ISPA Cyber Security Member Survey

DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCADDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME PARTNERSHIP TRAINING COOPERATION CYBER ESSENTIALS ANTIVIRUS FIREWALLS POLICE NCA DDOS HACKING CYBERCRIME CYBER SECURITY PHISHING SPYING MALWARE BOTNET ECRIME

Table of contents

1 Executive Summary 2

2 Introduction 4

3 Survey findings and analysis 4

3.1 Investment and priority 4

3.2 Nature and impact of attacks 5

3.3 Network protection 5

3.4 Consumer awareness and protection 6

3.5 Reporting and the role of Government and law enforcement 6

3.6 Summary of key findings 8

3.7 Recommendations for Government and law enforcement 8

4 Annex 1: Methodology and respondents 8

5 Annex 2: Complete Survey Responses 10

1 Executive Summary

ISPA surveyed a broad range of its membership on cyber security of varying size and customer base, but with a particular focus on smaller and medium sized ISPs. The questions focused on the following five areas:

- Investment and priority of cyber security within the business
- The nature and impact of cyber attacks
- Network protection measures
- Consumer protection and awareness
- Reporting and the role of Government and law-enforcement

Through the thirty questions, a number of clear findings emerged which demonstrate that cyber security is a priority for member, one that is only rising, with senior responsibility within the company as ISPs are subject to regular attacks. ISPs play a proactive role through network protection, consumer support and by working with authorities to help mitigate threats. Government and law enforcement should prioritise awareness raising and education, and improve how they deal with reports and coordination of cyber security.

ISPA's ten key findings from the survey are:

1. Cyber-security is an increasing priority for 79% of ISPs surveyed, 77% said spending is increasing and MDs or C-Suite executives are accountable for cyber-attacks
2. 92% are subject to cyber-attacks on a daily (31%), weekly (23%) or monthly (38%) basis
3. ISPs provide a wide variety of tools and services to protect networks and tools to end users
4. 85% of those surveyed said ISPs should have a proactive role to play in maintaining customer protection and mitigation
5. ISPs take a proactive approach, with 84% of those surveyed having reported incidents and breaches and 92% provide advice and tools
6. ISPs want Government to focus on awareness raising (64%) rather than creating new regulations (18%) to meet the challenges of cyber security
7. Law enforcement should prioritise better training (83%) and coordination with industry (83%), as well as increase funding (58%) and prosecutions (50%)
8. 91% are concerned about Government surveillance measures impacting on network security
9. There is inconsistency with how law enforcement deals with ISP incident reporting
10. While a large number of public bodies are in contact with ISPs, a third receive little or no contact

Recommendations for Government

To help address these findings, we have proposed five recommendations to Government:

1. Government should focus on education and awareness and work collaboratively with industry rather than resorting to legislation
2. Government must be mindful of the damage surveillance legislation can have on network security, such as the intrusive hacking powers within the Investigatory Powers Bill
3. Law enforcement should prioritise better training of officers and coordination of cyber security
4. There needs to be more consistency when an ISP reports a case to law enforcement so that where practicable all reports are followed up and investigated so that criminals can be brought to justice
5. Authorities must do more to reach out to the full breadth of the ISP industry, engaging them in information sharing work and consultation

2 Introduction

The increasing reliance on the Internet and digital services as part of everyday life has put cyber security firmly on the agenda for business, policymakers, Government, law enforcement, and many more. What may have once been considered a technical issue, cyber security is now a mainstream concern that cannot be ignored.

The role of all stakeholders, including that of ISPs, has come under further scrutiny following high-profile incidences and the continued growth of the Internet. Recent examples include official figures putting cybercrime at 40% of all online crime, a parliamentary select committee inquiry into ISP cyber security, ISPs ramping up their cyber security expertise and capabilities, a new and imminent Government cyber security strategy and work to incentivise cyber security take up. Security is and has always been a priority for ISPs and is fundamental to how an ISP runs its network, serves its customers and protects its reputation. For our members, cyber security has always been a major focus: they are the experts and ensuring secure, good quality and reliable online services are being delivered on a daily basis is their overriding priority.

As with other areas a partnership approach is often most effective, with different stakeholders fulfilling their role where they are best placed to. For cyber security this means government, law enforcement, internet companies, individual users, ISPs and others all playing their part in helping protect, mitigate and boost cyber security. To help better understand the role of ISPs in the debate, ISPA conducted a survey of its members across a range of areas.

3 Survey findings and analysis

The survey covered five priority areas and below is a summary of the responses and conclusions from each section of the survey.

3.1 Investment and priority

Secure and resilient networks are a long-standing priority area for our members. To shed further light on this we asked questions ranging from how members currently approach cyber security, where it sits in their business and level of spending.

Key findings

- **Cyber security is an increasing priority for ISPs**: 79% of respondents said that cyber security is a high or very high priority on a day-to-day basis, and this has increased significantly over the past few years.
- **MD or C-Suite have responsibility for cyber attacks:** For 93% of respondents, the MD/CEO or CTO/CIO has ultimate responsibility in the event of a cyber attack.
- **Cyber Security spend is increasing:** 77% of respondents are planning on spending more in the coming years, with 67% already spending more than 2% of their overall spend on cyber security.

ISPs manage cyber security in a variety of ways, with some having a security team that floats between departments, whilst others embed cyber into operational teams. The scale of spending was also varied, with one respondent estimating cyber security was responsible for "10% of overall IT spend".

3.2 Nature and impact of attacks

ISPs and telecommunications companies are in a unique position as they are not only subject to high levels of attacks to undermine their network infrastructure and data, but attacks against customers also travel across or make use of their infrastructure. This section asked about the most common threats faced by ISPA members, the frequency and regularity of attacks and how they are measured.

Key findings

- **More than half are attacked on a daily or weekly basis:** 31% of respondents are subject to daily attacks, 23% weekly and 38% monthly.
- **Phishing and DDoS key customer threats**: 73% of those surveyed said their customers are subject to phishing attacks, 64% suffer DDoS attacks, 36% telephony fraud and 9% botnets when asked what the most common sources of attack on their customers.
- **DDoS, SQL and phishing are most regular network attacks:** 91% of respondents said that they are subject to DDoS attacks, 64% SQL hacking, 36% phishing, 18% telephony fraud and 9% botnet when asked what the most common source of attacks on their networks was.
- Members find it **hard to quantify the costs** and impact on businesses of cyber security as its impact runs across the business.

3.3 Network protection

With attacks coming in a variety of forms and becoming increasingly sophisticated, this section focused on the steps taken by ISPA members to monitor and protect their networks against attacks. Proactive network protection is part and parcel of running an ISP and there are a variety of tools, services and practices used. Questions covered internal risk management processes and specific product and services used.

Key findings

- **A wide variety of tools and services are used to protect networks:**
    - 100% of respondents said that they use a firewall, 92% port blocking, 70% DDoS protection, 85% antispam, 46% DNS with a number of other tools and services listed (malware scanning, network sniffing, IPs and more) when asked about ways to identify and minimise risk.
    - 100% of respondents carry out security design and review, 69% auditing, 62% penetration testing and 8% simulated attacks when asked about vulnerability testing on their network
    - Almost two-thirds (64%) assess third party suppliers' security capabilities.

ISPs responded with a variety of different approaches to network protection, unsurprising given the variety of different network types there are. Some ISPs own and operate their own infrastructure when

others are more reliant on wholesale providers. One respondent says they use external contractors and on the relationship with suppliers, respondents detailed how they checked supplier's credentials and met staff to "understand their security capabilities."

3.4 Consumer awareness and protection

One of the important links in the cyber security chain is customers and end users. Often not as wise to the challenges of cyber security as ISPs, it can be hard for individuals to always know how to keep themselves safe and secure. ISPs helps customers behind the scenes on a daily basis on the network level, but also provide advice and guidance and free or paid for tools and services to help protect themselves and their devices. This section looked at the areas where ISPs play an active role, the tools and services they provide and practices adopted.

Key findings

- **ISPs have a proactive role to play on customer protection and threat mitigation** When asked about the areas in which ISPs should play an active role, 85% of respondents said that they should inform customers if their equipment is compromised, 85% thought ISPs should proactively increase the physical security of network infrastructure and 46% said ISPs should share information with Government and the wider industry.
- **Advice and network level protection is provided by ISPs:** 92% of respondents provide advice and guidance to customers, 83% network level protection, and 17% software updates.
- **Data breaches are reported**: 84% have notified customers about a data breach, the rest (16%) would if required.
- **Half of customers have asked about cyber security:** 50% of respondents said customers contacted them about cyber security, whilst an equal 50% have not;
- **Cyber security is good for business:** 75% have been asked about cyber security by potential customers with respondents adding that "security is a vital lever in the market".

ISPs are keen to work with their customers to make sure their connections are secure and want to be proactive in protecting customers. However, a number of respondents called for ISPs to do more to help customers, with one calling for a "considerable change in attitude" and doing more to share information on an industry wide basis.

Some business-focused ISPs also reported that customers would ask about security measures in choosing their ISP and sought out extra support for managing malware, fraud attempts and website security. This follows the long-standing trend for ISPs to offer a suite of managed services on top of Internet connectivity.

3.5 Reporting and the role of Government and law enforcement

A partnership is central to an effective approach to cyber security, with industry, end users, law enforcement and Government all playing their part. Government and law enforcement have important roles to play in demonstrating leadership, setting out expectations and prosecuting crime. This is a

live area, with Government currently taking the wide-ranging Investigatory Powers Bill through Parliament, with powers to legally hack private networks, and new obligations around data breach notification and minimum standards.

ISPA surveyed members on how they feel Government and law enforcement are performing in this area and their views on the various different schemes and initiatives. Members were further asked on their experiences reporting cyber attacks, information sharing and their relationship with the authorities.

Key findings

- **ISPs report attacks to the authorities with a mixed response from the police:** 83% of respondents have reported a cyber attack to the authorities, with 17% having never done so. Of these, 30% said that there was no interest or follow up, 20% have found that the complaint is usually followed up and investigated, whilst 50% said reports are occasionally followed and investigated.
- **90% share experiences** of dealing with cyber attacks with industry colleagues, with one respondent saying it was "vital to the success of the sector".
- **A large number of public bodies are in contact with ISPs but a third of ISPs receive no contact:** a wide array of public bodies contact ISPs about cyber security, with the ICO (30%), NCA (31%), NCCU (23%), Home Office (8%), CISP (8%) featuring, yet 39% of respondents have never been contacted.
- **Awareness of government legislation and initiatives is high**: when asked about government initiatives, programmes and legislation, 90% of respondents were aware of the Investigatory Powers Bill, 80% GDPR, 70% Cyber Essentials, 70% ISO 27001, 60% '10 Steps to Cyber Security ', but only 20% were aware of the Cyber Information Sharing Partnership (CISP).
- **Government should focus on awareness raising rather than new regulations:** 64% thought that Government should have a role in awareness raising, 55% said benchmarking good practice and guidance, another 55% provide funding for providers to increase their security, yet only 18% thought establishing new regulations and 9% thought no role in response to the role Government should have in ensuring networks in the UK safe and secure.
- **ISPs are concerned about Government surveillance impacting on their networks**: 91% of respondents were either very concerned or somewhat concerned about Government surveillance impacting or compromising the security of their networks.
- **Law enforcement should prioritise better training, coordination, funding and prosecutions**: When presented with a range of options to improve its handling of cyber crimes by law enforcement chose the following responses:
    - 83% responded with better training and upskilling
    - 83% a more coordinated approach with industry
    - 58% more funding
    - 50% wanted to see more prosecutions
    - 42% more proactive intelligence
    - 42% publish results of investigations

- 16% a new public body established

3.6 Summary of key findings

Across these six areas, the results reveal 10 key findings:

1. Cyber-security is an increasing priority for 79% of ISPs surveyed, 77% said spending is increasing and MDs or C-Suite executives are accountable when cyber-attacks hit
2. 92% are subject to cyber-attacks on a daily (31%), weekly (23%) or monthly (38%) basis
3. ISPs provide a wide variety of tools and services to protect networks and tools to end users
4. 85% of those surveyed said ISPs should have a proactive role to play in maintaining customer protection and mitigation
5. ISPs take a proactive approach, with 84% of those surveyed having reported incidents and breaches and 92% provide advice and tools
6. ISPs want Government to focus on awareness raising (64%) rather than creating new regulations (18%) to meet the challenges of cyber security
7. Law enforcement should prioritise better training (83%) and coordination with industry (83%), as well as increase funding (58) and prosecutions (50%)
8. 91% are concerned about Government surveillance measures impacting on network security
9. There is inconsistency with how law enforcement deals with ISP incident reporting
10. While a large number of public bodies are in contact with ISPs, a third receive little or no contact

3.7 Recommendations for Government and law enforcement

In light of these findings, ISPA members feel the cyber threat is growing and posing some significant challenges. Based on the findings of this survey, ISPA makes a number of recommendations:

1. Government should focus on education and awareness and work collaboratively with industry rather than resorting to legislation
2. Government must be mindful of the damage surveillance legislation can have on network security, such as the intrusive hacking powers within the Investigatory Powers Bill
3. Law enforcement should prioritise better training of officers and coordination of cyber security
4. There needs to be more consistency when an ISP reports a case to law enforcement so that where practicable all reports are followed up and investigated so that criminals can be brought to justice
5. Authorities must do more to reach out to the full breadth of the ISP industry, engaging them in information sharing work and consultation

4 Annex 1: Methodology and respondents

ISPA surveyed members from the period 9 May–8 July 2016 using a mixture of qualitative and quantitative questions. An email was sent to the main contact for each member company to fill in the survey, with two reminder emails sent. Those that responded are more likely to have an active interest in cyber security and so there is likely to be a degree of self-selection.

Overall there were thirty-two questions separated into six sections:

- General company information
- Investment and priority of cyber security in your company
- Nature and impact of cyber attacks
- Network protection
- Customer awareness and protection
- Reporting attacks and the role of Government and law enforcement

Cyber security is a sensitive subject for ISPs and it was made clear that respondents could omit their company name and role within the business. Of those who supplied this data, respondents were overwhelmingly from senior technical and operational roles and there was even split between primarily consumer ISPs (43%) and business to business providers (36%). Other respondents identified as hosting providers and Managed Service Providers.

5 Annex 2: Complete Survey Responses

Please see below for the full results, however company sensitive information and individual comments have been omitted and some questions allowed multiple selections, therefore may exceed 100%.

Cyber Security priority in day to day operations (using a 1-5 scale with 5 the highest priority)

- 1 **0%**
- 2 **14%**
- 3 **7%**
- 4 **50%**
- 5 **29%**

How has this priority changed?

- Stayed the same **29%**
- More **42%**
- Much more **29%**

Who manages cyber security in your company's day to day operations?

- Technical staff according to agreed policy
- Information Security Manager
- Group Technical Manger
- CTO and team
- Technical Director
- Network Architect and our Infrastructure manager
- Technical Team
- security director
- Managed by our NOC function

Who is ultimately responsible should your company suffer an attack?

- MD / CEO **57%**
- CTO / CIO / other C-level **36%**
- Middle management **0%**
- Operational staff **7%**

What percentage of your overall spend is on cyber security?

- 0.1- 0.5% **8%**
- 0.5 - 1% **8%**
- -1% 1.5% **17%**
- 1.5 - 2% **0%**
- 2%- 2.5% **8%**
- Over 2.5% **59%**

Will your company spend more on cyber security in the coming years?

- Yes **77%**
- No **23%**

How often is your network subject to cyber attacks?

- Daily **31%**
- Weekly **23%**
- Monthly **15%**
- Annually **31%**

How often are your customers subject to cyber attacks?

- Daily **23%**
- Weekly **23%**
- Monthly **38%**
- Annually **16%**

Does your company measure the cost of cyber attacks?

- Yes **23%**
- No **77%**

What are the most common attacks that your customers face? (More than 1 choice allowed)

- DDoS **64%**
- Botnet **9%**
- Phishing **73%**
- Telephony Fraud **36%**

What are the most common attacks that your network faces? (More than 1 choice allowed)

- DDos **91%**
- Botnet **9%**
- Phishing **36%**
- SQL Hacking **64%**
- Telephony Fraud **18%**
- Other **18%**

What, if any, products and services does your company use to identify and minimise risk? (More than 1 choice allowed)

- Firewall **100%**
- Port blocking **92%**
- Anti spam **85%**
- DNS **46%**
- DDoS Protection **70%**
- Other **23%** (answers inc. malware scans, targeted detection and IPS)

What, if any, procedures do your company use to carry out vulnerability testing on your network?

- Penetration testing **62%**
- Security design and review **100%**
- Auditing **69%**
- Simulated attacks **8%**
- Other **8%**

Do you assess third party providers' security capabilities?

- Yes **64%**
- No **36%**

In which of the following areas should ISPs play an active role?

- Informing customers if using out of date applications (e.g. unsupported web browsers) **38%**
- Informing customers if their equipment is known to be compromised (e.g. if the ISPs is notified by law enforcement that equipment on the network is part of a botnet) **85%**
- Disconnecting customers if their equipment is known to be compromised (e.g. if the ISPs is notified by law enforcement that equipment on the network is part of a botnet) **62%**
- Informing law enforcement if customers' equipment is compromised **15%**
- Sharing information about network resilience with industry colleagues and Government **49%**
- Proactively increasing the physical security of network infrastructure **85%**

Does your company provide customers with protection in any of the following ways?

- Advice and guidance **92%**
- Network level protection **83%**
- End user tools / software **8%**
- Software updates **17%**

Does your company notify customers about a data breach or an attack?

- Yes **75%**
- No **0%**
- Rarely **9%**
- Other **16%**

Do existing customers contact your company about cyber security?

- Yes **50%**
- No **50%**

Is your company asked about cyber security by potential customers?

- Yes **75%**
- No **25%**

How often does your company report cyber attacks to the relevant authorities?

- Always **16%**
- Occasionally **25%**
- Rarely **42%**

- Never **17%**

What is your experience of the response of the relevant authorities to your report?

- Always followed up, actively investigated and where possible perpetrators arrested **0%**
- Usually followed up and investigated and where possible perpetrators arrested **20%**
- Occasionally followed up and investigated **50%**
- No interest and no follow up at all **30%**

Does your company share experiences of dealing with cyber attacks with industry colleagues?

- Yes **33%**
- No **17%**
- Sometimes **33%**
- Other/comments **17%**

What Government/law enforcement bodies have contacted you about cyber security?

- Information Commissioners' Office **30%**
- National Crime Agency **31%**
- National Cyber Crime Unit **23%**
- Home Office **8%**
- Cyber Information Sharing Partnership **8%**
- Local police force **8%**
- None **39%**
- Other **8%**

Are you aware of, or participate in, the following initiatives, programmes and legislation?

- The Network Information and Security Directive **0%**
- The General Data Protection Regulation **80%**
- The Investigatory Powers Bill **90%**
- Cyber Essentials Scheme **70%**
- 10 Steps to Cyber Security **60%**
- Cyber Security Information Sharing Partnership (CISP**) 20%**
- ISO 27001 accreditation **70%**
- Cyber Security Innovation Vouchers **10%**

What role should the Government have in ensuring that telecommunications networks in the UK are safe and secure?

- None **9%**
- Awareness raising **64%**
- Help benchmark good practice and guidance **55%**
- Provide funding for network operators to increase their security **55%**
- Establish new regulations on how networks should be protected **18%**

How concerned is your company about Government surveillance powers (for example powers to hack in to networks and the retention of data) impacting on the security of your networks?

- Very concerned **55%**
- Somewhat concerned **36%**
- Not very concerned **9%**
- Not at all concerned **0%**
- Don't know **0%**

What could law enforcement do to improve its handling of cyber crime? (More than 1 choice allowed)

- More funding **58%**
- Better training and upskilling **83%**
- A more coordinated approach with industry **83%**
- Establish a new public body to address the area **16%**
- Greater number of prosecutions **50%**
- More proactive intelligence **42%**
- Publish results of investigations **42%**
- Other (please specify) **8%**