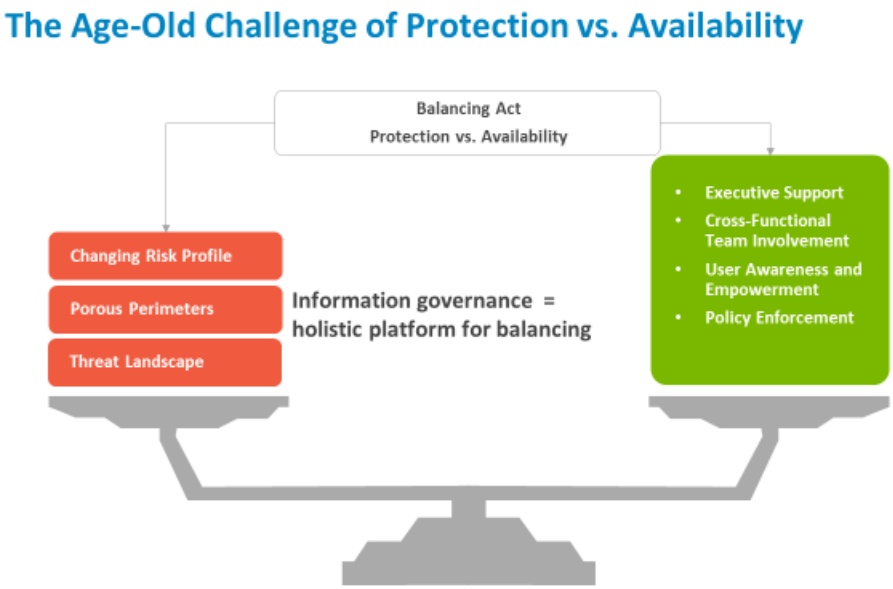
Cybersecurity: The Sky is Not Falling

by Deborah Butler, Esq.



This article is dedicated to Jason Baron, Esq., who suggested I write a blog after hearing these comments at a recent Today's General Counsel Institute in Atlanta, GA. Thank you Jason!

Deborah Butler, Esq. has built and led two global privacy programs (Unisys Corporation and Wyeth Pharmaceuticals, now Pfizer) as well as a global information governance program (Dell). She uses her business acumen from negotiating hundreds of complex commercial transactions to translate legal requirements to feasible business processes and to~~s well as~~ counsel business executives with the real-world consequences of information management decisions in mitigating information management risk and maximizing information value. One of her ~~my~~ mottos: "Compliance is good business."

No matter who wins an election, any election, information governance is a must-have for any data-driven business. For purposes of this conversation, let's define "information governance" as any and all activities involving and using data and, more specifically, the disciplines that have developed into organized activities, such as privacy, data security, e-discovery, business intelligence, data warehousing, CRM (customer relationship management) and Big Data/data analytics. And for data-driven companies, let's think about companies that are using data to drive, power and support their business models. From that perspective, that includes most, if not all, companies. Accordingly, for purposes of this conversation, let's target more intensive and extensive data-driven companies that rely on consumer behavior and preferences, such as ride-sharing and home-sharing companies, meal kit companies and online retailers as well as innovation companies that are relying on intellectual property and technology

to advance their business objectives. Indeed, developing innovative technology may very well be their business objective!

Having set this foundation, one of the key activities in any information governance framework is the protection of that data – commonly known as data security, data protection and even cybersecurity. We've heard lots of commentary that the sky is falling by reason of increasing (cyber) threats. I would submit that in spite of the increasing concern regarding safeguarding our data, the fundamental tension between protection and availability and between security and accessibility remains the same. We've been having this conversation since the advent of the Internet and we will continue it for as long as there's a need to have the right people access the right (amount of) data at the right time: i. In other words, for the foreseeable future. So, how do companies resolve this tension? By appropriately balancing security and availability. And those of you deep in the trenches of the CIA (Confidentiality, Integrity and Availability) triad of information security have , you've been working to balance this tension your entire careers. For all of us, this article is a kind of primer of how to begin to look at balancing increasing security threats, *no matter their future form*, against the critical success factors of appropriate data availability.

Starting with the protection factors, changing risk profiles is likely to be a constant part of a company's future. We've seen Google move from a search engine company to an innovation powerhouse whose activities range from developing wearables (e.g., Google Glass) to investing in Uber (ride-sharing company) and driverless cars. Taco Bell is moving from a take-out fast food fixture to a sit-down restaurant. Comcast has now partnered with its arch rival Netflix. We've seen it move from distributer of one kind of content to a multi-content house. All of the foregoing presented new risks for these companies. The important point, however, is that in order for these companies to grow and remain competitive they *chose* to assume these risks.

The same analysis applies to porous perimeters. Companies have chosen to permit their employees to access corporate networks and data from any device, anywhere on the planet. The days of exclusively "hard shell networks", "castle and moat" models, are fading. Employees are increasingly working remotely and not coming onsite to access their company's intranet. More importantly, the "consumerization of IT" or "reverse consumerization" – meaning that companies adopt what employees are using (e.g., Dropbox, social media – Facebook and Twitter) -- has upended the old model of employees adopting enterprise software. Consequently, companies need a way to ensure that employee preferences are appropriate (including safe) for the enterprise.

Last but not least, is the changing threat landscape. We used to have what many called "garden-variety" criminals: petty thieves stealing de minimis amounts of money. Now we have criminal enterprises devoted to stealing as much as possible. For example, if one person can steal a million credit card numbers and earn a $1.00 for each number in a few minutes, how attractive is that work? We now also have do-gooders, like Anonymous, who are stealing information to prove a point or share information they believe the world needs to know. To wit, the Ashley-Madison breach told us plenty of married people weren't being truthful about their personal relationships. Finally, we have nation-states, reportedly like North Korea involved in the Sony breach, perpetrating or supporting major security incidents, wholesale intellectual property thefts or releasing viruses into environments, such as the U.S. reportedly introducing the Stuxnet worm into Iran's nuclear development program.

So, what to do? Start thinking holistically. Safeguarding data is not just a technology problem. It's a multi-disciplinary undertaking that is not solved with a 6-month turnkey project. It is not a sprint; it's a marathon. It is a journey whose destination will have many stops but hopefully the stops will be less painful and disruptive because your company will have embraced the organizational change management necessary to prepare the company for a constant stream of threats. Risk mitigation need not be expensive, but it does need to be expansive. So take a deep breath, dive in and start with the four minimum critical success factors for securing your data:

1) Executive Support.
2) Cross-Functional Team Involvement.
3) User Awareness and Engagement.
4) Policy Enforcement.

Executive support is the most important requirement for sustainable change. Without it, "the flavor of the month" mentality prevails and the momentum generated for something new decreases precipitously. This isn't to say that grass roots efforts are without value. They are extremely helpful in socializing senior management on issues about which they may previously have been unaware. However, for long-term change, the Big Boss needs to support the initiative with whatever that support looks like in your company. (We'll talk about this (it's called culture) more below.)

Cross-company involvement is also key to any success in this area. The "usual suspects" of HR (for organizational change management), Legal (for compliance and regulatory guidance) and IT/Security (for information security technology) will, of course, be key players. The "missing link" is often the business people – the most important players on this team. The mission is to make the company's data safe(r) so that the business people can do their jobs. "Compliance" and business are not mutually exclusive. In fact, *Compliance means good business,* as we've learned from so many companies that did not comply. (Take a look at the FTC's website [insert link] for numerous examples.) Compliance is about revenue generation and revenue enhancement. Your mission, should you choose to accept it, is to help your business people, so make sure they are a part of your information security team. Find out what they'd like to do differently and build that into your design process. You will have a partner for life when you make a business person's job~~life~~ easier – help them reduce their cycle times, get their deals done faster and, most importantly, give them a conversation starter with, and a way to engage, their customers. Data security is top of mind for everyone so help your business people advise their customers that they can trust your company's data handling practices. Studies have shown that, without such~~that~~ trust, it is challenging, if not impossible, to build the strong, long-term relationships necessary to generate long-term profits.

User awareness and engagement is another important success factor. As noted above, information security is not just about technology. Information security involves people too. In fact, numerous pundits have declared that employees are the biggest security risk – not all the other threats that have been written about so extensively. This means that educating employees about their role in data protection is key. And education means more than a 20-minute annual training session. It means regular messaging and engagement about appropriate information management. And that means understanding *how* to engage your workforce, which means understanding your company's culture because "culture eats strategy for breakfast". (Peter Drucker) Therefore, you must engage your employees in a way that will resonate with them. And, returning to the note about executive support –

that support needs to be reflective or representative of that company's culture – in other words the type of support that will actually ~~"move the needle" –~~ positively and measurably change employees' behavior.

The fourth and final factor is **policy enforcement**. Because not all employees are motivated by carrots, some need ~~hammers or~~ sticks~~,~~. A ~~and a~~s Teddy Roosevelt used to say – "Speak softly, and carry a big stick." (Not my personal style, but necessary for some.) Therefore, a consequence management framework must be in place to help employees understand what happens if data isn't handled appropriately. Unfortunately, WIIFM ("what's in it for me") doesn't work for everyone. This framework should be built on metrics – whether compiled by external parties such as consultants, ~~or~~ internal audit or other "volunteers". (For example, I have found finance professionals to be extraordinarily helpful and very competent in this area.) Those metrics may also be leveraged~~helpful~~ for other purposes. Start with a baseline to be able to show progress. Be able to show stakeholders, such as (prospective) customers and regulators, that your company has a level of maturity in the information governance/information security space. Be able to show senior management that engaging management makes a difference in socializing the workforce. And it's also the place to start for "continuous improvement" – identifying the delta to continually refine the strategy for going forward.

In sum, the sky isn't falling. Information security risk can be mitigated reasonably, and that is all a company is required to do. A business need only address its security risk *reasonably* – based on its unique risk profile. Hopefully, this article helped highlight what companies need to consider in order to get started. I'm certainly happy to talk in more detail about this journey. Due to length constraints, we didn't cover a lot of ground, such as governance documents, governance networks, the role of technology and organizational change management methodologies. Nevertheless, "don't let the perfect be the enemy of the good". As the Chinese proverb proclaims, "A journey of a thousand miles begins with a single step". Good luck and thank you for listening!