FOLEY

FOLEY & LARDNER LLP

Guidebook:
Cybersecurity in the Pharma, Biotech, and Medical Devices Industries

Protecting Your IP and Confidential Information in Cyberspace

By Foley's Cybersecurity Team

TABLE OF CONTENTS

Cybersecurity in the Life Sciences and Medical Devices Industries: Protecting your IP and Confidential Information in Cyberspace[1]

I. INTRODUCTION

As a life sciences or medical device company, it is mission critical to protect lab books, drug and clinical test data, product formulas and production processes that underlie your patents, trade secrets and know-how from hackers and others. Given the interconnectivity of corporate data networks, it has become all too easy for cyber thieves to gain access to valuable information in your network, and monetize your hard-earned intellectual property (IP) or cause your company reputational or financial harms.

This Guidebook begins by discussing the importance of protecting vulnerable IP assets in cyberspace. It takes a look at the legislative landscape, with the impact of recent trade secret legislation and a brief discussion of the federal agencies that most frequently operate in the cybersecurity and life sciences space. It is followed by some of the tools for protecting your IP. After that, there is a discussion of practical policies and procedures which companies can implement to help avoid loss and comply with regulations. Recurring topics include: cybersecurity, data ownership, privacy issues and protectable IP.

This paper is focused more on companies in the life sciences and medical devices industry, their affiliates and business associates, clinical researchers (CROs), and third party vendors.

The purpose of this Guidebook is to help the reader focus on the cybersecurity and IP asset protection issues in an accessible and practical way:

Key steps for protecting your proprietary data and IP assets:

1 Identify and data map your IP assets within your physical and digital systems, both onsite and in the cloud, those in the hands of your remote vendors and clinical researchers as well.

2 Be aware of and implement contractual, physical and digital security systems to protect your IP assets.

3 Become aware of cybersecurity risks and implement basic security rules of the road and effective security policy programs to protect your IP assets.

4 Conduct constant risk assessments and evaluate and simulate how best to protect the company and its stakeholders in the event of a system and data breach.

5 Be aware that the Internet of Things and remote medical devices exponentially increase cybersecurity risks down to the device level.

6 Be aware of the legal framework to protect the confidentiality of your IP assets, as well as the liability and regulatory framework impacting cybersecurity in the life sciences and medical devices sectors.

II. PROTECTING VULNERABLE ASSETS IN CYBERSPACE

a. Background

Some of the most valuable assets of life sciences and medical device companies are in the form of IP and the personal information they have collected or processed. The IP of life sciences and medical devices encompass categories such as pharmaceutical and biotechnology patents (*e.g.*, apparatuses and medical device design

[1] The authors gratefully acknowledge the contribution of Michael C. Sweeney, J.D., Northwestern, MS in Bioengineering, Columbia University.

patents), copyrighted data sets and reports, and trade secrets (*e.g.*, clinical trial data, lab notebooks, certain pharmaceutical compositions, computer algorithms and production processes). Personal information is an umbrella category that can include financial information (*e.g.*, personal accounts, social security information, identifiers), personal health information (*e.g.*, medical history, demographic info, test and lab results, insurance information, etc.), and raw or aggregated medical data (e.g., information from heart, glucose and blood monitors, information posted or made available on social platform like WebMD, or other data collected from wearable devices, like the FitBit).

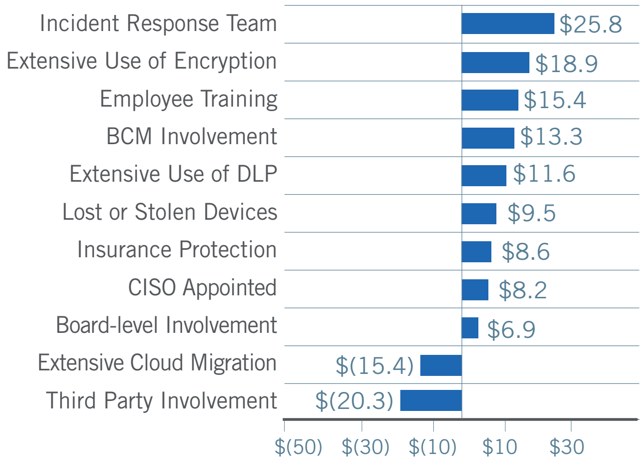
All of these assets have value to both the patients and the companies in the life sciences/medical devices space that utilize this information. The incredible value of digital life sciences and medical devices IP makes it a ripe target for cyber thieves and hackers. The real costs of a data breach, including the direct and indirect costs related to lost profits or customers, can be devastating to companies in any arena; but the healthcare and life sciences/medical devices industries are especially impacted, with the highest costs per capita in the event of a data breach[2] – $402 and $301, respectively, compared to the overall mean of $221.

This is why IP and data security are incredibly important to the sustainability of any life sciences/medical devices company. A company's data security program should include, at least, administrative policies and procedures, physical safeguards (*e.g.*, secure facilities and paper files) and technical safeguards (encryption, firewalls, etc.). It is also important to proactively plan for a security breach because even with reasonable protections in place, data breaches still occur often, and the costs are significant.

Breaches can result in large remediation expenditures and immediate harm to a company's reputation, making it all the more imperative that companies proactively plan for them.[3]

In a recent study sponsored by IBM, researchers analyzed sixteen factors to determine whether each factor increased or decreased the cost of a data breach.[4] Their results aligned well with the feedback in this paper. They found that having an incident response plan ($25.8 per capita), training employees ($15.4 per capita), using data loss prevent technologies ($11.6 per capita) and obtaining cybersecurity insurance ($8.6) all mitigated the mean cost of a breach ($221 per capita).[5] In addition, sharing information with an Information Sharing and Analysis Center can reduce the costs of a breach. Conversely, sharing sensitive data with other third parties ($20.3 per capita) and extensively migrating data to a cloud ($15.4 per capita) both significantly increased the costs of a data breach.[6]

Impact of 16 Factors on the per capita cost of Data Breach (11 Factors Selected)*



**2016 Cost of Data Breach Study: United States*, Ponemon Insitute LLC, June 2016

[2] *2016 Cost of Data Breach Study: United States*, Ponemon Insitute LLC, June 2016, pg. 7.

[3] Wolf, Christopher, *Introduction to Data Security Breach Preparedness with Model Data Security Breach Preparedness Guide*, American Bar Association, April 2012.

[4] *2016 Cost of Data Breach Study: United States*, Ponemon Insitute LLC, June 2016, pg. 9, Fig. 7.

[5] *2016 Cost of Data Breach Study: United States*, Ponemon Insitute LLC, June 2016, pg. 9, Fig. 7.

[6] *2016 Cost of Data Breach Study: United States*, Ponemon Insitute LLC, June 2016, pg. 9, Fig. 7.

b. Legislative Landscape

Below is a brief list of just some of the legislation that impacts or addresses the realms of cybersecurity and the life sciences and medical devices sectors.

- Electronic Communications Privacy Act (ECPA)
- Defend Trade Secrets Act (DTSA) & Uniform Trade Secrets Act (UTSA)
- Health Insurance Portability and Accountability Act (HIPAA)
  - HIPAA Privacy Rule: Addresses Protected Health Information (PHI);
  - HIPAA Security Rule: Addresses electronic PHI (ePHI), a subset of what the Privacy Rule encompasses.
- Health Information Technology for Economic and Clinical Health Act (HITECH) & the HIPAA Omnibus Rule
- Computer Fraud and Abuse Act (CFAA)
- Various FDA guidance
- Federal Trade Commission (FTC) Act – Section 5
- European General Data Protection Regulation (Regulation (EU) 2016/679)

c. Legislative Privacy Requirements

Any life sciences and medical devices cybersecurity discussion invariably must also address privacy requirements pertaining to medical data sets and patient information.

The HIPAA Privacy Rule defines and safeguards Protected Health Information.

> "The Privacy Rule standards address the use and disclosure of individuals' health information — called 'protected health information' by organizations subject to the Privacy Rule — called 'covered entities,' as well as standards for individuals' privacy rights to understand and control how their health information is used."[7]

Covered entities and their affiliates include health plans, health care clearinghouses, such as billing services and community health information systems, and health care providers that transmit health care data in a way that is regulated by HIPAA. If your device is a "Medical Device," the information you collect is most likely governed by HIPAA as PHI, for medical devices sold or used in the United States, or collecting information from U.S. residents.

42 U.S.C. Section 17931 of HITECH extends the entire Privacy and Security Provisions of HIPAA to the business associates of covered entities.[8] This includes the extension of updated civil and criminal penalties to pertinent business associates. These changes are also required to be included in any business-associate agreements among covered entities.

Another piece of legislation that often intersects with life sciences IP and data rights is the Computer Fraud and Abuse Act (CFAA). The CFAA "prohibits access to a computer, website, server or database either 'without authorization' or in a way that 'exceeds authorized access of the computer.'"[9] Section 1030(a)(2)(C) of the Act makes it a crime to obtain information from any "protected" computer if the conduct involves interstate or international communication. While not specifically directed at the life sciences, parties can originate civil actions under this law in the event of data malfeasance.

Finally on the domestic front, the FTC Act, Section 5 prohibits unfair or deceptive acts or practices, which can lead to an action by the FTC under the FTC Act, Section 5 when their medical IP or data is not regulated by HIPAA.

[7] U.S. Department of Health and Human Services, *Summary of the HIPAA Privacy Rule*, available at http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html. Accessed July 26, 2016.

[8] 42 U.S.C. §17931.

[9] Snell, Jim and Care, Derek, *Use of Online Data in the Big Data Era: Legal Issues Raised by the Use of Web Crawling and Scraping Tools for Analytic Purposes*, Bloomberg BNA: Privacy and Security Law Report, pg. 292.

Beyond United States federal and state law, there are also international data privacy provisions of which life science companies need to be aware. The European data protection framework just underwent radical change in 2016, with a new General Data Protection Regulation (GDPR) replacing the old Data Protection Directive.[10] The new GDPR will require many domestic firms that process the personal data of European citizens to update their privacy policy provisions and increase their cybersecurity protections for personal data. The GDPR will impact the use of the new EU-US Privacy Shield, binding corporate rules, and standard contractual clauses, user consent to legally transfer information from the European Union to other countries whose laws do not provide "adequate protection," and will require companies use the principles of privacy (and security) by design, conduct privacy impact assessments, and assign a data privacy officer to ensure compliance with GDPR. Failure to comply with the privacy and security requirements of GDPR may result in fines of up to four percent of an organization's worldwide annual revenue.

d. Protecting Trade Secrets and Other Confidential Information

Trade secret holders are particularly vulnerable to hackers and cybersecurity breaches. Other forms of IP, such as patents, are made publicly available, so there is less need to safeguard IP that has already been registered, although there are often trade secrets and other confidential information supporting and working in conjunction with patented items. Trade secrets, on the other hand, are usually known only to select employees and their protection, is often vital to the holder's economic viability.

Trade secret information is information that derives economic value (actual or potential) because it is not generally known; and that is the subject of reasonable efforts to maintain its secrecy.[11] Trade secrets are protected as long as the party can keep it secret, so once disclosed it is no longer a trade secret.

Trade secret protection derives from rights provided under state law (by statute, usually by adopting or modifying the Uniform Trade Secrets Act) or by common law, and more recently, federal law. Before the Defend Trade Secrets Act of 2016, the Economic Espionage Act was the primary basis for a cause of action under federal trade secret law.[12] The Economic Espionage Act of 1996 criminalizes the misappropriation of trade secrets related to, or included in, a product that is produced for or placed in interstate (including international) commerce, with the knowledge or intent that the misappropriation will injure the trade secret owner. Penalties include fines and imprisonment for up to ten years for individuals and fines of up to $5 million for organizations[13]

The Defend Trade Secrets Act of 2016[14] (effective for acts of misappropriation occurring on or after May 11, 2016) amends the Economic Espionage Act of 1996 to provide a "civil remedy" for misappropriation of trade secrets. The new § 1836(b) allows a trade secret owner to bring a civil action in federal court if the trade secret is related to a product or service used in, or intended to be used in, interstate or foreign commerce.

[10] "*Privacy Shield – Rejected. GDPR – Accepted: What This Means to Your Organization and What You Should Consider Doing Now*" Chung, Howell, Millendorf, Tantleff.

[11] (AIPLA Spring 2016 Trade Secrets Presentation) Gills, Jeanne M., *AIPLA 2016 Spring Meeting: What's Reasonable? Protecting and Enforcing Trade Secrets*, American Intellectual Property Law Association, May 19, 2016.

[12] Economic Espionage Act of 1996, 18 USC § 1831 et seq.

[13] AIPLA Spring 2016 Trade Secrets Presentation) Gills, Jeanne M., *AIPLA 2016 Spring Meeting: What's Reasonable? Protecting and Enforcing Trade Secrets*, American Intellectual Property Law Association, May 19, 2016 citing 18 U.S.C. § 1832.

[14] (AIPLA Spring 2016 Trade Secrets Presentation) Gills, Jeanne M., *AIPLA 2016 Spring Meeting: What's Reasonable? Protecting and Enforcing Trade Secrets*, American Intellectual Property Law Association, May 19, 2016 citing 18 U.S.C. § 1832.

Consequently, litigants may now pursue claims more easily in federal court. The new § 1836(c) provides that district courts shall have original jurisdiction of civil actions brought under the DTSA.

The upshot of trade secret protection in the life sciences and medical devices sectors is that trade secret law requires reasonable precautions, not extraordinary precautions or absolute secrecy – since it would be unreasonable if protecting the secret unduly hampered business operations. As such, according to case law, smaller companies may meet "reasonable safeguard" trade secret standards with fewer requirements.[15] Small to mid-cap companies' strategy should focus on information leaking to third parties, managing any departing or disgruntled employees, and preventing unwanted confidential third party information from being brought to your company.

e. Federal Agency Regulations and Feedback

1. Food and Drug Administration

The Food and Drug Administration (FDA) has the power to dictate cybersecurity and privacy requirements for regulated medical devices (subject to premarketing and post marketing regulatory controls).[16] Most devices used to diagnose, mitigate, treat or prevent disease fall within the ambit of FDA medical device regulation.[17]

The FDA has provided some guidance on medical device cybersecurity. They recommend that manufacturers of medical devices proactively plan for and assess cybersecurity vulnerabilities consistent with the FDA's Quality System Regulation.[18] This includes implementing the core principles of "identify, protect, detect, respond, and recover" from NIST's Framework for Improving Critical Infrastructure Cybersecurity[19]. The Quality System Regulation advises device manufacturers to understand, assess and detect the presence and impact of a cybersecurity vulnerability.

This in turn requires that the manufacturers define essential performance and develop mitigations to protect, respond, and recover from looming cybersecurity risks.

2. Federal Trade Commission

The FTC has the power to hold organizations responsible for their cybersecurity and privacy practices under FTC Act, Section 5 "unfair and deceptive practices." The FTC has also issued guidance on Cybersecurity for the Internet of Things, essentially finding that firms should encourage a culture of security, including creating senior executives who are responsible for and have authority to influence product security.[20] Companies should also implement "security by design" and consider security features upfront during product development instead of trying to secure products as an afterthought. Further advice included: (1) implementing defense-in-depth that incorporates security measures at several levels - considering how the consumer will use your product and identify potential security risks (2) using a risk-based approach – put the most resources toward protecting the most sensitive information, (3) considering the risks

[15] *Elm City Cheese Co. v. Federico,* 1999 Conn. LEXIS 369 (1999) (within small family-owned company, reasonable efforts satisfied where trade secrets shared only among family members and accountant and where plaintiff "kept confidential enough information to make it virtually impossible for its employees to use the rest of the information constituting its trade secret.").

[16] Surpin, Beni, *Managing Emerging Technology in Healthcare: Association of Corporate Counsel Presentation*, Foley & Lardner LLP, July 2016.

[17] FDA Basics, *What is a Medical Device?*, U.S. Department of Health and Human Services: Food And Drug Administration, accessed 7/27/2016, available at http://www.fda.gov/AboutFDA/Transparency/Basics/ucm211822.htm.

[18] Surpin, Beni, *Managing Emerging Technology in Healthcare: Association of Corporate Counsel Presentation*, Foley & Lardner LLP, July 2016.

[19] Version 1.0, Feb. 12, 2014, available at https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[20] Surpin, Beni, *Managing Emerging Technology in Healthcare: Association of Corporate Counsel Presentation*, Foley & Lardner LLP, July 2016.

associated with the collection and retention of information, only collecting what is necessary and retaining information collected only for as long as necessary, and (4) avoiding default passwords unless users are required to change the default passwords immediately.[21]

Also, for ease of integration with other systems and companies, the FTC recommends using generally accepted best security practices, such as well-recognized, established, and generally secure authentication and encryption techniques. This includes taking advantage of readily available security tools - many of which are free.

Finally, the FDA urges entities and individuals to establish effective approaches for updating security procedures and products. This includes staying up-to-date on known security vulnerabilities, such as those listed in the Common Vulnerabilities and Exploits (CVE) Database, the Common Weakness Enumeration (CWE), and the US-Computer Emergency Reediness Team (US-CERT) email list.

III. TOOLS FOR PROTECTING LIFE SCIENCE AND MEDICAL DEVICES ASSETS IN CYBERSPACE

a. Identifying and Protecting Your IP Assets[22]

- Inventory and document the ownership, development and value of your IP assets.
- Review the status of IP protection for your key IP assets, including federally registered IP rights (patents, copyrights, trademarks) and trade secrets.

1. Common IP Assets and Confidential Information

- Computer software
- Algorithms
- Database compilations
- Computer hardware design
- Drug and clinical test data
- Drug extraction and manufacturing processes
- Production and chemical processes
- Product formulas and ingredients
- Product blueprints, plans and drawings
- Manufacturing processes
- PHI
- PII
- Technical Reports
- Technical and testing data
- Product strategies and marketing plans and forecasts
- Business strategies and opportunities
- Customer lists
- Customer product use and preferences
- Other customer information
- Internal cost information
- Profit margins
- Pricing or financial information
- Computer systems and Email

2. "Efforts that are Reasonable under the Circumstances" to Protect Intellectual Property and Maintain the Secrecy of the Information

- Advising employees of the existence of IP or a trade secret.
- Limiting access to IP or a trade secret on a "need-to-know basis".
- Controlling premises access (offices, manufacturing plants), as well as access to documents and filing systems.
- Public disclosure of information through display, trade journal publications, advertising, or other carelessness can preclude protection.
- Reasonable use of a trade secret including controlled disclosure to employees and licensees and third parties (business partners, contractors, consultants, vendors) is consistent with the requirement of relative secrecy.
- Trade secrets can be lost through reverse engineering.

[21] Surpin, Beni, *Managing Emerging Technology in Healthcare: Association of Corporate Counsel Presentation*, Foley & Lardner LLP, July 2016.

[22] Burke, Francis J. and Winarski, Tyson Y., "Protecting Corporate Trade Secrets In A Digital Network Environment", 1 Privacy & Data Security Law Journal 56 (2005). Burke, Francis J. Jr., Kisicki, Mark G. and Nickerson, John B., "Protecting Trade Secrets in a Digital World", 4 Internet Law & Business 119 (2002)

3. Conduct Regular Intellectual Property Audits

- Limit access to IP and trade secrets.
- Make sure those who do come into contact with IP and trade secrets understand what is secret and why, how to ensure it remains so, what the consequences are for failing to follow the company's trade secret policy.
- Make your efforts commensurate with the value of the information at issue. The nature of efforts to keep IP and trade secrets from being disclosed should depend on the value of the information to its owner and others, as well as the nature of the information and the threat of disclosure.

4. Traditional Methods of Preserving IP

- Annually distributing a company-wide confidentiality policy (given on date of hire for new employees)
- Producing codes of conduct, employee handbooks or IP policies
- Requiring employees to sign trade secret/ confidentiality agreements respecting the trade secrets
- Alerting employees with a follow-up letter, reminding him or her of their obligations
- Distributing an acknowledgment form signed by the employee at date of hire and then annually
- Making materials available only to a handful of persons worldwide
- Attaching electronic sensors to documents
- Marking documents "Confidential: For Internal Use Only," and limiting distribution of such materials to employees with a "need-to-know" basis
- Implementing a clean desk policy
- Keeping records of persons to whom trade secret information was made available
- Documenting what confidential information was given, released, and returned.
- Enforcing disciplinary action against violators
- Inventorying items prior to employee departures
- Documenting efforts to develop and protect the trade secrets
- Conducting exit interviews
- Requiring confidentiality agreements with customers, vendors, third parties
- Sending a reminder of continuing obligations to maintain secrecy
- Logging and identifying materials
    - Collect all confidential documents and other information
- Advising employees of the existence of a trade secret
- Limiting access to the information on a need-to-know basis
- Locking offices, cabinets and safes
- Utilizing a check-out system
    - Acknowledgement of receipt of confidential proprietary or trade secret data
    - Acknowledgement of duties to safeguard and not disclose it
    - Restrictive legends ("Confidential" or "Trade Secret" status)
- Setting up security measures:
    - Sign-in procedures
    - Badges
    - Photo identification
    - Security personnel
    - Alarms
- Restricting access for visitors and employees
- Keeping "one-of-a-kind" documents and items under lock and key
- Using locked briefcases to transport the documents
- Limiting circulation of customer lists

5. Define Confidential Information

- Determine whether Confidential Information must be reduced to writing
- Determine whether it must be marked "Confidential" or "Proprietary"
- Determine whether it only relates to a particular subject, product, or process or is more general
- Determine whether the agreement will cover oral disclosures
- Determine whether the agreement will cover disclosures where the recipient has reason to know the information is Confidential
- Describe the purposes for which the Confidential Information may be used
- Disclaim various types of IP licenses
- Provide for the return of the Confidential Information

6. Confidentiality Agreements with Employees

- Protect the employer's trade secrets
- Prevent disclosure of such information both during and following the termination of employment
- Are generally enforceable in accordance with their terms
- Promise to return all such confidential information upon termination of employment
- Should be signed at the commencement of employment, or at the time the employee's position gives him or her access to proprietary information
- Recognize that employer has trade secrets and other certain confidential information
- State that employee will have access during the course of his or her employment
- State that information is "proprietary" to the employer
- Contain a promise by the employee to keep the information confidential
- Contain a promise that the employee will not use or disclose the information outside the workplace or to those without a "need to know" without the employer's consent

7. Confidentiality and NDA Agreements with Third Parties

Companies should enter into confidentiality and non-disclosure agreements with contractors, vendors, actual and potential business partners, potential merger and acquisition partners, joint ventures exposed to trade secrets, outside professionals and consultants. Ideally, these non-disclosure agreements are entered into at the onset of any discussions, before finalizing any formal agreement for the transaction. Similar to non-disclosure agreements with employees, these agreements set out affirmative obligations to limit the disclosure and use of confidential information and may extend for the duration of the relationship between the parties or longer. Because trade secret protection only continues for as long as the company maintains the secret, an important, but often overlooked provision in non-disclosure agreements is the maintenance of the secrecy of trade secrets indefinitely (or until no longer a trade secret). These agreements are enforceable through injunctive relief and damages, and well-drafted agreements will exclude breaches of confidentiality from a limitation of liability and contain explicit clauses permitting equitable relief.

8. Intellectual Property Protection in a Digital Network Environment

- The first level of security is to map the location of IP and other confidential information in the company's computer systems, to inventory the organization's IP and confidential information, to limit access to each category of information to limited groups of employees on a need to know basis, and to limit the number of IT administrators who can access each category of trade secret and confidential information.
- The company must focus broadly on electronic documents, databases, e-mail, instant messages and other electronic information, located on network drives, database management systems, ERP systems, desktop computers, laptop computers, smart phones, tablet computers and backup tapes and drives, and removable media such as portable drives, USB drives, floppy and CD/DVD drives.

- Digital information should be protected through electronic labeling, electronic locks, passwords, warning screens, encryption or coding or shrink wrap licenses or agreements on software provided to employees or vendors requiring that users agree to nondisclosure terms. It is also possible but impractical to place highly secret data on machines that are not connected to the network and have their own monitor.
- Printing, copying and downloading activity must be covered in the company's information security policies. It is common to opt for computers that have no USB, floppy or CD/DVD drives, or to disable them, or to utilize data loss prevention and information rights software solutions to block the transfer of the data out of the network system.
- Periodically monitor employee e-mails received through their company email on their own home computers or mobile devices, or forwarded to their personal accounts, especially around the time of mergers and acquisitions or other important events.

9. BYOD Policies

The use of mobile devices, including laptop computers, smartphones and tablet computers is exploding at exponential rates, including through Bring Your Own Device (BYOD) policies. Cameras and recording devices built into mobile equipment can overwhelm every other information security program in ways that are almost undetectable. One obvious defensive policy is to prohibit the use of camera enabled mobile technology on or around corporate premises. As employees move corporate information onto mobile devices to use while traveling, new challenges are encountered. Here are some mobile device protections which should be embodied in a corporate information security policy:

- Employee confidentiality agreements and policies must make clear that they apply to both corporate equipment and to mobile and personal equipment containing corporate information, e-mails and attachments or downloads.
- Employment policies must reflect and show employee consent that all corporate activities and communications on mobile and personal devices are subject to monitoring and may be accessed for corporate investigations.
- Employment policies must reflect and show employee consent that they are personally responsible for what happens with the device and data and information sent to or from the device and stored on it, including security and data breaches and messages sent from the device. Employees whose device is lost or stolen should be required to immediately report that occurrence to the IT department. The employees should be required to consent to remote wiping of the device, including personal information if necessary, in the event that the device is lost or stolen. The IT department should ensure that the security systems for the device are consistent with the security system used by the organization.
- Upon termination of employment, the employee should be required to turn over all devices and portable media to the IT department, ideally before exiting the organization, for wiping of all confidential and business information.

b. Data Mapping and Ownership Issues

The first step in securing digital assets and IP is to fully assess what you own and where it is located. Many large companies inadequately account for the location and security of their digital assets. When speaking to a CIO, they should be able to identify which valuable or confidential assets are stored on internal servers, external servers, in the cloud or some combination of the above. For example, would your company feel comfortable storing sensitive human resources information on Google Docs or some other cloud based program? In some instances, cloud or external storage may be acceptable, but in order to assess the safety of these procedures, an asset owner must first make a full accounting of exactly where their information is and identifying its value. Usually, the best way to perform these accountings is to do a "boots on the ground" survey of individual employees in a company. Ask those who handle protected information where they store it and how, then assemble an accurate depiction, or "Data Map," of the survey results.

c. Perimeter Security Software and Hardware

A network perimeter is where a company's network ends and the Internet begins. Due to wireless and VPN technology, the boundary is often not well-defined. When this boundary is poorly defined, many companies lose confidential data, and in turn productivity and revenue. Perimeter security is largely addressed by the company's firewall, but may also contain intrusion prevention and detection systems. However, with the increased risk from DoS attacks and malware scripts infiltrating past firewalls, additional security policies are often needed.[23]

Some of the dangers of a having a poorly guarded perimeter include:

1. **Stolen IP (including copyright or patent protected software products, such as applications and scripts).**
2. **Remotely accessed computers turned into "zombies" (computers used to send out spam and viruses automatically).**
3. **Locally hosted websites or intranet being removed, replaced, or modified.**
4. **SQL databases suffering "injection attacks," causing data loss and/or severe security compromises.**
5. **Remote employees accessing a system, leaving VPN connections at risk for hacking.**
6. **Virus and malware infections leading to identity theft, data loss, server and network crashes and lost productivity.**

For these reasons and others, securing your network perimeter is a vital step on the path to protecting IP and data.

Network segmentation can be an effective tool for protecting the network. "Risks to highly sensitive data (for example, credit card information, social security numbers, trade secrets, and IP) can be mitigated by separating the data from less secure networks and systems that can be accessed through the Internet.

For example, a server that contains sensitive employee information, such as Social Security numbers, can be segregated from servers that can be accessed by the public from the Internet."[24]

Other protective means include: effective firewall configurations, the use of intrusion detection and intrusion prevention systems, segregation through physical separation, or logical separation through the use of subnets. The company must also be concerned about the entry points to its system – which include the company's internet connectivity to the global internet and its local Wi-Fi connections, which may provide a pathway into its network to nearby users. The company should also be concerned with physical security at the perimeter, such as through locked network closets.

d. Information Rights Management (IRM)

> "Information Rights Management is the set of techniques and methods which protect the highly sensitive information of [an] organization irrespective of the file location, whether it resides 'in' or 'outside' the corporate boundaries. This happens as the permissions embedded inside the file don't allow unauthorized access, modification, copying or printing."[25]

IRM is typically used for the protection of financial documents and IP, such as pharmaceutical patents, design blueprints and executive communications.

[23] *Network Security: Firewall Configuration, Perimeter Security*, PlanetMagpie.com, available at http://www.planetmagpie.com/networksupport/networksecurity.aspx. Accessed July 25, 2016.

[24] (Foley Cybersecurity White Paper) Howell, Chanley T., et. al. *Taking Control of Cybersecurity: A Practical Guide for Officers and Directors*, 2015.

[25] Network Intelligence, *Information Rights Management – Implementation and Challenges*, pg. 5, available at http://www.slideshare.net/NIIConsulting/information-rights-management-irm. Accessed July 26, 2016.

"The rationale for using IRM is that the privacy information associated with the data must travel along with it. The copying of that data must not lose the associated rights to that information. Rights to modify, update, restrict, or even destroy that information must be retained by the individual it pertains to, even when a third party holds that information."[26]

"In a larger context, IRM helps organizations [enforce] corporate policy governing the secure flow of highly sensitive data… File protections are defined and enforced based on user's identity along with corporate policy on a given class of data. The best way to protect information is [often] to do it directly at the level of the information – and not at the level of many systems, which might change, transport or store the information."[27]

IRM capabilities[28]:

1. **"IRM can prevent restricted content from unauthorized modification, copying, printing or pasting."**
2. **"Disables the Print Screen feature in Microsoft Windows from taking snapshots of restricted content."**
3. **"Can restrict specific content exposure whenever it is sent."**
4. **"Supports file expiration tools, so that contents in documents are rendered un-viewable (or viewable) automatically after a set time."**
5. **"Full auditing, of both access to documents as well as changes to the rights/policy by business users."**

e. Endpoint Protection and Response Software

Endpoints in a network can include PCs, smart phones, laptops, point of sale (POS) terminals, and specialized equipment, such as bar code readers.[29] Under an endpoint security management system, endpoint devices have to comply with predetermined criteria before they can access network resources. The system itself can be purchased as software or as a dedicated appliance. Its job is to "discover, manage and control computing devices that request access to a corporate network." [30] Some of the typical elements include an approved operating system, a VPN client and up-to-date anti-virus software.[31] If the system identifies a device that does not comply with the predetermined restrictions, that device is given limited access or quarantined on a virtual local area network (VLAN). These quarantines can be controlled to varying degrees, for example, "the system may remove local administrative rights or restrict Internet browsing capabilities."

Endpoint security should be a critical consideration for health care and medical device providers. Medical device hijacking is on the rise.[32] Medical devices and healthcare systems in general are relatively easy targets because, like many other critical infrastructure systems, network connectivity, and therefore cybersecurity, are often afterthoughts. Due to this troubling trend, health care and medical device providers should consider a security by design approach that includes endpoint security. As with many IT devices, challenges exist for patching security bugs in medical devices once deployed – physical access to the device may be challenged by an invasive surgery, and there is no opportunity to "reboot" the device for a security patch to be applied. In a hospital environment, for example,

[26] Network Intelligence, *Information Rights Management – Implementation and Challenges*, pg. 5, available at http://www.slideshare.net/NIIConsulting/information-rights-management-irm. Accessed July 26, 2016.

[27] Network Intelligence, *Information Rights Management – Implementation and Challenges*, pg. 5, available at http://www.slideshare.net/NIIConsulting/information-rights-management-irm. Accessed July 26, 2016.

[28] Network Intelligence, *Information Rights Management – Implementation and Challenges*, pg. 6, available at http://www.slideshare.net/NIIConsulting/information-rights-management-irm. Accessed July 26, 2016.

[29] Rouse, Margaret, *Essential Guide: An IT Security Strategy Guide for CIOs*, TechTarget.com.

[30] Rouse, Margaret, *Essential Guide: An IT Security Strategy Guide for CIOs*, TechTarget.com.

[31] Rouse, Margaret, *Essential Guide: An IT Security Strategy Guide for CIOs*, TechTarget.com.

[32] yon, Scott, *Excellus Breach: Encryption Cannot Always Save the Day*, Law 360, October 6, 2015.

> "the wireless tablets used for charting by nurses making rounds or the imaging equipment in the lab down the hall running on an outdated, unpatched operating system -- any of these could be the weak link in the security chain that allows an attacker to gain a foothold into a network." [33]

Attackers can then expand their access through these initially compromised nodes, leaving the entire network vulnerable and patient lives at risk.

f. Penetration Testing

Penetration testing is the practice of testing the strength and vulnerabilities of a company's network with respect to attacks from outside of the network. Often this is performed by outside consultants under contract with the organization (with significant confidentiality requirements) who conduct "white box" testing of the network to determine its vulnerabilities. Systems are constantly changing, meaning a system that is relatively secure one month may not be as secure the next. Periodic penetration is required under the Payment Card Industry Data Security Standards for companies that process credit card information. Penetration testing every six months, or at least annually, is an important step in keeping a company's network secure against outside hacking attacks.[34]

As discussed above, the costs of a life science data breach or medical network hack are even more severe and costly (both financially and sometimes physically) than hacks in other arenas, so it is critical to actively test your computer systems for vulnerabilities.

g. Intrusion Detection Systems

Intrusion attempt logging is yet another way to prepare for and mitigate the effects of a cybersecurity breach. Similar in function to a firewall, an intrusion detection system monitors network activity within the organization (behind the firewall), while a firewall looks outward to prevent intrusions. For example, an intrusion detection system can be configured to trigger an alarm if a certain type of network traffic or activity matches a library of known attacks. It can also trigger an alarm if certain critical files are modified or deleted. Finally, the intrusion detection system can provide an alert if the network activity is not "normal," this may include instances where there is a higher or different type of activity.[35] An intrusion detection system has many benefits. It helps notify cybersecurity professionals of a potential security incident early, and may help provide critical forensics information to understand what the cause and scope of a security incident is.

IV. CYBERSECURITY RISKS

a. Cybersecurity Risks

1. Rising Information Security Risks

The FBI disclosed that it notified 3,000 companies that they had been a victim of a cybersecurity breach in 2013. The U.S. Director of National Intelligence ranked cybercrime as a top national security threat, higher than terrorism, espionage, and weapons of mass destruction. In May 2014, the U.S. charged five Chinese military hackers with 31 counts of cyber-espionage against American corporations including Westinghouse, SolarWorld, U.S. Steel, Allegheny Technologies, and Alcoa, to name a few. In September 2015, the U.S. government reported that over the previous five years, there had been over 700 successful cybersecurity attacks on American companies from China. These hit every state in the U.S., except North Dakota. Other nation-state factors that threatened U.S. industries included threats from Iran, Russia and North Korea.

[33] Lyon, Scott, *Excellus Breach: Encryption Cannot Always Save the Day*, Law 360, October 6, 2015.

[34] (Foley Cybersecurity White Paper) Howell, Chanley T., et. al. *Taking Control of Cybersecurity: A Practical Guide for Officers and Directors*, 2015.

[35] (Foley Cybersecurity White Paper) Howell, Chanley T., et. al. *Taking Control of Cybersecurity: A Practical Guide for Officers and Directors*, 2015.

By some estimates, hacking has caused an estimated $300 billion in annual losses in the U.S., and $749 billion to $2.2 trillion globally per year. This is estimated to cost 200,000 jobs in the U.S. alone (though probably higher) because companies are likely to underestimate the loss and underestimate the risks. Further, most IP breaches are not publicized.

2. The Human Factor

It is estimated that there are more than 7 million (known) cybersecurity vulnerabilities. Ten vulnerabilities accounted for 97% of the reported breaches. Most vulnerabilities have been known, with patches available, for months or years. This suggests that corporations neglect, for one reason or another, to regularly patch systems. It also suggests that becoming a hacker is relatively easy and takes very little skill: "script kiddies" can use scripts that exploit the old vulnerabilities with reasonable success.

Besides scripts for common vulnerabilities, hackers can now outsource their creation of phishing and ransomware attacks, now using technology to increase efficiency in attacking what is often the weakest link in security – the human element. There are now hacking services, such as sites referred to Reveton and Tox. These sites provide ransomware to hackers for a cut of the ransom. Ransomware, and phishing in general, continue to become effective because less 3% of phishing attack recipients report the suspicious email to their IT departments.36 Instead, over 30% of recipients open the email containing the phishing attack and 12% of recipients open the attachments. 37 IT departments have little time to respond – the median time for the first user to open the phishing email is a mere 1:40, and the median time for the first click on the malicious attachment is just 3:45. [38]

3. Why Now?

Cybersecurity is, or at least should be, at the top of almost every organization's agenda. The growth of the use of Big Data and the Internet of Things are examples of two catalysts for the rapid expansion and focus on all things relating to privacy and data security. As systems become more complex and interconnected with vendors, business partners, and other third parties, companies must take a closer look at their cybersecurity protocols in order to protect their data, IP, and sometimes the most important thing of all – their reputation. Moreover, organizations face increased liabilities when they don't pay close attention to cybersecurity, including those from class actions, regulatory enforcement actions, shareholder derivative suits, and State Attorney Generals. The U.S. Securities and Exchange Commission (SEC) has issued guidance that requires public companies to evaluate its cybersecurity risks, taking into account all available information, and may be required to publicly disclose cybersecurity relevant risks and cybersecurity.

4. Common Security Myths

The importance of cybersecurity has certainly risen in prevalence, over the last decade, in both the public and private sector but a number of myths still permeate common perception. This section will explore and debunk those myths.

Myth #1 "It's all about the data

Security must be designed to account for not only the protection of the data or information (including a company's IP), but for the information system itself. Security should be approached from both a holistic and segmented perspective. By focusing only on certain components, or the data, the entire system will be left vulnerable, which ultimately leaves individual segments and data susceptible.

[36] *Verizon 2016 Data Breach Investigations Report*, Verizon Enterprise Solutions, April 2016, pg. 18.

[37] *Verizon 2016 Data Breach Investigations Report*, Verizon Enterprise Solutions, April 2016, pg. 18.

[38] *Verizon 2016 Data Breach Investigations Report*, Verizon Enterprise Solutions, April 2016, pg. 18.

Organizations also need to consider the reputational harm as a result of the breach. In the U.S., indirect costs, including lost business, the cost to attract or retain customers, and the loss of confidence in a company often accounts for two-thirds of the cost of a data breach.[39]

Myth #2 "It's all about confidentiality"

Confidentiality of information is only one element. What is equally important is the integrity and availability of the information. The integrity of the information aims to ensure that the information has not been altered, maliciously, accidentally, or due to a system error. Putting security mechanisms in place to address the integrity of the information helps ensure, for example, that sensor information stored in a medical device is providing correct and accurate information to medical professionals, avoiding errors in diagnosis and treatment. Equally as important is the availability of information when requested. This is especially true in the life science and medical device industries, where the unavailability of information may result in the inability to diagnose a life-threatening condition.

Myth #3 "To be a hacker, you must be a technology genius"

Vast information and resources exist that allow even technical novices to "hack" systems. Not all hackers are former technology geniuses gone rogue. As described earlier, the age of vulnerabilities and the ease of obtaining exploits opens the doors to "script kiddies" and other average, ordinary, individuals to contribute to security incidents.

Myth #4 "It's an IT Department issue"

The IT department may be responsible for devising the security mechanisms to guard against external threats, but cybersecurity is an enterprise-wide issue that requires buy-in and direction from the board and upper management. Increasingly, board members are held responsible for neglecting their fiduciary duties when they ignore cybersecurity in their organization. Even if the IT Department implements strict safeguards, the strongest procedures will fail if employees are not educated on the important of security "hygiene" as security is only as strong as its weakest link.

Myth #5 "I can achieve (need) 100% security"

While there is no one-size-fits-all approach to security, it is also impossible to achieve 100% security. One study estimated that an organization that wanted to achieve the highest possible level of cybersecurity, which itself was only capable of repelling 95% of the attacks, would have to boost their spending on cybersecurity nine times.40 The study also found that in order to just to be able to stop 84% of the attacks, organizations would have double their investments in cybersecurity.[41]

As security protections are increased, the usability of the secured system decreases, and vice versa. Even if it was possible to stop 100% of the attacks, the system would not be usable for its intended purpose. Therefore, organizations should appropriately balance their security efforts with usability, and focus on managing the residual risks that remain after their investments.

[39] *2016 Cost of Data Breach Study: United States*, Ponemon Insitute LLC, June 2016, pg. 20.

[40] 2012 Survey of Technology Managers, Ponemon Insitute LLC and Bloomberg.

[41] 2012 Survey of Technology Managers, Ponemon Insitute LLC and Bloomberg.

Myth #6 "I'm safe. I have great security."

The biggest myth of all is the false belief that an organization is safe because it has "great" security. Thousands of new viruses and exploits are developed every day. According to an Imperva/Technion-Israel Institute of Technology Study, the initial threat detection (zero day) is only 5%. According to a Verizon Study: 83% of intrusions took weeks or more to discover. According to a Trustwave Holding Study, the average time to detect an intrusion is 210 days.

5. Sources of Risk

While security incidents due to hacking receive most of the attention in the headlines, in reality, data breaches occur due to a number of other sources. Threats come from the way organizations handle paper and other records, as well as the ways in which the access to electronic systems are guarded. A security program must be well-developed to guard against external hackers, but it is also important to keep in mind the impact of everyday actions.

One of the biggest threats a company faces is the risk from internal people and sources. Rogue employees, or malicious "insiders" that have access credentials and knowledge of company's confidential information are one of the largest risks a company faces.

Other sources of risk include "script kiddies" (a person who uses existing computer script or code to hack into computers), spies (industry or governmental), organized crime, cyber terrorists, "hacktivists", lap and disk drive manufacturers, smartphone apps, social engineering (requires no technical skill), and phishing. Phishing attacks are becoming more and more sophisticated by leveraging social media or corporate biography information to target specific employees for seemingly legitimate information. In fact, in 2013, nearly 450,000 phishing attacks cause estimated losses of over $5.9 billion. Large enterprises have a 1 in 2.3 chance of being targeted. While phishing has become more advanced, proper training can educate employees to recognize a few key concepts to spot a phishing email.

6. Security Rules of the Road

While there is no such thing as perfect security, and anti-virus software is never 100 percent effective, there are a number of best practices that organizations should implement and principles to be mindful of to help mitigate the risk of a security breach.

Companies should craft strong policies and protocols for passwords. Passwords should be generated based on a combination of upper and lower case letters and special characters. Passwords should never be written down or shared, even internally. If a password is compromised on one particular website, users should consider updating their passwords across all accounts as many people utilize the same or similar password across multiple accounts (although not recommended).

Aside from phishing attacks sent through email, there are a variety of other ways in which email may serve as a source of vulnerability. Attachments or hyperlinks should never be opened in an email unless you know the sender, and even then, exercise caution. PDFs are one of the most popular means of transmitting viruses.

Organizations should also educate their employees to beware of contacts from "information security" personnel or others requesting disclosure of access credentials or urgent request to issues checks or other provide other confidential and sensitive information.

The use of public internet and hot spots leave a system highly vulnerable to hacking and other attacks. VPNs and tethering should be used whenever possible. Especially in public settings, but even at work, terminals should not be left unattended while logged on.

V. DIRECTOR & OFFICER CYBERSECURITY ISSUES

a. Directors' and C-Level Executives' View of Cybersecurity

- More than 90% of corporate executives say they cannot read a cybersecurity report and are not prepared to handle a major cybersecurity attack.

- 98% of the most vulnerable have little confidence in their company's ability to monitor devices/users on their systems.
- 40% said they don't feel responsible for the repercussions of hacking and not personally responsible for cybersecurity or for protecting customer data.
- "It's the IT department's problem."[42]

b. Sources of Corporate Liability After a Security or Privacy Incident

- **FTC Enforcement Actions**
  These actions often lead to settlement or a consent decree, including fines and ongoing monitoring. Wyndham has challenged the Federal Trade Commission's (FTC) authority to enforce a company's cybersecurity practices.
- **FCC Enforcement Actions**
  The Federal Communications Commission (FCC) generally follows the FTC's lead for telecommunication companies and other companies within its authority. The FCC will now regulate broadband providers under the new FCC ruling that brings internet service providers under Title II of the Communications Act.
- **SEC Enforcement Actions**
  There have been no enforcement actions yet, but the SEC has indicated that disclosure requirements for public companies also include disclosure of cybersecurity risks and cybersecurity incidents.
- **State Attorneys General**
  State attorneys general enforce state privacy, breach notification, and data security laws (when applicable).

c. Cybersecurity Due Diligence for Directors and Officers[43]

- What are the greatest cyber security threats and risks to the company's highest-value intangible assets, and the most sensitive company and customer information? Does the company's risk management and assessment deal with protecting those assets and that information?
- What is the company's volume of cyber security incidents on a weekly or monthly basis? What is the magnitude/severity of those incidents? How much time and cost is incurred to respond to those incidents?
- What would the worst-case cyber incident cost the company in terms of lost business, system downtime, and reputational damage?
- What is the company's specific cyber security breach response and crisis management plan, and how will it respond to customers, clients, vendors, the media, regulators, law enforcement, and shareholders, traditional and social media, NGOs, bloggers? Have the plans been practiced in mock situations?
- What cyber security training does the company include in its compliance program?
- What due diligence does the company perform with respect to its third-party service providers?
- What cyber security due diligence is done as part of any acquisition?
- Has the company performed a cyber security IT audit of the company's systems, services and products to analyze potential vulnerabilities that could be exploited by hackers?
- What infrastructure enhancements have been adopted to show affirmative action to protect the company's IP, intangible assets, sensitive data and customer data and personal information?

[42] Source: Center for Strategic and International Studies survey that polled 1,530 non-executive directors and C-level executives from US, UK, Germany, Japan, and Nordic countries.

[43] Burke, Francis J., "Cyber Security and Cyber Risk Issues for Boards of Directors", Audit Committee Hot Topics Panel, Foley National Directors Institute, November 6, 2014 and Cloud Computing: Ethical, Privilege and Practical Issues Confronting Corporate Counsel Panel, ABA Corporate Counsel Annual Meeting, February 13, 2015.

d. *Board of Directors Risk Assessment Questions for the Company's Chief Information Officer, Chief Information Security Officer and IT Team*

- Where is the company's data stored geographically, and in what data centers? Has the General Counsel examined the legal issues in each jurisdiction?
- What is the computer architecture structure of the company's computer centers and data centers, are they accessible to company employees, customers and vendors and suppliers, and how? Are they accessible to mobile users and how? What computer and data centers are outsourced, and how? How much data has been placed into a cloud computing environment, in what architecture, and are the clouds being used private, public, or a hybrid? Given all the retail data breaches, does the company utilize point of sale terminals and are they being updated? Does the company use mobile payment hardware and software?
- Are company and customer and competitor data being commingled in databases or on servers or in the same cloud environment or kept separate and is either customer or company data exposed to competitors, vendors, suppliers or other parties? If so, what types of security measures or confidentiality agreements been implemented?
- What level and type of encryption and firewalls do the computer and data onsite centers, outsourced computer and data vendors and cloud-based providers use? What type of perimeter security system is used? Does the IT team or its consultants have expertise in these systems?
- What are the company's and vendors' backup and disaster recovery plans?
- What are the company's and the vendors' incident response and notification plans?
- What speed and level of access does the company have to security information on its data and customer data stored in company and outsourced computers and data centers and cloud locations in the event the company needs to respond to a regulatory request, internal investigation or litigation?
- How transparent are the vendor and cloud providers' own security systems? What access can the company get to the cloud provider's data center and personnel to ensure the security system is in place and functioning, while also making sure it can make a risk assessment and design a response plan?
- What are the vendor and cloud servicers' responsibilities to update their security systems as technology and sophistication evolves?
- What are the company, computer and data vendors, and cloud providers' ability to continuously monitor, detect, and respond to security incidents, and what logging information is kept in order to potentially detect suspicious activity?

VI. POLICIES AND PROTOCOLS

In conjunction with the software and hardware discussed above, all life science/medical device firms must develop internal policies to protect confidential health information and IP. On a macro level, the most effective protocols are those that: (1) restrict access to the information (*i.e.*, via comprehensive network security), (2) limit the number of people who know the information and have those people sign non-disclosure or confidentiality agreements (*i.e.*, employee agrees to confidentiality as part of their Employment Agreement; third parties and business contacts sign NDAs), and (3) mark any written material pertaining to trade secrets or protected IP as confidential and proprietary and/or follow-up in writing if there is a verbal disclosure.

a. *Common Components of Effective Security Policy Program*

1. Be aware of Federal and State requirements; tailor privacy policies as applicable.
2. Designate people responsible for security in the organization.
3. Conduct security training for employees.
4. Take reasonable steps to ensure vendors/service providers protect data.
5. Consider minimizing data collection.
6. De-identify where possible.
7. Conduct a privacy or security risk assessment initially and periodically thereafter.
8. Consider encryption, particularly for storage and transmission of sensitive information such as health data.

b. *Ten Key Elements of a Cybersecurity Risk Management Program*

1. Incident management
2. User education and awareness
3. Managing user privileges
4. Manage home and mobile computer working environments
5. Removable media controls
6. Malware protection
7. Monitoring
8. Secure configuration
9. Network security
10. Cybersecurity insurance

c. *Policies for Different Types of Company Technology*

1. Computer Systems

Life sciences/medical devices companies must take stock of all company computer systems including file and email servers, desktops, laptops, portable electronic devices, portable media drives (*e.g.*, thumb drives, CDs). They should also consider limiting social media access and reiterating the importance of IP protection, even in social media usage. On computers that house sensitive material, the information technology department should create limited access (*e.g.*, through usernames and passwords), implement restricted permissions (*e.g.*, by disabling copy and print functions and the ability to install programs and applications; limiting access to internet mail, ftp and public ports; and segregating access to sensitive information), keep logs of computer activity, and update virus protection suite and spam filters. Each of these steps can be a critical cog in maintaining airtight safety on a desktop or network computer.

2. Laptops and Portable Drives

Laptops and portable devices often require separate safety procedures. CIO's and technical services should create policies against files being transferred to personal computers (remote desktop, Citrix™, or other service to access files remotely) and when it comes to confidential matters, only allow use of company-issued laptops. Further, they should restrict the use of portable drives. Portable drives are especially problematic in the context of cybersecurity because they have such high capacity and are very small – for especially sensitive matters, it is recommended to review logs of mounted drives and copied files.

3. Portable Electronic Devices

For smartphones and tablets, it is necessary to have a well-crafted Bring Your Own Device (BYOD) policy that defines when it is appropriate to use personal versus company issued devices. It is also critical to monitor copies of files and e-mail access granted to remote or personal devices. Personal and remote devices often need specific security measures, such as separate passwords, tracking software in the event the device is lost, and remote deletion capabilities. Also, any temporary devices given to employees containing sensitive information should be returned and possibly subject to forensic examination upon the employee's departure.

d. Contractual Protections

1. Limiting Third Party Access to Critical Information

> "More and more companies are providing outside vendors and CROs with access to company networks for purposes of exchanging data. The vendor's network then, in essence, becomes an extension of the company's network. If the vendor has weak security, their network can be breached and then used to enter the company's network. The source of the Target security breach originated through a refrigeration, heating, and air conditioning subcontractor that had access to Target's network."[44]

Effective vendor due diligence and contractual restrictions can mitigate these risks. Agreements can specifically circumscribe the type of access a contract research organization (CRO) or vendor has to your network and the circumstances under which they can access it.

2. Indemnification

Indemnification clauses provide that one party will bear the monetary costs, either directly or through reimbursement, for losses incurred by a second party. Since granting vendors and CROs access to a network often creates vulnerabilities and increases the chance of an adverse event, indemnification clauses should be added to any service contracts agreed to between parties. The clauses help reduce the impact of any breaches or compromised IP.

3. Cyber Insurance

Yet another method to contractually reduce potential loss is to take out a policy for cybersecurity insurance. The policy should protect against a various incidents, including hacking, viruses, data theft and inadvertent loss of personal information. It is important to seek these policies out, because most general commercial liability policies either contain express inclusions or will not cover security incidents. If your company has cybersecurity insurance, it must be diligent about complying with the requirements of the policy. Some policies require a baseline level of data security to be implemented and maintained within the organization. A company's vendor due diligence and contracting process should ensure that vendors that handle information assets have adequate cybersecurity insurance. [45]

e. Incident and Data Breach Response Plans

Almost every state has also adopted laws that require notification of security breaches to consumers and often the attorney general. There are overarching patterns among most states, but each state can have different data breach notification requirements.[46] On the federal level, the FTC and the Department of Health and Human Services (HHS) enacted notification requirements that affect HIPAA covered business associates and other service providers that manage health data.[47] The HITECH Act requires entities covered by HIPAA to report data breaches affecting 500 or more persons to the HSS, to the news media, and to the people affected by the data breaches.

[44] (Foley Cybersecurity White Paper) Howell, Chanley T., et. al. *Taking Control of Cybersecurity: A Practical Guide for Officers and Directors*, 2015.

[45] (Foley Cybersecurity White Paper) Howell, Chanley T., et. al. *Taking Control of Cybersecurity: A Practical Guide for Officers and Directors*, 2015.

[46] See 50 State Foley Data Breach Notification Survey

[47] Wolf, Christopher, *Introduction to Data Security Breach Preparedness with Model Data Security Breach Preparedness Guide*, American Bar Association, pg. 1, April 2012.

The American Bar Association has produced literature on the "Do's and Don'ts of Responding to a data breach."[48] Their list follows:

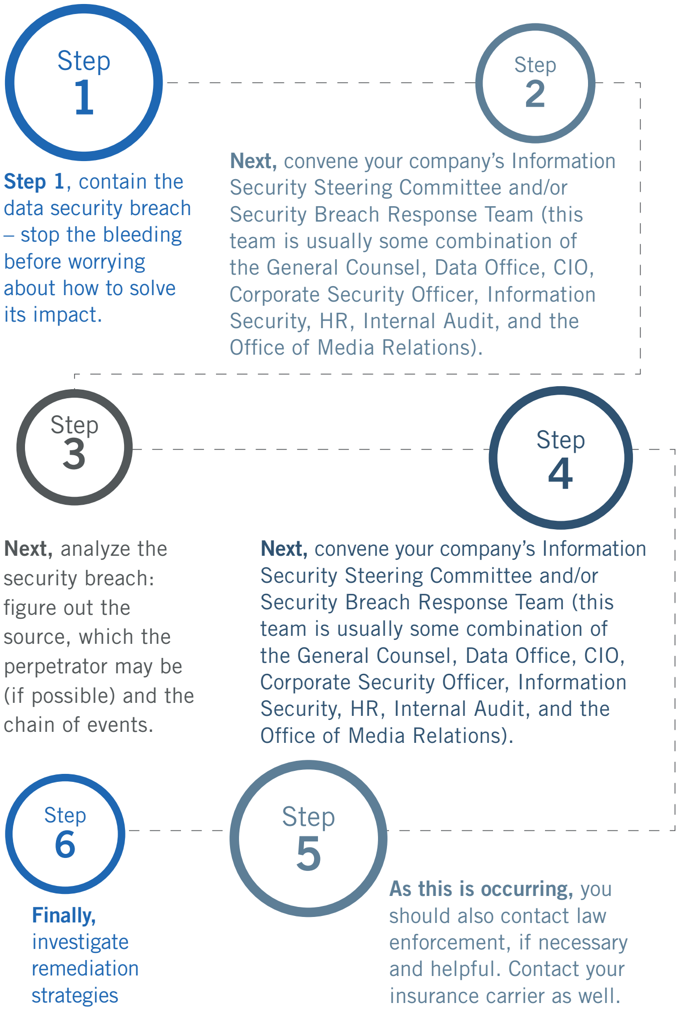
1. Do's

- Have a written post-breach response plan ready and tested before a breach occurs.
- Identify a breach response team and make sure people know what role they will play if a breach occurs.
- Know what regulations, statutes and contracts cover your post-breach obligations.
- When a breach occurs, do everything possible to prevent further exposure.
- Find out what happened as soon as possible and preserve the evidence.
- Contact your insurance carrier and seek legal advice regarding whether the breach triggers notification requirements and whether those notification requirements apply to your company.
- Have draft model notices ready to be customized depending on the facts.
- Contact law enforcement, credit reporting agencies, and regulators and keep them informed.

2. Don'ts

- Don't delay in providing notices when legal counsel determines they are required or advisable.
- Don't communicate with the public about the breach until you know the fundamental facts.
- Don't ignore important business customers and partners -- Keep them informed.
- Don't necessarily accede to every demand from a business customer or partner -- Weigh demands carefully in light of your total response plan.
- Don't forget to update your post-breach response plan regularly.
- Don't skimp in providing help to consumers – their goodwill could forestall legal difficulties.

As guidance, here are some steps that every company should immediately follow to mitigate and analyze an incident.[49]



Step 1, contain the data security breach – stop the bleeding before worrying about how to solve its impact.

Next, convene your company's Information Security Steering Committee and/or Security Breach Response Team (this team is usually some combination of the General Counsel, Data Office, CIO, Corporate Security Officer, Information Security, HR, Internal Audit, and the Office of Media Relations).

Next, analyze the security breach: figure out the source, which the perpetrator may be (if possible) and the chain of events.

Next, convene your company's Information Security Steering Committee and/or Security Breach Response Team (this team is usually some combination of the General Counsel, Data Office, CIO, Corporate Security Officer, Information Security, HR, Internal Audit, and the Office of Media Relations).

As this is occurring, you should also contact law enforcement, if necessary and helpful. Contact your insurance carrier as well.

Finally, investigate remediation strategies

In the event your company is acting as a service provider to another business for which personal data is held, develop a notification plan for that business customer.[50] Of course, the best strategy is to be as proactive as possible; before an event occurs, begin by developing a notification plan for affected individuals.

[48] Wolf, Christopher, *Introduction to Data Security Breach Preparedness with Model Data Security Breach Preparedness Guide*, American Bar Association, April 2012, pg. 1

[49] Wolf, Christopher, *Introduction to Data Security Breach Preparedness with Model Data Security Breach Preparedness Guide*, American Bar Association, April 2012, pg. 3.

[50] Wolf, Christopher, *Introduction to Data Security Breach Preparedness with Model Data Security Breach Preparedness Guide*, American Bar Association, April 2012, pg. 4.

f. Audits and Enforcement

IP protection strategy is only effective if adhered to, so it is important to conduct regular audits to ensure all of the policy and procedures outlined above are being followed. This includes ensuring internal and third party compliance and scheduling systematic review of all aspects of IP protection strategy.

VII. MEDICAL DEVICES ISSUES

a. Overview

According to the *Business Insider*, the number of connected devices, currently about 10 billion, will grow to 34 billion by 2020. Coupled with that, we will be facing an interesting challenge of mastering all that data and information overload given the real-time granularity in the data. ABI Research hypothesizes that by 2020 data volumes across connected devices will hit 1.6 zettabytes, or roughly 1.6 trillion gigabytes.

This section will address the following issues:

1. **What are the legal cybersecurity obligations for manufacturers of wearables and medical devices? What level of cybersecurity is appropriate for a given device?**
2. **What is the legal framework around the privacy of information obtained from wearables and medical devices?**
3. **What are the current trends in data ownership of health-related information collected from wearables and medical devices?**

b. FDA and the FTC Regulation of Medical Devices Cybersecurity

The FDA has the power to dictate cybersecurity and privacy requirements of regulated medical devices (subject to premarketing and post-marketing regulatory controls). Most devices sold directly to consumers explicitly disclaim that their device is not a medical device.

Even if the device is not a "medical device" and subject to the FDA, the FTC has the power to hold organizations responsible for their cybersecurity and privacy practices under Section 5 "unfair and deceptive practices."

c. FDA Guidance on Medical Device Cybersecurity

The FDA recommends that manufacturers of devices regulated as medical devices proactively plan for and assess cybersecurity vulnerabilities consistent with the FDA's Quality System Regulation. These manufacturers should implement the core principles of **identify, protect, detect, respond, and recover** from the NIST's Framework for Improving Critical Infrastructure Cybersecurity. This requires understanding, assessing and detecting the presence and impact of a cybersecurity vulnerability. Manufacturers should define the device's essential performance and develop mitigations to protect respond and recover from a cybersecurity risk.

d. FTC Guidance on Cybersecurity for the Internet of Things

Fundamentals of generally accepted best security practices:

1. **Take advantage of readily available security tools - many are free.**
2. **Test the security before launch.**
3. **Make security the default choice in preferences.**
4. **Establish an effective approach for updating security procedures and products.**
5. **Stay up to date on known security vulnerabilities.**

e. Data Ownership Issues

1. Defining Ownership

Who does and who should own patient data?

- The stakeholders involved are patients, provider organizations, personal health record service providers, insurance companies, health-data exchanges, and health-data banks.
- Distinguishing devices: What is data ownership for a wearable? What is data ownership for a medical device? When do they overlap?
- How do we address the conflict between patients' desire to control their data and the public's need to use those data for various worthy purposes (taking into account HIPAA, HITECH, the Common Rule, etc.)?

2. Data Ownership Issues

- Is collected data Health Information under HIPAA?
- For medical devices (as defined by the FDA) that send data directly to a covered entity, probably yes:
- Patients own their own Health Information.
- State law may assign ownership to records that contain Health Information.
- For most other wearables, personal "medical" devices, social media, and other health related platforms used by consumers:
- Consumers generally own this data, but may be modified by the manufacturer's Terms of Use.
- Most emerging technology Terms of Use have broad use rights for the vendor, even if they do not change the ownership.
- May include "social media" applications like FitBit, Jawbone, etc.

3. Data Monetization: HIPAA Final Omnibus Rule (2013)

- **The final omnibus rule sets limits on how protected health information is used and disclosed for marketing and fundraising purposes and prohibits the sale of an individuals' protected health information without their permission.**

f. Networked Healthcare: Medical Devices and Wearables

Identifying the risk: Medical devices are increasingly connected to other devices, the Internet, networks and portable media. These devices are more vulnerable to cybersecurity attacks than traditional, non-networked, devices. The level of security needed depends on a multitude of factors, including: the device's intended use, how it interfaces with other electronics, the environment in which it is used, the types and likelihood of cybersecurity vulnerabilities, and the level of patient harm.

Usability: How do healthcare device manufacturers balance between cybersecurity safeguards and the usability of the device in its intended environment of use (e.g. home use vs. health care facility use) to ensure that the security controls are appropriate for the intended users? For example, security controls should not unreasonably hinder access to a device intended to be used during an emergency situation.

g. Hacking

Deficiencies in the law: Even though the Computer Fraud and Abuse Act and the Federal Anti-Tampering Act impose stiff penalties for cyberattacks, it is often impossible to identify the actor behind a cyberattack, which greatly decreases these laws' deterrence power. While HIPAA incentivizes covered entities to protect personal health information, it does not apply to most medical device manufacturers or situations where malicious actors cause harm without accessing personal health information.

Three major types of attacks: (1) Cyberattacks on individual medical devices and wearables (e.g. hacking a pacemaker), (2) Cyberattacks on hospital networks, and (3) Cyberattacks leading to theft of medical information.

h. How Would You Know If You Have Been Hacked?

Examples:

1. **Various types of medical devices can be found through searches on Shodan, a website that details internet-connected devices.**
2. **Imagine the potential threat of ransomware on a medical device.**
3. **World renowned hacker Barnaby Jack demonstrated the ability to assassinate a victim with a pacemaker at BreakPoint 2012. In 2013, he had developed software to remotely send an electric shock to a pacemaker in a 50 foot radius and software to scan for insulin pumps within 300 feet and deliver a low or high dose of insulin as desired.**

4. A 2013 report found that more than 300 devices made by 40 manufacturers may be vulnerable due to default service technician passwords. Devices at risk include ventilators, anesthesia devices, drug infusion pumps, and external defibrillators.
5. MED JACK attack vector. Three separate hospitals, found extensive compromises of medical devices including X-ray equipment, picture archive and communication systems, and blood gas analyzers. MED JACK was used as an attack vector to open backdoors to exfiltrate other confidential information out, but it could also be used to compromise the integrity of the data as well.
6. Many implantable devices have wireless interfaces for status, reconfiguration, and "updates" that can be a vector for attack.

i. Privacy Compliance

1. Review Europe's GDPR, the rise and fall of the Safe Harbor, and Working Party Statement 29. Review the Privacy Shield and guidance for recent changes in trans-border data flows.
2. Compare requirements between GDPR and HIPAA.
3. Is there an exception for research purposes?

VIII. CONCLUSION

This Guidebook shows life sciences and medical devices companies how to identify, locate and map their IP assets, which may be found physically onsite but also in a computer network or in the cloud, in the possession of a key vendor, clinical researcher or CRO, an affiliate or business associate. It explains the legal framework to protect confidential information, but also the regulatory and liability framework that may come into play when data, especially PII and PHI, is lost or stolen. It shows the reader the fundamentals of contractual, physical and digital security systems, as well as effective security rules of the road and security programs. It illustrates the importance of director and officer due diligence in cybersecurity risk assessment, evaluating risk scenarios and data breach response simulations and plans. Finally, it shows how the Internet of Things and remote medical devices multiply cybersecurity risks and that protection must begin at the device level.

FOLEY

FOLEY & LARDNER LLP

PRACTICE LEADERSHIP

Jim Kalyvas
Chair - Privacy, Security & Information Management
Chair - Technology Transactions & Outsourcing
Los Angeles, CA
jkalyvas@foley.com
213.972.4542

Eileen Ridley
Chair - Privacy, Security & Information Management
Partner - Litigation and IP Litigation
San Francisco, CA
eridley@foley.com
415.438.6469

KEY CONTACTS & CONTRIBUTORS

Frank Burke
Partner - Privacy, Security & Information Management, Litigation, and IP Litigation
San Francisco, CA
fburke@foley.com
415.984.9870

Chanley Howell
Partner - Privacy, Security & Information Management and Technology Transactions & Outsourcing
Jacksonville, FL
chowell@foley.com
904.359.8745

Steve Millendorf
Associate - Privacy, Security & Information Management and Technology Transactions & Outsourcing
San Diego, CA
smillendorf@foley.com
858.847.6737

Aaron Tantleff
Partner - Privacy, Security & Information Management and Technology Transactions & Outsourcing
Chicago, IL
atantleff@foley.com
312.832.4367

Mike Overly
Partner - Privacy, Security & Information Management and Technology Transactions & Outsourcing
Los Angeles, CA
moverly@foley.com
213.972.4533

Jennifer Rathburn
Partner - Privacy, Security & Information Management and Technology Transactions & Outsourcing
Milwaukee, WI
jrathburn@foley.com
414.297.5864

Beni Surpin
Partner - Privacy, Security & Information Management and Technology Transactions & Outsourcing
San Diego, CA
bsurpin@foley.com
858.847.6736

Our Core Values

Clients First
Our clients are our first priority. When we provide quality work, value and superior service to our clients, our own success inevitably follows.

Diversity
We embrace diversity and are committed to the inclusion of our diverse attorneys and staff and to the success of all our people.

Integrity
We will adhere to high standards of ethics, professionalism and integrity and safeguard the reputation of the Firm at all times.

Trust and Respect
The success of our partnership stands on a foundation of trust, mutual respect, collegiality, communication and teamwork.

Stewardship and Accountability
As stewards of the Firm, we are accountable to one another and will commit our time, talent and energy to the Firm's success, growth and long-term prosperity.

Citizenship
We embrace our responsibilities to our communities and profession and will lead by example through civic, pro bono, professional and charitable service.

Professional Satisfaction
Our work should be professionally satisfying and provide competitive financial rewards while affording the opportunity to achieve a reasonable balance between professional demands and personal commitments.

Our People
Our people are our most valuable asset and their quality, creativity and dedication are indispensable to our success.

FOLEY

FOLEY & LARDNER LLP

BOSTON | BRUSSELS | CHICAGO | DETROIT | JACKSONVILLE | LOS ANGELES | MADISON | MIAMI | MILWAUKEE | NEW YORK | ORLANDO
SACRAMENTO | SAN DIEGO | SAN FRANCISCO | SHANGHAI | SILICON VALLEY | TALLAHASSEE | TAMPA | TOKYO | WASHINGTON, D.C.

ATTORNEY ADVERTISEMENT. The contents of this document, current at the date of publication, are for reference purposes only and do not constitute legal advice. Where previous cases are included, prior results do not guarantee a similar outcome. © 2017 Foley & Lardner LLP ■ MC1804