CLCT

WILLIAM & MARY
LAW SCHOOL

Cybersecurity and Information Security Newsletter

Issue 3 | September 3, 2020

Table of Contents

Please feel free to submit cybersecurity and information security news items or request related topics to Daniel Shin (dshin01@wm.edu).

Police body cameras sold on eBay contain video footage

Background

Hackers reportedly purchased discarded Axon police body cameras on eBay and were able to extract video footage using Foremost, a publicly available forensic data recovery software. *Introduction*, Foremost.

One of the hackers documented that the extracted video footage was not encrypted. @d0tslash, Twitter (July 1, 2020). The device that the hacker had purchased was a model from 2015 when encryption capabilities might not have been either available or mandatory to use for the camera. Based on the recovered video screenshots, at least one of the police body cameras probably belonged to military police at Fort Huachuca, a U.S. Army installation in southeast Arizona. Fort Huachuca houses various training facilities, including the United States Army Intelligence Center of Excellence. *U.S. Army Fort Huachuca*, U.S. Army. At the time of publication of this newsletter, it is still possible to find listings on eBay of Axon police body cameras.

Axon responded to this report by highlighting that the latest police body camera models have "enhanced security measures such as storage encryption to protect video from being retrieved from lost or improperly disposed cameras." Jerod MacDonald-Evoy, *Fort Huachuca Police body cam footage easily accessible after an eBay purchase*, AZMirror (July 2, 2020).

Analysis

Although encryption is an important tool to safeguard information, on its own it is not sufficient to fully protect all data that an organization may hold. Inventory management is another critical part of an effective cybersecurity and information security strategy. Setting up secure equipment disposal procedures, including the erasure of all data on data storage devices, is necessary to ensure that no sensitive information, including personally identifiable information, is inadvertently disclosed. Organizations should consider implementing best practices for data retention policies for all managed data during the entire data life cycle.

Merely deleting data may not be enough to prevent data recovery. Instead, organizations should consider additional measures, such as the clearing and sanitizing standards developed by the Department of Defense, to ensure that deleted data are not recoverable. *See*, *e.g.*, *SDelete v2.02*, Microsoft. As households purchase—and later discard—Internet-of-Things devices, consumers should also take extra steps to ensure that all data stored within discarded electronic devices have been removed before disposal.

Read the full article here.

Carnival reported ransomware attack and data breach in SEC filing

On August 17, 2020, Carnival Corporation ("Carnival") filed a Form 8-K with the U.S. Securities and Exchange Commission ("SEC") to report a ransomware and data breach incident that took place two days prior. Although there are no federal statutes mandating data breach disclosures, Carnival was mandated to report the ransomware and data breach attack under SEC regulations.

Background

Carnival reported that on August 15, 2020, it "detected a ransomware attack that accessed and encrypted a portion of [the company's] information technology systems. The unauthorized access also included the download of certain of [Carnival's] data files." Carnival Co., CURRENT REPORT Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 (Form 8-K) (Aug. 15, 2020). After detecting the intrusion, Carnival "launched an investigation and notified law enforcement, and engaged legal counsel and other incident response professionals."

Legal Background

After the stock market crash in October 1929, Congress passed the Securities Act of 1933 and the Security Exchange Act of 1934, which led to the creation of the SEC. The SEC was created to "restore investor confidence in [the U.S.] capital markets by providing investors and the markets with more reliable information and clear rules of honest dealing." *What We Do*, U.S. Securities and Exchange Commission.

Under federal securities laws, listed companies have legal obligations to meet certain reporting requirements aimed at informing investors and the SEC of relevant facts about the state of the company.

On February 21, 2018, the SEC published interpretive guidance "to assist public companies in preparing disclosures about cybersecurity risks and incidents." Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 17 CFR Parts 229 and 249. The guidance requires all publicly-traded companies to make timely disclosures of cybersecurity incidents through existing SEC reporting requirements. This requirement does not apply to not-listed companies.

Analysis

As a publicly-traded company, Carnival is regulated by the SEC. After discovering the cyber attack, the cruise line documented steps taken to remedy the incident and filed a Form 8-K under "Item 8.01 Other Events." The company determined that the cyber attack incident was an event deemed to be of importance for Carnival's security holders, even though "the Company does not believe the incident will have a material impact on its business." Carnival Co., CURRENT REPORT Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 (Form 8-K).

Carnival made a prompt cybersecurity incident disclosure to comply with SEC regulations. Although there is no federally mandated cyber attack disclosure law, current SEC regulations ensure that listed companies make prompt cybersecurity incident disclosures to protect investors. As such, SEC filings are an important source of information to track cyber attacks across the U.S. economy. Search SEC filings here.

Read the full article here.

Blackbaud paid a ransom to mitigate a data breach attack

Background

In May 2020, Blackbaud, a cloud software company incorporated in South Carolina, discovered and stopped a ransomware attack and a data breach. The company determined that a "cybercriminal removed a copy of a subset of data from [the company's] self-hosted environment," and the stolen data contained customer's data. *Security Incident*, Blackbaud.

Blackbaud paid a ransom to the cybercriminal to have all copies of the stolen data destroyed. After evaluating the situation, Blackbaud claimed that the company has "no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly." The company based this conclusion on investigations conducted by itself and third parties (which the company says includes law enforcement).

Although Blackbaud's Security Incident page does not identify which customers were affected by the cyber attack, at least three Virginia-based organizations are known to have been impacted by this incident: William & Mary, Virginia Commonwealth University, and the YMCA of Greater Richmond. *How a recent VCU data breach impacts alumni*, WTVR CBS 6 (Aug. 3, 2020).

Analysis

According to the National Cybersecurity Center of Excellence of the National Institute of Standards and Technology, having "an effective data recovery strategy and business continuity plan would eliminate the need to pay the ransoms," when an organization suffers a ransomware attack. Don Tobin, *Stop Paying Ransoms: Implement Data Recovery Strategy*, National Cybersecurity Center of Excellence (July 17, 2016). Paying ransom to cybercriminals does not guarantee that they will follow through with what had been agreed upon. On the contrary, paying ransom encourages other cybercriminals to continue pursuing ransomware attacks, because such attacks continue to be profitable. *Ransomware*, Federal Bureau of Investigation: Scams and Safety.

Unfortunately, paying ransom to cybercriminals is becoming a more regular occurrence. For example, in June 2020, the University of California, San Francisco, announced that it paid $1.14 million to cybercriminals to unlock encrypted data on computer systems within the School of Medicine. Davey Winder, *The University of California Pays $1 Million Ransom Following Cyber Attack*, Forbes (June 29, 2020). In another instance, the University of Utah confirmed in August that it paid $457,059 to prevent cybercriminals from leaking stolen student information online. Catalin Cimpanu, *University of Utah pays $457,000 to ransomware gang*, ZDNet (Aug. 21, 2020).

Similar to the University of Utah ransomware incident, Blackbaud claimed to have paid the ransom to ensure that the cybercriminal destroyed all copies of stolen data. From a risk perspective, stolen data is compromised data. There is no verifiable method to ensure that the cybercriminal deleted all copies of the stolen data. For instance, it is possible that the cybercriminal made multiple copies of the stolen data and placed them on different systems before entering into the ransom transaction. Even after a ransom is paid, there is still no guarantee of whether the cybercriminal carried out with his promise of deleting the stolen data.

Evidence of data deletion is difficult to produce and evaluate, especially if the deletion is conducted by an unknown third-party. A better approach is to assume that the stolen data is compromised permanently, unless law enforcement is able to apprehend the cybercriminal and obtain clear evidence that all of the stolen data was destroyed.

Read the full article here.