cowbell®

Cybersecurity Resource Guide

The Leading Cyber Insurance for SMEs | cowbell.insure

V.MAR23

2023 Cybersecurity Resource Guide

Introduction

Cyberattacks are a growing threat to small and medium-sized enterprises (SMEs) as bad actors view SMEs as easy targets. According to a recent survey, 88% of small business owners feel vulnerable to a cyber incident. This is mainly driven by the lack of resources in-house, as many of these businesses cannot afford professional IT solutions, have limited time to devote to cybersecurity, or simply don't know where to begin.

As a cyber insurance provider dedicated to SMEs, Cowbell is looking to close the gap for SMEs through our AI-powered continuous assessment of individual cyber risk. Cowbell's assessment is broad and deep in evaluating individual risk, using thousands of data points. The data consists of outside-in observations and inside-out risk information collected through partnerships with major infrastructure platforms and security vendors. AI gives us the computing power to compile Cowbell Factors, our proprietary risk ratings, in real-time and to continuously update these ratings as our platform incorporates new data.

Cowbell developed this guide for SMEs who need cybersecurity best practices that are easily implementable and effective immediately in protecting their infrastructure and data. The frequency of cyberattacks aimed at small businesses has increased, as 47% of SMEs had at least one cyber incident in the past year, but only 14% are prepared to defend themselves. At Cowbell, we have a skilled team of risk engineers ready to assist and discuss mitigation techniques to help reduce the likelihood of cyberattacks on your organization.

The best practices provided in this report are intended to bolster your cybersecurity posture; however, that does not eliminate the possibility of being a victim of a cyber incident. As a policyholder, if you're interested in sitting down with our risk engineering department for a deeper assessment of your environment, please reach out using this link and submit a request.

cowbell®

Table of Contents

Version 2 | Modified 05.12.23 | Approved 03.3.23

Enable Multi-Factor Authentication (MFA)

Having a strong password simply isn't enough nowadays. In recent years, threats to password security have heightened, which is why MFA adoption has grown substantially to strengthen account security. According to Microsoft, implementing MFA can "prevent 99.9% of attacks on your accounts". There are three main types of factors utilized, each entailing different authentication methods.

1. **Knowledge** – something you know
    a. Username and password or PIN are the most common examples. Sometimes organizations require security questions (e.g., pets name or first car).

2. **Possession** – something you have
    a. Physical tokens, smart cards, or mobile phones are common examples. Google Authenticator is a good example of an app on the phone as a token.

3. **Inherence** – something you are
    a. Fingerprints, voice, or facial recognition are common examples.

Difference between 2FA and MFA

- **2FA** - exactly two factors are used for the authentication process.
- **MFA** – two or more authentication factors are used to verify the user.

Recommendations

MFA through SMS (text messages) is generally the most common method as nearly everyone has access to a cell phone in today's world. However, it's not the most secure as it is vulnerable to spoofing/phishing, SIM swapping, RDP, and social engineering. While NIST recommends against using SMS for the above reasons, some form of MFA is better than nothing. Other options include authenticator apps and tokens.

We recommend using MFA on all mission-critical systems, email, remote access, and admin-level users.

How to Implement MFA

- **Google** – Personal and G Suite Admin
- **Microsoft 365** – All Users
- Popular Cloud Apps such as Zoom, Skype, Slack, Expensify, Square, Jira, and WordPress can be found here.

Cowbell Rx

- We have a list of authentication solutions on Cowbell Rx, and as a Cowbell policyholder, you may be eligible for a free consultation, preferred pricing, and other discounts. To name a few popular vendors, we recommend Okta and NordPass.

Enforce a robust password policy

What is a password policy?

A password policy consists of rules established to strengthen computer and network security. For example, many policies require a minimum length of at least ten characters, with a combination of upper- and lower-case letters, numbers, and symbols or special characters. In addition, reset requirements define how often you must change your password. We recommend doing it regularly (i.e., semi-annually). Lastly, passwords need to be unique. Avoid reusing passwords across accounts.

Consider using a password manager

Memorizing a unique, complex password for multiple platforms or systems can be a challenging and nearly an impossible task. However, a password manager can help solve that issue. A password manager software utility helps you securely store passwords and auto-fills into login pages. They assist in safeguarding every single online account you may have with a strong and unique password.

A Google study discovered 52% of people use the same password across multiple accounts.

Having a different password for each account will mitigate the domino effect of each account being compromised if a third party experiences a cyber incident.

Recommendations

Even with a strong password policy or a password manager, we have seen hackers increase their level of sophistication to steal our password credentials. Some of the methods they use are brute force attacks and phishing attempts. Therefore, we recommend pairing strong password policies with MFA to bolster your security. Lastly, Cowbell has developed a Password Policy, which covers recommended password length, complexity, and additional guidelines. Get a copy here - Cowbell Password Policy Guidelines.

Cowbell Rx

We may sound like a broken record, but if you're looking for a password manager provider, we have already done some of the legwork for you. Visit Cowbell Rx to see some of our preferred vendors, such as NordPass.

Create an Acceptable Use Policy

An Acceptable Use Policy (AUP), also known as a fair use policy, is a set of rules that outlines what employees can and can't do while utilizing the organization's internet access, network, data, or a specific piece of technology. In addition, the AUP will also cover the consequences of infringing the policy rules. See some examples below:

- Do - report any theft, loss, or authorized disclosure of confidential or proprietary information of the company.
- Don't - reveal an account password or passphrase to others and allow them to use your account.

Reasons to implement an AUP

An acceptable use can be the foundation of a more extensive IT policy; it helps employees have a clear understanding of data and technology usage. One of the benefits of implementing an AUP is that it can be proof of "due diligence" and protect the organization from reputational harm. This "due diligence" is essential

for organizations that have compliance requirements like HIPAA, PCI, GDPR, and others. It also helps communicate that cybersecurity is the responsibility of all employees, not just the IT department or other technical roles. An AUP combined with employee awareness training is part of building a good culture of cybersecurity.

What is Cowbell doing for the Acceptable Password Use Policy?

If your organization does not have an AUP or is having difficulty creating one, Cowbell offers a free AUP template to jumpstart the process. The template is completely customizable to meet your organization's needs. It is crucial to carefully evaluate the template to make sure it addresses all the necessary topics, eliminating any that are unnecessary or unenforced. After the policy is created, it is crucial to emphasize to employees its importance and establish procedures to enforce it. The policy should be reviewed frequently, preferably once a year, to ensure it still applies to the organization's evolving use of technology.

- Cowbell Acceptable Use Policy Template

Embrace cybersecurity awareness training and education

Employees are generally the first line of defense in preventing a cyber incident. A study conducted by Stanford University and security firm Tessian concluded that 9 out of 10 (88%) data breaches result from employee mistakes. With the frequency of cyberattacks rising along with their level of sophistication, it's imperative to embrace cybersecurity awareness training and education at your organization.

A well-trained organization in cybersecurity will reduce the risk to your organization's network. Fewer risks mean less financial loss due to cybercrime. A modest investment in security awareness training for all users (approximately $28k) has a 72% likelihood of significantly reducing negative business impact.

What does Cowbell offer?

At Cowbell, we have partnered with a leading cybersecurity awareness training provider, Wizer, which offers a library of 100+ microlearning videos that cover various and relevant security topics. You can deploy phishing simulation campaigns and collect trackable data to see how well your employees are doing and many other features.

For policyholders, we provide complimentary seats with preferred pricing beyond that limited seat amount. Instructions on how to get started can be found here.

For more information, download Wizer's document on how to build a cybersecurity awareness program.

Adopt good email hygiene

According to industry data, 77% of organizations faced business email compromise (BEC) attacks in 2021, which resulted in $2.4 billion in losses. This is an alarming metric as BEC continues to be the most common digital crime. This makes it even more important to adopt good email hygiene. We use email daily as it has become a major form of communication in our lives, and threat actors are well aware of that. They are actively exploiting this avenue with clever social engineering tactics to get individuals to provide credentials and transfer funds.

Recommendations

- Be cautious of all external emails and proceed with caution when receiving emails that request you to click or open attachments. If from an unfamiliar sender, it is better not to click or open any attachments and instead notify your IT or security personnel.
- Train employees to recognize BEC attacks. Provide employees with adequate cybersecurity training (see pg. 6 for more information).
- Look carefully at the email address. Threat actors use domains that look legitimate to trick employees. Therefore, it is crucial to confirm the exact spelling of the sender's name and company. Below is an example of typo-squatting. This is when the bad actor will present an address bar that

looks very similar to get a few people to provide emails and their passwords. See the example below.

    - **Legitimate** – Amazon.com
    - **Not legitimate** – Amazom.com

- Review emails carefully that request payments, use urgent language (i.e., “Final Notice”), or lack phone numbers for callback purposes. Also, emails with grammatical errors are big red flags.
- Conduct a callback to the person or organization making a request from a phone number you have on file or directly from their website. Especially when the request entails payment, changes in payment information, or contact information.

What to do if you’ve fallen victim

Quickly notify your bank and report the crime to the FBI's Internet Crime Complaint Center, local law enforcement, and your insurance provider.

Protect your email

Did you know that 90% of all cyberattacks begin with a phishing email? Therefore, your organization needs to implement security measures for email. Organizations can apply three common and free email authentication measures to its infrastructure. Please contact your IT team to confirm if these measures are already active. If not, we’ve provided helpful links below to activate. If you are a small business owner or unfamiliar with IP addresses or DNS configuration, consider contacting your internet domain registrar (e.g., GoDaddy, Bluehost, Domain.com.).

Sender Policy Framework (SPF)

SPF helps authenticate and allows the sender to specify which IP addresses are authorized to send emails on behalf of a particular domain. It also ensures that legitimate email from the domain is delivered. An SPF-protected domain is a good deterrent against bad actors.

- Enable SPF for MS 365
- Enable SPF for Google GSuite

DomainKeys Identified Mail (DKIM)

DKIM is another tool for email authentication that can help protect your organization from attackers from sending content/messages that appear to come from your domain. When enabled, DKIM ensures that emails received from a domain were not modified in transit.

- Enable DKIM for MS 365
- Enable DKIM for Google GSuite

Domain-based Message Authentication, Reporting & Conformance (DMARC)

DMARC works with the previous authentication protocols – SPF and DKIM, to verify mail senders and ensure that the destination email systems trust messages sent to your domain. Implementation of these measures provides additional layers of protection against spoofing and phishing emails. DMARC provides instructions on what to do with messages sent from your domain that fail SPF and DKIM inspection.

- Enable DMARC for MS 365
- Enable DMARC for Google GSuite

Establish patch management on software and hardware

Software and hardware updates are important for your digital safety and cybersecurity. Hackers love to exploit vulnerabilities to gain access to sensitive data or install malicious malware for a quick payday. Therefore, it's imperative to patch operating systems for your server and endpoint devices promptly. In addition to internal system updates, patches for external vendor products that are utilized in your environment should be updated as well.

Organizations should also be aware that software is exposed to the internet, such as web applications, mail servers, cloud applications, and web servers,. presents a greater risk as hackers are constantly scanning the internet for exploits. Thankfully, Cowbell Insights on Cowbell's platform provide helpful guidance to policyholders to improve their risk profile by offering recommendations to address identified security weaknesses on your internet-facing systems. In addition, when Cowbell Connectors are activated, Cowbell Insights deliver even more value by pulling recommendations and guidance when available from the connected infrastructure.

For example, with an activated Microsoft Connector, you can visualize Microsoft's recommendations to address specific security weaknesses in your Microsoft 365 (Office 365) environment.

Best practices for software updates

- Take inventory of the software and hardware within your environment. This will provide clear insight into what software and hardware you are using. Once completed, you can track vulnerabilities and discover patches that apply to your systems.
- Take a small subset of your systems and apply the patch or update to ensure no issues since every environment is unique. Once verified, roll out to the entire organization.
- Develop a patch management policy outlining what should be patched, when, and in what situations. Identify which systems need more attention within the policy.
- Apply patches quickly, as slow patch management to software leaves you vulnerable.
- Adopt automation where you can increase efficiency. If you cannot establish a patch management system internally, partner with a vendor to assist. Visit Cowbell Rx for potential vendors. It's important for the security of your business.

cowbell®

Implement a strong backup strategy

Data is a critical asset to every organization regardless of size. Having secure and reliable backups for data protection allows your business to reduce business disruptions or recover quickly from malicious attacks, such as ransomware.

Having a backup plan can help secure your sensitive data and systems. Consider implementing these backup best practices:

- Take data backup processes seriously and develop a plan aligning with your organization's objectives. Backing up data should be an ongoing practice.
- House more than one data backup. Consider the 3-2-1 backup strategy, which entails having three copies of your data, two media types for your backups, and one backup stored in an offsite location.
- Limit access to backups. This is called “least privilege access.” If a bad actor gains access to someone's credentials, they will only be able to impact areas to which they have access. As a result, the least privilege access limits insider threats, especially when combined with encrypted backups.
- Test your backups regularly (more than once or twice a year). Just because you have a backup, it doesn’t necessarily mean the data can be restored successfully. Therefore, backups should be tested frequently, including on-premise and off-premise backups. A 90%+ restoration should be the goal.
- Use an “air gap backup solution” strategy. This strategy simply entails storing backups in a different area that is offline and separate. This makes it difficult for ransomware hackers to intercept, gain access and interfere with it. Common methods today include cloud-based destinations.

Secure Network Infrastructure

As operational technology becomes increasingly connected to the internet; it’s becoming more evident that organizations should pay extra attention and strengthen the security around OT systems. The impacts of a cyber incident on

OT systems can be severe from a financial and operational standpoint, which could lead to a plethora of other impacts. For example, some high-profile security events impacting OT systems, including ransomware attacks, disrupted supplies of oil and meat in North America last year. In addition, the further spotlight was shined on OT security due to the Russia-Ukraine situation as CISA advised organizations of all sizes will be at risk and targeted by cyber-attacks meant to halt business operations due to sanctions imposed by the U.S.

According to Fortinet, 93% of organizations had 1+ intrusions in the past year; 78% had 3+. From that, 61% of intrusions impacted OT systems, and 90% of intrusions required hours or longer to restore service. It's clear that OT security should be on the mind of every organization, especially in the following industries:

- Manufacturing
- Utilities (oil, gas, electricity, and water)
- Distribution
- Mining
- Transportation (aviation, rail, traffic, and light management)
- Telecommunications

If you'd like to learn more about OT security and best practices to implement, please review our recent blog post on the subject here.

Develop an Incident Response Plan (IRP)

When your organization's reputation, revenue, data, and customer confidence is at stake, it's necessary to have a detailed incident response plan (IRP) in place. The goal of the IRP is to identify security incidents, get the situation under control, reduce the impacts caused by the threat actor and limit the time and costs of recovery.

How to build an Incident Response Plan

While there isn't a one-size-fits-all IRP, there are important frameworks each plan should entail as outlined by leading agencies such as the National Institute of Standard and Technology (NIST), Cybersecurity and Infrastructure Security Agency (CISA) and International Organization for Standardization (ISO).

The framework should cover the entire process, which includes preparation, detection, analysis, containment, and post-incident analysis. Learn more by reviewing the NIST Computer Security Incident Handling Guide.

What is Cowbell doing for Incident Response Plans?

If your organization has an IRP, consider sending it to Cowbell for review. Our dedicated risk engineers will evaluate your plan in detail and provide recommendations where needed. If you do not have an IRP or are having difficulty creating one, Cowbell has developed an IRP template that is free to use to jumpstart that process.

- Incident Response Plan Template

Recommendations

Having an IRP is a great first step, but if it fails to provide a suitable response to a threat, then it becomes worthless. Therefore, you should regularly test your IRP. It's better to prepare for a never-occurring threat than to find out that you are unprepared when one does. Conduct tabletop exercises in-house to prepare for potential scenarios that could occur, such as ransomware and phishing. These exercises will be valuable learning experiences better to prepare your organization for an efficient response to threats. In addition, it may allow you to identify areas of improvement. CISA has compiled Tabletop scenarios/exercises that you can use to conduct with your organization.

Business Continuity / Disaster Recovery Plan (BCDR)

What is a Business Continuity/Disaster Recovery (BCDR), and why is it important?

The Business Continuity/Disaster Recovery (BCDR) is a set of procedures to be carried out in the event of a disaster affecting the operations of your organization. It should provide guidance and support throughout all stages of a disaster, including disaster assessment, recovery, crisis management, BCP invocation, and

operation. It's important to note while BC and DR complement each other, they are different in their functionality and purpose. BC focuses on company-wide strategic planning, and disaster recovery is mainly IT-focused. Both are fundamental facets of an organization's overall risk management strategy and need to coexist to assist in alleviating the business impact of a potential disaster. According to some studies, three-quarters of small businesses do not have a disaster recovery plan in place, and 93% of businesses without Disaster Recovery who suffered a major data disaster were out of business within one year. Therefore, it's crucial to have such a plan in place, and Cowbell is here to help.

What is Cowbell doing for BCDR plans?

If your organization has a BCDR plan, consider sending it to Cowbell for review. Our dedicated risk engineers will evaluate your plan in detail and provide recommendations where needed. If you need a BCDR plan or are having difficulty creating one, Cowbell has developed a BCDR template that is free to jumpstart the process.

- BCDR Plan Template

Recommendations

Maintenance and testing of the BCDR plan are vital as they will assess its effectiveness and highlight areas of the plan that need updating or revising to support business recovery for the organization. As an important reminder, BC and DR go hand in hand; therefore, the testing process should be done in conjunction with IT/Network staff. CISA has compiled natural disaster tabletop scenarios/exercises that you can use to conduct with your organization.

Beware of remote access protocol

Over the last few years, we've seen many organizations shift to remote work due to the COVID-19 pandemic. Most organizations using Windows machines rely on Remote Desktop Protocol (RDP), which allows employees to access their office workstations and applications from their homes. This may be something your organization does as well. RDP is riddled with security concerns and is a highly targeted attack vector. In fact, it is the second leading entry point for deploying

ransomware behind phishing. However, the market is noticing a decline in RDP usage as organizations are migrating to the cloud and utilizing VPN services instead.

Ways to secure remote access

- Ensure remote access is encrypted
- Enable an authentication method for remote access (see pg 4)
- Require strong passwords
- Employ the principle of least privilege access (see pg 10)
- Require use of company hardware. Company-issued hardware is more secure as it will be loaded with anti-virus, password policies, etc.

How is Cowbell reducing RDP exposure?

Once Cowbell scanners pick up on an organization utilizing an RDP port, it is flagged and referred to the risk engineering and underwriting departments to address the exposure. The risk engineering team will meet with the client to determine if their exposure is legitimate or if their environment is properly secured.

If RDP is essential for your organization, Cowbell will recommend or confirm that RDP is encrypted and MFA is enforced.

If RDP is exposed and not essential for your organization, Cowbell will recommend closing the port and turning off the RDP feature.

If the RDP port is encrypted and MFA is enabled, then Cowbell will require the organization's IT/Security team to provide details on how they are securing RDP.

Reasons to purchase cyber insurance

Cyberattacks are nearly inevitable. All organizations that use technology or collect data are at risk of a cyber incident, regardless of whether they have the best defenses. Mistakes happen, and 88% of cybersecurity breaches are caused by human error. Therefore, if the worst happens, you must ensure your organization is prepared to recover.

Cyber insurance can provide that sense of safety, and below is a list of benefits and reasons why it is crucial to purchase cyber insurance coverage from Cowbell.

1. **Mitigate financial loss from cyber incidents** – Coverage entails many expenses triggered by a cyber incident: forensics, legal, notification, etc.
2. **Recover quickly from a cyber incident** – Cyber insurance helps minimize disruption to your business by bringing expert services to help you.
3. **Fulfill your contractual obligations** - Get coverage when you have time to evaluate your needs. Don't wait until you are under pressure to close a contract.
4. **Get coverages aligned with your unique needs** – Every business uses technology differently. Cowbell matches your unique risk exposures to recommend coverage.
5. **100% online application. Get coverage in minutes!** – Ask your agent for a quote, review coverages, and get protected in under five minutes. Cowbell only needs a domain and organization name.
6. **Visualize and monitor your risk exposure** – Log in to Cowbell's platform, view your risk ratings, and how they evolve. Avoid coverage gaps.
7. **Is your business as secure as your peers? Get Insights** – Compare your Cowbell Factors™ to industry peers.
8. **Speed of response from Cowbell's claims professionals** – Time is critical to limit the damage, and our claims team provides 24/7/365 coverage.
9. **Security Gap reviews** – Our risk engineering team is available to provide a full security assessment of your security posture and identify any gaps.

cowbell®

To set up a meeting with the Risk Engineering team, click here.