Help, our SIS is hacked!

Bart Bosma
bart.bosma@surfnet.nl

Many thanks to Fung Yee Poon and Niels Dutij for allowing me to tell this story and for helping with the story line and its intricacies.

SURF

https://www.surf.nl/

Agenda

- Disclaimer
- Background
- Day 1
- Day 2
- Day 3
- Damage & Resolution
- What about the police?
- Lessons learned

Disclaimer

Back-ground

Day 1

Day 2

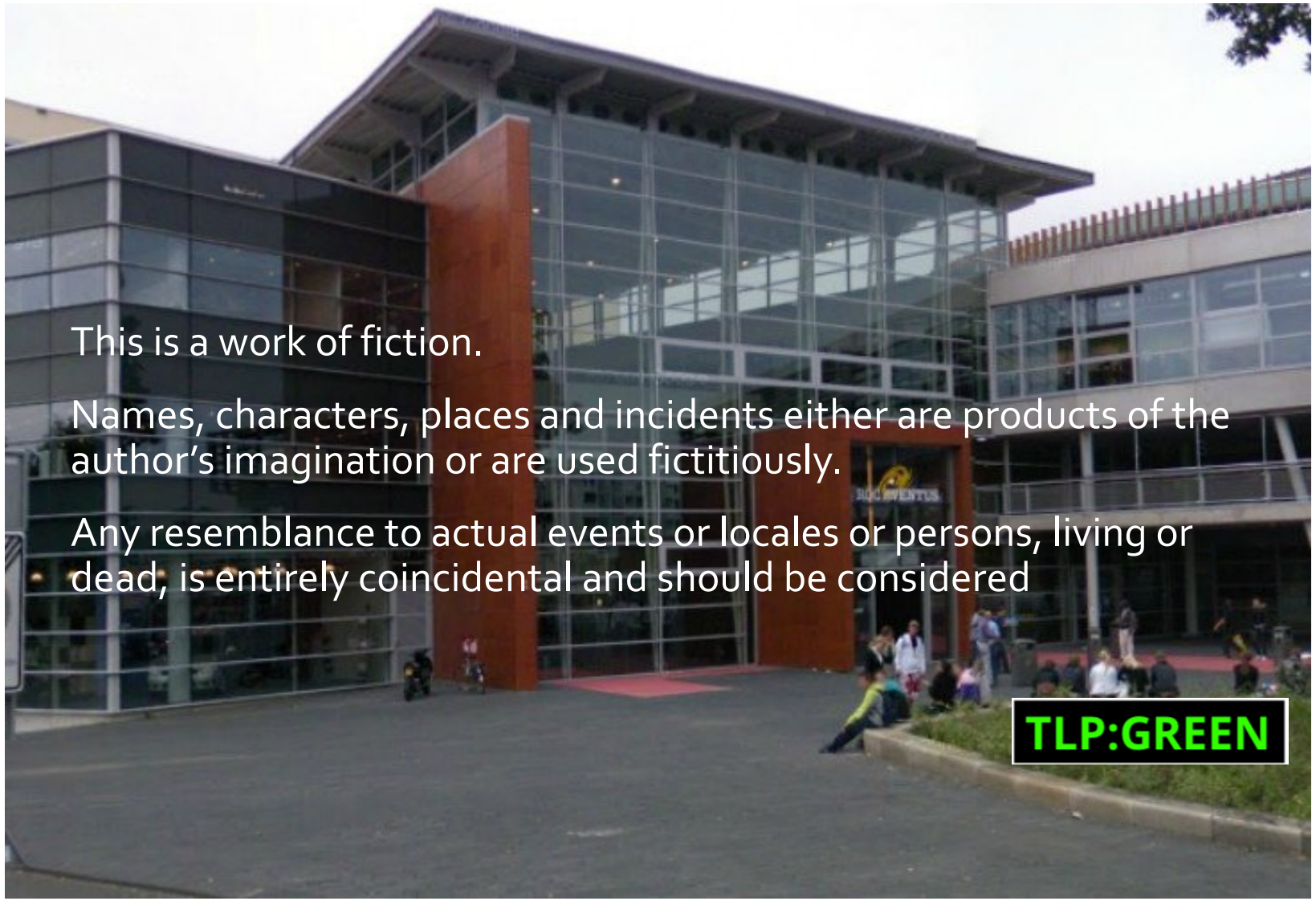
Day 3

Damage & Resolution

What about the police?

Lessons Learned

Disclaimer


This is a work of fiction.
Names, characters, places and incidents either are products of the author's imagination or are used fictitiously.
Any resemblance to actual events or locales or persons, living or dead, is entirely coincidental and should be considered
TLP:GREEN

Disclaimer

Back-ground

Day 1

Day 2

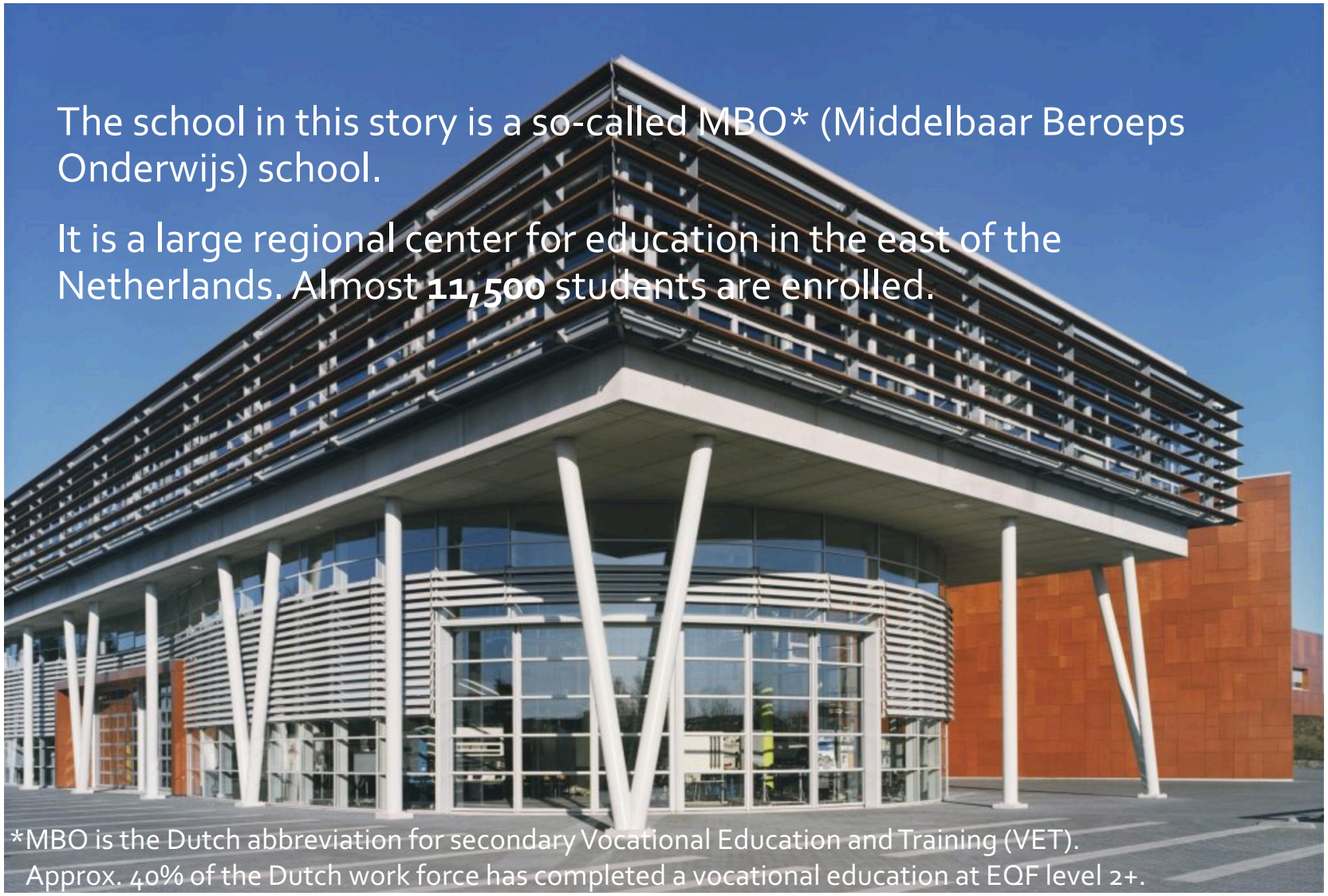
Day 3

Damage & Resolution

What about the police?

Lessons Learned

A little background



Disclaimer

Back-ground

Day 1

Day 2

Day 3

Damage & Resolution

What about the police?

Lessons Learned

– Day 1 –

- In the morning the service desk received notifications about some problems with the SIS from professors/teachers.
- Initial investigation revealed that the password of the vendor admin account had been changed.
  - Apparently it was possible to circumvent authorizations by manipulating the URL which gave access to a password reset option.
- No other changes were seen at that time.
- The vendor was notified and in the afternoon they reported that the problem was fixed. The admin password was reset.

Disclaimer

Back-ground

Day 1

Day 2

Day 3

Damage & Resolution

What about the police?

Lessons Learned

– Day 2 –

- Teachers reported that grades had actually been changed.
- More anomalies were found in the course of the morning (some functionality didn't work as it should).
- Around noon it was decided to assemble a crisis team.
- Later in the afternoon several e-mails were received from two rogue accounts. One of these was sent to all students detailing how one could obtain certain drugs.
- This triggered a new investigation, which revealed 2 previously unnoticed accounts with admin rights (aptly named: satan & lucifer).
- At 4 p.m. the DPO decided to have the application taken offline.
- All students were notified through the "studentapp" that the system was temporarily offline because of technical problems.
- The Dutch DPA was notified of a possible data breach and informed of the measures taken so far.
- A forensics specialist (*Hoffmann Forensics)* was enlisted to safeguard the logs, make an inventory of the damage and find other potential problems.
- A police report was filed (mainly to comply with the cyber insurance requirements).

3

Disclaimer

Back-ground

Day 1

Day 2

Day 3

Damage & Resolution

What about the police?

Lessons Learned

– Day 3 –

- The police and *Hoffmann Forensics* investigated log files at the vendor location.
- The DPA contacted the school with questions about the notification that was done the day before and the current status (not to be heard from again.)
- The notification to the DPA was adjusted from “grave incident” to “serious incident”.
- Application brought back online.

Disclaimer

Back-ground

Day 1

Day 2

Day 3

Damage & Resolution

What about the police?

Lessons Learned

What was the damage?

- About 14.000 mutations were made (on approx. 50.000 records in total):
  - student records altered
  - grades changed
  - access rights changed
  - pictures removed and altered
  - planned exams removed
- Some health records were touched, but in general impact appeared to be low.
- No evidence was found that data was extracted.
- Vendor indicated that a manual rollback of the database was impossible, only restoring a 2-day old backup was feasible.

What was the resolution?

- *Hoffmann Forensics* confirmed the integrity (data & authorizations) of the 2-day old backup.
- Management decided to restore the 2-day old database.
- Pen testing was performed before bringing the application back online to ensure the exploited vulnerability had been fixed.
  - Additional vulnerabilities were found (mostly fixed now).
- Other recommendations by *Hoffmann Forensics*:
  - implement two-factor authentication,
  - anonymize PII in testing environment,
  - perform security testing on a regular basis.


Disclaimer
Back-ground
Day 1
Day 2
Day 3
Damage & Resolution
What about the police?
Lessons Learned

What about the police?

- When the breach was discovered an attempt was made to file a police report.
- Initially the police refused to record the incident.
- After the DPO contacted an acquaintance who works for the police department in the same town and explaining the situation, the police came over after all to record the incident.
- The national cybercrime unit got involved and eventually provided a spokesperson to help communicate with the outside world.
- Two suspects were apprehended soon after the police conducted its investigation, one of whom turned out to be innocent, the other is still a suspect.
- The remaining suspect is known to the school and being investigated further.
- The police had other interests than the school once they got involved.

Disclaimer

Back-ground

Day 1

Day 2

Day 3

Damage & Resolution

What about the police?

Lessons Learned

Lessons learned

- Involve management sooner rather than later,
- Do not underestimate the number of actions to be taken, e.g.:
  1. Seek legal advice (crucial!)
  2. Contact DPA
  3. Contact journalists
  4. Contact students
  5. Contact official authorities and supervisory bodies, such as the VET council, the department of education, and the inspectorate
  6. Inform other schools about the incident
  7. Contact vendor for recovery
  8. Contact police for criminal investigation as well as communication
  9. Contact a forensics specialist

  → divide tasks!
- Make sure contact information is readily available and up-to-date!

Left to do…

- Criminal case is pending,
- Claim for the damage* filed,
  - direct cost
  - indirect cost
- Deal with cyber insurance company,
- Implement technical measures to prevent incidents in the future,
- Review crisis plan.

Disclaimer

Back-ground

Day 1

Day 2

Day 3

Damage & Resolution

What about the police?

Lessons Learned

Help, our SIS is

SURF

https://www.surf.nl/