CROWDSTRIKE

REQUEST FOR COMMENT RESPONSE

Proposal for New Telecoms Security Regulations and Code of Practice

May 10, 2022

I. INTRODUCTION

In response to the Department for Digital, Culture, Media & Sport's request for consultation on its proposal for new regulations and code of practice for telecoms security, CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. Our European Headquarters is based out of Reading UK, and we support a variety of UK organisations from FTSE100 to the Public Sector. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive threat hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organisations from data breaches and a variety of other cyber threats.

II. COMMENTS

The Department for Digital, Culture, Media & Sport has written thoughtful proposals on new regulations and a code of practice with the goal of improving the security of public telecoms networks and services. While we do not have feedback on every aspect, we do want to offer several points that may be of value to the Department as it continues the development of its proposals.

A. Principles-Based Frameworks Are Future Flexible

We applaud the Department's aim to enhance security in the critical telecommunication sector. In doing so, we believe that it is important to follow lessons learned from the financial sector and draw distinctions between

outsourcing critical operations versus augmentation of IT and security platforms. It is our observation that technologies and methodologies designed to achieve the aims of the proposed code of practice are increasingly dependent upon cloud-native approaches, cross border data flows, and 24/7 global threat hunting. Consequently, we advise a more nuanced approach than making a distinction to whether or not a vendor stores data in the UK as a key security risk factor.

Cybersecurity is best achieved where access to network data by defenders is permitted with practical safeguards, while unintentional transfers of such data via data breaches are thwarted by protecting against ever-evolving cybersecurity threats with innovative technologies. As a leading cybersecurity provider, it is our view that perhaps the most significant threat to telecommunication providers comes from threat actors operating unlawfully. While responsible operators and vendors adhere to robust compliance programs, cyber adversaries do not play by the cross border transfer rules.

We believe today's economy depends more than ever before on cross-border data flows and data portability. This trend will continue, especially in light of the digital transformation accelerated by Covid-19 and the "work from anywhere" movement. The importance of cross-border data flows is far-reaching, and affects individuals, entities, and society more broadly. Any restriction on cross-border data flow or data portability requirements could have adverse implications for UK innovation, jobs, access to services, and effective cybersecurity. This means that it is critical to provide telecommunications organisations with deference to make their own context-informed—and critically, risk-informed—decisions about cross-border data by adhering to core data protection principles related to the circumstances of specific transfers.

In order to remain future-flexible, it is important to prioritize the goal of protecting data regardless of where it is, rather than equating data protection with restrictions on cross-border data transfers and data portability. Consequently, providing as many means as possible to lawfully transfer data abroad will continue to afford UK telecommunication organisations the ability to create and use innovative technologies, including data security and privacy technologies, on a global scale.

Further, cross-border data flows and unrestricted data portability are necessary elements of some of today's most sophisticated cybersecurity solutions. Many of the most innovative technologies for protecting personal data against data breaches leverage global endpoint telemetry data, cloud-native Software-as-a-Service (SaaS) delivery, 24/7 global threat hunting, and cross correlation of indicators of attack. Moreover, modern IT infrastructure in general operates at cloud-scale and invariably involves cross-border data transfers.

B. Cybersecurity Best Practices

The Department has outlined some impactful security-focused points as it relates to how telecom networks and services can be secured, including preventing unauthorized access, active monitoring, remediation and recovery, as well as possible issues related to supply chains. Specifically, when assessing Regulation 6, it is important to ensure that telecommunications providers can achieve their aims by employing the very technologies and methods used by the most sophisticated regulated and unregulated entities. Here, we offer our views on effective security practices for the telecommunications industry.

i. Preventing unauthorized access

In situations where the actor does use broader or more ambitious targeting, they must still move laterally, escalate privileges, and take related steps to achieve their goal(s). Here, many more general cybersecurity practices and systems apply, and can help defenders identify and mitigate the breach. Endpoint tools can be most effective to this end because they provide granular information for analysis and do not rely upon expressly suspicious actions to generate detections, like many other types of defensive tools.

CrowdStrike recommends:

a. **Use risk-based conditional access to trigger MFA only when required to achieve the true "never trust" ethos of Zero Trust**. On the one hand, this can reduce friction for low risk, permitted use. On the other hand, this can radically increase barriers against unpermitted use, to

include dynamically presenting suspicious users/uses with a new MFA challenge within a permitted session.

b. **Extend identity requirements even to unmanaged systems or legacy systems that cannot typically use MFA.** By monitoring and using credentials (including SSO) tied to users and applications of those systems that can directly force an MFA, a risk based conditional access model can be setup to examine behavioral signals of identities (in real-time) at the identity store and determine anomalous activity that may require an MFA to be triggered by the monitoring system.

c. **Enforce the principle of least privilege at the identity-level**. Least privilege seeks to limit the scope of any system, effectively limiting the impact (or "blast radius") of a breach. Identity based segmentation monitors a user or application by the use of its credential, which is not based on the physical location or deployment model.[1] This can include where and how the credential is used, behavioral usage analysis, and other factors.

ii. Active Monitoring

Cybersecurity threats are exceptionally broad, and active monitoring fills an essential role. From our experience, defenders' key responsibility is **threat hunting**. Whether through supply chain attacks or otherwise, we know that adversaries periodically breach even very-well defended enterprises. Properly trained and resourced defenders can find them and thwart their goals. In our experience, whether organisations accept this premise -- that cybersecurity involves not just a passive alarm, but a sentry actively looking for trouble -- is the leading indicator of the strength of their cybersecurity program.

Central to hunting is properly instrumenting enterprises to support both automated and hypothesis-driven adversary detection. And the better-instrumented the environment, the more chances defenders give

[1] Traditional models of enforcing least privilege utilize network based segmentation, which relies upon limiting the application or user by IP address, domains, router rules (eg. ACLs), port communication, and other methods. Since most modern IT environments are hybrid and dynamic (and are not trivial to modify), these policy rules must be updated often and eventually fail to restrict the scope as a result.

themselves to intervene as a breach attempt progresses through phases, commonly referred to as the kill chain. Multiple opportunities for detection help avert "silent failures" -- where a failure of security technology results in security events going completely unnoticed.

iii. Remediation & Recovery

Some of the keys to a strong cybersecurity posture today include:

- **Speed**. We advise users that when responding to a security incident or event, every second counts. The more we can do to detect and stop adversaries at the outset of an attack, the better chance we have to prevent them from achieving their objectives. The reason for this is that adversaries move fast, especially when engaging in lateral movement through an enterprise. This means that measuring response time and severity, essentially a DEFCON for security, is critical to ultimately stopping a malicious chain of events and improving performance.

- **Machine Learning-Based Prevention**. The core of next-generation cybersecurity solutions is the ability to defeat novel threats. Machine learning and artificial intelligence are essential to this end, and leveraging these technologies is the best way to gain the initiative against adversaries.

- **Identity Protection and Authentication**: As organisations embark on a digital transformation to work from anywhere models, Bring-Your-Own-Device policies become commonplace, and cloud services multiply, enterprise boundaries continue to erode. This trend increases the risk of relying upon traditional authentication methods and further weakens obsolescent legacy security technologies. Identity-centric approaches to security use a combination of real-time authentication traffic analysis and machine learning analytics to quickly determine and respond to identity-based attacks.

- **Zero Trust.** Due to fundamental problems with today's widely-used authentication architectures, organisations must incorporate new security protections focused on authentication. Zero Trust design concepts radically

reduce or prevent lateral movement and privilege escalation during a compromise.

- **Extended Detection & Response (XDR).** Cybersecurity threats are exceptionally broad, and for too long industry players have focused on narrow solutions. No box on a network or a single-purpose software agent will address the full scope of the problem. Security teams demand contextual awareness and visibility from across their entire environments, including within cloud and ephemeral environments. The XDR concept seeks to apply order to a sometimes chaotic array of security tools by deriving actionable insights wherever they exist within the enterprise, and generate intelligence from what otherwise may be an information overload.

iv. Supply Chain

An initial intrusion or data breach is not always an adversary's end goal, and increasingly, threat actors leverage software supply chain attacks to achieve scale or compromise hard targets. Fundamentally, securing the supply chain is a complex third-party partner and vendor risk management problem that spans across numerous disciplines. It demonstrates that cybersecurity is an ecosystem issue, where organisations impact one another, either for better or worse.

We applaud the Department for recognizing this issue in the context of telecommunications vendors but again emphasize the importance of permitting telecommunication providers to exercise deference and discretion based on use case and risk mitigation factors when conducting an assessment. We note that different organizations, including those that offer third party services (such as acting as managed security services providers), will not in all cases have the same set of security controls, processes, or methods as their partners or customers. For example, expectations for uniform security program parameters may weaken third parties' ability to develop stronger security or risk management programs than their customers, which would potentially weaken security for each party. Uniform minimum standards may be appropriate in some instances but may reduce organizations' ability to design programs to their particular threat model(s). Adversaries are increasingly innovative and in practice not all organisations will be able to evolve their security controls in unison to defeat threats.

III. CONCLUSION

The Department's proposal provides a thoughtful analysis of a complex legal and policy area. As the Department moves forward, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend and emphasize that any legislative updates and proposed rulemaking focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/.

V. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley CIPP/E
VP & Counsel, Privacy and Cyber Policy

Robert Sheldon
Director, Public Policy & Strategy

Email: policy@crowdstrike.com

***