NetClean.

2021
NetClean Insights

The State of Child Sexual Abuse Material and the IT industry

Contents

NetClean Insights: The State of Child Sexual Abuse Material (CSAM) and the IT industry

The first NetClean survey of Senior Global IT professionals

Who we spoke to:

1035 Senior IT professionals

FIVE markets

31% C-Level

23% Directors

47% Managers

The IT industry remains profoundly unprotected against Child Sexual Abuse Material (CSAM):

64% **Of all organisations have experienced a case of CSAM in the last 5 years**

1/2 **Of all IT pros suspect illegal material is being stored on their organisation's devices**

In the US 59% of senior IT professionals thought that it was likely the dark web could be used undetected on their organisation's IT assets

Incidents of CSAM:

51% Involve laptops

1/3 Involve USB storage

57% Are repeat cases

6/10 IT Pros say Covid made incidents worse

7/10 IT Professionals underestimate the prevalence of Child Sexual Abuse Material (CSAM)

Read the full report and details of how you can take action to stop access to and stop the spread of child sexual abuse material at: netclean.com/netclean-insights

NetClean.

Introducing the 2021 NetClean Insights

This is a first of its kind survey of senior IT professionals assessing the threat that they face from child sexual abuse material (CSAM). By interviewing 1035 CSOs, CIOs Directors and Managers we are able to give a picture of the state of the industry's response to CSAM in 2021.

For the 2021 NetClean Insights we interviewed the most senior IT professionals in the US, the UK, Sweden, Belgium and the Netherlands. The respondents to the survey were drawn from firms with over 50 employees with most coming from firms with over 200 employees, including around a third from the very largest organisations with over 1000 employees working for them.

Respondents to the survey were recruited through online panels and incentivised for their time, but were not aware, at the time, that the survey was being conducted by NetClean so as to ensure answers were not biased in any way.

All interviews were conducted in a GDPR compliant manner and no details of names, company names or roles were collected. All data was completely anonymised.

Sample composition								
Country						Seniority		
Total	United Kingdom	USA	Sweden	Netherlands	Belgium	C-Level	Director	Manager
1035	151	706	109	35	34	320	233	482

Size					
Total	50-100 employees	100-200 employees	200-500 employees	500-1000 employees	1000+ employees
1035	84	106	205	331	309

Glossary of terms:

CSAM: Child sexual abuse material
Small organisations: 50-200 employees
Medium organisations: 200-1000 employees
Large organisations: 1000+ employees

“We’ve seen awareness of CSAM rise and now we can also see that IT industry leaders think it’s time for action”

Anna Borgström,
CEO NetClean

This brand new research, once again, brings home the scale of the challenge facing the IT industry from child sexual abuse material. It is a positive development that awareness of the problem is very widespread amongst senior IT professionals. There is also a willingness to take action and protect their organisations, what is needed now is to fulfil that promise of action and for the industry to take the next steps that leaders tell us are necessary – it is time to deliver.

The fact that we found over two thirds of organisations have experienced at least one incident of CSAM is a sobering reminder of the problem that the world faces. That over half of organisations have had a repeat incident is more sombre still. IT leaders are almost unanimously well aware of the problem that they face and we note that the more senior IT leaders are even more acutely aware of the issue of CSAM, especially CSOs and CIOs.

At the same time as being aware of the challenge IT leaders recognise that there are flaws in their current protection and that there is much more to be done by the industry in response to CSAM. It should be lost on no one that two thirds of the most senior IT professionals think it is still possible that CSAM could be viewed undetected on their assets and that over half say that their organisations respond to threats too late.

Alongside this self-awareness of the problem in the IT industry we found that there was a strong desire to put things right by taking action against CSAM. Seven in ten leaders in the IT industry think that their organisation should be doing more and nearly all say that they would consider buying specific protection against the CSAM threat. It’s time to deliver on that promise.

1

There are a large number of cases of CSAM across organisations

Almost all of the IT professionals, at all kinds of organisations, said that there had been cases of employees viewing child sexual abuse material over the course of the last five years.

Automated detection of CSAM gives a good indication of just how widespread it is, but in this survey we were able to confirm this prevalence independently from those on the front line.

Medium sized companies with between 200 and 1000 employees were worst hit with 71% reporting at least one incident of employees viewing child sexual abuse imagery within the last five years.

In large companies with over 1000 employees the situation was slightly less stark with over 65% reporting at least one incident and 57% reporting multiple incidents.

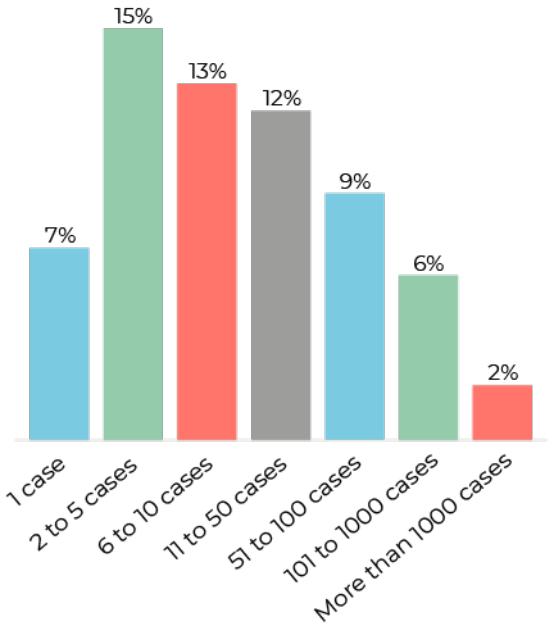
64%

OF ALL ORGANISATIONS HAVE EXPERIENCED A CASE OF CSAM OVER THE LAST 5 YEARS

57%

HAVE HAD REPEAT INCIDENTS WITHIN THE SAME ORGANISATION

A majority of organisations report having had cases of CSAM in the last five years and most of those have had multiple repeat cases despite having faced a first incident.



Q. For each of the following please say what experience your firm has had in the last five years: Employees viewing child sexual abuse material

These remarkable accounts of the scale of CSAM incidents stretch across different levels of seniority of interviewees too. C-level interviewees have had the most experience of CSAM cases with 67% saying that their organisation had experienced more than one case in five years.

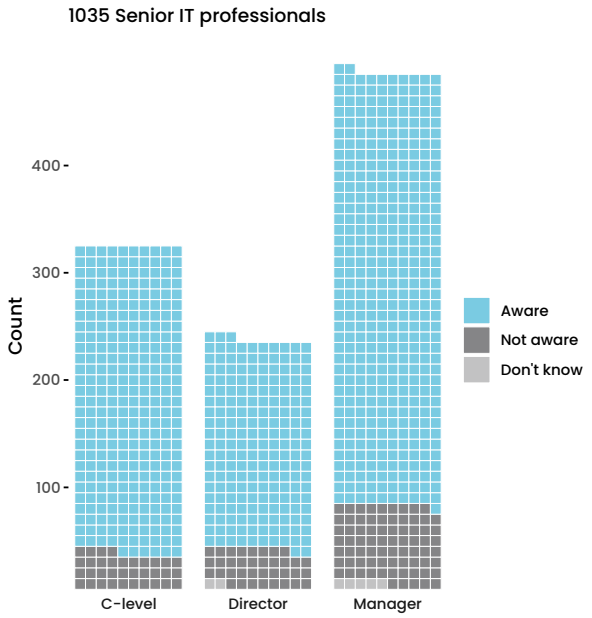
For IT Directors the figure is 50% having experienced more than one case and for Managers the figure is 54%.

Companies in the US (70%) are picking up more incidents than their colleagues in the UK (39%) and Sweden (60%).

2

There is a high level of awareness of the problem from within the IT industry

PEOPLE WHO WORK IN IT ARE WELL AWARE OF THE PROBLEM OF CSAM IMAGERY



Q. How much have you heard about the threat of Child Sexual Abuse Material (CSAM) to organisations like yours?

Knowledge of the scale of the CSAM problem is widespread. Out of everyone we interviewed 87% said that they had heard something about the threat that CSAM posed to organisations like theirs.

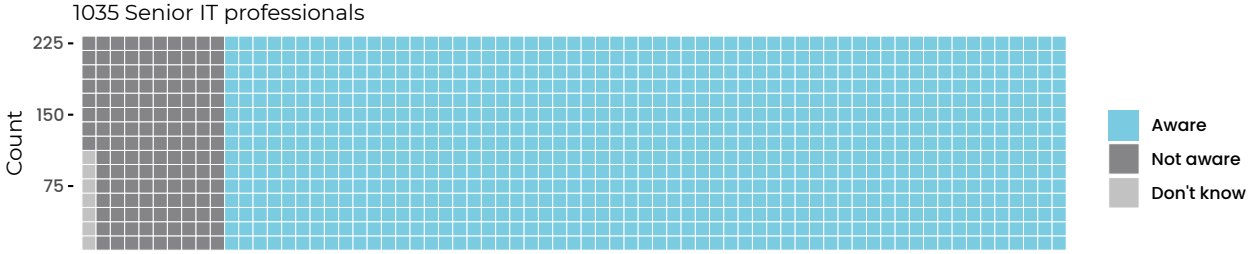
87%

HEARD SOMETHING ABOUT THE THREAT OF CSAM

Almost all C-level executives that we spoke to were aware of the threat of CSAM. 89% of them had heard something compared to 84% amongst the directors and managers that we spoke to.

Awareness was also slightly higher amongst senior professionals at firms with 500-1000 employees (91% having heard something) whilst it was slightly lower amongst the very largest firms with over 1000 employees where only 81% of the people we spoke to were aware of the threat posed by CSAM.

AWARENESS OF THE THREAT POSED BY CSAM TO ORGANISATIONS



Q. Thinking about your experience in the IT industry approximately what proportion of computers do you think have CSAM material on them?

3

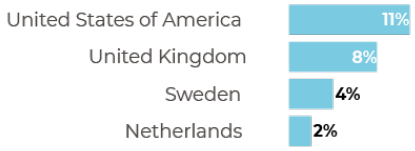
People are expecting the problem to get worse over the next year

Most people in the IT industry expect more cases of child sexual abuse material in the next year than in the last. When we net out those who say that the threat from CSAM is increasing against those that say it is likely to decrease the overall score is a +11 point lead for those saying it will increase over the next year.

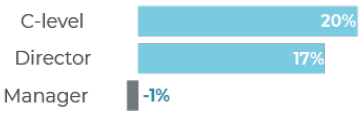
Amongst the most senior IT professionals, those at Director and C-suite level, the expectation of increases is even greater (+20 points for C-level and +17 for Directors).

The view from the largest companies is more positive than the view from smaller and medium sized organisations. The very largest companies taken together have a net negative expectation (only just at -3 points) for the trajectory of CSAM. Having said that, the IT professionals at companies of all other sizes have an expectation of increasing CSAM incidents over the next year

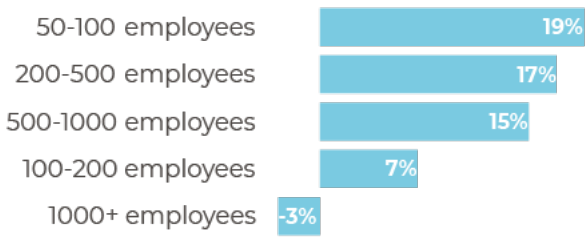
EXPECTATIONS ABOUT THE TRAJECTORY OF CSAM CASES ARE HIGHEST IN THE US AND LESS IN EUROPE.



C-LEVEL EXECUTIVES AND IT PROFESSIONALS IN LARGE COMPANIES ARE THE MOST LIKELY TO SAY THAT EMPLOYEES HANDLING ILLEGAL MATERIAL IS GOING TO INCREASE OVER THE NEXT YEAR



Q. Do you expect the following threats to increase or decrease for your organization in the next year? - Employees handling illegal or inappropriate material



Q. Do you expect the following threats to increase or decrease for your organization in the next year? - Employees handling illegal or inappropriate material

37%

OF ALL IT PROS WHO THINK THAT THE THREAT FROM EMPLOYEES HANDLING ILLEGAL MATERIAL IS ON THE INCREASE

4

IT professionals still underestimate the proportion of devices that have CSAM on them

1035 IT PROFESSIONALS SURVEYED, EACH REPRESENTED BY ONE DOT

- Accurate assessment of scale of CSAM
- Underestimates scale of CSAM

Q. Thinking about your experience in the IT industry approximately what proportion of computers do you think have CSAM material on them?

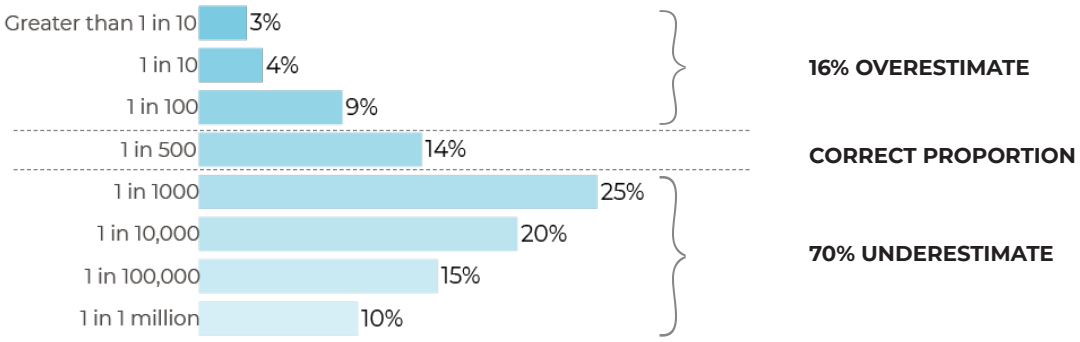
Despite the high levels of awareness about CSAM that we have registered in the IT industry at the macro scale, we found that there is still a fundamental underestimation of the proportion of computers that are actually affected by CSAM.

As past research has shown the true proportion is in the region of 1 in every 500[1] computers. However 70% of those surveyed provided some degree of underestimate of the prevalence of CSAM. 25% of IT professionals said that the true ration was 1 in 1000 computers containing CSAM which is half the true prevalence. 20% were out by over an order of magnitude and said 1 in 10000. Perhaps most alarming are the 15% who were 2 orders of magnitude out in saying 1 in 100,000 and the 10% who were 3 orders of magnitude away from the true figure – saying 1 in a million.

There was not much difference in the appreciation of the scale of CSAM at the micro level between more and less senior IT professionals. 68% of C-level executives still underestimated the prevalence.

1 NetClean Report 2018 https://www.netclean.com/netclean-report-2018/

A MAJORITY OF IT PROFESSIONALS RECOGNISE THE SCALE OF CSAM OVERALL, BUT UNDERESTIMATE THE NUMBER OF MACHINES IT IS ON

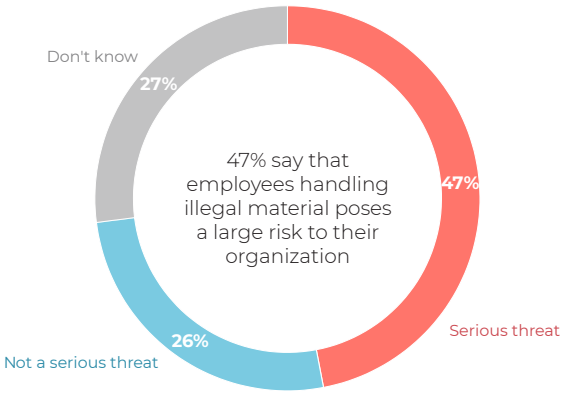


Q. Thinking about your experience in the IT industry approximately what proportion of computers do you think have CSAM material on them?

5

Senior IT professionals think employees handling illegal material poses a large risk to their organisations

JUST UNDER HALF SAYING 'LARGE RISK'



Q. How serious would these threats be for your organization were they to happen? - Employees handling illegal or inappropriate material

Just under half of the senior leaders in the IT industry think that their employees possessing illegal and inappropriate material poses a large risk to their organisation. Only 26% say that it poses a small risk.

"As well as the larger risk to children and society IT professionals are awake to the risk CSAM poses to their firms." *NetClean*

There is a stark difference in the assessment of risk between the UK and the US. In the UK only 34% of IT professionals said that their employee's possession of illegal or inappropriate material posed a large risk to their business' whilst in the US the figure was 18 points higher at 52%.

Smaller firms are also at the more complacent end of the spectrum. Only 33% of those at the smallest firms we surveyed (50-100 employees) said there was a large risk.

33%

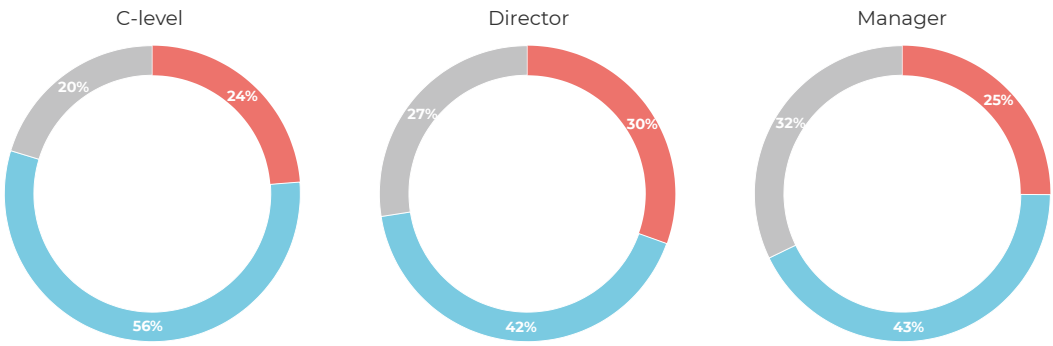
OF SMALLER FIRMS SAYING ILLEGAL MATERIAL POSES A LARGE RISK

People at C-level in the IT industry are by far the most ready to say that there is a large risk from employees handling illegal material. 56% of those in the C-suite say that it poses a large risk whilst only 42% of Director level IT professionals and 43% of Managers say the same.

56%

OF C-LEVEL IT PROFESSIONALS WHO SAY ILLEGAL MATERIAL POSES A LARGE RISK

A SLIGHTLY LOWER PROPORTION OF DIRECTORS AND MANAGERS SAY THAT CSAM POSES A LARGE RISK TO THEIR ORGANISATION.

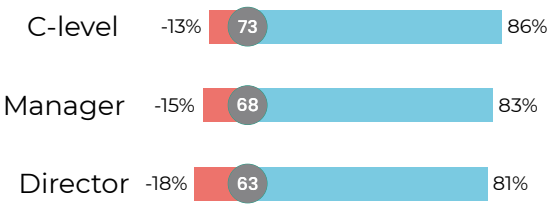


Q. How serious would these threats be for your organisation were they to happen? - Employees handling illegal or inappropriate material

6

Senior professionals do take CSAM incredibly seriously

CSAM IS TAKEN SERIOUSLY AT ALL LEVELS



Q. How serious would these threats be for your organisation were they to happen? - Employees handling illegal or inappropriate material

We asked our respondents to the survey about how seriously a range of individuals and leaders within each organisation took the threat from CSAM. Overall there is a widespread belief that the threat posed from CSAM is taken seriously by everyone, but there are crucial differences in magnitude. When making an assessment of how seriously they themselves took the threat, our senior IT professionals were confident that they took it seriously. Overall 60% said that they took it 'very seriously' and a further 24% said that they took it somewhat seriously. Only 15% said that they did not take the threat seriously.

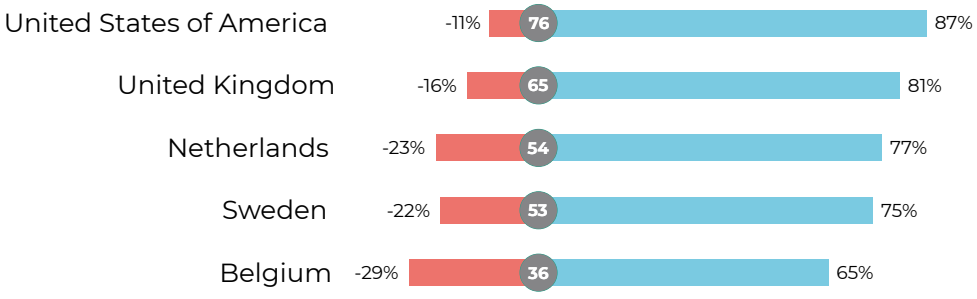
There is a widespread acceptance that organisations as a whole also take the threat of CSAM seriously. Overall 84% said that their organisation did take the threat either very or somewhat seriously. That extended to a very similar extent to the security and information leaders within each organisation (83% take it seriously). Although we were interviewing senior IT professionals we asked them to make an assessment of how seriously the management and executives outside of IT and security took the CSAM threat. The response was reassuring – 84% said that leaders outside IT took the threat from CSAM seriously. That is a figure very much in line with those IT professionals on the front line of the fight against CSAM and other illegal material.

There is slightly less certainty in Europe that leaders outside of IT are taking CSAM seriously.

86%

OF C-LEVEL IT PROFESSIONALS THINK THAT THEIR ORGANISATION TAKES THE CSAM THREAT SERIOUSLY

THERE IS SLIGHTLY LESS CERTAINTY IN EUROPE THAT LEADERS OUTSIDE OF IT ARE TAKING CSAM SERIOUSLY



Q. How seriously or not do you think leaders outside of IT take the threat of child sexual abuse imagery being watched or stored on company assets?

7

There is a widespread understanding that CSAM could be present in any organisation

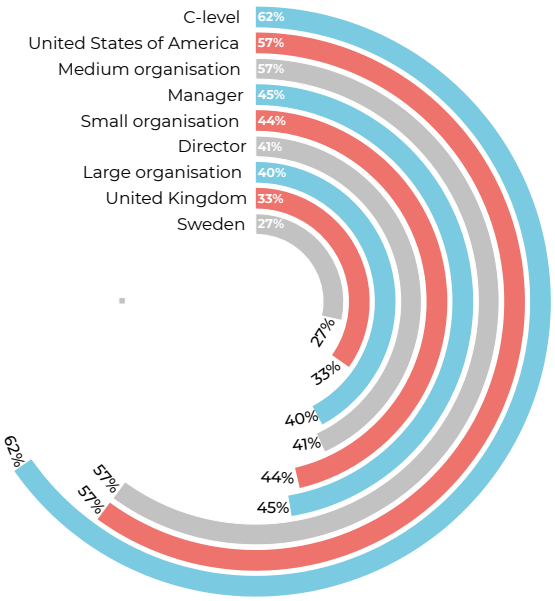
Having asked about the seriousness of the threat and how people treated the issue of CSAM, we asked whether there was a possibility that organisations could have CSAM on their systems and be unaware of it. We asked in two slightly different ways – the first 'Do you think that it is possible' and the second 'Do you think that it is likely'. The answers to the two were strikingly similar. 54% of our respondents said that it was possible CSAM could be stored on their systems, an assessment that was highest amongst C-level executives and those in some of the largest companies. Exactly half (50%) said that it was either very or somewhat likely that CSAM is being stored undetected somewhere on their systems. In fact 21% of IT professionals said that it is very likely.

The likelihood that CSAM could or is being stored undetected was, again, highest in the US and slightly lower in the European markets we surveyed. In the US, 63% of respondents think that it is at least possible that CSAM could go undetected on their systems. In the UK, for example, the figure is 41% - over two out of every five.

62%

OF C-LEVEL IT PROFESSIONALS THINK IT LIKELY THAT CSAM IS BEING VIEWED UNDETECTED ON THEIR ORGANISATIONS' ASSETS

A MAJORITY OF IT PROFESSIONALS THINK THAT IT IS LIKELY CSAM COULD BE UNDETECTED ON THEIR ASSETS



Q. Please say how likely you think it is that CSAM could be viewed, distributed and stored on your organisations' assets undetected?

A majority of IT professionals think that it is possible that CSAM is being accessed on assets owned by their organisation

	Country				Seniority			Size (employees)				
	Total	UK	USA	Sweden	C-Level	Director	Manager	50-100	100-200	200-500	500-1000	1000+
Likely	54%	36%	63%	30%	68%	45%	49%	55%	45%	57%	62%	46%
Unlikely	31%	41%	25%	53%	20%	41%	34%	24%	38%	30%	25%	40%

Q. Please say how likely you think it is that CSAM could be viewed, distributed and stored on your organisations' assets undetected?

8

Almost all the Senior IT staff we surveyed had heard of colleagues at firms dealing with CSAM incidents

Another way of thinking about the scale of CSAM within organisations is to assess the extent to which the IT professionals we spoke to have heard of colleagues at other firms dealing with real-life cases of CSAM. The answer was 82% of all the IT professionals we interviewed have personally heard of other firms who have dealt with CSAM that has been brought into their organisation.

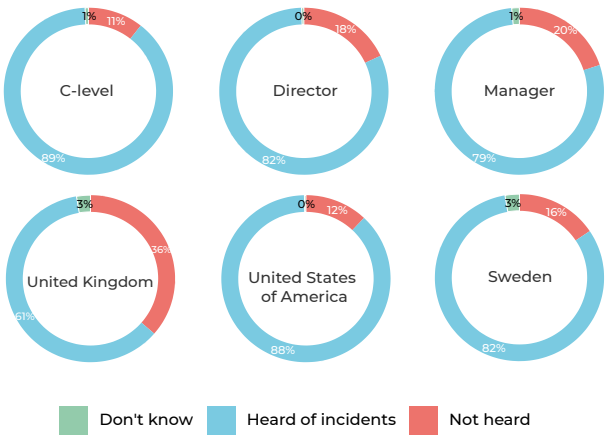
89% of C-level executives working in IT have heard of incidents from colleagues. 82% of Directors have and 79% of Managers have.

In the US 39% of respondents had actually heard 'a lot' about colleagues in other firms dealing with CSAM incidents, whilst in the UK only 20% had heard a lot. This was mirrored in the final figures for those who had heard anything from colleagues – 88% in the US and 61% in the UK.

82%

OF IT PROFESSIONALS HAVE PERSONALLY HEARD OF OTHER FIRMS WHO HAVE DEALT WITH CSAM THAT HAS BEEN BROUGHT INTO THEIR ORGANISATION

MORE SENIOR IT PROFESSIONALS AND THOSE IN THE US ARE MORE LIKELY TO HAVE HEARD OF CSAM INCIDENTS



"It is important for directors, managers and company owners to understand that a sexual interest in children is not something that goes away during business hours. Not only that. The accessibility of child abuse material is constantly increasing which means children are in danger of being sexually abused to meet the demands of creating new material to share. With the possibilities today to work from anywhere, at any time, with company property, connected to company network, there will be a risk of significance that employees at any level will execute their sexual interest in children by consuming child abuse material. But with today's solution to detect these individuals on company network you can choose to be a part of the solution to safeguard more children from being sexually abused and exploited."

Bjorn Sellstrom Superintendent Process Manager Internet-related Sexual Crimes on Children
Swedish Cyber Crime Center (SC3)
National Operations Department

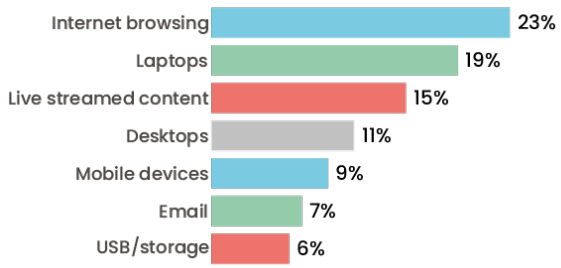
1/3

OF THESE INCIDENTS REPORTEDLY INVOLVED USB STICKS OR EXTERNAL STORAGE OF SOME KIND

9

After Internet browsers specifically, laptops are the second most common vector for illegal material cited by IT professionals

IT PROS TELL US THAT LAPTOPS ARE THE SECOND MOST COMMON VECTOR FOR SHARING CHILD SEXUAL ABUSE MATERIAL



Q. What do you think is the most common vector through which each of these threats is delivered: Employees handling illegal or inappropriate material

We asked about both Illegal material in general and CSAM in particular. When asked what the most common vector was for CSAM incidents on their organisations devices, our respondents cited a range of options with none accounting for more than a quarter of the responses and no single consensus about what the most common vector is. 23% said that internet browsing was the most common vector for CSAM in their experience, whilst second was laptops in general with 19% of the responses. Amongst smaller firms, the most common vector was in fact laptops and browsers and live streamed content on 15% and 14% respectively.

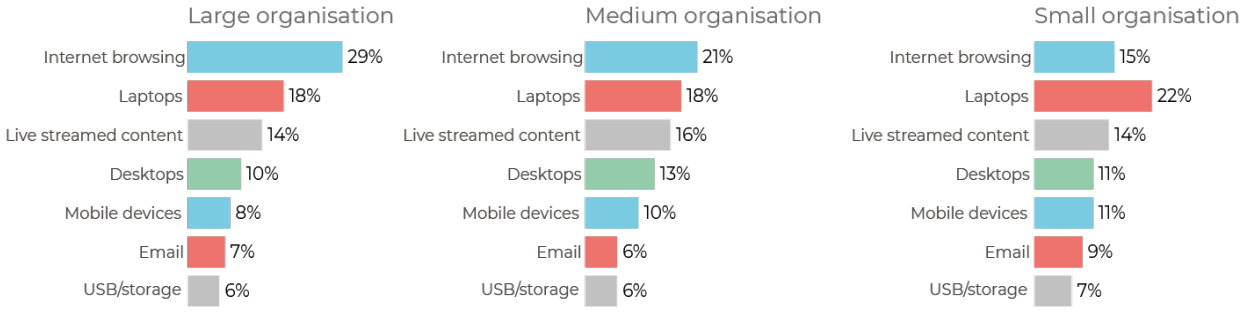
Mobile devices account for about 1 in 10 responses when we asked about the most common vector for CSAM (9% overall, 8% in the largest companies and 11% in the smallest). Desktops accounted for a very similar number of responses (11% overall, 10% in the largest companies and 11% in the smallest).

USB/storage devices generally and email account for a significant chunk of the remaining responses.

22%

OF SMALL ORGANISATIONS SAY THAT LAPTOPS ARE THE MOST COMMON VECTOR FOR CSAM IN THEIR EXPERIENCE

SMALLER ORGANISATIONS ARE MORE VULNERABLE TO STATIC DEVICES AND LESS VULNERABLE TO INTERNET SOURCES



Q. What do you think is the most common vector through which each of these threats is delivered: Employees handling illegal or inappropriate material

10

IT Professionals agree on some holes in their current armor against CSAM

54%

SAY THAT THEIR ORGANISATION RESPONDS TOO LATE TO THREATS

Despite saying overwhelmingly that they and their organisations take the threat of CSAM seriously, we were able to find widespread agreement on how our IT professionals may be coming up short at the moment. There was most agreement with the idea that filtering URLs for CSAM wasn't enough (73% agreed), followed by the idea that the dark web has made it easier for employees to access CSAM undetected.

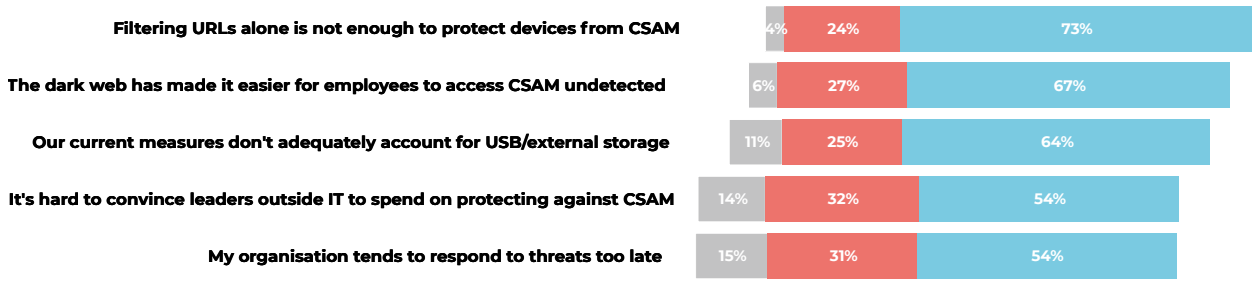
There was strong agreement also with the idea that current measures that are in place do not adequately account for the presence of USB/ external storage. Almost 1 in 3 strongly agreed with that statement.

WHEN ASKED IF THEIR ORGANISATION RESPONDS TOO LATE TO THREATS MOST IT PROFESSIONALS AGREE

Please say whether you agree or disagree with the following - My organization tends to respond to threats too late and only after they have happened

The final two issues that we picked up in the survey were the difficulty in persuading leaders outside of IT to spend on protection and the sluggish nature of many responses to the threats faced (54% agreed with both).

IT PROFESSIONALS AGREE THAT THERE ARE SOME CRUCIAL HOLES IN THEIR CURRENT DEFENCES AGAINST CSAM



Q. Please say whether you agree or disagree with the following...

73% **SAY THAT FILTERING URLS ON ITS OWN IS NOT ENOUGH TO PROTECT DEVICES FROM CSAM**

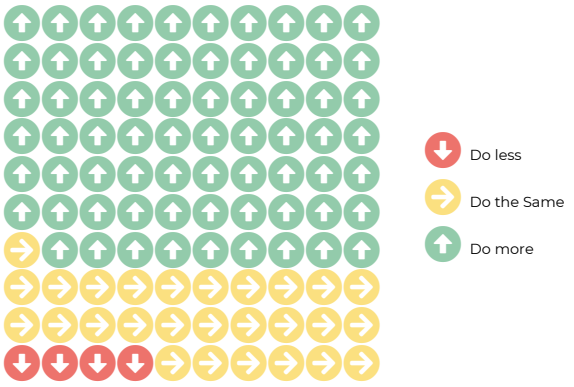
11

There is a near unanimous view that more action is necessary by multiple parties, not least the industry itself

69%

OF IT PROFESSIONALS THINK THEIR ORGANISATION SHOULD DO MORE TO TACKLE CSAM

IT PROFESSIONALS WANT THEIR ORGANISATIONS TO DO MORE TO TACKLE CSAM

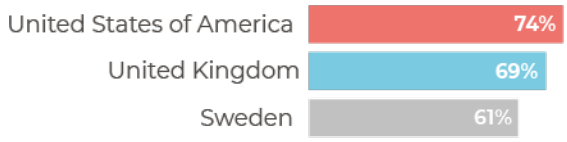


Q. Please say whether you think the following organisations should do more or less to tackle CSAM: My organisation

Almost all IT professionals want to see the organisations they work for do more to tackle CSAM. 69% of IT professionals think their organisation should do more to tackle CSAM and only 27% think they should carry on as they are. The feeling was strongest amongst the most senior executives – 76% of the C-suite IT professionals we spoke to said that they wanted their organisations to do more to tackle CSAM. Amongst Directors and Managers the feeling was slightly less widely held, but still attracted support from a large majority of respondents (64% amongst Directors and 61% amongst IT Managers).

The feeling that more should be done to counter CSAM also spread well beyond the organisations that our respondents in IT worked for. When asked whether the government should do more, 75% said it should and 19% said it should continue to do the same amount. The feeling was most widely held in the US, where 79% said the government should do more and only 5% that they should do less.

IT PROFESSIONALS ALSO WANT THEIR GOVERNMENTS TO DO MORE



Q. Please say whether you think the following should do more or less to tackle CSAM: The government

There was also a feeling that ISPs could be doing more, although to a slightly lower degree. 73% said that ISPs should do more to combat CSAM and 21% said they should carry on as they are.

The IT industry in general fared similarly with 78%, saying they should do more along with social media companies, who 76% of respondents said should do more.

+74%

THE NET FIGURE IN THE US FOR THOSE SAYING THE GOVERNMENT SHOULD DO MORE TO TACKLE CSAM

12

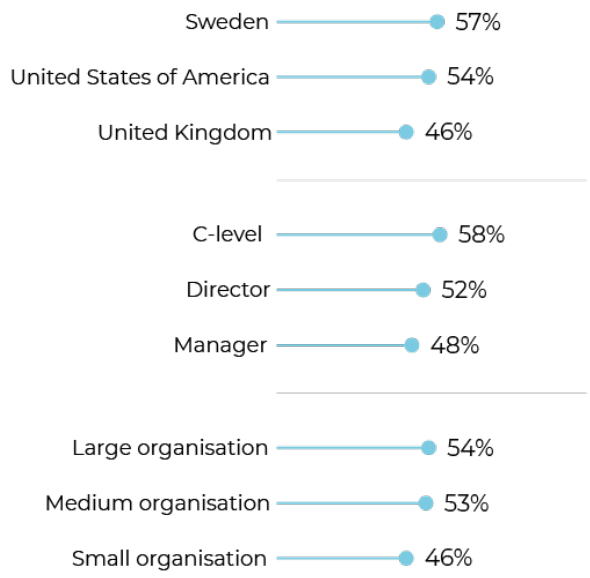
Almost all IT professionals open to considering specific protection against CSAM

Perhaps in response to the impetus for their organisations to do more that we have found amongst senior IT professionals, almost all of those that we spoke to would definitely consider or might consider purchasing specific forms of protection against CSAM in their organisations. When we asked about software to protect against CSAM in general, 89% of our respondents said that they were considering it in some form.

When we asked specifically about proactive software that scans for CSAM, 91% of all those we spoke to were considering it in some form – over half (52%) definitely would consider it and another 37% might consider it.

The C-suite are the most open to considering, with 58% saying they definitely would. Larger organisations are also more likely to consider purchasing specific protection with 54% saying the definitely would consider doing so.

A MAJORITY OF IT PROFESSIONALS DEFINITELY ARE CONSIDERING PROACTIVE DETECTION AGAINST CSAM



Q. For Protection against CSAM generally please say whether your organization would consider purchasing it or not

"My experience is that companies have control measures put in place to prevent a breach of copyright laws, but they don't have the same level of protection to ensure that illegal material, such as child sexual abuse material, isn't used on company devices. While there is a high awareness of the problem, IT and Business Managers don't always want to acknowledge the issue could be within their own organisations due to fears and concerns with the perceived complexity of how best to deal child sexual abuse material. I have heard stories of companies that discover CSAM on their networks and with fear of the police taking all devices, they just deleted the imagery and terminated the employment contract. The problem with this approach is that the victims of the CSAM are being ignored and the perpetrator is free to get a new job elsewhere and to continue on with their activity. Companies need to better understand their legal and moral obligations and how they should act in these types of situations. As IT professionals, we have a responsibility to act ethically and morally. In this case, it can have a direct impact on a child being saved or not."

Brian Honan, CEO of BH Consulting and globally renowned security expert

9 in 10

IT PROFESSIONALS WOULD CONSIDER PURCHASING SPECIFIC PROTECTION AGAINST CSAM

13

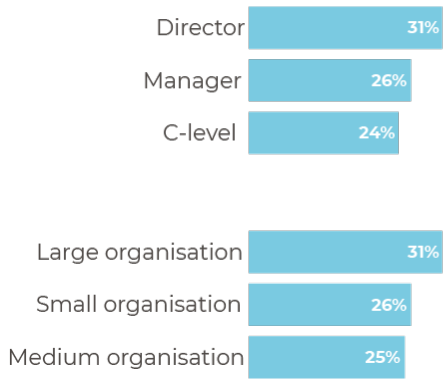
The purpose-driven case for tackling CSAM remains incredibly strong with IT professionals

The strongest arguments that our IT professional respondents find for taking action to keep CSAM off their systems are purpose-based. When asked to select the top two, rather than falling back on the benefits to their organisations directly, most selected arguments that relate to the broader purpose of their organisations and the contribution they can make to society in general. 50% of those interviewed said that the best reason to keep CSAM off their system was to help stop CSAM crime in the first place. 43% said that doing so helps safeguard children.

The third most selected argument involves the reduction in other threats that may also be associated with CSAM. 27% of senior IT professionals said that the best argument was the reduction in viruses and other threats.

Notably, those at larger organisations are more persuaded by this argument, as are those at director level in their organisations.

DIRECTORS AND THOSE AT LARGE ORGANISATIONS ARE MOST PERSUADED BY THE ARGUMENT THAT STOPPING CSAM STOPS OTHER THREATS



Q. Thinking about the risk posed by CSAM which of the following are the best arguments for taking action to keep it off your company's assets? – Reduces the risk of bringing in other threats

50%

SAY THAT THE BEST REASON TO KEEP CSAM OFF COMPANY ASSETS IS TO HELP STOP CSAM CRIME

THE TWO BEST ARGUMENTS FOR KEEPING CSAM OFF IT SYSTEMS ARE BOTH HEAVILY PURPOSE-DRIVEN

Q. Thinking about the risk posed by CSAM which of the following are the best arguments for taking action to keep it off your company's assets? (Select the top two)