



# WLCG Risk Assessment ?update

*Ian Neilson*

*RAL STFC UK*

# Traceability

*“The impact of security incidents on WLCG depends on the degree of compromise, but also heavily on the degree of traceability implemented on the affected services and resources..*

*Traceability is an extremely important aspect of computer security, and most incidents whose cause could not be determined will most likely re-occur within the next months.*

*Traceability is a key element to incident response and a sufficient level of traceability is essential to protect WLCG against misused identities and keeping services operational.”*



# Assets

- Trust / collaboration
- Reputation
- Intellectual property
- Data protection
- Digital identities
- CPU resources
- Data Resources
- Network Resources
- Services
- Data Integrity



Science & Technology  
Facilities Council

# Threats

- Misused identities
- Attack propagation
- Negative publicity
- Incidents .. not bound by WLCG policies
- DoS from external ..
- Data removal/corruption/..
- Exploit of VO/middleware vulnerability
- Exploit of serious OS vuln
- Insecure config leading to undesirable access
- Insufficient protection of info. leading to sensitive data leakage
- Threats originating from trust services



# WLCG Risks Analysis 2012

<a href="https://twiki.cern.ch/twiki/bin/view/LCG/WLCGSecurityTEG"><u>https://twiki.cern.ch/twiki/bin/view/LCG/WLCGSecurityTEG</u></a>	<i>Likelihood, Impact (5)</i>
– Misused identities	5,3 -> 15
– Attack propagation between WLCG sites	3,4 -> 12
– Exploitation of a serious OS vulnerability	4,3 -> 12
– Threats originating from trust services	2,4 -> 8
– Negative publicity on a non-event	2,4 -> 8
– Insecure configuration leading to undesirable access	3,2 -> 6
– Insufficient protection of info. leading to sensitive data leakage	3,2 -> 6
– Incidents on resources not bound by WLCG policies	1,4 -> 4
– Exploitation of a serious VO/middleware software vulnerability	2,2 -> 4
– Data removal/corruption/alteration	1,3 -> 3
– DoS from an external organisation	1,1 -> 1



Science & Technology  
Facilities Council

# WLCG Risks Analysis 2012

<a href="https://twiki.cern.ch/twiki/bin/view/LCG/WLCGSecurityTEG"><u>https://twiki.cern.ch/twiki/bin/view/LCG/WLCGSecurityTEG</u></a>	<i>Likelihood, Impact (5)</i>
– Misused identities	5,3 -> 15
– Attack propagation between WLCG sites	Likelyhood already at 5!
– Exploitation of a serious OS vulnerability	4,3 -> 12
– Threats originating from trust services	2,4 -> 8
– Negative publicity on a non-event	2,4 -> 8
– Insecure configuration leading to undesirable access	3,2 -> 6
– Insufficient protection of info. leading to sensitive data leakage	3,2 -> 6
– Incidents on resources not bound by WLCG policies	1,4 -> 4
– Exploitation of a serious VO/middleware software vulnerability	2,2 -> 4
– Data removal/corruption/alteration	1,3 -> 3
– DoS from an external organisation	1,1 -> 1



Science & Technology  
Facilities Council

# WLCG Risks Analysis 2012

<a href="https://twiki.cern.ch/twiki/bin/view/LCG/WLCGSecurityTEG">https://twiki.cern.ch/twiki/bin/view/LCG/WLCGSecurityTEG</a>	<i>Likelihood, Impact (5)</i>
– Misused identities	5,3 -> 15
– Attack propagation between WLCG sites	3,4 -> 12
– Exploitation of a serious OS vulnerability	
– Threats originating from trust services	2,4 -> 8
– Negative publicity on a non-event	2,4 -> 8
– Insecure configuration leading to undesirable access	3,2 -> 6
– Insufficient protection of info. leading to sensitive data leakage	3,2 -> 6
– Incidents on resources not bound by WLCG policies	1,4 -> 4
– Exploitation of a serious VO/middleware software vulnerability	2,2 -> 4
– Data removal/corruption/alteration	1,3 -> 3
– DoS from an external organisation	1,1 -> 1

**Use of more “standard” software stacks**



Science & Technology  
Facilities Council

# WLCG Risks Analysis 2012

<a href="https://twiki.cern.ch/twiki/bin/view/LCG/WLCGSecurityTEG"><u>https://twiki.cern.ch/twiki/bin/view/LCG/WLCGSecurityTEG</u></a>	<i>Likelihood, Impact (5)</i>
– Misused identities	5,3 -> 15
– Attack propagation between WLCG sites	3,4 -> 12
– Exploitation of a serious OS vulnerability	4,3 -> 12
– Threats originating from trust services	2,4 -> 8
– Negative publicity on a non-even	<b>Federated identity, credential translation services</b>
– Insecure configuration leading to undesirable access	3,2 -> 6
– Insufficient protection of info. leading to sensitive data leakage	3,2 -> 6
– Incidents on resources not bound by WLCG policies	1,4 -> 4
– Exploitation of a serious VO/middleware software vulnerability	2,2 -> 4
– Data removal/corruption/alteration	1,3 -> 3
– DoS from an external organisation	1,1 -> 1



# WLCG Risks Analysis 2012

<a href="https://twiki.cern.ch/twiki/bin/view/LCG/WLCGSecurityTEG"><u>https://twiki.cern.ch/twiki/bin/view/LCG/WLCGSecurityTEG</u></a>	<i>Likelihood, Impact (5)</i>
– Misused identities	5,3 -> 15
– Attack propagation between WLCG sites	3,4 -> 12
– Exploitation of a serious OS vulnerability	4,3 -> 12
– Threats originating from trust services	2,4 -> 8
– Negative publicity on a non-event	2,4 -> 8
– Insecure configuration leading to undesirable access	3,2 -> 6
– Insufficient protection of info. leading to sensitive data leakage	3,2 -> 6
– Incidents on resources not bound by WLCG policies	<b>Media and public/gov. awareness</b>
– Exploitation of a serious VO/middleware software vulnerability	
– Data removal/corruption/alteration	
– DoS from an external organisation	



Science & Technology  
Facilities Council

# WLCG Risks Analysis 2012

<a href="https://twiki.cern.ch/twiki/bin/view/LCG/WLCGSecurityTEG"><u>https://twiki.cern.ch/twiki/bin/view/LCG/WLCGSecurityTEG</u></a>	<i>Likelihood, Impact (5)</i>	
– Misused identities	5,3 -> 15	
– Attack propagation between WLCG sites	3,4 -> 12	
– Exploitation of a serious OS vulnerability	4,3 -> 12	
– Threats originating from trust services	2,4 -> 8	
– Negative publicity on a non-event	2,4 -> 8	
– Insecure configuration leading to undesirable access	3,2 -> 6	
– Insufficient protection of info. leading to sensitive data leakage	3,2 -> 6	
<b>– Incidents on resources not bound by WLCG policies</b>	<b>1,4 -&gt; 4</b>	
– Exploitation of a serious VO/mid	<b>Commercial cloud use, operations and financial risk</b>	
– Data removal/corruption/alteration	1,3 -> 3	
– DoS from an external organisation	1,1 -> 1	



Science & Technology  
Facilities Council

# WLCG Risks Analysis 2012

<a href="https://twiki.cern.ch/twiki/bin/view/LCG/WLCGSecurityTEG"><u>https://twiki.cern.ch/twiki/bin/view/LCG/WLCGSecurityTEG</u></a>	<i>Likelihood, Impact (5)</i>
– Misused identities	5,3 -> 15
– Attack propagation between WLCG sites	3,4 -> 12
– Exploitation of a serious OS vulnerability	4,3 -> 12
– Threats originating from trust services	2,4 -> 8
– Negative publicity on a non-event	2,4 -> 8
– Insecure configuration leading to undesirable access	3,2 -> 6
– Insufficient protection of info. leading to sensitive data leakage	3,2 -> 6
– Incidents on resources not bound by WLCG policies	1,4 -> 4
– Exploitation of a serious VO/middleware software vulnerability	2,2 -> 4
– <b>Data removal/corruption/alteration</b>	1,3 -> 3
– DoS from an external organisation	

? Encryption ransomware



Science & Technology  
Facilities Council

# WLCG Risks Analysis 2012

<a href="https://twiki.cern.ch/twiki/bin/view/LCG/WLCGSecurityTEG"><u>https://twiki.cern.ch/twiki/bin/view/LCG/WLCGSecurityTEG</u></a>	<i>Likelihood, Impact (5)</i>
– Misused identities	5,3 -> 15
– Attack propagation between WLCG sites	3,4 -> 12
– Exploitation of a serious OS vulnerability	4,3 -> 12
– Threats originating from trust services	2,4 -> 8
– Negative publicity on a non-event	2,4 -> 8
– Insecure configuration leading to undesirable access	3,2 -> 6
– Insufficient protection of info. leading to sensitive data leakage	3,2 -> 6
– Incidents on resources not bound by WLCG policies	1,4 -> 4
– Exploitation of a serious VO/middleware software vulnerability	2,2 -> 4
– Data removal/corruption/alteration	1,3 -> 3
– DoS from an external organisation	1,1 -> 1

JANET DDOS



Science & Technology  
Facilities Council

# Acknowledgements

*Dave Kelsey, Maarten Litmaath, Steffen Schreiner, Von Welch, Romain Wartel, John White, Christoph Witzig*

*And the members of the WLCG Security Technology Evolution Group*



Science & Technology  
Facilities Council