CFO

Cybersecurity Action Plan: 7 Tips for Small Business CFOs

These practical steps help finance chiefs enhance or build practices to prevent cybersecurity risk.

Published March 26, 2024

Steve McNally
Contributing Writer

Just_Super via Getty Images

A data security breach is one of the CFO's biggest nightmares. The bad actors are getting creative at their trade, causing our nightmares to become increasingly vivid and scary. Your nightmares may entail viruses, worms, trojans, spyware, bricking, and/or other malware. Or maybe they are triggered by whaling or another form of phishing. Or maybe crypto-jacking, man-in-the-middle attacks, zero-day exploits, or a good old-fashioned brute force attack keeps you up at night.

These nightmares can be especially intense for the small business CFO who lacks a knight (e.g., a chief information security officer) to come sleigh the cyber-dragon. Here are seven practical actions CFOs can take to sleep better at night.

1. Build Personal Awareness

CFOs — especially small business CFOs — must take a leading role in protecting their organizations' systems, networks, and programs from digital attacks.

First, though, you must build your awareness. Familiarize yourself

with the types of cyber attacks, cyber attackers, and defensive measures in your arsenal. Understand relevant laws and regulations regarding electronic transactions, consumer protections, cybercrimes, and privacy and data protection requirements (which can be quite complex for a global organization). And polish your risk management skills, gaining comfort with cybersecurity-related risk management tools and best practices.

In addition to reading articles like this, I highly recommend completing relevant programs such as IMA's Cybersecurity & Data Practices Certificate Program to build a solid foundation.

2. Educate Your Finance Team

Employees often represent your weakest cyber link — potentially even members of your own team. While you would expect finance professionals to be attuned to the significant and growing risk of cyberattacks, I know of a small business corporate controller who was tricked into sending vendor payments to a bad actor's account. The company was already short on cash and, unfortunately, didn't recover.

For some employees, it's a lack of awareness; for others, carelessness. Either way, if an employee clicks on a malicious link or provides sensitive information to a bad actor, the entire organization is at risk.

Require new employees to certify they understand your cyber policies and existing employees to renew their certifications annually. Provide company-wide training, including stories of cyber victims and tips on how to avoid being one of them. Conduct phishing campaigns (we do them monthly), requiring anyone who "falls victim" to complete personalized training. And meet one-on-one with "the careless" as necessary.

3. Adopt Cyber Policies

Before employees can certify they understand and will follow your cyber policies, these policies need to be clearly defined. For too many smaller organizations, however, they are not.

Consider implementing an acceptable use policy (to set expectations of employees when using computers), a communications equipment policy (to outline how equipment communicates data and acceptable ways to use this data), a risk assessment policy (to define who is accountable for assessing, classifying, and managing cyber risks), and a data breach response policy (to clarify who has accountability for what in case of a data breach).

To draft these policies, consider leveraging the SANS Institute's free policy templates.

4. Invest in Cyber Insurance

The question is more likely "when" than "if" your organization will face a cybersecurity incident, so consider investing in a standalone cyber policy to mitigate the risk of financial loss due to data breaches, ransomware attacks, and other incidents. The cost of this coverage has been steadily rising, though, especially for organizations with poorly designed and/or implemented cybersecurity programs.

Carefully review all attestations in the application, which must be complete and accurate. Make sure you fully understand your policy, including controls that must be in place (e.g., dual authentication, check pre-approvals, etc.), reporting turnaround time, and other requirements. And maintain a hard copy of the policy (just in case).

5. Know and Mitigate Your Risks

You can more effectively assess your risks by designing and implementing a comprehensive cybersecurity program:

- Select a framework, such as the National Institute of Standards and Technology's (NIST's) Cybersecurity Framework, The Center for Internet Security (CIS) Control Framework, or the Information Systems Audit and Control Association's (ISACA's) Control Objectives for Information and related Technology (COBIT) Framework.
- Conduct a baseline assessment. Leveraging NIST CSF 1.1, which is organized into five key functions (i.e., identify, protect, detect, respond, and recover) and multiple activities (e.g., the protect function includes activities like protecting sensitive data, conducting regular backups, and training users). We worked through a comprehensive series of questions aligned with these functions and activities to identify strengths and potential gaps in our program.
- Develop action plans and prioritize those action plans that address the most concerning gaps identified during your baseline assessment.

6. Develop Business Continuity and Related Plans

How will you respond amid an unfolding cyberattack? Will you be able to make good decisions during the stress and chaos of a live event?

Several years ago, as part of the leadership team for Campbell's Napoleon Operations, I participated in a four-hour crisis management and business continuity plan exercise. That year's theme was a severe flu outbreak. New information was revealed throughout the exercise, forcing us to refine our plans. That

exercise enabled the team to more effectively respond when COVID-19 hit.

Your ability to manage cyberattacks and other crises significantly improves if you have already documented actionable crisis management, IT disaster recovery, and business continuity plans, even if they are only loosely linked to the actual crisis at hand.

7. Adopt a Continuous Improvement Mindset

As the bad actors become increasingly creative, we must become increasingly vigilant in assessing their threats and proactive in enhancing our cybersecurity programs. Conduct a new baseline assessment and compare it against your original, reassessing gaps and re-prioritizing your action plans. Stay attuned to new cyberattack schemes and best practices to prevent them from impacting your organization. If you leverage NIST CSF 1.1, consider upgrading to NIST CSF 2.0 (NIST's updated framework, released February 26, 2024, has been expanded to include new features highlighting the importance of governance and supply chains). Invest in automation and artificial intelligence to combat modern fraudster sophistication. And consider engaging an incident response firm or cybersecurity partner. In short, adopt a continuous improvement mindset.