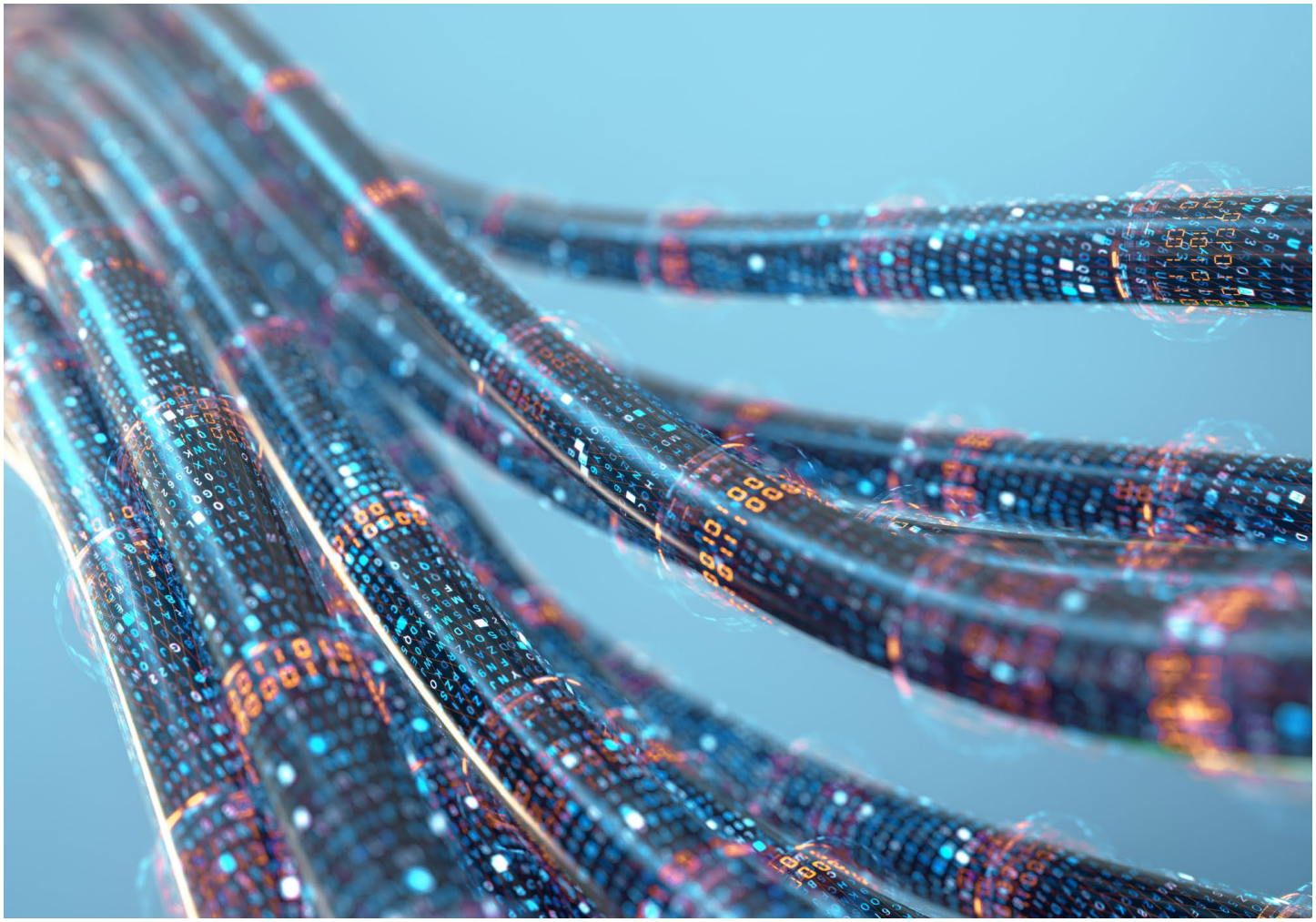
WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Shaping the Future of Cybersecurity and Digital Trust

Cybercrime Prevention
Principles for Internet Service Providers

January 2020



World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland
Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744
Email: contact@weforum.org
www.weforum.org

Contents

Preface

Alois Zwinggi
Head of the Platform for Shaping the Future of Cybersecurity and Digital Trust
World Economic Forum

Since established in March 2018, the World Economic Forum Platform for Shaping the Future of Cybersecurity and Digital Trust has focused on building a platform to facilitate the development of a community of public- and private-sector leaders dedicated to identifying the challenges that the unprecedented evolution of technology is posing, sharing insights, building the required capabilities and shaping the global processes needed to ensure security and trust in the digital space.

With its partners, the Forum works to highlight and promote measures and policies pioneered in specific organizations or countries that have proven able to generate impact in mitigating cybersecurity risks. One community in particular can have a systemic impact on the global landscape – that is organizations that provide and manage the networks across which communications take place. These organisations have the ability to address some of the most common cyber threats at their source to protect their consumers. Many cyberattacks occur by exploiting relatively simple weaknesses and can increasingly be detected and mitigated before they reach potential victims.

The World Economic Forum and its global partners have developed this set of best practice principles for Internet Service Providers (ISPs)[1] and other organizations involved in supporting or providing online communications. The aim is to make it substantially more difficult for criminals operating online to benefit from unlawful gains at the expense of innocent members of the public.

The World Economic Forum Platform for Cybersecurity and Digital Trust seeks to drive collaboration across public and private sectors to make the “barrier to entry” for attacks far more robust and the penalties for attack much stronger. The “pain” of being caught must outweigh the potential gain. Through our platform, the World Economic Forum can use its unique position to generate broader cooperation across public- and private-sector stakeholders at the most senior levels to lead a fundamental change in approach that shifts the very economics of cyberattacks by deterring criminals from their attempts to undermine the digital economy.

Foreword

Kevin Brown
Managing Director, BT Security
BT Group
United Kingdom

Philip Reitinger
President and CEO
Global Cyber Alliance
USA

A number of studies and surveys describe the impact of cybercrime around the world and attempt to quantify the scale of the threat. The financial impact of cybercrime on businesses and individuals continues to rise, with Accenture estimating that the cost of cybercrime to businesses has risen by 72% over the past five years.[2]

The key principles set out here seek to capitalize on the fact that for the most part, profit margins for individual attacks are small.[3] Any activity which can be taken that raises the cost of conducting cybercrime or has an impact on profits therefore impacts the return on investment and criminals' motivation to carry out attacks in the first place. Widespread adoption of relatively straightforward, industry-standard practices and protocols such as those included in these principles will have a measurable effect on the harm caused by cyberattack. Implementation will raise the barrier to entry for adversaries to conduct attacks and thereby reduce the impact of a large number of relatively common online crimes.

ISPs and other providers of communication services and infrastructure hold a unique position in the online ecosystem. The principles herein should help to facilitate discussion at the most senior levels of these organizations regarding their posture towards prevention and detection of cybercrime, as well as the extent to which such organizations are collaborating with their peers for the common good.

These principles can be used to raise minimum standards across the online ecosystem and to raise the profile of these issues within the telecommunications sector and beyond. Through workshops and discussions on these principles, the emerging consensus has been that they should be used to facilitate discussion and collaboration between the private sector, governments and regulators. While the organizations that support the online ecosystem through their infrastructure and services can play a role in stopping cybercrime at its root, the public sector and national and global regulatory bodies also have a role in supporting these efforts. We will focus on this area of public -private collaboration as a second phase of this work, to encourage the development of policy frameworks that can incentivize adoption of responsible behaviours.

Ultimately, by working collaboratively, ISPs will be better equipped to protect their customers and defend their own networks than they can by working alone. The contributors to this document believe that it is the responsibility of ISPs to take action and not knowingly allow malicious activity that they have identified to reach their customers.

Executive Summary

Four key principles are proposed for implementation by ISPs to address malicious activities being carried out online that impact a high number of consumers. Each principle is considered from the perspective of the challenges it seeks to address and proposes demonstrable evidence from service providers on the benefits of implementation. More technical detail on how each principle could be implemented is also provided in recommendations linked to each principle. An annex details known information sharing forums which ISPs should consider joining.

Areas for further work are also proposed, in particular the consideration of how governments and the public sector might do more to establish appropriate policy frameworks that would provide the best incentives to ISPs to act securely. Key areas of focus for a second phase of work will include defining roles and responsibilities for securing online ecosystems while ensuring that lines of accountability are clear; ensuring that actions taken are transparent and uphold principles relating to maintaining an open internet; and work to define frameworks which incentivize adoption of best practice in a harmonized manner.

The best-practice principles are intentionally set at a high level to allow them to be easily understood by a senior, non-technical audience. Further details on implementation are provided in recommendations under each principle.

It is recommended that ISPs adopt the following key principles:

1. **Protect consumers by default from widespread cyberattacks and act collectively with peers to identify and respond to known threats**
2. **Take action to raise awareness and understanding of threats and support consumers in protecting themselves and their networks**
3. **Work more closely with manufacturers and vendors of hardware, software and infrastructure to increase minimum levels of security**
4. **Take action to shore up the security of routing and signalling to reinforce effective defence against attacks**

The intention here is not to provide technical guidance on protecting networks or critical infrastructure from external risks – these are dealt with in numerous other fora and guidance. This set of principles focuses on the more strategic actions that the ISPs that have collaborated on this work believe an ISP should be able to take for the purpose of protecting consumers from common online crimes, thereby helping to “clean up” the internet on the whole.

Incentives for Action and Expected Outcomes

There are a range of actors across the online ecosystem who could take action against high-volume online crimes. ISPs have a specific and instrumental role to play as carriers of internet traffic and in their consequently privileged position in being able to tackle head on some of the strategies deployed by cyber criminals.

These four principles may of course also apply to organizations that would not consider themselves as ISPs. The World Economic Forum and the partners involved in the development of these principles would encourage all organizations able to enact some, if not all, of these principles to do so.

The principles developed and advocated are based on the experience of ISPs globally that have focused their attention on protecting their customers from known malicious activity and have been able to evidence the benefits their application brings. The broad benefits of adopting more responsible behaviours include the following key outcomes:

- **Building trust in online services.**
  If ISPs are able to instil greater trust in their services, this should help to build the confidence of consumers and other service providers in the safety and reliability of the online environment. This in turn should help to boost economic activity and wider service offerings.
- **Freeing up networks from malicious activity increases profit margins.**
  A growing proportion of the internet is consumed with traffic that is malicious or fraudulent[4], and ISP infrastructure is commonly used to host botnets and other criminal activity. By reducing this overall volume while maintaining customer value and average revenue per customer helps to increase profit margins. In addition, in the falling price per user of the telecoms market it is important to continually increase the offering to maintain the price and margin level. Adding cybersecurity protection to the basic offering or as an optional extra saleable service maintains or even increases the average revenue per user (ARPU).
- **Contribution to the health of the national online ecosystem.**
  Many ISPs are a fundamental element of their national digital ecosystems and often categorized as critical national infrastructure. By helping their "home economy" they are demonstrate that they are acting responsibly, and therefore may help to build good relationships with the national regulators.
- **Reducing overheads of fraud and criminal complaints, detection and reporting.**
  Complaints of fraudulent or criminal abuse from customers cost ISPs money. One recent survey provided estimates showing that an average European ISP is likely to spend over 3 million Euros a year handling abuse-related complaints. Additional costs arise as a result of ISP law enforcement liaison officers or teams engaging lawful processes to remove criminal sites, which is often required to comply with regulations. Adopting high-level principles to help reduce malicious activity from reaching consumers may help to reduce this overhead, for example by addressing issues before they become a problem for consumers.
- **Corporate social responsibility (CSR).**
  Increasing activity to protect customers helps benefit consumers and the wider online ecosystem. It is "the right thing to do" and therefore can help to build towards the organization's CSR goals.
- **Reputational and brand advantages.**
  There are marketing advantages to be gained if an appropriate and recognized brand or endorsement is made in the security of a provider's services. This will allow consumers to make an informed choice between providers that have made an effort to improve the internet on the customer's behalf and those that have not.

ISPs have a unique opportunity to lead a values-based approach to the ways in which their technologies, services and infrastructure are used. In working together in a responsible manner, ISPs can help to support the use of technologies by society and contribute to the common good.

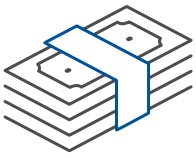
Context – Scale of the Threat

The most common threats facing ISPs and their customers are:

1. **Social engineering fraud** – this refers to the use of communications technology, generally email, to manipulate user behaviour and disclose confidential information, often for financial gain.

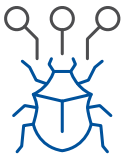
According to the 2019 Verizon Data Breach Report, **33%** of data breaches in 2018 included social attacks and **32%** involved phishing.[5]

Phishing and social engineering attacks are now experienced by **85%** of organizations.[6]

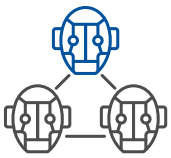


The FBI estimated a loss of over **$1billion** as a result of Business Email Compromise (BEC) fraud by US businesses and individuals in 2018.[7]

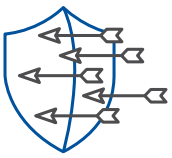
2. The **distribution and deployment of malware** for various purposes, in particular to support the operation of botnets.



Accenture analysis of nearly **1000** cyberattacks highlighted malware as the most frequent attack overall and, in many countries, the most expensive to resolve.[8]



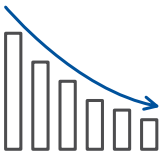
One banking botnet was used to steal more than **€36million** from 30,000 customers over a 90-day period.[9]



BT are blocking over **100million** attempted malware communications every month in order to keep their customers safe.

3. The deployment of various techniques to undermine naming and routing protocols, largely for the purpose of conducting **Denial of Service (DoS) attacks**.

DDos attacks can represent up to **25%** of a country`s total internet traffic when they are occurring.[10]



Research indicates that web-based attacks and DoS attacks are the main contributing factors to revenue loss.[11]

The average cost of downtime associated with DoS attacks in 2018 was **$221,836.80** per attack.[12]

Principle 1. **Protect consumers by default from widespread cyberattacks and act collectively with peers to identify and respond to known threats**

1.1 What challenge does this principle address?

ISPs can play a vital role as a first line of defence by identifying and helping prevent or mitigate widespread attacks before they reach the consumer. If ISPs take action, then the likelihood of attacks being successful could potentially reduce dramatically. BT's Cyber Index[13] provides a good indication of the scale of attacks that can be prevented if action is taken at the ISP level. As well as taking action on their own networks, ISPs can increase information sharing with their peers on threats, while ensuring that the default protection they are providing to customers is transparent.

One example of a threat posed that can be more successfully addressed at the ISP level is malware that is often downloaded onto a device as a result of a successful phishing email and can be leveraged in numerous ways to establish or advance attacks. Once deployed, malware is generally controlled by "command and control" servers that are used to send commands to compromised systems and receive stolen data. These servers also act as the headquarters for compromised machines in a botnet and can be used to disseminate commands that can, for example, steal data, spread malware further and disrupt web services.

Botnets can be used and monetized by criminals in an increasing number of ways, for example by distributing a range of scams or ransomware and mining cryptocurrencies. Criminal gains can vary depending on the tactics used, but in one example a banking botnet was used to steal more than 36 million Euros from 30,000 customers over a 90-day period.[14]

The cost of botnets is largely borne by ISPs, with the impacts being passed onto their customers and society as a whole. Research has indicated that almost 85% of botnet infrastructure is located in consumer ISP networks, with the remaining 15% being placed in hosting centres.[15]

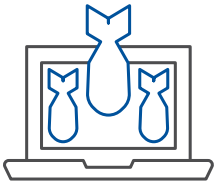
1.2 How can this principle create impact?

While businesses and users have a role to play in ensuring their systems are adequately protected and patched to ensure that malware cannot be deployed, ISPs can also play an important role in helping to monitor for known malware, protecting users and mitigating the impact of botnet infrastructure in their networks and sharing information with their peers. Implementation of this principle can help to create the following impact:

- Preventing malware from reaching consumers devices in the first place will reduce the spread of botnets and resultant costs for both consumers and ISPs
- Sharing information on widespread threats and how to address them across the ISP community will enable more comprehensive responses and make it more difficult for criminals to succeed in their attacks
- Building collective resilience and increasing the likelihood that attacks will be prevented from spreading and impacting consumers and the wider economy

CASE STUDY BT GROUP

BT have worked with the National Cybersecurity Centre (NCSC) and other ISPs in the UK in order to block malicious malware connections that would cause harm to customers. BT are blocking over one hundred million attempted malware communications every month to safeguard their customers and have led an initiative in the UK to encourage other ISPs to work collaboratively to share and act on information about malicious domains. This not only protects customers but also helps to ensure the safety and security of the UK's online space, much of which is critical national infrastructure. BT are now publishing these statistics on their Cyber Index[16]which demonstrates the positive impact of this initiative



9%

Decrease in DDoS events over the quarter

11%

Decrease in scam activity over the quarter

45%

Increase in phishing attacks over the quarter

111 million

Connections to malware sites blocked per month

Source: BT Cyber Index 2019, data from April to June 2019

CASE STUDY PROXIMUS

The general public is not always aware of a malware attack on their personal device. The Botnet Eradication Program, a joint initiative of Proximus and the Centre for Cybersecurity Belgium (CCB), aims to reduce active botnet participation from customer devices in Belgium.

CCB will inform Proximus – a telecommunications and ICT company operating in the Belgian and international markets, providing services to residential, enterprise and public customers – of the IP addresses of customers that have been connecting to known command and control (C&C) centres. Proximus will then act by identifying the customers corresponding to the respective IP addresses and informing them that at least one of their devices is most likely infected with malware. The customers will be directed to an awareness page hosted by safeonweb.be. This page will assist them in cleaning their device(s).

The Botnet Eradication Program will thus protect the public by tackling the problem at its source, namely removing the malware from their devices. The increased awareness on the dangers associated with botnets and malware will be a positive side effect.

CASE STUDY KOREA TELECOM

KT is a leading operator with both wireline and wireless networks in service in the Republic of Korea, with total assets of KRW 33.8 trillion and operating revenue of KRW 23.4 trillion. The company has recently developed a platform called GiGA Secure Platform (GSP), where public organizations and companies are able to share and protect against malicious code and websites. The platform collects and detects threat information in order to respond to threat attacks that interfere with network stability as a result of attacks being launched via IoT devices. GSP has collected and analysed on average 20 million URLs per day within the KT network and about 5.3 million malicious IPs, URLs and patterns have been registered by the GSP this year. Daily threat collection information has been updated on a monthly basis and is currently being provided to customers on a trial basis.

1.3 Recommendations for implementation

1.3.1 Consumer protection by default

Protection by default of consumers by ISPs can lead to the discussion of important questions regarding how ISPs should define what should and should not be blocked from reaching customers. Efforts are underway in a number of countries to explore criteria for how to decide what should and should not be blocked, and to ensure transparency on processes undertaken and oversight. For example, in the EU efforts are underway to consider how ISPs might best implement the guidance set out by ENISA on Article 3(3) of the Open Internet Access Regulation[17] which helps National Regulatory Authorities (NRAs) to decide whether or not a provider is allowed to take a security measure, for example blocking certain traffic, to protect the security of networks, services using the networks, or end-user equipment. Consumers should also be cognizant of the activities taken by their ISP to protect them from attacks and have the opportunity to opt out if desired.

BT have also worked to establish a Malware Information Sharing Platform (MISP) in the UK, which includes input from the National Cybersecurity Centre and helps ISPs share information on known threats. KT also runs a similar platform in South Korea, and a number of platforms listed in the Annex also provide mechanisms for information sharing.

If the majority of ISPs choose to protect their customers by default from objectively harmful sites, the world as a whole will be significantly better off in terms of reducing the harm caused by cyberattack.

> **Recommendation 1:** Protect consumers by default from known cyberattacks, ensuring that the consumer is informed of such efforts and has the opportunity to opt out if desired.

> **Recommendation 2:** Collaborate with peers and national and supranational regulatory bodies to determine the most suitable ways to collaborate and protect consumers by default, working together to define new oversight mechanisms and regulatory frameworks where needed.

Principle 2. **Take action to raise awareness and understanding of threats and support consumers in protecting themselves and their networks**

2.1 What challenge does this principle address?

Humans, whether they are in a professional or personal setting, are often the primary target of an attacker and provide the simplest access to systems and data. While protecting consumers by default so they are less exposed to attacks that target human weakness is therefore preferred, this is not always possible. Actions also need to be taken to help raise awareness and build in solutions or a "second layer of defence" to help protect individuals from direct attacks.

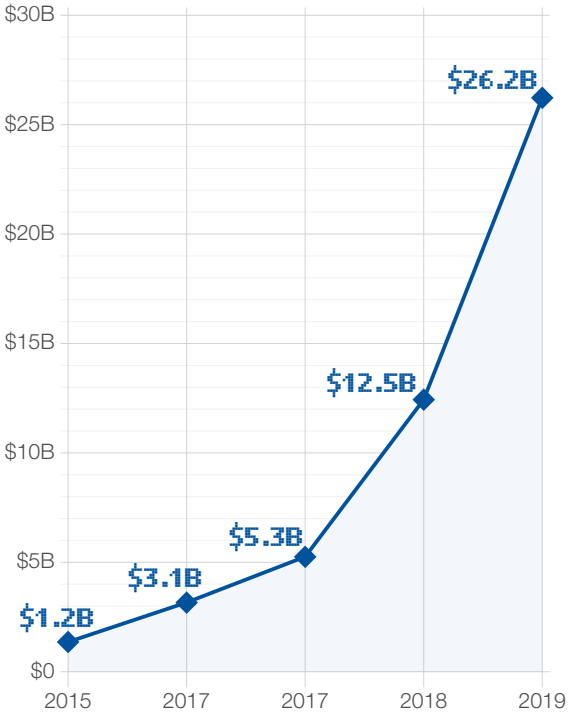
There are a range of ways in which human weakness or vulnerability can be exploited but phishing attacks, where spam emails are sent to users encouraging them to disclose information or click on "fake" links remain the most frequent form of social engineering.[18] Criminals use such attacks to obtain personal data, hijack accounts, steal identities, initiate illegitimate payments or convince the victim to undertake other activity that could reveal information about themselves or their activities. Such links can also be used by criminals to install malware on the user machine. Phishing and social engineering attacks are now experienced by 85% of organizations.[19] Other attacks that do not use email as the primary vector include vishing (where phone calls are used) or smishing (SMS.)

While phishing attacks are often targeted fairly indiscriminately, more targeted crimes, or "spearphishing" also include Business Email Compromise (BEC), where the scam emails sent purport to be from the recipient's CEO or other senior figure in their organization, instructing the recipient (often in the financial department) to transfer funds to an account controlled by the criminal. BEC schemes can be operated using a variety of techniques, for example through targeted phishing emails, spoofing domain names or purchasing domain names which are similar to the CEO's account.

All of these types of social engineering attacks are relatively simple to execute and do not require significant expenditure, technical know-how or equipment on the part of the attacker. Their economic impact, however, can be great, with the FBI estimating a loss of over $1 billion as a result of BEC fraud by US businesses and individuals in 2018.[20]

Due to such schemes focusing on exploiting human behaviour, many of the solutions to addressing social engineering fraud centre around awareness raising and education. Where action can be taken to reduce the likelihood of spam emails reaching inboxes in the first place, it should be. But help is also needed to ensure consumers are equipped to defend against threats that are more difficult for ISPs to stop.

Total global reported losses due to BEC fraud. October 2015-July 2019. Source: FBI



2.2 How can this principle create impact?

By educating consumers, ISPs can help to improve the understanding of internet attack vectors that leverage end-user ignorance, as well as providing guidance and technical measures to support consumers in defending against more sophisticated attacks. Implementation of this principle will help to create the following impact:

- Reduce the financial and reputational impact of phishing attacks and resultant identity fraud and theft
- Help to generate communications and awareness raising between members of the public and responsible cyber authorities, leading to greater trust and enabling quicker response mechanisms
- Reduce the amount of spam and fraudulent email sent in the first place, thus reducing the potential for attack and freeing up communications pipelines

CASE STUDY SAUDI TELECOM COMPANY GROUP

Saudi Telecom Company (STC) Group, the leading telecoms provider in Saudi Arabia and one of the world's largest in the MENA region, has worked with its partners to overcome the ever-increasing threat of SMS spam and fraud. To do so, STC has implemented a spam and fraud control solution that provides in-depth defence in a multiple-layer approach.

The first layer comprises a spam shield or smart filter that functions on a real-time machine-learning algorithm to evaluate and update SMS filtering rules. The evolving dynamic rules are implemented on an hourly basis to stop suspicious and malicious SMS traffic.

The second layer is composed of the integration of the SMS gateway with the state-of-the-art Threat Intelligence Platform (TIP). The platform receives feeds from various internal and external sources and forwards links considered to have a high probability of being malicious to the SMS gateway to identify and block SMS messages containing such links before reaching the customer. This proactively aims to protect the customers from malicious SMS messages.

The third layer is the STC Domain Name Server (DNS) system, in turn connected to the TIP. The TIP enables the DNS system to identify and block queries regarding any malicious domain. The aim is to protect customers from any suspicious links embedded in their SMS messages.

The fourth layer is handset protection; STC has collaborated with leading handset protection partners to provide their customers with additional automatic protection against viruses, malware, spyware and harmful links.

The last defence layer takes the form of customer awareness campaigns. A dedicated contact phone number is at the service of customers to report any suspicious SMS so that it can be examined and blocked at source if necessary.

The five defence layers have drastically reduced the number of SMS spam and fraud messages sent through STC's SMS services. STC's network registers up to 338 million SMS per day, 20 million of which (or 6% of the SMS registered in the network) are on average blocked or rejected due to suspicious or malicious features. This improvement is just the tip of the iceberg, with STC continuously improving the process and technology to achieve better results.

CASE STUDY PROXIMUS

Proximus - being a founder of the Cybersecurity Coalition.be - is actively involved in the creation and deployment of the yearly national awareness campaign, an initiative from the Centre for Cybersecurity Belgium (CCB) and the Cybersecurity Coalition.be.

For the fifth consecutive year, the CCB and the Coalition launched a national Cybersecurity Awareness campaign for the general public. “Relax and think twice before clicking on a link” is the slogan of this year’s campaign. The campaign starts from the observation that internet users are still not cautious enough when clicking on a link in an email or opening attachments and so fall quickly into the phishing trap.

This campaign encourages the public to forward suspicious messages to suspicious@safeonweb.be. In 2018, the CCB received no less than 650,000 emails via this email address. After an automatic scan of the mails, the national CERT managed to block 15,000 fraudulent websites. As of October 2019, the CCB had received 1 million messages from affected citizens.

The ambition is to go yet further, by creating a Belgian Anti-Phishing Shield. This will be a public-private partnership project to warn the public when they are about to access a malicious website as a consequence of a phishing attack.

Based on alerts reported by the public, the National CERT and incident response teams from various industry partners, including Proximus, will work together to rapidly share information about phishing websites. Following a thorough validation by the National CERT, the ISPs will be asked to redirect the user to a warning page. Consequently, when the users are being tricked into clicking on a phishing link, they will be protected from losing their personal information or being infected by a malware.

CASE STUDY TELSTRA

Many large organizations work to take down phishing domains that imitate their brands and target their customers for fraudulent purposes. In addition to protecting their own customers, Telstra has recognized the unique opportunity they hold as Australia’s largest ISP to use their visibility of threats to identify phishing campaigns impacting the broader community.

To do this, they have established a team to gather spam reports from their customers, partners and the public to identify new patterns and trends impacting the Australian economy. Next, they compare and match this analysis against several threat intelligence feeds to curate a holistic summary of the latest threats.

Telstra then pushes this information to the Australian Cybersecurity Centre (ACSC) and other organizations as a manual threat feed for them to action. This action could take the form of monitoring or blocking domains on their respective networks, providing further analysis to feed back to the intelligence community or remediating compromised systems. By providing this service they help to provide actionable ecosystem-wide threat information to improve security across a range of Australian entities.

Email credential harvesting continues to be one of the most prevalent forms of phishing. On average every week they identify hundreds of stolen user credentials captured via phishing emails. These credentials belong to everyone from home users, employees of small to medium businesses, to large corporations. Where they identify a large number of Australian credentials these are also shared with the ACSC and partners for remediation.

2.3 Recommendations for implementation

2.3.1 Consumer guidance

Education and awareness raising are key instruments to defend against social engineering attacks and there are many examples of good practice in deploying such campaigns.[21]

ISPs can also use their role and engagement with consumers to help build a knowledge base around incidents and threats and encourage consumers to proactively protect themselves (for example on how to safely use devices connected to their networks). These activities can improve security not just for the end user and the ISP but for the online ecosystem as a whole.

Also important is the availability of easily accessible contacts for customers to connect with and report incidents to in the event of fraud or suspected criminal activity. ISPs have a significant role to play in ensuring that any reporting mechanisms are appropriately aligned with national schemes and law enforcement initiatives. Likewise, ISPs should consider the mechanisms they have in place for informing consumers of suspicious activity or vulnerabilities identified on their systems.

ISPs might also wish to consider the merits of providing guidance and awareness raising campaigns to others in addition to consumers to broaden take up of initiatives and improve the security of online ecosystems.

> **Recommendation 1**: Provide customers with a minimum level of guidance on security best practice and with routes for reporting suspicious activity that are linked with national initiatives where relevant.

> **Recommendation 2**: Establish mechanisms for quickly informing consumers of suspicious activity or vulnerabilities identified on their systems and provide assistance to them in addressing any issues where required.

2.3.2 Email security

ISPs can play a crucial role in helping to protect the integrity of email and thereby protect consumers against social engineering fraud, in particular by assisting with the implementation of an internet standard called Domain-Based Message Authentication, Reporting and Conformance (DMARC).[22] DMARC helps to ensure that the owners of email domains can have greater control over who can use their email addresses (the “from” address in an email), and as such help to reduce the volume of emails that are “spoofed” by changing the “from” address to a domain they do not own.

DMARC implementation does not entirely stop spoofs, but if implemented at scale will significantly raise the cost of conducting attacks for a significant group of attackers. Effective implementation also plays an instrumental role in helping to build and reinforce public trust, in particular in relation to well-known brands whose email domains might otherwise be used for fraudulent purposes. It is also interesting to bear in mind that whether an organization has implemented DMARC effectively or not is public information and as such could be used to gauge how much the organization is trying to do to protect its customers. It can therefore be seen as key to building trust in online services and brands.

The UK Government has demonstrated the effectiveness of using DMARC in government domains. HM Revenue and Customs were in the top 20 most phished domains globally, a rating which reduced significantly soon after their implementation of DMARC.[23] The US and the Netherlands governments are also mandating DMARC implementation on their domains.

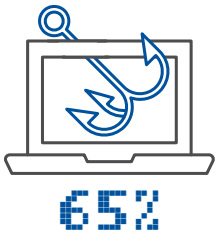
> **Recommendation**: Implement DMARC on network-owned domains and help customers implement DMARC on their domains.

2.3.3 Defence against smishing

Although SMS messaging is decreasing, there remain security risks associated with attempts to conduct smishing attacks, which, like phishing attacks, confuse the recipient into trusting the message (for example an authentication message sent by a bank) and then clicking on an embedded link that takes them to a fraudulent site with the intention of harvesting data and credentials, or in the worst case scenario, payments.

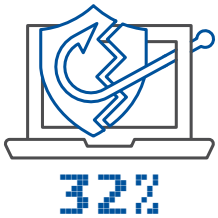
The main cause of this phenomenon is the increasing presence of mobile phones and smartphones in particular. SMS and instant messages are a cheap, effective and popular method of communication. In some countries they are more likely to be opened and read than other communication forms, which makes them a channel of choice for phishing attacks and spam. Operators can help to identify where this takes place and work to control the use of the "from" addresses which are used in the transmission of SMS messages and to centralize the reporting of unusual behaviour. The Mobile Ecosystem Forum (MEF)[24] is working on initiatives with industry to reduce fraudulent SMS activity.

> **Recommendation:** Collaborate with partners across the ecosystem to understand the risks of smishing on networks and seek to implement measures to 1. reduce it, and 2. report unusual behaviour



65%

Of targeted attack groups used spear phishing as the primary infection vector

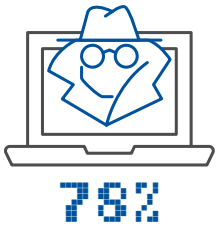


32%

Of breaches involve phishing

48%

Of malicious email attachments are office files



78%

Of cyber espionage incidents had phishing involved

Source: Europol. Internet Organised Crime Threat Assessment (IOCTA) 2019

Principle 3. **Work more closely with manufacturers and vendors of hardware, software and infrastructure to raise minimum levels of security**

3.1 What challenge does this principle address?

Some networking hardware, particularly low-cost customer premises equipment or CPE devices are often seen as an easy target due to the fact that the firmware and passwords in such devices have well-known default administrative passwords and user IDs, are easily compromised and may also not be easily updated. Attacks can be conducted on end-user equipment provided by the network provider to its customer as well as devices that can be bought and connected to the network. The increasing number of devices that are connected to the internet has a corresponding impact on the risks posed by devices to the online ecosystem, with the Mirai botnet being one example of how poorly secured devices can lead to high impact online attacks.[25]

In 2018, the FBI advised that users of certain types of routers should restart them after Cisco researchers discovered 500,000 routers were compromised by malware.[26] As the Internet Society points out, "another way to assess the scope of the problem is to track how many types of malware are designed for IoT devices".[27] They reference a Kaspersky Labs report in which they document a threefold increase in the number of malware variations used to attack IoT devices in the first half of 2018.[28]

There have also been examples of this equipment generating malicious traffic itself. While it is difficult to fix all vulnerabilities in such equipment, action can be taken to minimize by default the harm those vulnerable devices can cause. At the time of writing, however, there is a distinct lack of focus on designing secure IoT products, with some suggesting that "less than 10% of IoT companies have a straightforward way for security researchers to interact with, securely manage or update devices".[29]

As the online and physical worlds increasingly become intertwined, online attacks against internet-connected devices could in future have severe impacts on the physical world. For example, ransomware attacks against home security or life-affecting systems such as heating devices or water systems could lead to serious implications for individuals and communities.

3.2 How can this principle create impact?

There is of course no one-size-fits-all approach to managing devices securely and wider interactions with the supply chain. Relationships and product offerings managed by ISPs will differ depending on their approach and wider business considerations. For example, the costs of purchasing secure IoT equipment also needs to be considered against the benefits. ISPs are encouraged to play their part in creating momentum and raising awareness so that the use of secure devices become the norm. Implementation of this principle can help to create the following impact:

- Decrease the potential attack surface for criminals to launch attacks and consequently reduce impact of potential crimes on both consumers and ISPs
- Incentivize good security practices among consumers and increase security standards and transparency across supply chains
- Increase the security of connected ecosystems and the stability of the communications infrastructure that underpins it

3.3 Recommendations for implementation

3.3.1 Use of management protocols and increased vendor security

Attacks can be conducted using end-user equipment including equipment provided by the network provider to its customers and connected to the telecommunications circuit (otherwise known as consumer premises equipment (CPE) such as routers or network switches). There have also been examples of this equipment generating malicious traffic itself. It is difficult to fix all vulnerabilities in such equipment, but action can be taken to minimize by default the harm those vulnerable devices can cause.

Most of the attacks perpetrated via this equipment have relied on certain management -related protocols being available from the WAN side by default. We would therefore recommend all ISPs to consider restricting protocols that are not generally required by the majority of customers, such as telnet, SSH, UPNP and SNMP inbound to consumer endpoints by default. Evidently, customers requiring these should be able to re-enable them – and it is likely those that need these protocols understand how to secure them. It is also recommended that all ISPs block CPE management protocols[30] from being routed from outside their network unless there are valid reasons for not doing this, as well as to ensure that their management plane is not accessible from the internet.

> **Recommendation 1**: Consider restricting protocols that are not generally required by the majority of customers to prevent damage that can be caused by vulnerable devices. Block CPE management protocols from being routed from outside the network unless there are valid reasons for not doing this, and ensure the management plane is not accessible from the internet.

There are a growing number of initiatives and guidance aiming to help secure consumer devices and to incentivize the producers of these devices to ensure security is an integral part of their design. For example, a set of principles for how to secure consumer IoT devices was recently endorsed by the European Technical Standards Institute (ETSI).[31] The Internet Society has also produced an IoT Trust Framework, which seeks to raise the level of security for IoT

CASE STUDY SAUDI TELECOM COMPANY GROUP

STC inevitably deals with many different suppliers and Managed Service Providers (MSPs) worldwide. This makes the challenge to STC's cybersecurity team in protecting the company from harm particularly complex.

To address the challenges posed by supply chain threats, STC first defined clear third-party standards and policies to be applied at all phases of any project prior to contract award, during the on-boarding process, and even after project delivery. All third-party suppliers and MSPs must adhere to these standards and policies, including the evaluation of the entity's security risk, the use of contractual clauses on security such as the right to audit and defined responsibilities and liabilities, awareness activities and third-party audits. As a result of implementing these controls, STC has been able to raise the security of its suppliers, thus contributing to the wider online ecosystem as well as protecting their own consumers from a range of threats.

CASE STUDY BT GROUP

BT has identified issues where routers with management exposed to the internet are being targeted for attack by cybercriminals. The company has developed a set of standards for configuration to ensure their routers are not exposed and also proactively seeks to identify any BT-managed devices that are exposed, resolving any issues identified so as to ensure the security of their networks and customers.

devices and related services to better protect consumers and the privacy of their data.[32] California has also become the first state in the US to pass a specific IoT cybersecurity law that specifies certain measures that must be taken by manufacturers to secure devices.[33]

> **Recommendation 2**: Support and incentivize the adoption of initiatives and frameworks to provide clarity on acceptable minimum standards for IoT devices across the supply chain.[34]

CASE STUDY EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE

The ETSI specifications set out that the three main criteria to look out for in buying internet-connected devices, which should help protect against a large number of attacks, are:

1. Ensure that devices are not pre-set with passwords that expect to be changed by the consumer, but that are unique. This would have helped prevent the Mirai attack and removes the onus on the consumer to change passwords.

2. Companies that produce internet-connected devices and services should provide a point of contact to which issues can be directly reported. This allows companies to be able to respond in a timely manner and fix any issues.

3. Software updates or "patches" to connected devices should be easy to implement and timely. This ensures that software glitches, which could provide a vulnerability to attack, can be corrected.

Principle 4. **Take action to shore up the security of routing and signalling to reinforce effective defence against attacks**

4.1 What challenge does this principle address?

Many criminals deploy strategies that rely on manipulating the ways in which traffic is routed on the internet to launch attacks that are largely aimed at compromising the availability of networks and services. Many such attacks are result of criminals violating the underlying assumptions relating to identity which are implicit in the routing, naming and addressing systems on the internet. Many such attacks result in DoS that can have a significant impact on both the reputation of affected organizations and their ability to conduct business operations.

As well as spoofing email addresses for the purposes of social engineering or deploying malware, criminals can also use similar tactics to mimic or interfere with IP addresses in the hope of gaining access to data that might be inserted to a "fake" website such as financial or identification data. Similarly, although less commonly, criminals can steal entire "address blocks", which can have a profound effect on the mapping of IP addresses.

Criminals can also reroute internet traffic for similar purposes or to conduct different types of attack. One recent survey of ISPs established that over 70% of them were affected by spoofing related attacks.[35]

One of the criminal deployments of IP source address spoofing is to conduct Distributed Denial of Service attacks through "reflection-amplification" attacks that direct traffic to the spoofed address and overwhelm networks and servers. This can lead to a significant impact on both ISPs and their customers, both in terms of damage to the brand, as well as negative impacts on the operations of customers as a result of denial of service. According to one report, 65% of DoS attacks were aimed at communications service providers in the third quarter of 2018.[36]

In addition to these types of routing attacks, criminals are also increasingly adopting strategies that seek to manipulate the Domain Name System (which manages how human-readable web addresses are translated into machine-readable IP addresses) so as to reroute traffic to scam websites and obtain data from unsuspecting consumers. This is yet another example of the fragility of the underlying assumptions regarding identity on the internet.

4.2 How can this principle create impact?

Adopting this principle could have a significant impact on the online ecosystem as a whole and could also bring efficiencies to ISPs that would have greater clarity on their peering relationships with partners. Implementation of this principle can help to create the following impact:

- Drive efficiency and transparency between ISPs on peering relationships with partners
- Reducing the likelihood of potentially catastrophic attacks on some of the fundamental pillars of how internet communications take place
- Decreasing lost revenue and value to ISPs

CASE STUDY KOREA TELECOM

To more securely manage the vulnerabilities of SS7, KT adopted the guidance issued by the GSMA. When harmful SMS is detected, they are blocked by IT systems to protect their customers. In addition, KT sets a routine process of monitoring and detecting other SMS which could cause potential threats.

KT has been responding to threats such as small payments, information leakage attempts, multi-character transmission and smartphone control that are sent to SMS or SNS through Smishing Blockage. KT collects URL and app information from security systems installed on the network and determines whether they are malicious or not through code analysis. URLs that have been judged to be malicious are passed to the harmful site blocking system and the SNS forwarding system, and blocks are executed for the site and SNS in real time. As a result of these efforts, Smishing text and distribution sites have been blocked more than 12 million times a year.

4.3 Recommendations for implementation

ISPs can take a range of protocol related measures to make it more difficult for criminals to manipulate traffic routing and conduct man-in-the-middle, denial of service and other attacks:

4.3.1 Signalling and routing-implementing effective infrastructure protocols

There are a number of security issues related to the ways in which traffic is routed on the internet that make it relatively easy for malicious actors to, for example, generate traffic from spoofed IP addresses (source address spoofing) or to reroute traffic at large scale (destination address spoofing.)

A protocol called Border Gateway Protocol (BGP) is used by ISPs and carriers to describe how traffic should flow around the internet. Networks “advertise” these routes, and a router will make a least-cost decision on how to send packets via these routes.

Adversaries can announce a low-cost route to a particular destination which will then be automatically chosen, and the traffic potentially redirected to an unintended or fraudulent destination, thus potentially impacting negatively on an end user who may be redirected to a fraudulent website. Much can be done to prevent these routes from being “hijacked”, beginning with greater collaboration between ISPs to better understand how routes are chosen and how current peering relationships between ISPs work in practice. In some countries, ISPs have started

CASE STUDY PROXIMUS

Like KT, Proximus is also following GSMA recommendations through the implementation of countermeasures like Home Routing and Signalling Firewall. The countermeasures block unauthorized signalling messages on Proximus’ network and stop criminals from abusing the telecoms network in order to launch attacks.

In this way, Proximus not only protects its own subscribers, but also the subscribers from abroad that roam on Proximus network in Belgium.

CASE STUDY BT GROUP

BT are working on a number of measures to improve routing and signalling in the UK to help protect customers and contribute to the security of the wider online ecosystem in the UK and beyond. For example, through a GSMA-led initiative, they are collaborating with mobile operators to be able to better identify malicious SS7 messages and to develop industry standards on SS7.

to collaborate to monitor current BGP routing and have developed a platform through which some classes of BGP hijack can automatically be detected. For example, BT has worked with global partners across public and private sectors to try to improve industry standards for protecting BGP and to better identify malicious rerouting.

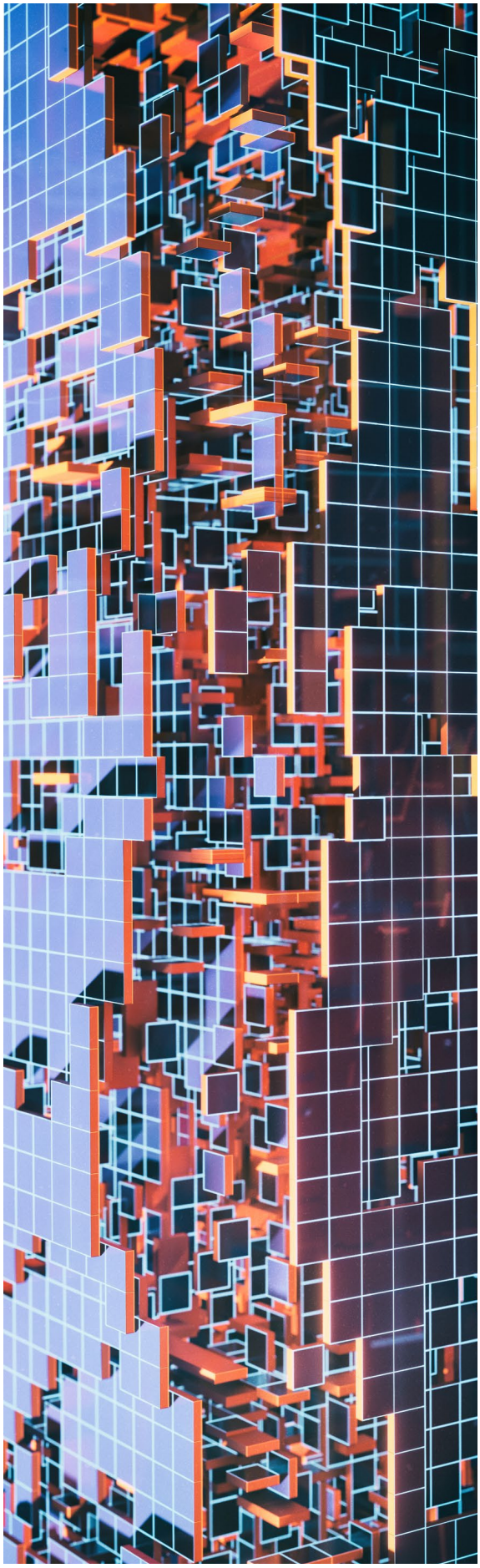
> **Recommendation 1**: Understand current BGP peering relationships and seek to collaborate with peers to better identify BGP hijacks and be able to effectively respond.

The global initiative on Mutually Agreed Norms for Routing Security (MANRS) encourages implementation of crucial fixes to reduce the most common routing threats, including route leaks and hijacks, source IP spoofing.[37]

CASE STUDY MUTUALLY AGREED NORMS FOR ROUTING SECURITY

The Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Internet Society, that provides crucial fixes to the most common routing threats and can help to address many of the challenges faced by ISPs. External analysis of the benefits of the project was commissioned[38] which determined that "for service providers, there are considerable benefits to participation. It can increase their value to customers and potentially increase revenue. The MANRS directives are a useful guide to increasing operational efficiency while contributing to the improvement of the security of the internet community. The combination of customer impact and internal benefit should be sufficient motivation for providers to become part of this growing community".

> **Recommendation 2**: Strongly consider joining the MANRS project and implementing MANRS requirements.



Source address spoofing is commonly used by adversaries in DDOS attacks which use a spoofed source IP address of a single compromised machine that pretends to be a large number of machines. When ISPs filter traffic coming from the edge of their networks (known as “ingress filtering”) it is much more difficult for source addresses to be spoofed. An internet standard called BCP38 (& 84) explains how to carry this out. Though correct implementation will not mean it is harder for a network to be impacted by a DDOS attack, it does mean that it is harder for machines on the network to be used in a DDOS attack against others, thereby reducing the volume of malicious activity on networks and the costs associated with this, which can be reinvested in other ways to provide a better service for customers.

> **Recommendation 3**: Implement BCP38 (or similar) ingress filtering to reduce the ease with which some types of DDOS can be undertaken and the value of infrastructure to attackers.

While DNS is not the only protocol that can be abused to enact DoS attacks (other connectionless protocols, such as Network Time Protocol can also be easily abused), ISPs can also help to shore up the use of DNS in DoS attacks through limiting access to DNS (and other connectionless protocols to their consumers, as well as ‘rate limiting’ their DNS servers).

> **Recommendation 4**: Appropriately manage access to and use of protocols such as DNS which can be used to enact DoS attacks.

Telecoms operators will also be familiar with Signalling System No. 7 (SS7) which is the protocol by which international telecoms networks communicate with each other in order to route calls, send SMS and allow users to roam between countries. This protocol has little security built in and it is therefore easy for adversaries to exploit SS7 vulnerabilities. This can allow an adversary to geolocate a user’s phone, for example, or reroute calls and SMS messages and get networks to release encryption keys. This can cause significant knock-on implications, for example when SMS messages are used for multifactor authentication. It not feasible to change the standard, but ISPs can comply with basic guidance issued by the GSMA[39] that details some simple filtering that operators can undertake to protect their users, as well as collaborating to ensure that the next generation of signaling protocol (DIAMETER) is better secured.

> **Recommendation 5**: Raise awareness of the security vulnerabilities of SS7 and implement relevant solutions (e.g. the GSMA SS7 filtering standard) to better protect customers. Ensure that the next generation of signalling is better secured.

To reduce the risk of attackers inserting fraudulent mappings between domain names and the IP addresses those domain names reference, ISPs that operate resolvers can enable DNS Security Enhancement or DNSSEC validation. DNSSEC inserts cryptographic signatures over DNS data, allowing DNSSEC validators to verify the DNS data have not been modified since those data were DNSSEC-signed.

> **Recommendation 6**: Enable DNSSEC validation in resolvers and encourage customers to DNSSEC-sign the zones for which they are authoritative.

Conclusions and Next Steps

The working group that contributed to the development of these principles agreed that all ISPs should explore and ideally commit to implementing the principles and recommendations set out here on their own networks due to the significant impact this could have on the security of global online ecosystems. The principles were discussed at the World Economic Forum Annual Meeting on Cybersecurity in November 2019 and were endorsed by a range of partners who urge their broad adoption.

The working group and wider partners also identified a number of additional activities which could help to drive this work forward in support of ISP efforts to counter many of the threats posed by high-volume attacks. The most important of these is to initiate a discussion between governments and regulators on how policy frameworks can be established that incentivize responsible behaviours by ISPs to promote security while at the same time upholding principles of openness and neutrality.

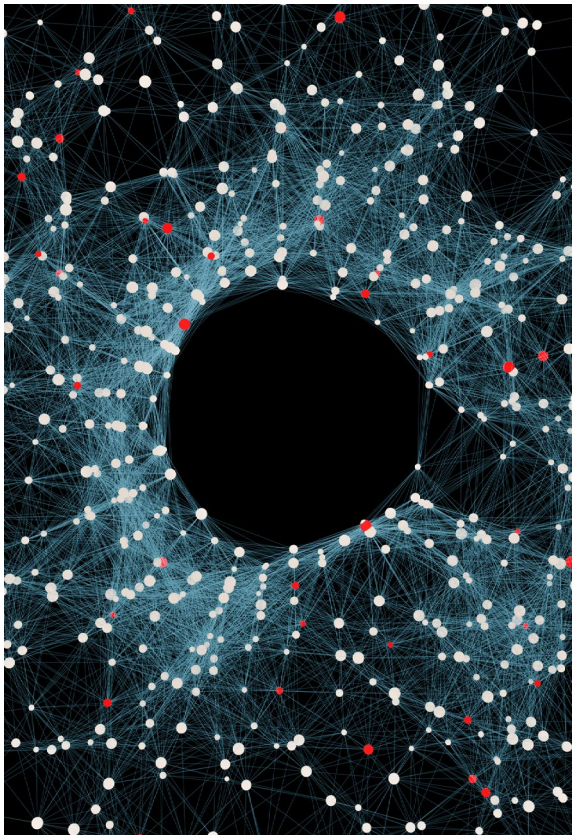
A number of next steps proposed will be taken forward by the working group, which will seek deeper collaboration from public-sector partners in the subsequent phase of work. As the international organization for public-private cooperation, the World Economic Forum's unique position and platform can serve to strengthen public-private collaboration and encourage the adoption of best practice as well as development of further solutions.

– **Greater public-sector collaboration**

  Many of the activities suggested here could be supported further through closer collaboration between the public and private sectors. Governments and regulators have a role to play in setting the conditions for ISPs and others to undertake the right behaviours, both through incentivizing activities and ensuring that regulations and oversight provide adequate and responsible frameworks for ISPs to take necessary actions on their networks for their positive impact on the consumer and the online ecosystem as a whole. Government also has a role to play in supporting communication and awareness raising on cybercrime prevention.

The Forum has previously developed guidelines for public-private collaboration on cybercrime and resilience, in particular through the publication of Advancing Cyber Resilience: Principles and Tools for Boards in 2017[40] and subsequent board governance toolkits. The Forum will continue its work in this area, with a particular focus on specific sectors or communities, including communications providers. The work will aim to consider three specific issues:

1. Providing greater clarity on the respective roles and responsibilities of public and private sectors in ensuring the safety and security of the internet
2. Ensuring respective actors remain accountable for their actions to promote safety and security, and that all actions are transparent and uphold principles of openness and transparency
3. Developing policy frameworks that can incentivize the adoption by the private sector of behaviours that will contribute to the security of online ecosystems



Additional activities that can be undertaken and we will explore further in collaboration with our partners and in support of related initiatives include:

- **Driving broader information sharing on known threats and malicious sites**

  As explained above, increased information sharing between ISPs can significantly aid responses to new and evolving threats and responses. While some ISPs already share a great deal of useful information on known malicious traffic traversing their networks and there are various national initiatives in place to encourage this, much more can still be done to scale such efforts up to a global level. This includes building on successful initiatives and tools such as MISP, which has been used to good effect in the UK, more widely in Europe, as well as in the US and Australia, and is starting to be used in other parts of the world.

- **Collaboration to improve IoT security**

  The proliferation of IoT devices means that risks from connected devices are likely to increase. As explained above, more can be done to set minimum security standards for consumer devices as well as for critical network equipment. Standards are emerging, but increased efforts to help secure their adoption and consistency would benefit the online ecosystem as whole. Information sharing initiatives and those that attract and analyse malicious activity via so-called "honeypots" also help to improve ability to respond and defend against such attacks

- **Peer comparisons and analysis**

  To drive good behaviours and incite competition between ISPs and others, such as hardware manufacturers, on the provision of secure service to customers, initiatives could be undertaken to allow such organizations to more easily compare their practices and, more importantly, to allow customers to be informed about the level of security and protection offered.

- **Measuring impact**

  Further work to better understand the positive impact of the principles here and other such initiatives would contribute to making the case for wider adoption. Initiatives such as the MANRS Observatory[41] and BT's Cyber Index[42] are model examples.

Annex 1: Known Information Sharing Initiatives

There are a number of information sharing initiatives at local, regional and global level. Many are based on the MISP open source software which enables communities to share information about threats and cybersecurity indicators.[43]

– FIRST has a MISP at the disposal of their members (Global coverage)

– ETIS has some of its operator members connecting MISP (European coverage)

– NATO has industrial contractual partnerships with some operators in which information is also being shared through MISP (NATO member coverage)

– GSMA has a MISP at the disposal of their members, primarily (but not restricted to) sharing telecom IoC's (Global coverage)

Other cybersecurity information sharing initiatives exist at a broader level, for example the Cyber Threat Alliance[44], a not-for-profit organization working to improve the cybersecurity of the global digital ecosystem through enabling real-time sharing of threat information in the cybersecurity field. Sector-based information sharing and analysis centres also exist, most formally in the US, but with increasing global participation.[45]

Contributors

Lead Author

Amy Jordan — Project Lead, Future Networks and Technology, Platform for Shaping the Future of Cybersecurity and Digital Trust

The World Economic Forum would like to like to thank the following partners and contributors to this publication:

BT Group

Deutsche Telekom AG

Emirates Integrated Telecommunications Company (Du Telecom)

Europol, European Cybercrime Centre (EC3)

Global Cyber Alliance (GCA)

International Telecommunications Union (ITU)

Internet Society

Korea Telecom

Proximus

Saudi Telecom Company Group

Singtel

Telstra

Numerous other contributors supported this work by providing input, expertise and thoughtful commentary. Our thanks to Miguel de Bruycker, Belgian National Cybersecurity Centre; Kathryn Condello, CenturyLink; Amy Lemberger, GSMA; David Conrad, ICANN; Tim Stevens, King's College London; Amy Hogan-Burney, Microsoft; Ian Wallace, NewAmerica; Scott Stevens, Palo Alto Networks; Miguel Sanchez San Venancio, Telefonica; Andre Arnes, Telenor; Ian Levy, UK NCSC.

Endnotes

1. Providers of internet services to public customers that have the ability to undertake actions on their networks to identify malicious activity and prevent it from reaching their customers. The acronym ISP in this document refers to any organization involved in the provision of online communications able to implement the principles set out.

2. Accenture Security. 2019. *The Cost of Cybercrime*. p. 11. https://www.accenture.com/t00010101t000000z__w__/nz-en/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf (link as of 03/01/2020)

3. National Cyber Security Centre (NCSC). 2017. *Cyber crime: understanding the online business model*. p. 10. https://www.ncsc.gov.uk/news/ncsc-publishes-new-report-criminal-online-activity (link as of 03/01/2020)

4. Imperva. 2019. *Bad Bot Report 2019: The Bot Arms Race Continues*. p. 11. https://www.imperva.com/resources/resource-library/reports/bad-bot-report-2019-the-bot-arms-race-continues/ (link as of 03/01/2020)

5. Verizon. 2019. *Data Breach Investigations Report 2019*. https://enterprise.verizon.com/resources/reports/dbir/

6. Accenture Security. 2019. *The Cost of Cybercrime*. p. 13. https://www.accenture.com/t00010101t000000z__w__/nz-en/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf (link as of 03/01/2020)

7. Anderson, Barton, Böhme, Clayton, Gañán, Grasso, Levi, Moore and Vasek. 2019. *Measuring the Changing Cost of Cybercrime*. p. 16. https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_25.pdf (link as of 03/01/2020)

8. Accenture Security. 2019. *The Cost of Cybercrime*. p. 13. https://www.accenture.com/t00010101t000000z__w__/nz-en/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf (link as of 03/01/2020)

9. Check Point. 2012. A *Case Study of Eurograbber: How 36 Million Euros was Stolen via Malware.* https://www.checkpoint.com/downloads/product-related/whitepapers/eurograbber-malware-bank-customers-millions-stolen.pdf (link as of 03/01/2020)

10. 2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics. Cybercrime Magazine. https://cybersecurityventures.com/cybersecurity-almanac-2019/ (link as of 17/01/2020)

11. Accenture Security. 2019. *The Cost of Cybercrime*. p. 20. https://www.accenture.com/t00010101t000000z__w__/nz-en/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf (link as of 03/01/2020)

12. NETSCOUT. 2018. *14th Annual Worldwide Infrastructure Security Report (WISR).* https://www.netscout.com/report/ (link as of 03/01/2020)

13. BT. 2019. *Cyber Index*. https://www.btplc.com/Digitalimpactandsustainability/Humanrights/Privacyandfreeexpression/cyberindex/index.htm (link as of 03/01/2020)

14. Check Point. 2012. A *Case Study of Eurograbber: How 36 Million Euros was Stolen via Malware.* https://www.checkpoint.com/downloads/product-related/whitepapers/eurograbber-malware-bank-customers-millions-stolen.pdf (link as of 03/01/2020)

15. Anderson, Barton, Böhme, Clayton, Gañán, Grasso, Levi, Moore and Vasek. 2019. *Measuring the Changing Cost of Cybercrime*. p. 20. https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_25.pdf (link as of 03/01/2020)

16. BT. 2019. *BT's Cyber Index reveals the scale of today's cyber threat*. https://newsroom.bt.com/bts-cyber-index-reveals-the-scale-of-todays-cyber-threat/ (link as of 03/01/2020)

17. Enisa. 2018. *Guideline on assessing security measures in the context of Article 3(3) of the Open Internet regulation*. https://www.enisa.europa.eu/publications/guideline-on-assessing-security-measures-in-the-context-of-article-3-3-of-the-open-internet-regulation (link as of 03/01/2020)

18. Europol. 2018. *Internet Organised Crime Threat Assessment (IOCTA) 2018.* https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018 (link as of 03/01/2020)

19. Accenture Security. 2019. *The Cost of Cybercrime*. p. 13. https://www.accenture.com/t00010101t000000z__w__/nz-en/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf (link as of 03/01/2020)

20. Anderson, Barton, Böhme, Clayton, Gañán, Grasso, Levi, Moore and Vasek. 2019. *Measuring the Changing Cost of Cybercrime*. p. 16. https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_25.pdf (link as of 03/01/2020)

21. Examples include the EU's European Cybersecurity Month https://cybersecuritymonth.eu, the UK's Cyber Aware campaign https://www.ncsc.gov.uk/section/information-for/individuals-families and Singapore's Cybersecurity Awareness Alliance https://www.csa.gov.sg/gosafeonline/content/cyber-security-awareness-alliance (links as of 03/01/2020)

22. RFC7489. https://tools.ietf.org/html/rfc7489 (link as of 03/01/2020)

23. Though it is difficult to prove that this is a direct result of DMARC implementation, it is highly likely that this played a key contributing effect, alongside other work undertaken by Her Majesty's Revenue and Customs (HMRC) and NCSC, including on take-downs.

24. Mobile Ecosystem Forum. https://mobileecosystemforum.com/ (link as of 03/01/2020)

25. Cloudflare. 2019. *What is the Mirai Botnet?.* https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/ (link as of 03/01/2020)

26. Esage, Alisa. 2018. *FBI launches international alert for cisco routers for being easy to hack*. Information Security Newspaper. https://www.securitynewspaper.com/2018/05/31/fbi-launches-international-alert-cisco-routers-easy-hack/ (link as of 03/01/2020)

27. Online Trust Alliance. 2019. *2018 Cyber Incident & Breach Trends Report*. https://www.internetsociety.org/wp-content/uploads/2019/07/OTA-Incident-Breach-Trends-Report_2019.pdf (link as of 03/01/2020)

28. Kaspersky. 2018. *New IoT-malware grew three-fold in H1 2018*. https://www.kaspersky.com/about/press-releases/2018_new-iot-malware-grew-three-fold-in-h1-2018 (link as of 03/01/2020)

29. Rogers, David. 2019. *Is Device Management the Key to a Secure IoT?.* Pelion IoT Blog. https://blog.mbed.com/post/secureiot (link as of 03/01/2020)

30. For example: Broadband Froum. *TR-069*. https://www.broadband-forum.org/download/TR-069_Amendment-6.pdf (link as of 03/01/2020)

31. ETSI. Internet of Things. https://www.etsi.org/technologies/internet-of-things (link as of 03/01/2020)

32. Internet Society. 2018. *IoT Trust by Design: The OTA IoT Trust Framework*. https://www.internetsociety.org/resources/doc/2018/iot-trust-by-design (link as of 03/01/2020)

33. California Legislative Information. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327 (link as of 03/01/2020)

34. For example by implementing the ETSI TS 103 645. *Cyber Security for Consumer Internet of Things*. https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf (link as of 03/01/2020)

35. Lichtblau, Franziska. 2018. *Understanding the spoofing problem*. APNIC Blog. https://blog.apnic.net/2018/02/09/understanding-spoofing-problem/ (link as of 03/01/2020)

36. Nexusguard. 2018. *DDoS Threat Report 2018 Q3.* https://www.nexusguard.com/threat-report-q3-2018 (link as of 03/01/2020)

37. The MANRS project seeks to encourage BGP best practice implementation. The link https://www.manrs.org/isps/participants/ lists all the ISPs globally that have voluntarily implemented the MANRS Actions. The description of MANRS Actions can be found here: https://www.manrs.org/isps (links as of 03/01/2020)

38. MANRS. 2017. *Better MANRS for Service Providers*. https://www.manrs.org/wp-content/uploads/2017/10/MANRS-Service-Providers-Case.pdf (link as of 03/01/2020)

39. GSMA FS.11 for SS7 and GSMA FS.19 for DIAMETER

40. World Economic Forum. 2017. *Advancing Cyber Resilience: Principles and Tools for Boards*. https://www.weforum.org/whitepapers/advancing-cyber-resilience-principles-and-tools-for-boards (link as of 03/01/2020)

41. https://observatory.manrs.org/ (link as of 03/01/2020) The MANRS Observatory measures network adherence to MANRS — their "MANRS readiness" — a key indicator of the state of routing security and resilience of the internet. To measure "MANRS readiness" for a particular network a set of metrics is used, one for each action. For example, to measure to what degree Filtering (Action 1) is implemented we will measure the number of routing incidents where the network was implicated either as a culprit or an accomplice and their duration. Similar metrics are calculated for their anti-spoofing capabilities (Action 2), presence of contact information (Action 3) and completeness of routing information in public repositories, such as IRRs and RPKI (Action 4). This data is gathered from trusted third-party sources, such as BGPStream.com, CIDR report, CAIDA Spoofer and RIPEStat. The measurements are passive, which means that they do not require cooperation for a measured network. That allows us to measure the MR-indices not only for the members of the MANRS initiative, but for all networks in the internet (at the moment more than 65,000).

42. BT. 2019. *BT's Cyber Index reveals the scale of today's cyber threat*. https://newsroom.bt.com/bts-cyber-index-reveals-the-scale-of-todays-cyber-threat/ (link as of 03/01/2020)

43. MISP. https://www.misp-project.org/ (link as of 03/01/2020)

44. Cyber Threat Alliance. https://www.cyberthreatalliance.org/ (link as of 03/01/2020)

45. ISACs. https://www.nationalisacs.org/ (link as of 03/01/2020)

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0)22 869 1212
Fax: +41 (0)22 786 2744

contact@weforum.org
www.weforum.org