Mukhammad Andri Setiawan, PhD

andri@uii.ac.id

Data breaches: Mitigate, Strategy, and Challenges

Online Training OIC-CERT
27 October 2020

Hello!

- **Chief Information Officer**, *Universitas Islam Indonesia*
- **Lecturer, Informatics Department**, *Universitas Islam Indonesia*
- **Training & Community**, *Indonesia Network Information Center (IDNIC)* - Asosiasi Penyelenggara Jasa Internet Indonesia (APJII)
- **Main contact & Administrator**, *eduroam Indonesia, Global WiFi Roaming Network*
- **Infrastructure team**, Indonesia Research Education Network (IdREN)
- **Cisco Instructor Trainer**, Cisco Netacad Indonesia for CCNA and Cisco CyberOps

Some notable breaches

China behind massive Australian National University hack, intelligence officials say

Officials fear data breach may be used to recruit students or university alumni as informants

Made for minds.

TOP STORIES MEDIA CENTER TV RADIO LEARN GERMAN

GERMANY CORONAVIRUS WORLD BUSINESS SCIENCE ENVIRONMENT CULTURE

TOP STORIES / WORLD / ASIA

ASIA

Zhenhua data leak exposes China's new 'hybrid warfare'

A Chinese data company has harvested information on millions of people, allegedly on behalf of Beijing's intelligence services. Analysts say democracies should pay more attention to the strategic use of open source data.

Mitigate

If you fail to plan, then you are planning to fail

(famously attributed to Benjamin Franklin)

Treat your data important

- But which one?
  - Start to have some prioritization
  - Remember the creed, **security vs convenience**

Who (actually) owns the data?

- Make users aware of their own respective data (credentials, personal data, unit/department's data)

Document the response process

- Create incident response check lists
  - Use this reference: https://www.sans.org/score/checklists

Some checklists from SANS

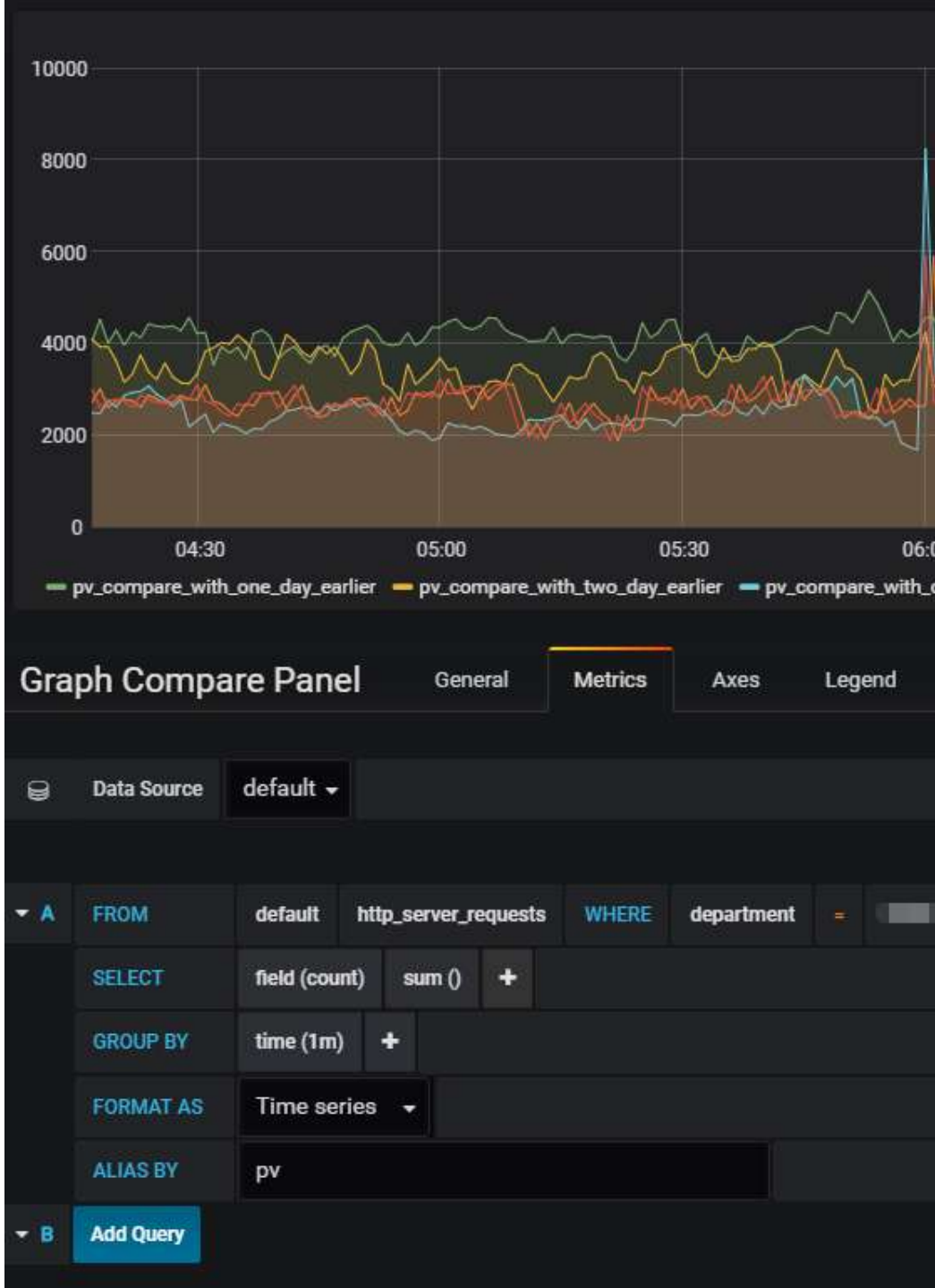
- **e.g. Wireless for enterprise**
  - ❑ Policy
  - ❑ WLAN architecture
  - ❑ Configuration management
  - ❑ Any site survey previously?
  - ❑ Any end user training?
  - ❑ Is there any end point protection?
  - ❑ What kind encryption been deployed?
  - ❑ Has all AP's got their password reset?
  - ❑ Is there any logging & monitoring?
  - ❑ Is there any session timeout?
  - ❑ Is there any wireless client isolation?
  - ❑ How do you secure your RADIUS?
  - ❑ Is there any regular security assessments?

OWASP Checklist

- Other than SANS, we also can get checklist from OWASP
- **e.g. Web Application**
  - Application lockout – making sure attacker cannot reset/lockout user's account
  - Adequate authorization
  - Authentication needs to be in HTTPS
  - Password quality
  - When resetting password, there should be some "obstacle"
  - Is there any session timeout? Can a session be re-used?
  - Is web server properly configured? Has directory listing been denied?
  - Is there any error handling and it doesn't show any error messages?
  - Does it implement the latest SSL/TLS?
  - Can the application invoke terminal command?
  - etc.

Setup a baseline

- Monitor our network throughly to create a baseline



Log is invaluable treasure

- Monitoring is essential
- Never underestimate logs, they provide you lots of insights

Long term mitigation plan

- Have a zero-day vulnerability response
  - Patching up systems with updates
- Employee training
- Have a change management function in the organization

When breach happens

How do you know that your system has been breached?

- In most cases, you don't!
  - (only 33% of organizations were aware that they had been breached – FireEye report 2013)
- So, how do we know that our system has been breached?
  - Looking into where the traffics went (monitor the packet, or DNS requests)
  - **Look into stolen passwords**

1

Lay down your plan for short term and long-term strategy

2

Short term:

- Isolate
- Create local copies (chain of custody)
- Close any potential backdoors
- If possible, use 3rd party providers

What to do next?

What about medium and long term?

Revisit back to the mitigation plan

Have expert response team – work as cross-functional response team

- Digital forensics
- Legal
- HR
- Operations/SRE
- Management

Thoroughly check

- Asses the nature and the scope of the breach
  - What kind of data been accessed or misused
  - Number of records been accessed
- Follow every piece of evidence until we are certain that we have uncovered all attackers' traces
  - access logs
  - error logs
  - dns request logs


Invite 3rd party

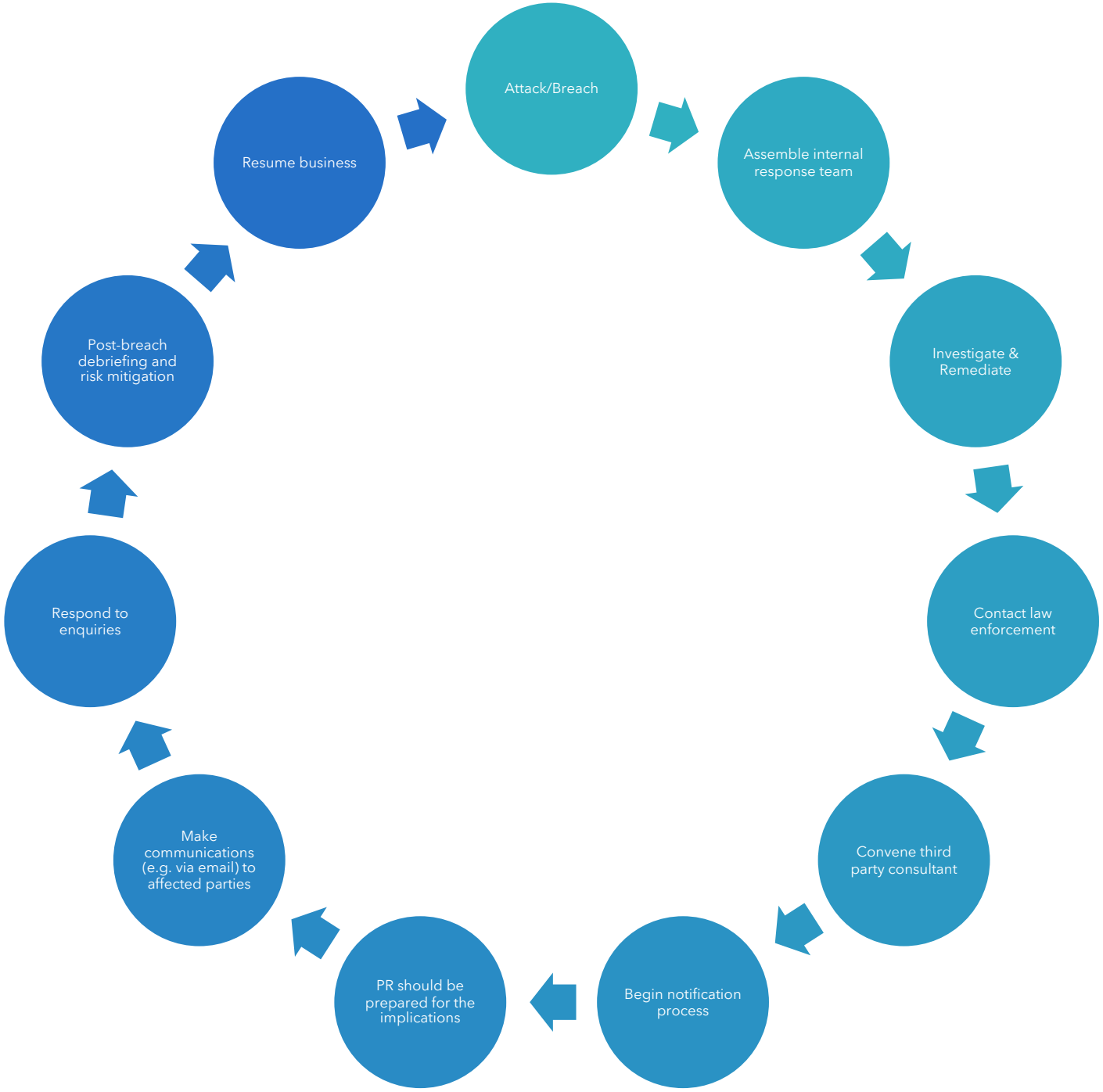
Communications

- **Embarrassment?** Maybe. **Inconvenience?** Definitely
  - But those are not excusing to quietly went without notification
  - Legal actions may be taken due to this
- What kind of information should be given to the stakeholders (including public, if necessary)
  - Summary of the breach and its consequences
  - Description of the measures taken to address the breach

Debriefing

- Review process should be taken to these things
  - Policies and procedures
  - Risk assessments
  - Suitability of using external providers to insure the damage that might happen in the future
  - Technologies to be used
- Amend/update the policies if necessary

Data breach lifecycle



Challenges

The weakest link in security-chain

- Humans remain the weak link in corporate data protection
  - They often felt false security sense of cybersecurity of cybersecurity vendors
- Most firewall helps to speed up the time to detect an incident, but not stopping all kind of attacks

Train more and more and more …

- Provide users/employees examples of what to look for and how to respond
  - Make sure that users know how to identify different types of breaches e.g. theft/loss, hacking, employee snooping, malware
  - Do's and Don'ts
  - If necessary, cyber security team train employees **discreetly** by hacking them through phishing, human error, or fake websites
  - Make sure that employee received proper information so that they know, what kind of data is sensitive
- **Unfortunately**, there is no one-size-fits-all approach to cybersecurity training

IT Policy and IT Governance

- It’s not merely a document that is created and then archived
- We need to **walk the talk**

Thank you