cowbell®

Recommendations to Prepare a Cyber Insurance Application

The Leading Cyber Insurance for SMEs | cowbell.insure

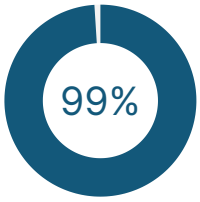
V.JUN22

No business - large or small - is immune to cyber incidents. Cybercriminals deploy cyberattacks at scale, targeting thousands of small organizations with tools looking for cybersecurity weaknesses, such as lack of encryption, weak passwords, or employees who click on a phishing email. Such weaknesses fall into the category of basic cybersecurity hygiene which always needs to be maintained.

The recommendations below help minimize an organization's exposure to cyber threats, speed the recovery process in case of a cyber event, improve insurability, accelerate the insurance application process, and optimize insurance premium.

① Multi-factor authentication (MFA) - Why it is important?

When MFA is enabled on an account, cybercriminals can't access the account even if they have stolen the account credentials (username and password) because MFA requires one or several additional factors (secrets) generated dynamically that only the account owner has.



Experts from Microsoft, Google, and elsewhere suggest that users who (MFA) for their accounts end up blocking 99.9% of automated aka bot attacks.

What to Do

1. Enforce MFA for all users on email, cloud applications, and for remote access.
2. Preference to be given to authentication apps (examples: Google Authenticator or Duo Security) over SMS/text messaging, since phones are vulnerable to SIM swapping, fake SIM recovery messages, and other unauthenticated SIM attacks.

MFA is easy to deploy and effective against many forms of attacks operated at scale against SMEs. MFA is available out-of-the-box for free with most systems along with central enforcement. If you have more than 50 employees and need to deploy MFA at scale on many systems, contact us at support@cowbellcyber.ai and we will put you in touch with relevant partners.

Note: Everybody should activate MFA on all personal accounts (online banking, email,...) in addition to professional accounts.

② Cybersecurity Awareness Training - Train employees to recognize malicious (Phishing) emails

Phishing emails trick the receiver into clicking on a malicious link, allowing the cybercriminals to install malware on systems. Phishing emails are often the first point of intrusion for ransomware attacks.

One bad click on a phishing email can lead to weeks of business interruption and a multi-million dollar ransom demand!

Phishing emails always look legitimate or coming from a person of authority to entice the receiver to overlook basic email validation: Is the “from” email valid, Is the URL/link provided correct? Training teaches employees how to quickly check the validity of an email.

What to Do

1. Cowbell’s policies include 20 seats in Wizer’s Cybersecurity Awareness Training Program.
2. If you don't have a security training program in place, we will require that you deploy one for renewal.

③ Have an Incident Response Plan in place and tested

Cyber incidents are times of crisis for any organization and preparation is paramount. An incident response plan documents step by step what to do, whom to contact, and who should be involved. An Incident Response Plan is a living document that should be tested and updated on a regular basis as the organization evolves, new systems get deployed, and new risk resources come into play.

To help policyholders, Cowbell has published a recommended Incident Response Plan.

Download Your Copy →

④ Isolated, Offline Backups

The worst-case scenario is, of course, when an organization has to face a cyber event such as a ransomware attack. Having readily available backups gives options to negotiate with criminals if needed including recovering data and systems without having to pay the ransom.

Backups should be in place on all critical data and systems that are deployed and managed in-house. Businesses that depend on third-party systems to run their operations should systematically check with those about their backup procedures. It is recommended to opt-in for backup options available from all system providers.

Backups should be isolated from the internet and other systems, fully encrypted, and MFA should be enabled for all accounts having access to backups.

⑤ Other Recommendations

Depending on the industry, size of business, and historical information, Cowbell's underwriting team might request additional information or require other controls to be in place such as:

- Annual penetration testing.
- Deployment of Managed Detection and Response, Endpoint Detection and Response (EDR) and Intrusion Detection System.

Resources

1. Cowbell's risk engineering team (riskengineering@cowbellcyber.ai) is available to address further questions on the above.
2. Every business can get access to their Cowbell Factors to gain visibility into their risk exposures.

Get Your Cowbell Factors →