30th ANNUAL FIRST CONFERENCE
KUALA LUMPUR
June 24-29, 2018
30 YEARS OF INCIDENT HANDLING

Security and Privacy Incident Response at Ericsson

Thomas Grenman

FIRST™
Improving Security Together

Ericsson PSIRT

TEAM BACKGROUND

Team established in 2004
Accredited by Trusted Introducer (GEANT/TF-CSIRT) in 2005
Full membership in FIRST since 2006
Main organization located in Finland
Current team size 1+13

FIGURES

Products and services deployed in over 180 countries
Our managed networks serving over one billion subscribers
Tracking vulnerabilities in close to 500 active products
17.000+ vulnerabilities analyzed yearly
3.000+ vulnerabilities registered yearly in vulnerability database

MAIN OPERATIONS

Vulnerability management (monitoring and alerting)
Product security assurance

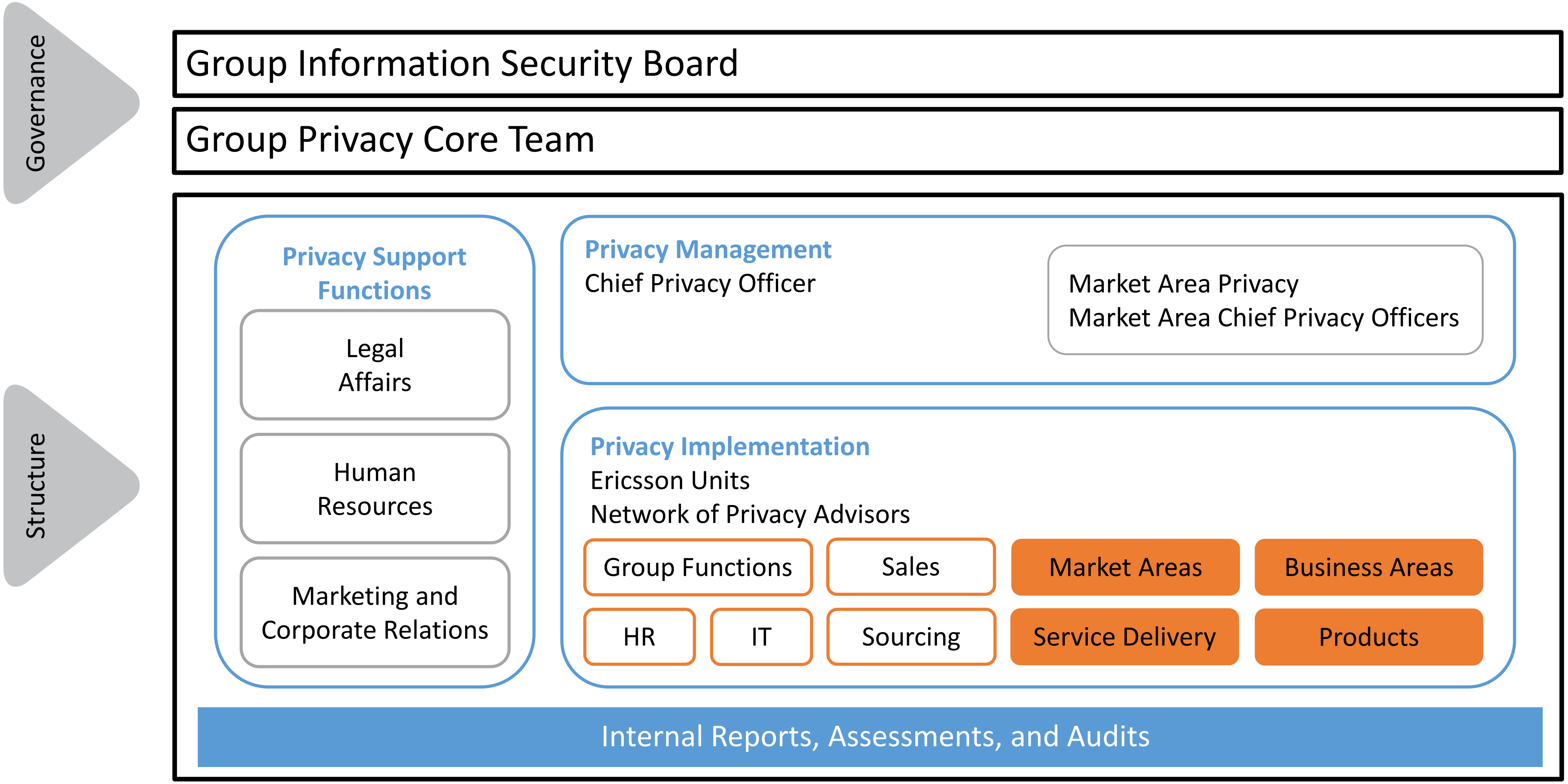
- risk assessments
- privacy impact analysis
- security and vulnerability assessments

Development and maintenance of assessment methodology and tools
Triage and product related incident response
Tier-2 support for security issues raised by customers

COOPERATION

Active cooperation with national / international CERT communities
Contacts established with vendor and operator CSIRT teams
Participating in EU Commission workgroups
Contributing to ETIS

Privacy Governance



Governance

Group Information Security Board

Group Privacy Core Team

Structure

Privacy Support Functions

Legal Affairs

Human Resources

Marketing and Corporate Relations

Privacy Management
Chief Privacy Officer

Market Area Privacy
Market Area Chief Privacy Officers

Privacy Implementation
Ericsson Units
Network of Privacy Advisors

Group Functions

Sales

Market Areas

Business Areas

HR

IT

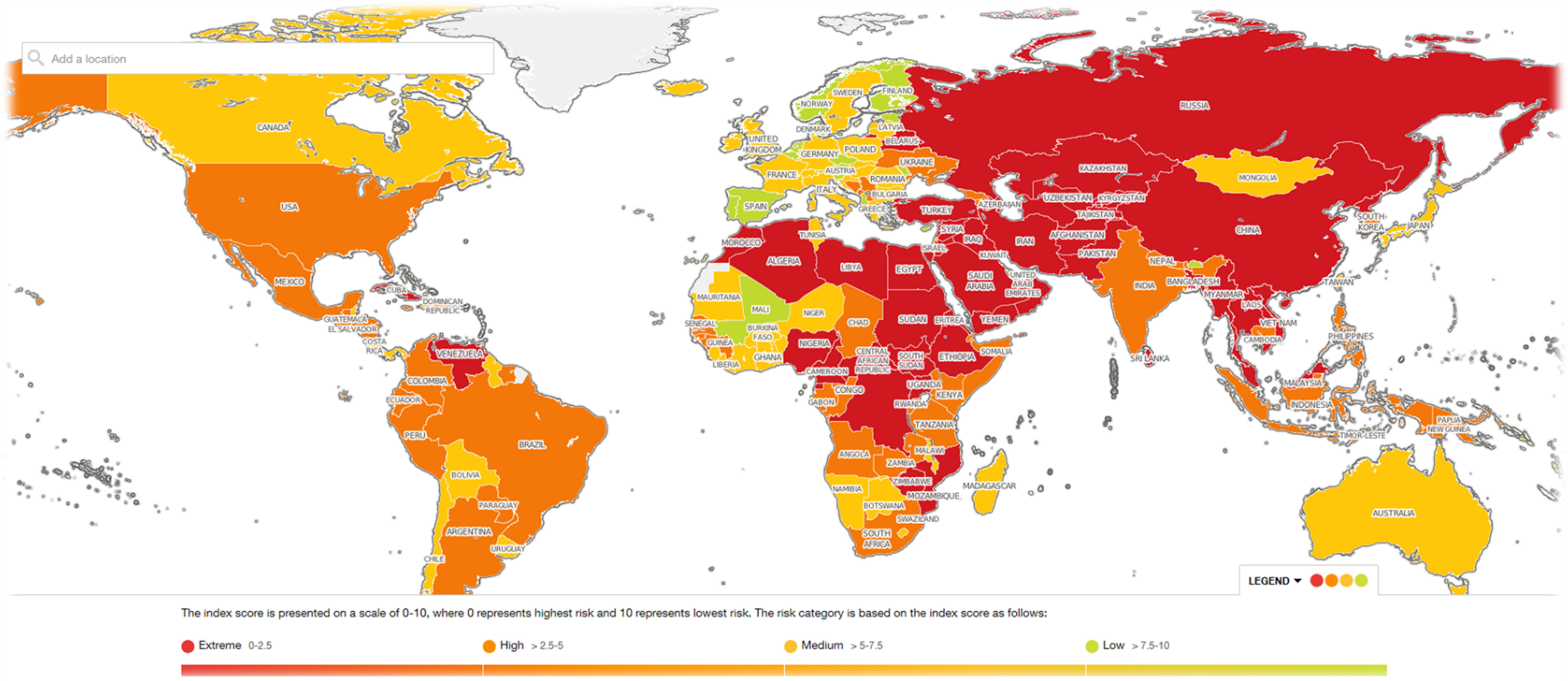
Sourcing

Service Delivery

Products

Internal Reports, Assessments, and Audits

Privacy Risk Heatmap



The index score is presented on a scale of 0-10, where 0 represents highest risk and 10 represents lowest risk. The risk category is based on the index score as follows:

● Extreme 0-2.5	● High >2.5-5	● Medium >5-7.5	● Low >7.5-10

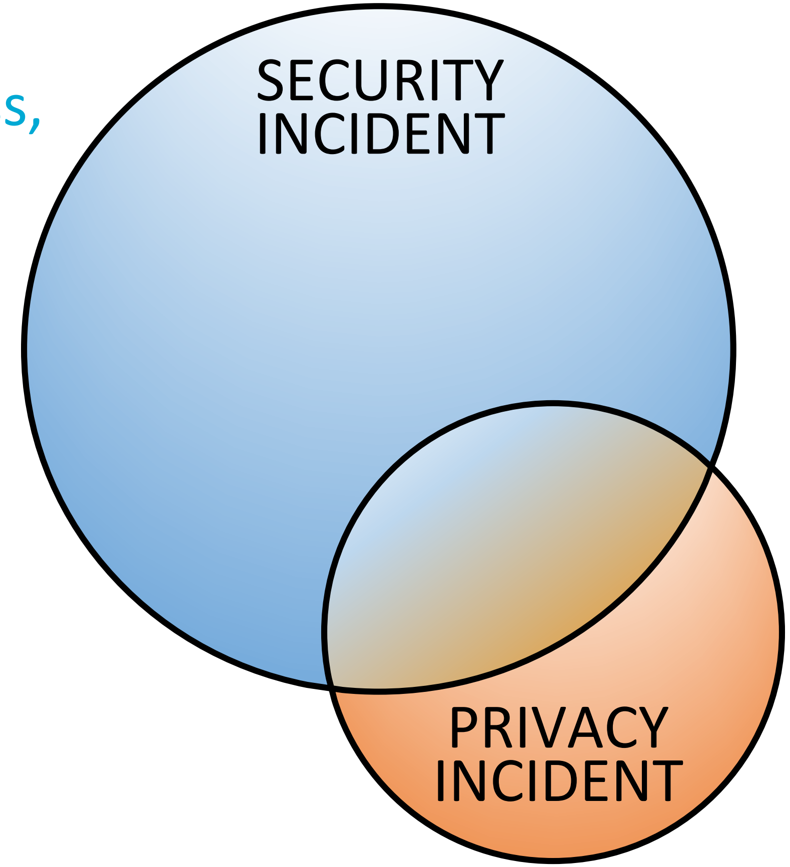
https://maplecroft.com/portal/#/portal/aod/scorecards/index/right_to_privacy/map

Incident Handling Flow

- The incident process cover everything from identification of a reported case up to closure and follow up of the final incident report
- Customers rarely report incidents directly to PSIRT, instead they file support cases
- The first step of the handling process is to determine if the incident is product related and if privacy aspects need to be taken into account
- Potential privacy incidents with activate the privacy officer(s) and trigger a subprocess for determining Ericsson’s relationship to the Data Subjects

Privacy and Security Incident Relationship

Protecting information from unauthorized access, disclosure, modification or destruction

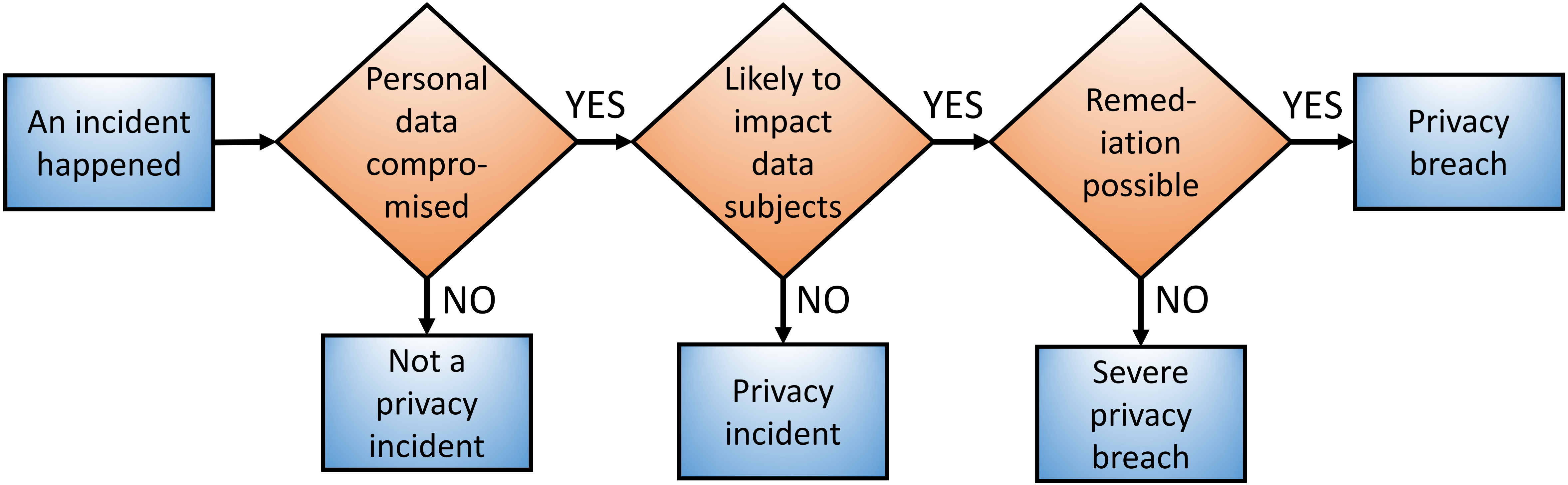


Respecting a fundamental right to the protection of personal data

Incident Triage

- Appoint an incident lead
- Verify and record provided initial information
- If applicable, support in assessing the privacy impact
- Identify the urgency and criticality in order to prioritize the case
- Create a response strategy plan (and keep it updated)
- Identify and handshake with essential stakeholders (e.g., administrators, technical experts, KAMs, service delivery manager, privacy officers, etc.)
- Determine the need to preserve forensic evidence
- Clarify the outcome and the expectations of the incident investigation

Privacy Incident vs. Privacy Breach



Incident Communications

- Keep stakeholder up-to-date during investigation
  - regional service delivery managers
  - involved product organization
  - customer
- Additional communications for privacy incidents
  - approve all communications through appointed privacy officer
  - depending on the local legislation, communicate with DPA, other public authorities and directly with data subjects (if needed)
- If needed, PSIRT will assist in formulating a privacy breach notification

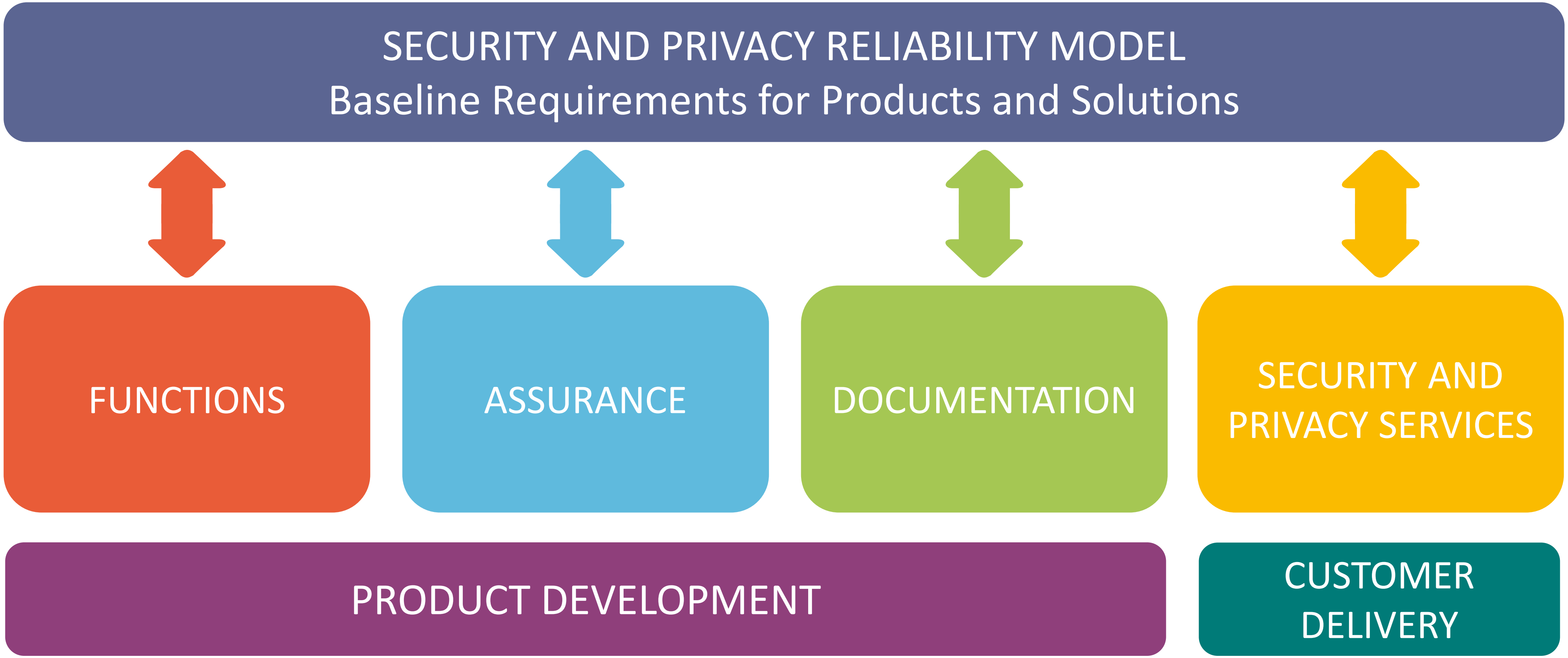
Common Causes of Privacy Incidents

- Lack of security controls
    - loss of equipment containing data
    - transfer, sale or disposal of equipment containing data (without wiping it first)
    - use of equipment without adequate transfer or storing protection for data
    - failing to protecting against intrusion into equipment containing data
    - insufficient rights to access or modify data (e.g., wrongful access, tampering)
    - inadequate security or access controls for data in print or electronic format
    - processing data without or in contradiction with consent

Common Causes of Privacy Incidents (cont.)

- Lack of privacy controls
  - low privacy awareness and data handling competence within staff, contractors and third parties
  - lack or inadequate provisions to protect privacy in contracts or in agreements on processing and information sharing
  - lack of data recognition
  - transfer of data outside country without adequate protection measures
  - lack or privacy processes or policies at Data Controller's or Processor's end
  - lack of policy implementations or consent management in product, services, and operations

Security and Privacy by Design



SECURITY AND PRIVACY RELIABILITY MODEL
Baseline Requirements for Products and Solutions

FUNCTIONS

ASSURANCE

DOCUMENTATION

SECURITY AND PRIVACY SERVICES

PRODUCT DEVELOPMENT

CUSTOMER DELIVERY

Implementation Examples

Baselined Logging and Data Tagging

- A minimum criteria for logging
  - **Who** accessed personal data
  - **When** was the data accessed
  - **What actions were performed** on the data
  - **Data item tags** applied to personal data

Before Subscription-Id-Data 919961345678

After Subscription-Id-Data [1]919961345678[/1]

Data Item	Tag
MSISDN	[1]
IMSI	[2]
IMEI	[3]
Location (LAC / Cell ID)	[4] / [5]
Location (Other)	[6]
IP-address	[7]
First Name	[8]
Last Name	[9]
…	

Implementation Examples (cont.)

Pseudonymization of Log Files

Normal log file in plain text

```
[Mon 2017-05-29 13:37:00 +0300] Received purchase request from user [1:123]smith
[Mon 2017-05-29 13:37:00 +0300] User [1:123]smith phone number [2:123]358123456789
[Mon 2017-05-29 13:37:00 +0300] Transaction by user [1:123]smith using credit card [3:123]342433922947072
[Mon 2017-05-29 21:31:46 +0300] Received purchase request from user [1:456]johnson
[Mon 2017-05-29 21:31:46 +0300] User [1:456]johnson phone number [2:456]358123454321
[Mon 2017-05-29 21:31:47 +0300] Transaction by user [1:456]johnson using credit card [3:456]510510510510510
...
```

De-identified log file with format preserving encryption

```
[Mon 2017-05-29 13:37:00 +0300] Received purchase request from user [1:123]aqugj
[Mon 2017-05-29 13:37:00 +0300] User [1:123]aqugj phone number [2:123]397174510075
[Mon 2017-05-29 13:37:00 +0300] Transaction by user [1:123]aqugj using credit card [3:123]187624087423143
[Mon 2017-05-29 21:31:46 +0300] Received purchase request from user [1:456]omqnfjh
[Mon 2017-05-29 21:31:46 +0300] User [1:456]omqnfjh phone number [2:456]038601359323
[Mon 2017-05-29 21:31:47 +0300] Transaction by user [1:456]omqnfjh using credit card [3:456]199738641157294
...
```

Key Takeaways

- As a Data Controller or Data Processor
  - know the data, know where it is stored, know the local legislation
  - have (rehearsed) processes in place, have well-defined responsibilities
  - agree on communications channels, get to know the local DPA, agree on templates (e.g., breach notification)
  - avoid making contracts that can block or slow down your investigation
  - transfer legal liability for data protection to parties involved in data processing
  - employ forensic investigators or keep a shortlist of local third parties that quickly can aid with needed technical investigation
  - have the technical capability to notify victims (potentially in the millions)

Key Takeaways (cont.)

- As a technology provider
  - identify and document personal data being processed by the product
  - have requirements in place to ensure that the product privacy impact is assessed
  - implement needed technical features to
    - allow classification of personal data according to local regulation and law
    - ensure high data quality (allow updating or deleting outdated information)
    - enable data de-identification, anonymization, and scheduled erasures acc. to retention times
    - enable data transfers (through machine-readable exports and imports)
    - allow fine grained access controls to all processed data item
    - protect confidentiality and integrity of personal data at rest and when in transfer
    - collect sufficient logging (i.e., audit trails) for all vital privacy related events

30th ANNUAL FIRST CONFERENCE
KUALA LUMPUR
June 24-29, 2018
30 YEARS OF INCIDENT HANDLING

Thank You!

FIRST™
Improving Security Together