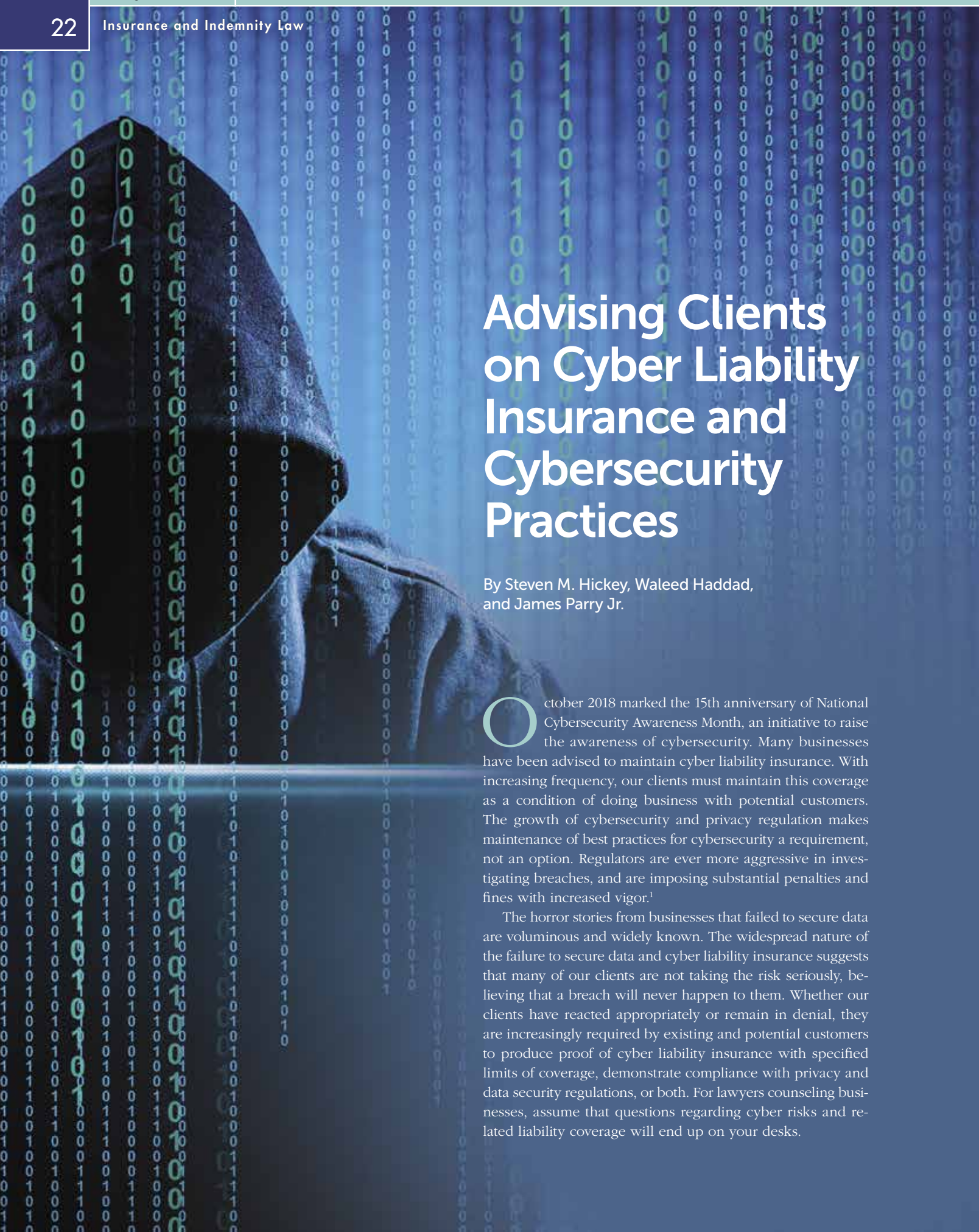

Advising Clients on Cyber Liability Insurance and Cybersecurity Practices

By Steven M. Hickey, Waleed Haddad, and James Parry Jr.

October 2018 marked the 15th anniversary of National Cybersecurity Awareness Month, an initiative to raise the awareness of cybersecurity. Many businesses have been advised to maintain cyber liability insurance. With increasing frequency, our clients must maintain this coverage as a condition of doing business with potential customers. The growth of cybersecurity and privacy regulation makes maintenance of best practices for cybersecurity a requirement, not an option. Regulators are ever more aggressive in investigating breaches, and are imposing substantial penalties and fines with increased vigor.[1]

The horror stories from businesses that failed to secure data are voluminous and widely known. The widespread nature of the failure to secure data and cyber liability insurance suggests that many of our clients are not taking the risk seriously, believing that a breach will never happen to them. Whether our clients have reacted appropriately or remain in denial, they are increasingly required by existing and potential customers to produce proof of cyber liability insurance with specified limits of coverage, demonstrate compliance with privacy and data security regulations, or both. For lawyers counseling businesses, assume that questions regarding cyber risks and related liability coverage will end up on your desks.

A list of the questions we are (or soon will be) asked by our clients follows. In this article, we attempt to provide answers and insights to common cybersecurity and insurance questions:

- Do existing liability coverages extend to cyber liability?
- What is covered in the available cyber liability policies?
- Are there data security problems not dealt with in cyber liability policies?
- Does cyber liability coverage require the policyholder to have a cybersecurity program in place?
- What is a cybersecurity program?
- Will we secure lower cyber liability insurance premiums if we have a security program in place?

Does existing liability coverage extend to cyber liability losses?

Probably not. It is unwise for business clients to rely on their commercial general liability (CGL) policy for coverage if a cyber-related loss occurs. Traditional CGL policies cover the insured for losses resulting from bodily injury and property damage. Property insurance typically addresses "direct physical loss" to tangible property. Cyber-related losses generally involve loss or damage to data, computer programs, and other intangible assets, and the costs of restoring data, extortion, customer notification, ongoing identity protection for customers affected by a breach, forensic experts, legal and public relations experts, and more. These losses do not fall within the ambit of CGL or property coverage.

There are cases in which coverage was extended under general liability policies by the courts. These relatively rare decisions often involved losses for invasion of privacy rights and defamation under the "personal and advertising injury" portion of the CGL coverage form.[2] These cases are an exception and will become increasingly rare now that the International Organization for Standardization (ISO) has developed a form exclusion for cyber-related losses.[3] In July 2014, the ISO released an exclusion for access or disclosure of confidential or personal information and data-related liability. It excludes coverage for losses arising from a data breach concerning confidential or personal information, including patents; trade secrets; processing methods; customer lists; and financial, credit card, health, or any other nonpublic information. This exclusion provides a limited exception when the breach results in bodily injury arising out of electronic data.[4]

Certain types of cyber liability claims might fall within the directors and officers (D&O) liability forms or other errors and omissions coverage, and these should be maintained for reasons beyond the possibility that they might apply to some aspect of a cyber-related loss. Generally, they will not provide coverage for losses sustained in cyber incidents; if they do, coverage will be minimal.

What do cyber liability policies cover?

Cyber liability policies typically provide first-party and third-party liability loss coverages.[5]

First-party coverage[6]

- Breach response or crisis management costs
- Data recovery and computer program costs
- Cyber extortion/ransomware loss
- Business interruption loss
- Social engineering fraud loss
- Payment Card Industry Data Security Standard (PCI-DSS) fines

Third-party coverage[7]

- Data and network event liability
- Media liability[8]
- Regulatory defense and penalties, including privacy

Many cyber liability policies cover defense against regulatory claims only, without coverage for the penalties and fines imposed by regulatory agencies. Others offer coverage for penalties and fines along with the cost of defense. For any company that maintains personal identifiable information or protected health information, notification of a data breach is necessary and required by law in many states.[9] In our experiences, most cyber policies extend coverage for costs of

AT A GLANCE

The growth of cybersecurity and privacy regulation makes maintenance of best practices for cybersecurity a requirement, not an option.

Policyholders should not rely on traditional liability insurance to provide coverage for cyber liability losses.

Increasingly, businesses must demonstrate adequate cyber insurance coverage and best practices in data protection.

privacy breach notification up to a specified number of potential victims. They often provide coverage for public-relations specialists to manage potential damage to a company's reputation; attorneys to address regulatory investigations and penalties; and forensic IT professionals to determine the how, when, and scope of the breach. This "crisis management" coverage is not an aspect of general liability, property, D&O, or other forms of errors and omissions insurance.

Crisis management does not carry the same importance for all businesses, but certain aspects of breach-response coverage will usually be important to an insured. While most carriers include coverage for breach response, the assistance varies by insurer. Some policies offer a list of experts and tutorials while others have an approved team of responders activated upon notice of breach. At least one carrier provides a separate limit (e.g., $1 million) that applies only to breach-response costs and does not erode the policy's aggregate coverage limit.[10]

Under most forms for third-party cyber liability, coverage is provided on a "claims made" and reported basis. Most policies provide for a defense, with defense expenses charged against and reducing the aggregate limit of liability. The wrongful act or breach need not take place during the policy period for coverage to apply under most policies so long as the claim is first made and reported to the insurer within the inclusive dates of coverage.[11] In addition, our experiences have been that some carriers will provide, upon request, "full prior acts" coverage, which provides coverage for an unknown incident that occurred before the inception of coverage.

First-party liability coverage is generally for losses first discovered during the policy period. In some policies, crisis management and breach remediation costs must relate to wrongful acts taking place during the policy period and incurred within a specified time (for example, 12 months) following the wrongful act. Extortion/ransomware incidents have seen the highest increase.[12]

Should a cybersecurity program be in place before applying for cyber liability coverage? Which should be done first—securing coverage or establishing a security protocol?

Usually, underwriters do not require a cybersecurity assessment or program before processing an application for cyber liability insurance. Generally, underwriters do not deny an application for insurance because these assessments have not been completed or a monitoring program is not in place.

A cybersecurity "gap assessment" of a client's computer network and the establishment of a security-monitoring program typically take longer to complete than securing coverage. It is advisable to review available cyber liability policies and apply for coverage as soon as practicable without waiting for completion of a gap assessment.

If the client completes a gap assessment before securing cyber liability coverage, will the assessment result in a lower policy premium?

For first-time applicants, the answer is no. It is unlikely that a completed gap analysis or an established security plan will affect the initial policy premium. It will, however, expand the pool of insurance companies willing to underwrite the risk, and possibly provide broader coverage forms and higher primary limits. In subsequent policy years, completing a gap assessment, remediating vulnerabilities, and establishing a security-monitoring program (without experiencing a breach) may result in a lower premium. Ultimately, the goal is for clients to put themselves in the best situation with the underwriter compared to other risk.

What is a gap assessment, and what is cybersecurity monitoring?

This depends on the security framework (regulations and guidelines) applicable to the client's business. Some regulations and guidelines apply to a broad range of industries and businesses,[13] while others are tailored to specific markets such as the healthcare industry or banking and financial industries.[14] There are state, national, and international regulations.[15] There are guidelines issued by industry organizations that aren't law, but reflect widely accepted best practices.[16] Often, these frameworks overlap. More than one security framework may apply to your client. Regrettably, security within an organization is rarely addressed until there has been a breach or an audit by a regulator. Qualified cybersecurity providers will determine the frameworks and security protocols that will address an incident before it occurs.

The security guidelines and regulations most commonly implicated in U.S. business are:

- PCI-DSS: The Payment Card Industry Data Security Standard provides guidelines for the security of networks that maintain payment card information.[17]
- HIPAA and HITECH: Government-issued, mandatory regulations for protecting personal health information. These regulations apply to healthcare providers broadly and to many businesses that are vendors to health providers, including law firms engaged in their business or the defense of certain actions against them.[18]
- GDPR: The General Data Protection Regulation has the force of law in European Union countries and applies to non-EU businesses that process personal data of subjects in the EU.[19]
- NIST: Guidelines issued by the National Institute of Standards and Technology are not mandatory and are not a singular set of controls, but are widely accepted; customers may require compliance.[20]
- ISO: Guidelines issued by the International Organization for Standardization consist of many sub-frameworks pertaining to a variety of industries. ISO 27001/27002 addresses data security.[21]

Security gap assessment

A security gap assessment is the first phase of most compliance efforts. It evaluates an organization's security posture and focuses on various security principles within each department. It identifies concerns or weaknesses in policy, procedure, and configurations. Completing a gap assessment is an integral step in developing an IT and organizational risk analysis, which is a control requirement for most compliance frameworks and an industry best practice. It should explain the vulnerability of the network and the steps needed to protect it.

The assessment begins with interviews of the client's personnel to learn about how data is processed, transmitted, and stored internally and externally. It includes an assessment of existing digital security measures, physical security practices, remote users, equipment (including smartphone access), and more. A gap assessment may involve vulnerability scans or penetration testing to detect digital pathways into a network and its vulnerabilities.

A security gap assessment may include:

- Study of network and data flow within the organization
- Inspection of security for onsite and offsite locations
- Review of information security risk matrix
- Review of change management processes
- Review of security incident response
- Review of disaster recovery and business continuity
- Review of new hire, employee transfer, and employee termination processes
- Review of internal and external applications
- Review of software development processes
- Review of existing security awareness and programs
- Review of firewall and router rule sets
- Review of third-party risk assessments
- Review of internal information security policies[22]

Security monitoring

The second phase of a security program is the continuous compliance of technology, people, and processes. This phase typically includes implantation, configuration, and monitoring of the same components reviewed during the gap assessment. Necessary tools and resources are strategically overlaid into the organization's network. Security tools are implemented to ensure a layered security strategy to protect the organization's critical data and operations. These tools and systems ensure continuous monitoring and real-time alerts if an attempted or successful breach occurs. The monitoring of systems and applications is an integral part of a security strategy, but so too is training. Trained personnel are the first line of defense.[23]

The most common form of malicious attack is email phishing, where attackers—impersonating customers, vendors, or others—send emails hoping to get employees to click, execute, or download malicious content. Training personnel in security awareness helps balance layered security and the requirements of normal business operations. Continuous compliance efforts are essential, including monitoring, maintenance, and documentation on a regular basis.

Conclusion

This article was designed to answer the most basic questions about cyber liability insurance and cybersecurity programs. Ultimately, our clients will require the services of insurance and cybersecurity experts. Clients should know that insurance agents who handle their business policies may not have sufficient knowledge on cyber liability coverage to provide adequate service. Many agencies have individuals who specialize in cyber liability coverage or associate with agencies that have these specialists. Clients should inquire about their agents' experience in this developing area of coverage.

Cybersecurity firms have certified experts in security assessments and monitoring protocols. This is not something

that should be left to any IT vendor. Important certifications to ask for include CISSP (Certified Information Systems Security Practitioner), CISA (Certified Information Systems Auditor), CEH/CPT (Certified Ethical Hacker/Certified Penetration Tester), PCIP (Payment Card Industry Professional), and HITRUST-CSF practitioner (Health Information Trust Alliance–Common Security Framework). Although it is not essential for a single consultant to have all of these certifications, the greater the areas of certification the more likely the consultant will possess the education, experience, and skills required to properly advise the client.[24]

It is important for counsel to verify that the compliance program and related documentation prepared by the cybersecurity vendor meet applicable statutory requirements. Clients may have to produce this documentation in response to legal or regulatory proceedings or for examination by potential customers with cyber insurance and security requirements. ■

Steven M. Hickey is a shareholder in the law firm of Hickey, Cianciolo, Finn & Atkins PC in Troy. He serves on the SBM Insurance and Indemnity Law Section Council. His firm practices in insurance coverage analysis and insurance-related litigation.

Waleed Haddad is a partner and security/compliance director at Access Interactive in Novi. He is certified as a HITRUST-CSF practitioner, payment card industry professional (PCIP), certified ethical hacker, and penetration tester (CEH/CPT). He has developed and continues to develop security and compliance programs from the ground up within the financial, government, education, and healthcare sectors.

James "Jamie" Parry Jr., CIC, is a principal with Mason McBride, Inc & Summit Risk Management LLC in Troy. He is a certified insurance counselor and has served on several insurance company advisory councils. Mason McBride/Summit is a Trusted Choice Independent Insurance Agency and a member of the Keystone Group, providing insurance and risk management services.

ENDNOTES

1. Rizkallah, *The Cybersecurity Regulatory Crackdown*, Forbes (August 25, 2017) <https://www.forbes.com/sites/forbestechcouncil/2017/08/25/the-cybersecurity-regulatory-crackdown/#afbb3314573d> [https://perma.cc/B7GL-8J3V] and Ruzic, *Increased FTC Enforcement Highlights Need for Cyberregulatory Coverage*, Bradley Arant Boult Cummings LLP (March 6, 2018) <https://www.lexology.com/library/detail.aspx?g=1b9815c9-5126-41ea-9a00-22d3026bcd74> [https://perma.cc/6UJ3-JB4S]. All websites cited in this article were accessed January 31, 2019.
2. *Travelers Indem Co of America v Portal Healthcare Solutions*, 35 F Supp 3d 765 (ED Va 2014).
3. ISO Endorsement CG 21 06 05 14 (Exclusion—Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability—With Bodily Injury Exception).
4. *Id.*; Insurance Journal, *ISO Comments on CGL Endorsements for Data Breach Liability Exclusions, Interview with Ron Beiderman* (July 18, 2014) <https://www.insurancejournal.com/news/east/2014/07/18/332655.htm> [https://perma.cc/WZ6E-WC2R].
5. For example, Travelers' CyberRisk Form CYB-3001 (Ed 07-10); Beazley Breach Response Form F00653 112017 ed; Chubb Form 14-02-22815TX (10/2017); and Chubb Forefront Portfolio 3.0 Cybersecurity Coverage Part 14-02-17276 (12/2010), among many others.
6. *Id.*
7. *Id.*
8. Generally, "media liability" coverage is for claims of unauthorized use of copyright, trademark, defamation, disparagement, plagiarism, and interference with an individual's right of publicity.
9. Cal Civ Code § 1798.81.5 (2016) and § 1798.91.04 (2019); Colo Rev Stat § 6-1-713.5 (2018); and Conn Gen Stat § 38a-999b (2015) and § 4e-70 (2015). See National Conference of State Legislatures, *Data Security Laws/Private Sector* (January 4, 2019) <http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx> [https://perma.cc/53VF-Y3Q5].
10. Beazley Breach Response Form F00653 112017 ed.
11. The policies referenced in n 5 provide this coverage.
12. *Id.*
13. E.g., General Data Protection Regulation of the European Union (GDPR) <https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en> and ISO/IEC 27001-ISO/IEC 27002 <https://www.iso.org/isoiec-27001-information-security.html> [https://perma.cc/VU5G-496A].
14. E.g., 45 CFR Parts 160, 162, and 164. For HIPAA Privacy and Security Rules and HITCH Rules, go to US Dep't of Health & Human Servs, *Health Information Privacy* <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html>.
15. E.g., see nn 9, 13, and 14.
16. E.g., Payment Card Industry Data Security Standards <https://www.pcisecuritystandards.org/pci_security/> and ISO/IEC 27001-ISO/IEC 27002.
17. Payment Card Industry Data Security Standard v 3.2.1 (May 2018) <https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss>.
18. HIPAA Regulations 45 CFR Parts 160, 162, and 164 and HITECH Act Regulations 42 CFR Parts 412, 413, 422, and 495.
19. The European Parliament and the Council of the European Union, Regulation (EU) 2016/679 (General Data Protection Regulation) (2016) <https://gdpr-info.eu/>.
20. National Institute of Standards and Technology, *Cybersecurity Framework: Framework Documents* (April 2018) <https://www.nist.gov/cyberframework/framework> [https://perma.cc/VBB2-VUBG].
21. ISO/IEC 27001:2013 <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en> [https://perma.cc/3LKA-CYXT].
22. These steps in a security gap assessment are drawn from the security frameworks most commonly encountered in the cybersecurity business, like those listed in nn 17–21.
23. The importance of trained personnel is emphasized in all of the important cybersecurity frameworks, including those listed in nn 17–21.
24. Hoffman, *10 Most Popular Certifications Needed for Cybersecurity Careers*, InCyberDefense (August 28, 2018) <https://incyberdefense.com/exclusive/10-certifications-cybersecurity-careers/> [https://perma.cc/Z7SN-Q52K] and Tittel & Lindros, *Best Information Security Certifications 2019*, Business News Daily (November 29, 2018) <https://www.businessnewsdaily.com/10708-information-security-certifications.html> [https://perma.cc/9BLW-MX2B].