BIG PHISH AND CYBERSECURITY

JEREMY D. RUCKER, *Dallas*
Spencer Fane, LLP

Co-author:
SHAWN E. TUMA, *Plano*
Spencer Fane, LLP

State Bar of Texas
36TH TEXAS FORUM: THE POWER OF THREE
FIRM, CORPORATE, AND GOVERNMENT PERSPECTIVES FOR PARALEGALS & ATTORNEYS
March 29, 2019
Austin

CHAPTER 8

JEREMY D. RUCKER

Cybersecurity & Data Privacy Attorney

214.459.5880

jrucker@spencerfane.com

www.jeremydrucker.com

BIOGRAPHICAL INFORMATION

EDUCATION

Texas A&M University School of Law, JD, 2016

UNIVERSITY OF TEXAS AT ARLINGTON, B.B.A. Management, 2011, *Summa Cum Laude*

Jeremy is an attorney in the Dallas office of Spencer Fane, LLP and focuses his practice on cybersecurity and data privacy protection. With experience handling numerous cybersecurity and data privacy protection issues, and exposure to various transactional and litigation issues, Jeremy has a breadth of experience needed to ensure client needs are thoroughly and efficiently met.

RECENT PRESENTATIONS AND PUBLICATIONS

- Protecting People: Can you Identify and Protect Your Very Attacked Persons?, SecureWorld, 2019
- Privileges: Understanding the Applicability in Cybersecurity Cases, Texas Bar Journal, October 2018
- “The Legal Perspective of a Data Breach,” ISACA North Texas Chapter
- “Cybersecurity,” State Bar of Texas Advanced Civil Trial (San Antonio), TexasBarCLE
- So You’ve Had a Breach. Now What?, Risky Business, Information Systems Security Association
- Cybersecurity Update (co-presenter), Collin County Bench Bar 2018, Collin County Bar Association
- Planning for a Cyber Breach, DALL’s 2018 Spring Institute, Dallas Association of Law Librarians
- What Every Lawyer Needs to Know About Cybersecurity, Plano Bar Association, PBA CLE
- Cybersecurity Overview, Civil Litigation/Appellate Section, Collin County Bar Association CLE
- Cybersecurity for Solos and Small Firms, Solo/Small Firm Section, Collin County Bar Association CLE
- I’ve Been Hacked: What Do I Do Now?, Essentials of Business Law: Protecting Your Business, TexasBarCLE
- Transactional Practice of Law, Business Law Panel, Texas A&M Business Law Society, October 2017
- Cybersecurity and Data Breach Issues: An Overview, TAPS 2017 Seminar, Paralegal Division-State Bar of Texas

SHAWN E. TUMA

Cybersecurity & Data Privacy Attorney

972.324.0317

stuma@spencerfane.com

www.shawnetuma.com

BIOGRAPHICAL INFORMATION

EDUCATION

Regent University School of Law, JD, 1999, *Magna Cum Laude*

Northwestern State University, BA, 1994, *with Honors*

PROFESSIONAL ACTIVITIES

- *Practitioner Editor*, Bloomberg BNA Texas Privacy & Data Security Law
- *Board of Advisors*, University of North Texas Cyber Forensics Lab
- Board of Directors & General Counsel, Cyber Future Foundation
- *Policy Council*, National Technology Security Coalition
- *Cybersecurity Task Force*, Intelligent Transportation Society of America
- Cybersecurity & Data Privacy Law Trailblazer, National Law Journal (2016)
- Texas SuperLawyers – Top 100 Dallas / Fort Worth (2016)
- D Magazine Best Lawyers in Dallas (2014 – 2016)
- Texas SuperLawyers (2015-16)
- *Secretary*, Computer and Technology Section, State Bar of Texas
- *Board*, Collin County Bench Bar Conference
- *Past-Chair*, Collin County Bar Association Civil Litigation & Appellate Section
- College of the State Bar of Texas
- Privacy and Data Security Committee of the State Bar of Texas
- North Texas Crime Commission, Cybercrime Committee
- InfraGard (FBI)
- Information Systems Security Association (ISSA)
- International Association of Privacy Professionals (IAPP)
- *Contributor*, SecureWorld
- *Editor*, Cybersecurity Business Law Blog

Shawn is an accomplished author with several published works on various legal-technology topics. He is a frequent speaker on business cyber risk issues such as cybersecurity, computer fraud, and data privacy law.

Shawn's presentations and publications are available here: https://shawnetuma.com/about-the-author/presentations-publications/

TABLE OF CONTENTS

BIG PHISH AND CYBERSECURITY

I. EXPERIENCED LEGAL COUNSEL HAS ESSENTIAL ROLE IN MANAGING CYBER RISK

Companies are beginning to understand that cyber is an overall business risk, not just a technical issue. Now they must realize that cyber is also a legal issue. The easiest way to understand why is to ask these two questions: “Why do we know about the data breaches of Target, Yahoo, Equifax, and all the others?” “Did those companies air their dirty laundry just because they believed it was the right thing to do?”

Of course not! They did so because laws and regulations made them. Those laws and regulations require companies to disclose their breaches and mandate things such as who they must notify, when and how they must notify, what must be communicated, and what must be done for those who were impacted. As these rules demonstrate, having data creates risk and one of legal counsel’s roles is to help companies manage that risk.

A. Real world experience for assessing and managing risk.

To effectively manage cyber risk, companies must understand what their real cyber risk is because they cannot manage that which they do not know or understand. The process of assessing a company’s overall cyber risk is one of the most crucial step in the risk management process. It is the foundation.

Attorneys who have substantial experience in dealing with cyber risk enables them to better understand how to manage cyber risk, including legal and regulatory liability that leads to significant risk in this environment. Think about this: How many cyber incidents or data breaches has your company’s information technology, security, and management teams been through or even observed firsthand?

Counsel with many years of experience serving as a “breach guide” or “breach quarterback,” leading companies through the cyber incident and data breach response process, will have been involved in hundreds or thousands of cyber incidents and data breaches. This real-world experience is invaluable for helping companies understand the real-world risks they now face. Without such practical experience, companies are more likely to spend their resources chasing some of the hyped-up threats that make the best sales pitches, conference talks, and news headlines—it isn’t always the most exotic and sophisticated attacks that cause the most problems.

Diving deeper, such counsel will have a unique perspective on the most common attack tactics that have been used in the past and that are currently being used against certain types and sizes of companies, in certain industries, with certain types of data and business models, and in certain markets. They will also understand the types of attacks that are most likely to lead to *reportable* data breaches. They will have a better understanding of the laws and regulations applicable to the jurisdictions in which the companies operate and what they require in terms of securing information, disclosing breaches of such information, and the all-important question of distinguishing between a *non-reportable* incident and a *reportable* data breach, a subtle yet bet-the-company distinction.

Deeper still, by calling on their history of cases they will have a unique understanding of those things that companies did right and those things that were ineffective or led to problems. Because no two are alike, this insight provides a deeper understanding of what caused many cyber incidents, how they happened, and what could have prevented them. Once an incident has occurred, the focus shifts to an understanding of what companies did right or wrong, or could have done but did not do, that may have improved the response and better mitigated the situation. Finally, it enables them to uniquely understand the true harm to companies that such cyber incidents cause, from the initial panic, administrative burden and confusion, and disruption of operations, to the loss of business opportunities due to the companies being focused on the incident, to the better-known harms like the costs of remediation and incident response, negative publicity, and the decrease in business value and stock prices.

When working with companies on their cyber risk management programs, one of the most frequently asked questions is, “how do you prioritize the steps in your strategic action plan?” Because companies can’t “boil the ocean” (i.e., fix every problem) and companies do not have unlimited resources to throw at this problem, they must be able to evaluate the risks and develop a strategic action plan that prioritizes those things that should be done first. There is a lot more to consider than the traditional risk formula of “risk = probability x loss” because there are important business factors that must be considered. When evaluating how to prioritize the actions to take, the analysis translates into something more akin to “risk = probability x loss x time to implement x impact on the business and resources x benefits - hindrance.” To work through an analysis such as this requires not only drawing on real-world experience to understand the most likely risks companies face, but also requires having an understanding of the overall business, its operational needs, the practicalities of the business environment, and the many competing interests that must be considered. Analysis of such complexities is an essential skill for legal counsel.

With cyber risk, even the most extensive and effective risk management programs cannot come with guarantee. The problem is not a static problem that can be solved, rather, it involves an active adversary that is continuously evolving its strategy and tactics to find more effective ways of attacking and exploiting its intended victims. And, as with security in general, the company must get it right 100% of the time and the attacker needs only one lucky shot. Because of this, when it comes to legal and regulatory liability, the question is usually not as simple as "did the company have a data breach?" but is more like, "before the company had the data breach, was it taking reasonable measures to protect its network and data to keep from having a data breach?" Well-documented evidence of its diligence can go a long way.

B. There is no substitute for experienced legal counsel in managing cyber risk.

In today's business environment, cyber is unquestionably a legal issue and experienced legal must be integrally involved in helping companies manage their cyber risk.

II. CYBERSECURITY FUNDAMENTALS FOR ALL ORGANIZATIONS

A. Introduction.

The threat to information is ubiquitous. Cybersecurity and protecting information are issues that evoke equal parts of fear and confusion for business leaders, information technology and security professionals, and the legal professionals they rely on for advice. Anyone who has been involved in a real data breach will easily understand why an effective analogy for describing cybersecurity incidents is to imagine being in a building that is on fire. There is panic, there is fear, there is chaos, there is confusion. It is a crisis situation.

What could be worse? Not only could it have been your company's information that was compromised in the cybersecurity incident, but it could have been your customers' most sensitive information—or your biggest customer's customers' most sensitive information—all but ensuring that biggest customer becomes a former customer. These situations will be discussed in more depth in future sections.

1. The Most Important Point of this Guide: All Companies Must Have Adequate Cybersecurity Defenses.

Protecting company data requires taking the same precautions that are taken for protecting any other kind of data. Whether the attackers are after employee social security numbers, customer payment card data, embarrassing emails from the CEO, the company's crown jewel trade secrets, or highly sensitive client data, the central objective is to prevent the attackers from being able to access it. Attackers that are going to try and access this data are going to do so by trying to attack the company itself. If they are unsuccessful at attacking the company directly, they will likely try gaining access through a third-party by first attacking a third-party with whom the company does business and then using that access point to pivot inside the company. This is why third-party risk is now a key focus in cybersecurity.

Accordingly, the most important point to remember is that if you want to protect your company's data from cyber attackers, you must first ensure that your company is adequately protected. Second, you must ensure that those third-parties with whom your company does business are adequately protected.

While a discussion of highly sophisticated cybersecurity tools and tactics may be more entertaining, if the goal is to improve companies' cybersecurity defenses effectively, it must begin with the basics which will be the focus of this guide.

B. The Impact of Cybersecurity Law.

1. Cybersecurity is a Legal Issue.

The laws that govern what must be done in response to a cybersecurity incident or data breach are not optional. The author discussed these laws and the legal duties associated with these events, reporting these events to law enforcement, and disclosing them to government regulators in the *Guide to Reporting Cybersecurity Incidents to Law Enforcement and Governmental Agencies* ("*Reporting Guide*").[1] When there is a duty, as explained in the *Reporting Guide*, in most cases the duty is mandatory.

There is a grave misunderstanding among many business leaders who believe that when their company has had a data breach, notifying the affected individuals and appropriate governmental agencies is optional. Unfortunately, the author encounters this on a regular basis. This problem is perpetuated by there being far too many lawyers who do not practice in the cybersecurity and privacy area of law and, out of ignorance, advise such clients that it is really not that serious and is being blown out of proportion. This advice is wrong and should qualify as malpractice.

If you need further convincing, ask yourself whether you believe that companies like Target, Home Depot, Neiman Marcus, Spec's, Ashley Madison, and Yahoo aired their dirty laundry publicly solely because they believed it was the right thing to do. They had to—cybersecurity is a legal issue—the laws require companies to disclose this information

[1] Shawn E. Tuma, *Guide to Reporting Cybersecurity Incidents to Law Enforcement and Governmental Agencies*, BUSINESS CYBERSECURITY LAW, (Dec. 4, 2016), https://shawnetuma.com/cyber-law-resources/guide-reporting-cybersecurity-incidents-law-enforcement-governmental-regulatory-agencies/

and mandate how they disclose it, when they disclose it, what information they disclose, what they do for those affected, and to whom it must be disclosed. If you find your company in this position and fail comply with these legal duties, you do so at your peril and their peril.

2. The Conundrum of Cybersecurity Law Schizophrenia.

One reason cybersecurity engenders so much fear is because of how uniquely this area of law, policy, and public perception treat organizations that have experienced data breaches. This is one of the few, if not only, situations where the victim of an illegal act is transformed into the wrongdoer. In the more typical scenario, an organization is attacked by an illegal act or, at a minimum an impermissible act, directed against its computer network. The wrongful act against the organization's network causes harm to the organization. At that point in time, however, the organization then begins to be viewed as the wrongdoer when the focus of the blame shifts to the organization for allowing itself to succumb to the attack.

Unauthorized access to computers, often referred to as "hacking," and data breach are two sides of the same coin and more often than not the organization is blamed for both. What is even more unfortunate is that companies' primary legal vehicle for protecting against these kinds of misuses of their computer networks are the unauthorized access laws, primarily the federal Computer Fraud and Abuse Act[2] (CFAA) and the Texas' Breach of Computer Security[3] (BCS) law, and there is a growing movement among those in the "no limit" crowd and "security research" crowd that seeks to substantially limit companies' abilities to use these laws in most cases, especially those in which the misuse is by privileged users (insiders) which accounts for over 70% of all data breaches. This legal schizophrenia puts companies dead center in a conundrum in which there is no upside. Cybersecurity can be scary but it becomes far more dangerous when ignored.

C. Understanding the Basics of Cybersecurity and Cyberattacks.

1. What are the Objectives?

You cannot effectively fight against something that you do not understand. If you want to be effective in defending your company against cyberattacks, you must have a better understanding of what cybersecurity entails. To understand the objectives of cybersecurity we must understand what we are trying to protect against and that encompasses many things. First, what kind of activities are we trying to protect against? Second, what kinds of data are we trying to protect? Third, what kinds of attack vectors are we trying to protect? Fourth, what is the most challenging aspect of all – the evolving nature of cyberattacks?

2. The Activities We Are Protecting Against: The Cia of Cybersecurity.

When they hear the words *data breach*, people usually think of situations where cybercriminals removed data from a network such as in the well-publicized Target, Home Depot, and Neiman Marcus cases. While stolen data certainly constitutes a data breach and a cybersecurity incident, those situations can exist when data is not stolen (commonly referred to as exfiltrated). One of the fundamental principles of cybersecurity is often referred to as "the CIA of security":

> Almost from its inception, the goals of computer security have been threefold: confidentiality, integrity, and availability—the "CIA" of security. *Confidentiality* ensures that only those individuals who have the authority to view a piece of information may do so. No unauthorized individual should ever be able to view data to which they are not entitled. *Integrity* is a related concept but deals with the modification of data. Only authorized individuals should be able to change or delete information. The goal of *availability* is to ensure that the data, or the system itself, is available for use when the unauthorized use or once it.
>
> As a result of the increased use of networks for commerce, to additional security goals have been added to the original three in the CIA of security. *Authentication* deals with insuring that an individual is who he claims to be. The need for authentication in an online banking transaction, for example, is obvious. Related to this is *nonrepudiation*, which deals with the ability to verify that a message has been sent and received so that the sender (or receiver) cannot refute sending (or receiving) the information.[4]

[2] Computer Fraud and Abuse Act of 1986, Pub. L. No. 99–474, 100 Stat. 1213 (codified at 18 U.S.C. § 1030 (2008)).

[3] TEX. PENAL CODE § 33.02. Texas' Breach of Computer Security is a criminal law that has a civil cause of action if the conduct constituting the violation was committed knowingly or intentionally, which is Chapter 143 of the Texas Civil Practice and Remedies Code, titled the Harmful Access by Computer Act (HACA). *See* TEX. CIV. PRAC. & REM. CODE § 143.001.

[4] Greg White, COMPTIA SECURITY+, p. 7 (3rd Ed. 2011).

> What this means is that the objective of cybersecurity must focus on protecting the confidentiality, integrity, and availability of information and making sure that it is authentic and can be verified as such.

3. Who Are the Attackers?

While not always an "attacker" in the sense that they have the requisite intent to be a "bad guy," the reality is, the biggest threat to most organizations' data comes from their own people. People are the weakest link when it comes to protecting information.

a. Internal Threats*.*

Statistics show that the vast majority of organizations' information that is improperly disclosed or taken is done so by people within the organization—insiders. Internal threats can be either accidental or intentional.

(1) Accidental Internal Threats.

First, there are those people who are careless, negligent, or poorly trained and do things that accidentally lead to a disclosure of confidential organization information. This often happens by clicking on email links, social media, or websites that are spear phishing attacks. Other times it is through simply talking too much and trusting others when they should not, whether at cocktail parties or in response to direct social engineering attacks. Finally, it can be losing a smart phone, leaving a thumb-drive, or losing a laptop with confidential information.

(2) Intentional Internal Threats.

Intentional internal threats come from an insider in your organization who intentionally takes organization information which leads to its disclosure or use against you. A few of the reasons why they may do this is because they:

- contributed to the development of the information and believe they have a right to it
- want to keep a memoir of their work
- want to keep a copy for ideas in the future
- plan to use it to compete against you in the future
- have some ownership in the business and believe they have a right to it

Others may, with the best of intentions, store the information on personal devices or accounts while working for your organization but later, once no longer working there, re-discover the information and decide to use or disclose it at that time.

Regardless of the reason, recent studies show that more than 60% of the insiders who leave an organization take confidential information with them—oftentimes sensitive information—and many plan to use it to compete against the organization. In these situations, these insiders' activities may violate both the federal and Texas unauthorized access laws which provide for criminal and civil remedies.[5]

(3) Warning: Insider Taking Information May Trigger Organization Data Breach.

What is worse is, when they do this, they trigger a data breach by the organization from whom they are taking it. The Texas data breach notification law is titled *Notification Required Following Breach of Security of Computerized Data*,[6] and provides as follows:

> (b) A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information <u>shall disclose any breach of system security</u>, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, <u>acquired by an unauthorized person</u>. The disclosure shall be made as quickly as possible, except as provided by Subsection (d) or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

[5] For a more in-depth discussion of these laws as they apply to insider misuse, see, Shawn E. Tuma, *Federal Computer Fraud and Abuse Act and Texas Computer Crime Statutes*, (June 17, 2016), http://www.slideshare.net/shawnetuma/federal-computer-fraud-and-abuse-act-and-texas-computer-crime-statutes

[6] TEXAS BUS. & COMM. CODE § 521.053 (emphasis added).

The law defines "breach of system security" as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data."

What this means is that, when sensitive personal information (SPI) is entrusted to an organization and is protected within the confines of the organization, accessible only by its employees who are under an obligation to maintain the confidentiality of such information, it is considered legally "secure." However, when an employee leaves his or her employment and takes that data with him or her, outside of the legal confines and security of the organization's network and without that continuing duty of confidentiality of the organization, that is now an "unauthorized acquisition … [that] compromises the security, confidentiality, or integrity of" the SPI and constitutes a data breach. This is certainly not a popular way of viewing the law but the author believes it is accurate.

b. External Threats.

External threats can be either random or targeted.

(1) Random External Threats.

Random attacks can occur when your information is taken as part of bigger criminal scheme such as a burglary in which files, data and equipment are stolen.

Random attacks are also how we would describe many hacking attacks, where hackers steal data from organizations without having any idea of what the data actually is and not knowing its value. A hacker's goal is to penetrate your organizations' computer system and then establish a connection between your system and theirs to use for exfiltrating data from your computer system. The data is usually packaged with other random data and sold in bulk on the black market (the Dark Net) much the way banks package bad debt to sell to debt collectors. The data is sold based on volume, not the value of its content, which is why your organization's data is just as valuable as anyone else's for most random hacking attacks.

(2) Targeted External Threats.

Targeted external threats are those situations where someone who is not a part of your organization specifically sets about to steal your organization's information. An example of this could be a burglar specifically targeting your organization but, in reality, people have found that it is far more efficient to commit crimes using computers than crowbars. More often than not, when your business has information that someone else wants, they will take it with a smartphone camera, video, or directly through your computer system—not a busted-out window. This is most common in corporate espionage cases where a competitor seeks to steal your organization's information but does not have someone on the inside to assist.

c. Blended Targeted Threats.

Common threats in today's highly-competitive business environment are blended targeted threats.

(1) Departing Insider Leaving for a Competitor.

The most common scenario is when an employee of your business is planning to go work for one of your competitors. Before resigning and while still in a position to have access to your organization's valuable information, that employee begins taking information and giving it to your competitor to undermine your organization and give an unfair advantage to his future employer.

(2) Disloyal Insider Planted for Corporate Espionage.

A less common, but more egregious situation is where a competitor has a disloyal employee (or contractor, member of cleaning crew, housemaid, etc.) planted as a trusted insider within your business (or home) and that person stays there, continuously providing a point of access to your computer system or directly exfiltrating your valuable information to the competitor over an extended period of time. The bigger problem with this is, when you are dealing with information, you cannot see it disappearing as you can with physical assets being stolen, and it can go on for years undetected. This is a classic example of corporate espionage. Not only are private businesses involved in this type of espionage but there are also many foreign state-sponsored corporate espionage operations directed toward American businesses.

4. <u>What Kinds of Data Are We Trying to Protect?</u>

Cybercriminals attack businesses to attempt to gain access to many different kinds of data that the organization has, or has access to, that it may not even realize it has. The obvious starting point is the organization's own company data but beyond that, organizations usually have their workforce's data and customer and client data. From there, they often have data belonging to third parties that it may have collected through its work including that of its third-party business associates that could prove to be very valuable. These are just some examples of the data that businesses must protect from cybercriminals.

Virtually every business has some form of intellectual property, that is, something unique or remarkable about the way it makes a product or provides a service that sets it apart from the competition. This is something that gives it a competitive advantage and is usually something it has spent significant time and resources to develop, many times in the form of trade secrets. Unfortunately, in today’s business environment, honor and integrity are not always the rule and many businesses find their intellectual property is being taken and used to compete against them. When considering the data that needs to be protected, businesses should pay special attention to their intellectual property.

5. What Are the Attack Vectors We Are Trying to Protect?

Cybercriminals will use any means of attacking a business that they can find. The most direct means of attack is against the company’s network through vulnerabilities that can be found by what some like to refer to as “security research” which, many times is legitimate, but many times is not. Attackers will attempt to gain access into the company’s network by focusing on its website, email system, company owned and BYOD devices that employees use as well as portable devices such as infected USB drives to gain an entry point into the network.

In some cases they may use sophisticated GSM / mobile telephone type devices to exfiltrate data from the network outside of the firewall or intrusion detection or intrusion prevention systems. They may also infect websites of third-parties that they know company insiders will visit so that, upon visiting the sites, the company insiders will then download the malware into the company’s network.

Speaking of third-parties, third-party risk or, what is often referred to as supply chain risk management (SCRM), is now one of the hottest trends in cybersecurity. And, for good reason. What we have learned is that the more a company prepares its own defenses and hardens itself against cyberattack, the more the attackers evolve their techniques by doing things such as using vulnerable third-parties with a connection to the intended target to be the vehicle that facilitates their attack.

6. The Most Challenging Aspect of All—the Evolving Nature of Attacks.

Have you heard of the national retailer that what was hit with a perfectly timed cyberattack on Black Friday ’13 that resulted in credit card data from roughly 110 million customers being taken? The company is Target. Target, however, was not attacked directly. Cyber criminals launched an email spear phishing campaign at Fazio Mechanical Services — Target’s third-party HVAC vendor — and someone at Fazio opened the email, clicked on the link giving the criminals access to their system where they sniffed around until they found the login credentials that Fazio used to log into Target’s vendor portal, which they then used to gain access into Target’s computer system.

a. Sun Tzu on Cybersecurity.

The lessons of Target, Fazio, and third-party attacks go back to the great Sun Tzu on Cybersecurity:

- “In all fighting the direct method may be used for joining battle, but indirect methods will be needed to secure victory.”
- “You can be sure of succeeding in your attacks if you attack places which are not defended.”
- “The spot where we intend to fight must not be made known; for then the enemy will have to prepare against a possible attack at several different points; and his forces being thus distributed in many directions, the numbers we shall have to face at any given point will be proportionately few.”

Most businesses focus their energy on securing their own networks but focus very little on examining the networks of their business associates and other third parties that they allow to access their networks.

Around 500 B.C. Sun Tzu taught that if an enemy — a cyber criminal — wants to attack your company’s computer network, they would be wise to do so by attacking indirectly, such as through your company’s business associates and other third-parties who have access to your network. Cyber criminals may be a lot of things, but they are not dumb … the successful ones, anyway.

Combatting the unique and unprecedented nature of business cyber risks is the essence of cybersecurity. Cyber risks are continuous and evolving, therefore, cybersecurity must also be a continuous process that is always evolving to anticipate and defend against the threats. This work is never done. Such is the nature of cybersecurity. When defending against cyber risks, there are known-knowns that we can prepare for and there are unknown-knowns that we can learn about and then prepare for. But, there are also unknown-unknowns that do not even exist at this moment but that are quickly becoming unknown-knowns. These are the real challenge but that is where it is most evident that cybersecurity is not a science, it is an art.

D. Examples of Attacks.

1. The Stuxnet Attack.

Exfiltrating data is not the only way a bad actor does can cause harm. Consider the effectiveness of the Stuxnet malware. Delivered by an employee who could not resist the temptation to pick up a free (infected) USB drive left in the parking lot of an otherwise secure facility, once inserted into the network, the malware covertly made its way to the computer program running the Siemens industrial control systems that it was designed to attack. Once there, it subtly increased the speed at which the supersonic uranium-enrichment plant centrifuges operated so that they would tear themselves apart.[7] The sophisticated Stuxnet was designed to then eliminate all traces of its existence from the network, leaving investigators with no clue as to what caused the problem.[8]

Does this state-sponsored cyberattack sound too fantastic to happen to companies in the business world?

2. The German Steel Mill Attack.

In 2014, a German steel mill was the target of a sophisticated cyberattack in which hackers surreptitiously attacked and took control of the production management software for the steel mill, took over most of the plant's control systems and caused substantial material damage to the physical site. That is, they altered the *integrity* of the software data. While this may sound like the plot of a James Bond movie, the reality is, the intrusion into the steel mill's network was not terribly complicated. In fact, it started with a basic spear phishing email:

> In other words, hackers send fraudulent emails seemingly coming from sources that were well-known or reliable to the recipient, which usually encourage the recipient to open an attached document or visit a website containing a malware. In this case it was an attached file. Once the file was opened the malware was injected into the sales software of the plant. From there, it made its way through the network while damaging numerous systems and industrial automation components.[9]

While attacks like Stuxnet and the German steel mill can now easily be carried out by non-state actors, they do not have to be. Do you think countries like China, Iran, North Korea, and Russia are not directing their cyber-based industrial espionage activities toward companies in the United States?

3. The Sony Attack.

Sony would certainly beg to differ after the November 24, 2014 when the North Koreans attacked with malware that spread from computer to computer erasing everything stored on 3,262 of the company's 6,797 personal computers and 837 of its 1,555 servers topped off with a deleting algorithm that overwrote the data seven different ways so that nothing could be recovered.[10] To make matters worse, not only did the attackers destroy Sony's data, but they had also stolen it before they began that phase of the campaign:

> Over the next three weeks they dumped nine batches of confidential files onto public file-sharing sites: everything from unfinished movie scripts and mortifying emails to salary lists and more than 47,000 Social Security numbers. Five Sony films, four of them unreleased, were leaked to piracy websites for free viewing. Then the hackers threatened a 9/11-style attack against theaters, prompting Sony to abandon The Interview's Christmas release.[11]

The attackers destroyed Sony's data (*availability*), exfiltrated sensitive data of Sony's employees (*confidentiality*), exfiltrated highly valuable intellectual property (*confidentiality*) and obtained a trove of highly-confidential and embarrassing emails from Sony's executives that gave rise to one of the first examples of *shame hacking*, that is, using

[7] *See* David Kushner, *The Real Story of Stuxnet*, IEEE SPECTRUM (Feb. 26, 2013), http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

[8] See Shawn E. Tuma, What Does CFAA Mean and Why Should I Care?" A Primer on the Computer Fraud and Abuse Act for Civil Litigators, 63 S.C. L. REV. 141, 145 (2011).

[9] *Cyberattack On A German Steel-Mill*, Sentryo (May 31, 2016), https://www.sentryo.net/cyberattack-on-a-german-steel-mill/

[10] Peter Elkind, *Inside the Hack of the Century*, FORTUNE (June 25, 2015), http://fortune.com/sony-hack-part-1/

[11] Id.

hacked data for embarrassing or extorting people by threatening to expose such compromising data if they do not comply with the demands made of them.[12]

4. Ashley Madison, Brazzers, and Adult Friend Finder Attacks.

We have been observing an evolution in hackers' tactics from going after data that could be directly monetized, such as payment card data, to going after data that can be monetized indirectly through extortion, such as the Ashley Madison data. The hack of Brazzers porn site is similar to the Ashley Madison hack in that the real opportunity for monetization lies not in the intrinsic value of the data itself, but in the opportunity to use the data to embarrass and extort others into paying money to keep it secret.

The Brazzers data dump from the hackers includes email addresses, user names and passwords spelled out in plain text,[13] which can certainly lead to embarrassment for those who would not want their spouses, significant others, co-workers, employers, employees, parents, children, pastors, congregation, or constituents to know they are members of such a site. But, it gets worse. This wasn't just a porn site, it was a forum that porn fans used for discussing their favorite porn scenes, favorite performers, and their own fantasies.[14]

5. The Lessons to Be Learned from Each of These Attacks.

a. Sophisticated attacks are often by non-state actors.

Do you think that only state actors like those involved in Stuxnet or the Sony attack have the capability to execute such cyberattacks? The code for the Stuxnet malware made its way into the cyber-wild and has been modified and used by private actors many times. Information on how to carry out similar attacks, even if to a somewhat lesser degree, is readily available on YouTube—and certainly the Dark Web, where one can also purchase the actual tools needed to carry out the attack.

b. Cyber attacks are used to destroy physical assets.

The Stuxnet and German steel mill attacks both demonstrate how effectively cyber attacks can be at destroying physical assets. For the former, it was uranium enrichment centrifuges and the latter was manufacturing equipment.

c. Cyber attacks are used to destroy data by making it inaccessible to its owners.

The North Korean cyber attack on Sony demonstrates that these attacks are oftentimes carried out to make information inaccessible, not just to steal information. In this example, the attackers installed malware with a deleting algorithm that overwrote the data seven different ways so that nothing could be recovered. Clearly their intention was to cause substantial harm, not just steal data.

d. Cyber attacks are used for "shame hacking"—i.e., using sensitive information for extortion or embarrassment.

The Sony case also demonstrates that cyber attacks are used for obtaining sensitive data that may not be intrinsically valuable but can be used for extortion or embarrassment if it is revealed. In the Sony case, the hackers released its Executives' information from their email folders and all of the personally and professionally embarrassing email conversations they had exchanged.

In the Ashley Madison, Brazzers, and Adult Friend Finder breaches we saw a similar form of *shame hacking*. In those cases the hackers obtained information about who were members of the services and their sexual preferences and fantasies, such information not being intrinsically valuable, however, of the nature that would cause tremendous embarrassment to those individuals should such information become public. Because of this, after obtaining the information the hackers tried to monetize it by making extortion demands on the companies.

One more timely example of this could be that of a well-known politician whose campaign chair fell for a simple Gmail phishing attack that led to the revelation of sensitive embarrassing emails that were revealed to the public during the campaign.[15] While it makes many people feel better to say this was the product of a sophisticated state-sponsored cyber attack orchestrated by the Russians, the reality is, even an amateur lone hacker is capable of carrying out an email phishing campaign.

[12] Shawn E. Tuma, *David Beckham's Exposed Emails Exemplify Shame Hacking Threat*, BUSINESS CYBERSECURITY LAW, (Feb. 6, 2017), https://shawnetuma.com/2017/02/06/david-beckhams-exposed-emails-exemplifies-shame-hacking-threat/

[13] *Brazzers porn account holders exposed by hackers*, BBC, (Sept. 6, 2016), http://www.bbc.com/news/technology-37285715

[14] Id.

[15] Ben Gilbert, *Hillary Clinton's campaign got hacked by falling for the oldest trick in the book*, BUSINESS INSIDER, (Oct. 31, 2016), http://www.businessinsider.com/hillary-clinton-campaign-john-podesta-got-hacked-by-phishing-2016-10

e. Humans are the weakest link and social engineering is the most common means of attack regardless of sophistication.

The most important point to realize is one that is rarely emphasized about both the Stuxnet and German steel mill attacks, which are considered to be truly sophisticated attacks, is that social engineering was the entry point for those attacks and is far and away the most common avenue of attack for all cyberattacks.

Social engineering is, generally speaking, using deception to trick people into doing dumb things.[16] With Stuxnet, it was picking up a USB drive from the parking lot and plugging it into a secure network environment. In the German steel mill case, it was clicking on a file that was included with a phishing email. For Target, it was the clerical employee working at Fazio that clicked on the link in the phishing email. For the politician, it was the campaign chair responding to a phishing email by entering his account login credentials to a fake site designed to collect such information.

The problem with all of this is, while many businesses (and others, like politicians) claim they have been victimized by the super sophisticated "unprecedented" exotic, real, James Bond-like hacking attacks, the legitimate ones are rare. The vast majority of the cybersecurity incidents businesses experience are because of much simpler things like lost USB drives, stolen laptops, or highly-effective phishing scams.[17] Here are a few excerpts of Verizon's well-respected *2016 Data Breach Investigations Report*[18] that confirm that businesses that spend their resources addressing the basics will be focusing on a significant part of the cybersecurity problem:

- "Phishing has continued to trend upward ... and is found in the most opportunistic attacks as well as the sophisticated nation-state tomfoolery." (p. 12)
- "The majority of phishing cases feature phishing as a means to install persistent malware." (p. 21)
- "63% of confirmed data breaches involved weak, default or stolen passwords." (p. 24)

The point of this discussion is not to say that businesses do not need advanced cybersecurity defenses—they certainly do—but they must not neglect the basics. Businesses that want to improve their cybersecurity must focus on how to defend against the threat of social engineering and the most effective way to do that is by training their employees to recognize social engineering attempts and resist the temptation to fall for them.

E. Real Cybersecurity That Companies Need to Protect Themselves and Their Digital Assets.

The following is a non-exhaustive list of critical cybersecurity measures that companies must implement in order to improve their cybersecurity defenses. A checklist of these measures is included in Section IV. There are many more that should be considered, however, these points are discussed here because many times they are overlooked and not addressed in many traditional "cybersecurity defenses" discussions in favor of the more exotic, sophisticated, and expensive defenses.

1. Leadership to Foster a Culture of Security.

Companies must not only obtain "buy in" by firm leadership but must also have leadership so committed to cybersecurity that they are the leaders in establishing and fostering a culture of security.

A compelling meme recently circulated on LinkedIn which depicted two scenes. The first had 3 people pulling a block labeled "business" and on top of the block was an individual sitting at a desk pointing forward. The person sitting on the business, at the desk, was labeled "boss." In the second, 4 individuals were now pulling the business and no one was sitting on it. In this, the person in front was labeled "leader."[19]

Within any organization, the culture always starts at the top in works its way down. When it comes to establishing a culture of cybersecurity this principle remains true. Moreover, when it comes to lapses in cybersecurity in many cases the company executives are the first to fail. Oftentimes this is because they believe they do not need to abide by the same policies and procedures that are imposed on the employees and they have themselves exempted from them, not understanding that they to need the protections of those policies and procedures.

2. Strategy Such That Someone Always Understands the Big Picture.

The cybersecurity industry has become a FUD (fear, uncertainty, doubt) inspired, gadget driven space where each day someone is anxious to sell others on why their new product or service is the latest-greatest solution to solve all

[16] Shawn E. Tuma, *1 Step to Improve Your Company's Cybersecurity Today*, BUSINESS CYBERSECURITY LAW, (Apr. 25, 2016), https://shawnetuma.com/2016/04/25/1-step-to-improve-your-companys-cybersecurity-today/

[17] Id.

[18] *2016 Data Breach Investigations Report*, Verizon, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

[19] Boss v. Leader Meme, http://www.thememesfactory.com/boss-vs-leader/

your company's cybersecurity worries. And, they are always "DOD approved"! The problem is, while everybody is touting their own preferred solution and businesses are buying one here, one there, and another over there, there is rarely anyone who is standing back looking at the big picture to see if all of the security gaps are being filled, how well the solutions play with each other (or whether they counteract each other), and whether anybody even knows how to work it all. Most organizations are missing a head coach and they desperately need one to establish and understand the overall strategy and make sure it is executed.

3. Strong Physical Security Is Essential for Strong Cybersecurity.

Cybersecurity and physical security are inextricably intertwined such that you cannot have adequate cybersecurity without adequate physical security. Many cybersecurity incidents are caused by lost or stolen devices, such as laptops, mobile phones, USB drives, and even servers being stolen from locations such as office buildings. Unless such devices are properly encrypted, each of those thefts are data breaches for the organization from which they were stolen.

Beyond that, however, one of the first steps that cybercriminals take when launching a cyber-attack is to try and gain physical access to the computer network infrastructure of the adversary which makes it much easier to install malware, key loggers, credential sniffers, or even GSM devices to exfiltrate information outside of the organization's network firewall and data loss prevention systems. Many times, such access is available because the organization does not have their physical facilities adequately secured and has their critical network components stored in a location that is easily accessible. In other cases, however, they do attempt to protect against physical access but the hackers are creative and will do things such as use social engineering to pretend they are part of IT maintenance or a copier, telephone, or other type of repairman to gain such assess. At other times they will do things such as "tail gate" kind and helpful employees through secured entrances that require credentials to enter. Or, they may recruit members of the janitorial service that services the facilities and use their access to gain entry.

4. Strong Cybersecurity Focuses First on the Basics.

In the past, the following measures were recommended for companies and their employees because it was generally understood that they were the ones with access to your company's data and networks. As previously discussed, however, third parties have become a primary vector of attack and in many cases, third parties also have access to your company's data and networks for various purposes. Accordingly, where appropriate and possible, the measures that are recommended for within your company are also recommended for any third parties that have such access. The objective, after all, is to focus on and protect the data and network—wherever it may be and however it may be accessed.

a. Policies and Procedures.
b. Training of All Employees.
c. Phish All Employees (Especially Executives).
d. Password Policies.
e. Security Questions.
f. Signature Based Antivirus / Malware Detection.
g. Multi Factor Authentication.
h. Backups Segmented from the Network

Close your eyes and envision this scenario: Your company CIO calls and tells you that someone just clicked on a link in a phishing email and now all of the company's (or firm's) network has been encrypted with ransomware and the attackers are demanding a $50,000 Bitcoin payment to provide the decryption keys and if it is not paid within 72 hours, the decryption keys and the data will be destroyed forever.

This is a very real scenario and at this time is one of the most common methods of successful cyberattack on a global scale. You could try and pay the ransom but there are several problems with that (in addition to the FBI publicly discouraging it):

- First, you are relying on there being honor among thieves and trusting that the attackers will honor their word if you pay the ransom. Some of these criminals are known for upping the demand after receiving their first payment.
- Second, do you even know how or where to get $50,000 in Bitcoin?
- Third, can you even get $50,000 in Bitcoin within 72 hours (it is very difficult)?
- Fourth, do you have the ability to spend $50,000 on this anyway?
- Fifth, assuming you can comply and actually pay it, if they provide the decryption keys and the data is decrypted, will you be back up and running as though it never happened? The author has had one client describe this situation

as purchasing a brand-new Cadillac and while driving it home from the dealership having a collision that totals out the car such that it is in thousands of pieces then taking those pieces to the nearest "shade tree mechanic" and asking that person to put it back together—that is what your network will "run" like after being decrypted assuming all else goes well.

- Finally, assuming you are willing to pay $50,000 to support and encourage more criminal activity, actually do pay the ransom and can get back up and running, the cybercriminals now know that you have money and are willing to pay up. Do you think you are now safe from future attack? In many cases, they will have latent malware in your network that will open the door to a future attack. Even if they don't, however, these criminals communicate with one another and word spreads quickly.

Shortly after the CIO makes this call, she realizes that the company has a backup of the network from yesterday that can be restored to avoid paying the ransom. She is excited and your client is excited because she just realized that the company's most valuable intellectual property—the software technology that is highly proprietary, has never been revealed to anyone else, and is the sole reason for the company being in existence—is on the network and that is the only source for it in existence. Without this asset, there is no company.

Within 5 minutes, the CIO calls back: the backups were also encrypted by the ransomware. There goes the company and, with it, your most lucrative client.

It has become well known that the best defense to ransomware (right after training employees not to click on links or open email attachments) is to have a reliable backup of the network that can quickly be restored. Cyber criminals have learned this and following the teachings of Sun Tzu, have adapted their strategies by writing malware that will not only encrypt the primary network but will also seek out and encrypt all backups that can be reached. The way businesses began adapting to this tactic has been to have the backup segmented from the network so that the ran somewhere could not reach it. This has proven to be an effective tactic and is something all businesses should be doing at this time.

Unfortunately, as always, the attackers are aware of this strategy and are again adapting their techniques even as this guide is being drafted. Understanding that shortly after an attack, businesses that have a segmented backup will move quickly to restore that backup and bring it online, they have begun installing latent "time bomb" type malware that will lurk in the system and wait until the backup is brought online and then encrypt that as well. Because of this evolving tactic, it is important that any business that has a ransomware attack obtain the assistance of a highly-qualified cybersecurity forensics firm to seek out and destroy all traces of the ransomware.

5. Encryption and, for Hyper-Sensitive Information, Air-Gapping.

"Encryption is the process of encoding information so that only the sender and the intended recipient can use that information."[20] According to noted computer security expert, technologist, rocket scientist and encryption evangelist Ronald L. Chichester, "[e]ncryption is viewed widely as the single best security measure that one can take to secure digital information." According to Chichester, "all forty-seven states that have data breach/notification laws cite encryption as a valid mechanism ("safe harbor") to protect data and preclude the need to notify victims if the security of an information system is breached."[21]

Encryption, however, like other cybersecurity protections is not guaranteed and as more sophisticated hackers obtain more powerful computers, such as through quantum computing, much of what we consider to be securely encrypted files may no longer be secure. For information that is so sensitive that no chances can be taken, such as the secret formula to Coca-Cola, such information should be encrypted and also air-gapped. "An air-gapped computer is one that is neither connected to the internet nor connected to other systems that are connected to the internet."[22] "A true air gap means the machine or network is physically isolated from the internet, and data can only pass to it via a USB flash drive, other removable media, or a firewire connecting two computers directly."[23]

[20] Ronald L. Chichester, *Be a Hero: Encrypt Documents for Free in 3 Steps, and Learn Enough to Teach Your Clients and Opposing Counsel*, http://159.203.94.12:8080/Plone/publications/be-a-hero_v1.pdf/@@download/file/Be%20a%20Hero_v1.pdf (see Appendix B).

[21] Id.

[22] Kim Zetter, *Hacker Lexicon: What is an Air Gap?*, WIRED, (Dec. 8, 2014), https://www.wired.com/2014/12/hacker-lexicon-air-gap/

[23] Id.

6. Adequate Logging Is Critical.

It is now essential that companies use adequate logging to detect intrusions and unauthorized activity in their network. Intrusions will happen and it has become virtually impossible to stop all intrusions. However, as the author explained in the *Reporting Guide*,[24] not all intrusions into the network are data breaches or even incidents, some may be relatively harmless cybersecurity events.[25] The problem is, how do you know whether an intrusion was an event, incident, or a full-blown data breach and, if so, the extent of the breach? In other words, how do you know if you need to notify 100 employees of something like their personal W-2 information was accessed or 1 million customers around the world that their banking information was stolen?

The most valuable thing your company can have at this time is accurate and detailed logging data that shows when the intrusion occurred, where it came from, how long they were in your network, what they accessed while in your network, and what if anything was exfiltrated from the network or infiltrated into your network.[26] When you seek help from law enforcement, the first thing they will want to see is the logging data to aid them in doing their forensic analysis. It is critical to any investigation.

This means the company must retain these logs for an adequate period of time. Statistics often show that the average length of time before an intrusion is detected is 205 days[27] and in some cases it can be much longer.

7. Third-Party Security and Supply Chain Risk Management.

Centuries ago the great Sun Tzu, in his teachings on cybersecurity, explained that when it comes to data security, you must be wary of your business associates and other third parties. A prime example of this is how the hackers that attacked Target did so by first attacking one of its vendors, Fazio Mechanical Services, and then using that access to pivot their way into the Target network environment. This attack was discussed previously.

In early 2014, as the world was learning the details of this indirect means of attack used against Target, people began to gain a better understanding of what it means to focus on *third party risk* and *supply chain risk management* (SCRM) in the cybersecurity context.

The Federal Trade Commission (FTC) was paying attention as well. In the enforcement action *In re GMR Transcription Services, Inc.*,[28] it required GMR to follow the following 3 steps when working with third party service providers that will have access to or store confidential customer data: (1) *investigate* the service provider's cybersecurity practices before hiring them; (2) *obligate* the service provider to adhere to the appropriate level of data security protections, which is done through contractual obligations; and (3) *verify* (i.e., audit) that the data service providers are complying with those contractual obligations.

The Securities and Exchange Commission (SEC) was also paying attention and produced a document titled *OCIE Cybersecurity Initiative* for the National Exam Program of the Office of Compliance Inspections and Examinations.[29] In this, the SEC devoted an entire section to *Risks Associated With Vendors and Other Third Parties* and strongly indicated that it would be focusing on cybersecurity protections for investor data maintained in third party databases.[30]

The focus on third party risk and SCRM in cybersecurity has grown steadily. In January 2017, the National Institute of Standards and Technology (NIST) issued a proposed draft update for the *Framework for Improving Critical Infrastructure Cybersecurity*, more commonly known as the *Cybersecurity Framework*. While the *Cybersecurity Framework* is not binding on most private organizations, technically, it is viewed by the FTC and other regulatory agencies as being the gold standard and something they look to in evaluating organizations' cybersecurity practices in enforcement actions. According to NIST, the proposed update focuses on "[p]roviding new details on managing cyber supply chain risks, clarifying key terms, and introducing measurement methods for cybersecurity, the updated

[24] Shawn E. Tuma, *Guide to Reporting Cybersecurity Incidents to Law Enforcement and Governmental Agencies*, BUSINESS CYBERSECURITY LAW, (Dec. 4, 2016), https://shawntuma.com/cyber-law-resources/guide-reporting-cybersecurity-incidents-law-enforcement-governmental-regulatory-agencies/

[25] *Id.* at https://shawntuma.com/cyber-law-resources/guide-reporting-cybersecurity-incidents-law-enforcement-governmental-regulatory-agencies/#_Toc465982678

[26] *See* Dwight David, *Cybersecurity 101: The criticality of event logs*, (Nov. 21, 2016), http://www.csoonline.com/article/3143618/techology-business/cybersecurity-101-the-criticality-of-event-logs.html

[27] David Martin, *The average time to detect a cyberattack is 205 days — here's how to protect your company*, BUSINESS INSIDER, (Jul. 13, 2016), http://www.businessinsider.com/heres-how-to-protect-your-company-from-a-cyber-attack-2016-7

[28] Consent Order, *In re GMR Transcription Services, Inc.* (Aug. 14. 2014), https://www.ftc.gov/system/files/documents/cases/140821gmrdo.pdf

[29] OCIE Cybersecurity Initiative, SEC, (Apr. 15, 2014), https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf

[30] *Id.* at p. 4.

framework aims to further develop NIST's voluntary guidance to organizations on reducing cybersecurity risks."[31] The proposed framework adds "Supply Chain Risk Management (SCRM)" as a "Framework Core" function and highlights the following 4 key goals for organizations and their business partners: (1) coordinating cybersecurity efforts with suppliers of IT and OT (operational technology); (2) enacting cybersecurity requirements through contracts; (3) communicating how cybersecurity standards will be verified and validated; and (4) verifying that cybersecurity standards are met.[32] Do you notice the familiar theme?

8. <u>Incident Response Plan: Tabletop Testing, Reassessment, Revision—Perpetually.</u>

We are nearing a point where the minimum standard of care for any type of organization will require that it have an Incident Response Plan (IRP) for cybersecurity incidents. The SEC recently reinforced this statement in its consent decree with *SEC v. R.T. Jones Capital Equities Management* in which it stated, "Firms must adopt written policies to protect their clients' private information and they need to anticipate potential cybersecurity events and have clear procedures in place rather than waiting to react once a breach occurs."[33] The IRP should be long enough and short enough to be effective for using in a time of crisis.[34] To gain a better understanding of what this means, consider the Cybersecurity Incident Response Checklist in Appendix A which identifies many of the basic things that need to be done when responding to a data breach. Then, develop an IRP that will make it more efficient to do those things.

There is more, however, than simply having an IRP. Recognize that when your organization needs an IRP, it will be in a time of extreme crisis in chaos because it will have just had a data breach. To put this in context, all but the smallest of buildings and offices likely have a plan in place for how to respond to a building fire. But, is that all? Usually, no, because what good is a plan if no one knows about it, knows they have a role in the plan, or understands how to execute the plan? Accordingly, there are things called "fire drills" where the key people who have a role in executing the plan will assume their roles in a simulated building fire situation and practice executing the plan.

That is exactly what organizations need to do with their IRP. This is what is called tabletop testing of an IRP and is something that should be done at least annually but preferably more often. Through this tabletop testing, the people involved will discover weaknesses in the plan, new developments within the organization that require modification of the plan, and other information that indicates the plan should be reassessed and revised to be more effective. This process never ends and, fortunately, results in a more efficient incident response team and a more effective IRP that is perpetually evolving.

9. <u>FTC Start with Security Guide.</u>

The Federal Trade Commission (FTC) published a guide for businesses to evaluate their cybersecurity practices against FTC enforcement action decisions, *Start with Security: A Guide for Business*.[35] This guide is as useful for companies as it is for businesses and recommends taking the following steps:

1. Start with security.
2. Control access to data sensibly.
3. Require secure passwords and authentication.
4. Store sensitive personal information securely and protect it during transmission.
5. Segment your network and monitor who's trying to get in and out.
6. Secure remote access to your network.
7. Apply sound security practices when developing new products.
8. Make sure your service providers implement reasonable security measures.
9. Put procedures in place to keep your security current and address vulnerabilities that may arise.
10. Secure paper, physical media, and devices.

[31] *NIST Releases Update to Cybersecurity Framework*, NIST, (Jan. 10, 2017), https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework

[32] *Cybersecurity Framework Draft Version 1.1*, NIST, (Jan. 10, 2017), https://www.nist.gov/sites/default/files/documents/2017/01/30/draft-cybersecurity-framework-v1.1-with-markup.pdf

[33] Consent Decree, *SEC v. R.T. Jones Capital Equities Management*, https://shawnetuma.com/2015/11/27/sec-v-r-t-jones-shows-the-sec-has-a-role-in-regulating-cybersecurity/

[34] Shawn E. Tuma, *Cybersecurity: How Long Should an Incident Response Plan Be?*, Business Cybersecurity Law, (July 1, 2016), https://shawnetuma.com/2016/07/01/cybersecurity-how-long-should-an-incident-response-plan-be/

[35] Federal Trade Commission, *Start with Security: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

F. The Importance of Preparing to Respond to an Incident: "You Do Not Drown from Falling into the Water."

While there is little that any organization can do to change the cybersecurity law schizophrenia, there are things that organizations can do to minimize the harm that results from cybersecurity incidents. Much of this chaos and confusion can be limited by having a written Cybersecurity Incident Response Plan that key players understand and has been practiced. Having such a Plan is essential.

You do not wait until your building is on fire to start planning how to get out. Similarly, you should not wait until you are in the middle of a cybersecurity incident to start planning how your company will respond. You cannot plan for everything, but you can plan for a lot, and doing so removes a lot of the confusion and chaos and gives some order to how to approach and handle the situation. Consider this saying and then apply it to cybersecurity: "You don't drown by falling in the water; you drown by staying there."[36]

Organizations do not face catastrophic loss simply because they have a cybersecurity incident; they face catastrophic loss when they have not prepared and are unable to respond to or recover from a cybersecurity incident. An Incident Response Plan is critical for helping companies respond to and recover from cybersecurity incidents.

1. Tuma's Cybersecurity Incident Response Checklist.

The author has guided many organizations through the data breach incident response process and has assisted many with preparing their Incident Response Plans. Section IV to this guide is the *Cybersecurity Incident Checklist* that the author has prepared which shows some of the most common steps that must be taken during the incident response process. Many of these steps should be completed within the first few hours after learning of the incident, certainly within the first few days which further highlights why it is so important to be prepared. It is important to note that this is only an abbreviated checklist. It is neither a comprehensive incident response policy nor an incident response plan and should not be substituted as such.

2. FTC Data Breach Response Guide.

The Federal Trade Commission (FTC) published a guide for responding to data breaches, *Data Breach Response: A Guide for Business,*[37] that recommends companies take the following steps:

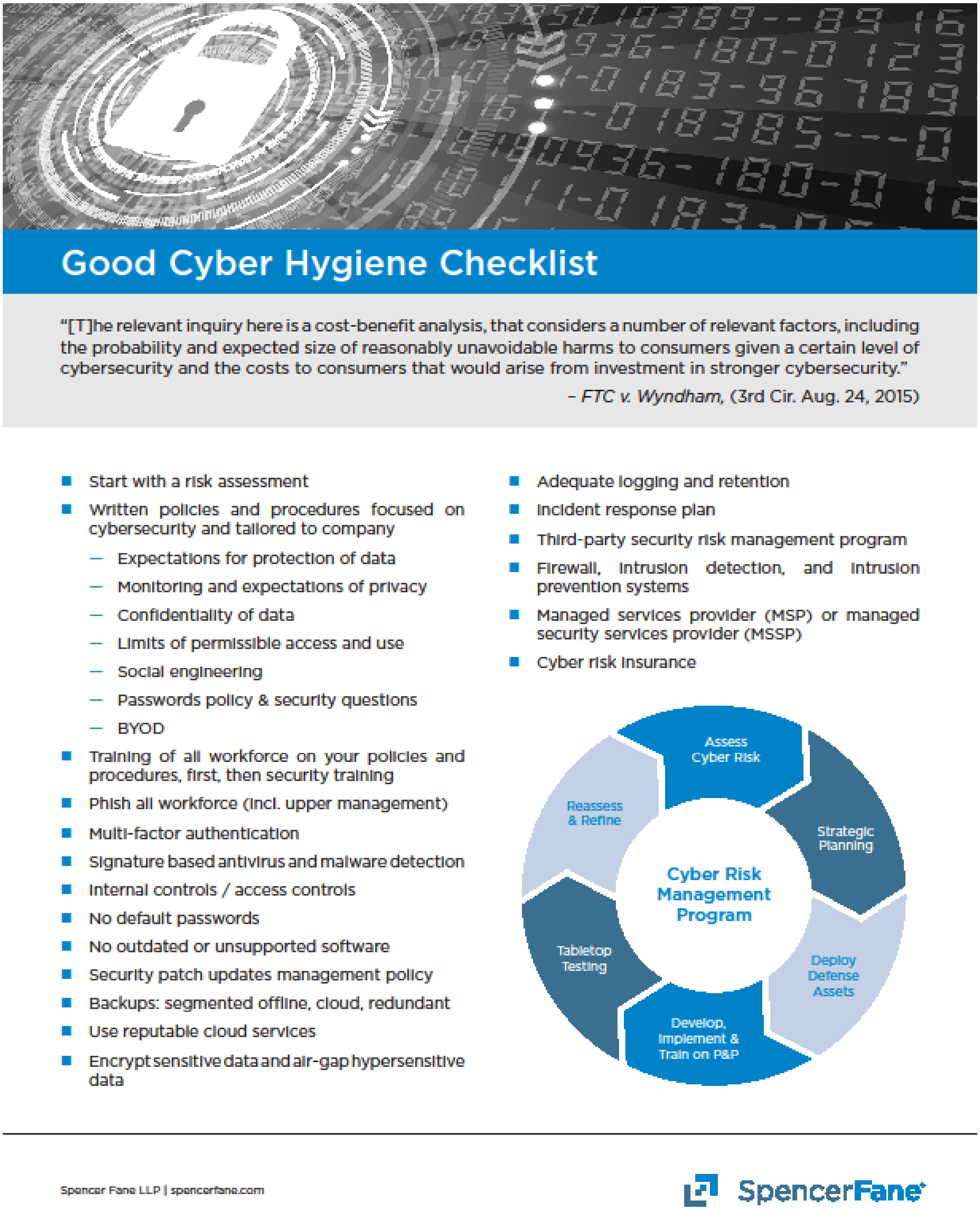
- *Immediate Steps*
  - Fix Vulnerabilities
  - Assemble a team of experts
    - Identify a data forensics team
    - Consult with legal counsel
  - Secure physical areas
  - Stop additional data loss
  - Remove improperly posted information from the web
  - Interview people who discovered the breach
  - Do not destroy evidence
- *Next Steps*
  - Think about service providers
  - Check your network segmentation
  - Work with your forensics experts
  - Have a communications plan
- *Send Notification*
  - Determine your legal requirements
  - Notify Law Enforcement

[36] Edwin Louis Cole, https://www.brainyquote.com/quotes/quotes/e/edwinlouis170162.html

[37] Federal Trade Commission, *Data Breach Response: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf.

- Did the breach involve electronic health information?
    - Health breach resources
- Notify affected businesses
- Notify individuals

III. GOOD CYBER HYGIENE CHECKLIST



Good Cyber Hygiene Checklist

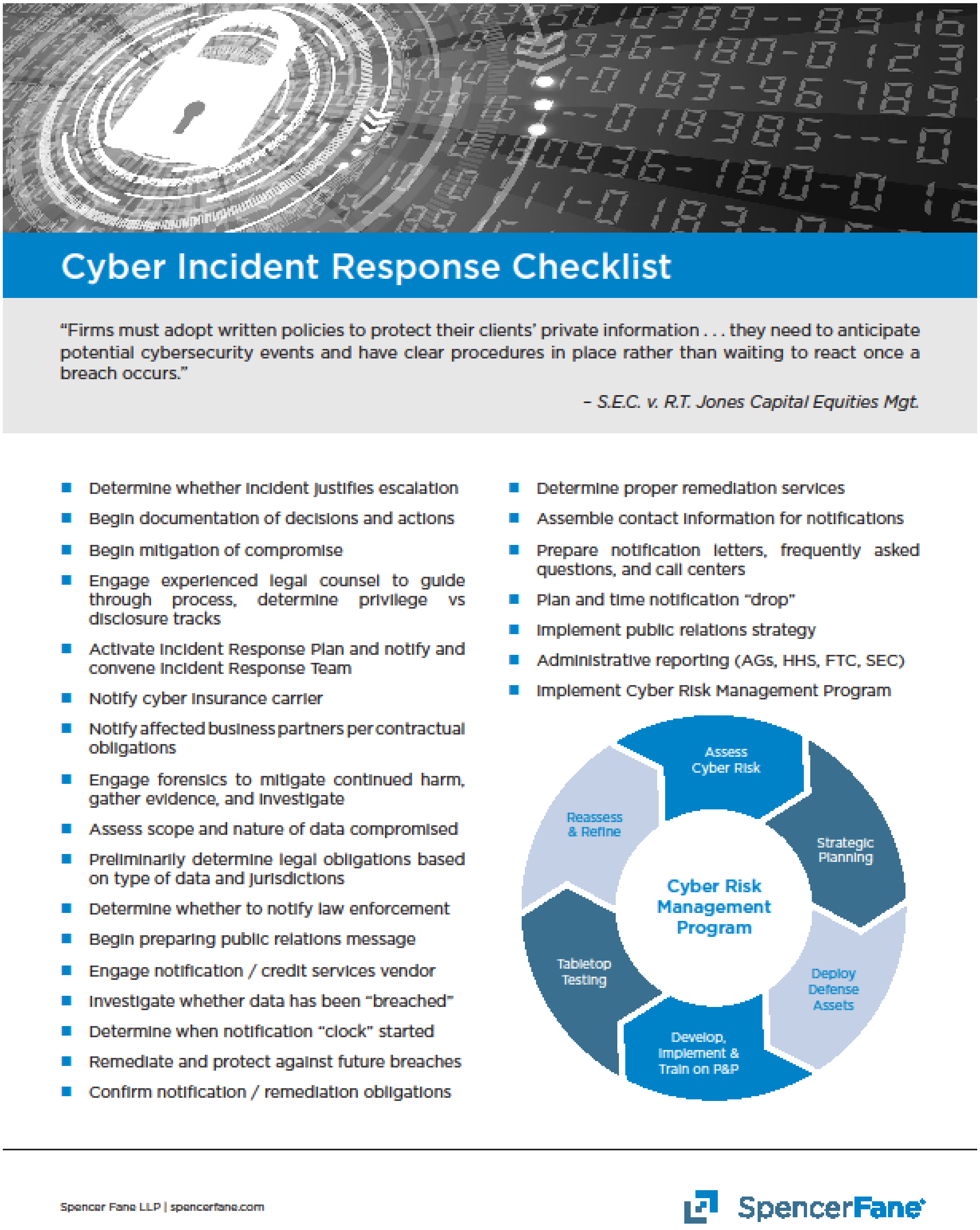
> "[T]he relevant inquiry here is a cost-benefit analysis, that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity."
>
> – *FTC v. Wyndham*, (3rd Cir. Aug. 24, 2015)

- Start with a risk assessment
- Written policies and procedures focused on cybersecurity and tailored to company
  - Expectations for protection of data
  - Monitoring and expectations of privacy
  - Confidentiality of data
  - Limits of permissible access and use
  - Social engineering
  - Passwords policy & security questions
  - BYOD
- Training of all workforce on your policies and procedures, first, then security training
- Phish all workforce (incl. upper management)
- Multi-factor authentication
- Signature based antivirus and malware detection
- Internal controls / access controls
- No default passwords
- No outdated or unsupported software
- Security patch updates management policy
- Backups: segmented offline, cloud, redundant
- Use reputable cloud services
- Encrypt sensitive data and air-gap hypersensitive data
- Adequate logging and retention
- Incident response plan
- Third-party security risk management program
- Firewall, intrusion detection, and intrusion prevention systems
- Managed services provider (MSP) or managed security services provider (MSSP)
- Cyber risk insurance

Spencer Fane LLP | spencerfane.com

SpencerFane

IV. CYBER INCIDENT RESPONSE CHECKLIST



Cyber Incident Response Checklist

> "Firms must adopt written policies to protect their clients' private information . . . they need to anticipate potential cybersecurity events and have clear procedures in place rather than waiting to react once a breach occurs."
>
> – *S.E.C. v. R.T. Jones Capital Equities Mgt.*

- Determine whether incident justifies escalation
- Begin documentation of decisions and actions
- Begin mitigation of compromise
- Engage experienced legal counsel to guide through process, determine privilege vs disclosure tracks
- Activate Incident Response Plan and notify and convene Incident Response Team
- Notify cyber insurance carrier
- Notify affected business partners per contractual obligations
- Engage forensics to mitigate continued harm, gather evidence, and investigate
- Assess scope and nature of data compromised
- Preliminarily determine legal obligations based on type of data and jurisdictions
- Determine whether to notify law enforcement
- Begin preparing public relations message
- Engage notification / credit services vendor
- Investigate whether data has been "breached"
- Determine when notification "clock" started
- Remediate and protect against future breaches
- Confirm notification / remediation obligations
- Determine proper remediation services
- Assemble contact information for notifications
- Prepare notification letters, frequently asked questions, and call centers
- Plan and time notification "drop"
- Implement public relations strategy
- Administrative reporting (AGs, HHS, FTC, SEC)
- Implement Cyber Risk Management Program

Spencer Fane LLP | spencerfane.com

SpencerFane