Are you practicing SecurITy? A Checklist for Non-Technical Executives

Is your business protected? Keeping the lights on and keeping your business running is priority number one every day. If you aren't practicing SecurITy, you may be risking your ability to best serve your clients. With cyber attacks becoming the norm and more businesses making headlines with breaches, find out what you can be doing to protect your future and improve your business' performance.

1. Do you have a Risk Management strategy in place?

__ 0. No strategy in place
__ 1. Initial/ad-hoc (no formalized process; occasional, intermittent activities)
__ 2. Minimal strategy (process is not documented, not formally communicated or trained)
__ 3. Defined strategy (process has been documented and communicated through training)
__ 4. Measurable strategy (process is regularly monitored and measured for performance)
__ 5. Optimized strategy (process has been refined over time through continual improvement)

Definition:

Personally Identifiable Information (PII): Defined as information that can be used on it's own or with other information to identify, contact or locate a single person.

At the very least, you should have information security policies and procedures documented and signed off by every employee, from the CEO down to the part-time intern. A designated information security officer should also be assigned to handle questions as well as manage and update strategy.

Classify all data handled by your company into categories by varying sensitivity levels. Personally Identifiable Information (PII), usually made up of a person's name and another piece of identifying information about that individual; this can include items like social security number or address. Any PII or Protected Health Data should fall into the highest sensitivity classification.

Ideally, you should have a full risk management framework in place that takes into account business strategy and includes regular monitoring and review of all risks.

2. Do you know who has control over your network and data?

__ 0. No knowledge of network and data access
__ 1. I can track some access to systems, but can't narrow it down to individual user
__ 2. I can track all individual access to systems
__ 3. I can track all individual access to systems and am alerted to high risk activity

Nobody in the company should have the ability access, modify or use technology without authorization. You should have strict processes in place for when employees enter, move within or leave the company. These processes should limit the

17 State Street / 40th floor / New York, NY / 10004 / KalkiConsulting.com / 855.GO.KALKI / 855.465.2554

KALKI

amount of access an employee is given based on need. There's no reason to give employees access to data they don't need to complete their job.

> *SecurITy is IT transformed. We are redefining what you can expect from IT. SecurITy is reliable, consistent and empowers your business to perform at its best.*

To maintain an audit trail and be able to track user activity, make sure all of your accounts are separated by user, especially administrative accounts (i.e. don't use a single administrative account for multiple users). The same goes for any vendor accounts on your systems.

3. Do you have procedures in place for initiating projects and managing technology changes?

__ 0. No processes in place
__ 1. Initial/ad-hoc (no formalized process; occasional, intermittent activities)
__ 2. Minimal processes (process is not documented, not formally communicated or trained)
__ 3. Defined processes (process has been documented and communicated through training)
__ 4. Measurable processes (process is regularly monitored and measured for performance)
__ 5. Optimized processes (process refined over time through continual improvement)

You should have a project initiation process which all new and proposed projects go through to determine what risks or issues may be introduced by the project. This process should investigate any technology assets touched by the project, other affected projects, project cost and any risks introduced to the business during the course of the project.

Any changes to technology should undergo a formal change management process by which all risks of the change are investigated and information provided to all business units which may be affected. Changes should only be started once these risks have been communicated and approved by management and affected business units.

4. Do you have Information Security training and awareness programs in place?

__ 0. No Information Security training
__ 1. Ad/hoc or periodic training
__ 2. Annual information security training
__ 3. Annual training and regular awareness communications and campaigns

Do your employees know how to recognize malicious emails or viruses, avoid and report them? Do you find that people write down sensitive data, have trouble managing passwords or are willing to give out their credentials over the phone?

A chain is only as strong as its weakest link. In many businesses, human error or lack of knowledge often proves to be the weakest link. Many attacks can be traced back to something that could easily be solved with a little old-fashioned knowledge. Arm your employees with the tools and knowledge to protect themselves and the business.

Score Yourself

0 - 4: High Risk

Your business is at a high risk for data loss or breach. If you don't have the knowledge base in-house to make improvements, it might be time to talk to an outside resource about securITy.

5 - 10: Getting IT Going

You've made some strides in making your IT more secure, but there are still ways to improve. Figure out where your weakest area is and start there. Bringing in someone who is an expert in that area will speed up improvement.

11 - 16: On Top of IT

Congratulations - you have taken some serious steps to protect your business from data loss and breaches. There's always room for improvement. Make sure each area undergoes regular review and update to keep up with changes.

17 State Street / 40th floor / New York, NY / 10004 / KalkiConsulting.com / 855.GO.KALKI / 855.465.2554

KALKI