FORTINET

ATT: Committee Secretary Parliamentary Joint Committee on Law Enforcement
PO Box 6100
Parliament House
Canberra ACT 2600
le.committee@aph.gov.au

Questions on Notice - Parliamentary Joint Committee on Law Enforcement inquiry into the capability of law enforcement to respond to cybercrime.

Fortinet thanks again the Parliamentary Joint Committee on Law Enforcement for the opportunity to appear in front of the committee and provide comments into the capability of Australian law enforcement to respond to cybercrime. Please see below additional responses resulting from the appearance.

Questions on Notice:

1. PROOF HANSARD pp 33-34

Further insights on what the threat landscape looks like from a cybercrime perspective:
Fortinet Threat Intelligence Report (provided to Committee).

In the second half of 2023, the cybersecurity landscape experienced various significant developments—like the rise in sophisticated attacks targeting large-scale enterprises and critical industries—that impact every organisation.

During this period, Fortinet observed more targeted ransomware attacks, new botnets and malware strains, and an uptick in IoT exploits. Notably, adversaries are moving quicker than ever, exploiting new vulnerabilities 43% faster than in the first half of the year. This finding underscores the need for organizations to improve their patch management processes, ensuring that they're updating software regularly to protect against fast-moving adversaries. Vendors also play a vital role in enabling customers to mitigate vulnerability risk. Every vendor has a responsibility to dedicate themselves to radical transparency, introducing robust security scrutiny at all stages of the product development lifecycle and proactively searching for and disclosing vulnerabilities.

Ransomware Is on the Rise, particularly among Critical Industries and it's no surprise that the threat of ransomware continues to keep security teams up at night. Across our sensors, ransomware detections surged 13 times higher over the first half of 2023. That was followed by a 70% drop during the latter half of the year, during which we also saw fewer organizations detecting ransomware variants. We witnessed a shift away from the traditional "spray and pray" ransomware strategy, with cybercriminals taking a more targeted approach and asking for higher ransom demands. Industrial organizations—including energy, healthcare, manufacturing, transportation, and automotive—experienced almost half (44%) of all ransomware and wiper detections in the second half of the year.

IoT Devices Hold Attackers' Interest While New Malware Strains and Botnets Emerge" - Our FortiGuard Labs team monitors an array of globally deployed sensors that collect trillions of threat events worldwide each day. This unique vantage point gives us a detailed view of the threat

landscape, including how exploit, malware, and botnet trends change.
Not surprisingly, IoT devices were popular targets, with attackers exploiting everything from firewalls to routers during the year's second half. This is why Secure by Design in IoT devices being explored by the Australian Government is so important moving forward. For the new exploits identified, attacks occurred an average of 4.76 days after discovery, which is 43% faster than the time-to-exploitation observed in 1H 2023. This underscores the need to use EPSS as an early warning system, as well as the importance of prioritizing patching efforts to mitigate the vulnerabilities most likely to be exploited.

Shedding Light on Dark Web Activity: While much of our telemetry shows us what actions attackers have taken previously, darknet intelligence helps us anticipate what adversaries may do next. In the last six months of 2023, threat actors discussed targeting organizations within the financial services industry most often, followed by the business services and education sectors. More than 20 significant zero days were shared on the dark web, and over 850,000 payment cards were advertised for sale.

Encouraging Responsible, Radical Transparency Across the Industry: Disrupting cybercrime requires a culture of collaboration, transparency, and accountability on a larger scale than possible with each entity working independently. Cybersecurity vendors have a crucial role to play in this endeavour and by partnering with the Australian Government we can help address this growing problem.

Fortinet Annual Skills Gap Report also reveals a growing connection between cybersecurity breaches and skills shortages. The survey was conducted among over 1,850 IT and cybersecurity decision-makers from 29 countries and locations. Survey respondents come from a range of industries, including technology (21%), manufacturing (15%), and financial services (13%).
Key findings from the report include:

- Organizations are increasingly attributing breaches to the cyber skills gap.
- Breaches continue to have significant repercussions for businesses, and executive leaders are often penalized when they happen.
- Certifications continue to be highly regarded by employers as a validator of current cybersecurity skills and knowledge.
- Numerous opportunities remain for hiring from diverse talent pools to help address the skills shortage.

The Cyber Skills Gap Continues to Impact Companies Worldwide - An estimated 4 million professionals are needed to fill the growing cybersecurity workforce gap. At the same time, Fortinet's 2024 Global Cybersecurity Skills Gap Report found that 70% of organizations indicated that the cybersecurity skills shortage creates additional risks for their organizations.

Other findings that highlight the impact of the growing skills gap on companies across the globe include:

- Organizations are attributing more breaches to a lack of cyber skills. In the past year, nearly 90% of organizational leaders (87%) said they experienced a breach that they can partially attribute to a lack of cyber skills, up from 84% in the 2023 report and 80% the year prior.

- Breaches have a more substantial impact on businesses. Breaches have a variety of repercussions, ranging from financial to reputational challenges. This year's survey reveals that corporate leaders are increasingly held accountable for cyber incidents, with 51% of respondents noting that directors or executives have faced fines, jail time, loss of position, or loss of employment following a cyberattack. Additionally, more than 50% of respondents indicate that breaches cost their organizations more than $1 million in lost revenue, fines, and other expenses last year—up from 48% in the 2023 report and 38% from the previous year.
- Boards of directors' view cybersecurity as a business imperative. As a result, executives and boards of directors increasingly prioritize cybersecurity, with 72% of respondents saying their boards were more focused on security in 2023 than the previous year. And 97% of respondents say their board sees cybersecurity as a business priority.

Based on these findings the importance of Cyber security is only increasing and the threat environment expanding. From a legislative perspective there are some pressure points at the domestic and international level.

Capacity and Capability Building:

Domestically we can see some inconsistency to training opportunities offered for both general awareness training and technical skill opportunities. A national standard in particular for awareness training could be explored to equip the public with the knowledge to help identify scams, cybercrime attacks etc. This could be like the standards in occupational health and safety training for example. Cyber awareness training moving forward should not be a nice to have but a need to have.

Good Cyber Hygiene:

As outlined Fortinet's threat report there is a continue lack of patching and addressing known vulnerabilities and this is increasingly being exploited by the cybercriminal. Moving forward the Australian Government could increase communication/education campaigns around the need to patch/update. Departments like the ATO who have regular reporting periods/engagement with citizens could help with this regular focus on updating. Good cyber hygiene will require continual investment moving forward.

Balancing Defence and Offense Capabilities:

While building better cyber defences is essential, equal emphasis should be placed on identifying and punishing cybercriminals. Further ongoing investment towards proactive enforcement efforts is crucial to deter cyberattacks. Some of the needed investment can be provided by the private sector and providing a legislative framework that will enable companies to support and provide capability quickly and effectively.

Collaboration and International Cooperation:

Cybercrime often transcends borders, necessitating collaboration among law enforcement agencies globally. Further international treaties and agreements facilitate information sharing and further joint investigations need to be developed. This obviously takes time, effort and investment but is and will need to become a fundamental pillar in international engagement.

Better Cybercrime metrics and reporting:

We need to ensure that we are improving our data collection on cybercrime and provide standardised reporting streams to ensure we have a clearer picture of cybercrime impacting Australians. By understanding the scale and impact of cybercrime, policy makers can make more informed policy changes to address the problem. For example having one Government Agency taking the lead on receiving and collecting the data would provide a clear pathway for companies like Fortinet to engage with. In return it would also enable the extensive insights/data that companies like Fortinet have to be used by the Australian Government.

2. PROOF HANSARD pp 34-35

Proposal for Subsidised Cyber Security Services for Small Businesses: As cyber threats continue to evolve and increase in frequency, the need for robust cyber security measures is increasingly vital to protect Australian interest.

There are a multitude of sophisticated cyber defence solutions in the market offered by Cybersecurity leaders like Fortinet. However, many of these solutions are aimed at the enterprise end of the market and the cost of procuring and the complexity of operating these services often puts them out of reach for small businesses, leaving them vulnerable.

To address this issue, Fortinet proposes the establishment of a pool of subsidised public-private cyber security services. These services would be offered as affordable subscription bundles, combining the expertise and efficiency of the private sector with government support.

The proposed services could include security defence systems such as:

- Security Monitoring: Continuous monitoring of network and system activities to detect and respond to potential threats in real time.
- End Point Protection: Comprehensive protection for all endpoints, including desktops, laptops, and mobile devices, to prevent malware, ransomware, and other cyber threats.
- Mail Scanning: Advanced email filtering and scanning to identify and block phishing attempts, spam, and malicious attachments.
- Web Scanning: Proactive scanning of websites to detect vulnerabilities and prevent unauthorized access or data breaches.
- Two-Factor Authentication (2FA): Enhanced security through multi-factor authentication, reducing the risk of unauthorized access to sensitive information.
- Cloud Security: Protection of cloud-based services and data, ensuring secure access and storage for businesses leveraging cloud technology.

These services would be made available to small businesses at a significantly reduced cost through government subsidies.

The benefit of establishing this type of model would allow small businesses to access similar levels of protection as larger enterprises, reducing their vulnerability to cyber-attack. Leveraging the expertise of the private sector with government oversight and leadership will stimulate the Australian cyber security ecosystem; inline with the Government vision for Cyber by 2030.

3. PROOF HANSARD pp 35-36

PDF of the book '*Cyber Safe – A Dog's Guide to Internet Security*' will be provided to the committee. A box of 60 books will also be sent to the Committee via Parliament House committee address for Member's electorates.

4. PROOF HANSARD pp 36

Gaps in the Cyber Security Strategy: We have attached Fortinet's submission to the Cyber Security Strategy for the committee's reference but two key areas where more Government/private partnership can help is through Education and Training.

EDUCATION – Continual expansion of Cyber Security Awareness and Training- as per the Skills Gap report 87% of breaches can in some part be attributed to a lack cyber skills or awareness.
This is why Fortinet Australia is proud to provide our Information Security Awareness and Training service at no cost to every public and private school in Australia. Building on our successful roll out in the United States, we have provided a local, customised version to teachers and school administrators to help raise cyber awareness through training in all Australian primary and secondary schools. By working with both the public and private education sectors to help schools train their staff and faculty with skillsets and knowledge that could prevent them from falling victim to popular threat methods, such as social engineering attempts, and reduce the likelihood of a cyber breach. This grass roots efforts are becoming more and more important to help address cybercrime more and Governments at all levels need to increase this type of training and prioritise cyber awareness training in employee development and learning opportunities.

Fortinet has also recently expanded this program to students in the United States and are currently piloting curriculum-based content for Australian students in South Australia.

SKILLS – Fortinet's Annual Skills Gap Report states there is a significant world wide skills gap it is surprising that for example as part of the National Skills agreement in South Australia, the SA Government have removed Cyber as a Fee Free offering. Federal and State Governments need to continue to invest in cyber training and through private/public partnerships can access practical and relevant micro credentialing courses and industry expertise.

Please contact Nicole Quinn, Head of Government Affairs APAC if any clarification or further information is required -