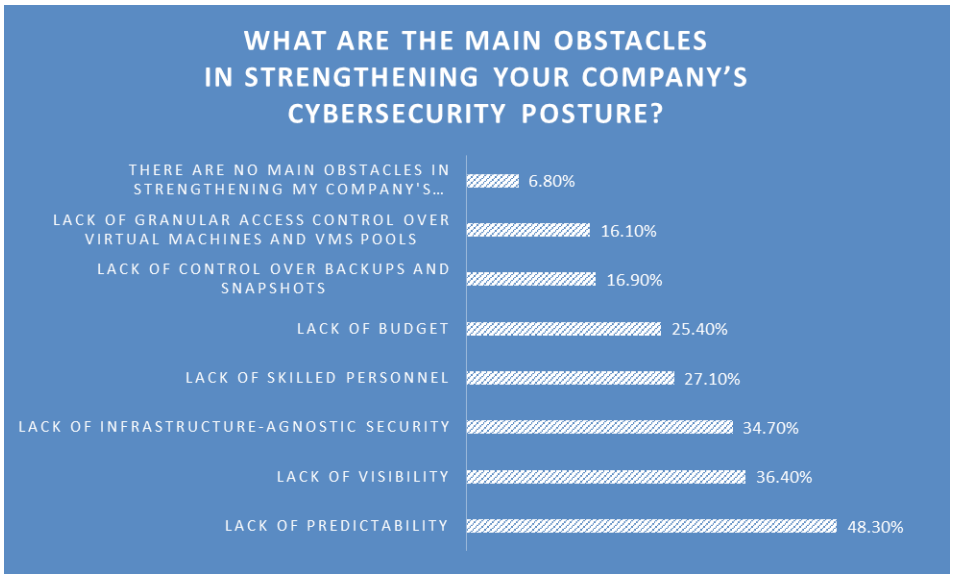


83.9 percent think forensic capabilities and visibility tools **(EDR) help prevent future attacks**. **In addition to preventive security controls like traditional security solutions and Firewall, 86.4 percent also have security tools, processes and staff to detect and respond to advanced attacks.** 66.7 percent use in-house security tools, processes and staff to detect and respond to advanced attacks, while **33.3 percent outsource** these functions.

Of the 12.7 percent that do not yet have the security tools, processes and staff to detect and respond to advanced attacks, 40 percent plan to outsource it, 33.3 percent will do it in-house, 13.3 percent don't know how to go about it and 13.3 percent have no plans yet.

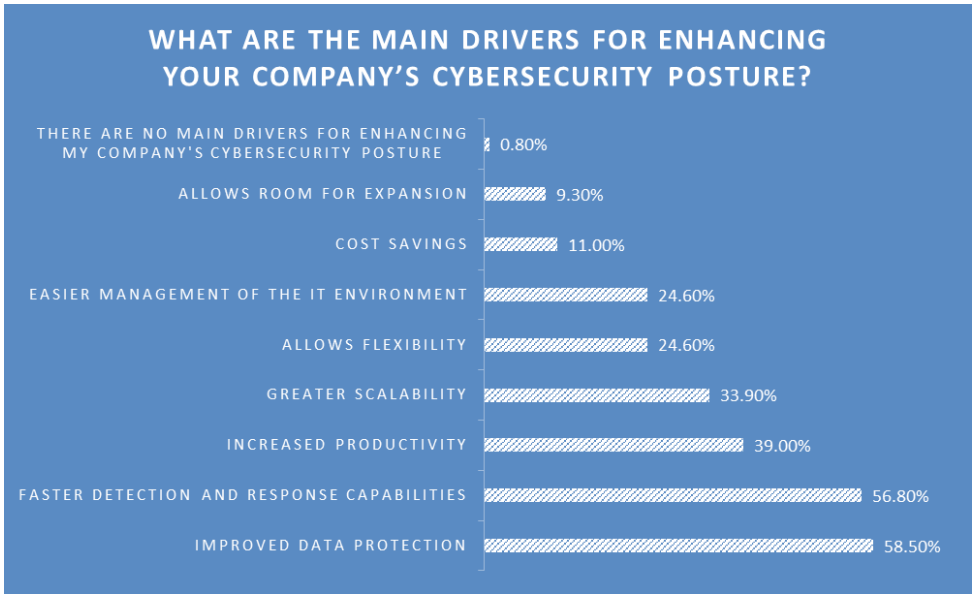
The main obstacles in strengthening their company's cybersecurity posture are a **lack of: predictability** (48.3%), **visibility** (36.4%), **infrastructure-agnostic security** (34.7%), **skilled personnel** (27.1%), **budget** (25.4%), **control over backups and snapshots** (16.9%) and **granular access control over virtual machines and VMs pools** (16.1%). 6.8 percent feel there are no main obstacles to strengthening their company's cybersecurity posture.

Figure 12: Obstacles in strengthening cybersecurity posture



For the financial industry, **the main drivers for enhancing the company's cybersecurity posture** are improved data protection (58.5%), faster detection and response capabilities (56.8%), increased productivity (39%), greater scalability (33.9%), allows flexibility (24.6%), easier management of the IT environment (24.6%), cost savings (11%) and room for expansion (9.3%).

Figure 13: Main drivers to enhance cybersecurity posture

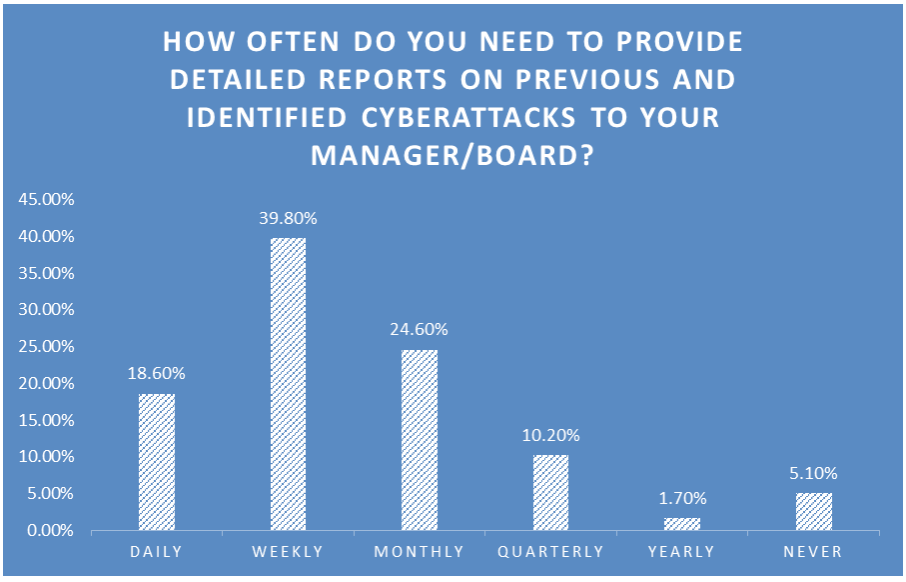


According to CISOs in the financial sector, **the best security defense approach against advanced attacks in their organization are next-generation security (endpoint detection and response capabilities) (67.8%),** security audits (46.6%), traditional security (antimalware and endpoint protection solutions) (41.5%), layered security (24.6%), log monitoring (22.9%) and cybersecurity trainings (22%).

Figure 14: The best security defense approach

18.6 percent of respondents are asked to provide **detailed reports on previous and identified cyberattacks to their manager/board on a daily basis**. **39.8 percent report on a weekly basis**, 24.6 percent report monthly, 10.2 percent quarterly and 1.7 percent yearly. 5.1 percent never prepare reports.

Figure 15: Detailed report rate to upper management



82.2 percent feel that, **to become GDPR-compliant, in-depth security incident reports provided by EDR solutions will be needed for future cyberattacks**. 15.3 percent don't think this is the case.

The survey of financial institutions, conducted in February-March 2018 by Censuswide for Bitdefender, included 118 IT security purchase professionals from large organizations with 1,000+ PCs and data centers, based in the US and Europe.

What Measures Can Financial Services CISOs Take to Ensure Network Safety?

To safeguard their networks, CISOs need to adapt security policies to the constant fluctuations of the security landscape or face reputational damage, revenue loss and even fines for failing to protect consumer data privacy. Online transactions are at the core of business models in financial institutions, so cybercriminals will try to hijack the systems to intercept data and use it in illicit activities such as financial fraud. The internet is critical for this industry – any disruption of service would cause operation shutdown and the business could lose revenue.

To begin with, to respond to internal threats, CISOs should look into training their employees about security threats, social engineering and the risks of bringing their own devices to work. Attacks are more complex by the minute, hackers are improving their strategies by coming up with new attack methods and more sophisticated and stealth APTs, so keeping up with the threat landscape could turn out to be a real challenge for some IT executives. Because companies still take long in detecting breaches, by detection time, the sensitive data will have already been exposed and company affected.

When it comes to protecting critical assets and mitigating risks, regular security upgrades must be performed, as well as looking into recurrent threats such as third parties, which may call for significant budget and team increases. Systems need a key defense at the hypervisor level to fend off attacks, and this can be achieved through multiple lines of defense that can eliminate blind spots and provide advanced threat protection. Additional layers of protection can ensure optimal infrastructure protection by increasing infrastructure visibility and stopping attacks before they even take place, without affecting system performance.

Besides maintaining control of the situation and doing their best to stay ahead of threats, financial organizations also have to adhere to industry standards and ensure regulatory compliance. The Economic Growth, Regulatory Relief, and Consumer Protection Act, also known as Dodd-Frank Repeal, signed by US President Donald Trump earlier this year, the European Union's GDPR (General Data Protection Regulation), PSD2 (Payment Services Directive 2), the PCI DSS 3.2 (Payment Card Industry Data Security Standard) and a number of other often clashing regional regulations target the financial industry, making compliance tough and guidelines unclear. These protocols, however, might help in protecting critical frameworks.

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers. More information is available at http://www.bitdefender.com/.

BD-Business-Oct.10.2018-TK#: 70585