The Joint Committee on the National Security Strategy (JCNSS) inquiry into cyber security with a focus on the UK's critical infrastructure

Submission from:

Glasswall Solutions Limited

Primary author: Greg Sim – Group Chief Executive
Marketing & PR: Chris Dye – VP Marketing

About Glasswall

Glasswall eliminates zero-day malware attacks in business documents by reversing the traditional paradigm of looking for malware, Glasswall 'looks for good'. Glasswall's patented deep file inspection, remediation, sanitisation and document regeneration technology ends the threat from document based malware. Glasswall doesn't relying on detection signatures, completely disarming and regenerating clean, standard-compliant files whilst preserving their full usability. The technology seamlessly integrates within Email architectures and via an API into Data Guard and Diodes to deliver real-time protection from file-borne threats.

Executive Summary

- **Email attachments are the easiest route into any organisation's systems**
- **Traditional anti-virus cannot keep up with the volume of new malicious attacks**
- **More than 90 per cent of successful cyber-attacks commence with the triggering of malicious code in an email attachment**
- **70 per cent of file-based attacks are in the unstructured data of attachments. This means that simply by applying common standards it is possible to significantly reduce the level of threat very significantly**
- **Security experts G Data calculate a new type of malware is being created once every 4.2 seconds**
- **75 per cent of the malware disarmed by innovators using file-regeneration technology has been found to be unique to each target**
- **Current traditional signature based anti-virus and associated reactive technologies are failing by 10 per cent and more in email gateways**
- **The only effective solution to defend against these attacks and the deliberate corruption of email-bound documents lies in file-regeneration technology that produces a benign, sanitised file at sub-second speeds which is checked against the manufacturers' standards**

1. The types and sources of cyber threats to Critical National Infrastructure (CNI) in the UK

1.1 Email attachments are the easiest route into any organisation's systems because they are so vital to the conduct of everyday business. Even with the advent of new collaborative messaging platforms email will still remain the primary business communication technology of choice for the foreseeable future due to its wide adoption and ease of accessibility.

1.2 More than 90 per cent of successful cyber-attacks commence with the triggering of malicious code in an email attachment. Email attachments such as Word files or Excel spreadsheets are part of the explosive growth of unstructured data that is providing criminals with their biggest opportunity. We know that 70 per cent of file-based attacks are in the unstructured data of attachments. This means that simply by applying common standards it is possible to significantly reduce the level of threat very significantly.

1.3 Unfortunately, the sophistication of social engineering now makes it extremely difficult to ensure that thousands of employees always spot the emails sent by criminals that lure them into unwittingly clicking on malicious code.

1.4 Cyber criminals of all backgrounds have become adept at hiding malicious code in the structure of common office documents or an attached functional element, such as a macro or Javascript. They then pair the attachment with a socially-engineered email that deceives an employee into clicking on the document and triggering an instant ransomware attack or a zero-day malware download.

1.5 As a result of the open nature of email and the inherent security risks that go along with this method of communication all the component organisations that make up our CNI and Critical Economic Infrastructure need to vastly intensify their efforts to protect themselves from this vector.

1.6 Reliance on traditional anti-virus technology to defeat these threats is doomed to failure. The anti-virus industry's gatekeepers cannot keep up with the pace of invention among criminals and are incapable of identifying the new pieces of code that indicate an attack is being attempted.

1.7 Acknowledged security experts G Data calculate a new type of malware is being created once every 4.2 seconds. Typical AV and associated reactive technologies are failing by 10 per cent and more in email gateways, which leaves millions of pieces of malware free to enter an organisation.

1.8 In addition, testing by the Department of Homeland Security and National Security Agency has found that the data collected by the anti-virus industry through heuristics is misleading.

1.9 Vastly increasing this level of threat, 75 per cent of the malware disarmed by innovators using file-regeneration technology has been found to be unique to each target, with new malware wrapped up in a new file each time. This increases the amount of time it takes for identification with conventional AV security, offering far greater opportunities for compromise.

1.10 Among the hackers most recent exploits is the latest variant of Locky ransomware which has been tailored to exploit a glaring long-term vulnerability in Windows, using Microsoft's Dynamic Data Exchange (DDE), a feature that allows the transfer of data between Windows applications, and almost is exclusively used to point to data sources inside a network. Hackers have discovered how to use DDE to distribute 'weaponised' Office documents posing as legitimate documents such as invoices which contain ransomware.

1.11 Supply-chain partners too are now vulnerable to being employed as malware hubs as criminals penetrate the security of their devices. Once criminals have secreted their malware on a PC, scanner or PDF-writer, professional bodies and service-providers can unwittingly become hubs for the distribution of malware to more high-profile or valuable targets.

1.12 Sandboxing solutions are also barely effective, since hackers are able to write code that recognises a sandbox environment and temporarily shuts itself down until it has passed through.

1.13 And despite best-practice training and easily-available threat information, employees in nationally critical organisations continue to open attachments that appear to be from familiar people or companies. Glasswall research found that 62 percent of survey respondents admitted they do not check the legitimacy of email attachments that come from an unknown source, while a small, but dangerous minority said that they always or usually trust email attachments from people they have never heard of.

1.14 Defeating the polymorphic nature of these new threats requires innovation such as file-regeneration technology. This supplants targeting the bad, with techniques that look for and validate the "known good" in each file, rendering the constant innovation of criminals redundant. No matter how inventive the criminals are, any departure from the manufacturer's standard in common file-types such as Word, Excel, PDF or PowerPoint will fail to be admitted to the

organisation, whether it is in the active elements or as is increasingly the case, in the structure of the file itself.

1.15 Validating a file's legitimacy against its "known good" in the manufacturer's standard – right down to byte level – provides a point of comparison that cannot be bettered. A clean and benign file in its original format is generated in fractions of a second, which can be sent out again and passed along without any interruption to business.

1.16 This enables organisations to reassert control and bring security to the file-level, which is where it is most needed. Critical infrastructure businesses can give themselves the initiative by using this technology's deep file-inspection, remediation and sanitisation tools to eliminate malicious documents before their systems.

1.17 Although there is no silver bullet in cyber security, file-regeneration is the most immediate solution to the threats faced by our CNI and CEI.

2. The extent to which the Government's definition of 'critical national infrastructure' is still valid in an interconnected economy

2.1 Definitions of Critical National Infrastructure remain valid.

2.2 As the nature of our infrastructure has become more diverse and dispersed, so too have the points of vulnerability. With even the smallest of devices connected to the Internet of Things (IoT), each has now become a potential gateway to the entire system of a power company or transport network. Consequently, employees, many of whom carry company-provided smart devices, provide a dual pathway for hackers into business systems and personal infrastructure.

2.3 The attack on San Fransisco's MUNI transport system (2016) showed how criminals or activist disruptors can cripple a city, while data breaches ranging from activities during the last US election, to the National Health System in the UK have put sensitive private data in the hands of unknown, and in many cases, state-sponsored, hacking groups.

2.4 Although alarming, none of these attacks were quite as severe in terms of the scale of infrastructure affected as the attack on the Ukrainian energy grid in December 2015, which plunged thousands of home into cold darkness.

2.5 Investigations subsequently attributed the disruption to a BlackEnergy malware attack that targeted and successfully infected the systems of three regional operators, making it the first power outage in history to be publicly confirmed as caused by hackers.

2.6 The developers of BlackEnergy, dubbed the Sandworm Gang, are believed also to have been responsible for a handful of attacks aimed at government agencies in Ukraine and Poland, including a 2014 breach targeting the North Atlantic Treaty Organisation. In Ukraine's tense political climate, certain authorities were quick to blame the Kremlin, though evidence of any connection between the Sandworm Gang and Moscow has so far been unproven.

2.7 Just weeks after the blackout in Ukraine, Israeli Energy Minister Yuval Steinitz shocked those attending the CyberTech 2016 computer security conference with news that the nation's Electricity Authority had been the target of a "severe" malware attack. Though Steinitz was adamant that the attack did not result in any power outages, The Times of Israel reported that some of the authority's computer systems had to be shut down for two days following the attack.

2.8 The world of cybercrime expands each day, leading to the current state of affairs in which even national infrastructure organisations are vulnerable to the growing sophistication of hackers. To audiences around the world, the ability of hackers to worm their way into critical infrastructure

and even cause mass blackouts is understandably shocking. To those with a deep familiarity of the cyber security field, this handful of events, while still alarming, has not come as such a surprise.

3. Learning points drawn from the 2011 Cyber Security Strategy and the fitness for purpose of the 2016 Cyber Security Strategy in relation to CNI

4. The effectiveness of the strategic lead provided by the National Security Council, Government Departments and agencies, and the National Cyber Security Centre, and the coherence of cross-government activity

4.1 The government's launch of the National Cyber Security Strategy has been excellent news, given the huge growth in the dangers to businesses around the globe from targeted attacks, such as threats hidden in email attachments.

4.2 The National Cyber Security Strategy still needs to come to terms with the severe dangers posed by these threats and embrace the technological innovation which is needed. Conservatism and reliance on outdated methods are still in danger of undermining our defences.

4.3 The majority of organisations are still deploying security solutions that search in the wrong places and are designed to remove previously identified threats or signatures. But the reality is that criminals have moved on and are attacking the lifeblood of organisations, striking at the heart of the business email systems with weaponised documents.

4.4 There must be wider recognition that traditional signature-based AV security no longer cuts the mustard and that criminals are also using social engineering techniques, gaining a detailed picture of people and organisations all along the supply chain so they can achieve maximum impact.

4.5 While investment in cyber-security training is a positive step, too much of the focus is on detecting and mitigating attacks that have already happened. Prevention is much better than cure and innovative solutions that eliminate malware attacks must be the way forward, allied to an approach that hands the initiative back to organisations by putting them in charge of security policy in relation to files.

4.6 The only effective solution to defend against these attacks and the deliberate corruption of email-bound documents lies in file-regeneration technology that produces a benign, sanitised file at sub-second speeds which is checked against the manufacturers' standards.

4.7 The government's investment in the recruitment of cyber security talent has been very encouraging, however. With billions of connected devices in the world, we need bold innovation. The government's vigour in tackling the menace of cyber-crime now needs to be taken as seriously in CNI and CEI.

4.8 Why is it though, that many national infrastructure organisations have a legacy of utilizing outdated IT and operating systems, such as Windows XP, that are no longer supported by manufacturers? Reliance on Windows XP or inadequate security patching were blamed for leaving NHS hospitals open to the WannaCry ransomware attack in May this year.

4.9 We need greater speed of innovation. Once something is deemed functional and reliable with a good safety record, there is less motivation to update or upgrade it. More alarmingly, malware running on Industrial Control Systems (ICS) networks is sometimes tolerated for longer periods, provided it does not disrupt operations. This has to end.

5. The effectiveness of the Government's relationships with, respectively, private-sector operators and regulators in protecting CNI from cyber attack

5.1 There has been minimal legislation globally to drive cyber risk-reduction to protect industrial control systems (ICS). No government seems motivated to make any significant changes to the status quo when addressing the risks associated with ICS and Supervisory Control and Data Acquisition (SCADA) systems.

5.2 The question must be asked about government policy that allows some the world's largest organisations the freedom to operate with fewer restrictions. National infrastructure organisations which do not have adequate security measures in place are jeopardizing their financial viability and potentially putting the livelihoods – and even lives – of employees and citizens at risk.

6. The balance of responsibilities between the Government and private-sector operators in protecting CNI against cyber attack

7. The consistency of approach in the UK to legislation, regulation and standards governing each CNI sector and cyber security

8. The availability of skills and expertise to the relevant Government Departments and agencies, to regulators and to private-sector operators of CNI

9. The extent to which the UK's approach to the cyber security of CNI draws on or represents international best practice

9.1 We can learn from the example of the North American Electric Reliability Corporation (NERC), which is a not-for-profit corporation designed to improve the reliability and security of the bulk power system in the United States, Canada and Northern Mexico. As the federally-designated Electric Reliability Organization (ERO) in North America, NERC develops and enforces mandatory standards that define requirements for reliable planning and operation of the bulk power system.

9.2 NERC has been instrumental in implementation of the Critical Infrastructure Protection (CIP) standard, which provides a cyber security framework for the identification and protection of Critical Cyber Assets that control or affect the reliability of North America's bulk power systems. In 2006, the US Federal Energy Regulatory Commission (FERC) made the CIP Cyber Security Standards mandatory for all Registered Entities identified by NERC, and enforceable across all users, owners, and operators of the bulk power system in the United States.

9.3 NERC and its regional entities also routinely monitor compliance. A number of methods, including regular and scheduled compliance audits, random spot-checks, and additional specific investigations as warranted, are used to identify where the standard may have been violated. Failure to comply can result in fines of up to $1 million per day, per incident, until a state of compliance is ultimately achieved.

-End-

Glasswall Solutions Limited – January 2018