Data Protection Health Check – How to Interpret Your Score and What to Do Next

WHY SHOULD YOU CARE?

Business owners and leaders have a responsibility to mitigate and manage threats and risks as well as manage the growth of their companies. A key part of risk involves data privacy and cybersecurity. Fundamentally, you should care because your buyer cares. The right question to be ask is, "Does my company's systems, policies and procedures have the foundation and the flexibility to withstand compliance scrutiny and respond to inevitable data risks?" And of course, you and your team must have demonstrable cyber security controls in place to protect data and show these working controls during due diligence when you decide to sell your business, obtain investment or take your business public.

According to the authors of the article, *2020 Data Privacy Trends to Watch in M&A*, (Law.com):

> *"Data privacy is squarely in the spotlight of not only consumers and government regulators, but also of senior management, boards of directors, and shareholders, in particular in light of the impacts of COVID-19. There has been an increase in cybercrime and hackers wanting access to the surplus of online information generated from the world economy now "working from home."*
>
> *Data privacy in M&A is complex, with increased security incidents reported on disclosure schedules and elaborate data security representations and warranties in the transaction agreements. Now companies will need to be even more sensitive to the uptick of cybercrime and its impact on valuations and latent issues post-close. As the economy moves forward and M&A activity picks back up, companies need to be highly sensitive to the potential for post-closing issues, which should be weighed when considering price and post-close integration."*[1]

WHAT'S AT STAKE?

While I do not believe in scaring ourselves as a way of motivation, it is sobering to learn of companies that did not put adequate data privacy and security safeguards in place and the consequences they faced. Some firms seem to get away with data breaches and manage to stay in business. This is because they have a long runway of sustainability and deep pockets to pay fines, penalties and a bevy of lawyers, e.g., Equifax and Facebook.

Most businesses, however, have not been as fortunate. According to a study published in Inc., 60 percent of small businesses shut down within 6 months of a cyberattack.[2] According to a CISCO research study, companies that invest in cybersecurity and privacy remain viable, whereas small to medium enterprises often cannot withstand a data breach.[3] Consider these companies who failed to establish sufficient data protection and had to shutter operations for good:

MyBizHomepage

The online company was once valued at $100 million, but when the chief executive fired the chief technology officer and two other senior officers, who did not agree with the owner's decision not to sell the company, the trio launched a revenge attack that crippled the site. After the company spent over $1 million in an attempt to resolve the breach, the company's board decided to take the site down because it had been rendered useless.

Nirvanix

Although the details of the swift Nirvanix departure are unclear, consumers were left scrambling for new providers and services. It only took six weeks for the company to transform from business as usual to demanding customers remove their data quickly and with little notice. The company went belly-up not much later.

Code Spaces

According to SC Magazine, Code Spaces, a former SaaS provider, is one of nearly 60% of small businesses that fail within six months of being hacked. The company was accessed via its Amazon Elastic Compute Cloud control panel. The hackers erased data, backups, offsite backups, and machine configurations before attempting to extort the business by claiming a "large fee" would resolve their issues. Code Spaces took steps to change all of its passwords, but the damage was done. The criminal had already created backup logins. Code Spaces was unable to continue operations as it acknowledged that the company had suffered debilitating damages to both its finances and reputation.

BUSINESS VALUE

Here are five ways data privacy brings business value:

1. ***"Keep the lights on;" in other words, to meet compliance of regulatory bodies and government.*** Compliance is fundamental to being able to run a viable business. Every company must accept that compliance is a non-negotiable cost of doing business.
2. ***Prevent data breaches and deal with incidents swiftly.*** A data breach can hurt your customers, you partners, your employees and your business. Companies can ill afford to ignore cybersecurity. Insufficient data protection means lost customers, stakeholder trust, and could also result in multi-year penalties, fines and civil suits for years after a data breach occurs. Don't open yourself to becoming an albatross.

3. ***Implement Privacy by Design in Business Operations.*** Businesses that implement privacy protections will strengthen and grow their business become preferred by consumers over their competitors which do not provide such controls. A Pew report[4] found that it is important to 93% of Americans to have control over the entities and individuals who are allowed to get information about them, and 90% said that they want to control the specific types of information that was collected about them. These attitudes seem to be similar worldwide.
4. ***Keep your brand value and enhance it.*** According to a Forbes Insights report, 46% of organizations damaged their reputation as a result of a data privacy breach. Ponemon has also documented research that shows how impactful data breaches are in brand reputation.[5]
5. ***Differentiate your company and gain competitive advantage through "living trust" day in and day out.*** Since 2017, nearly 75% of US households have significant concerns about online privacy. The tide is turning as people switch to applications and companies who have strict cybersecurity controls in place, along with Privacy by Design (PbD) (see #3 above) rather than being exclusively driven by convenience. If you show you truly care about your customers', employees' and partners' privacy and protecting the information they have given you about themselves, you will have a tremendous advantage over companies that do not make privacy a priority or key value. According to 2021 Cisco Privacy Research, for every dollar that a company invests in data privacy, they realize a return of $2.70.

INTERPRETING YOUR SCORE

In this section, you can learn about the data protection score ranges and what they mean in terms of risk – business continuity, compliance and driving enterprise value.

Every organization has work to do in terms of meeting compliance continually. In addition to establishing a sustainable program, businesses also adjust and respond to new market conditions and enacted regulations and laws. As the adage goes, it's a journey, not a destination.

Building a foundational program from scratch typically takes between one and two years. Then companies maintain their program with a combination of internal teams, outsourced teams, monitoring and management platforms, and often leveraging firms that provide Privacy as a Service and a Data Protection Officer (DPO). Cybersecurity and data privacy are truly interdisciplinary efforts, requiring sponsorship and guidance from the board and executive team as well as expertise from IT, business units, including marketing, sales, customer service and product development, compliance, legal, operations and more.

If we think about compliance on a continuum, most organizations are somewhere in the middle. Highly regulated industries tend to have more mature compliance programs – for obvious reasons, i.e., no one wants to go to jail or pay a whopping fine – but know that there is no such thing as "perfect" compliance. Given the changing nature of business and regulatory landscape, we can count on uncovering new gaps that we must address as a company. What regulators look for is a company's commitment to compliance through demonstrated action and evidence.

Given the patchwork of US State laws and US Federal regulations and laws, companies have smartly invested in their data protection and cybersecurity programs and obtained one or more certifications, such as SOC2 or ISO27001. Though there is not certification for data privacy per se, many companies have adopted a comprehensive data privacy framework such as the EU's General Data Protection Regulation (GDPR), even if they are not subject to the GDPR. By doing so, these companies are able to not only comply with various jurisdictional compliance but capitalize on their customers' increased awareness and demand for better data privacy.

HIGH RISK – SCORE 0 - 19

If you scored between 0 and 19, your organization carries significant risk. That's the bad news. The good news is that you can mitigate risk fairly quickly by concentrating on a few priority tasks.

What to do now

If you don't have a cybersecurity program, start one. Choose a standard such as the Center for Internet Security (CIS) and start by building your security controls. Focus on CIS controls 1 through 6 and 13. You must implement the controls which means you have a working documented set of steps to demonstrate that each control is actually working. Remember that it is all about what you *actually* do, not what you say you do.

If you do have a nascent cybersecurity program, the next step is to adopt a standard and identify your risks and gaps. Prioritize them and get to work on a remediation plan.

High risk companies often do have a data privacy program even if they have some elements of operational cybersecurity. If this is your situation, start by mapping out where your prospects, customers, employees and partners reside and what data you process in serving these constituents. You may consider adopting the GDPR framework and add in known elements in US obligations, such as the two California laws, the current CCPA and the upcoming CPRA.

Use the Data Protection Readiness Checklist to guide you. You can download the checklist here: https://www.rethinkprivacy.com/data-protection-resources-for-businesses/ (or email me nalini@rethinkprivacy.com and I will send it to you).

Your first goal is to be able to answer yes to questions 13, 14, 15, 10 and 16. Once you have the foundational cybersecurity controls working, your next goal is to build out remaining cybersecurity and data privacy in your organization so that you can answer yes to each of the 20 questions in the checklist.

MEDIUM RISK – SCORE 20 - 34

If you scored between 20 and 34, your organization carries moderate to high risk. You have some areas that are working and that you can leverage. That's the good news. But you have work to do to shore up your programs and mature them over time. That's the not so good news. You have a bit of a head start from companies who haven't gotten their program in place yet and like the companies that scored high risk, you too can mitigate risk fairly quickly by doing a few key tasks.

What to do now

Since you either have a cybersecurity program in place or you are working at it, and you also a standard that your company has adopted, the next step is to perform an assessment or perhaps an internal audit. Identify your current risks and gaps, create your remediation plan and get going on closing the gaps.

You likely have some data privacy areas covered, for example, perhaps you have your data privacy standard, an initial Records of Processing Activities (ROPA) and Data Processing Agreements (DPA), but your ROPA is out of date, you haven't reviewed your Privacy Policy or public Privacy Notice within the last year or two.

Use the Data Protection Readiness Checklist to aid your brainstorming about the set of tasks you will tackle to shore up your data privacy program. You can download the checklist here: https://www.rethinkprivacy.com/data-protection-resources-for-businesses/ (or email me nalini@rethinkprivacy.com and I will send it to you).

The goal is to build your program so that you answer yes confidently to each of the 20 questions in the checklist.

LOW RISK – SCORE 35+

If you scored 35 or more, your organization is in great shape in terms of cybersecurity and data privacy. Though no organization can eliminate risk, you have a moderate to low level of risk and you have put sound tested strategies in place to manage and mitigate your risks on a continuous basis. That's quite a feat and congratulations!

In my experience spanning nearly three decades, I can count the number of companies that have reached this point on my hands.

Even though you have an amazing data protection program, you likely realize that you have a couple areas that could improve.

What to do now

Start by performing an internal review or audit of your cybersecurity controls. If you have obtained one or more IT security certifications, dig out those implementation plans and documentation from your cybersecurity certification process.

Next, review your data privacy program, starting with your Records of Processing Activities (ROPA), Data Processing Agreements (DPA) and Vendor Risk Management program. Review your systems where you process data and your prior Data Privacy Impact Assessments (DPIA). Imagine yourself as the M&A lead that wanted to buy your company or work with you on an IPO, what questions and documentation would you need to provide, what processes and controls need attention now?

Use the Data Protection Readiness Checklist to aid your brainstorming about the set of tasks you will tackle to shore up your data privacy program. You can download the checklist here: https://www.rethinkprivacy.com/data-protection-resources-for-businesses/ (or email me nalini@rethinkprivacy.com and I will send it to you).

The goal is to make sure your program is working well and that you answer yes confidently to each of the 20 questions in the checklist.

RESOURCES:

Visit rethinkprivacy.com/data-protection-resources-for-businesses/

- Detailed Data Protection Checklist
- Four Biggest Data Privacy Mistakes in Data Privacy Programs That Could You're your Business
- Schedule a complimentary Data Protection Strategy Session

Cybersecurity Frameworks

Center for Internet Security

https://www.cisecurity.org/

National Institute of Standards and Technology

https://www.nist.gov/cyberframework

Cybersecurity Frameworks Summary

https://cyberexperts.com/cybersecurity-frameworks/

Data Privacy Resources

https://www.gdpreu.org/

International Association of Privacy Professionals (IAPP)

https://iapp.org/

US State Comprehensive Privacy Law Comparison

https://iapp.org/resources/article/state-comparison-table/

Thank you for taking the time to assess your business in terms of data protection. I wish you continued success, wellbeing and prosperity.

Regards,
Nalini

Want to talk through your data protection needs?

Call 720-500-6674 and speak with Nalini to set up your strategy session.

Or book your session here:
https://app.harmonizely.com/nalini/dpconsult

About Nalini

Nalini C. Indorf Kaplan is blessed to pursue her passions of data privacy, digital ethics and clinical chaplaincy. Nalini has over 30 years of entrepreneurial experience and management consulting. She is also an ordained Rabbinic Chaplain and Spiritual Director through ALEPH, the Alliance of Jewish Renewal.

Nalini helps 7 and 8 figure business owners and CEOs build and manage their data privacy programs so that they not only comply with the law but lower risk, manage compliance and grow revenue even if they don't have the staff to run a program. She works with organizations on how to create and maintain trust, security and digital privacy. All in the service of growing sustainable businesses and organizations through meaningful relationships. For more information, visit ReThinkPrivacy.com.

[1] https://www.law.com/legaltechnews/2020/05/07/2020-data-privacy-trends-to-watch-in-ma/?slreturn=20210323115649
[2] https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html
[3] https://www.cisco.com/c/en/us/products/security/smb-security-outcomes-study.html
[4] https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/
[5] https://www.csoonline.com/article/3019283/does-a-data-breach-really-affect-your-firm-s-reputation.html