F-Secure softwerx

2019 SECURITY PRIORITIES IN THE FINANCE SECTOR

Benchmark your organization against your peers

Finance and insurance companies tend to be up-to-date with cyber security. Their security concerns center around keeping their valuable data safe while complying to industry standards. Compared to other sectors they more often manage their data security in-house rather than use managed security services. One in four financial companies have detected more than five attacks in the past 12 months.

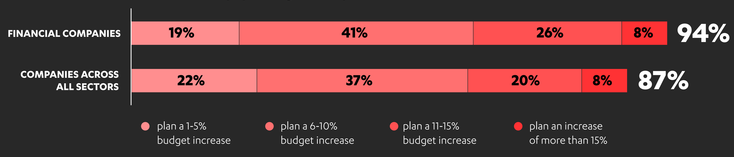
SECURITY PRIORITIES IN THE NEXT 12 MONTHS

TOP 5

1	2	3	4	5
Cloud security - Ensuring security of cloud applications and components such as Office 365 and AWS	Preventing data breaches and loss of customer or company data / IP	Ensuring protection against malware and ransomware	Preventing or limiting threats by malicious insider	Ensuring compliance to industry standards such as GDPR, HIPAA, PCI, etc
24%	**23%**	**22%**	**21%**	**21%**

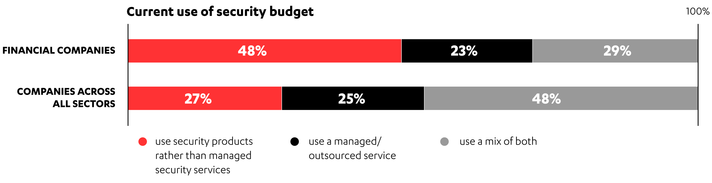
To meet these priorities, security budgets are increasing more than in other sectors

Planned security spending in next year



THE FINANCE SECTOR HAS A PREFERENCE FOR IN-HOUSE PRODUCTS

Current use of security budget



Average number of security brands used:

4.5 financial companies

3.1 companies across all sectors

Financial companies employ cyber security personnel in-house and they are willing to use cyber security as products. This is why the number of security brands used in financial companies is higher than average.

TOP 5
Security solutions used

1. Email security & spam filtering
2. Network firewall
3. Endpoint security (anti-virus) for computers
4. Security for servers
5. Gateway web security/content filtering

25% of companies have an advanced threat protection / detection and response solution

55% are interested in advanced threat protection solutions

8% plan to purchase in the next 6 months

TOP 5
Consulting services purchased in the past year

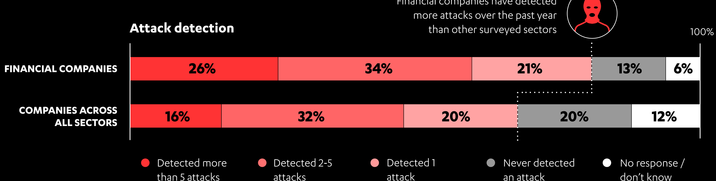
1. Employee security awareness improvement
2. Vulnerability assessment
3. Security strategy and advisory
4. Privacy management (e.g. GDPR)
5. Threat analysis (e.g. red teaming)

90% of financial companies have used cyber security consulting services to improve their ability to resist attacks

81% OF FINANCIAL COMPANIES HAVE DETECTED ATTACKS IN THE PAST 12 MONTHS

Attack detection

Financial companies have detected more attacks over the past year than other surveyed sectors



STUDY METHODS AND COVERAGE

3350 respondents from IT decision makers and influencers
12 countries: Finland, Norway, Sweden, Denmark, UK, France, Belgium, Netherlands, Germany, US, India, Japan
Methodology: Online survey
Data collection in October and November 2018
Company sizes: 25-199, 200-249, 500-999, 1000-4999, 5000+

"ALL SECTORS" MEANS:

Finance
Insurance
Healthcare (both public and private)
Manufacturing
Wholesales
Utilities (incl. Energy)
Retail
Telecom & Communication Technologies/ICT Services
Public sector (central government)
Public sector (local government)
Education
Non-profit organizations
White collars intensive services (e.g. accounting, engineering, consulting etc.)
Blue collar intensive services (e.g. construction, cleaning, restaurants, hotels etc.)
IT services
Transport or logistics
Defense & Law Enforcement

F-Secure softwerx