Major Failure in the C-Suite: CEOs Need to Take More Caution In Cybersecurity

6 min read

Key Takeaways

- Getting Serious In The C-Suite: 40% of IT leaders believe that, when it comes to cybersecurity, the CEOs of their companies are weak links.
- Be Aware of the Most Common Kinds of Cyber Attacks: The most common attacks that target high-level executives include spear phishing, whale phishing, email impersonation, business email compromise, account takeovers, and social media impersonations.
- Protect Every Network Entry Point: Securing network entry points has always posed a challenge to both IT and physical security professionals in the workplace.

Why is my business not making money? Why are we not able to grow? What are the problems holding us back?

$575 billion?!...

The cost of cybercrime on the global economy, according to a report from IBM, is between $375 billion to $575 billion US dollars annually in actual monetary losses, reputational damage, data leaks, and even national security expenses [1].

In the past, cybersecurity has largely been a technical issue left to the IT department. However, C-suite executives are beginning to recognize that cybersecurity is a concern that needs to be addressed operationally and strategically from the top down with safety measures starting at the leadership level.

Getting Serious About Cybersecurity in the C-Suite

CEOs rank cyber threats as the second most serious among all economic, social, political, business, and environmental threats, according to PwC's 24th Annual Global CEO Survey. This put cybersecurity as a top priority, ranking just slightly below addressing the threats posed by the pandemic and global health crisis [2].

PwC's survey makes it clear that business leaders are well aware of the risks posed by cybercriminals. However, IBM also reports that while 65% of C-suite executives say they are highly confident in their cybersecurity plans, only 17% demonstrate the highest degree of security and are truly secure.

Businesses at the global level (general network security) are not the sole target of cybercriminals. As it turns out, these criminals like to go for the big fish first, specifically targeting the CEOs, CFOs, COOs, CMOs, and everyone else operating at the executive level or on your board of directors.

A 2020 study from Vanson Bourne and MobileIron reported that 60% of IT leaders say C-suite executives are the number one target of cyberattacks.

Despite being painfully aware of the risks that technology poses, these top-tier employees, unfortunately, do not always adhere to the strictest of cybersecurity policies and

procedures. Almost 40% of IT leaders believe that, when it comes to cybersecurity, the CEOs of their companies are weak links [3].

The same study found that 76% of CEOs admit to bypassing cybersecurity policies and procedures to save time. They admit to bypassing security protocols even though 84% of executives have admitted to being the target of at least one attack within the previous year [4].

"There's also an intangible value associated with having an additional set of eyes on our books, expert watching out for anomalies and issues. That gives us peace of mind."

-DeAnna Swearingen, COO, Quimbee

Seeking peace of mind? Start with having the right team and technology in place.

Now that we've made the risks very clear- let's get into steps to take to prevent them.

6 Cybersecurity Tips for Top-Tier Business Leaders

1. Never Sacrifice Security for Speed

When it comes to cybersecurity, you should never take shortcuts. Even though your time (and that of all your C-suite executives is very valuable), it's not worth risking a cyberattack.

Any damage from a cyberattack will undoubtedly end up costing you more than the time required to change your passwords every 90 days or the time needed to adhere to whichever security protocol you'd rather not follow.

Plus, it's worth considering the sticky situation your IT employees must navigate when a high-level executive requests their assistance with bypassing security protocols. IT professionals are then put in the position of choosing between compromising the company's security or refusing a request from a superior (or even their boss's boss).

→ **To keep business operations secure and workplace morale positive, just take the time to follow your company's cybersecurity policies.**

2. Remember That Cybersecurity Directly Affects Business Outcomes

Think about the way that implementing strong protocols and practicing good cybersecurity helps you build your business.

→ **Nowadays, every company collects some form of data from their clients, and this personal information must be stored securely.**

In every business, good cybersecurity gives your clients peace of mind that their personal data is safe with you.

Additionally, you might not have a breach today or tomorrow, but if you skimp on cybersecurity and don't take your company's protocols seriously, you will eventually suffer a successful cyberattack. Whether an attack leads to monetary losses, lawsuits, or reputational damage, it will hurt your bottom line.

3. Be Aware of the Most Common Kinds of Cyber Attacks

The most common attacks that target high-level executives include spear phishing, whale phishing, email impersonation, business email compromise, account takeovers, and social media impersonations.

Read More: Safeguard your Business - Best Practices to Protect Against Cyber Threats

In all of these scenarios, criminals leverage personal data and even public information to personalize attacks that target C-suite executives, board members, and other high-ranking people involved in your company.

→ **By ensuring everyone is aware of and trained on the signs to look for, it could help prevent these attacks from happening to your organization.**

4. Protect Every Network Entry Point

Securing network entry points has always posed a challenge to both IT and physical security professionals in the workplace. Then the rise of the smartphone and cloud storage further complicated access points. The pandemic has made the security challenge even more complex.

The pandemic-induced shift to remote workplaces forced businesses into a sudden increase in network access points, and new-fangled network structures with employees working from home and needing access to the company's network from new devices on internet connections that might or might not be secure.

This has left many IT professionals struggling to bring their cybersecurity measures, policies, and protocols up to speed.

→ **As the leader of your business, it's important to recognize the challenge that your IT professionals are likely facing right now so that you can provide them with the support and resources they need to ensure your company's digital assets remain secure, despite the new complexities.**

5. Practice Security at Sign In

→ **Create added layers of security when you sign into various programs and networks by using different passwords and two-factor authentication whenever it's possible.**

This will ensure that even if one of your passwords is somehow leaked, that every other system you sign into will remain secure.

Two-factor authentication makes it more difficult for hackers to access your personal accounts and information – even if your passwords leak.

6. Build Buy-In by Leading by Example

People are key when it comes to stopping cyber attackers in their tracks. Whether it's a phishing scam or an attempt at social engineering, most cyberattacks typically involve some element of human error where someone in your organization (maybe even you) accidentally clicks a dangerous link or gives out information that they should not.

To convey the seriousness of cybersecurity and constant vigilance, even the top executives in your company need to lead by example. Doing so will help you get buy-in throughout your business.

→ **When the people you manage witness you attending cybersecurity training sessions and subsequently following protocol, they'll follow suit and so will the employees working beneath them.**

"The IRS is at my door! What do I do?"

👉Protecting Your Business Against Fraud: Listen to the full episode here!

Most Importantly, Leave it To The Professionals

Cybersecurity is not something to take lightheartedly.

Even if you have a solid background in IT, as a business leader, you're likely too busy running your business to dedicate enough time to shoring up your network and ensuring robust cybersecurity protections. It's an IT professional's job to stay on top of the latest threats, viruses, and scams to ensure your hardware, software, and people are fully protected to minimize points of entry and overall risk.

Outsourcing your back office is one of the safest measures to take- especially when it comes down to the security of your financial data. It's essential to have someone dedicated

to protecting your business's digital assets, monetary assets, data, personal information, and reputation from cybercriminals.

---

[1] https://www.ibm.com/downloads/cas/M94RB4WR

[2] https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2021.html

[3] https://www.theceomagazine.com/business/innovation-technology/cybersecurity/

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