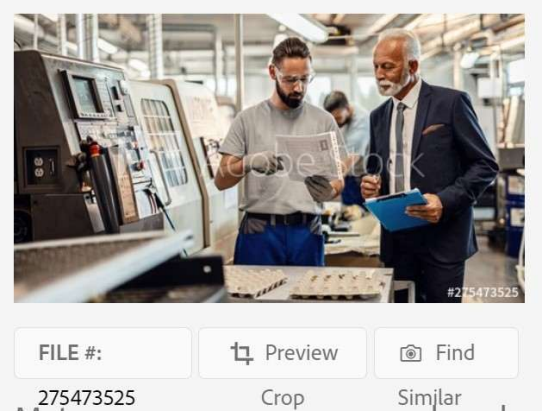
Industrial Cybersecurity for the CISO
Annex 1

Micro Learning Module

MLM-050-D

Industry	–	Process
Principal Role	–	Owner
Professional Role	–	All
Enterprise Phase	–	Master Planning



Author

Vytautas Butrimas

Author's presented views do not represent the official position of NATO

Turn on your audio and click start to begin video

START

Annex 1: Industrial Cybersecurity References

The following is a selection of cybersecurity references and links that may be useful for CISOs:

I. Overview of industrial cybersecurity. Video lecture "Cybersecurity of Critical [x] infrastructure", Riga conference Oct 2019
   I. I will also share a link to a presentation made to the DSS ITSEC 2019 Conference in Riga which will give you an idea of I start at the 1 hour 7 minute mark https://www.facebook.com/DSSITSEC/videos/688528324963820/

II. Information Technology vs Operational Technology issue
   a. Butrimas, V. The Cybersecurity Dimension of Critical Energy Infrastructure, perConcordiam Vol 3-4 pp.12-17. 2012 https://perconcordiam.com/v3n4-eng/
   b. Cyber mishap causes nuclear power plant shutdown Hatch, http://www.homelandsecuritynewswire.com/cyber-mishap-causes-nuclear-power-plant-shutdown
   c. IT and ICS cybersecurity: a "Tale of Two Cities" , http://scadamag.infracritical.com/index.php/2017/08/21/1984/
   d. Weiss, J., Are the Good Guys as Dangerous as the Bad Guys – an Almost Catastrophic Failure of the Transmission Grid, Control Global, 11/02/2017 https://www.controlglobal.com/blogs/unfettered/are-the-good-guys-as-dangerous-as-the-bad-guys-an-almost-catastrophic-failure-of-the-transmission-grid/
   e. Horden, N., Cybersecurity in Public-Safety Communications, Mission Critical Communications, September-October 2018 pp. 14-19. http://digital.olivesoftware.com/Olive/ODN/MissionCriticalArchive/default.aspx?olv-cache-ver=20181018023533

III. Cybersecurity capacity identification and building
   a. NCSS Good Practice Guide, ENISA 2016, https://www.enisa.europa.eu/publications/ncss-good-practice-guide
   b. National Cyber Security Strategies Guidelines & tools, ENISA https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools
   c. List Cyber Security Strategy Documents, NATO CCDCOE, https://ccdcoe.org/library/strategy-and-governance/
   d. Butrimas, V., National Cyber Security Organisation: Lithuania, NATO CCDCOE 2015, https://ccdcoe.org/library/publications/national-cyber-security-organisation-lithuania/

Industrial Cybersecurity References

III. Importance of applying the correct CEIP policies and strategies

a. Butrimas, V., Towards a Cyber Safe Critical Infrastructure: Answering the 3 questions, http://scadamag.infracritical.com/index.php/2018/02/21/towards-cyber-safe-critical-infrastructure-answering-3-questions/ February 21, 2018.

b. Microsoft Cybersecurity Policy Framework, https://www.microsoft.com/en-us/cybersecurity/content-hub/Cybersecurity-Policy-Framework 2018

IV. Public Private Partnership best practice

a. US DHS Industrial Control System CERT (ICS-CERT) , https://us-cert.cisa.gov/ics

b. KraftCERT Norway's ICS-CERT, https://www.kraftcert.no/english/index.html

c. CyberGym: Who We Are. https://www.cybergym.com/company/

V. Multi-stakeholder cyber threat protection efforts

a. A Digital Geneva Convention to protect cyberspace, Microsoft, https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace 2017

b. Parker, B. (2017) Bots and bombs: Does cyberspace need a 'Digital Geneva Convention'?. Irinnews. Available from http://www.irinnews.org/analysis/2017/11/15/bots-and-bombs-does-cyberspace-need-digital-geneva-convention [Accessed 16th October 2018]

c. OSCE

i. OSCE CONFIDENCE-BUILDING MEASURES TO REDUCE THE RISKS OF CONFLICT STEMMING FROM THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES https://www.osce.org/pc/227281?download=true

d. United Nations

i. United Nations General Assembly (2015) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/70/174 (22nd July)

ii. Tikk, E. and Kerttunen, M. (2018) Parabasis. Cyber diplomacy in stalemate. Norwegian Institute of International Affairs. Available from https://www.nupi.no/Publkasjoner [Accessed 16th November 2018]

Industrial Cybersecurity References

VI. Some noteworthy cyber-attacks against Industrial Control Systems

a. Stuxnet malware at nuclear enrichment facility
   i. See Ralph Langer's Deep Dive on Stuxnet lecture: https://www.youtube.com/watch?v=zBjmm48zwQU
   ii. http://www.digitalbond.com/blog/2016/06/20/s4-classic-video-langners-stuxnet-deep-dive/
   iii. https://www.langner.com/to-kill-a-centrifuge/ or https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf
   iv. See Kim Zetter's book on Stuxnet listed on page 6 (Books) of these references

b. Steel mill in Germany
   i. https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf
   ii. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014.pdf?__blob=publicationFile&v=3

c. Against ICS in Ukraine
   i. https://www.eset.com/int/industroyer/
   ii. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
   iii. Slowik, J, Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

d. Hatman/Triton malware compromises safety instrumented systems at energy facility
   i. https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%E2%80%94Safety%20System%20Targeted%20Malware_S508C.pdf
   ii. https://dragos.com/blog/trisis/TRISIS-01.pdf
   iii. http://scadamag.infracritical.com/index.php/2018/08/28/targeting-control-and-safety-instrumented-systems-sis-new-escalation-of-cyber-threats-to-critical-energy-infrastructure/

Industrial Cybersecurity References

Malware crafted to target ICS or which has indirectly affected ICS

a. NotPetya
   i. https://www.us-cert.gov/ncas/alerts/TA17-181A
   ii. https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/
   iii. https://www.itnews.com.au/news/maersk-had-to-reinstall-all-it-systems-after-notpetya-infection-481815?eid=65&edate=20180130&utm_source=20180130&utm_medium=newsletter&utm_campaign=sc_weekly
   iv. http://www.darkreading.com/attacks-breaches/ransomware-attack-on-merck-caused-widespread-disruption-to-operations/d/d-id/1329503
   v. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (nice story on implications of NotPetya by journalist Andy Greenberg and worth reading)

b. CrashOveride/industroyer
   i. https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-206-01
   ii. https://www.eset.com/int/industroyer/?source=newsroom&campaign=industroyer
   iii. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_6.pdf

c. Using cyrpto mining malware on ICS systems (new trend)
   i. https://www.wired.com/story/cryptojacking-critical-infrastructure/?mbid=email_onsiteshare

Industrial Cybersecurity References

About ICS standards

a. ISO standards for Petroleum and related https://www.iso.org/ics/75/x/
b. htttp://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
c. About ISA https://www.isa.org/standards-and-publications/isa-standards/
d. "Quick Start Guide: An Overview of the ISA/IEC 62443 Standards" https://gca.isa.org/isagca-quick-start-guide-62443-standards
e. ANSI/ISA-62443 Security for Industrial Automation and Control Systems http://isaeurope.com/iec62443/
f. Good news for ICS protection: ISA providing new ISA/IEC 62443 based industrial cybersecurity training, http://scadamag.infracritical.com/index.php/2017/03/17/good-news-for-ics-protection-isa-providing-new-isaiec-62443-based-industrial-cybersecurity-training/
g. IEC 61850 is a standard for vendor-agnostic engineering of the configuration of Intelligent Electronic Devices for electrical substation automation systems to be able to communicate with each other. https://en.wikipedia.org/wiki/IEC_61850
h. https://www.api.org/~/media/Files/Policy/Cybersecurity/2018/Defense-in-Depth-Cybersecurity-in-the-Natural-Gas-and-Oil-Industry.pdf

IX. About conferences and trainings in cybersecurity of ICS

a. https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT
b. https://www.isa.org/isa-training/online-training/
c. https://www.isa.org/events-conferences/
d. BlackHat https://www.blackhat.com/
e. Dale Petersons S4 conference lectures https://www.youtube.com/c/S4Events/videos
f. Chaos Computer Club http://www.ccc.de/en/
g. CS3STHLM – the Stockholm international summit on Cyber Security in SCADA and Industrial Control Systems https://cs3sthlm.se

Industrial Cybersecurity References

Selected sources for current information about ICS https://ics-cert.us-cert.gov/

i. Subscribe to newsletters https://us-cert.cisa.gov/ics

ii. https://ics-cert.us-cert.gov/ICS-CERT-Feeds

iii. Overview of Cyber Vulnerabilities for ICS https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities ,accessed on October 23 2018

a. Professional Journals

i. https://www.isa.org/standards-and-publications/isa-publications/intech-magazine/

b. Books

i. Robert Radvanovsky (Editor), Jacob Brodsky (Editor) , Handbook of SCADA/Control Systems Security, Second Edition 2nd Edition, https://www.amazon.com/Handbook-Control-Systems-Security-Second/dp/1498717071/ref=mt_hardcover?_encoding=UTF8&me=

ii. Ralph Langner, Robust Control System Networks: How to achieve reliable control after Stuxnet. https://www.amazon.com/Robust-Control-System-Networks-Langner/dp/1606503006

iii. Greenberg, Andy, Sandworm A new era of cyberware https://www.amazon.com/Sandworm-Cyberwar-Kremlins-Dangerous-Hackers/dp/0385544405

iv. Zetter, K., Countdown to Zero Day Stuxnet and launch of the worlds first cyber weapon, https://www.penguinrandomhouse.com/books/219931/countdown-to-zero-day-by-kim-zetter/

v. Joe Weiss, Protecting Industrial Control Systems from Electronic Threats, https://www.amazon.com/Protecting-Industrial-Control-Systems-Electronic/dp/1606501976/ref=sr_1_fkmr0_1?s=books&ie=UTF8&qid=1519289278&sr=8-1-fkmr0&keywords=Joe+Weiss+Electronic

Industrial Cybersecurity References

XI. Strategy choices coming in the future

a. Butrimas, V., International Implications of securing our SCADA/control system environments , Robert Radvanovsky (Editor), Jacob Brodsky (Editor) , Handbook of SCADA/Control Systems Security, Second Edition 2nd Edition, pp. 82-104. https://www.amazon.com/Handbook-Control-Systems-Security-Second/dp/1498717071/ref=mt_hardcover?_encoding=UTF8&me=

b. SCADASEC List : Where to discuss industrial control systems with colleagues from all over the world https://groups.io/g/scadasec

c. Industry 4.0 / Fourth Industrial Revolution is “Coming to a Scada near you.”

   i. Recommendations for implementing the strategic initiative INDUSTRIE 4.0 https://www.acatech.de/wp-content/uploads/2018/03/Final_report__Industrie_4.0_accessible.pdf

   ii. Brave new Industrie 4.0 https://www.youtube.com/watch?v=ZrZKiy2KPCM

   iii. Cyber-Physical Systems: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf

   iv. Rob Joyce, Chief, Tailored Access Operations, National Security Agency, USENIX Enigma 2016 Conference - Disrupting Nation State Hackers, https://www.youtube.com/watch?v=bDJb8WOJYdA

   v. Demchak, Chris C. and Shavitt, Yuval (2018) "China’s Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom’s BGP Hijacking,"Military Cyber Affairs: Vol. 3 : Iss. 1 , Article 7. DOI: https://doi.org/10.5038/2378-0789.3.1.1050 Available at: https://scholarcommons.usf.edu/mca/vol3/iss1/7

Industrial Cybersecurity References

XII. Last but not least

a. Butrimas, V., Ensuring the security and availability of critical infrastructure in a changing cyber-threat environment: Living dangerously, Routledge Handbook of International Cybersecurity, T., Enekken, Kerttunen, M., Ed., Routledge 2020. https://www.routledge.com/Routledge-Handbook-of-International-Cybersecurity-1st-Edition/Tikk-Kerttunen/p/book/9781138489011

b. NATO CMX Exercises with cyber and critical infrastructure https://www.hzscr.cz/hasicien/article/nato-annual-crisis-management-exercise-cmx-2012.aspx

c. https://enseccoe.org/en/newsroom/nato-ensec-coe-preparing-for-the-flagship-ttx-coherent-resilience-2019/399

d. International cyber norms for states: GCSC Global Commission on Stability of Cyberspace https://cyberstability.org/

e. Butrimas, V., The Cybersecurity Dimension of CEI perConcoridam page 12 https://perconcordiam.com/v3n4-eng/ 2012

f. http://www.theguardian.com/uk-news/2014/jan/23/londons-victoria-line-suspended-after-control-room-is-flooded-with-cement

g. San Bruno pipeline rupture 2010 report https://www.cpuc.ca.gov/uploadedFiles/CPUC_Public_Website/Content/Safety/Natural_Gas_Pipeline/News/AgendaStaffReportreOIIPGESanBrunoExplosion.pdf

h. http://www.ntsb.gov/doclib/reports/2002/PAR0202.pdf

i. Integrity Management of Gas Transmission Pipelines in High Consequence Areas https://dms.ntsb.gov/public/57000-57499/57122/569749.pdf

j. List of downloadable reports on pipeline accidents https://web.archive.org/web/20080509192228/http://www.ntsb.gov/publictn/P_Acc.htm

k. Title: Pipeline Accident Report: Pipeline Rupture and Release of Gasoline, Olympic Pipeline Company, Bellingham, Washington, June 10, 1999 NTSB Report Number: PAR-02-02, adopted on 10/8/2002 [Summary | PDF Document]NTIS Report Number: PB2002-916502 https://web.archive.org/web/20080410164408/http://www.ntsb.gov/publictn/2002/PAR0202.pdf

Industrial Cybersecurity References

XII-b. Last but not least

a. https://www.controldesign.com/articles/2015/the-father-of-the-plc-explains-its-birth/ Richard "Dick" Morley

b. https://en.wikipedia.org/wiki/Taum_Sauk_Hydroelectric_Power_Station

c. IEA Digitalisation and Energy https://www.connaissancedesenergies.org/sites/default/files/pdf-actualites/digitalizationandenergy3.pdf

d. Guidance on Improving Resilience of National and Cross-Border Energy Networks, 13 November 2017 NU AC/98-D(2017)0005 NATO Industrial Resources and Communication Services Group (IRCSG Industry)

e. DC Metro Crash 2009 http://www.ntsb.gov/publictn/2010/RAR1002.pdf https://trid.trb.org/view/934283 https://www.ntsb.gov/investigations/AccidentReports/Reports/RAR1002.pdf

f. https://ics.sans.org/media/Media-report-of-the-BTC-pipeline-Cyber-Attack.pdf more speculative from Bloomberg https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar

g. IT vs OT vs ICS models http://icsmodel.infracritical.com/ http://icsmodel.infracritical.com/

h. Top 10 tuning tips for control engineers https://www.controleng.com/articles/top-10-tuning-tips-for-control-engineers/

i. https://www.createdigital.org.au/measure-manufacturing-equipment-efficiency/

j. Eight 8 questions to ask about your industrial control systems security https://www.csoonline.com/article/3262641/critical-infrastructure/8-questions-to-ask-about-your-industrial-control-systems-security.html

k. Modbus guide for field technicians http://www.modbusbacnet.com/includes/pdf/MODBUS_2010Nov12.pdf

l. https://www.controleng.com/articles/inside-the-competition-for-the-first-plc/

m. https://www.auma.se/produkter/marknader/olja-gas/auma-sa072-162-med-ac012/

n. Texas City refinery explosion 2005 https://www.youtube.com/watch?v=c9JY3eT4cdM

   a. https://www.csb.gov/file.aspx?DocumentId=5596

   b. https://www.youtube.com/watch?v=goSEyGNfiPM

Industrial Cybersecurity References

XII-c. Last but not least

a. Boeing 737 Max Crash Report https://transportation.house.gov/imo/media/doc/2020.09.15%20FINAL%20737%20MAX%20Report%20for%20Public%20Release.pdf
b. https://www.ntsb.gov/investigations/AccidentReports/Pages/PLD18MR003-preliminary-report.aspx
c. Diesel Gate https://www.bbc.com/news/business-34324772
d. https://www.controlglobal.com/blogs/unfettered/diesel-cheat-scandal-affects-almost-12-million-vehicles-an-industrial-strength-cyber-event/
e. Maroochy Shire 2000 Case Study https://www.mitre.org/sites/default/files/pdf/08_1145.pdf
f. http://www.pbs.org/wgbh/nova/next/tech/cyber-attack-german-steel-mill-leads-massive-real-world-damage/
g. https://www.pbs.org/wgbh/nova/article/cyber-attack-german-steel-mill-leads-massive-real-world-damage/
h. http://www.wired.com/2015/01/german-steel-mill-hack-destruction/
i. https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/
j. https://www.linkedin.com/pulse/how-search-icsscada-systems-using-shodan-muhammad-mesbah/
k. Purdue Model http://www.pera.net/
l. Brodsky, J., http://scadamag.infracritical.com/index.php/2017/07/27/how-a-process-works/
m. https://dale-peterson.com/2019/02/14/ics-security-patching-never-next-now/
n. https://www.rockwellautomation.com/en-us/products/software/factorytalk.html
o. http://sccs.sourceforge.net/man/sccs.me.html
p. https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/
q. https://www.nytimes.com/2019/02/12/us/politics/trump-china-wireless-networks.html

Author – Vytautas Butrimas

Vytautas Butrimas has been working in defense and cyber security roles for over 30 years including:

- Vice-minister at the Ministry of Communications and Informatics, Republic of Lithuania responsible for Information Society programs.
- Defense Policy and Planning Director, Lithuanian Ministry of National Defense (MoND) responsible for preparing the first Military Defense Strategy.
- Deputy Director responsible for IT security at the Communications and Information System Service (CISS) responsible for preparing the first National Defense System Cybersecurity Strategy
- Chief Adviser for the MoND of Lithuania with a focus on cybersecurity policy, including the national task force that wrote the Lithuanian Law on Cybersecurity
- Member (Presidential appointee) of the National Communications Regulatory Service's Council (RTT-Coucil)
- Cybersecurity Subject Matter Expert for the NATO Energy Security Center of Excellence (NATO ENSECCOE) who performed a Cyber Risk Study of the ICS Used in the NATO Central Europe Pipeline System (CEPS)

Please click here to provide feedback on this MLM.