GridPP Security Background

David Crooks & David Kelsey (STFC)

GridPP41 29 Aug 2018

Aims and activities

Background paper - work towards case for support in GridPP6

- Security, Trust & Identity
  - Security – Risk management, security plans, technical and operational controls, operational security (handle incidents, vulnerabilities, monitoring, training, security challenges, procedures), …
  - Trust – management controls (aka policies), collaboration with other Infrastructures, SCI, WISE, US Internet2, ESnet, EU GEANT, US NSF/TrustedCI, …
  - Identity – EUGridPMA, IGTF, REFEDS, FIM4R, Internet2, GEANT, UK AAI bodies
- An ongoing process to manage security risks
  - Aim is to maintain: *Confidentiality, Integrity and Availability*

US NIST Cybersecurity Framework v1.1

Https://www.nist.gov/cyberframework

A never-ending CIRCLE of activity!

Credit: N. Hanacek/NIST

(Some) Background

- GridPP started many of the groups/activities (or was a co-founder)
  - CA Coordination Group (2000), Security Requirements/Risk Analysis (2001), WLCG Security Policy (2003), Joint (WLCG/EGEE) Security Policy (2004), WLCG/EGEE CSIRT/OSCT (2005), SVG (2006), SCI (2010), FIM4R (2011), WISE (2015), …
- Many lead roles for GridPP security people (over the years)
- Everything we do (even for EU/EGI) benefits WLCG
- The WLCG CSIRT in Europe **is** the EGI/EOSC-hub CSIRT
  - Plus the WLCG Security Officer at CERN
- Our work in WLCG is vital to security of Data and Services, e.g.
  - DavidC co-leading WLCG SOC working group
  - DavidK is the WLCG policy coordinator
- Other EGI/EOSC-hub security partners are not so closely engaged with WLCG

History: role for a “Grid” CSIRT

- NREN CSIRTs versus EGEE/EGI CSIRT
  - Research Security vs Enterprise security
  - User/Identity based incidents versus DDOS, port scans, web services, …
- Many NREN CSIRTs claimed a Grid CSIRT was not needed
  - But we convinced them!
  - We tackle different threats and add value
- EGI CSIRT is now fully Certified by Trusted Introducer (since 2014)
  - Very positive comments at a Jisc UK Security and AAI meeting Andrew Cormack (Jisc) about the EGI CSIRT

EGI CSIRT Collaborations

- Oct 2012: Trusted Introducer
  Member of TERENA TF-CSIRT
- EGI CSIRT is an accredited team in the European database of CSIRTs
- Oct 2014: full certification
- EGI-CSIRT collaborations
  - Public and non-public vetted networks
    - FIRST and NREN CERTS
  - Grid-SEC: coordinated response to cross-grid security incidents (vetted security representatives from WLCG, OSG, XSEDE, EGI)
  - **WISE** and related Trust bodies

Another tribute

- Ian Bird's statement from his TNC2011 Keynote talk (Prague)
  - while he was discussing "Grids versus Clouds"
- "The reason we have a Grid is because we need to collaborate and we need to share resources. So no matter what we do and no matter what technology we deploy underneath we will always have a Grid. Our network of trust and all of the security infrastructure that goes with that is of enormous value to us and I don't think we want to lose that. I think it is also of enormous value to eScience in general because I think this is one of the things that allows people to collaborate across these infrastructures and I think that probably should sit on top of the pile as one of the major achievements of this 10 years of work on Grids."
- https://tnc2011.terena.org/web/media/archive/7A
  - (audio/video archive - at 41 mins 35 secs)

Cybersecurity: We Don't Have It Right Yet

Von Welch
Director, Trusted CI
Director, IU CACR

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

2018 NSF Cybersecurity Summit

August 22nd, 2018

Cybersecurity Is a New Profession.

Is It Possible We Don't Have It Right Yet?

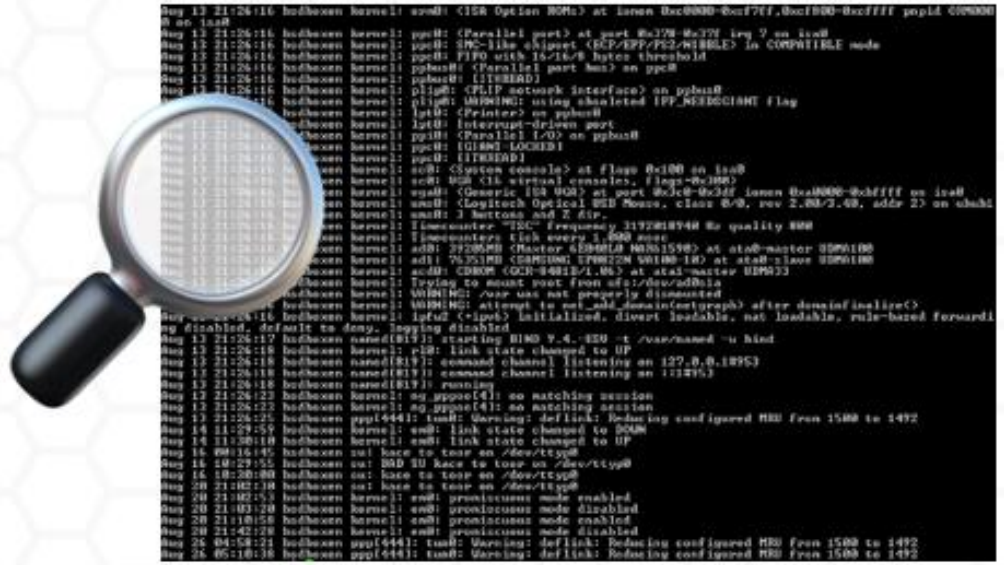
The Dreaded Cybersecurity Demo

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

The Copper Plumbing Problem: Your House After Copper Plumbing

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

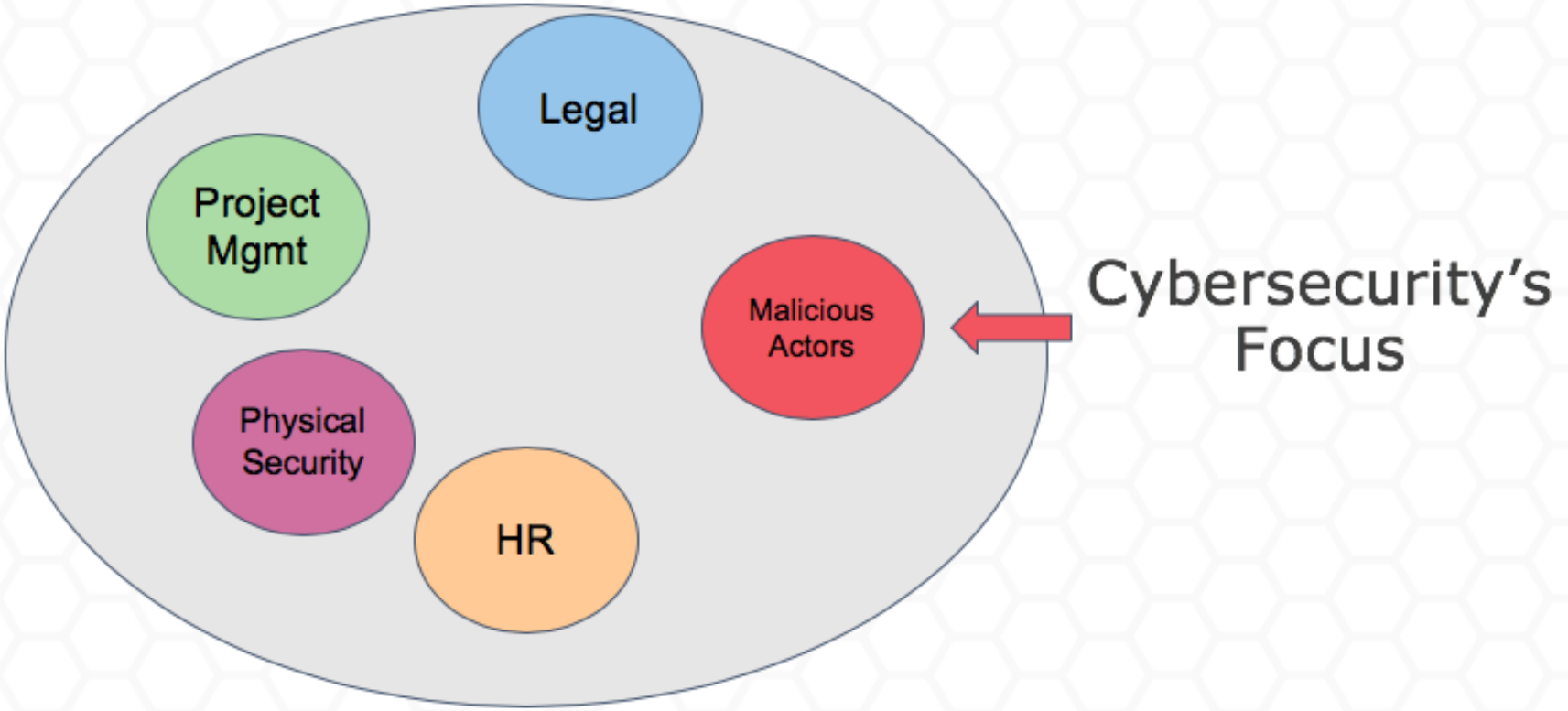
The Usual Cybersecurity Demo



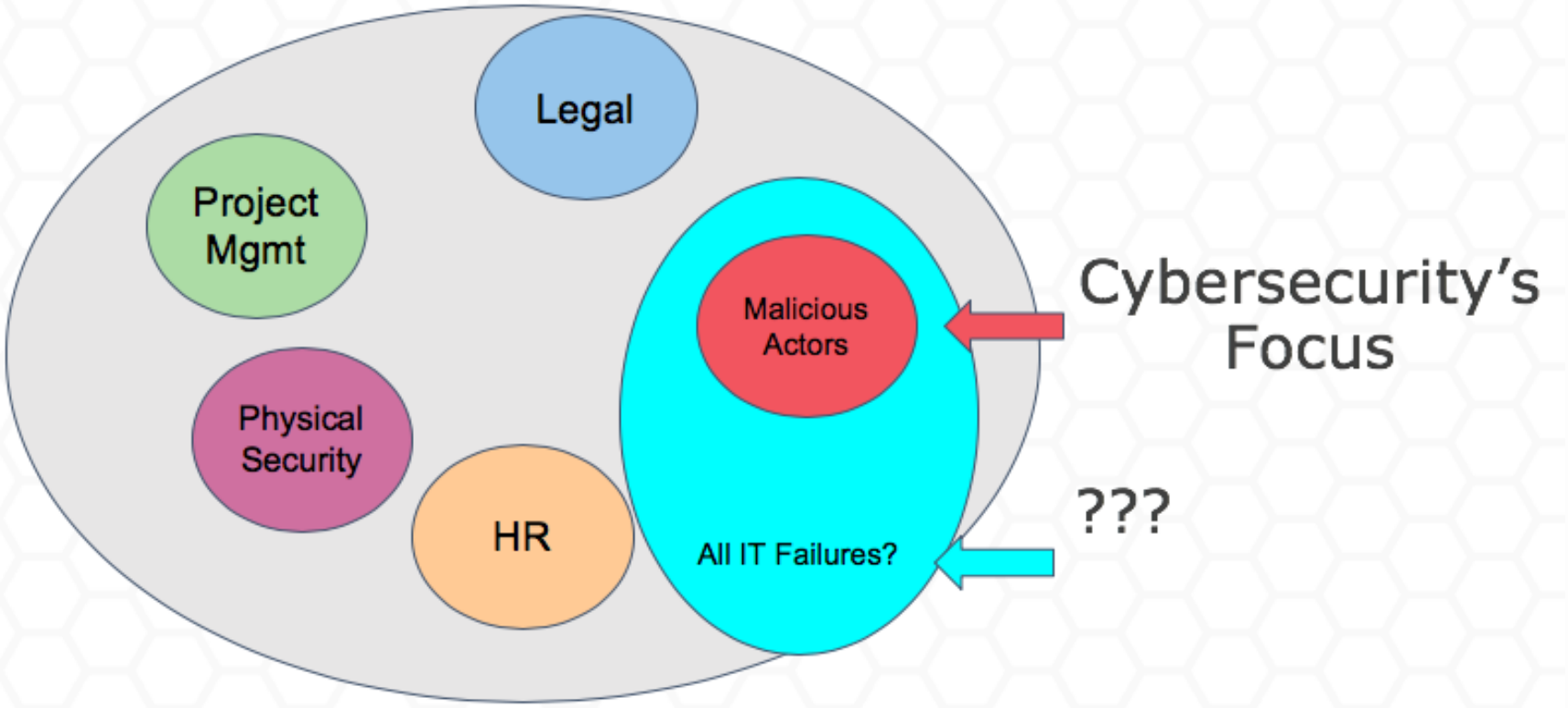
http://bsdpants.blogspot.com/2010/08/truncated-syslog-messages.html

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

The Risk Pool: What Keeps A Project Leader Awake



The Risk Pool: What Keeps A Project Leader Awake



Worthy of more thought!

Cybersecurity for Science

Confidentiality
Integrity
Availability

Efficient
Trusted
Reproducible

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Security, Trust and Identity FY18/19

2018-19 activities and source of funding

- GridPP5 & WLCG (1.5 FTE)
  - Security — 0.9 FTE
  - Trust and Identity Management — 0.45 FTE
  - Co-funding for EGI — 0.15 FTE
- EU H2020 EOSC-hub (0.7 FTE) / EGI Core (0.15 FTE)
  - Security, Trust and Identity Management — 0.85 FTE
- EU H2020 AARC2
  - Trust and Identity Management — 0.6 FTE
- STFC/RAL PPD National Labs
  - Security — 0.25 FTE

Total funded effort = 3.2 FTE (across 4 people)
of which 1.5 FTE is GridPP5

What should we bid for in GridPP6?

- The UK NGI team works very well and should continue in GridPP6
- Increasing technical complexity increases risk
- Decreasing Tier 2 effort may increase the security risk
  - And emphasises importance of a central team
- We play an important role in UK/EU and WLCG and we want to continue
  - Build on our success
  - As the basis for a larger/more general activity in the UK
- Security is ONGOING – new threats, new risks, new mitigations
  - Handling incidents, vulnerabilities, monitoring, evolution of policies and procedures, training and dissemination, compliance, collaboration, global trust
  - New AAI technologies

Future funding – our proposal

- Largest uncertainty – will EU Framework Europe funding happen? (BREXIT)
  - If allowed, we will seek funding in EOSC/EGI
  - If not then seek UKRI funding
- To continue doing everything we need ~3 FTE (~2 Security, ~1 Trust & Identity)
- We MUST continue supporting GridPP security (~1.0 FTE)
- and WLCG Security & international collaboration (~1.0 FTE),
  - including Trust & Identity
  - and we need appropriate T&S funds

- We should aim to build a broader UK team
  - to meet needs of growing infrastructures and more communities (UK IRIS etc)
- TOTAL size of team ~5 FTE
  - Of which we should bid 2.0 FTE from GridPP6

Questions and discussion?