Cyber Liability

10 quick wins to reduce your cyber risk

1. Keep software and hardware up to date

There are many free tools that conduct vulnerability scans of your network, both internal and external, to identify any existing vulnerabilities, whether on a server, operating system or application in use. According to Verizon's 2020 Data Breach Investigations Report, the exploitation of unpatched vulnerabilities was the second most common breach cause. Vulnerability scanning tools, like OpenVAS, are easy to use, free, and can identify vulnerabilities that should be remediated to avoid such common breaches.

2. Implement Multi-Factor Authentication

Multi-factor authentication is an essential security control for any organization. However, if there are constraints on rolling out MFA to all users, at a minimum, organizations should enforce it for access to administrator accounts. This means that when a threat actor gains a foothold in a network, they won't be able to laterally compromise the administrator account using tools like Mimikatz and other credential stealing malware.

3. Manage use of remote services

In 2020 the FBI published a warning regarding vulnerabilities related to Remote Desktop Protocol as it remains the primary entry point for hackers. We recommend disabling or removing remote services wherever possible. Do not allow remote access directly from the internet and instead require access via VPN, again, with MFA enforced. Ensure that separate credentials are used for remote access to users' devices and whitelist IP addresses that are allowed to connect via RDP.

4. Perform phishing training

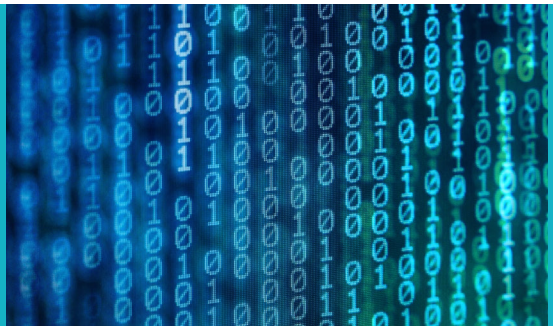
Many successful cyber security incidents still rely on human error. As such, basic user security awareness training focused on the threat of phishing can significantly reduce cyber risk. Free phishing training can be found online and is generally simple to use. This training should be repeated at least quarterly to ensure users remain aware of the threat.

5. Use a password manager

Passwords are the first – and often only – layer of defense for systems and applications. Due to the ever-increasing number of applications and accounts employees use for professional and personal use, many employees re-use weak passwords across different accounts so that they can remember them all. When passwords are compromised, this endangers all accounts that share the compromised password. A password manager overcomes these issues by issuing and securely saving unique passwords for all accounts, only requiring the employee to remember one strong password to access the password manager, instead of dozens of weak passwords.

2nd

The exploitation of unpatched vulnerabilities was the second most common breach cause[1]



280

Data breaches take an average of 280 days to detect and contain[2]

6. Backup your data securely

To respond effectively to a wide range of different cyber attacks, an organization needs to ensure it has recent backups. Hackers, particularly in ransomware incidents, target backups, by either deleting or encrypting them so that they cannot be used to restore data. As such, it is crucial to keep backup data off of the corporate network. Cloud backups with versioning are a good option, especially for small and mediums sized organizations.

7. Separate professional and personal account usage

Many organizations lack visibility for the applications in use on their devices, particularly when their employees are working from home. It is important to ensure that employees are aware that they are prohibited from using personal accounts for operational reasons. This provides a virtual firewall between an individual's professional and personal cyber risk.

8. Block macro-embedded email attachments

One of the most common ways a threat actor will gain access to a network is through a phishing email containing a malicious attachment. Once opened, the attachment's payload exploits a vulnerability or directly executes on the user's system. Use restrictions such as blocking emails with macro-embedded attachments (.docm, .xlsm, etc.) unless absolutely necessary for business purposes.

9. Enable logging and increase log retention

One of the most important aspects of incident investigation and response is an examination of the relevant server / device / application logs that serve as evidence during an incident investigation. Many organizations have not enabled logging or have a retention period so short that it will not be useful for investigation. IBM's 2020 Cost of a Data Breach Report states that data breaches take an average of 280 days to detect and contain.

10. Check for involvement in data breaches

One quick method of checking whether employees have been involved in previous data breaches is to run their enterprise email address through HaveIBeenPwned. This allows users to check whether their email address has been involved in any data breaches that have been uploaded to the platform. If any users have been involved in a data breach, they should immediately change the password to the affected account and any other accounts that use the compromised password. This risk emphasizes the importance of not reusing passwords across multiple accounts.

1. According to Verizon's 2020 Data Breach Investigations Report
2 According to IBM's 2020 Cost of Data Breach Report

To learn more, contact your AXA XL Cyber underwriter.

S-RM is a global consultancy that helps clients manage regulatory, reputational and operational risks.

6590_09/2020