

Cyber - Attacks: An Existential Threat to Small Businesses

by **MICHAEL SIPE, Chairman — Vistage Int'l 667**

In today's digital-first world, businesses are constantly navigating a complex web of risks — economic fluctuations, political instability, evolving consumer behaviors, and rapid technological change. But amid this uncertainty, one threat stands above the rest: **cyberattacks**.

While artificial intelligence dominates headlines with promises of disruption and innovation, the more immediate and pressing danger to businesses — both large and small — is cybercrime. Ironically, the same technological progress that drives growth also increases our exposure to digital threats. As AI becomes more mainstream, the tools available to hackers grow more advanced, making the risk landscape increasingly treacherous.

The High Cost of Cybercrime

The financial toll of cyberattacks is staggering. In 2024, the **average cost of a data breach in the U.S. is \$4.88 million**. But this figure doesn't reflect the full impact. Breaches disrupt operations, erode customer trust, damage reputations, and often lead to long-term consequences that are difficult to quantify.

These attacks are no longer limited to global corporations. **Small and mid-size businesses (SMBs)** — once thought to fly under hackers' radar — are now firmly in the crosshairs. According to the recent Vistage **CEO Confidence Index** data, 5% of CEOs reported a cyber incident involving lost or compromised data, up from 4% the previous year. Additionally, 20% experienced incidents that didn't result in data loss, and 27% reported that a customer or supplier had suffered a cyber-related breach.

The message is clear: **cybercrime is not a matter of if, but when**, and its ripple effects extend across the entire business ecosystem.

The Good News: CEOs Are Getting Smarter

Despite the growing threat, there's a positive trend: more CEOs are recognizing the importance of cybersecurity. As of late 2024, **58% report having a current cybersecurity strategy reviewed at least annually** — a significant leap from just 38% in 2017.

However, that leaves a troubling 42% either without a plan, working on one, or relying on outdated strategies. For nearly half of SMBs, that means a high level of exposure to devastating attacks.

In today's landscape, cybersecurity isn't just an IT responsibility. It's a **core business function** that requires active oversight from the top. And for companies without strong defenses, **complacency could be their undoing**.

Three Critical Actions Every CEO Must Take

To stay ahead of cyber threats, CEOs must adopt a proactive stance. Here are three essential — yet often overlooked — pillars of a strong cybersecurity approach:

1. Build a Response Plan



GRAPHIC | COURTESY OF VISTAGE INT'L 667

Too often, business leaders assume a cyberattack won't happen to them. That mindset is dangerous.

Every organization must have a detailed **incident response plan** to handle worst-case scenarios. Questions like "What if hackers demand a ransom?" or "How do we restore operations quickly?" should be addressed in advance — not during the heat of a crisis.

An effective response plan should cover:

- Internal and external communication protocols
- Backup and recovery procedures
- Legal and insurance coordination
- Defined roles for every team member during an incident

Being prepared doesn't eliminate risk, but it dramatically reduces chaos and speeds up recovery when the unexpected happens.

2. Audit Third-Party Vendors

Your cybersecurity is only as strong as your weakest partner. Every cloud service, payment processor, IT contractor, and software platform your team interacts with introduces potential risk.

Research shows that **third-party breaches are 40% more expensive** than internal ones. That's why CEOs must take an active role in ensuring vendor security, including:

- Conducting regular audits
- Requiring security certifications
- Setting clear contractual expectations
- Monitoring compliance with data protection regulations

Digital convenience cannot come at the cost of digital vulnerability. **Trust must be earned — and verified.**

3. Train Your Entire Team

Despite sophisticated technology, the most common point of failure is still human error. And hackers know it.

Thanks to tools like generative AI and deepfake technology, bad actors can now craft incredibly convincing phishing emails and impersonation attempts. A single misstep by an employee — no matter their role — can open the door to a full-scale breach.

The solution? **Comprehensive, company-wide cybersecurity training**. Every employee should understand:

- How to identify suspicious emails or requests
- The basics of social engineering and phishing
- Proper escalation procedures if they suspect a threat

Regular drills, simulated attacks, and clear communication channels can transform your workforce from a liability into your first line of defense.

The Evolving Role of the CEO

As the cyber threat landscape evolves, so too must the role of the CEO. Leaders can no longer delegate cybersecurity entirely to IT departments. Instead, they must act as **champions of digital resilience**, ensuring security is embedded into the organization's strategy, culture, and budget.

That includes:

- Making cybersecurity a board-level discussion
- Allocating appropriate resources and talent
- Staying informed on emerging risks and technologies
- Holding themselves accountable for organizational preparedness

The consequences of inaction are far too great. A single breach can erase years of progress and cost millions. But the businesses that prepare now will be more resilient, more agile, and more trusted by customers and partners alike.

The Time to Act is Now

Cybersecurity is no longer optional. It's not a line item to be reviewed once a year or a checkbox on a compliance form. It's a **daily operational imperative** — and a critical leadership responsibility.

Whether you're leading a fast-scaling startup or managing a seasoned enterprise, the digital risks you face are real — and growing. But so are the tools, strategies, and knowledge needed to defend against them.

Don't wait for a breach to prioritize cybersecurity. **The cost of inaction isn't just financial — it could be existential.**

For deeper insight into this constantly evolving landscape, consider joining our Vistage Peer Group — where top-performing business leaders connect, learn, and grow together.

Michael Sipe is an executive coach, business consultant, and mergers and acquisitions. Michael-Sipe.com • Vistage.com • CrossPointe Capital.com • 10xGroups.com

ENVISION BEND
SHAPING OUR FUTURE

CITY CLUB
OF CENTRAL OREGON
Conversation Creates Community

Community Vision Summit
Innovations in Workforce Housing
Presented by City Club and Envision Bend

April 17th
Unitarian Universalist
Fellowship of Central Oregon
5:30-7:30 p.m.
**doors/resource fair opens at 5:00 p.m.*

Register at cityclubco.org