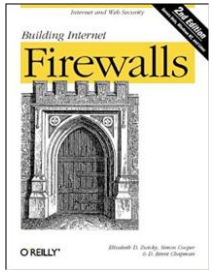
IT/Dev CONNECTIONS

Lessons from the Fire Department

Incident Command for IT

Brent Chapman
Principal
Great Circle Associates

Delivered by KNect365 TMT an Informa business



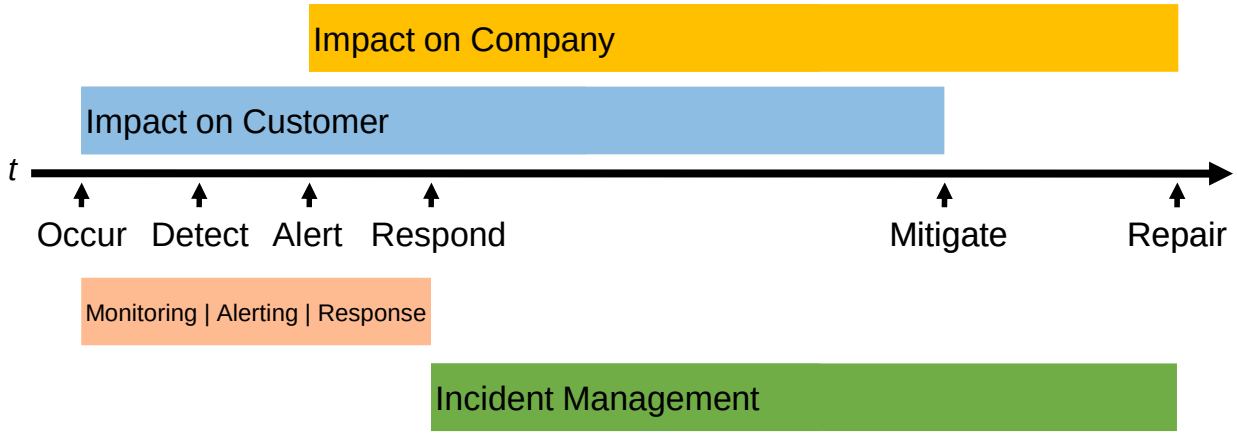
Delivered by
KNect365
TMT
an Informa business

IT/Dev CONNECTIONS

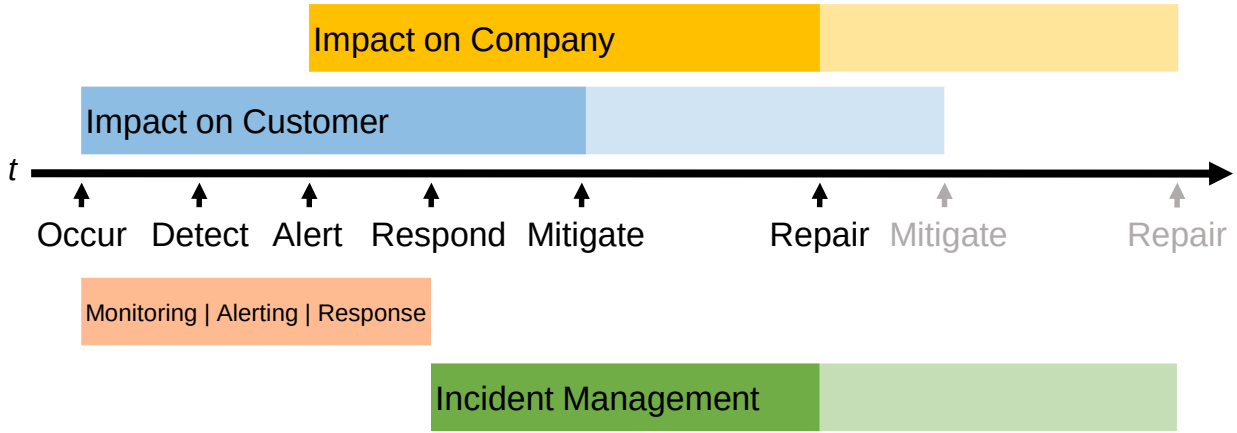
Incident Response is a critical capability

Delivered by KNect365 TMT an Informa business

Incident Timeline



Incident Timeline



IT/Dev CONNECTIONS

Normal Operations vs. Emergency Operations

Delivered by KNect365 TMT an Informa business

IT/Dev CONNECTIONS

It’s somebody else’s emergency

Delivered by KNect365 TMT an Informa business

Do your thinking in advance

IT/Dev CONNECTIONS

Measure your responses

Delivered by KNect365 TMT an Informa business

IT/Dev CONNECTIONS

Dispatch vs. Notification

Delivered by KNect365 TMT an Informa business

IT/Dev CONNECTIONS

Keep an eye on the clock

Delivered by KNect365 TMT an Informa business

IT/Dev CONNECTIONS

Incident Command System works well for IT incidents

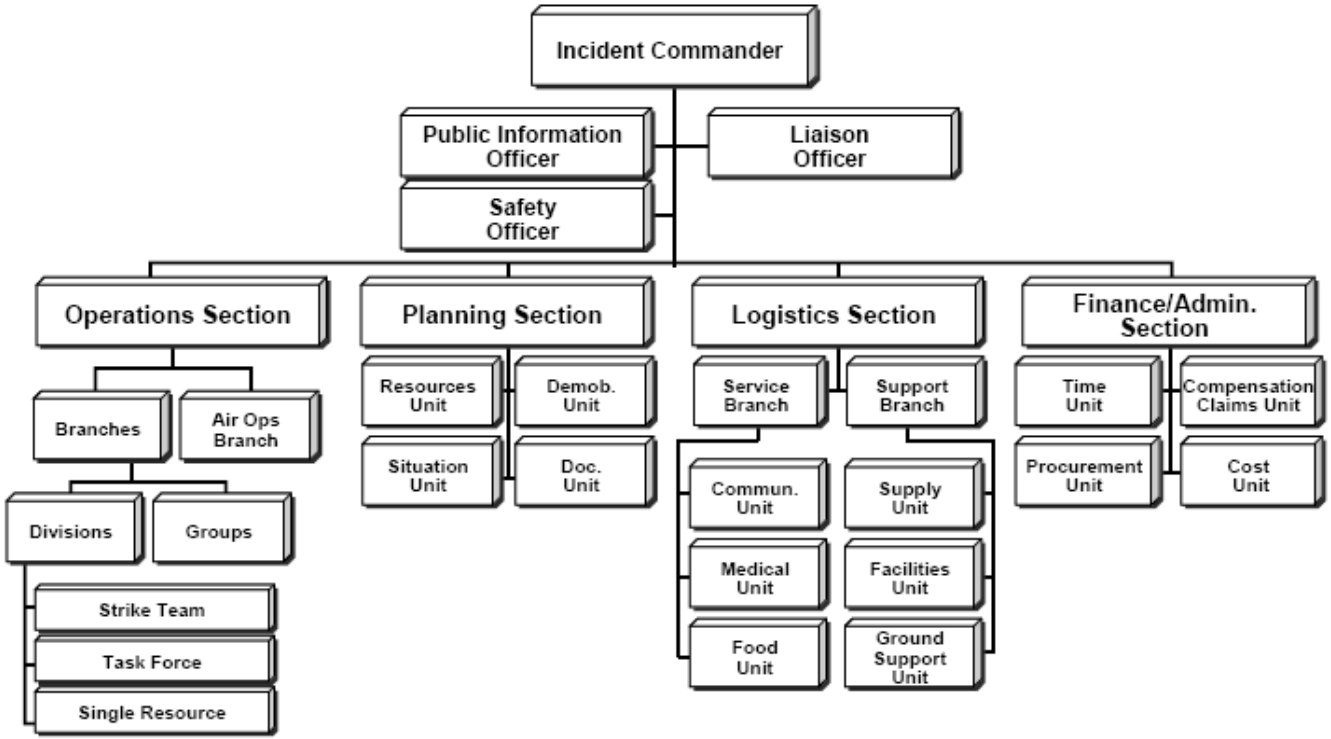
Delivered by KNect365 TMT an Informa business

Key ICS Principles

- Modular & scalable organization structure
- Manageable span of control
- Unity of command
- Explicit transfers of responsibility
- Clear communications
- Shared action plans
- Management by objective
- Time management
- Comprehensive resource management
- Designated incident facilities

These are not the normal rules we work by, but they work better in an emergency

Canonical ICS Org Chart

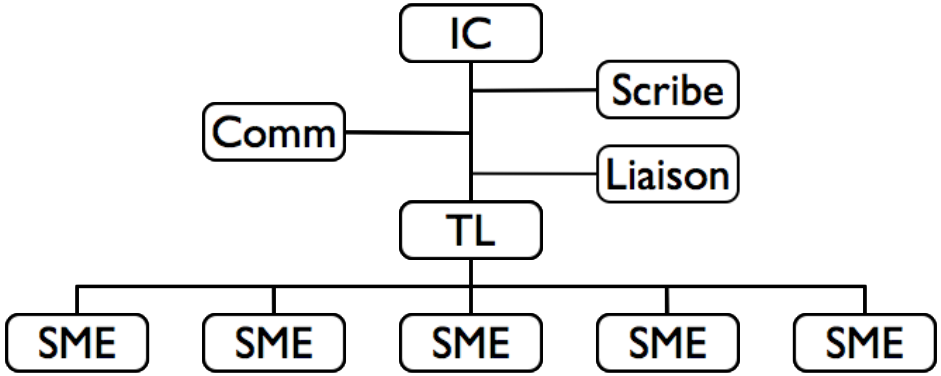


IT/Dev CONNECTIONS

A few tweaks make ICS work even better for IT incidents

Delivered by KNect365 TMT an Informa business

Org chart for IT incidents

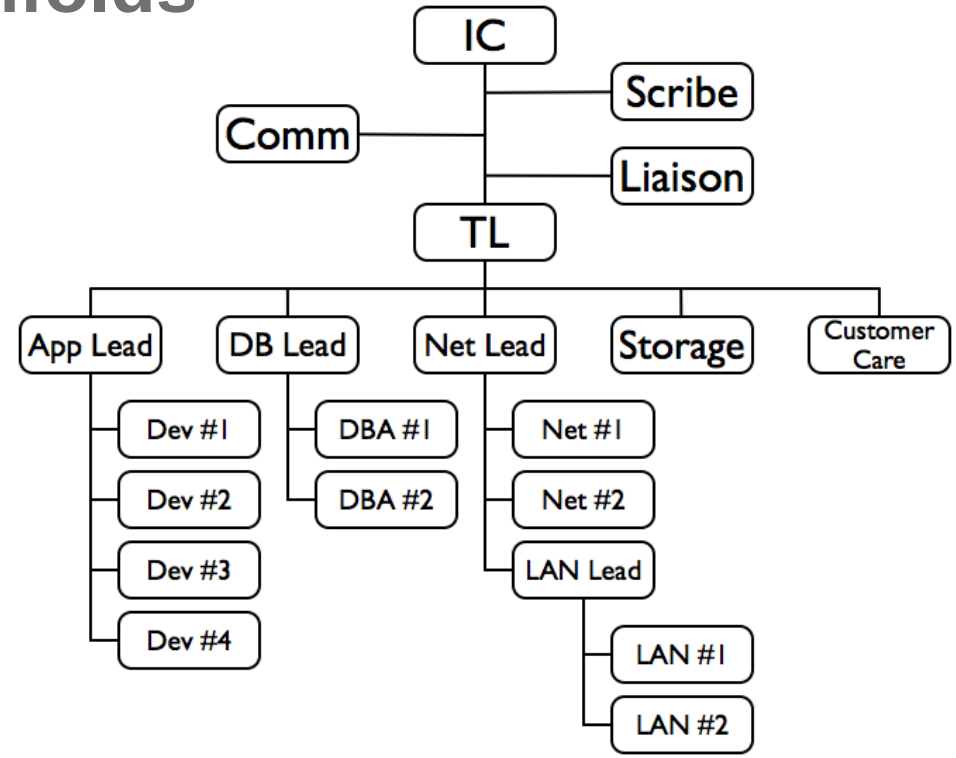


IC = Incident Commander

TL = Tech Lead

SME = Subject Matter Expert

Org chart grows as incident unfolds



IT/Dev CONNECTIONS

Focus on roles, not individuals

Delivered by KNect365 TMT an Informa business

IT/Dev CONNECTIONS

Practice, practice, practice, then practice some more

Delivered by KNect365 TMT an Informa business

Text-based comm tools work better than phone bridges

IT/Dev CONNECTIONS

Channel-oriented chat works better than ad hoc multi-party chat

Delivered by KNect365 TMT an Informa business

IT/Dev CONNECTIONS

Checklists are powerful and under-appreciated

Delivered by KNect365 TMT an Informa business

IT/Dev CONNECTIONS

Blameless Postmortems are the key to improving over time

Delivered by KNect365 TMT an Informa business

IT/Dev CONNECTIONS

Senior managers can inadvertently disrupt incident response

Delivered by KNect365 TMT an Informa business

Questions? More info…

Please contact me!

Brent Chapman
brent@greatcircle.com
@brent_chapman

Available for consulting, training, conferences, public speaking, and in-house presentations

These slides available at `j.mp/grtcrcl-181017`

PagerDuty Incident Response docs: `response.pagerduty.com`