Cybersecurity Precautions CEOs Need to Take Now to Avoid Lost Profit

7 min read

Key Takeaways

- **Shocking Cybersecurity Statistics** In 2020, 75% of organizations around the world were hit with at least one phishing attack.
- **How to Recognize a Cyberattack?** You and your employees need to understand what one looks like and the methods that are commonly used to access private information
- **Business Cybersecurity 101: Prevent Attacks With Cybersecurity Awareness Training:** The best way to strengthen the people in your organization against cyber threats is with regular cybersecurity training..

Every CEO's worst nightmare: your client's portal was **hacked**! Here's your next move...

Cybercrime continues to rise and become an increasingly significant threat. While the thought of a data breach on your own organization is nightmare-worthy, having your client's information leaked welcomes a new level of horror.

Luckily, there are precautions you can take to protect yourself and your clients from cybercrime.

Many business owners believe their companies are too small to be worth a cybercriminal's time and that they can get by simply flying under the radar.

Small and medium businesses (SMBs), however, are actually prime cybercrime targets specifically because the people running them don't believe they will be attacked.

Subsequently, many SMBs are underprepared, under-protected, undertrained, and completely vulnerable to cybersecurity threats. SMBs have fewer resources available for surviving losses, managing their reputation, and weathering a cybersecurity storm.

As a result, **60% of small businesses fail within six months of suffering a cyberattack** or data breach. [1]

Shocking Cybersecurity Statistics

- In 2020, 75% of organizations around the world were hit with at least one phishing attack [2].
- Cyber insurance claims for ransomware attacks grew by 260% in 2020 [3].
- Ransomware attacks impacted 40% of SMBs in 2020 [4].
- A 2019 study found that 34% of data breaches involved internal actors [5].
- Roughly 60% of people use the same password across accounts at home and at work [6].
- 47% of businesses experienced five or more attacks in 2020 [7].

- 94% of ransomware makes its way into a business's network via email [8].
- More than 80% of cybersecurity attacks are related to phishing [9].
- 65% of cybercriminals use spearphishing as their preferred attack method [10].

First things first- How to Recognize a Cyberattack?

To recognize a cyberattack, **you and your employees need to understand what one looks like and the methods that are commonly used to access private information**, infect a network with ransomware or malware, or to access the system in another way.

While email has always presented cybersecurity challenges to business owners, it has become an increasingly common point of entry for attackers. With the workplace changes brought about by the pandemic and more employees working remotely, our teams are further apart and we're getting used to communicating over email, instead of using the office phone system or simply talking in person.

Hackers use email to launch phishing and spearphishing campaigns which aim to leverage personal information (about an executive in your company, employee, client, or vendor) in order to trick the recipient (usually an employee) into revealing more personal information, clicking a malicious link, or downloading files containing malware or ransomware.

Sometimes these malicious emails come from outside of your network. Other times, email accounts get hacked and the emails then come from within the network.

For example, a remote employee's account could become compromised, allowing a hacker to then send a malicious email to all of that person's contacts (including clients, business contacts, and personal contacts). Those recipients might then open the email – it came from a trusted source, after all – click the links, visit a site designed to mimic one that's routinely used, and enter personal information. Or, perhaps, they might be tricked into downloading malicious ransomware onto the business's network. The hacker would then

have the personal information that was entered on the decoy website or would have successfully planted ransomware in the business's network.

Cyberattacks can also occur through email without anyone's account being compromised in the first place. Attackers can create email domains that appear legitimate or look like they belong to a coworker or manager and make requests for the person to send payments. Attackers can also pose as vendors, stating that their payment addresses have changed.

Unfortunately, cyberattacks are increasing exponentially because more people are falling for it and it's becoming simpler and cheaper for criminals to create fake domains and automate the phishing process. With increasingly dispersed remote workplaces and multiplying network access points, we've also become more vulnerable.

Cybersecurity threats will happen. Your business will be targeted. Your business will be the victim of a cybersecurity attack. It's necessary to accept that your business is vulnerable so that you can start taking action to protect your business now.

How to Protect Your Business From Cyberattacks

Shore up your physical network. Implement strong password security protocols and two-factor authentication. Additionally, your IT department should regularly pull your network's access logs and make note of any unusual activity so that you can immediately address it.

You should also ask any vendors you work with and third-party members of your supply chain about their security protocols. Only work with other companies that take cybersecurity seriously. This will help reduce cyberattacks that are supply chain and vendor-related.

In addition to shoring up virus protection, firewalls, and physical security, **it's of primary importance that you provide cybersecurity training to your employees because each and every person working inside your company represents a potential network entry point.** Employees need to be trained about the importance of remaining vigilant when it

comes to cybersecurity and they should be provided with the tools, knowledge, policies, and procedures they need to understand exactly how to be vigilant in an effective way.

Business Cybersecurity 101: Prevent Attacks With Cybersecurity Awareness Training

Yes, it's important to shore up your network and various network access points with firewalls, antivirus protection, and physical security in your office. (Also, don't forget about mobile phones and employees who are working from home.) However, it's also essential that business owners recognize that each and every person working in a business is a potential weak spot that cybercriminals can and will target.

Business owners must put not just the best IT security practices in place, but they also need to implement policies and procedures while creating rules for employees that create a culture of cybersecurity within the business. Employees should be educated and held accountable for helping to maintain the security of the business, your customers' personal information, and all of the business's digital assets.

The best way to strengthen the people in your organization against cyber threats is with regular cybersecurity training. Whether you hire an outside cybersecurity consultant or task your IT department with training your employees, do not overlook this very important step.

You need to teach your employees what they should be on the lookout for – especially when it comes to password security and social engineering threats like email hacks, phishing, and spear phishing. Schedule annual, biannual, or quarterly security meetings to update everyone on the latest threats and ensure cybersecurity is always at the top of everyone's mind.

In addition to providing training, **it's also smart to test your employees by routinely performing fake cybersecurity attacks** and then paying attention to how many people open the "malicious" email, click links, download files, respond, or divulge personal information. After the "cyberattack" has been performed, you can hold a meeting to

discuss the training event, the results, and provide additional training to address any weaknesses revealed by the test.

Additional security measures that can be taken with your personnel include:

- Creating and implementing security procedures around personally identifiable information (PII) like social security numbers, addresses, phone numbers, and email addresses. Be careful about where and how you list and store this information.
- Secure payment methods (sending and receiving) – do not accept payment changes or new information over email
- Implementing dual authentication for all business logins

Build a culture where employees feel safe reporting unusual incidents or mistakes they might have made regarding cybersecurity. The sooner an employee comes forward about accidentally downloading a file, clicking a link, or sharing personal information, the sooner you can begin the process of evaluating the risk, isolating the incident, and containing any potential damage or losses.

Remember That CEOs Are Vulnerable, Too

As a business leader, it's easy to get caught up in the daily rush of your work-life and responsibilities. As a result, many CEOs and other executives in the c-suite forget that they are primary cyberattack targets. One study revealed that 76% of CEOs admitted to forgoing cybersecurity protocols in the name of saving time, even though 84% also reported being the target of at least one cyber attack in the previous year [11].

Of course, your time is valuable, but so are the future and reputation of your business. Paying attention to cybersecurity, following your own security protocols, and investing your business's resources in cybersecurity protections and training will pay off dividends. Just remember it's no longer a question of if your business will be targeted, it's only a question of when.

Be Prepared- Profits Are On The Line!

Cybersecurity threats will happen. Your business will be targeted. Your business will be the victim of a cybersecurity attack. It's necessary to accept that your business is vulnerable so that you can start taking action to protect your business now.

Outsourcing your back office is a step in the right direction. There are no second chances when it comes down to the security of your financial data (and your clients!). It's essential to have someone dedicated to protecting your business's digital assets, monetary assets, data, personal information, and reputation from cybercriminals. (Plus... it saves you $$$ in the long run!)

---

[1] https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/

[2] https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

[3] https://securityintelligence.com/posts/ransomware-2020-attack-trends-new-techniques-affecting-organizations-worldwide/

[4] https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends//

[5] https://www.bitglass.com/blog/the-rise-of-insider-threats-in-verizons-dbir#:~:text=In%20Verizon's%202019%20report%2C%20the,has%20been%20increasing%20since%202015.

[6] https://securityboulevard.com/2018/05/59-of-people-use-the-same-password-everywhere-poll-finds/

[7] https://www.idagent.com/blog/was-the-2020-twitter-hack-caused-by-a-phished-password/

[8] https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html

[9] https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html

[10] https://www.varonis.com/blog/cybersecurity-statistics/

[11] https://www.forbes.com/sites/louiscolumbus/2020/05/29/cybersecuritys-greatest-insider-threat-is-in-the-c-suite/?sh=596e94cd7626