vb 2019 LONDON 2 – 4 October 2019

WHY COMPANIES NEED TO FOCUS ON A PROBLEM THEY DON'T KNOW THEY HAVE

Richard Matti & Anna Creutz
NetClean Technologies, Sweden

{richard.matti; anna.creutz}@netclean.com

ABSTRACT

There is a type of crime, breach of company policy, misuse of company assets and security threat that is often overlooked: as one in 500 employees use their work computer to handle child sexual abuse material. This crime and misuse of company assets is something that businesses and organizations need to address as a security and brand protection issue. It also needs to be addressed in order for organizations to remain ethical corporate citizens.

Individuals who consume child sexual abuse material on their work computer exhibit risk-taking behaviours and are at risk of being blackmailed. Their actions also put companies at risk of multiple types of IT attacks.

Taking action to stop child sexual abuse material from being accessed or distributed using company assets is a concrete and tangible way for businesses to act on and comply with the UN's Sustainable Development Goals.

Organizations are in a unique position to stop this crime from being committed with the use of their devices. In doing so, organizations will act as ethical corporate citizens and safeguard children, while adhering to legislation and policy compliance, managing security risks, and protecting the company's IT environment, its employees and its brand reputation.

RESEARCH BASIS FOR THIS PAPER

Over the last four years, *NetClean* has produced the *NetClean Report* – a report on child sexual abuse crime. It is largely informed by a survey conducted among law enforcement professionals working with child sexual abuse crime in more than 30 countries across the world. The 2018 report also included an interview survey with businesses that detect child sexual abuse material on work computers in their IT environment. Together, those businesses represented nearly 270,000 work computers with software installed to detect child sexual abuse material. This paper is based on findings from the 2016 [1], 2017 [2] and 2018 [3] reports.

A SECURITY THREAT THAT IS OFTEN OVERLOOKED

According to advisory company *Gartner*, the total spending on information security products and services is predicted to reach more than US$124 billion in 2019 [4]. The top three drivers for security spending are security risks, followed by business needs and industry changes.

Security risks are often immediately associated with threats from outside the organization. However, many threats also come from the inside. According to ENISA (European Union Agency for

Cybersecurity) in its Threat Landscape Report 2018 [5], approximately 54% more organizations recorded a growth of insider threats in 2018 and approximately 48% of the companies still perceive the detection of insider threats as a great challenge for their security team. According to the report, the three most common types of insider threat are:

- the malicious insider, who acts intentionally
- the negligent insider, who is just sloppy or does not comply with the organization's policies and security instructions
- the compromised insider, who acts unintentionally as the means for the true attacker.

An example of the scale and cost of insider threats are data breaches. According to *Verizon*'s 2019 Data Breach Investigations Report [6], more than one third (34%) of attacks involved internal actors, and in 2018 the Ponemon Institute reported that data breaches cost companies an average of US$3.86 million globally [7].

Crime in the workplace and misuse of company assets

There is a type of insider cybercrime, breach of company policy, misuse of company assets and security threat that is both intentional and often overlooked. The *NetClean Report 2018* showed that as many as one in 500 employees use their work computer to handle child sexual abuse material [3].

This is a crime that most individuals and businesses probably do not consider a possible threat. Yet, apart from being a very serious crime committed using company assets, and a breach of company policy, there are also many security risks connected to this illicit conduct. A person handling child sexual abuse material on a work computer is engaging in risky behaviour. Visiting unregulated websites and media, or using unverified USB sticks, creates a risk of multiple types of cyber attacks. Further, depending on the position of the individual within the company, there is a risk of blackmail, and there is a risk of damage to brand reputation.

This is a crime not often talked about in the context of business and the workplace. Therefore it is important to understand some basic facts about it in order to understand the risks that it represents to private industry as well as to public sector organizations. The following is a brief overview of the crime and why it is important to address it both from a business and a societal point of view.

DIGITALIZATION AND CHILD SEXUAL ABUSE CRIME

Digitalization, connectivity and child sexual abuse material

Whilst physical child sexual abuse is a human crime, the consumption and distribution of child sexual abuse material is a technology-driven crime. Increasing digitalization and connectivity, global Internet penetration, and easy access to devices such as laptops, smartphones, tablets and thumb drives has led to countless positive developments and opportunities. However, as is always the case, technology can be used for both good and bad. The four *NetClean* reports together show that the volume of child sexual abuse material available and shared over the Internet is increasing, and that the material is distributed through all possible channels. It is downloaded, consumed and distributed at all times of the day and week.

Circulation

The volume of child sexual abuse material in circulation is staggering and increasing. Three quarters of the police officers surveyed in the *NetClean Report 2017* [2] reported an increasing and more demanding workload, primarily due to more investigations and more data. They also reported that their biggest investigations can contain up to 100 million images, of which 10 million are child sexual abuse images. In the 2016 report [1], Homeland Security Investigations in the US stated that their average case contained 6TB of data that needs to be analysed to find the pertinent material, and INTERPOL shared that they had handled a gigantic seizure with 40TB of child sexual abuse material.

Also in the 2016 report, the Swedish Internet service provider (ISP) *Tele2* shared that it blocked 500,000 searches for known websites showcasing child sexual abuse material every month.

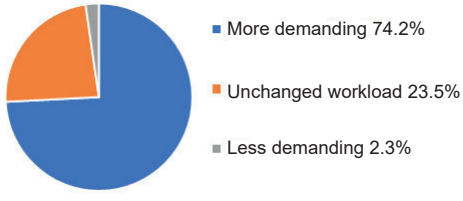

Figure 1: Reported change in workload in 2016 for law enforcement professionals working with child sexual abuse investigations [2].

Distribution

Peer-to-peer (P2P) sharing is the most common way for child sexual abuse to be distributed (it was mentioned by 90.4% of the surveyed police officers), followed by Darknet/TOR (43%), social media platforms (37.9%), cloud-based services (34.9%), instant messaging (34.9%), email (21.3%), websites on the open Internet (17.3%) and physical mail (6.3%) [2].

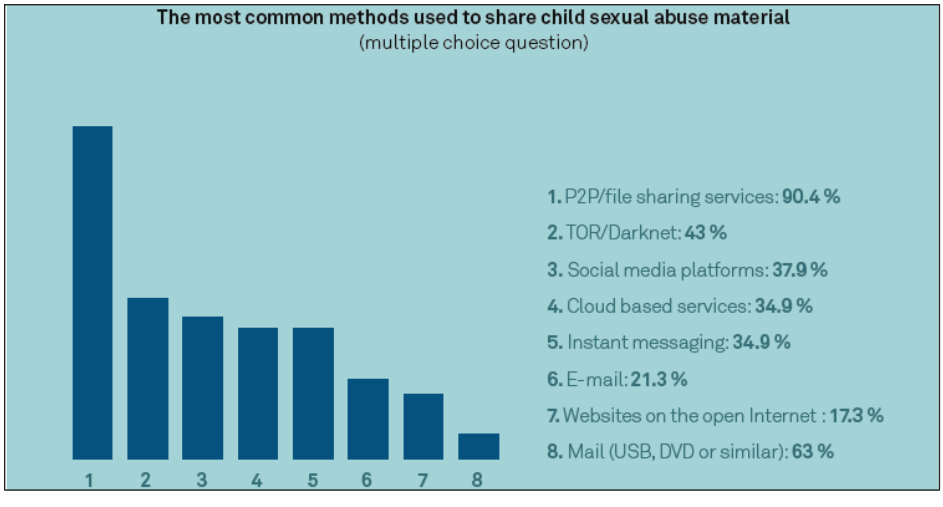

Figure 2: The most common methods used to share child sexual abuse material [1].

On social media platforms material is most commonly shared (or at least most commonly discovered) on the social media platforms that gather the most people, such as *Kik*, *Facebook*, *Snapchat*, *Twitter*, *Instagram*, etc.

Consumption patterns

Data from ISPs from around the world show that searches for websites containing child sexual abuse material take place every day of the week, 24 hours a day. There is a peak in searches on Sundays, and also between 10pm and 1am.

The pattern for child sexual abuse material being handled on work computers is similar. It is most common for employees to use their work computer to handle such material outside of working hours, during evenings, holidays and work trips.

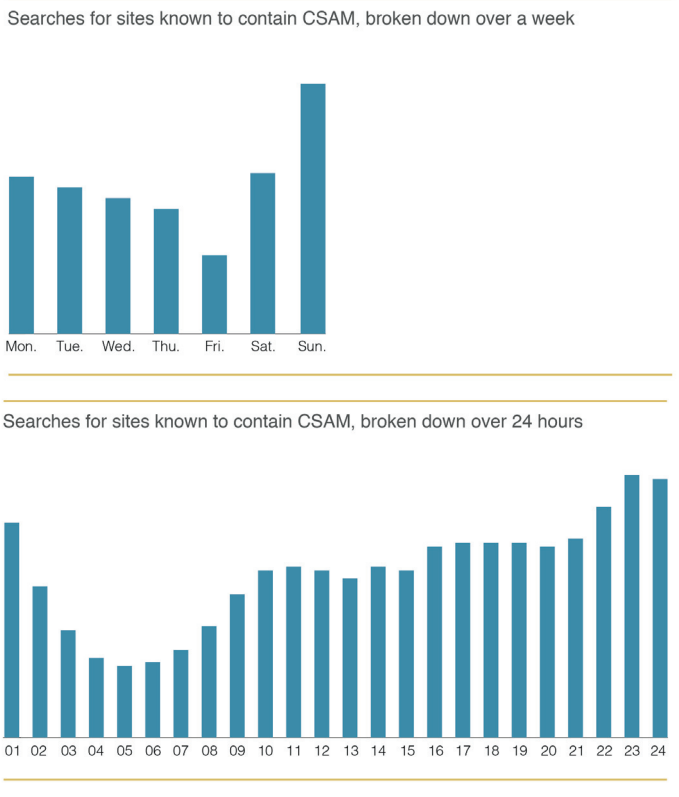

Figure 3: Searches for sites known to contain child sexual abuse material (CSAM). Data extrapolated through technology that blocks child sexual abuse material in ISP networks [2].

The challenge of anonymization technologies

One of the major challenges in finding child sexual abuse material, as well as identifying and safeguarding children, is encryption and anonymization technologies such as TOR, VPN and proxy

servers. Encryption is a challenge as it is impossible to detect and stop child sexual abuse images in encrypted traffic. Anonymization technologies are a challenge because they disguise the identity of the user. In the *NetClean Report 2016*, more than one third of the surveyed police officers pointed to encryption and anonymization as one of the major challenges and an increasing trend [1].

THE CONSUMER OF CHILD SEXUAL ABUSE MATERIAL

There is no typical offender

It is easy to buy into the myth of the consumer of child sexual abuse material as the man in the raincoat lurking around a primary school, or as the socially awkward outsider. However, research shows that contrary to this perception there is no typical offender.

Apart from the large majority being men, the *NetClean Report 2017* showed that consumers of child sexual abuse material are most commonly between 20 and 50 years of age, which mirrors the general demographics of the USA, Europe and Australia, where the majority of the survey respondents are based [2]. The offenders are often in a relationship, but may not be, and most of them have children in their proximity in some way. This could be through their own family (their own children or their partner's children), extended family, friends/neighbours or similar, recreational activities or professional life. The most common way for offenders to have access to children is through family or extended family.

Nearly two thirds of the police officers surveyed said that offenders in their investigations are usually in employment. Offenders come from all professions, all levels within organizations, and all segments of society.

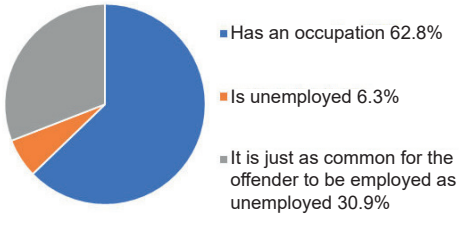

Figure 4: Employment status of suspects who are being investigated for viewing or disseminating child sexual abuse material, as reported by law enforcement professionals.

Correlation between consumption of child sexual abuse material and hands-on child sexual abuse

Although there is a debate as to the exact number (hence the wide span) there is a 30 to 85 per cent correlation between viewing child sexual abuse material and committing hands-on/physical child sexual abuse [1].

When police officers were asked what is the most common way for a hands-on offender to get in contact with their victims, they answered family (72,5%), extended family (65%), Internet (51,3%), friends/neighbours (48,1%), recreational activities (33,8%) and professional life (20,3%) [2].

THE IMPORTANCE OF ACTING AGAINST CHILD SEXUAL ABUSE MATERIAL

Child sexual abuse material – crime scene and re-victimization

Child sexual abuse material goes far beyond just being an image or a video. It is a documented crime scene of a serious crime that has an extensive and long-term negative impact on the quality of life of the victim depicted. As terrible as the image is, it also presents the opportunity to identify both the child and the perpetrator to ensure that the child is safeguarded. This makes every detected image important.

The spread of child sexual abuse images also causes re-victimization. A Swedish study showed that children who have been sexually abused are even more traumatized if they know that the abuse has been documented. The trauma is further accelerated if they also know that the images have been disseminated online [8]. As a result, it is important that every measure is taken to limit the spread of child sexual abuse material.

Child sexual abuse crime and misuse of company assets

As mentioned earlier in this paper, one in 500 employees use their work computer to handle child sexual abuse material, most commonly outside of working hours, during evenings, holidays and work trips. The material is also sometimes handled during down-time in the workplace, e.g. during lunch hours or early in the morning.

1 / 500

The 2018 *NetClean* report showed that the most common method for accessing child sexual abuse material on a work computer is via a privately owned USB stick. Most frequently the person has turned off the Wi-Fi and disconnected the computer from the network before connecting the USB stick. The average software 'alert' for child sexual abuse material is usually for two to five images, or sometimes up to 20 images. However, when the computer is examined more closely, more material is usually found. And when detection of images results in a house search, this also frequently unearths more child sexual abuse material in the home.

Roughly half of the surveyed businesses stated that they frequently find large amounts of adult pornography on the computers that have been used to handle child sexual abuse material. Some companies also reported finding torrent clients on the computers, and they reported instances where they found child sexual abuse material stored together with sensitive business information.

The surveyed businesses reported that the individuals in the organizations who were found to consume child sexual abuse material were from all professions and all levels within the organizations. The alerts were biased towards individuals with higher academic achievement; however this was believed to be because they more often have work computers, in many cases laptops. Many of the businesses also stated that there is a certain bias towards employees who have a background in technology. They were exclusively male, ranging from their 20s to pension-age, but most commonly between 30 and 50 years of age. The organizations also reported that it was slightly more common for those individuals to be in a relationship and to have children [3].

To summarize some of the findings that pertain to businesses, one in 500 work computers are used to handle child sexual abuse material. The workplace is a risk environment as nearly two thirds of surveyed police officers state that the offenders in their investigations are usually in employment.

Consumers of child sexual abuse material come from all professions, all levels within organizations, and all segments of society.

It might seem strange that people are willing to risk using their work computers to commit this type of crime. The risk is probably negated by the fact that the work computer is perceived as private. It is not shared with anyone else – neither family members nor colleagues – and it is often a laptop.

A SECURITY RISK, POLICY COMPLIANCE, BRAND PROTECTION AND SUSTAINABILITY ISSUE

The workplace as a risk environment

As the research shows, the workplace is a risk environment for child sexual abuse crime and consumption of child sexual abuse material, both from a business and cybersecurity perspective, and from a sustainability and societal point of view. Below is more information about risks to businesses and the impact on society in general.

Addressing the misuse of company assets and the crime of handling child sexual abuse material in the workplace involves adhering to legislation and policy compliance, as well as managing security risks. It is also a way of protecting both employees and brand reputation, acting as an ethical corporate citizen and complying with the UN's Sustainable Development Goals.

Adhering to legislation and company policy

Prevent crime in the workplace and protect company assets

Accessing and handling child sexual abuse material on a work computer is a serious crime committed using company assets. Therefore, safeguarding the organization's computers and other devices so that they are not used to commit crimes is a legal issue. It is important both to work to prevent crimes from occurring and to enable the employer to detect crimes if they do occur.

Policy compliance

Most organizations have a policy that states either explicitly or inexplicitly that it is unacceptable to view or download illegal material such as child sexual abuse material on company assets, whether it be during working hours or in the employee's spare time. Handling child sexual abuse material on a work computer is therefore not only a serious crime, but also a breach of policy.

Managing security risks

Risk-taking behaviour

A person who views or downloads child sexual abuse material is engaging in risky behaviour and represents a tangible security risk to the company. It is reasonable to assume that a person who is willing to engage in this type of risky behaviour might break other laws or flaunt company policies. As mentioned earlier, roughly half of the businesses interviewed in the *NetClean Report 2018* stated that when they find that child sexual abuse material has been handled on a work computer, they frequently also find large amounts of adult pornography on the same computer and sometimes sensitive business information stored together with the illicit material [3].

Risking multiple types of cyber attacks

Employees visiting unregulated websites and media incur the risk that their visit can be traced back to the organization. This, in turn, increases the risk of other attacks such as DDoS-type cyber attacks, spam and other threats. There is also a risk that the person will download malware when downloading illicit or unwanted material, and the same thing can happen with unverified USB sticks. Some of the interviewed businesses and organizations in the *NetClean Report 2018* reported that they had found torrent clients on the affected computers [3].

Blackmail

People who engage with this type of illicit material are vulnerable to both threats and blackmail. This is a big security risk if the individual has a prominent position in the organization or if they handle sensitive material that they can be blackmailed to divulge.

Protecting both employees and company brand

Protecting employees

Another risk is that other employees, in particular those in IT roles, will be subjected to the illicit material left by other individuals within the organization on company devices and networks. Being subjected to child sexual abuse material can cause trauma, especially if repeated several times. If the organization fails to actively detect the material, the only way of discovering it is by other employees in the organization. By protecting the organization against child sexual abuse material, the employees are also safeguarded from the risk of being subjected to this offensive material.

Protecting and strengthening the company brand

By making sure that the company has done what it can to manage the risks and worked to protect the organization and its employees, the company brand is also protected. It is a proactive way of limiting the risk of a media crisis. It is also an employer branding initiative, which is often seen in a very positive light within the organization. There is evidence that taking action on societal issues strengthens public opinion of the company brand. A study by *Gartner* showed that 48% of the general population expect companies to take a public stand on social issues regardless of the issue's relevance to corporate objectives. The research showed that not only do stakeholders respond to companies taking a stance, they also respond in a positive manner three out of four times [9].

Ethical corporate citizenship and the broader societal perspective

UN's Sustainable Development Goals

It has become increasingly important for businesses to act as ethical corporate citizens and take corporate social responsibility for stakeholders outside of immediate core business. The UN's Sustainable Development Goals and Agenda 2030 [10] articulates this even more clearly and puts pressure on businesses to take action on key global issues: '16.2 – end abuse, exploitation, trafficking and all forms of violence and torture against children'.

Taking action to stop child sexual abuse material from being accessed or distributed with the help of company assets is a concrete and very tangible way for businesses to act on and comply with the sustainable development goals.

The safeguarding of children

By detecting child sexual abuse material in the workplace, businesses assist law enforcement in locating individuals with a sexual interest in children, and ultimately help rescue and safeguard children, providing them with a brighter future.

TECHNOLOGIES TO STOP CHILD SEXUAL ABUSE MATERIAL

Law enforcement, policy makers, civil society, NGOs, academic researchers, public sector organizations and private industry all work to try to solve this issue and protect children from harm. However, much more can be done. One of the first steps is to use available and effective technology. There are a number of technologies available that are used to address the problem, e.g. crawlers, blocking technologies, filter technologies, artificial intelligence, robust hashing technologies and binary hashing technologies.

Crawlers are used by NGOs to find child sexual abuse material. They then send a notice to the web host to take down the material. Blocking technologies are used by ISPs to block known child sexual abuse material in their networks (however this only works on unencrypted traffic). Artificial intelligence applications are still in their early development in this context but are developing fast and will soon be possible in use in a number of different contexts to aid the existing technologies.

The technologies available to businesses to block or detect child sexual abuse material in their own IT environments are filter technologies and hashing technologies.

Each of the different technologies has strengths and limitations, depending on the context in which they are used. More information on the different technologies and how they work is gathered at [11].

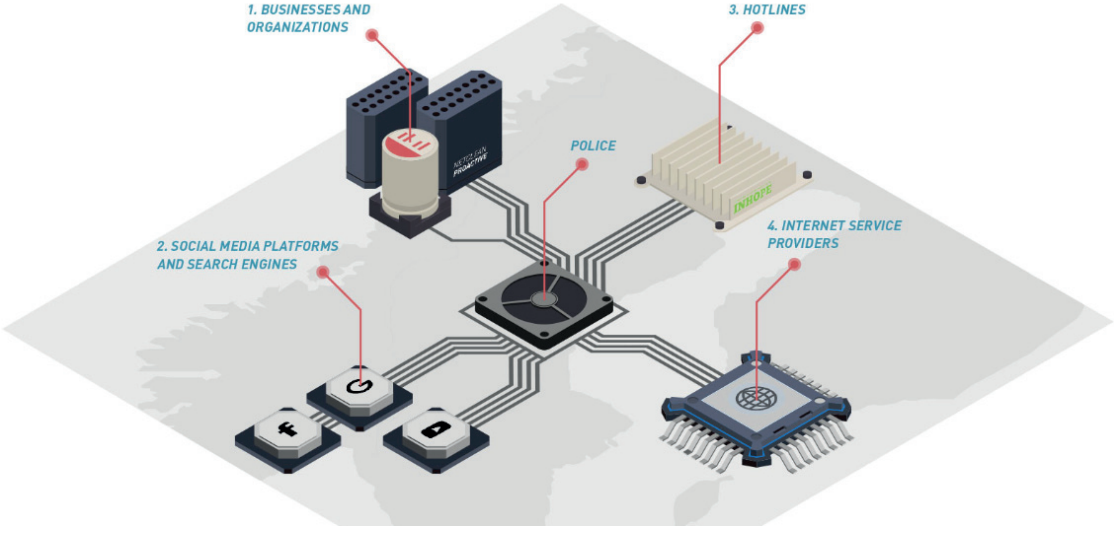

Figure 5: Technologies to stop child sexual abuse material.

Using web filters to block child sexual abuse material

Filter technologies are primarily used to manage security threats such as service disruptions, ransomware, phishing, etc. While they can also be used to block websites known to contain child sexual abuse material, they have several weaknesses in the context of blocking such material. The first is that they are only as effective as the intelligence put into the solutions – the lists of domains or URLs known to contain harmful material. Keeping those lists up to date requires a lot of work and continuous updates, and as the primary focus of these solutions is other types of threats, child sexual abuse material unfortunately comes a long way down the list. The other weakness is that they only block known URLs or domain names, thus missing all other ways of distributing the material (such as P2P, Darknet, social media platforms, or when someone uses a USB stick to access the material). Therefore, although using web filters is helpful, it is not enough and does not protect the organization and its assets against child sexual abuse material [12].

Using hashing technology to detect child sexual abuse material

In addition to using filter solutions, businesses can install software designed specifically to detect child sexual abuse material. The software works similarly to an anti-virus programme, but instead detects when child sexual abuse material is handled on a computer. To identify the images, hashing technology is used [13]. When law enforcement investigates child sexual abuse cases, they produce a hash, a unique 'digital fingerprint', of each image. These hashes are then added to a database, which is used in the software to match against images handled on the work computer. This means that the software installed only detects child sexual abuse material that has already been classified by law enforcement. At detection, an alert is sent to designated individuals within the organization who handle the incident and report it to the police.

CASE STUDY: PROTECTING BUSINESS IT ENVIRONMENT CAN LEAD TO THE SAFEGUARDING OF CHILDREN

This is an actual case from an organization in Sweden that uses software that detects child sexual abuse material on work computers.

In 2013, the organization received an alert that one of their employees had used a USB stick to access child sexual abuse material on his work computer. The alert contained five files, with images that were classified as child sexual abuse material, but not of the most severe category. The images were verified and the police initiated an investigation. A search of both the workplace and the individual's home was planned and later executed.

Meanwhile, the employee had been away from the office for a week. When he returned, the computer sent alerts for four more instances that had occurred while the individual was using the computer away from the office. The alerts were from different times of the day and included a larger number of files.

During the house search the suspect's computer and other devices were seized, including his mobile phone. When the police examined the contents of the mobile phone, they found newly produced material: images and videos depicting the sexual abuse of two young children living with the suspect – his partner's children.

Further investigation revealed that the suspect was acting in collaboration with another man, who directed the sexual abuse of the children, which was live-streamed to him via *Skype*.

As a result of the workplace detection, the police investigation and the judicial process, both men were sentenced to jail and the children were safeguarded.

CONCLUSION

The distribution and consumption of child sexual abuse material is a technology-driven crime, furthered by increasing digitalization and connectivity. The volume of material available and shared over the Internet is increasing, and the material is distributed through all possible channels, at all times of the day and throughout the week. There is no typical offender: the consumer of child sexual abuse material is usually a man, but can be of any age, profession, and from any level of organization or segment of society. As there is a correlation between consuming child sexual abuse material and committing hands-on sexual abuse, detecting child sexual abuse material also makes it possible to identify and safeguard children.

Individuals who consume child sexual abuse material on their work computer engage in risky behaviour and are at risk of being blackmailed. Their actions also put the company at risk for multiple types of IT attacks. While one in 500 work computers are used to handle child sexual abuse material, this is a risk often overlooked, and there is an over estimation of the capability of web filters to handle this problem. Where many other technologies fall short, detection on work computers is an effective way to circumvent the problems presented by encryption and anonymization technologies (such as the Darknet).

Organizations are in a unique position to act on this issue and stop crimes from being committed with the use of company devices. The installation of software that detects child sexual abuse material on work computers should be a hygiene factor for ethical businesses. It has the dual benefit for the organization of acting as an ethical corporate citizen and safeguarding children, as well as adhering to legislation and policy compliance, managing security risks, and protecting the company's IT environment, its employees and its brand reputation.

REFERENCES

[1] The NetClean Report 2016. NetClean. https://www.netclean.com/the-netclean-report-2016/.

[2] The NetClean Report 2017. NetClean. https://www.netclean.com/netclean-report-2017/.

[3] The NetClean Report 2018. NetClean. https://www.netclean.com/netclean-report-2018/.

[4] Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019. Gartner. https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019.

[5] ENISA Threat Landscape Report 2018. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

[6] 2019 Data Breach Investigations Report. Verizon. https://enterprise.verizon.com/resources/reports/dbir/.

[7] Ponemon Institute Cost of a Data Breach Study 2018. IBM Security Intelligence. https://securityintelligence.com/series/ponemon-institute-cost-of-a-data-breach-2018/.

[8] Jonsson, L.; Svedin, C-L. (2017) Barn utsatta för sexuella övergrepp på nätet [translation: Child victims of online sexual abuse]. http://www.allmannabarnhuset.se/wp-content/uploads/2017/02/Rapport-Sexuella-%C3%B6vergrepp-p%C3%A5-n%C3%A4tet..pdf.

[9] Navigating New Stakeholder Expectations: greater clarity on engaging in contentious social issues. Gartner. https://www.gartner.com/en/corporate-communications/trends/navigating-stakeholder-expectations.

[10] 2030 Agenda for Sustainable Development. United Nations. https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E.

[11] Technologies to stop child sexual abuse material. NetClean. https://www.netclean.com/technical-model-national-response/.

[12] Can filter technologies help to stop child sexual abuse material? NetClean. https://www.netclean.com/technical-model-national-response/filter-technologies/.

[13] Hash values – fingerprinting child sexual abuse material. NetClean. https://www.netclean.com/technical-model-national-response/hash-values-fingerprinting-csam/.