After Equifax and WannaCry:

Security Practices and Expectations

VARONIS

We've all seen the headlines: Breaches are hitting high-profile organizations almost daily. We wanted to know if professionals responsible for cybersecurity in their organizations are shoring up their security, what approaches they are taking, and if they believe they are prepared to ward off the next big attack.

KEY FINDINGS

- Nearly half of the respondents believe it is likely their organization will face a major, disruptive attack in the next 12 months. Despite the headlines and concern that an attack is likely, most respondents feel that their organizations are well positioned to protect themselves from attack. Respondents also report that their leadership teams think their organizations are prepared for an attack.

- Attackers that successfully get onto a network can move laterally if access to information is available. Yet surprisingly only 66% of U.S. organizations and 51% of EU organizations (57% overall) fully restrict access to sensitive information on a "need-to-know" basis. Organizations in Germany are the least likely to restrict access on a need-to-know basisw (38%).

- As shown with the DNC and Equifax breaches, attackers can get onto a network and spend weeks or even months stealing sensitive information before anyone knows they've been compromised. Despite these dangers, 8 out of 10 respondents in the EU and the U.S. are confident or very confident that hackers are not currently on their network.

- Massive breaches like the one disclosed by Equifax and ransomware attacks such as WannaCry are serving as a wake-up call for organizations to shore up their security: 8 out of 10 respondents in the EU and U.S. report that they have changed, or plan to change, their security policies and procedures.

- Over the past two years, about a quarter of organizations have experienced data loss, data theft, and/or ransomware. German firms were particularly hard hit ransomware: 34% of respondents in Germany reported that their organization was a victim of ransomware in the past 2 years.

- A majority (67%) of respondents reported their organizations have cybersecurity insurance policies. They are least prevalent in the U.S. (62%) and most common in France (75%).

- Looking ahead to 2018, respondents reported a variety of cybersecurity concerns. Overall, data theft and data loss concern them the most, closely followed by ransomware, cloud, and compliance.

ABOUT THE SURVEY

Varonis commissioned SSI to conduct a survey to determine the top concerns, approaches and experiences of IT professionals involved in cybersecurity on topics such as ransomware, technology and data security.

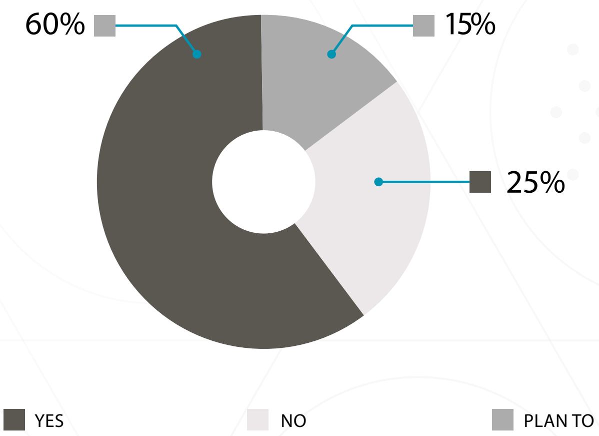
- 500 surveyed: 200 in the U.S., 100 each in the UK, France and Germany
- All respondents are full-time employees involved in IT and personally responsible for cybersecurity
- Respondents are from organizations with more than 1,000 employees
- All respondents work for organizations that collect, generate or possess sensitive datasuch as PII and payment card information
- Respondents work in many sectors: technology and software, financial services, industrial/manufacturing, public sector, retail, healthcare/pharmaceutical, education and research, transportation, energy and utilities and others.
- The survey was conducted between September 28 – October 6, 2017

Security Expectations and Readiness

There have been several widespread cyberattacks over the past few years (for example, WannaCry and the attack on Equifax). Based on these attacks, has your organization changed or does it have plans to change its security policies and procedures?

The massive breaches and ransomware attacks in the news are serving as a wake up call for organizations to shore up their security. 8 out of 10 respondents in the EU and the U.S. report that they have changed, or plan to change, their security policies and procedures.

▼ POLICY CHANGES BASED ON PUBLICIZED PAST ATTACKS



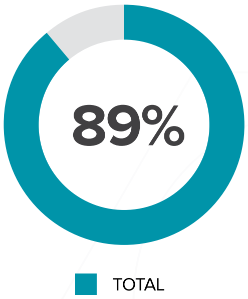
▼ IN DEPTH: SURVEY RESULTS BY COUNTRY AND REGION:

	US	EU	UK	DE	FR
Yes	59.0%	61.0%	61.0%	56.0%	65.0%
No	24.0%	27.0%	21.0%	33.0%	26.0%
Plan to	18.0%	13.0%	18.0%	11.0%	9.0%

How do you rate your organization's ability (staff, resources, technology) to protect itself from a cyberattack? How do you think your leadership team would rate your organization's ability to protect itself from a cyberattack?

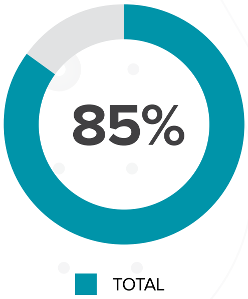
Most respondents (89%) express confidence in their cybersecurity stance and feel that their organizations are in a good position to protect themselves from attack, and that their leadership feels similarly.

▼ ORGANIZATION ABLE TO PROTECT ITSELF FROM CYBERATTACK



US	EU	UK	DE	FR
90%	89%	93%	86%	86%

▼ LEADERSHIP VIEWS ORIGANIZATION AS ABLE TO PROTECT ITSELF

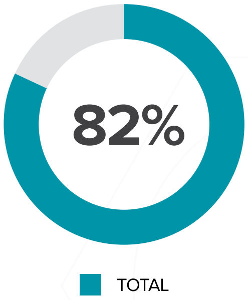


US	EU	UK	DE	FR
86%	84%	85%	82%	84%

How confident are you that hackers do not currently have access to information on your private network?

In many high-profile attacks, attackers are able to gain access to an organization’s networks and lurk undetected for days, weeks or even months -- and sometimes even longer. Yet 8 out of 10 respondents in the EU and the U.S. are confident or very confident that hackers do not already have access to their networks.

CONFIDENCE HACKERS DON’T HAVE CURRENT ACCESS

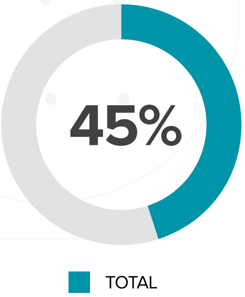


US	EU	UK	DE	FR
84%	81%	85%	81%	78%

How likely do you think it is that your organization will experience a major, disruptive attack in the next 12 months?

Despite reporting a high level of confidence, 45% believe it is likely they will face a major, disruptive attack in the next 12 months.

LIKELIHOOD OF FACING ATTACK IN NEXT 12 MONTHS

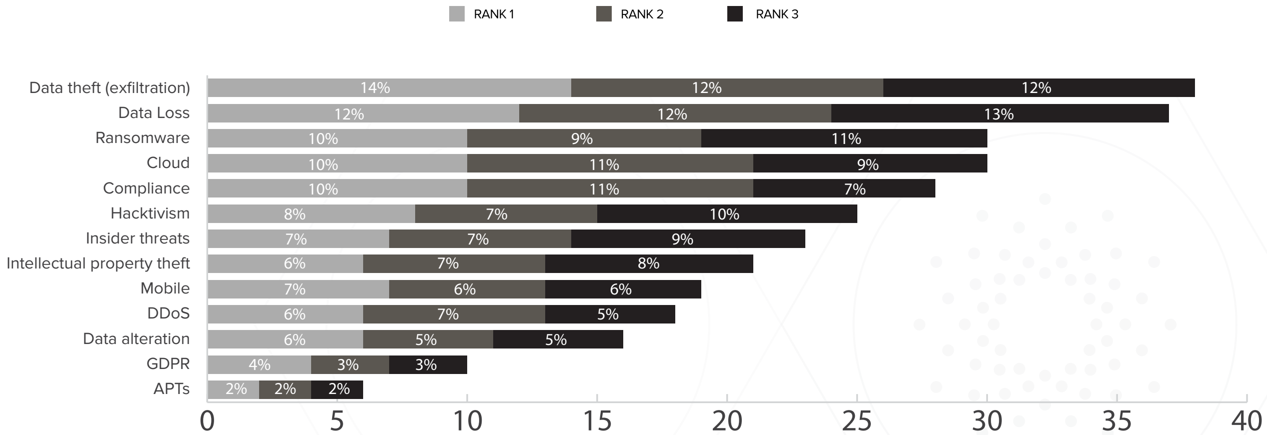


US	EU	UK	DE	FR
42%	42%	46%	48%	48%

What's Next: Security Concerns in 2018

What are your organization's Top 3 cybersecurity concerns for 2018?

What is keeping cybersecurity professionals up at night? Overall, data theft and data loss are of most concern, closely followed by ransomware, cloud, and compliance. Data theft and data loss are in the top 5 concerns in all areas surveyed.



Ransomware and cloud also appear as top concerns in all areas but Germany, where mobile and DDoS are its unique concerns. Compliance is among the top 5 concerns in the U.S. and UK, while hacktivism is a top 5 concern in Germany and France.

▼ U.S. RESPONDENTS REPORTED THAT DATA THEFT, DATA LOSS AND COMPLIANCE ARE THEIR TOP 3 CONCERNS.

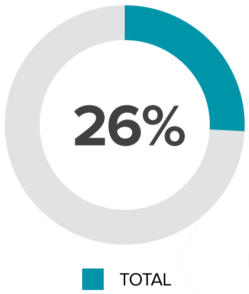
US		Total EU		UK		Germany		France	
Data theft	43%	Data loss	38%	Data loss	37%	Data loss	47%	Data theft	38%
Data loss	36%	Data theft	34%	Data theft	36%	Hacktivism	32%	Data loss	30%
Compliance	36%	Cloud	29%	Ransomware	34%	Data theft	29%	Cloud	30%
Ransomware	32%	Ransomware	28%	Cloud	34%	Mobile	28%	Hacktivism	29%
Cloud	31%	Hacktivism	26%	Compliance	32%	DDoS	28%	Ransomware	26%

Cyberattack Experience

As far as you know, has your organization experienced the loss or theft of company data over the past two years?

- Over the past two years, about a quarter of organizations surveyed have experienced data loss or data theft.
- In the U.S., that percentage is slightly lower (23%) than compared to the EU (29%).

▼ EXPERIENCED LOSS OF THEFT OF DATA IN PAST 2 YEARS



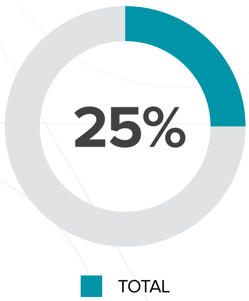
US	EU	UK	DE	FR
23%	29%	27%	29%	30%

Has your organization been the victim of a ransomware attack in the past two years?

Over the past two years, a quarter of organizations surveyed were a victim of ransomware.

- German firms were most likely to be victimized by ransomware (34%)
- In the U.S. and UK, about 1 in 5 surveyed was a victim of ransomware
- In France, nearly one-third (31%) of organizations experienced ransomware

▼ VICTIM OF RANSOMWARE PAST 2 YEARS



US	EU	UK	DE	FR
21%	28%	20%	34%	31%

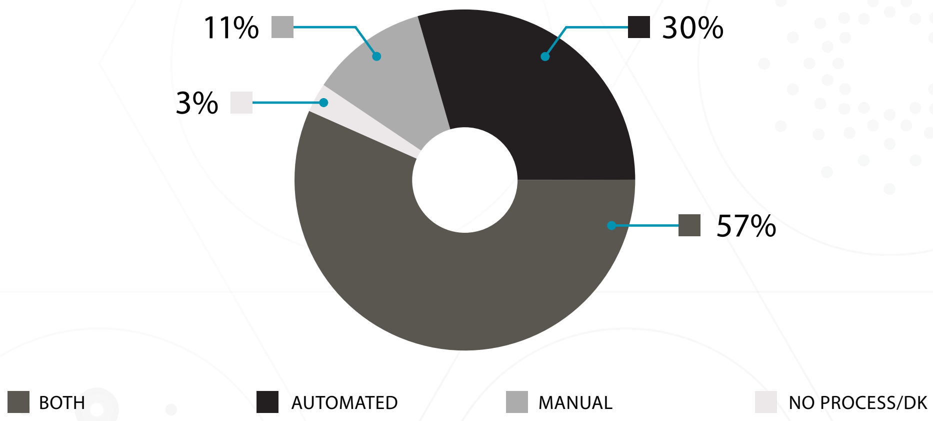
Protecting Sensitive Information

How does your organization identify sensitive information, such as customer payment and personal identifying information?

There's a lot of talk about automating security. Yet manual techniques for detecting and locking down data are still very common.

- 50% or more of all respondents reported that their organization uses a combination of automated and manual approaches for identifying sensitive data
- Only about 25-36% rely fully on automation
- 11% rely on manual processes

WAYS OF IDENTIFYING SENSITIVE INFORMATION



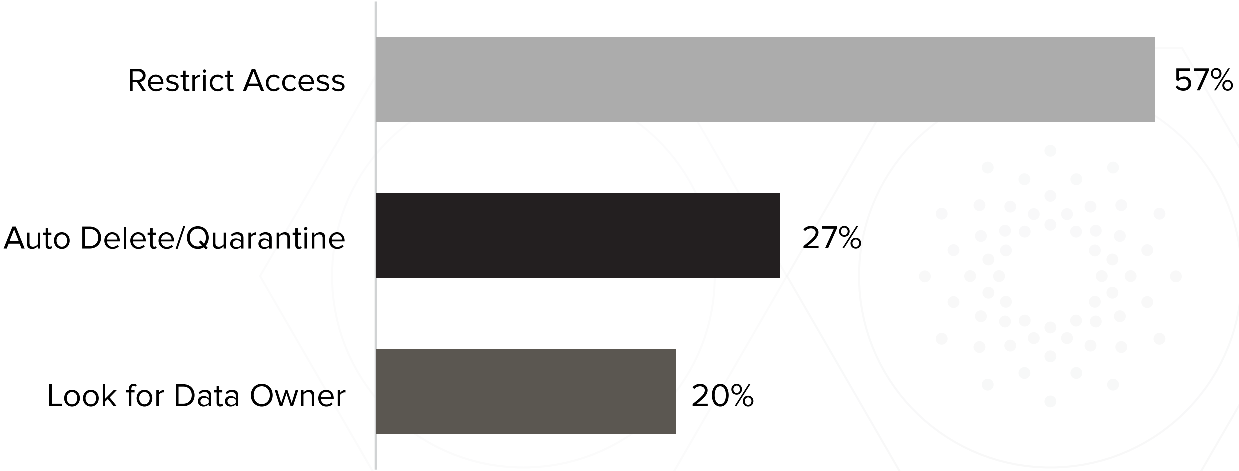
IN DEPTH: SURVEY RESULTS BY COUNTRY AND REGION:

	US	EU	UK	DE	FR
Use automation to look for and identify sensitve files	34.5%	30.3%	30.0%	25.0%	36.0%
Use manual "labeling" approach	7.5%	14.0%	15.0%	17.0%	10.0%
Use both automated and manual approaches	66.0%	52.0%	50.0%	56.0%	50.0%
Organization does not have formal process for identifying sensitive data	0.5%	3.0%	3.0%	2.0%	4.0%
Don't know	1.5%	0.7%	2.0%	0.0%	0.0%
Total	100.0%	100.0%	100.0%	100.0%	100.0%

Once your organization identifies sensitive information, what is the most likely next step in handling that data?

When sensitive information resides in folders that aren't obviously owned by anyone, finding the owner can be a tedious, manual process. 20% of respondents are still relying on this manual approach. About half of the respondents restrict access, while the remaining quarter automatically delete or quarantine the information.

▼ NEXT STEP



▼ IN DEPTH: SURVEY RESULTS BY COUNTRY AND REGION:

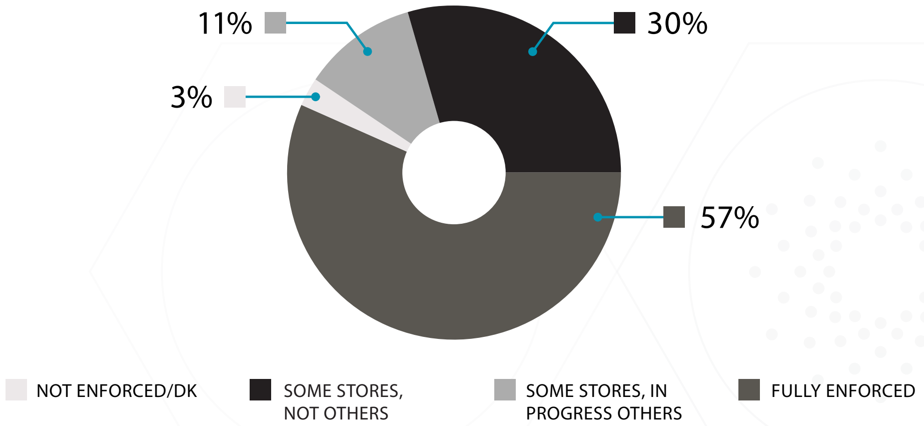
	US	EU	UK	DE	FR
We usually need to look for a data owner	16.0%	22.3%	23.0%	18.0%	26.0%
We delete or quarantine it automatically	20.0%	31.3%	21.0%	36.0%	37.0%
We restrict access either through access control lists, encryption, or both	63.0%	45.3%	55.0%	46.0%	35.0%
Other way (please specify)	0.5%	0.0%	0.0%	0.0%	0.0%
Don't know	0.5%	1.0%	1.0%	0.0%	2.0%
Total	100.0%	100.0%	100.0%	100.0%	100.0%

Does your organization restrict access to sensitive information on a need-to-know basis?

Organizations are getting better at restricting access to sensitive data.

- On average, 57% of all respondents reported that their organizations fully restricts access to information on a need-to-know basis
- 4 in 10 organizations do not fully restrict access to sensitive information on a need-to-know basis

NEED TO KNOW RESTRICTION ACCESS



IN DEPTH: SURVEY RESULTS BY COUNTRY AND REGION:

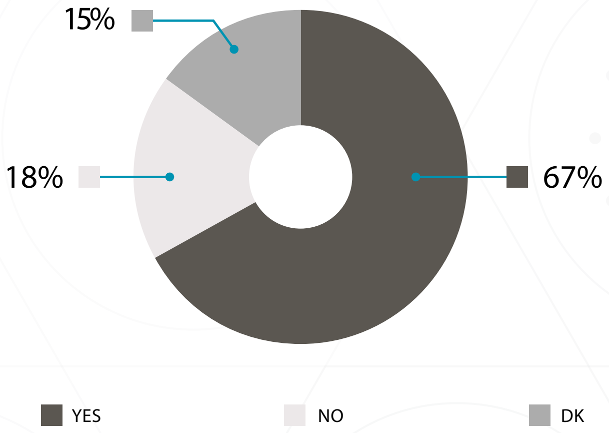
	US	EU	UK	DE	FR
Yes, fully enforced	65.5%	51.3%	58.0%	38.0%	58.0%
Yes, enforced for some data stores but not others	23.5%	34.0%	24.0%	46.0%	32.0%
Yes, enforced for some stores and in process for others	9.5%	11.3%	17.0%	17.0%	8.0%
No, not enforced	1.5%	2.3%	0.0%	0.0%	2.0%
Don't know	0.0%	1.0%	1.0%	1.0%	0.0%
Total	100.0%	100.0%	100.0%	100.0%	100.0%

Does your organization have a cybersecurity insurance policy?

The majority of organizations surveyed have cybersecurity insurance policies to limit their liability and cover costs resulting from a data breach.

- In the EU, 7 out of 10 professionals reported their organization had a cybersecurity insurance policy
- In the U.S., 6 out of 10 reported their organization had a cybersecurity insurance policy
- Overall, cybersecurity insurance policies are least prevalent in the U.S. and most common in France

▼ CYBERSECURITY INSURANCE POLICY



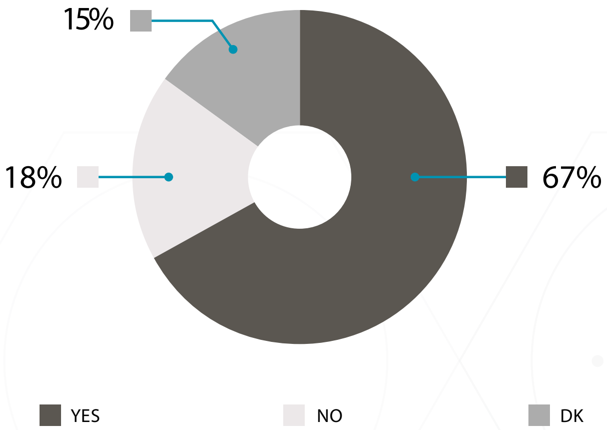
▼ IN DEPTH: SURVEY RESULTS BY COUNTRY AND REGION:

	US	EU	UK	DE	FR
Yes	62.0%	71.0%	68.0%	69.0%	75.0%
No	22.0%	16.0%	11.0%	24.0%	13.0%
DK	17.0%	13.0%	21.0%	7.0%	12.0%

Approximately what percentage is devoted to each of the following areas?

Organizations are dedicating more resources (expenditures and labor) to protecting their data, with the remaining resources divided almost equally to networks and systems.

▼ RESOURCES DEDICATED TO CYBERSECURITY BY AREA

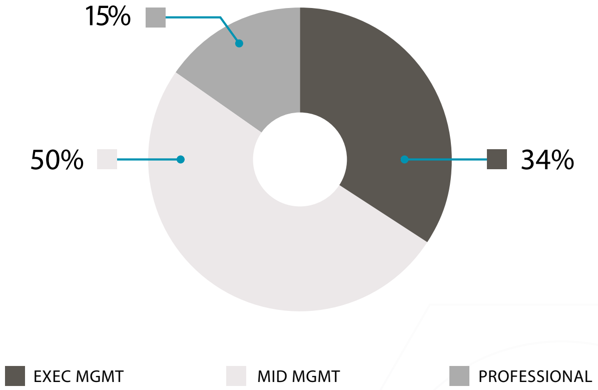


▼ IN DEPTH: SURVEY RESULTS BY COUNTRY AND REGION:

	US	EU	UK	DE	FR
Yes	62.0%	71.0%	68.0%	69.0%	75.0%
No	22.0%	16.0%	11.0%	24.0%	13.0%
DK	17.0%	13.0%	21.0%	7.0%	12.0%

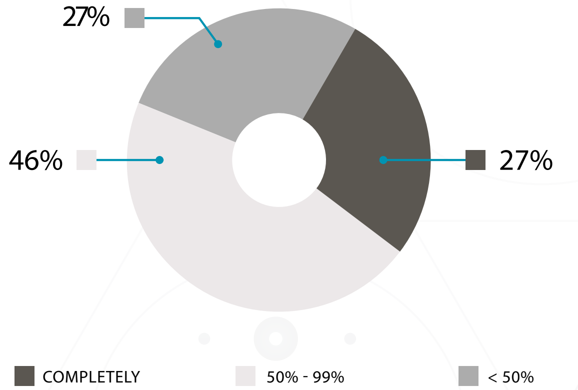
About the Respondents

PRIMARY JOB FUNCTION IN IT



	US	EU	UK	DE	FR
Exec mgmt	24.0%	42.0%	32.0%	38.0%	55.0%
Mid mgmt	58.0%	45.0%	49.0%	55.0%	31.0%
Professional	19.0%	13.0%	19.0%	7.0%	14.0%

ROLE DEDICATED TO CYBERSECURITY



	US	EU	UK	DE	FR
Completely	28.0%	27.0%	24.0%	27.0%	29.0%
50% - 99%	42.0%	49.0%	44.0%	59.0%	45.0%
< 50%	31.0%	24.0%	32.0%	14.0%	26.0%

FIRM SIZE

	US	EU	UK	DE	FR
1,000 - 1,999 Employees	24.5%	27.7%	24.0%	36.0%	23.0%
2,000 - 2,999 Employees	7.0%	12.7%	12.0%	11.0%	15.0%
3,000 - 4,999 Employees	18.0%	21.3%	50.0%	25.0%	18.0%
5,000 or more Employees	50.5%	38.3%	3.0%	28.0%	44.0%
Don’t Know	0.0%	0.0%	2.0%	0.0%	0.0%
Total	100.0%	100.0%	100.0%	100.0%	100.0%