IAPP Asia 2025: Privacy Forum + AI Governance Global

9-10 July
SINGAPORE

#APF25

Data Under Fire – Battling a Ransomware Attack with Confidence

WELCOME AND INTRODUCTIONS

Eli Serota

Cybersecurity & Data Privacy Communications Lead at FTI Consulting

Wei Loong Siow

Legal Counsel & Data Protection Officer at Changi Airport Group

Jennifer Archie

Partner at Latham & Watkins

Mervyn Heng

Senior Manager for Policy & Technology at Personal Data Protection Commission (PDPC)

Instructions & Considerations

- For the purpose of this exercise, we ask that you suspend disbelief under the circumstances presented.
- The developments that we will present today would typically occur over a period of days or weeks, rather than just a few hours.
- The scenario posed will become progressively more challenging, through a series of ‘escalating injects’ which will complicate the current situation.
- Please note there are no ‘right’ or ‘wrong’ answers usually, but your participation will make for a better discussion.

Please scan the QR code shown to participate in the simulation and live polls:

Join at

slido.com

#2213 682

Background

- Griffanti Global is a privately-owned e-commerce marketplace, which provides a platform for multinational companies (MNCs) and small-and medium-enterprises (SMEs) to sell a variety of consumer goods through their online platform.

- The company is headquartered in Singapore, but also has employees based in Malaysia, India, Germany, and the United States

- As part of the sales process, Griffanti Global collects customers names, addresses, and emails. Payments are processed by a third-party independent vendor and not stored on Griffanti Global's servers.

Setting the Scene

Challenges logging in and suspicious notes are reported to the IT team from Singapore-based employees. Teams notice the e-commerce marketplace has also been taken offline and is now inaccessible.

!!! IMPORTANT INFORMATION!!!

Attention! We hacked your network and now Griffanti Global database is safely encrypted with reliable algorithms. No one except us can access the files now. We also took your website offline. But don't worry. It is easy to recover in a few steps.

First, you must not alert the CSA or any other law enforcement. Second, your company must contact us within 24 hours to purchase a unique private decryptor key that is securely stored on our servers for $7 million USD in the form of bitcoin. You must make payment in 10 days. This is the only way to restore your system.

How to contact us?

1) [Recommended] Download a special TOR browser: https://torproject.org
2) Open our website in the TOR browser: https://griffantiglobal.com/182992
3) Follow the instructions on this page.

After payment, the data will be removed from our disks and the decryptor key will be given to you, so you can restore functionality and files.

Immediate Steps

Information Technology (IT) team escalates the issue to your COO

Your COO declares a cybersecurity emergency

The Crisis Management Team (CMS) is assembled

The CMT engages external advisors (legal, regulatory, and communications)

LET’S BEGIN

Inject #1

You receive an inquiry from Osmond Chia at The Straits Times around rumours of a cyber attack at the organisation.

Cyber attack at Griffanti Global

OC

Osmond Chia

To John

9:32 AM

John –

Sources tell me that Griffanti Global has suffered a ransomware attack and I can see your e-commerce marketplace is offline. Do you have a comment on this? Is it true the hackers also stole thousands of confidential documents, including private customer data and supply chain contracts?

I'm writing a story that is set to publish in about an hour. Let me know ASAP. Thanks.

Osmond Chia

Do not edit
How to change the design

Inject #1: How would you respond to Osmond?

ⓘ The Slido app must be installed on every computer you're presenting from

slido

Inject #2

Your VP of Human Resources, receives an inquiry from an employee concerned about their ID number and bank information.

Employee Data Impact?

SB

Sharon Berry

To John

11:18 AM

John –

I'm sure you have a lot going on but wanted to bring this to your attention. One of our site engineers who saw the ransom note has emailed me to ask if their information was impacted by this incident. They seem to be most concerned about their ID (passport) and banking information for payroll. What should I tell them?

Thanks,
Sharon

SVP, Human Resources and Employee Engagement

Do not edit
How to change the design

Inject #2: What do you tell employees?

ⓘ The Slido app must be installed on every computer you're presenting from

slido

Inject #3

Merchants who sell products through the website have noticed it is down, and are starting to send inquiries, questionnaires, and call account managers directly.

Employee Data Impact?

GE

Gino Evrard

To John

12:49 PM

John –

As discussed, I spoke to all our account managers this morning. Almost everyone has gotten emails and phone calls from merchants with questions about the incident. A few have forwarded the security questionnaires they've received (see attached) asking for responses before the end of today. Please let me know who these should go to.

Thanks,
Xin Hui

Customer Relationship Lead

Inject #3

HAMILTON HAMMOCKS

1) When did the incident occur?
2) Have any indicators of compromise (IOCs) been identified?
3) What have you done to better secure the network in the future?
4) Can you provide a letter of attestation of network security?
5) Can you commit to providing the full forensic report?
6) Out IT team would like to have a phone call, what is your earliest availability?
7) Was any of our data impacted?

Do not edit
How to change the design

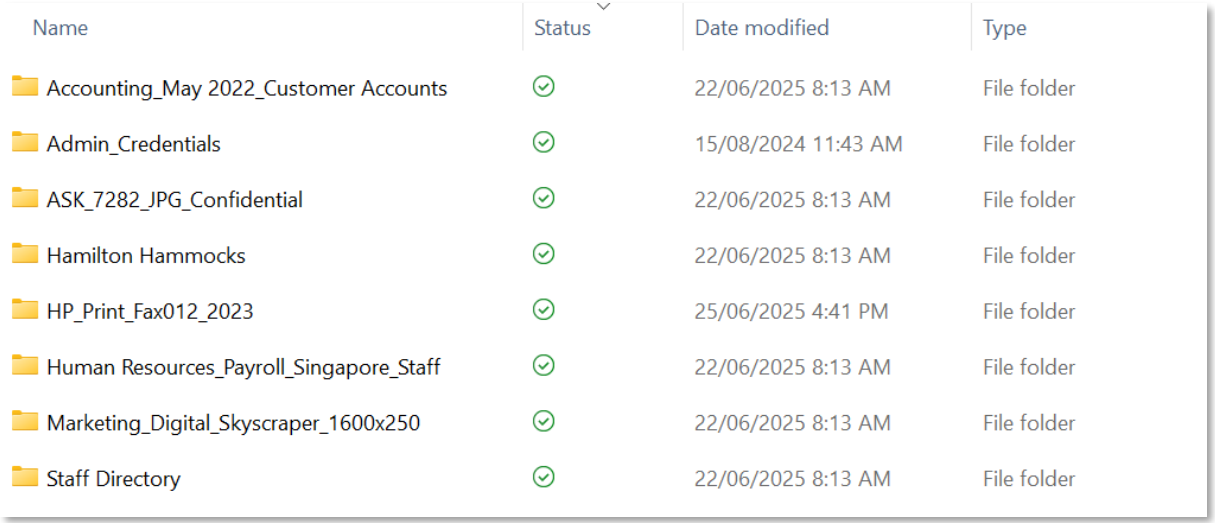
Inject #3: How do you organize responses to your merchants?

ⓘ The Slido app must be installed on every computer you're presenting from

slido

Inject #4

You have **engaged with the threat actor** and have received **proof of life** from the threat actor, Conti, that alleges they have exfiltrated business sensitive data.



Name	Status	Date modified	Type
Accounting_May 2022_Customer Accounts	✓	22/06/2025 8:13 AM	File folder
Admin_Credentials	✓	15/08/2024 11:43 AM	File folder
ASK_7282_JPG_Confidential	✓	22/06/2025 8:13 AM	File folder
Hamilton Hammocks	✓	22/06/2025 8:13 AM	File folder
HP_Print_Fax012_2023	✓	25/06/2025 4:41 PM	File folder
Human Resources_Payroll_Singapore_Staff	✓	22/06/2025 8:13 AM	File folder
Marketing_Digital_Skyscraper_1600x250	✓	22/06/2025 8:13 AM	File folder
Staff Directory	✓	22/06/2025 8:13 AM	File folder

Inject #4

Following confirmation that business sensitive data has been exfiltrated, your CEO calls to ask about the status of the ransom payment.

Voicemail Transcription:

*"Hey John. I understand it's been confirmed the threat actor has exfiltrated some of our client's data. What's the status of our ransom payment decision? I don't want to pay them under **any circumstances.** When are we discussing? Please get back to me as soon as possible. Thank you."*

Do not edit
How to change the design

Inject #4: What are some considerations around paying a ransom?

ⓘ The Slido app must be installed on every computer you're presenting from

slido

Inject #5

Personal Data Protection Commission (PDPC) Singapore discovered that Griffanti Global has been listed on a dark-web ‘shame site’ by the threat actor.

Case No.: GG-2004-H4782
Attention: John Doe

NOTICE TO PRODUCE DOCUMENTS AND INFORMATION FOR INVESTIGATION UNDER THE PERSONAL DATA PROTECTION ACT 2012

1. The Personal Data Protection Commission (the “PDPC”) is presently conducting an investigation under section 50 of the Personal Data Protection Act 2012 (the “PDPA”) to ascertain whether there have been breaches of the PDPA. The circumstances relating to the investigation are set out in brief at Annex 1.

2. For the purpose of the above-mentioned investigation, pursuant to paragraph 1 of the Ninth Schedule to the PDPA, you are hereby required to provide to the PDPC the documents and information specified in the attached Annex 1, including a written response to the queries therein, within **fourteen (14) days** from the date of this Notice (that is, by 24 July 2025).

Fictitious

Do not edit
How to change the design

Inject #5: How are you responding to the regulators/enforcement agencies?

ⓘ The Slido app must be installed on every computer you're presenting from

slido

QUESTIONS?

How Did Things Go? (We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the Cvent Events app.
2. Enter **IAPP APF25** (case and space sensitive) in search bar.
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".