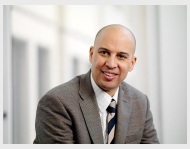
Growing Threat Information Sharing Beyond Detect and Respond

Bernard Parsons



Bernard Parsons
CEO and Co-Founder
Becrypt

Biography

Bernard Parsons is the CEO and Co-Founder of Becrypt (www.becrypt.com).

Establishing Becrypt in 2001 with the aim of addressing the growing security requirements of endpoint technology, Bernard has built the company into a leading supplier of end-user device security products and services, with a focus on product assurance, multiple platform support and flexible delivery: from being embedded within the platform, to hosted within the Cloud.

Furthermore, Bernard has ensured Becrypt helps the most security-conscious organisations to be positioned as leaders in enabling value from the use of secure technology.

For his dedication to digital technology, Bernard was bestowed with an MBE in the 2018 New Year's Honours List.

Keywords (*keywords to be supplied by Ellen)*
Paper type Research

Abstract

There has been considerable talk in recent years about the importance of cybersecurity information sharing. By exchanging cyber threat information within a sharing community, organizations can leverage the collective knowledge, experience, and capabilities of that sharing community to gain a more complete understanding of the threats the organization may face. However, many organizations are wary of sharing sensitive cybersecurity information, yet those which share cyber threat information can improve their own security postures as well as those of other organizations.

Introduction

Threat information sharing is recognised as an important and evolving topic within cyber security. The need for organisations to collaborate on the protection of IT systems is, in part, driven by the highly collaborative and diverse ecosystem of threat actors, with an ever-greater overlap of tools, techniques and teams targeting the public and private sector. Where organisations effectively share experiences and insights that may be unique to them, broader communities can benefit at scale – a rising tide lifts all boats.

IT Security

Much has been done to improve the sharing of threat intelligence, both nationally through the National Cyber Security Centre's[1] (NCSC) Cyber Security Information Sharing Partnership[2] (CiSP), as well as within specific communities of interest. However, it continues to be recognised that more needs to be done, as reflected by initiatives such as the Financial Sector Cyber Collaboration Centre, announced by UK Finance in 2018. Calls continue for Government, or specifically the NCSC, to share more advanced threat intelligence given their unique visibility of the evolving threat landscape.

However, balancing the risks associated with information disclosure, relating to both vulnerabilities and evolving adversary capabilities, will always create a practical limit to both the speed and extent to which this can be done.

Evolving cyber defence

There is, however, another area in which the NCSC possesses unique capabilities that is both valuable to the industry and easier to share, but which has to date been demanded far less. Threat intelligence sharing is primarily about detection and response, however in its role as the National Technical Authority, much of the NCSC's guidance, as delivered to Government, is focused initially on defence. After all, architecting systems that are well protected and minimise the likelihood of compromise is the first step to a successful detection and response strategy.

In the pre-NCSC era, very little of the architectural advice for the Government's classified networks would have been relevant to the needs of many in the private sector. Government systems were typically built as bespoke, expensive and exhibiting poor usability, with all system requirements subservient to security – an approach which, ironically, often undermined security.

In recent years, the Government has evolved to make better use of modern technology and meet the expectations of a modern workforce. As a result, many of the newer Government systems, even those that operate at higher levels of classification, now leverage commercial technology. This offers the levels of functionality, flexibility and usability that private sector employees would be familiar with, whilst still achieving the levels of security required for sensitive Government systems.

However, as far as information sharing is concerned, relatively little has so far been done, in terms of more broadly communicating the innovations and experiences gained within government in recent years.

Moving towards informed risk management

Cyber-related IT transformation within Government has been achieved by significant advances at product and architectural level. This has been driven by both the NCSC's world-leading expertise and the shift within exemplar Government departments towards informed and effective risk management.

The resulting 'defence in depth' architectures allow departments to proportionately manage the risks that are important to them. This can be achieved by employing

IT Security

products that provide a high degree of assurance against well-articulated security claims – claims that can be independently validated. High Assurance products deployed within appropriate architectures allow risk to be quantified in a way that is difficult to achieve in systems that are primarily reliant on probabilistic defences – be that signature or other forms of anomaly detection.

Such technologies may be necessary but are not sufficient for achieving well-quantified and well-managed technical risk in today's diverse and evolving environments. This encapsulates cloud, mobile big data, IoT and the myriad of technology trends that even the most security-conscious organisations need to adopt at pace.

Driving demand for better cyber

The broader sharing of relevant guidance by the NCSC certainly shows signs of growing, with recent examples being published architectures for secure data import, and publicising work focused on secure mobility.

However, the pace and extent of sharing does need to be driven by demand from the private sector. Arguably today, the market is far from optimised to drive demand for better cyber security technology and services. One absent market lever is the necessary assurance schemes and standards that can appropriately define what good looks like, and how technical risk can be better quantified and managed.

Existing schemes are not yet sufficiently mature to cope with the scale, agility and innovation required. Instead, many organisations are reliant on the more subjective opinions of sources such as industry analysts, who may be more subject to marketing budgets than an informed and detailed analysis of a new product or service capability.

Encouragingly, the Government does have a current focus on innovating in the product and service assurance spaces, with active initiatives within the NCSC and through the Cyber Growth Partnership (CGP). The CGP in particular is keen to reach out to broader stakeholder communities, encouraging the private sector to play a greater role in such initiatives.

This is being achieved through using its unique perspective to help inform and improve the common standards of assessing technology and best practice, particularly for the sometimes slightly under-valued topic of cyber defence. If successful, the UK would be well positioned within the domain ofcyber, to establish a rising tide that does indeed lift all boats.

Reference	
1	https://www.ncsc.gov.uk/
2	https://www.ncsc.gov.uk/section/keep-up-to-date/cisp