FlexProtection

Flex-Protection.com – Data Protection Services

Top Seven Best Practices

1. Have a comprehensive, documented Security Policy.

Yes, even a small company, a non-profit association, or a small government department should have such a policy. Here is where you will identify strategies, practices, and rules to help avoid data breaches and compromised systems. You won't know where you stand or where you are going without a roadmap.

2. Spend the most resources on protecting the crown jewels.

Determine which systems, databases, and networks have the most critical data, the stuff you cannot operate without. And direct your efforts and resources toward protecting these assets.

One good tactic is to draw out a graph with the "importance of data" along one axis and with "effort/cost to protect" on the other. Then plot your systems and potential projects on the graph, and focus your protection resources on the Low Cost / High Importance data items. For example, strengthening password policies does not cost much and can have a big impact.

3. Place a high priority on user education.

Most data breaches and security problems can be traced to failure to observe sensible practices, or to understand the impact of certain habits. In fact there are many user habits and practices that can create an exposure that leads to serious breaches.

Yes, there are also purely technical attacks that can infiltrate your network and do great harm. But user education – and online testing with E-learning – can greatly enhance the security awareness level of management and end-users. And user education generally produces a lot of "bang for the buck".

4. Hire a Penetration Tester.

Or designate an internal resource – probably an IT professional - to take on that role. A "Pen Tester" will know how to use software tools to test for vulnerabilities and even launch attacks against your servers or network (while doing no actual damage). Make sure there is a mutual, documented understanding from the outset about what is to be tested and how to protect (and back up) live data to minimize risk.

5. Separate computers, networks, and servers when possible.

If you operate a web server, try to keep it on a different network from the one your users are on. Your web site WILL BE attacked regularly, and you don't want a successful hacker fishing around in your user's computers. For similar reasons, keep applications and databases on different machines. Keeping your public-facing systems in the Cloud may help in some cases, but that may not be ideal for other reasons.

6. Get cost-effective help.

Completing any form at Flex-protection.com will get you to a quick and useful "discovery conversation", and that's what we recommend. And there are loads of other cyber security experts out there, at various costs. Build a long-term relationship based on common-sense practices and improvements. When a consultant makes recommendations, they should make sense to you, and no project should disrupt your business and make your life more complex.

Share the burden of figuring everything out and building a better set of policies and defenses. You will soon find that there are many industry best practices beyond the examples listed here.

7. Stay with it.

No one wants to be the CEO, VP, or Director who passed up a chance to increase data security and then got hacked. So most leaders are willing to seriously consider a cybersecurity enhancement project. But improving your data protection posture is not a one-time event. New threats emerge every day, and your defenses have to be revised over time. From now on, data security is a part of doing business.

Please send any questions to rep@flextraining.com.