ISPA CYBER SECURITY SURVEY 2018

October 2018

ISPA CYBER SECURITY SURVEY 2018

1 Executive summary

ISPA has once again surveyed its membership on their experiences and views regarding cyber security. Respondents came from different parts of the Internet value chain, with varying customer bases and ranging in size from small to large ISPs. The thirty-four questions focused on the following 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

The responses strongly indicated that cyber security remains a high priority for ISPs and is an area that they are investing in heavily. ISPs continue to play a proactive role in network protection, offering a range of cyber security features and guidance to customers. There is a shared view that cyber security would improve with greater collaboration and coordination between ISPs, Government and law enforcement agencies.

1.1 Key findings

ISPA's key findings from the survey are as follows:

1. An overwhelming majority (94%) of ISPs surveyed indicated that they expect to increase their investment in cyber security over the next three years, with 31% of respondents predicting that their cyber security spending will increase by more than 30% over this period. This represents a 15% increase in the number of companies who intend to invest in this area compared to the 2016 survey.

2. Cyber security remains an important priority for ISPs, with 61% of respondents stating that cyber security is a high or very high priority in their company's day-to-day operations. The fact that most ISPs expect to invest heavily in cyber security in the coming years, but a smaller percentage of them identify cyber security as a high priority, indicates that a robust cyber security regime is regarded as common practice amongst ISPs.

3. 88% of ISPs that responded are regularly subject to cyber attacks, with 44% experiencing daily attacks. This represents an increase from the 2016 survey in which 75% of ISPs were subject to regular attack. DDoS and phishing were the two most common forms of attack faced by respondents.

4. ISP's customers are largely the ultimate target of cyber attacks, with 69% of cyber attacks targeted at respondents' customers as opposed to their own networks.

5. Confusion about data breach thresholds and reporting systems persists, with responses suggesting that some ISPs may be unsure about what constitutes a reportable breach. The fact that 25% of ISPs who reported experiencing a breach subsequently reported it to the authorities suggests that more needs to be done to educate industry about reporting requirements and the most appropriate channels through which to report breaches. While not all breached need to be reported, given that the regulatory framework has matured in the past 12 months, with GDPR and NIS bedding in, we would expect the proportion of breaches being reported to increase.

6. The majority (86%) of respondents are implementing or planning to implement elements of Active Cyber Defence measures, as recommended by the National Cyber Security Centre (NCSC).

7. All respondents believe that ISPs should play a proactive role in cyber security, with 78% stating that they already offer dedicated cyber security services to their customers.

8. ISPs are divided on the importance of sharing their experiences of dealing with cyber attacks with industry colleagues: with 50% of respondents not doing so as a matter of routine. This contrasts with the finding that 40% of respondents think that the handling of cyber crime could be improved if there was better collaboration and coordination amongst the internet industry.

9. 62% of respondents suggested that the handling of cyber crime could be improved if law enforcement agencies took a more coordinated approach to the problem; with 31% suggesting that better cyber crime training for law enforcement officers was necessary. These were also the top two priorities reported in the 2016 survey.

10. ISPs want the Government to focus on setting out a clearer strategy and standards for cyber security, raising awareness of good cyber security practice, particularly amongst SMEs, and providing financial assistance or subsidies to businesses wishing to enhance their cyber security.

1.2 Recommendations to Government

ISPA's recommendations to Government are as follows:

1. Government should set out clear and practical minimum cyber security standards for industry, which are regularly updated to take account of evolving threats.
2. Government should focus on raising awareness of best practice in cyber security, using targeted subsidies, such as vouchers, to help raise standards.
3. Government should streamline the number of organisations involved in the cyber security landscape to minimise confusion and duplication, including on areas like breach reporting.
4. Law enforcement agencies should take a more coordinated approach and boost training to improve consistency in cyber crime enforcement outcomes.
5. There needs to be a significant improvement in online cyber crime reporting processes to help and facilitate the sharing of information between interested parties.

2 Introduction

Cyber threats are one of the most significant security challenges of our time, with the potential to impact governments, businesses and individuals as well as national infrastructure and the economy. Indeed, cyber security continues to enjoy a high-profile in both the media and policy circles, as well as enhanced public awareness, following several major cyber-attacks, including WannaCry, in 2017. ISPs play a unique role in protecting both their own network and customers and are often the first port of call for online users.

Security remains a major focus for ISPs as it is fundamental to running and maintaining their networks and, as such, is central to their business. In the time elapsed since ISPA's previous cyber security survey in 2016, ISP investment in cyber security has increased and looks set to continue on this trajectory, with the average investment in cyber security by ISPA's members predicted to increase by a quarter (see 3.1) over the next three years.

Despite the efforts of industry, Government and law enforcement agencies, certain challenges to the effective implementation of cyber security remain, such as: the sharing of information, coordination and awareness of best practice.

At this juncture, with new regulations bedding in, stakeholders feel they are well placed to assess the strengths of measures currently being taken, as well as help improve strategies for overcoming the barriers that continue to stand in the way of best practice.

3 Survey findings and analysis

The survey was split into five issue areas: investment and the priority of cyber security within the business; the nature and impact of cyber attacks; network protection measures; consumer protection and awareness; and, reporting and the role of Government and law enforcement. An overview of the findings from each section is set out below.

3.1 Investment and priority

Secure and resilient networks are of the utmost importance to ISPA's members. The questions in this section were targeted at understanding how our members currently approach cyber security.

Key Findings:

- **Investment in Cyber Security continues to grow:** 94% of respondents indicated that they expected their company's spend in this area to increase over the next 3 years. The mean predicted increase in spending on cyber security amongst our survey participants was 25%.
    - **Context:** These figures indicate an increase over the growth predicted in the 2016 survey (79%) reflecting the increasing priority of the issue and accelerating investment.

- **Cyber security remains a major operational issue:** Over 61% of respondents rated the priority of this issue as 'high' or 'the highest' in their company. The priority of cyber security was further emphasised by the respondents, 90% of whom said that the responsibility for Cyber Security rested with their CEO/MD or CTO/CFO.
    - **Context:** Whilst the rating of the importance of cyber security relative to other priorities of respondent's companies fell from the 79% reported in the previous survey, there has been no equivalent drop in the level at which responsibility is taken for cyber security. This indicates that cyber security has now become more of an accepted 'business as usual' issue rather than an emergency response to external events. Despite having a diverse membership both in terms of activity and size, there is a consensus in ISPA that 'best practice' in cyber security includes responsibility at senior executive level; not just at times of elevated threat but as part of normal business.

- **Strategy and Regulation are now the primary drivers of the increased focus on cyber security:** Approximately 39% of the firms surveyed felt that company strategy was the biggest single driver while 33% felt that it was regulation.

- **Context:** Only 17% of respondents considered customer 'push' to be the primary driver of the focus on cyber security. We would therefore surmise that, on this issue, both Government and industry are leading the response to the growing menace rather than simply responding to customer losses or other problems. Experience of financial loss by the ISPs was not mentioned as a driver of the increased focus and expenditure.

3.2 Nature and impact of cyber threats

ISPs are not only subject to high levels of attacks to undermine their network infrastructure and data, but also to attacks against customers that make use of their networks. The questions in this section were focused on the nature and frequency of the threats faced by ISPA members.

Key Findings:

- **The number of cyber attacks is increasing:** 44% of respondents experience attacks on a daily basis and 31% on a weekly basis.
  - **Context:** In the 2016 survey, the equivalent figures where 31% and 23% respectively. We believe that this change reflects the increasing rate of cyber crime and the growing threat.

- **The primary targets of cyber attacks on ISPs are the ISPs' customers**: Whilst ISPs have experienced attacks directed specifically at them, in most cases (over 69%) the attacks are aimed at their customers – through the ISP.
  - **Context:** This highlights the fact that, for ISPs, cyber security is a customer service issue as much as a technological issue. Best practice should, therefore, be to accompany cyber security programs with customer security information, training and services. The ISP's cyber security measures should be seen as the first line of defence for customers.

- **The two most common types of cyber attacks are DDoS and phishing:** This is the case for both customers and networks. Other types of attack include BotNets, Data Breaches, SQL Hacking, Telephony Fraud and RansomWare.
  - **Context:** These results are broadly in-line with those of the previous survey. Respondents did not report any major change in emphasis or new type of attack.

- **A mechanism for assessing economic Impact remains elusive**: 75% of respondents' companies do not assess the economic impact of security breaches.
  - **Contex**t: Whilst the proportion of firms seeking to measure economic interest is still small (25%) this represents progress from 2016. The issue is complex and

there exists no standardised measurement of economic loss which would be generally applicable or practical. The increase in spend on staff and systems to combat cyber attacks (See 3.1) is itself only one element of the economic cost. As the greatest impact of cyber crime is on the customers of ISPs, so the greatest economic cost is spread across a very large number of firms, many of which are not motivated to disclose economic information concerning loss.

3.3 Network protection

Cyber attacks are becoming ever more sophisticated and take a variety of forms. Questions in this section focused on the steps taken by ISPA members to monitor and protect their networks against attacks.

Key Findings:

- **There are a variety of software and system approaches used to combat cyber attacks:** 25% of respondents used the combination of a firewall, port blocking, anti-spam, DNS filtering, DDoS protection, alongside other protection measures, to combat cyber attacks. Of the specific protection measures taken, firewalls, port-blocking and DDoS protection were widely used by respondents as primary or supplementary tools.
    - **Contex**t: The responses indicated a variety of different approaches taken by ISPs, which is reflective of the diversity of both ISPs and ISPA members.

3.4 Consumer awareness and protection

ISPs play an active role in protecting consumers and raising awareness of cyber security issues. On a network level, ISPs help customers behind the scenes on a daily basis; however, the vast majority provide advice and tools to help consumers to protect themselves. This section looks at the areas, tools and services ISPs provide to protect consumers.

Key Findings:

- **The principal tools of customer protection remain network protection and advice and guidance.** In line with our earlier finding that respondents believe that technical defences against cyber attacks must be used alongside customer service approaches, with all respondents using a combination of these approaches to help protect customers. On the technology side, most companies (43%) have been focussing on DMARC (e-mail blocking) tools and/or DNS Malware blocking tools. Furthermore, 7% of respondents used Border Gateway Protocol (BGP) measures.
    - **Context:** The variety of approaches to customer protection continues to reflect the varied businesses of ISPA members: there is no, 'one size fits all' approach for customer protection. The process of deploying updated

and new tools to combat cyber attacks is a continuous one, which is likely to remain a significant cost for both ISPs and their customers for the foreseeable future.

- **77% of respondents offer their customers a dedicated cyber security service:** 22% of such services are provided at no cost to the overall service, whereas 56% are a chargeable additional product.
    - **Context:** The large range in size and activity of customers, serviced by ISPA members, means that dedicated cyber security services are not necessarily relevant to all; nevertheless, such services are available and their take-up is a customer's choice.

3.5 Reporting and the role of Government and law enforcement

The effective collaboration of industry, Government and law enforcement agencies is pivotal to effective cyber security. ISPA surveyed members on their views regarding how Government and law enforcement are performing in this area and on the functioning of various schemes and initiatives.

Key Findings:

- **Confusion about data breach thresholds and reporting systems persists:** with 25% of ISPs who reported experiencing a breach subsequently reporting it to the authorities. This suggests that more needs to be done to educate industry about reporting requirements and the most appropriate channels through which to report breaches.
    - **Context:** The proportion of respondents reporting breaches to external agencies is broadly in-line with that which was reported last year. However, given that the regulatory framework has matured in the past 12 months, with GDPR and NIS bedding in, we would expect the proportion of breaches being reported to increase. Furthermore, the value to ISPs and their customers of such reporting appears not to be fully understood or accepted by around half of respondents. This may be due to difficulties in communication with the plethora of different agencies involved in monitoring, investigating and prosecuting cyber security. Further research is needed to establish causes.

- **ISPs show a high level of awareness of Government regulations and initiatives in cyber security:** With the exception of "Ten Steps to Cyber Security" which only 31% of respondents were aware of, the six major initiatives and regulations members were asked about (see questionnaire) were widely known and understood. The General Data Protection Regulations (GDPR) and ISO 27001

Accreditation were the most widely known, with 100% of respondents indicating that they were aware of them. The National Cyber Security Centre Active Cyber Defence Program was also well recognised (88%).

  - **Context**: Awareness of regulations and initiatives has increased slightly from last year's level (which was itself categorised as 'high'). We would therefore suggest that low levels of reporting are not likely to be due to lack of knowledge but rather may be related to the number of different agencies and reporting channels, problems presented by analogue reporting systems, as well as the lack of feedback available.

- **Communication with law enforcement agencies concerning cyber security is fragmented**: respondents reported that they had had no contact with the Home Office or the NCA. The agencies that respondents had dealt with most were Local Police Forces (33%) and the ICO (27%).
  - **Context:** This issue was also prioritised in 2016. The lack of a clear pathway for reporting cyber security issues and receiving information is seen as discouraging more extensive reporting.

- **Increased coordination between law enforcement agencies is a priority**: the sharing of information between enforcement agencies and the follow up of cases is viewed as patchy.
  - **Context**: As noted in 2016, the need for better communication and coordination in law enforcement remains a priority for ISPs. However, whereas the training of law enforcement staff was seen as an equally high priority on 2016, this is no longer the case, with only 31% of respondents stating that it was a high priority.

4 Annex 1: Methodology and respondents

ISPA surveyed members from the period 7th July – 3rd August 2018 using a mixture of qualitative and quantitative questions. Those that responded are more likely to have an active interest in cyber security and so a degree of self-selection is probable.

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 split between primarily consumer ISPs (25%) and business to business providers (45%). Other respondents included VoIP providers (5%) and hosting providers (20%).

5 Annex 2: Complete survey responses

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

On a scale of 1-5 (with 5 being the highest), what priority does cyber-security have in terms of your company's day-to-day operations?

- 1: **6%**
- 2: **11%**
- 3: **22%**
- 4: **33%**
- 5: **28%**

Who manages cyber-security as part of your day-to-day operations?

- Director
- Network & Security Manager
- Network Operations Team
- Network Architect
- GSOC Team
- IT Manager
- Information Security Manager
- CTO
- Head of Security
- DPO
- System Team
- Head of Products
- R&C Manager
- ISM

Who is ultimately responsible for cyber security within your company?

- MD/CEO: **39%**
- CTO/CIO or equivalent: **50%**
- Middle-management: **6%**
- Operational staff: **6%**
- Other: **0%**

Have you encountered any difficulties recruiting skilled cyber security staff?

- Yes: **17%**
- No: **83%**

Do you expect the amount your company spends on cyber-security to increase in the next three years?

- Yes: **94%**
- No: **6%**

By how much do you expect the cyber-security spend to increase by in the next 3 years?

- 0%: **6%**
- 1-10%: **25%**
- 11-30%: **38%**
- 31-50%: **25%**
- 50-75%: **0%**
- 76%-: **6%**

What has been the single biggest factor driving cyber security in your business?

- Regulation: **33%**
- Customer demand: **17%**
- Company strategy: **39%**
- Market conditions: **6%**
- Other: **6%**

To what extent is cyber security driving new business growth in your business?

- Large: **0%**
- Medium: **39%**
- Small: **61%**

How often is your company subject to cyber-attacks?

- Daily: **44%**
- Weekly: **31%**
- Monthly: **13%**
- Other (please specify): **13%**

Overall, who is the ultimate target of these attacks?

- You (the service provider): **6%**
- Your customers: **69%**
- Other: **25%**

What is the most common form of attack that your company faces?

- DDoS: **25%**
- Data breaches: **6%**
- Botnets: **13%**
- Phishing: **25%**
- SQL hacking: **6%**
- Telephony fraud: **6%**
- Ransomware: **6%**
- Other: **13%**

Does your company assess the economic impact of cyber-attacks on the business?

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

Have you reported a breach to the authorities in the past 12 months?

- Yes: **25%**
- No: **44%**
- Have not needed to do so: **31%**

If yes, was the experience of reporting it straightforward and positive?

- Yes: **50%**
- No: **38%**
- Other: **13%**

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

- Yes: **6%**
- No: **50%**
- Sometimes: **44%**

Does your company use any of the following products or services to identify and minimise risk?

- Firewall: **81%**

- Port blocking: **38%**
- Anti-spam: **31%**
- DNS filtering: **31%**
- DDoS Protection: **43%**

Do you think ISPs should play an active role in the following?

- Informing their customers if they use out of date applications (e.g. an old and unsupported version of Internet Explorer)?: **33%**
- Informing their customers if their equipment is known to be compromised (e.g. if the ISP is notified by law enforcement that equipment on the network is part of a botnet)?: **93%**
- Disconnecting customers if their equipment is known to be compromised (e.g. if the ISP is notified by law enforcement that equipment on the network is part of a botnet)?: **60%**
- Informing law enforcement or other relevant authorities if customers' equipment is known to be compromised?: **20%**
- Sharing information about network resilience and threats with competitors and Government?: **47%**
- Proactively increasing the physical security of network infrastructure?: **60%**
- Blocking and filtering of domains associated with malware: **73%**

Are you aware of the National Cyber Security Centre Active Cyber Defence programme?

- Yes: **88%**
- No: **12%**

If yes, are you implementing or planning on implementing any of the following Active Cyber Defence measures?

- None: **14%**
- DMARC (email protection): **43%**
- DNS Malware blocking: **43%**
- BGP: **7%**
- SS7: **0%**
- Other: **14%**

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

- Advice and guidance: **47%**

- Network level protection: **47%**
- End user tools / software: **7%**
- Updates: **20%**
- Encryption: **7%**
- Other: **13%**

If you offer customers a dedicated cyber security service, is this:

- Free: **22%**
- Paid for: **56%**
- Other: **22%**

Which of the following Government regulations and initiatives are you aware of?

- The Network Information and Security Regulation: **56%**
- The General Data Protection Regulation: **100%**
- The Investigatory Powers Act: **81%**
- Cyber Essentials Scheme: **81%**
- 10 Steps to Cyber Security: **31%**
- ISO 27001 accreditation: **100%**

Have recent regulations made you improve your approach to cyber security?

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

Which Government/ law enforcement bodies have you had dealings with in relation to cyber-security?

- ICO: **33%**
- NCA: **0%**
- NCCU: **7%**
- Home Office: **0%**
- Other Govt department: **13%**
- Local Police force: **33%**
- Action Fraud: **13%**
- Other: **13%**

Generally speaking, what is your company's experience of reporting cyber-crime to the authorities?

- Positive: **46%**

- Negative: **46%**
- Mixed: **8%**

What could law enforcement do to improve its handling of cyber-crime?

- More funding: **8%**
- Better training: **31%**
- New laws: **0%**
- A more coordinated approach: **62%**
- New public body to address the area: **8%**
- Other: **15%**