THOMASLLOYD

EMPLOYEE INFORMATION

Notification about a recent cyber incident

Dear employees and colleagues,

As an international company operating in critical infrastructure in Asia, we, like many other companies and service providers in our sector, regularly experience attempts to attack our IT infrastructure systems. These attempts are usually successfully repelled by our IT Infrastructure & Cybersecurity Department and the external service providers we cooperate with in this area.

Nevertheless, we would like to inform you about a recent cyber incident in accordance with the relevant legal provisions of the General Data Protection Regulation (GDPR), even though neither the ongoing operation of our IT systems, websites, and portals was interrupted, nor did the company or our customers suffer any financial damage, as we currently cannot rule out unauthorized access to parts of personal data.

We take every (suspected) incident very seriously. The security and protection of data are of the highest priority at ThomasLloyd. We have clear and binding guidelines for IT and data security. We immediately investigate any indications of possible data leaks. We are currently thoroughly examining the above-mentioned incident, focusing first on the authenticity of the data and then on how the data might have been obtained. According to current knowledge, it is likely a locally limited incident.

We would like to provide you with some information about the incident so that you can understand what happened, how you might be affected, how we have responded, and what additional steps can be taken to protect your data if you wish.

What happened?

Recently, we identified an incident that affected a part of our internal IT systems. Upon discovering the incident, we immediately executed response protocols, initiated an investigation with the support of external cybersecurity and forensic experts to analyse the incident, and implemented our business continuity plans to minimize disruptions to our business operations and ensure the continued security of our IT systems. The goal of working with our experts was to contain and fully resolve the incident, as well as to receive recommendations to strengthen our security posture against potential future threats and implement these to secure and strengthen our IT systems. As soon as the aforementioned cyber-attack was detected, we stopped access to further systems. There was no interruption of regular operations, and systems were not encrypted.

Which data and systems are affected?

The affected online storage also contains personal data and files. A partial download of these data and files from the servers and their publication on the dark web cannot be completely ruled out at this time. We have no evidence that personal data stored with us has been or will be misused.

The personal data affected by the incident could include all data provided to us in the course of the employment relationship, such as for your personnel file or data you have stored on our servers yourself.

Explicitly not affected are customer passwords and thus access to customer accounts. It is generally not possible to change the data associated with ThomasLloyd customer accounts, as this would require authorization by a ThomasLloyd employee. No direct payments or other transactions can be initiated through the accounts.

How did we respond to the incident?

To best protect your data and minimize the risk of similar incidents in the future, we conducted a full system review and initiated extensive containment measures immediately after learning of the incident, including isolating our network, improving our intrusion detection capabilities, and strengthening our response mechanisms. We have proactively informed the relevant authorities comprehensively about the incident and reported it to the competent data protection supervisory authorities in a timely manner.

What could happen to the data and what are the potential consequences?

It cannot be completely ruled out that, if personal data has been disclosed or will be disclosed, it could be used on the internet to the detriment of customers or their authorized representatives, or that third parties could impersonate the affected individuals. Every cyber incident inherently carries the following risks, regardless of the company:

- Attackers could publish personal data on dark web platforms and make it accessible to third parties.
- Attackers or third parties who have obtained your data could send you emails with malware attachments. If you open the attachments of such an email, your device could be infected with malware.
- Attackers or third parties could contact you to extort you with the stolen or published data.
- If attackers have obtained copies of your identification documents, they could use them as templates to create illegally forged copies.
- Bank data could also be used to initiate unauthorized money transfers, especially if combined with other data.
- With information such as name, account details, and email address, hackers could commit identity theft. Goods could be ordered at your expense and risk, especially if you use the same password for different shop systems.

What can you do in general?

As a general practice, we recommend that you always be vigilant against phishing attempts, including the risk of identity theft and fraud, especially with messages and emails that seem unusual to you, and never click on links without careful consideration. There are various precautions you can take to protect your data, including:

- Protect your personal data and report unusual activities.
- Use complex passwords and change them regularly.
- Avoid opening suspicious-looking email attachments.
- Regularly check your account statements and credit reports for fraudulent or irregular activities.
- Further information and recommendations on data security can be found on the website of the Federal Office for Information Security.

We would like to remind you that such an incident and the associated information are generally confidential. Nevertheless, we have prepared similar communication for third parties outside the company – including our customers, business partners, and other stakeholders – which can be shared in case of inquiries.

We sincerely regret that it was necessary to contact you under the given circumstances and thank you for your understanding and support. The security of your data has always been and remains our top priority. We can therefore assure you that we will do everything to ensure the long-term resilience of our IT systems and prevent such an incident from happening again.

If you have any questions about the incident or this notification, please feel free to contact your direct supervisor (MD/C-Level) or your HR contact person at any time.

Finally, we would like to expressly thank you for your support and commitment.

Best regards,

Miriam Plater
Chief People Officer