DREW & NAPIER

DREWTECH SERIES

CHAPTER 5

Bringing hygiene online

— The MAS Notice on cyber hygiene

28 April 2020

LEGAL UPDATE

In this Update

The Monetary Authority of Singapore's Notice on Cyber Hygiene comes into effect 6 August 2020. Compliance is mandatory, and the goal of the notice is to push financial institutions to take adequate steps to protect themselves from the increasingly pervasive nature of cyberthreats.

This update looks into the six measures which the Notice requires a financial institution to put in place.

03
INTRODUCTION

04
SIX STEPS TO CYBER HYGIENE

07
CONCLUSION

INTRODUCTION

Hand washing has come back into vogue, though it probably should have never gone out in the first place. However, in the resurgence of awareness on physical hygiene, it remains equally important to ensure minimum appropriate cyberhygiene as a daily part of your life.

The Monetary Authority of Singapore's Notice on Cyber Hygiene ("**Notice**") comes into effect 6 August 2020. Compliance is mandatory, and the goal of the notice is to push financial institutions to take adequate steps to protect themselves from the increasingly pervasive nature of cyberthreats.

While the notice applies to regulated financial institutions, it is also useful as broad level guidance for any organisation on important steps that can be taken to secure your systems.

Unfortunately, there is no such thing as computer sanitizer that you can lather on multiple times a day to rid your systems of malware. This means that if you are a risk manager or in-house counsel at your organisation, you should take steps to understand your organisation's cybersecurity profile and ask yourself if you have taken reasonably practicable steps to secure yourself. The question is: what is "reasonably practicable"?

"Reasonably practicable" has been defined as being something less than "physically possible". Generally, not every measure that can be taken must be taken. Instead, the quantum of risk must be weighed against the sacrifice involved in the measures necessary for averting the risk, whether in money, time, or trouble of implementation. These measures must be taken where the risk is not insignificant in relation to the sacrifice. Put another way, a particular measure, such as the implementation of a specific firewall policy, need not be taken if the expense of implementing such a policy is disproportionately large compared to the risk of not implementing it. This weighing of risk is done before an incident occurs and not after, since hindsight is 20/20.

There are numerous risks to consider when we think about how "cyberhygienic" we need to be. These include the prevalence of malicious actors currently seeking to subvert security systems, the target profile of the financial institution, and the sensitivity of the data that is at risk. On the other side of the weighing scale, organisations have to consider the cost and inconvenience of implementing such measures. While there may be exceptional circumstances, given the significantly increased dependency on information technology and the ever increasing threat environment, it is likely that the cost of implementing controls are usually far outweighed by the risks of not doing so.

SIX STEPS TO CYBER HYGIENE

The Notice provides for six measures which must be put in place:

(a) Securing the use of every administrative account to prevent unauthorized access.

(b) Addressing system vulnerabilities in a timely manner, by applying relevant security patches where available and instituting controls where they are not.

(c) Establishing a set of written security standards and ensuring compliance with the same.

(d) Implementing controls at the network perimeter.

(e) Implementing malware protection.

(f) Implementing multi-factor authentication for critical systems as well as systems used to access customer information.

A. Securing administrative accounts

An administrative account is a user account that has full privileges and unrestricted access to the system. It holds the metaphorical keys to the kingdom, being able to not only access and edit any information on almost all aspects of your organisation's system, but also modify the rights of other users.

Administrator accounts should as a matter of course be guarded jealously. While the obvious concern is misuse by a disgruntled employee, the threats are multifarious. Every administrator account is a target for hackers and cybercriminals because hacking into one opens a conduit of unlimited access to the institution.

Even without the concern of malicious misuse of administrator privileges, there is always the concern of accidental use. The more administrator accounts there are, the greater the possibility of a careless mistake by a mid-level systems technician propagating a faulty build across the entire institution, breaking it for everyone.

Just as keys to physical premises would not be given out to any employee without first ensuring that they can be trusted, administrator access should only be given to those who require it to go about their daily activities, which in all likelihood would be the organisation's head of information technology.

B. Applying security patches

A security patch is akin to a seasonal flu shot. It updates the system against new vulnerabilities, preventing opportunistic attackers from exploiting flaws in the system which were not discovered when first installed. As more exploits are discovered, more security patches must be applied. This is not a once-off fire-and-forget remedy, but one requiring constant vigilance.

Yet, just as a vaccine may not be available immediately, security patches may also not always be available. The Notice requires that institutions take steps to reduce any risk posed by such vulnerability where patches are not available. This can take the form of shifting critical information off an affected system for which no patch is available.

Depending on the severity of the vulnerability and the sensitivity or criticality of the information, one such step is “air-gapping” the device, the social distancing measure for computers. This involves removing the system from any network whatsoever, both wired and wireless. The only way to get information off the isolated system is therefore by using removable media such as jump drives. While even this will not protect against the most esoteric and modern threats, it will help in reducing the risk.

C. Establishing a written set of security standards and ensuring compliance

In the same way clear instructions have been lauded as being essential in controlling the spread of public health threats, a written set of security standards is essential to ensure a clear understanding of the security standards throughout the organisation. At the same time, for this to be effective, steps must be put in place to ensure compliance.

D. Implementing controls at the network perimeter

Any financial institution must have access to the internet. Clients wish to access their data, and employees working offsite must be able to connect to their workstations if any work is to be done. Yet, the internet, while useful, is rife with threats. The same pathway that grants an authorised employee access to essential data for their work can be subverted by a malicious actor on the internet to gain the same access to the system.

Border controls for networked systems are therefore just as important as those for humans. A network perimeter defence serves the role of reducing or altogether preventing external threats from gaining a foothold in an institution’s system, thereby maintaining the integrity of the system. While they do so in a variety of ways, at the highest level of abstraction, a

network perimeter defence monitors incoming and outgoing traffic at the border between the institution's system and the outside world. Traffic with the appropriate passphrases and identifiers that mark the source as trusted is let through, and traffic to and from suspicious sites is refused.

E. Malware protection

In the event that something does get into the system, the next level of defence is malware protection. This is the immune system of cybersecurity, ensuring that any worms, Trojan horses, or any of the multitude of security threats are deleted from the institution's systems. However, these malware protection systems must be updated at regular intervals to remain effective, and may not offer protection against all hostile attempts to subvert a security system. It is therefore essential, but cannot be the only line of defence.

F. Multi-factor authentication

Multi-factor authentication has been around for some time, and refers to the use of two or more factors to verify an account holder's identity. One factor is traditionally the password. However, the strength of a password is often suspect: passwords which are hard to guess and hack are equally hard to remember.

Institutions should consider implementing modern forms of multi-factor authentication, such as a time-based authenticator app or a physical token which can be plugged into a workstation. There are numerous such commercial solutions, which have been tested and are compatible with most modern systems.

The strength of multi-factor authentication is that it makes it much harder for a would-be attacker to gain access to an account. Not only must she obtain the password to the account, she must also successfully intercept the second method of authenticating identity.

In recognition that such a system may take some time to implement, however, MAS has granted a concession for a period of six months, till 5 February 2021, if the financial institution has:

(a) Conducted a risk assessment to identify the risks posed by non-compliance in implementing multi-factor authentication.

(b) Implemented controls to reduce the risks identified.

(c) Appointed a committee or member of the senior management who has agreed with the risk management and approves the implemented controls being sufficient to reduce the risks.

CONCLUSION

KEYPOINT

Cyberhygiene is no less important that physical hygiene. With so much of our lives now online, the risks of a cyberattack or ransomware event can have drastic effects on our lives.

Quite apart from the fact that compliance with the Notice is mandatory for regulated financial institutions, all organisations would be well advised to implement these elements of cyberhygiene, in the interest of protecting essential and critical systems, as well as customer information.

Remember to wash your hands, not your computers.

UPDATES IN DREWTECH SERIES

1. Chapter 1: The Importance of an Exit Strategy in Technology Contracts <6 March 2019>
2. Chapter 2: Employees, Technology and A Legal Hangover – Bring Your Own Problems? <4 June 2019>
3. Chapter 3: I host, you post, I get sued? <24 September 2019>
4. Chapter 4: Diabolus ex machina <18 February 2020>
5. Chapter 5: Bringing hygiene online – the MAS notice on cyber hygiene <28 April 2020>

The content of this article does not constitute legal advice and should not be relied on as such. Specific advice should be sought about your specific circumstances. Copyright in this publication is owned by Drew & Napier LLC. This publication may not be reproduced or transmitted in any form or by any means, in whole or in part, without prior written approval.

For questions or comments, please contact:

Rakesh Kirpalani
Director, Dispute Resolution &
Information Technology
Chief Technology Officer
T: +65 6531 2521
E: rakesh.kirpalani@drewnapier.com

Timothy Oen
Associate, Dispute Resolution &
Information Technology
E: timothy.oen@drewnapier.com

Drew & Napier LLC

10 Collyer Quay
#10-01 Ocean Financial Centre
Singapore 049315

www.drewnapier.com

T : +65 6535 0733
T : +65 9726 0573 (After Hours)
E : mail@drewnapier.com

DREW & NAPIER