REQUEST FOR COMMENT RESPONSE

European Data Protection Board: Guidelines 01/2021 on Examples regarding Data Breach Notification (adopted 14 January 2021)

2 March 2021

I. INTRODUCTION

In response to the European Data Protection Board's (EDPB) request for public consultation on *Guidelines 01/2021 on Examples regarding Data Breach Notification* ("Guidelines"), CrowdStrike offers the following views.

We approach this public consultation from the standpoint of a leading international, US-headquartered cloud-native cybersecurity provider, with various establishments in the EU, that defends globally-distributed enterprises from globally-distributed threats such as intellectual property theft, financially-motivated crime, destructive attacks, and data breaches. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is shaped by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

We welcome the opportunity to consult on this complex and important matter. It is clear from the draft Guidelines that the Board has invested considerable time and effort into addressing possible breach scenarios. We think the approach used in the Guidelines, distinguishing between confidentiality breaches, integrity breaches, and availability breaches, is thoughtful and appropriate. Further, we appreciate the level of detail provided and believe the selected cases offer a realistic and relatively comprehensive representation of contemporary breach issues.

A. *EDPB's Selected Examples of Breach Notifications*

In addition to the examples provided by the draft Guidance, CrowdStrike, with its frontline experience, believes it is important to contemplate several additional scenarios.

1. *Cloud-centric breaches*

As workloads and data storage increasingly move from traditional endpoints to cloud offerings, cyber threat actors have expanded their targets. In fact, cyber threat actors often do not discriminate between personal or general, on-premise enterprise environments versus cloud environments. They target resources and data wherever they exist, and frequently move between local and cloud environments in an attempt to achieve their objectives.[1] This is one reason why accidental data exposures that happen through, for example, misconfigured cloud storage environments are also increasingly a source of potential privacy issues. Moreover, threat actors use cloud hosting to disguise their intrusions as benign network traffic, and a variety of legitimate software and cloud hosting services to access company networks.

2. *Infiltrated Networks*

In 2020, CrowdStrike Intelligence observed a great number of state-sponsored threat actors infiltrate networks to steal valuable data on vaccine research and government responses to the pandemic.[2] Such infiltrated network attacks may be used for other purposes and represent another common method used by threat actors to access data.

3. *Initial Access and Exploitation*

[1] George Kurtz, Testimony on Cybersecurity and Supply Chain Threats, Senate Select Committee on Intelligence (Feb. 23, 2021), https://www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary.

[2] CrowdStrike's Threat Report 2021, https://www.crowdstrike.com/global-threat-report.

Monitoring tools are another method by which company networks are compromised. Once installed, monitoring tools have the ability to collect information about the host, enumerate files and services on the system, make HTTP requests to arbitrary URLs, write/delete/execute arbitrary files, modify registry keys, terminate processes and reboot the system.[3]

That said, overbroad guidance could have adverse implications by exposing individuals or entities to a high volume of extraneous notifications and thereby desensitizing the importance and purpose of such notifications. We recommend that guidance on cloud environments observe the distinctions we enumerate in **section B** ("Critical Distinctions within Breach Notifications"), below.

B. *Critical Distinctions within Breach Notifications*

In general, we believe breach notification guidance should reflect the following distinctions:

1. *Alerts v. Incidents*

In cybersecurity, an important distinction exists between alerts and incidents, which should help inform notification scenarios and standards. In most cases, those using contemporary cybersecurity solutions should be alerted to malicious activity occurring in their environment. The nature of these alerts may vary, and could cover something like the installation of malicious software on one system, or the compromise of a single account. In scenarios where defenders see these alerts and address them quickly, then frequently such an issue does not meet any reasonable standard of a cybersecurity "incident," where the threat actor has not meaningfully achieved their objective, accessed sensitive information, and the like.

These scenarios emphasize a few key points. The first is the importance of speedy detection and response. At CrowdStrike, we recommend that organizations measure performance in metrics and meet the "1-10-60 Rule," which holds that defenders should aim to be alerted to a security issue within one minute; have a

[3] CrowdStrike's Threat Report 2021, https://www.crowdstrike.com/global-threat-report.

human investigate it within 10 minutes; and isolate or remediate the issue within 60 minutes.[4] The second is to "hunt" aggressively for threat actors within a network, because frequently automated systems fail to alert defenders to sophisticated threat activity, which must be found through hypothesis-driven searching. Third, and most importantly, it takes big data to support the first two objectives. In cybersecurity, raw telemetry data about computer processes, which may include identifiable information, is integral to distinguishing signals from noise. Sometimes, it is only by virtue of collecting this data early detection is possible, and breaches can be contained before the rise to the threshold of becoming major incidents.[5]

2. *Impacts vs. Serious Impacts*

Another important distinction that merits discussion is that of impacts versus serious impacts. Not all breaches have the same level of severity. For example, an incident where a threat actor sees a list of user names might have a small or negligible impact on affected parties. Whereas, another incident in which a threat actor exfiltrates complete financial or medical records may have a severe impact.

The standard used in case 2.1 (paragraph 21, "The data controller should consider the impact and severity of the breach") is consistent with GDPR's risk-based approach to data breach notification and should be emphasized throughout the Guidance. Consideration of the impact and severity of a breach is important not only when initially assessing evidence of an intrusion but also in discerning the efficacy of mitigation measures. Consequently, this criteria should explicitly inform risk determinations in assessing whether or not there is an actual risk to the rights and freedoms of data subjects.

[4] A more in-depth explanation of this concept is available here: https://www.crowdstrike.com/resources/crowdcasts/the-1-10-60-minute-challenge-a-framework-for-stopping-breaches-faster/.

[5] CrowdStrike, Data Protection Day: Harnessing the Power of Big Data Protection, https://www.crowdstrike.com/blog/data-protection-day-cybersecurity-best-practices/

3. *Mitigated vs. Unmitigated Impacts*

The final distinction is that of mitigated impacts versus unmitigated impacts. Threat actors may choose to target an organization in a series of steps, rather than in a single attack. In fact, an initial intrusion into an enterprise is often not a threat actor's end goal. Instead, threat actors may first deploy a backdoor, harvest credentials, or use other methods in order to move laterally throughout a network and to their ultimate objective.[6]

A threat actor may be stopped at any of the steps in the killchain, and this raises important questions that impact the breach notification process - namely, if a breach is mitigated, does the obligation to notify still exist? For example, if a threat actor enters an enterprise with the goal of exfiltrating data but is stopped before the infiltration occurs, the possible resulting impact of the incident has been mitigated. In such an example, it is a breach when the threat actor enters the network but it could have been a substantial breach if the goal of data exfiltration was reached. Ultimately, this means that a data breach in and of itself may not pose a risk to the fundamental rights and liberties of data subjects where successful steps have been taken to mitigate the breach and prevent exfiltration.

C. Commentary on Breach Notification Process and Style

We would like to emphasize the importance of enabling a quick and easy breach notification process. Our recommendation is that there should be a common template, applicable across all EU member states. A standard template would be most effective if it was available in a common language and permitted reporting in a common language, such as English. In an era of cross-border data breaches, such standardization would streamline breach reporting by reducing administrative burdens and complexities, empowering affected parties to comply with obligations while also creating a rich EU-wide breach dataset for assessing trends and informing policy making.

[6] George Kurtz, Testimony on Cybersecurity and Supply Chain Threats, Senate Select Committee on Intelligence (Feb. 23, 2021), https://www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary.

CrowdStrike supports the future application of an appropriate one-stop-shop mechanism while bringing clarity to the exceptions that would allow data protection authorities, besides a lead supervisory authority, to act on cross-border action.

Moreover, speed is of the essence. As CrowdStrike advises its customers and emphasizes here, every second counts when responding to a data breach, security event or incident. Mere seconds can be the difference between stopping a threat actor at the outset of an attack or allowing them the opportunity to continue lateral movement through an enterprise and achieve their objective. Threat actors move quickly and thus, measuring response time and severity is critical to stopping malicious events.

For this reason, CrowdStrike would welcome an easy to access, joint, central breach reporting tool on a European level in plain language to help organizations submitting international breach notifications. The reporting should be accepted in English language in order to reduce time spent necessary for engagement of external counsel and translation.

D. Guidance on Appropriate Security Measures

CrowdStrike believes that breaches can be prevented by ensuring that appropriate organizational, physical and technological security measures have been taken. For example, it is vital for organizations to incorporate new security measures that put an emphasis on authentication, such as Zero Trust. Zero Trust requires users to reauthenticate or re-establish permission for whichever device or resource they want access to, as opposed to authenticating once on a device and automatically having access to all the resources therein.[7] This holistic view of authorized identity helps to reduce or prevent lateral movement and privilege escalation during a security incident or event.

[7] CrowdStrike's Threat Report 2021, https://www.crowdstrike.com/global-threat-report.

There is often a misconception that breaches can only be stopped through proper patch management and by the use of appropriate anti-malware detection systems. In reality, cybersecurity threats are exceptionally broad and niche solutions can be too narrow. The full scope of a problem will not be resolved by a box on a network or a single-purpose software agent. Effective breach prevention requires contextual awareness and visibility across environments, including within cloud and ephemeral environments.

Many data breaches take place without the use of malware, leveraging instead harvested credentials, misconfigured account services, native or legitimate administration tools, or supply chain attacks.[8] Accordingly, appropriate security measures must include more than anti-malware detection systems and patch management. For example, the European Union Agency for Cybersecurity (ENISA) advises in its "State of the Art" guide that extended detection and response (XDR) solutions should be considered to protect against breaches.[9] XDR seeks to apply order to a sometimes chaotic array of security tools by deriving actionable insights wherever they exist within the enterprise, such as from endpoint detection and response (EDR) data, authentication logs, and network telemetry. Consequently, we recommend that the EDPB's guidance echo ENISA's recommendations and use all-encompassing nomenclature to reflect security technologies beyond "anti-malware detection systems."

III. CONCLUSION

The EDPB's recommendations are a thoughtful response to the complex legal and policy issue of data breach handling and management. CrowdStrike is in the business of data protection and presents its feedback in the context of understanding the diversity of its own customers IT management and security organizations, as well as technologies dependent upon cross-border data flows. As the EDPB further considers the proper guidelines regarding breach notification, we

[8] CrowdStrike's Threat Report 2021, https://www.crowdstrike.com/global-threat-report.

[9] IT Security Act (Germany) and he EU General Data Protection Regulation: Guideline "State of the Art" Technical and Organizational Measures, Teletrust (2021), https://www.teletrust.de/fileadmin/user_upload/2021-02_TeleTrusT-Guideline_State_of_the_art_in_IT_security_EN.pdf.

reiterate the importance of reviewing with an eye towards protecting personal data in a holistic manner that incentivizes the adoption of strong cybersecurity safeguards. Threat actors innovate at a record-pace, and it is important to determine clear and common rules for quick and easy data breach notification that applies to ever-evolving threats. Ultimately, parties responsible for data should be incentivized not only to prevent breaches but also to mitigate the impact in the event of a breach. Consequently, guidance should also promote the adoption of sophisticated security safeguards to protect against breaches.

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 4 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. Privacy and public policy inquiries should be made to:

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

Dr. Christoph Bausewein CIPP/E
Director & Counsel, Data Protection & Policy

Email: policy@crowdstrike.com

***