

March 28, 2024

Jim Agnew
CEO
Edge Imaging

Dear Jim Agnew:

**Re: Breach Notification - Cyber attacks
Edge Imaging File 1408-6198-4010
OIPC File P24-96000**

I am the investigator assigned to complete the monitoring of a privacy breach reported to this office on February 21, 2024. This report is made pursuant to section 36 of the *Personal Information Protection Act* (PIPA). This report examines the adequacy of protective measures taken by Hill International, Inc. (the organization) under section 34 of PIPA. This report makes findings and contains conclusions, but no order is made under section 52 of PIPA.

On February 5, 2024, Entourage, a third party service provider to Edge Imaging, recognized a cyber incident on its cloud server due to a compromised username and password of one of its server accounts. The result was a ransomware attack where the threat actor removed student and/or teacher photo images on a storage container on that server. The breach affected individuals all across Canada and an estimated 25 schools in BC.

Entourage states that the photos were “raw” and likely contained no other identifying information such as associated names, schools, grades, location, or captions. However, there may have been some metadata associated with the photos depending on the device from which the photos were uploaded. For instance, it is possible that metadata such as time the photo was taken and the location of the photo may have been attached to some photos.

The photos span the last 24 months (school years 2022/23, and 2023/24). Edge Imaging’s own IT systems were not accessed or affected at all.

Protection of Personal Information

Organizations in British Columbia are under a statutory duty to protect the personal information in their custody or under their control. Section 34 of PIPA sets out this duty and states:

34 *An organization must protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.* The former Commissioner examined the meaning of “reasonable security” and said that:

...adequacy of personal information security should be measured on an objective basis, not according to subjective preferences or opinions. Reasonableness is not measured by doing one’s personal best. The reasonableness of security measures and their implementation is measured by whether they are objectively diligent and prudent in all of the circumstances. While “reasonable” does not mean perfect, in some situations “reasonable” may signify a very high level of rigour.

Response to the Privacy Breach

This office has identified key steps to managing a privacy breach. Organizations must make every effort to recover the personal information, to minimize the harm resulting from the breach and must take steps to prevent future breaches from occurring. It is in this context that I have reviewed and evaluated the actions of Edge Imaging in response to this privacy breach.

Breach Containment

Upon discovering the breach, Entourage immediately engaged with forensic experts to assist with the investigation of the incident and containment.

Furthermore, Entourage states it has taken the affected AWS cloud server offline to contain the breach; rotated all Entourage credentials as well as updating the credentials that were known to have been compromised; removed all credentials from all developers for the affected environment such that they no longer will have access to the Canada servers unless they are working on fixes for the affected installation; and engaged a security audit firm to audit and monitor their platform to prevent this from happening again.

Risk Evaluation

In order to determine what additional steps are immediately necessary, organizations are expected to evaluate the risks associated with the breach.

The risk of harm in this case is hurt or humiliation. As of the date of the report, there is no evidence that any potentially impacted information was used for an unauthorized purpose.

Notification

Notification of affected individuals can be an important mitigation strategy. The key consideration overall should be whether notification is necessary in order to avoid or mitigate harm to an individual whose personal information has been inappropriately collected, used or disclosed. In order for notification to be effective, it should be conducted in a timely enough manner so that affected individuals can take the required steps to avoid or mitigate the potential harm.

Edge does not have the ability to identify those who may have been affected by the cyber incident. On February 8, 2024, Edge began notifying all affected schools and the privacy officers of affected school boards to help them communicate with their school community about this incident. As of February 21, 2024, it had notified 25 school boards that are impacted in BC, affecting 15,294 files in total.

As recommended by this office, Edge posted indirect notification of the breach on its webpage and provided a further update to all affected schools that some photos may have contained metadata.

Prevention Strategies

An organization is required to have reasonable security arrangements to protect personal information in its custody or under its control.

The organization has been working with external resources to investigate and remediate this incident, and is constantly evaluating its administrative, physical and technical safeguards in order to keep its systems secure. Many of these steps are described in the containment measures.

Finally, it's important to note that Edge Imaging needs to proactively address privacy risks in contractual agreements with third-party service providers such as the various school boards. This could include having clear processes and policies in place for handling personal information and a data breach response plan that assigns roles and responsibilities for managing an incident and meeting regulatory reporting obligations.

Conclusion

In summary, after reviewing the actions take by the organization in responding to this breach, I am satisfied that its response to the breach was compliant with section 34 of PIPA. The organization made a reasonable effort to mitigate potential harm to the affected individuals that may result from this breach and has taken appropriate steps to prevent future similar incidents.

This concludes the monitoring of this privacy beach and I have closed this file. If you have any questions or if there is any information you would like to add at a later date, please contact me by email at lcoopsie@oipc.bc.ca.

Sincerely,

A handwritten signature in cursive script that reads "Laine Coopsie".

Laine Coopsie
Investigator