How Safe Is Your Business?

Why Cybersecurity Equals Job Security for CEOs, CFOs and Others

How much do you worry about being hacked? How much *should* you worry?

In 2017, cyber-attacks doubled from 2016 levels—and the insider phrase now is "It's not *if,* but *when*, you'll be attacked." In fact, organizations are silently and invisibly breached every day, with the private and confidential information of consumers, customers or corporations harvested leisurely by terrorists and criminals. Obviously, this has become an issue that CEOs and other leaders need to take much more seriously than in the past.

Amazingly, these breaches do not result from decisions made at the brain-surgeon level. Most cybersecurity (cyber) hacks are enabled by simple errors or laxity in areas like basic software and IT hygiene. This includes the failure to provide minimal security awareness training.

Why does this happen? Well … who likes changing passwords, or waiting for that security-code text or phone call, especially when you have ever-growing workloads and tight deadlines? And "the Suits" exempt themselves from the basic common-sense procedures which everyone else must endure. Hacks become inevitable.

Enable or compound this with lack of tone at the top and failure to allocate reasonable resources.

Did Richard Smith, the Equifax CEO, preside over his own ouster, an immense destruction of shareholder wealth, or both, in the recent hack of 143 million consumers, which allowed access to names, Social Security numbers, birthdates, addresses and, in some cases, driver's license numbers? The jury is still out.

Off-the-record discussions at the recent international CyberHub Summit considered the recent spate of CEOs, CFOs and CTOs actually losing their job due

Call Gary Patterson at 678-319-4739 or Gary@FiscalDoctor.com to discuss your unique situation.

to preventable cyber hacks. And seldom disclosed, events like these are happening ***daily*** at smaller middle-market companies.

Why do seemingly simple weaknesses exist to be exploited by nefarious third-world groups? How often does the tone at the top support politically and financially counter-initiatives? Key to the Equifax debacle was the failure to maintain software patches that address known vulnerabilities. The fallout was compounded with a level of hesitation far less acceptable today than in the past, combined with officers selling their stock.

Bur before you start spending any money for an external assessment of your cyber exposure, we suggest that you start with *Three-Minute Self-Scoring Review*. The more honestly you answer, the more you'll get out of it.

Step One. Answer the following two questions.

On a scale of 1 to 10:

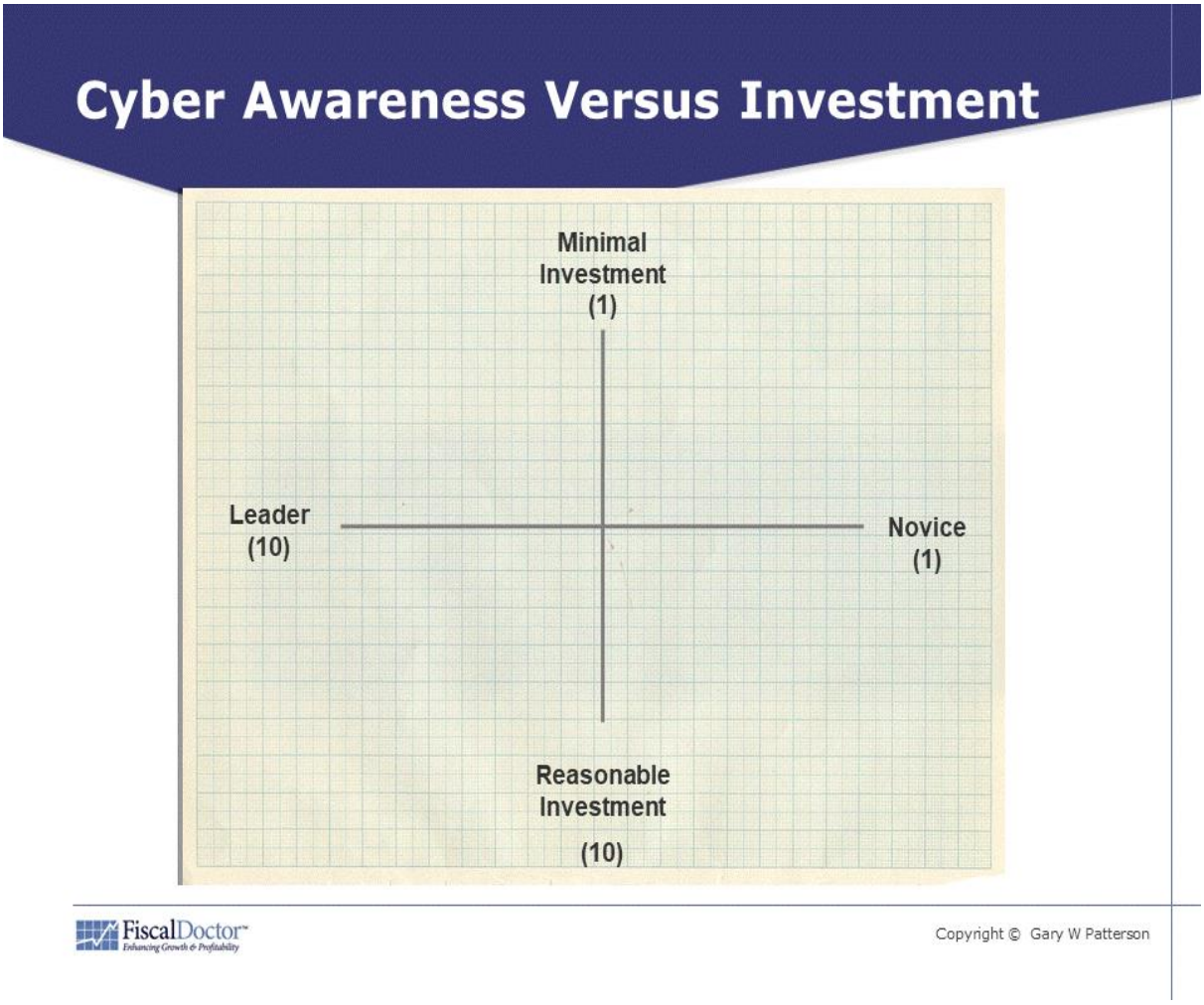
Awareness. If 10 means you could probably lead a cyberthreat panel discussion — and 1 means that you hear your people say the word "cyber," but you're not sure what your real level of preparation is — how aware is your business?

Investment. If 10 means you have already done a cyber or security overview and are implementing those recommendations — and 1 means there actually may be resources available, but nothing is budgeted to consider this until next year or later — at what level is your business investing?

Step Two. Mark your answers on the two axes below:

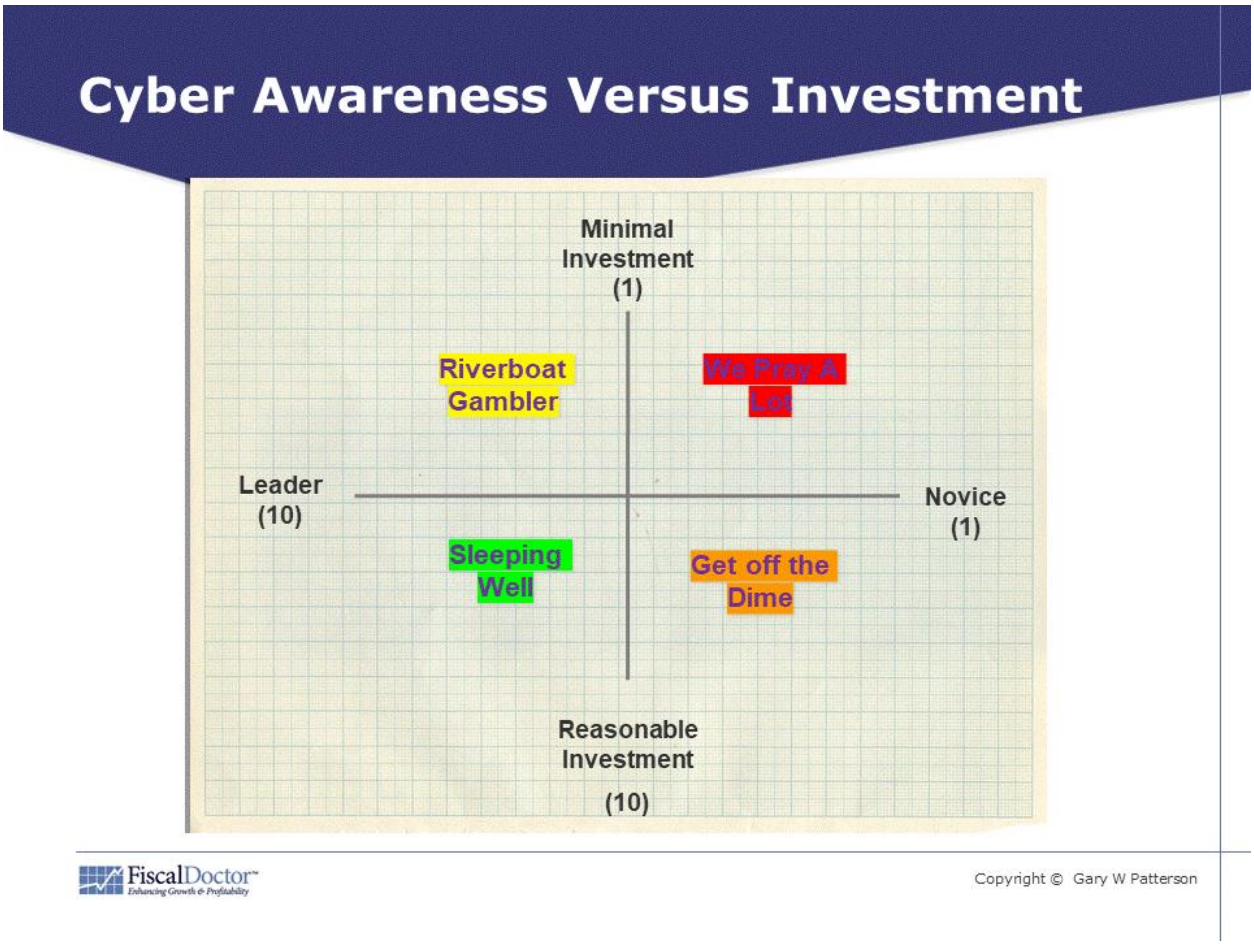
Mark your numerical answer for Awareness on the horizontal continuum from Leader to Novice.

Mark your numerical answer for Investment on the vertical continuum from Reasonable Investment to Minimal Investment.



Draw a line between the two points to note which quadrant your business falls into.

Step Three. Consider the implication of your business's quadrant on the *Cyber Awareness Versus Investment* below.



We Pray — ***a Lot*** in the upper right corner suggests limited, even minimal, budget is available for cyber-risk management and control, combined with limited, even novice, understanding of cybersecurity and your risks.

Get Off the Dime in the bottom right corner suggests a reasonable budget is available for cyber-risk management, but with a limited understanding of cybersecurity and your specific exposures.

Riverboat Gamblers in the upper left quadrant are aware of both cybersecurity and possible cyber exposures, but prefer to kick most of the cans down the road, addressing issues slowly and hoping there won't be an attack.

Sleeping Well in the lower left quadrant suggests a strong understanding of overall cyber issues, along with a commitment to managing the organization's risks with a reasonable budget (and the accompanying political clout and finances needed).

Unless your business is willing to assess its level of cybersecurity, both culturally and from a resource investment standpoint, your C-Suite is leaving itself wide open to be second-guessed and worse.

Step Four. The CEO and key reports burrow deeper, evaluate cyber-exposure areas, create an action plan, invest necessary resources and then execute the plan.

This includes coming to grips with the fact that you cannot protect everything — but you can reasonably manage your exposure. Your priority should be to strategically protect the crown jewels of the organization.

Step Five. Rinse and repeat.

Business has always faced some level of cyber threats. Threats are countered only to see new threats arise requiring new counter-threats.

Where can you be more proactive to get in front of these risks?

Before doing anything else, you need to address the tone at the top. Only then will it be possible to manage risks and drive compliance with adequate resources. After all, the reputation and jobs you save may be your people, colleagues or even yourself.

Spread the word.

As originally published in Corporate Compliance Insights
http://www.corporatecomplianceinsights.com/how-safe-is-your-business/

About Gary W. Patterson

Gary W. Patterson, president & CEO of FiscalDoctor®, works with leaders who want to uncover their blind spot before it finds them, so they can make better decisions. He can also help increase your profitability, providing access to 100 best-of-the-best experts who are often better and cheaper than incumbents. Gary can be reached at 678-319-4739 or gary@FiscalDoctor.com.

Take Away Points:

1

_____
_____

2

_____
_____

3

_____
_____

Then What? Action Plan

I will

_____
_____

By _____

With support from/accountability

To _____

Call Gary Patterson at 678-319-4739 or Gary@FiscalDoctor.com to discuss your unique situation.