Mitigate Cyber Risks with the Right Security Controls

What are the right controls for your organization? Here's how to be sure.

By Chris Moschovitis

In its framework for improving cybersecurity, the National Institute of Standards and Technology lists five duties: "Identify, protect, detect, respond, and recover."

Notice that "prevent" isn't one of them. There is no "prevent" in cybersecurity.

But, although there's no way to prevent cybersecurity risks, there is a clear, three-step method to mitigate them and keep you safe:

1. Evaluate Your Risks

Each nonprofit has a different risk tolerance. The right controls for one organization will prove excessive for the next, and not enough for the third. Therefore, the first thing you must establish is your organization's risk appetite. That must be set by the board.

2. Analyze Your Assets

Next, get a grip on your organization's assets. What, exactly, are the things of value you're trying to protect, and what are the threats against them? Is it a matter of protecting intellectual property? Donor data? Classified information? Reputation? Is it a question of physical security? Insider threats? In short, what does your world look like, and where are the threats coming from?

3. Apply the Right Controls

You're now ready to apply the right controls. Remember: Controls "do" things. They aren't some abstract notion; they do-the-do! There are four kinds of controls:

Preventive controls provide barriers to attack. Now you'll argue that we began this article by claiming that there is no "prevent" in cybersecurity. You're right, but remember, controls "do things." A preventive control hasn't prevented the attack, but, like the barrier on the street that stops the runaway truck from hitting the building, it prevents an aspect of the attack. Think of it as a locked door that confines the threat and keeps the problem from escalating. Another example of a preventive control is segregation of duties. Your systems administrator shouldn't know the database password, and the database administrator shouldn't know the systems password. Security awareness training is another excellent example of a preventive control.

Detective controls are like motion detectors: They know the door has been opened, and they do something about it. Either they close it, or they alert someone. Examples of detective controls include system monitoring applications, intrusion detection systems, anti-virus, and anti-malware solutions.

> "What does your world look like, and where are the threats coming from?"

Corrective controls fix or restore the environment. For example, applying the right security patches and upgrades is a corrective control. Restoring your data from backup is another corrective control.

Compensatory controls are those designed to compensate for some of the damage. A disaster recovery site is a compensatory control. Cyber insurance can also be a compensatory control. A backup generator, a second set of servers or computers, and the ability to switch over operations to another country are all compensatory controls.

Keep in mind that some solutions span two or more of these four control classes. For example, an anti-virus/anti-malware solution can be a preventative control, a detective control, and a corrective one all at the same time. It's like getting your flu shot each year. You hope that, armed with the inoculation, your body will detect the attack of the flu virus and take corrective action, keeping you healthy. But if you still end up sick, that's where your compensatory, chicken-soup control kicks in, making life a little less miserable.

Form Your Strategy

What's the right blend of controls for your organization? It depends on risk appetite, type of asset, type of threat, regulatory environment, budget, and available skill sets. You need to take all these factors into consideration in developing your defense-in-depth cybersecurity strategy.

Remember: You have a tremendous advantage over your attacker, or any expert: You know your organization better than anyone else. You know what's of value that needs protection. So, more than any solution out there, trust yourself and your judgment, and apply pragmatic controls. S

Chris Moschovitis (Chris.Moschovitis@tmg-emedia.com) is co-author of History of the Internet: 1843 to the Present *and CEO of tmg-emedia.com.*

Identify and Control Your Risks

Here is information on some of the threats you may want to keep an eye on (NonprofitWorld.org):

Know the Risks before You Head to the Cloud (Vol. 30, No. 6)

Setting Up a Control System for Your Organization (Vol. 16, No. 3)

The Neighborhood Just Got Bigger: Protecting Trademarks in the Expanded Internet (Vol. 31, No. 6)

Legal Advice on Using the New Media (Vol. 28, No. 6)

Risk Management: How to Protect Your Assets (Vol. 26, No. 1)

Keep Your Online Identity Safe (Vol. 35, No. 4)

What Is the Board's Role in Managing Risk? (Vol. 15, No. 5)

Coming Up in *Nonprofit World*

- 35 Ways to Enhance Your Organization
- Plan for Succession with Four Simple Rules
- Is Your Coworker a Jerk, or Does He Need a Doctor?
- Creating a Culture of Productivity
- Embrace Mindfulness as a Leadership Practice
- Being a Force for Good with Advanced Analytics
- What Are the Three Most Boring Words in Fundraising Appeals?
- When Board Members Say Good-bye
- E-Mail Mistakes that Could Be Damaging Your Fundraising Efforts
- How to Solve the Biggest Problem with Corporate Giving
- Triggering Overtime with the Swipe of a Credit Card

And much more . . . .