Guest Post: The Missing Link of Cybersecurity — Time for a Cyber Risk Check-Up

By Kevin LaCroix on March 7, 2019 Posted in Cyber Liability

The threats to data security are substantial. Every organization faces some level of cyber risk. So how do we get better at cybersecurity? That is the question that Paul Ferrillo and Christophe Veltsos ask in the following guest post. Paul is a shareholder in the Greenberg Traurig law firm’s Cybersecurity, Privacy, and Crisis Management Practice. Chris is is a professor in the Department of Computer Information Science at Minnesota State University, Mankato where he regularly teaches Information Security and Information Warfare classes. I would like to thank Paul and Chris for their willingness to allow me to publish their article as a guest post. I welcome guest post submissions from responsible authors on topics of interest to this blog’s readers. Please contact me directly if you would like to submit a guest post. Paul and Chris’s article is set out below. Please be sure to also see the item at the end of the post about International Women’s Day.

Chris and I write, teach, and give a lot of pro bono advice regarding cybersecurity and cyber risks to organizations of all sizes and across a variety of sectors. But while organizations have made some progress in the past 5 years, that progress is slow, too slow given the pace of change, the growing attack surface, and given attackers’ rapidly evolving skills. So, we asked ourselves “how can we help this nation get better with cybersecurity?”

We both realized that there’s ONE thing that you can only afford to put off for so long… your digital health. But before we connect health and cyber, let’s review what we mean when we talk about cyber risk.

Just What Constitutes Cyber Risk?

Many people still don’t get the concept of cyber risk, or get the basic idea but fail to connect it to their “world,” their organization with its multitude of IT systems and the data that is the lifeblood of their business. Yet cyber risk is something that we should spend a lot more time thinking about, engaging with, much like a good friend that one checks in with on a regular basis, for our mutual benefit. But what is cyber risk?

This is how RSA — a well-known name in the cybersecurity domain — defines cyber risk:

Cyber risk is commonly defined as exposure to harm or loss resulting from breaches of or attacks on information systems. However, this definition must be broadened. A better, more
encompassing definition is “the potential of loss or harm related to technical infrastructure or the use of technology within an organization.”

Events covered by this more comprehensive definition can be categorized in multiple ways. One is intent. Events may be the result of deliberately malicious acts, such as a hacker carrying out an attack with the aim of compromising sensitive information, but they may also be unintentional, such as user error that makes a system temporarily unavailable. Risk events may come from sources outside the organization, such as cybercriminals or supply chain partners, or sources inside the organization such as employees or contractors.


Ok, this is a great definition, but to a layperson it might be a lot more confusing than meets the eye. How are networks attacked? By who? How do you make a system temporarily unavailable? What is supply chain risk, and how can you understand it? How should a lay person get his or her arms around the cyber risk of his or her organization? By thinking of cyber risk just like you would consider your own personal, yet very real, health risk.

Good Cyber Health is Like Good Physical Health

In physical health there are certain metrics that your doctor might use to describe someone who is healthy. Body weight, fasting blood sugar (<100mg), cholesterol (less than 200mg), no bad habits like smoking and drinking, and exercise (the type of exercise, frequency, and duration). These, for the most part, are measurable facts. Everyone knows these items of good health. Everyone abides by them. They work. And if you consistently score “in the red” on these indicators, eventually your health will catch up with you… in a critical sort of way!

But there are other indicators that might affect your health that doctors sometimes consider. Things outside of the human body. What sort of work does this patient do? Regular physical labor? Or a high-stress environment like a securities trading floor with 200 high strung traders? Does the patient walk for exercise? Or do they mountain climb in the Himalayas? What health issues exist in the patient’s immediate family? Is everyone healthy? Or did parents and grandparents have early heart attacks below age 60? Obviously, numbers are everything. Outside forces can also impact a person’s health. But the good part is that once we know about these outside risk factors, then we can deal with them. For an overweight, pre-diabetic, sedentary person, the easy fix — I mean remediation — might be to lose some weight and start exercising 45 minutes per day.

In cybersecurity, we have very little recognizable (by the lay person) metrics of good cyber health which poses a potential risk, which if left untreated for too long can result in serious disruptions and have a costly impact. Cyber risk can be confusing. The way technology issues can impact the business with such speed and force is new to many business leaders. While the risks come from the cyber domain, the effects can be felt across the business, even across geographic locations.

Cyber Risk Health Factors — The 2019 Edition

Here is our non-exhaustive list of cyber health factors for you to consider. Like our physical health factors, all the questions in the list are measurable or at least answerable. These questions really represent the basics of cybersecurity. And the basics matter a lot in cybersecurity. Trying to skip the basics to jump directly to advanced issues is like trying to climb Half-Dome yet having never climbed more than a dozen flights of stairs.

We added scores in the left column to make this a bit more concrete. For each question, the maximum score is 5 points if the answer to the question is “yes, we do that fully/well.” If the answer is only a maybe, then it’s a partial score of 2 (2 out of 5). If the answer is “no, we don’t do that” then 0 points.

**Security Awareness, Social Engineering, Phishing**
- **How much do you train your employees on Security Awareness, Social Engineering, Phishing?**
  - Full: 8+ hrs per year
  - Partial: 4-8 hrs per year

- **Do you conduct regular phishing tests of your staff?**
  - Full: yearly and it includes executives

- **Do you have an incident response and crisis communications plan?**
  - Full: yes and it is reviewed after major incidents

- **Do you practice your incident response and crisis plan with top leadership and the board?**
  - Full: yes, yearly or more frequently

**Technical Controls**
- **What is the average time it takes you to patch a critical vulnerability?**
  - Full: under a week
  - Partial: 1-3 weeks

- **Do you use two-factor or multi-factor authentication?**
  - Full: for all access to sensitive data
  - Partial: in some cases only

- **Do you have email filters to keep malicious email from reaching the desktops of your staff?**
  - Full: yes, prior to deployment and before any major changes

- **How often to you back up your network and workstations per month?**
  - Full: daily-weekly
  - Partial: weekly-monthly

- **Do you have a control that rejects or flags poor quality passwords (e.g. dictionary words)?**
  - Full: automatic
  - Partial: check has to be manually performed

- **Do you practice least-privileged access for all those accessing your network?**
  - Full: access is set to automatically expire

- **Are vulnerability assessments performed on a frequent basis?**
  - Full: 4+ times per year
  - Partial: 1-3 times per year

- **Do you have 24/7 security or network operations center (or equivalent managed service)?**
  - Full: the SOC/NOC detected & reported activity during the last pen-test

**Policies, Security Management and Oversight**
- **Do you have tested backup policies and procedures?**
  - Full: tested yearly or more frequently

- **Do you have a policy for passwords — for staff, IoT devices, and other devices?**
  - Full: default passwords are changed quickly & bad passwords are rejected

- **Do you have a third-party vendor due diligence program for those with access to your network?**
  - Full: yes and it is audited yearly

Is there someone assigned oversight responsibility for cybersecurity? Full: person is provided proper support (visibility, authority) and budget

Do you practice your incident response and crisis plan with top leadership and the board? Full: yes, yearly or more frequently

Are cyber risks reviewed by top leadership and the board? Full: yes, yearly or more frequently

Do you review your cyber risk insurance policy regularly to ensure adequate coverage? Full: reviewed yearly or more frequently such as after an incident

Here our hypothetical company got a score of 33 out of a possible total of 100 points. Not terrible but not great. But it’s a starting point, a baseline that is indicative of its overall cyber health. And like high blood sugar or diabetes, one can deal with those issues through remediation.

So in our case, you don’t have some email solution to keep spearphishing emails away from employee desktops. Spearphishing is an enormous risk today to corporate America. So this element is definitely a cyber risk of high priority. Say too that your organization has not fully installed multi-factor authentication yet, and further only backs up its server once every two weeks (on site, and to a server attached to the network). These are realistic elements of risk in smaller organization, and we don’t mean to criticize if this is you. Yet cyber risk is cyber risk, and all together your risks here of a successful malicious attack are pretty high. Is it time for another cheese burger and fries? Nope. Not here; it’s time for remediation of these known risks.

Let’s consider a different case. Suppose you are a large organization, yet you don’t have a functional third-party vendor due diligence program — you send out questionnaires, but that’s it. Coupled with this, you don’t remember the last time you audited your least-privilege access program. This puts you at of an attack from a third party vector where the criminal actor can steal the credentials of your vendor and use them to gain access to a treasure-trove of your company’s data.

**Situational Awareness Helps – Navigating IT and OT Risks**

As noted above, a notorious attack vector into a company’s network is that intrusion via a third party vendor or business partner. But it’s important, just like with health risks, to be aware of your surroundings too outside of your prime IT network. What if you managed a very successful manufacturing business that was heavily dependent on the Internet of Things (“the IoT”) to drive operations and control machines and run the shop floors. Now you would be faced with a different set of risk, as both your Operational Technology (OT) and Information Technology (IT) could be impacted by the poor security of IoT devices. In this case, an infection in one could spread to the other, quickly halting your entire operations, and the costs could quickly add up to millions of dollars. So, not only is there a different network but you are again dealing with third party vendor risk too.
What would the remediation be in this case? Certainly, policies and procedures around IoT and hard-coded passwords can help correct the situation. Expansive machine learning monitoring systems can help too. But no remediation is perfect. But what if you had 5 manufacturing plants around the country, not just one? And what if your purchasing and plant managers were focused only on cost savings and efficiencies, and not paying any attention to the security of the IoT devices.

What if you ran a shipping company, with large, ocean going container ships traveling the world’s oceans every day. And suppose the ship’s systems were running on an outdated operating system — perhaps released 5 or 10 years ago — and it had not been patched since then? Time for remediation. Time for updating. Time for patching. And for the love of all things fuzzy and cute, install an anti-GPS spoofing solution so your ship can always make it where its supposed to go regardless of the bad guys trying to send you off course. Indeed, not just data and networks could be at stake. The health and welfare of the crew could be at issue ultimately too.

Assessments and Insurance

Finally, it goes without saying that full blown health, welfare AND cybersecurity assessments are well thought of by insurance companies. Conduct no assessment and be a little overweight with some high blood pressure? You might not like your premium on your next year’s health or life insurance policy. Same goes when you are purchasing cybersecurity insurance. Regular cyber assessments show that you understand that cyber risk can impact — or possibly cripple — your business. Regular cyber assessments plus following the remediation plan being suggested means “you get it,” and that you realize that uncorrected cyber risk can “give your business a heart attack.”

But starting walking 3 miles a day, losing 20 pounds and stop smoking? A much better way to get insurance. And a much better way to managing your physical risk. And to live a long life.

This is why “cyber risk” is like human physical risk. It really is pretty similar if you think about it. No matter what the measurable indicators (obesity in one case, lack of a spearphishing solution in the other) are, we can deal with these risks though assessment and remediation. And it in many cases, for not a lot of money.

Since you’ve read this far, here’s a toast to better “cyber health” through a better understanding of cyber risk. Your organization’s prosperity and longevity depend on your honest and earnest attention to this issue of cyber risk. Tick, tock, don’t wait any longer.

[i] Here is our point system in a nutshell. Yes/no questions receive 5 points for yes or “fully implemented” answers, 0 points for no or “not implemented” answers. For questions with multiple levels of answers, you score 5 points for “fully implemented”, 2 points for “partially implemented”, otherwise 0 points. Tally up all the scores; the higher the score the better.