Paper

Bitdefender®

Companies blame competition for corporate cyberespionage

(A survey of US, UK, French, German, Italian, Swedish and Danish IT execs)

Executive summary

In the past year, top corporations suffered an increase in security incidents and breaches, with a significant rise in documented advanced persistent threats (APTs) and targeted attacks aimed at both companies and government entities (such as APT-28 and, just recently, Netrepser).

APTs are complex cyber tools crafted for high-profile entities that operate by silently gathering sensitive data over long periods. This type of attack is intended to exfiltrate sensitive data or silently cripple industrial processes. In this context, concerns for security are rising to the top, with decisions taken at the board level in most companies.

When pointing fingers, CISOs perceive competitors as the main interested party that would target their organisations for corporate or industrial espionage (61 percent). Hacktivists come second at 56 percent and foreign state-sponsored attackers third, at 48 percent.

These findings are revealed in a survey released today by security firm Bitdefender. The study explores, in detail, the pressures advanced persistent threats (APTs) place on 1,051 IT security professionals from large enterprises with 1,000+ PCs and data centers, based in the US, the UK, France, Italy, Sweden, Denmark and Germany.

Both IT decision makers and CEOs are concerned about security, not only because of the cost of a breach (stock price decrease / business interruption / unavailable resources / direct financial losses), but also because the reputation of their companies is at risk when customer data is lost or exposed to criminals.

On top of this, migrating corporate information from traditional data centers to a cloud infrastructure has significantly increased companies' attackable surface, creating new threats and more worries to CISO offices regarding the safety of their data.

A small minority are not concerned with APTs

More than half (58 percent) of IT security decision makers say their companies could 'definitely' be targeted by cyberespionage campaigns using advanced persistent threats (APTs). Another 36 percent of respondents say their IT infrastructure could 'possibly' be targeted in high-level cyberespionage actions that exfiltrate intelligence systematically. Less than 4 percent of IT decision makers say APTs are not a real concern in their working environment.

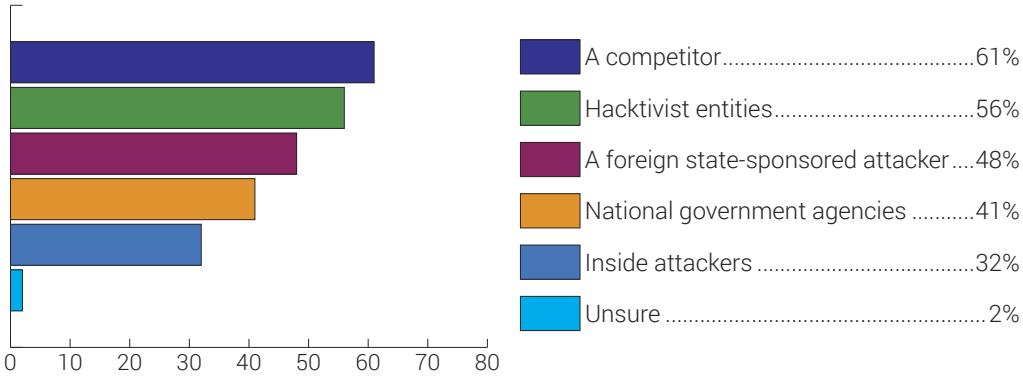
Most advanced persistent threats are not limited to state-sponsored attacks, as enterprises can also fall victim to attackers that exploit zero-day vulnerabilities to install highly targeted malware to spy on companies and steal intellectual property.

Bitdefender's survey confirms that competitors, hacktivist entities, foreign state-sponsored attackers, and national government agencies could target organizations with advanced attacks.

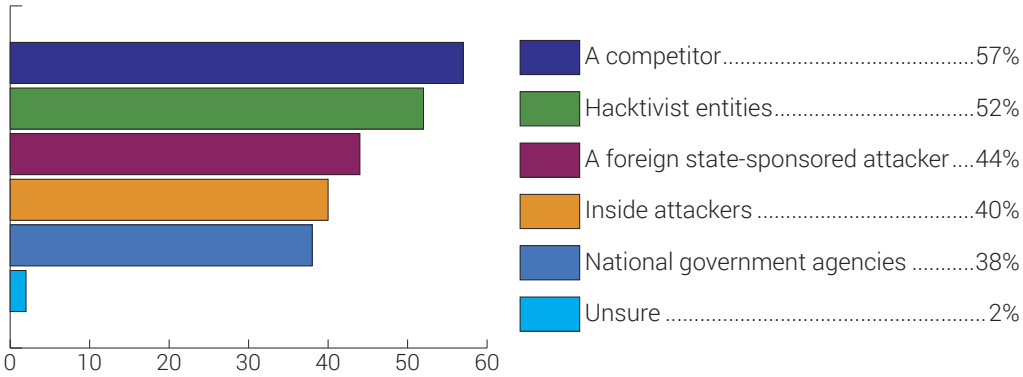
German and French companies fear competitors more than companies in the other countries surveyed, while the Danes are the only respondents to say they could be targeted by hacktivist entities most. National government agencies could be behind an APT according to 58 percent of the Swedish IT execs (far more than the global average), while foreign state-sponsored attackers are mostly blamed by respondents in Sweden (55 percent) and France (51 percent). Inside attackers were mentioned most by US respondents, with one in four saying a targeted attack would involve the complicity of an existing or former employee.

CHART 1

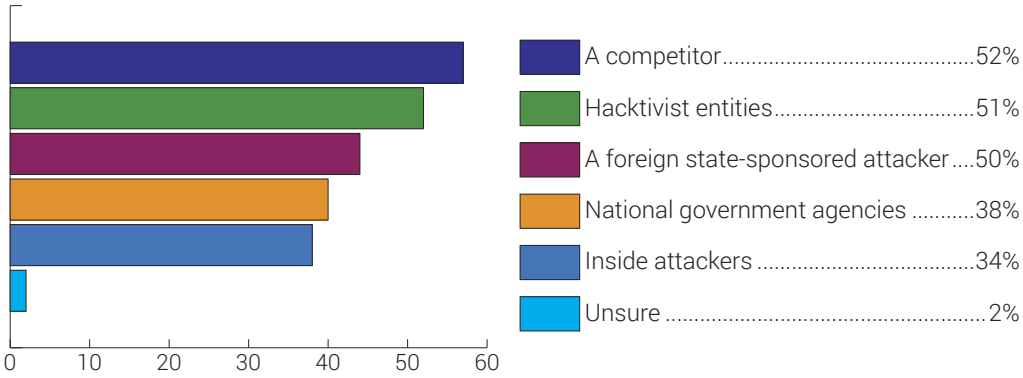
Who do you think could target your organization with an advanced persistent threat? (global results - %)



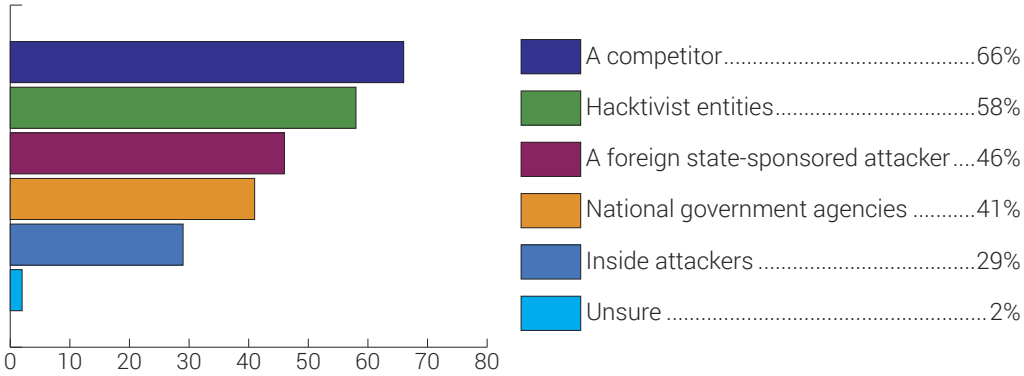
United States of America



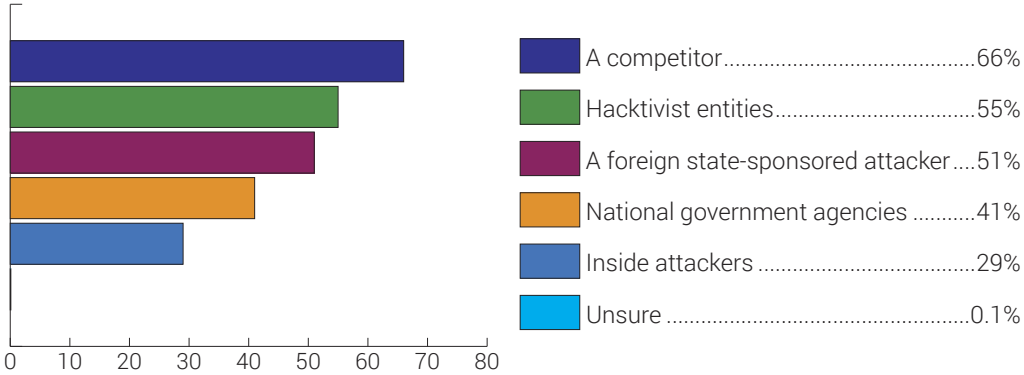
United Kingdom



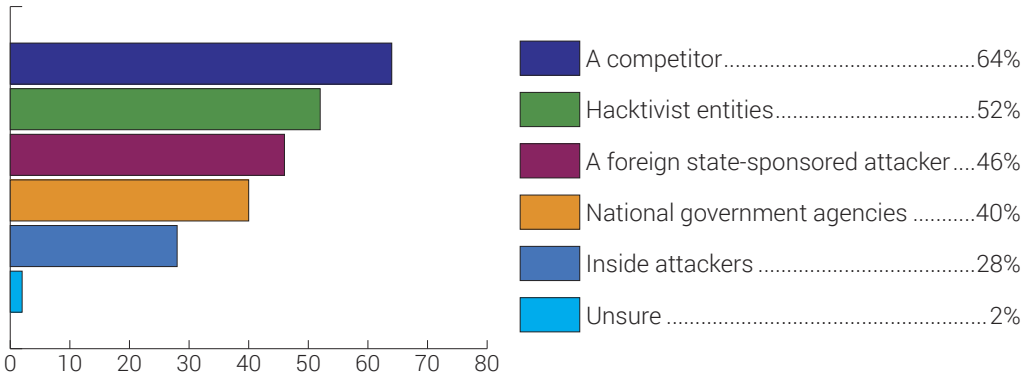
Germany



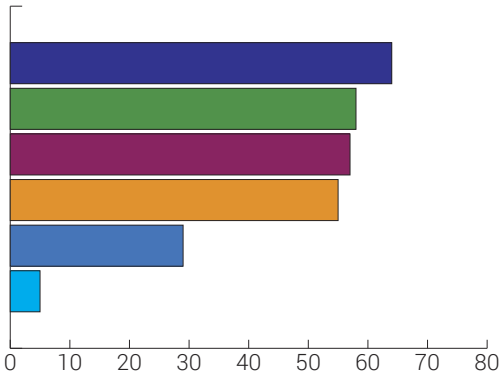
France



Italy

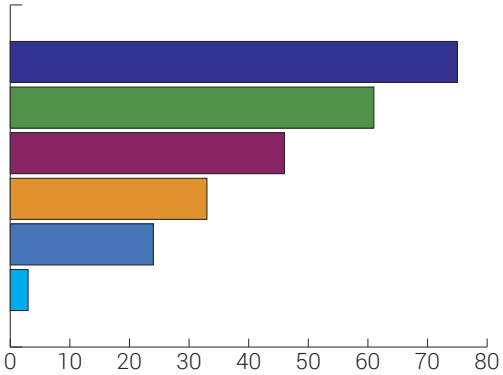


Sweden



- A competitor.....64%
- National government agencies 58%
- Hacktivist entities.....57%
- A foreign state-sponsored attacker....55%
- Inside attackers 29%
- Unsure 5%

Denmark



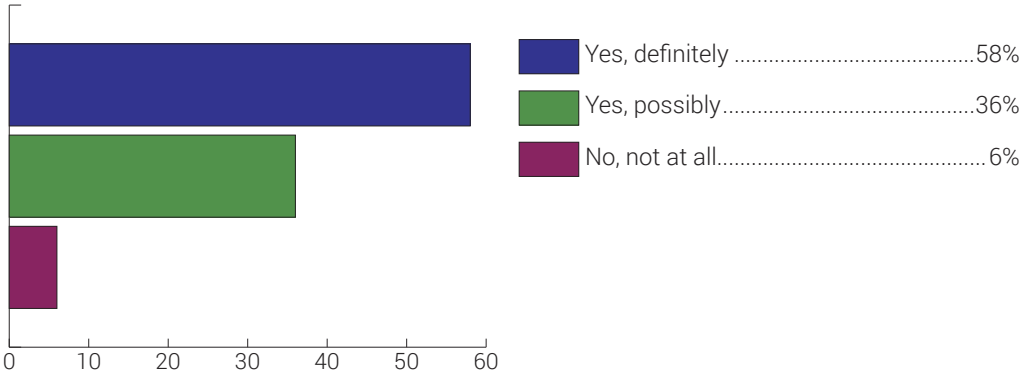
- Hacktivist entities.....75%
- A competitor.....61%
- A foreign state-sponsored attacker....46%
- National government agencies 33%
- Inside attackers 24%
- Unsure 3%

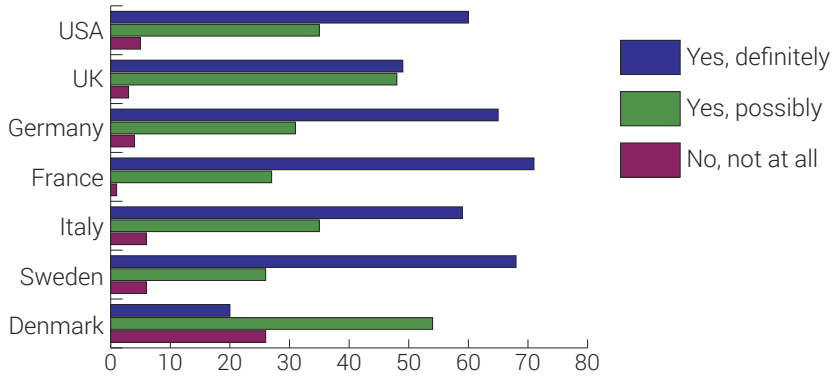
Targeted attacks impact decisions at the board level

French, Swedish and German IT execs fear APTs most (with far more positive responses than the global average). In contrast, only 20 percent of Danish respondents say they could "definitely" be a target and 26 percent even say it's not a possibility. UK respondents are the most uncertain, with 48 percent of them saying they could "***possibly***" be hit by a targeted attack.

CHART 2

Do you think your organization could be a target of an APT? (global results - %)





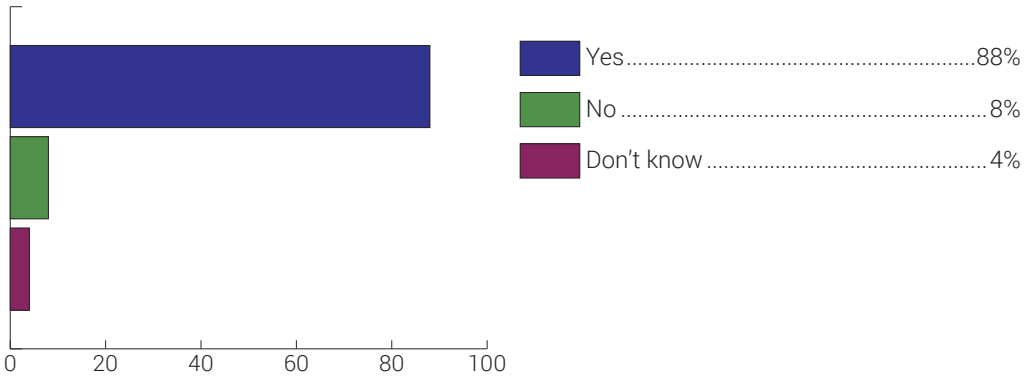
Answer/country	USA	UK	Germany	France	Italy	Sweden	Denmark
Yes, definitely	60	49	65	71	59	68	20
Yes, possibly	35	48	31	27	35	26	54
No, not at all	5	3	4	1	6	6	26

Concerns for security are rising, with decisions taken at the board level in most companies. Both IT C-suite decision makers and boards are increasingly concerned about security, not only due to the cost of a breach, but also because the companies' future is at stake when the most valuable data is exposed to interested attackers.

As a result, almost 90 percent of boards address cybersecurity as a serious risk management issue with severe reputational and financial consequences. According to the survey, security has reached board level in the overwhelming majority of large companies from France (95 percent), Italy (94 percent), Germany (91 percent) and the United States (90 percent). Lower, yet still good, numbers have been reported in Sweden (85 percent), the United Kingdom (81 percent) and Denmark (74 percent).

CHART 3

Does the board of directors address cybersecurity as a serious risk-oversight issue with severe reputation and financial consequences? (%)



The risks are real, and businesses need to mitigate risks

75 percent of US respondents state the worst consequences of an attacker gaining access to their companies' most valuable asset would be the financial cost and reputational damage. However, few say the financial cost could lead to bankruptcy 35%. In Sweden, 65 percent of those surveyed expect cyber criminals accessing prized assets could lead to the downfall of the company.

Reputational costs are perceived most as a main threat in the UK, where almost 80 percent of respondents have mentioned it as the most dangerous risk to their business, almost triple the percentage of Italian IT execs.

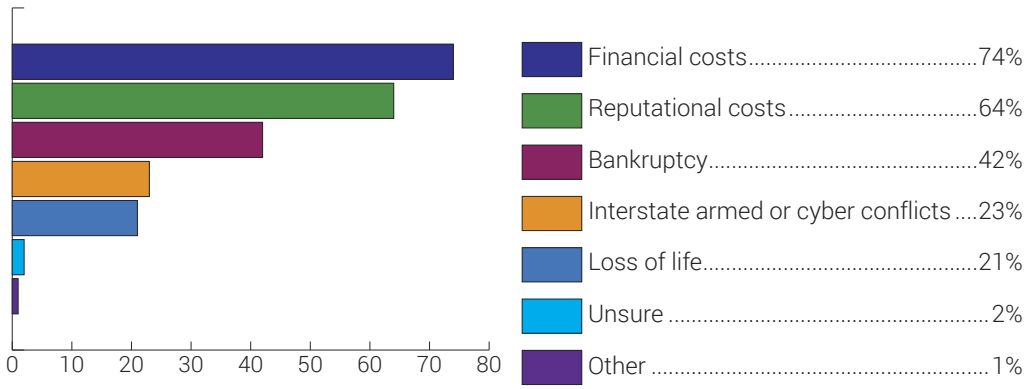
Even if it sounds alarming, loss of life – mentioned by 39 percent of the Swedes - is a severe yet real consequence of an APT. Targeted attacks could also aim at critical national or transnational infrastructures (i.e. nuclear power plants, national energy grids, urban water supplies, transportation management systems, traffic controller systems, hospitals and other healthcare facilities). In a modern environment where automation has become a reality, targeted attacks can practically **paralyze countries and, unfortunately, lead to human casualties.**

Exfiltrating sensitive data could also be leveraged by governments for military purposes too. An obvious example of information-stealing APTs is Net Traveler. Quietly stealing information since 2004, more than 22 gigabytes of data pertaining to aerospace, nanotechnology, nuclear power cells, lasers, drilling, manufacturing in extreme conditions, and radio wave weapons have been exfiltrated without triggering any bells and whistles for years.

Loss of life has been also mentioned by many respondents in Germany (nearly 30 percent), and the US (almost 20), while far more Italians fear financial losses (85 percent) than Danes (55 percent).

CHART 4

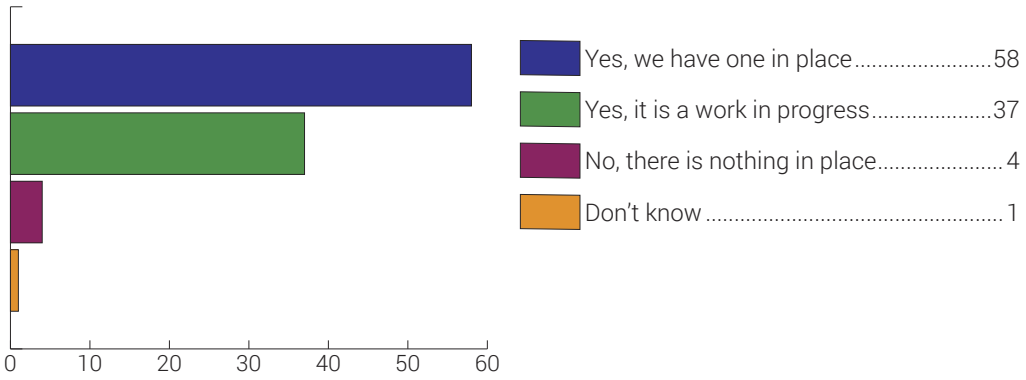
What are the worst consequences you fear if an APT attacker accesses the most valuable data or infrastructure? (global results - %)

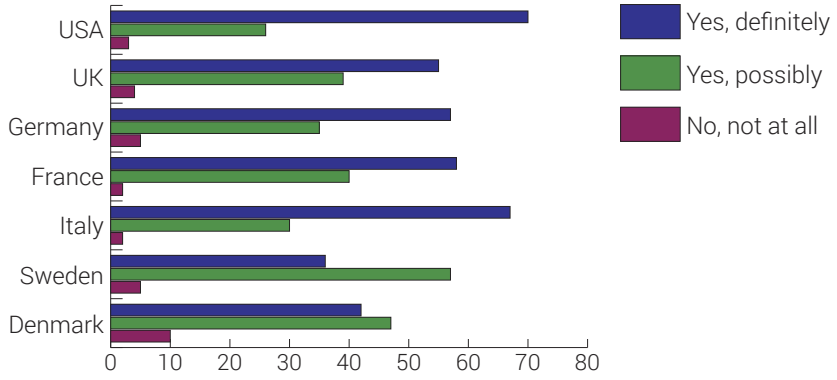


Most organisations (58 percent) have an incident response and disaster recovery plan in place in case of an APT attack or massive breach, and 37 percent have started developing such a strategy. Less than 4 percent lack these types of procedures. According to the survey, the best prepared are companies from the US and Italy (more than two-thirds of respondents say they have an APT incident response plan in place), while the least prepared are those from Sweden and Denmark (where only four in 10 respondents have completely implemented such a mechanism).

CHART 5

Does your organization have an incident response or disaster recovery plan in case of a major security breach / APT? (%)





Answer/country	USA	UK	Germany	France	Italy	Sweden	Denmark
Yes, we have one in place	70	55	57	58	67	36	42
Yes, it is a work in progress	26	39	35	40	30	57	47
No, there is nothing in place	3	4	5	2	2	5	10

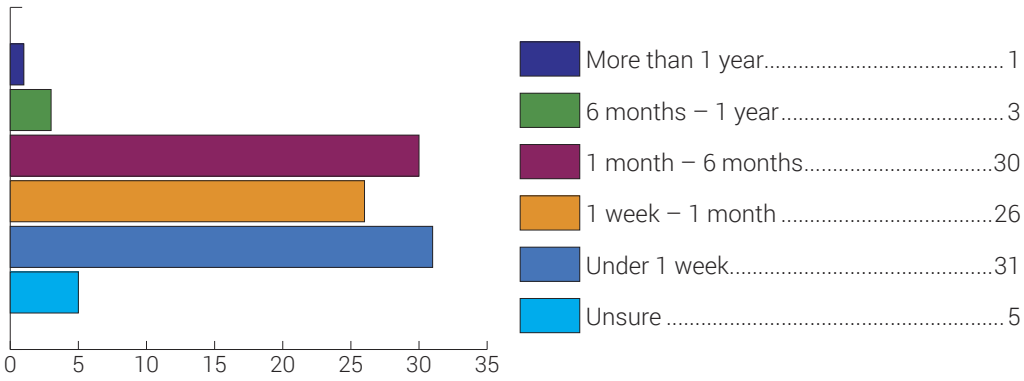
The risks aren't always visible, but they are ever present

Most IT decision makers say it would take a few months to detect an APT (30 percent), but, surprisingly, more than a quarter (26 percent) say they would only need a few weeks to uncover modern sophisticated threats. This might show many surveyed IT execs fear, but underestimate, the potential complexity of these threats.

"Cyberattacks can go undetected for months and, in most cases, breaches stem from zero-days and kernel-level malware," Bitdefender's Senior eThreat Analyst Liviu Arsene says. "This is precisely what APTs turn to, because it keeps them from being detected. Kernel exploits and rootkits can evade traditional endpoint security solutions to gain full control over the operating system."

CHART 6

How long would it take you to detect an APT attack? (%)



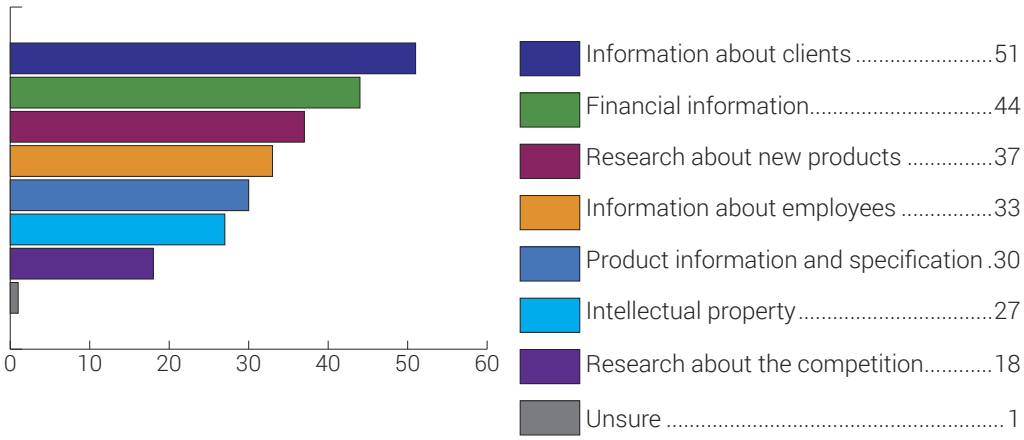
Companies mostly fear losing information about their customers (51 percent), followed by financial information (44 percent), information about certain employees (33 percent), research about new products (37 percent), product info and specifications (30 percent), intellectual property (27 percent), and research about the competition (18 percent).

Some 68 percent of the execs surveyed perceive layered defense, a mix of multiple security policies and tools designed to fight modern threats and penetrations, as the best defense against advanced persistent threats. Next-gen solutions, security audits, traditional security and log monitoring were also mentioned by more than a third of the respondents.

A previous study by Bitdefender revealed that companies in the US would pay an average of $124,000 to avoid public shaming scandals after a breach. Some 14 percent would pay more than $500,000. Companies based in the UK would pay an average of £82k to avoid public shaming scandals after a breach, while 5 percent would pay more than £500k. German CISOs would spend €80,000 on average.

CHART 7

Which are the high-value assets the company is afraid of losing? (%)



Methodology

The survey, conducted in April-May 2017 by Censuswide for Bitdefender, included 1,051 IT security purchase professionals from large enterprises with 1,000+ PCs and data centers, based in the US, the UK, France, Italy, Sweden, Denmark, and Germany.

About Bitdefender

Bitdefender is a global security technology company that provides cutting edge end-to-end cyber security solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a provider of choice in both hybrid infrastructure security and endpoint protection. Through R&D, alliances and partnerships, Bitdefender is trusted to be ahead and deliver robust security you can rely on. More information is available at http://www.bitdefender.com/

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-Jul.13.2017-Tk#: crea1615