Security-Policy
NET Nexus of Emerging Technologies

BRIEFING NOTES

# BN-15-COVID19-June2020

DATA SECURITY AND REMOTE WORK IN WAKE OF COVID-19

Authors: Whitney Gagnon[1], Julian Spencer-Churchill[2]

[1] Undergraduate student, Department of Political Science, Concordia University, Montreal, Canada

[2] Professor, Department Political Science, Concordia University, Montreal, Canada.

SUMMARY

- The purpose of this briefing note is to review possible data security issues – and their strategic ramifications - highlighted by the massive shift toward remote work in the wake of the COVID-19 pandemic.

CONTEXT

- As a greater number of both key personnel and supporting staff are moved to remote, working-from-home situations, the availability of information and real-time updates in ongoing situations becomes a key point of possible failure.
- Maintaining data security and access to information from remote locations without compromising security or creating new vulnerabilities in access becomes crucial.
- There is no doubt that both China and the U.S. will suffer a loss of legitimacy following the crisis due to failures to respond to necessities of the moment, and it is probable that an event such as a major data breach would have a similar effect on the DND/CAF.

ISSUES

- Increased reliance on remote / cloud data (increased remote access increases the potential gate ways and vulnerability points for security breaches).
- Security of VPN access to sensitive information (authentication and identification of inappropriate use/adversarial attack).
- Real-time availability of information and support for individuals and teams overseas or on assignment.
- Recent spike in cyberattacks related to increased number of people working from home on unsecured systems (e.g. the WHO leak in April).
- Need to identify / defend against compromised log-in information from phishing scams, key logging algorithms, etc.

KEY CONSIDERATIONS:

- Additional delay in receiving support information for individuals deployed or working overseas can pose a risk to individual safety, as well be deleterious to mental health during this time of increased situational stress.
- Biometric identifiers for authentication limit the possibility of unauthorized access, but raise ethical questions regarding individual privacy / ownership of biometric information, as well as opening the possibility of any data breach also compromising stored personal biometric information.

- Artificial intelligence (AI) can augment the ability of systems to identify unauthorized access by identifying adversarial attacks and aberrant access to data and systems through employee VPN connections, but may create disproportionate false positives in groups that are forced by pandemic conditions to work odd hours (for example, individuals with young children, individuals with disabilities).
- Access to physical hardware supporting networks and cloud systems may be compromised by travel restrictions. Teams maintaining physical infrastructure may be at disproportionate risk of contracting the virus – requiring both increased care in managing IM/IT teams and need for additional redundancies within the teams to respond to potential illness/disability.

OPTIONS AND RECOMMENDATIONS:

- Maintain core of key personnel to provide technical and logistic support to remote (overseas and working-from-home) individuals and teams, and provide rapid response for any IM/IT issues that arise.
- Recommend having multiple core teams working with disaggregated servers to provide real-time redundancies in the event of illness or compromise of teams or infrastructure.
- Enforce strict guidelines and training of personnel in order to reduce potential vulnerabilities and points of failure in individual systems. If possible, have access to restricted information operate within information “jails” on remote machines.
- Block chain encryption, due to the possibility of a built-in time delay on re-encrypting compromised information, can aid in early detection of indicators of compromise. Coupled with AI monitoring of data infrastructure may be able to significantly reduce the damage caused by cyber-attacks (for example emerging threats such as new advances in quantum computing – block chain encryption will not stop a quantum computing attack but will make one easier to detect and counter).
- Increased use of biometric identifiers in the VPN authentication process will reduce the possibility unauthorized access to systems (but will require clear guidelines regarding appropriate use and privacy, as well as appropriate encryption within the network holding the authentication data).

REFERENCES

Ali, Omar, Anup Shrestha, Akemi Chatfield, Peter Murray "Assessing information security risks in the cloud: A case study of Australian local government authorities." *Government Information Quarterly* 37(1)(January 2020): 1-20. https://doi.org/10.1016/j.giq.2019.101419.

AlgorithmWatch. "AI Ethics Guidelines Global Inventory." Last modified April 2020. https://inventory.algorithmwatch.org/about.

De Guzman, Jaybie A., Kanchana Thilakarathna, and Aruna Seneviratne. "Security and Privacy Approaches in Mixed Reality: A Literature Survey." *ACM Computing Surveys* 52 (6)(January 2020): 1–37. doi:10.1145/3359626.

Enderle, Rob. "CylancePERSONA: The First AI Solution to the Password Problem." *EWeek*, April 25, 2019. Accessed June 10, 2020.

Gilbert, Francoise. "Connected Devices--Privacy and Cybersecurity Legal Issues." *Licensing Journal* 39 (9) (October 2019): 1–12.

Groom, Frank M., Kevin Groom, Stephan S. Jones. *Network and Data Security for Non-Engineers.* Boca Raton: CRC Press, 2017.

Kovalcik, Justin and Mike Villalobos. "Automated Storage and Retrieval System: From Storage to Service." *Information Technology and Libraries* vol. 38(4)(Dec 2019): 114-124. https://doi.org/10.6017/ital.v38i4.11273.

Li, Liyuan, Tor Kar-Ann and Li Haizhou. *Advanced Topics in Biometrics*. Singapore: World Scientific, 2012.

Murray, Maryanne. "Block Chain Explained." *Reuters Graphics*. Published June 15, 2018. http://graphics.reuters.com/TECHNOLOGY-BLOCKCHAIN/010070P11GN/index.html.

Noguerol, Luis O. "Are Tokenization, Moving Target Protection Technology, Biometric Authentication, Machine Learning, Artificial Intelligence, and Quantum Cryptography the Saviours on the Cybersecurity War?" *Journal of IT and Economic Development* 10(1)(April 2019): 11-15. Accessed June 10, 2020.

Raab, Charles D. "Information Privacy, Impact Assessment, and the Place of Ethics." *Computer Law and Security Review: The International Journal of Technology Law and Practice* 1 (3) (March 2020): 1-16. https://doi.org/10.1016/j.clsr.2020.105404.

Trope, Roland L. "To Secure, or Not Secure, Data Integrity-That Is the Question: Cybersecurity Developments." *Business Lawyer* 75 (1) (Winter2019/2020 2019): 1655–66.

World Health Organization. "WHO reports fivefold increase in cyber attacks, urges vigilance." April 23, 2020. https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance.

Zhongshu Gu, Brendan Sataformaggio, Xiangyu Zhang, and Dongyan Xu. "GEMINI: Guest-transparent honey files via hypervisor-level access redirection." *Computers and Security* vol. 77 (August 2018): 737-744. https://doi.org/10.1016/j.cose.2018.02.014