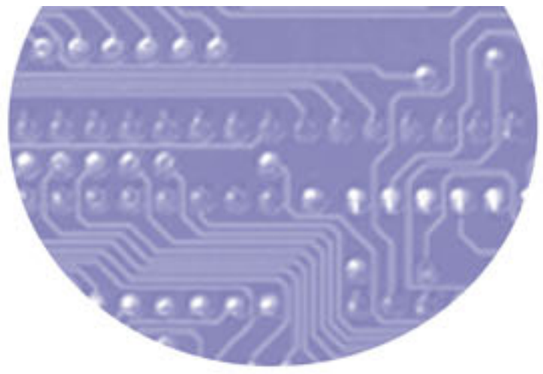

Wolters Kluwer

Wolters Kluwer
The Computer & Internet Lawyer
Distribution Center
7201 McKinney Circle
Frederick, MD 21704

TIMELY REPORT
Please Expedite

March/9900528922

Events of Note

March 1, 2017—
New York, NY:
"Counseling Clients in the Entertainment Industry 2017—Book Publishing; Current Developments in Entertainment and Sports Litigation; Film." For further information, please browse to *www.pli.edu*.

March 6–7, 2017—
San Francisco, CA:
"TechLaw Institute 2017: The Digital Evolution." For further information, please browse to *www.pli.edu*.

March 6–7, 2017—
New York, NY:
"Advanced Licensing Agreements 2017." For further information, please browse to *www.pli.edu*.

March 15, 2017—
New York, NY:
"Advanced Trademark Law 2017: Current Issues." For further information, please browse to *www.pli.edu*.

March 16, 2017—
New York, NY:
"Advanced Copyright Law 2017: Current Issues." For further information, please browse to *www.pli.edu*.

March 17, 2017—
New York, NY:
"Ethics in Social Media 2017." For further information, please browse to *www.pli.edu*.

March 29–30, 2017—
New York, NY:
"TechLaw Institute 2017: The Digital Evolution." For further information, please browse to *www.pli.edu*.

March 20–21, 2017—
Santa Monica, CA:
"2017 Intellectual Property Institute at USC." For further information, please browse to *http://weblaw.usc.edu/why/academics/cle/ip/assets/docs/IPIbrochure.pdf*.

What We Talk about When We Talk about "Reasonable Cybersecurity": A Proactive and Adaptive Approach

By Kevin L. Miller

Data breaches have become so commonplace that only the truly far-reaching events seem to get noticed anymore. However, a recent breach that exposed the data of 6.4 million children, in what experts called the largest known hack affecting youngsters,[1] even got the attention of the US Congress.[2] On November 14, 2015, VTech, "the global leader in electronic learning products from infancy to preschool and the world's largest manufacturer of cordless phones," was hacked.[3] The stolen data included the children's names, gender, and birthdates, as well as the mailing addresses and email addresses of their parents, secret questions and answers for password retrieval, IP addresses, and download history.[4] There was enough information in the breach that complete family profiles could be reconstructed. Also exposed were the kids' photos, audio recordings, and chat logs gathered by "Kid Connect," a service that allows parents with a smartphone app to chat with their kids via a VTech tablet.[5] The logs, pictures, and recordings could be traced back to specific usernames, allowing those possessing the hacked data to identify the people chatting and being shown in the photos.[6] The hacker who perpetrated the attack anonymously disclosed to a reporter, "Frankly, it makes me sick that I was able to get all this stuff."[7]

The hacker gained access with an "SQL-injection" attack, a well-known way of using rogue database query language to bypass security and allow free access to the information inside.[8] An analysis by Troy Hunt, a cybersecurity expert, revealed that VTech had failed to enact even the most basic of security measures, including failing to secure the data in transit with basic SSL (Secure Sockets Layer) encryption, storing security questions and answers in unencrypted plaintext, and failing to enhance password "hashes" by "salting."[9] All of these measures have been standard practice in systems security for at least a decade.[10] "It's taken me not much more than a cursory review of publicly observable behaviours [*sic*] to identify serious shortcomings," Hunt wrote.[11]

The VTech hack demands our attention not only for the sensitivity of its victims, but also because VTech's example so sharply contrasts with reasonable conduct and good practice. Studying VTech's experiences and choices can provide organizations and their counsel with valuable insights about how they *should* be approaching cyber risk. This article provides an overview of the cybersecurity legal framework and advocates for a proactive and adaptive approach to managing cyber risk that transcends today's reactive paradigm.

Legal and Regulatory Framework of Cybersecurity

The current US legal framework for cybersecurity is a patchwork, consisting of a number of overlapping federal standards aimed at regulated entities in various sectors, state cyber breach notification laws, state statutes, and case law arising from consumers' actions against companies. Despite the lack of a comprehensive standard, a requirement for organizations to implement affirmative cybersecurity practices has arisen as a result of the body of administrative law stemming from Federal Trade Commission (FTC) enforcement actions. Although the FTC lacks any specific statutory authority to regulate cybersecurity policy, it has repeatedly used its broad § 5 authority to prohibit "unfair or deceptive acts or practices in or affecting commerce" to enforce data protection standards against companies.[12]

A "deceptive" act is a representation or omission that is likely to mislead a consumer into using a product or service.[13] In the context of cybersecurity, when an organization claims in its Web site security policy that it "adequately secures data" but then fails to implement good cybersecurity practices, it has committed a deceptive act subject to FTC action.[14] The agency also may

Kevin L. Miller is a shareholder at Labyrinth Law PLLC, *http://www.labyrinthlaw.com*, where he is an intellectual property, patent, and technology law attorney. His practice focuses on cybersecurity, privacy, and other legal issues arising from cutting-edge technologies. Before becoming an attorney, he was a software engineer and architect for several major technology companies and an adjunct professor of computer science. He also is the author of several articles on cybersecurity and privacy issues and a book on software development design techniques. This article was originally published in the September-October 2016 issue of *The Florida Bar Journal*, Vol. 90, No. 8, and is reprinted with permission and modifications.

interpret the existence or lack of a given cybersecurity practice as "unfair" when it causes, or is likely to cause, injury to consumers.[15] In contrast to the "deceptive practices" standard, the organization does not need to have represented itself to consumers as having adequate data security.[16] Moreover, no actual cyber breach needs to have occurred for an FTC action under either standard.[17]

Despite the lack of a comprehensive standard, a requirement for organizations to implement affirmative cybersecurity practices has arisen as a result of the body of administrative law stemming from Federal Trade Commission enforcement actions.

Although the precise boundaries of the FTC's authority are unsettled, during the course of approximately 100 cases the agency has established an evolving conception of "reasonable cybersecurity" in general commerce.[18] Further, the FTC has been less than sympathetic with organizations that allege "reasonable cybersecurity practice" is too amorphous a standard for guidance. Indeed, at a panel discussion on cybersecurity issues on March 9, 2016, FTC Commissioner Terrell McSweeny expressed incredulity that organizations continue to claim that "reasonable security" is an ambiguous term.[19] Guidelines for implementing reasonable security processes are "all over our website," said Commissioner McSweeny. "It means having a process, appointing responsible people for implementing the process, providing training, and so on .... Companies not making any attempts at reasonable security measures are doing so at their own risk."[20] The risk to which Commissioner McSweeny refers is the legal and regulatory risk of FTC audit and enforcement activities.[21]

Regulated Sectors

In addition to the FTC baseline oversight applicable to general commerce, many business sectors have individualized practices, standards, and regulatory bodies. In some cases, these define a rigid compliance framework to which businesses in that sector will be held accountable by overseeing regulatory agencies. In other cases, the practices and guidelines are not rigidly enforced or audited, but instead frame the understanding of reasonable cybersecurity practice for that sector. Although each of the individual regulatory agencies has its own enforcement personnel and objectives, most have a "reasonable cybersecurity" standard and interpret that standard in light of the practices and guidelines applicable to that sector.

The individual practices and guidance of each agency are too numerous and complex to comprehensively discuss in this article, but a few examples are illustrative. The Federal Communications Commission (FCC) has powers similar to the FTC's to regulate broadcasters and common carriers under § 222 for their treatment of customer data.[22] The FCC recently previewed new draft broadband privacy rules that would extend the requirements for minimum security processes and consumer data breach notification to Internet service providers.[23] The Commodity Futures Trading Commission (CFTC) broadly requires reasonably designed cybersecurity practices for companies operating in the financial markets, and has drafted numerous guidelines relating to the security of transaction data and consumer personal and financial information.[24] The CFTC chair views cybersecurity as "the primary risk to financial markets."[25] The Consumer Financial Protection Bureau (CFPB) enforced a consent order and $100,000 civil monetary penalty against Dwolla, Inc., an online payment platform.[26] Among other things, Dwolla claimed, but failed, to comply with payment card industry (PCI) standards.[27] This example shows that the CFPB is willing both to interpret and enforce external industry standards when regulated entities are deceptive about compliance. Dwolla also failed to encrypt even the most sensitive customer data, including bank account information and Social Security numbers, contradicting its claim to encrypt and store securely 100 percent of consumers' information.[28] The consent order mandated that Dwolla obtain outside auditing for a period of five years to ensure compliance with "procedures and standards generally accepted in the profession."[29]

State Law

Cyber breach notification laws now exist in 47 states.[30] In general, these laws require companies to notify consumers when their "personal information" is divulged during a cyber breach, though the laws vary in details such as the timing and method for notification.[31] On July 1, 2014 in Florida, for example, the Florida Information Protection Act (FIPA)[32] replaced and strengthened the prior cyber breach notification law.[33] Florida's law is relatively unique and progressive in several aspects. For instance, Florida expands the meaning of "personal information" from items such as Social Security and financial account numbers to include user names, email addresses, and security questions/answers, recognizing that this information may be used to compromise multiple online accounts.[34] Florida requires notification to the state attorney general when more

than 500 individuals in Florida have been affected by the cyber breach, even when a "risk of harm" exception can be invoked to avoid notifying the affected individuals themselves.[35] The new law also permits the Florida attorney general to request copies of forensic reports, breach plans and policies, and other information from organizations when necessary.[36] The Florida law retains the previous statute's provision of monetary penalties for failure to notify within the required 30-day period.[37]

Notification laws in other states also have become more stringent. Until recently, most state statutes made available an exemption or "safe harbor" from notification requirements when the stolen data was encrypted.[38] As of July 1, 2016, Tennessee is the first state to remove the literal encryption safe harbor from its cyber breach notification statute.[39] Although Tennessee still allows companies to perform a "risk of harm" analysis that may exempt them from notification requirements, Tennessee's new law recognizes that encryption is not a panacea, especially when outdated or flawed encryption protocols were used or the encryption key was compromised. California also has amended its cyber breach notification law to eliminate the safe harbor for encryption as of January 1, 2017.[40]

Several states, including Florida, Connecticut, and California, also have been active in devising forward-looking approaches to enforcement. The recent Florida statute now includes a "reasonable cybersecurity"-like standard, requiring organizations to "take reasonable measures to protect and secure data in electronic form containing personal information."[41] Connecticut requires a publicly-posted privacy policy.[42] Like the FTC and other federal agencies, Connecticut is willing to bring enforcement actions even when no data breach has occurred.[43] Connecticut also works closely with federal agencies to bring coordinated enforcement actions.[44] Further, the California Attorney General's Office issued its "Data Breach Report 2012-2015," outlining businesses' responsibilities to protect personal information and report data breaches.[45] The report states that, "failure to implement *all* the [Center for Internet Security's Critical Security controls] that apply to an organization's environment constitutes a *lack of reasonable security*" under the state's information security statute.[46]

Other Initiatives

Other forms of guidance, such as those promoted by industry groups or related to the nature, origin, or target of the data itself, can shape the meaning of "reasonable cybersecurity" over time. For instance, federal statutes mandate a variety of restrictions on how the data of children and students must be treated regardless of the operative business sector. The Children's Online Privacy Protection Act (COPPA) regulates the collection and storage of data for children ages 13 and under.[47] The Family Educational Rights and Privacy Act governs educational privacy.[48] Adding an additional layer of complexity, Common Sense Media, a non-profit policy group, recently announced a privacy evaluation initiative to conduct compliance reviews of education technology companies with respect to federal law and guidance from the Department of Education's "Model Terms of Service."[49] In some cases, international law can even come into play; for example, the European Union General Data Protection Regulation (GDPR) mandates a separate and rather onerous set of restrictions on companies that store, possess, or use the data of individuals residing in the EU member states.[50]

Late in 2015, Congress passed the Cybersecurity Information Sharing Act (CISA), which establishes a statutory framework to encourage the voluntary sharing of cybersecurity information between companies and the government.[51] Among other things, CISA offers liability protection for companies that share cyber-threat info via a Department of Homeland Security Portal.[52] The hope is that the portal will increase cooperation between companies in identifying and stopping new cyber-threats. It is not far-fetched to think that, although information sharing is voluntary, a time is coming in the near future when keeping up-to-date on known threats using cybersecurity information portals may become an established part of reasonable cybersecurity practice.

Proactive vs. Reactive Cybersecurity

The near-ubiquity of state cyber breach notification laws is testament to the practically universal belief that organizations should notify individuals when hackers steal their data. This bare statutory duty has in some cases disoriented companies with respect to their deeper legal obligations under a reasonable cybersecurity standard. Companies have become quite adept at enacting incident response plans to notify customers and relevant agencies, offer affected individuals a year of credit monitoring, and hire cyber-defense contractors to review and secure their data systems after the fact. However, such plans are directed at what to do after one's defenses have failed, rather than implementing reasonable cybersecurity to avoid problems. To analogize, in hurricane-prone Florida it would be the difference between a disaster preparedness plan that included a family meeting point, a list of what to load in the car before evacuation, and the insurance policy details, as opposed to a plan that includes installing storm windows, extra strapping on the house to tie the roof, frame, and foundation together, cleaning the gutters, and solving those pesky drainage problems.

It is clear from the foregoing discussion that an organization has affirmative responsibilities to protect key customer data, and that the notion of reasonable security is shaped by and evolves with technology, regulatory guidelines, and common practices in a business sector. These responsibilities, and the company's burden to implement a process that adapts to changing practice over time, must be proactive, rather than reactive, at its core. As Troy Hunt wrote during the aftermath of the VTech hack, "Despite the frequency of these incidents, companies are just not getting the message; taking security seriously is something you need to do before a data breach, not something you say afterwards to placate people."[53]

An organization has affirmative responsibilities to protect key customer data, and that the notion of reasonable security is shaped by and evolves with technology, regulatory guidelines, and common practices in a business sector.

A "Reasonable Cybersecurity" Process

What might a proactive plan for reasonable cybersecurity look like? To begin to answer that question, consider Massachusetts. The state requires that companies storing or using personal information about a state resident develop a written information security plan (WISP) for protecting the data.[54] The Massachusetts regulations mandate such sensible computer security protocols as: (1) user authentication and access controls (*i.e.*, having user accounts with passwords and restricting access to electronic data to individuals who reasonably need it); (2) encryption of data when it travels across public networks or resides on portable devices; (3) changing vendor-default passwords; (4) monitoring systems for unauthorized access; and (5) keeping malware detection software reasonably up-to-date.[55] The regulations also require employee training and minimum yearly audits of the security measures.[56]

Clearly, such preparations transcend the act of creating (and posting on the company Web site) a "privacy and security policy" intended to assure customers that "only the highest grade of encryption is used" and "we never share your data with anyone," etc. WISP-like plans may deal with certain very basic security threats at the time the plan is drafted, and for some organizations eliminating such already well-known weaknesses can be a huge leap forward. A WISP might have prevented the real-life FTC enforcement actions against companies for storing data for longer than necessary, failing to encrypt data,[57] and failing to have proper access controls.[58]

However, a company can comply with WISP regulations and still fall short of true preparation. Little in Massachusetts' WISP regulation suggests a process by which VTech could have identified and known about the SQL-injection attack that compromised its systems, even though such attacks have been a known weakness for more than a decade. Yet, basic security errors such as these drive the security community crazy and severely damage a company's reputation. Such errors also can result in FTC enforcement actions; at least one case has been brought by the FTC for a company's failure to provide protection from known security threats (SQL injection) in code libraries.[59] However current VTech's systems might have been at the time they were created, they failed to acknowledge or adapt to changing cyberthreats. Writing about the VTech breach, Troy Hunt said: "There's a sense of systems from a bygone era … you get the distinct sense that VTech's [IT] assets were created a long time ago and then just … left there."[60]

Security by Design

What is important to an organization is not necessarily what is on the plan today, but whether it is positioned to continuously identify and mitigate new types of risks and react to new legal standards. Most organizations have a mixture of technologies and data systems to secure, so effective cybersecurity needs to account for a range of issues, from operations, configuration, and maintenance of third-party products, to patching "open source" code libraries embedded in custom software, to securely designing new custom software capabilities. Optimally, cybersecurity is integrated into the design phase of a data system or technology and serves as an opportunity to introduce security and privacy by design, as well as good "data ethics."

Effective cybersecurity needs to account for a range of issues, from operations, configuration, and maintenance of third-party products, to patching "open source" code libraries embedded in custom software, to securely designing new custom software capabilities.

Achieving security by design means involving business units and legal counsel at important checkpoints during conversations about system architecture. Such checkpoints have traditionally not been part of a development

team's process, but are increasingly necessary to combat today's cybersecurity risk. To assist in the development of cross-functional process teams, the National Institute of Science and Technology (NIST) has constructed a "Cybersecurity Framework" that aims to help an organization "align its cybersecurity activities with its business requirements, risk tolerances, and resources."[61] The framework is meant to be applicable to a wide range of sectors and is intended to be used by an organization to create (or enhance) its individualized processes adapted from sector-specific guidelines. For organizations just starting to grapple with cybersecurity compliance processes, the NIST framework can be used as a template for creating a new, adaptive cybersecurity process.

Business units need to be involved to help ensure that the data being collected is reasonably related to the objective of the product or service in the marketplace. An organization needs to know why it is gathering each piece of information it collects; who it is gathering the information from, where it is stored (*e.g.*, locally on the device or in the cloud); what it is to be used for in both the short and long term; how long the organization needs to retain it; and with what entities the company shares the data. Doing this effectively requires a dialogue among IT, business units, and legal counsel, and likely involves senior management and board oversight to frame these questions in the context of current and future business goals.

Left to their own devices to design a data model for a new system, data architects naturally gravitate toward systems that maximally inter-relate data with the least redundancy, a design principle called "normalization." Loosely speaking, the goal of normalization is a system in which any given data entity can be related to any other.[62] Just as many companies would have done, VTech designed a normalized data structure that easily cross-linked children, parents, and other collected data and metadata. When a hacker was able to compromise VTech's relational database with an SQL-injection attack, VTech's databases yielded its secrets in all their clear, optimized, and interrelated glory.[63] This allowed the hacker to see the complete picture of familial relationships and attributes with very little effort.

This data model efficiently served the purposes of VTech's IT department, but was independent of any tangible business objective and almost certainly did not factor in the very real legal and reputational risk of compromising the privacy and security of children. Had a reasonable cybersecurity process been followed, a conversation with the legal department might have quickly revealed the requirements of COPPA. Stakeholders with other perspectives might have inquired whether videos and chat logs needed to be stored "in the cloud" rather than remaining on the local device. This single decision transformed the company's risk dramatically—from little or no liability to massive liability for compromising the privacy and security of millions of children and adults.

Following a rational process to link business objectives and risks to data system design has a related benefit to consumer privacy and the organization's cyber risk; it naturally steers the organization toward the "principle of least data."[64] Lacking any outside direction, IT sometimes takes the perspective that almost any data that can be gathered should be—an extension of Parkinson's Law: "Data expands to fill the available storage space." This happens because IT, lacking knowledge of a long-term strategy for a product line, over-gathers data "just in case." This natural IT instinct has been further exacerbated in recent years by low-cost, scalable data storage and the rise of "big data analytics," which promises to transform massive, loosely-related, and often unstructured data-sets into "business intelligence" using predictive algorithms to see unanticipated relationships between data.[65]

However, every piece of data collected carries a burden and a responsibility. For example, many companies take the unreflective, default stance of building a customer login profile and storing all the customer's card and personal data for even the simplest one-time transaction. Because PCI standards dictate that stored credit card information (such as card numbers, expiration dates, and CVV codes) be encrypted, storing it carries some risk.[66] A company can identify the business drivers behind storing credit card data by asking relevant questions, such as:

- Does the business need the card number for a single charge?
- Is it offering a service that has recurring monthly charges of the same amount?
- Is it storing the data for convenience to the customer in returning to the online store?
- Is this a convenience that the customer actually *wants,* or does it deter some customers?
- Is the business storing the data to preserve information for accounting or auditing purposes?
- Does the business value of storing all this information exceed the risk if the systems are compromised?

A process that identifies and prioritizes business objectives and risks, the applicable legal frameworks, and applies those metrics to each unit of data being stored

has a much better chance of reducing the risk of a cyber breach.

New Risks: The Internet of Things

Concern for the security and privacy of user information is no longer confined just to what users deliberately share with companies over Web sites or in the course of purchase transactions. New forms of data, collected from new kinds of devices, have altered the landscape dramatically in recent years. Loosely categorized as the "Internet of Things," or "IoT," devices are as far-ranging as smart thermostats for adaptively controlling home climate control systems, Internet-accessible door locks, fitness bracelets that track vital statistics over time and provide health assessments, pacemakers that can be remotely configured, and connected automobiles. To perform their functions, these devices gather, store, and transmit vast quantities of passive data that is capable of exposing sensitive facts about users such as health status (*e.g.*, high blood pressure, pregnancy), location, and habits. In some cases, this information is actively biometric (*e.g.*, fingerprints, facial recognition, retinal pattern) or quasi-biometric (*e.g.*, resting heart rate; breathing patterns; walking speed and cadence; even the force, pattern, and speed of a "swipe" motion on a touch device). A compromise of biometric data carries with it a new level of risk, because biometric data is—unlike passwords—generally immutable; once lost, a fingerprint is lost forever and can no longer be reliably used as an access control mechanism for devices.

Companies are being called upon, with increasing insistence, to treat this data responsibly. In January 2015, the FTC issued its "IoT Privacy and Security Report."[67] The Report reiterated the agency's position that reasonable security should be incorporated into IoT devices, even while acknowledging that the principle of least data (or "data minimization") may be difficult to apply in devices that use machine learning algorithms to make predictions from large quantities of passively-gathered historical data.[68] Industry groups such as the Biometrics Institute have formed to encourage responsible use of biometric data by vendors who incorporate active or quasi-biometric capabilities into their products. The group has released biometrics privacy guidelines to offer best practices to organizations for protecting biometric data and complying with regulatory principles.[69] Moreover, a consortium of consumer privacy and children's privacy groups filed an FTC complaint on December 6, 2016, against Genesis Toys and Nuance Communications, Inc., for a range of violations of COPPA and § 5 of the FTC Act for failure to implement reasonable cybersecurity measures in several Internet-connected toys.[70]

The risks of poor cybersecurity in IoT devices can go beyond loss of the personal data of the device owner. In mid-September 2016, one of the most powerful distributed denial-of-service (DDoS) attacks to date was launched by a botnet named "Mirai" that was constructed from insecure IoT devices.[71] Mirai seeks out IoT devices that are still using their factory-default passwords, takes control of the devices with new firmware, and converts them into zombie machines for launching the DDoS attacks to bring down Web sites across the Internet.[72] Since the attacks, two US Senators have written a letter to the FTC urging it to use its authority to force IoT manufacturers to improve the security of their devices.[73]

Good Cybersecurity Is Good Business

Cyberbreaches cost companies worldwide an average of $4 million per incident in direct losses.[74] And, the associated reputational risk may be far worse than the direct costs, if the reaction of parents and security personnel to the VTech hack are any indicator. Around 44 percent of consumers claim that it is impossible for a company to win back their confidence after it has lost their personal data.[75] That may be why cybersecurity is *the* top concern of 70 percent of public company directors, according to a recent survey.[76]

Around 44 percent of consumers claim that it is impossible for a company to win back their confidence after it has lost their personal data.

Providing potential customers with good security and privacy can have an indirect benefit on the bottom line, as well. Most people have had the experience of changing their minds about buying a product because something in the check-out process made them feel uneasy about the transaction. In fact, surveys show that approximately 17 percent of online transactions are abandoned during check-out due to concerns about payment security.[77] Increasingly, an effective arrow in a company's marketing quiver is its ability to communicate respect for customer data and good data privacy ethics. When the company openly and accurately (not falsely!) describes its cybersecurity philosophy and measures, and shows the consumer a professional approach, its ability to close the sale can only improve.

An effective process also advances an organization's ability to work with outside partners. Cybersecurity insurance carriers, for instance, have become increasingly rigorous and sophisticated with their requirements; to

be insurable at a cost-effective rate (or at all), companies are being asked to provide detailed information about their cyber risk management programs. Insurers also are carving out coverage exclusions for risky behaviors. In addition, working with third parties as a service provider, or even becoming party to a merger, acquisition, or joint venture becomes much easier with an effective cybersecurity process. Practically every good business transaction agreement today has substantial cybersecurity-related representations and diligence requirements. This issue often is overlooked by companies until the deal gets tanked because one side realizes during its diligence that the other side is clueless about cybersecurity and exposes them to massive risk. This outcome is a real tragedy in an age when a majority of new startup companies' "exit strategy" hinges on being acquired by a larger entity.

Conclusion

The technological and regulatory landscape of cybersecurity and data privacy is complex and difficult to navigate, with a number of players, standards, and objectives that are sometimes in tension with one another. The only way for organizations to keep up with it is not to form a static policy, but a dynamic process that is capable of adapting to changing technology and incorporating ongoing changes in guidance. The days are rapidly coming to a close, if not gone already, when reasonable cybersecurity practice does not include security by design development models and a proactive process for seeking out and combating ongoing cyberthreats. In this new environment, legal counsel should strive to work with organizations proactively, as an integrated part of the process team, rather than merely *after* a breach occurs.

Notes

1. FAQ About Cyber Attack on VTech Learning Lodge, VTech.com, *https://www.vtech.com/en/press_release/2016/faq-about-cyber-attack-on-vtech-learning-lodge/* (last updated Mar. 17, 2016).
2. Press Release, Senator Ed Markey, Sen. Markey and Rep. Barton to VTech: How Do You Protect Children's Information? (Dec. 2, 2015) (available at *http://www.markey.senate.gov/news/press-releases/sen-markey-and-rep-barton-to-vtech-how-do-you-protect-childrens-information*).
3. Corporate Profile, VTech.com, *https://www.vtech.com/en/about-us/* (last accessed Mar. 25, 2016); FAQ, *supra* n. 1.
4. Troy Hunt, "When Children Are Breached—Inside the Massive VTech Hack," *Troyhunt.com*, Nov. 28, 2015, *http://www.troyhunt.com/2015/11/when-children-are-breached-inside.html*.
5. Lorenzo Franceschi-Bicchierai, "Hacker Obtained Children's Headshots and Chatlogs From Toymaker VTech," *Motherboard*, Nov. 30, 2015, *http://motherboard.vice.com/en_us/read/hacker-obtained-childrens-headshots-and-chatlogs-from-toymaker-vtech*.
6. *Id.*
7. *Id.*
8. Hunt, *supra* n. 4.
9. *Id.*
10. *See, e.g.*, Christoph Wille, "Storing Passwords—done right!," *AspHeute.com*, Jan. 5, 2004, *http://www.aspheute.com/english/20040105.asp*. However, salted passwords have been in use in UNIX systems since the 1970s.
11. Hunt, *supra* n. 4.
12. 15 U.S.C. § 45.
13. *Id.*
14. *See, e.g.*, Petco Animal Supplies, No. 032-3221 [F.T.C. May 5, 2005].
15. *See, e.g.*, FTC v. Neovi, Inc., 604 F.3d 1150, 1156 (9th Cir. 2010).
16. *See id.*; *see also* 15 U.S.C. § 45(n).
17. *See, e.g.*, Guess?, Inc., No. 022-3260 [F.T.C. Aug. 5, 2003].
18. *See* Data Security, FTC.gov, *https://www.ftc.gov/datasecurity* (last accessed Mar. 27, 2016).
19. Terrell McSweeny, Comm'r. of the Fed. Trade Comm'n., Address at Cybersecurity for a New America 2016 Conference (Mar. 9, 2016).
20. *Id.*
21. *Id.*
22. 47 U.S.C. § 222.
23. News Release, Fed. Communications Comm'n, Chairman Wheeler's Proposal to Give Broadband Consumers Increased Choice, Transparency & Security with Respect to Their Data (Mar. 10, 2016) (available at *http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0310/DOC-338159A1.pdf*).
24. *See, e.g.*, System Safeguards Testing Requirements for Derivatives Clearing Organizations, 80 Fed. Reg. 80113 (Dec. 23, 2015) (to be codified at 17 C.F.R. pt. 39); System Safeguards Testing Requirements, 80 Fed. Reg. 80139 (Dec. 23, 2015) (to be codified at 17 C.F.R. pts. 37, 38, 49).
25. System Safeguards Testing Requirements for Derivatives Clearing Organizations, 80 Fed. Reg. at 80137.
26. *See* In the Matter of Dwolla, Inc., No. 2016-CFPB-0007 (C.F.P.B. Mar. 2, 2016), available at *http://files.consumerfinance.gov/f/201603_cfpb_consent-order-dwolla-inc.pdf*.
27. *Id.* at ¶ 20 and 27.
28. *Id.* at ¶ 27.
29. *Id.* at ¶ 52.c.x.
30. *See* Security Breach Notification Laws, Nat'l Conference of State Legislatures, *http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx* (last updated Jan. 4, 2016).
31. *Id.*
32. Fla. Stat. § 501.171.
33. Fla. Stat. § 817.5681.
34. Fla. Stat. § 501.171(1)(g).