Security@LIGO

Abe Singer

Now: NERSC, LBL

Then: LIGO

The “I Love Me” slide

4 sites, ~200 staff, ~1000 “users”

1 root compromise

~3 reflection attacks (outbound)

~3 phish

~1 minor incident per month

Must be doing something right... (and without firewalls)

Fundamental scientific research in the field of observational gravitational waves, with the single overriding goal to maximize scientific output.

LIGO [security] policy is to properly plan and implement security in a way that supports the scientific mission in a minimally intrusive manner that enables reliable access to data and use of LIGO

LIGO [security] policy is to properly plan and implement security in a way that supports the scientific mission in a minimally intrusive manner that enables reliable access to data and use of LIGO

Security enables Science

No do-overs

Have a plan you can defend

Context based risk assessment

The Interferometer

The Data

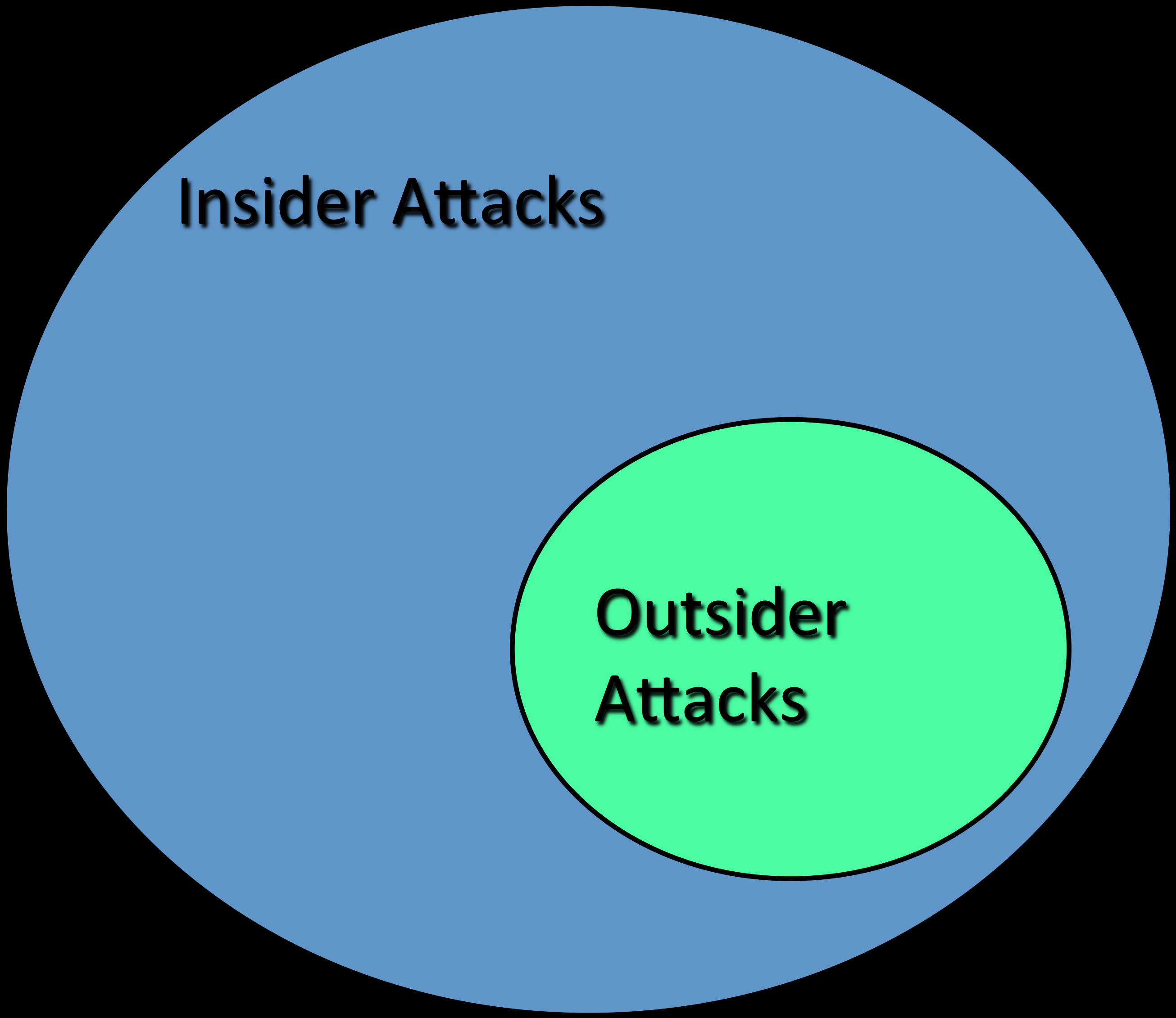
Observation Runs

(Data Analysis)

(IT Infrastructure)

the APT

the Insider


Insider Attacks
Outsider Attacks

!firewall

trust relationships

trustworthiness

acceptable risk

blocking a port costs *something*

time == money (a *lot*)

impact on operations/users

changing passwords has a cost

Identify what risks mitigated

Usability

Uniformity

Impact on workflow

Enable science

Intrusion disruption vs operation disruption

Risk assessment, mitigation, residual risk

Directorate (management) acceptance of risk

security reviews
a bunch of people in a room
documentation and presentations
identify risks and mitigations
document along with residual risk
things for further review
report for Directorate with action items
Directorate sign-off

User accounts will get compromised

Mitigate exposure to just that user

Focus on host, user, and application security

Security baseline for OS and applications

Configuration Management

Strong (enough) authentication

Single sign-on (where possible)

Token OTP for critical systems

Bastion host w/OTP for interferometer

privileged access control

because sysadmins are the biggest risk

comprehensive logging and monitoring

Incident response preparedness

The interferometer network

A few other tidbits

Software reviews

vulnerability scanning

penetration testing

The detection

real or not?

the difficult part

shout out to the sysadmins

Security when the CSO leaves

https://jobs.caltech.edu/postings/5270