Audit Committee Report BH.02.JUN0519.R03
June 5, 2019

Report To: **Audit Committee, Board of Health**
Submitted by: **Dr. Nicola Mercer, Medical Officer of Health & CEO**
Subject: **CYBER RISK**

RECOMMENDATION(S):

(a) That the Audit Committee makes recommendation to the Board of Health to receive this report for information.

BACKGROUND:

Wellington-Dufferin-Guelph Public Health (WDGPH) has a comprehensive and reliable infrastructure to support organization capacity. An effective cybersecurity strategy is one of the key enablers that WDGPH employs to ensure that all interconnected information systems are protected. Cyberthreats are continuously evolving each day and the statistics presented from a global standpoint speaks volumes to the associated risks that can impact an organization.[1] WDGPH has made significant progress in implementing risk mitigation strategies to reduce any impacts to the organization. However, as the extension of internet connectivity into computing devices and everyday objects accelerates, a continuous and collective cybersecurity effort by everyone at WDGPH is required. Information security is the responsibility of the entire organization.

PUBLIC HEALTH AND/OR FINANCIAL IMPLICATIONS:

Cyber Risk

Cyber risk is defined as any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems.[2] In a world where digital transformation is exponentially growing each day, cyber-attacks have become one of the most significant risks confronting organizations.

The internet is vast, consisting of billions of websites and users from across the world. This immense foot print provides cybercriminals an opportunity to exploit a multitude of cybersecurity threats. Cybercriminals are constantly trying to find new and innovative ways to increase the scale and sophistication of their activities to infiltrate organizations. There are multiple avenues for causing disruption to an organization's information technology ecosystem such as: stealing passwords, exploitation of weaknesses within business-related applications and network intrusions. However, one of the most common channels for exploitation is through social engineering and its relation to perhaps the weakest and most difficult to control vulnerability, the human mind.

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information.[3] Social engineering attacks can come in the form of phishing or luring a person to divulge valuable information via an email or a telephone call. Other significant threats are also predominantly spread through emails, known as malware, short for malicious software. Malware is software intentionally written to steal or encrypt data. Currently, ransomware is one of the most popular types of malware used by cybercriminals. Ransomware encrypts data within computer systems and cybercriminals demand payment in digital currency, usually Bitcoin, in return for decryption of the data.

Ransomware attacks have increased over 97 percent in the past two years with over 850 million ransomware infections detected in 2018.[4] Certain industries, such as healthcare, have historically been the main target for cybercriminals. Statistically, 90 percent of healthcare organizations experienced an increase in ransomware infection rates from 2017 to 2018.[4] This proliferation of attacks in the health care sector attributed to approximately half of the total ransomware incidents reported in 2018. [4] From a cost perspective, recent studies have found that the per capita cost of a data breach in healthcare is approximately $408 USD per stolen record.[5] Futuristically, as healthcare organizations become more interdependent and interconnected, it is estimated that healthcare related ransomware attacks will likely quadruple with organization's falling victim to a successful cyber attack every 11 seconds by 2021.[6,7]

An organization can incur direct and indirect costs resulting from cyber attacks. Direct costs refer to tangible losses in revenue, decreased profitability, fines, lawsuits and remediation. Resulting psychological, reputational and societal harms propagated by such attacks are the indirect costs that can lead to further disruptions.

By mid-2018, Canada was third in reported breaches on a global scale with 48 incidents.[8] Of the then 48 breaches reported, a total of 12,551,574 records were exposed with an average of approximately 260,000 records per breach. As per the Canadian Centre for Cyber Security, in May 2018, cybercriminals contacted two Canadian banks, claiming to have accessed the personal information of tens of thousands of clients. The cybercriminals threatened to release the information unless the banks paid them 1 million CAD in ransom. Both banks refused to pay, offered clients free credit monitoring, and pledged to cover any money lost from affected bank accounts due to fraud.[9] A recent public health sector example is Algoma Public Health. Their key information systems were infected by a ransomware attack, leaving the organization crippled for multiple weeks and the extent of the damage is still unknown.

To further illustrate the notion that no organization is fully immune from cybercrime, a fraudulent email was sent to a targeted employee within the administrative services division at a local institution requesting a change to the banking information for an existing employee. The banking information was changed, and funds were deposited to the cybercriminal account. After investigating and reporting to the necessary authorities, the funds were recovered, and the cybercriminal is still unknown to authorities.

Therefore, it is important to keep in mind that despite investments in sophisticated IT security systems, there is still a chance that any organization could fall victim to a successful cyber attack because of the human element. The best cyber risk defense an organization can have in this digital era is to stay current on innovative IT security solutions and ensure that all staff are appropriately trained to identify obvious IT security threats. As cybercriminals follow the path of least resistance, adopting a people-centric cybersecurity strategy can minimize the risks associated with an organization's drive towards digital transformation.

Mitigation Measures

There is no secret weapon against cyber threats that exists today. This is where a defense in depth cybersecurity strategy comes into play. A defense in depth strategy is an approach to cybersecurity in which a series of mechanisms are layered in order to protect valuable data and information.

Here are key risk mitigation steps that any organization should employ:

- Regularly update and patch all computer systems and business applications;
- Grant users the minimum access required to perform assigned duties;
- Conduct user awareness training campaigns on a continuous basis;
- Conduct annual threat risk assessments such as phishing campaigns;
- Develop an Incident Response Plan to deal with cyber attack related business disruptions;
- Develop a data back up and restoration strategy. For example, onsite and offsite backups occurring on a daily, weekly and monthly basis;
- Implement intrusion detection and prevention technologies; and
- Implement a security system that requires more than one form of verification when a user remotely accesses the organization's network. For example, a password and a randomly generated code.

Being adequately prepared for sophisticated attacks with the emergence of digitization is going to require ongoing financial support for IT security products and services. From a global standpoint, it is predicted that spending on cybersecurity will exceed $6 trillion annually by 2021, an increase from $3 trillion in 2015.[7] Support by senior leadership is also pivotal to facilitate and promote the changes that may be required throughout an organization to enhance its security posture.

WDGPH Security Posture

WDGPH takes cybersecurity very seriously. The organization employs a defense in depth cybersecurity strategy across all technological platforms, that is, securing the perimeter of the organization down to training end users to detect anomalies. Also, WDGPH uses an industry standard zero-day anti-virus solution and an adaptive security appliance to help protect the network and end users from viruses and malware. To further ensure that the agency is aligned with recent advancements in cyber threats, an annual threat risk assessment is performed by an external consultant. Using the results of this assessment, recommended strategies are implemented to better mitigate any risks. Furthermore, a revamp of all IT policies and procedures was recently conducted according to industry best practices. WDGPH has an incident response plan - risks, consequences, and the impact associated with a cyber attack identified in the organizations risk register along with risk control and mitigation tactics.

In securing the digital realm, people, process, and technology are the key drivers aligned with the vision of the organization's cybersecurity strategy. Improvements to user awareness campaigns, implementation of next-generation technologies with the use of artificial intelligence and auditing are all on the multi-year IT operational plan to further improve the security posture of the organization.

Conclusion

Cyber risk is here to stay. Organizations need to continuously adapt to the changing environment to combat the evolution of threats. Moving forward, the focus on managing the risks associated with cybersecurity will be key for any organization. It is also important to recognize that although risk

mitigation strategies are intended to reduce the probability and impact of an attack, all organizations are susceptible. WDGPH will continue to treat cyber threats as a critical risk to the organization and ensure that effective measures are instituted to remain secure in this digitally changing landscape.

REFERENCES:

1. The Cost of Cybercrime [Internet]. 2019. [cited 2019 May 24] Available from: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf
2. Cyber risk and risk management [Internet].2019. [cited 2019 May 24] Available from: https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/
3. Social engineering [Internet]. 2019. [cited 2019 May 24] Available from: https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html
4. Dobran B. Ransomware statistics [Internet]. 2019. [cited 2019 May 24] Available from: https://phoenixnap.com/blog/ransomware-statistics-facts
5. Healthcare data breach costs [Internet]. 2018. [cited 2019 May 24] Available from: https://www.hcinnovationgroup.com/cybersecurity/news/13030528/healthcare-data-breach-costs-remain-highest-at-408-per-record
6. Healthcare Cybersecurity Report. [Internet]. 2019. [cited 2019 May 24] Available from: https://www.herjavecgroup.com/2019-healthcare-cybersecurity-report/
7. Annual Cybercrime Report. [Internet]. 2019. [cited 2019 May 24] Available from: https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/
8. Canada a prime target for cybersecurity attacks [Internet]. 2019. [cited 2019 May 24] Available from: https://www.itworldcanada.com/article/canada-is-a-prime-target-for-cybersecurity-attacks-in-2019/414201
9. Data Breaches [Internet]. 2018. [cited 2019 May 24] Available from: https://cyber.gc.ca/en/guidance/data-breaches

APPENDICES:

NONE.

Original Signed Document on File

Prepared by:	Reviewed by:	Approved by:
Emerson Rajaram, Manager, Information Technology	Dr. Kyle Wilson, Director, Information Systems & Chief Privacy Officer	Dr. Nicola Mercer, Medical Officer of Health & CEO