# What Type of Management Is Required to Stop Serious Cyberattacks?

The actual level of cyberrisk that many organizations face is now far out of alignment with what top management would consider an acceptable level of cyberrisk. In 2017, Warren Buffett, the chairman and chief executive officer (CEO) of Berkshire Hathaway, publicly called cybersecurity "the number one problem with mankind."[1] Consistent with his assessment, every year the number and the severity of losses in the information security and privacy areas gets progressively worse.

Although many statistical indicators could be cited, the Ponemon Institute/IBM *2019 Cost of a Data Breach Report* provides a good illustration of this trend. It states that the average cost of a data breach in the United States is US$8.19 million. This is up from US$7.91 million in 2018.[2] Results from prior years of the study show a pattern of increasingly severe consequences associated with information security and privacy breaches. The fact that both organized crime and nation-states have now become frequent attackers is yet another cause for justified alarm. The mounting losses are actually a motivator: Cyberattacks are so financially lucrative now that they strongly incentivize attackers to fully exploit existing vulnerabilities for their own gain, and they should incentivize top management to pay more attention to this area.

One might logically conclude that the continual upswing in the cost of cyberattacks and the costs


**Charles Cresson Wood,** JD, CISA, CISM, CGEIT, CIPP/US, CISSP
Is a management consultant and an independent compliance auditor located in Mendocino, California, USA. With more than 40 years of experience in this field, he has worked with more than 125 organizations in the information security and privacy areas. He is best known for his book *Information Security Policies Made Easy*. He is also the author of two related books, *Information Security Roles and Responsibilities Made Easy* and *Corporate Directors' & Officers' Legal Duties for Information Security and Privacy: A Turn-Key Compliance Audit Process*. He can be reached at *www.dutiesaudit.com*.

**Jody R. Westby**
Is the chief executive officer (CEO) of Global Cyber Risk, a Washington DC, USA-based consultancy that specializes in cyberrisk assessments, incident response planning, cybergovernance, and digital inventories and data mapping. She also serves as adjunct professor at Georgia Institute of Technology's School of Computer Science (Atlanta, Georgia, USA). Westby chairs the American Bar Association's (ABA's) Privacy and Computer Crime Committee, is co-chair of the ABA's Cybercrime Committee and has served four terms on the ABA President's Cybersecurity Legal Task Force. She speaks globally and is the author of six books and numerous articles on cybersecurity, privacy and cyberrisk management. She is a professional blogger for *Forbes* and authors a regular column on cybersecurity issues for *Leader's Edge* magazine. She can be reached at *www.globalcyberrisk.com*.

they impose on victims should cause the US Congress, the United Nations and business associations to become more involved in addressing the issue. In actuality, very little progress has been made in the United States or globally to counter these trends. Globally, it is similarly clear that the harmonization of laws and regulations is urgently needed because the existing legal and economic system fails to incentivize proper action to address this important area.[3,4] The Council of Europe Convention on Cybercrime (also known as the Budapest Convention)[5] was opened for signature on 23 November 2001 and became effective 1 July 2004. The treaty's intent was to harmonize substantive and procedural cybercrime laws for signatory countries to help facilitate cybercrime investigations. After nearly 20 years, 65 countries have agreed to the treaty, but with approximately 230 countries and territories connected to the Internet, the Convention is far from being a global solution.

Inconsistencies in cybercrime legal frameworks are only one part of the cybercrime problem. Differences in privacy and cybersecurity laws—especially in the United States—exacerbate the problem. Every US state now has its own version of a breach notification law, and many of these contain prebreach information security program requirements. Many of the states are following California's lead with its California Consumer Privacy Act (CCPA) and are considering similar, broader privacy laws.

With the EU General Data Protection Regulation (GDPR), its Directive on Security of Network and Information Systems, EU Cybersecurity Act, and the EU Cybersecurity Certification Framework, the legal landscape for privacy and cybersecurity is extremely fragmented, and it is difficult for organizations to meet their compliance requirements. A more standardized and coordinated approach is badly needed, not just nationally, but internationally as well.[6,7,8,9]

This type of integrated and broadly applicable, multilateral legislative effort will take considerable time, but there are steps that each organization can take on its own, right now, to help reverse the continual rise in cyberattacks. It is widely known that Albert Einstein said, in effect, that one cannot solve problems with the same thinking that created them. This notion is applicable to harmonizing legal frameworks and changing the continual rise in cybercrime and its cost to business.

For more than two decades, the management of IT risk, including privacy and information security, has been handled the same way: It has been managed as a technical issue, not a management issue. However, it is, and always has been, properly both a technical and a management effort. To transform the fragmented approaches to privacy and information security, a different type of thinking is needed. All cyberrisk management begins with roles and responsibilities and appropriate oversight using those roles and responsibilities.

"FOR MORE THAN TWO DECADES, THE MANAGEMENT OF IT RISK, INCLUDING PRIVACY AND INFORMATION SECURITY, HAS BEEN HANDLED THE SAME WAY."

The implementation by organizations of well-established management principles for information security and privacy results in fewer cyberattacks and better enterprise risk management. The focus here is on management's rigorous clarification, assignment, and evaluation of roles and responsibilities for information security and privacy. This approach can be implemented by all organizations, including private sector firms, charitable and nonprofit organizations, and government agencies and departments.

## Focus on Roles and Responsibilities

Operating systems involve millions of lines of code; system architectures of IT networks involve subnetworks, servers, routers and switches, each with their own configuration; security software tools often have incompatible conceptual frameworks; and third-party vendors often have different business models and security controls.

Management cannot be expected to understand all of that, let alone comprehend all that must be done to protect the network, systems and data in such environments. Accordingly, management must delegate responsibility for the management of these technical aspects to chief information officers (CIOs), chief information security officers (CISOs), and chief privacy officers (CPOs) or data protection officers (DPOs).

Nonetheless, top management cannot delegate the overall management and governance of information technology, privacy and information security; it is a responsibility that must be retained at the director and officer level. To be clear, members of the top management team must not only perform some of the work themselves, but they must delegate key responsibilities for some of the work and exercise oversight of that work. This requires clarity about the roles and responsibilities to be performed by boards and executives and the CIO, CISO, CPO/DPO and their teams. Many organizations lack clarity about the roles and responsibilities of these positions, which also means they lack clarity about how to manage information security- and privacy-related risk.[10, 11]

There is plenty of publicly available evidence behind previous data breaches to support the observation that organizations do not have a clear understanding of what they must do to establish an acceptable level of information security and privacy for their operations. A review of the US Federal Trade Commission's (FTC's) privacy and security enforcement cases reveals a long list of gaps in privacy and information security programs that the FTC determined amounted to an unfair or deceptive trade practice.[12] These gaps, which can include something as basic as failing to regularly install software patches, have resulted in very serious and expensive breaches, often involving the personal data of millions of people.

For example, the Equifax breach in 2017 involved 147 million individual credit reports.[13] The attack on Equifax exploited a vulnerability[14] in unpatched software that the company knew about and for which a patch existed, and the attackers were able to thereby gain access to the company's network and data. The FTC, the US Consumer Financial Protection Bureau (CFPB) and US attorneys general from 50 US states reached a settlement with the credit bureau for US$575 million.[15] In another example, Facebook was fined a record US$5 billion by the FTC for repeatedly using deceptive disclosures and settings with respect to its user privacy controls, in violation of an existing FTC order it was under. The Facebook settlement also required:

> *Facebook to restructure its approach to privacy from the corporate board-level down and established strong new mechanisms to ensure that Facebook executives are accountable for the decisions they make about privacy, and that those decisions are subject to meaningful oversight.*[16]

> "MANAGEMENT TEAMS AT MANY ORGANIZATIONS GENERALLY WANT THE TECHNICAL STAFF TO HANDLE PRIVACY AND INFORMATION SECURITY MATTERS AND NOT GET INVOLVED THEMSELVES."

Although the same is increasingly true globally, these US enforcement and regulatory efforts in response to cyberattacks reveal the ability of regulators at the federal and state levels to work together in their enforcement and reach a unified settlement. The FTC has also begun to place more emphasis on management's involvement in privacy and information security. In an effort to strengthen FTC orders with respect to privacy and information security, on 6 January 2020, the FTC outlined three major changes that could be expected in future orders. Those orders would be more specific, increase third-party assessor accountability and "elevate data security considerations to the C-suite and board level."[17]

There are a few generalizations that can be fairly made about current privacy and information security management practices, irrespective of whether those efforts are being performed in-house or by third parties. First, there is a widespread desire for top managers to keep their hands off of these matters. For example, management teams at many organizations generally want the technical staff to

handle privacy and information security matters and not get involved themselves.

However, information security governance best practices and standards[18] and current court decisions require all levels of management, including the board of directors (BoD), to be actively involved with information security and privacy. Thus, information security and privacy cannot be entirely delegated. In fact, taking such an approach may constitute a breach of management's fiduciary duty of loyalty (duty to monitor).[19]

Second, there is a pervasive misconception by top management at far too many organizations that privacy and information security can be solved by buying a variety of technical tools and outsourcing the related work. Although products and services are important components of privacy and cybersecurity programs, they cannot replace the human element of these issues, nor can they replace the clarification of roles and responsibilities that has to be performed in-house. Consider that 90 percent of the information security and privacy incidents reported to the UK's Information Commissioner's Office (ICO) in 2019 were attributable to human error.[20] Other reports indicate that employees are the weakest link in a cybersecurity program and are the targets of spam and phishing campaigns. Likewise, a 2019 Microsoft report revealed that employees and executives alike are targeted by cybercriminals in spam and spear phishing campaigns.[21] The human element of information security and privacy is clearly not being addressed adequately.

Third, another foundational misconception about information security and privacy held by management and BoDs is that this area can be relegated and assigned to IT staff. In actuality, many IT personnel are not very knowledgeable about information security and privacy, and they have had no formal training on these issues—their expertise is in IT. Information security and privacy are enterprise issues because information is used by, and fluidly moves throughout, organizations and, therefore, this area must be addressed in a multidisciplinary manner with cross-departmental and cross-organizational participation. This means that it must be coordinated and managed at the highest levels of the organization.

This also means that information security and privacy must be the responsibility of everyone in the organization, with key roles for the management and governance of these areas clearly defined, including those of the BoDs. The place to start—the foundation on which all other management and governance activities are based—is the clear and definitive articulation of privacy and information security roles and responsibilities by senior management and its BoDs.

"ALTHOUGH PRODUCTS AND SERVICES ARE IMPORTANT COMPONENTS OF PRIVACY AND CYBERSECURITY PROGRAMS, THEY CANNOT REPLACE THE HUMAN ELEMENT OF THESE ISSUES."

## Plumbing as an Apt Metaphor

History can be a lesson for those in the information security and privacy field. There is no need to repeat the same mistakes. In 1926, a group of Los Angeles plumbing inspectors realized that there were no uniform specifications for the installation and maintenance of plumbing systems.[22] At that time, disease was rampant, and it was, in part, spread by improper sanitation (e.g., leaky toilets). Working with sanitation engineers, mechanical engineers, journeymen plumbers and public utility officials, these plumbing inspectors developed the Uniform Plumbing Code, which went on to be revised and adopted by many standards bodies including the American National Standards Institute (ANSI), American Society of Sanitary Engineering (ASSE) and the World Plumbing Council (WPC). Among other things, that plumbing code defined the tasks to be performed by various participants such as the journeyman plumber, the inspector and the manufacturer.

Improper sanitation can be analogous to the way that information security and privacy is practiced at many organizations today. In the information

security and privacy areas, numerous standards and best practices have been developed, they are largely consistent, and they have been mapped to one another. The problem is that organizations are not integrating them into their information security and privacy programs, and their management and executive teams are not exercising appropriate oversight to even know or understand that their in-house efforts are deficient. At the most fundamental level, laws should ensure that the required roles and responsibilities for privacy and information security will be performed, but even that is rarely understood, often out-of-sync with other incentive systems, and not sufficiently specified or kept up to date.[23]

This appeal to clarifying the minimum roles and responsibilities for information security and privacy teams is based on the belief that this is central to allocating appropriate funding and implementing information security and privacy programs aligned with best practices and standards. These responsibilities include regular risk assessments that must be reviewed and signed off on by directors and officers. Clearly defined and assigned roles and responsibilities are the first step toward establishing a viable culture supportive of information security and privacy. For example, the US Department of Justice's "Evaluation of Corporate Compliance Programs," a document used when determining fines and other penalties after a violation of the law, includes a discussion of roles and responsibilities as well as corresponding organizational structure.[24]

## Next Steps

The essence of the suggested approach is role clarification, role assignment, role negotiation, role monitoring and role reporting to interested parties. The assignment of key roles and responsibilities for cybersecurity and privacy are management tasks and a well-established component of good management practice.[25, 26, 27] In the information security and privacy realm, this approach has most often not been sufficiently adopted by organizations because the area has erroneously been perceived to be solely a technical concern.

Today, it is generally accepted that information security and privacy are cross-functional, cross-organizational activities. It is long past the time for generally accepted management practices to include information security and privacy so that the assets of the organization will be better protected and cyberattacks will be reduced. The added benefit is serving as a good corporate role model and achieving a competitive advantage.

> "THE ROLES OF THE KEY INDIVIDUALS ACROSS AN ORGANIZATION WHO ARE RESPONSIBLE FOR INFORMATION SECURITY AND PRIVACY MUST BE EXPLICITLY ASSIGNED."

It also boosts compliance. Formal roles and responsibilities for top management and BoDs in IT governance are not only a good idea to mitigate losses, but they also are now required by law.[28] At far too many organizations, both top management and BoDs have not been adequately briefed about information security and privacy compliance requirements and their particular roles and responsibilities. Legal statutes and regulations best practices and standards, and case law require senior management and BoDs to protect the assets of the organization. For example, both top management and the BoD have a legal duty to personally investigate, pay attention to and reasonably respond to hazardous conditions that are related to the organization.[29]

Furthermore, it is well established that officers and directors have a duty to make sure that the organization meets its compliance requirements.[30] If executives and board members have not adequately met these responsibilities, they have not fulfilled their roles, and they run the risk of shareholder derivative suits for breach of their fiduciary duties to the organization.[31]

## The Foundation for Improving Information Security and Privacy Maturity

The following six recommendations embrace not just proven good management practices but also the minimum requirements of the law and best practices and standards for information security and privacy.

These recommendations focus on roles and responsibilities as the critical foundation needed to develop and maintain an information security and privacy program with appropriate oversight to help turn the tide on both the mounting losses and the erosion of trust that accompany those losses. These recommendations enable organizations to get out in front of the train and lay some new track. Like railroads, the Internet has become another foundational infrastructure system that supports enormous growth in productivity and the economy.[32]

> "FAR TOO MANY ORGANIZATIONS ASSIGN INFORMATION SECURITY AND PRIVACY RESPONSIBILITY TO THE CIO OR A PERSON ON THE IT STAFF AND STOP THERE."

Some of these basic, legally mandated roles and responsibilities for information security and privacy governance are nondelegable duties that top management or the BoD must perform. For example, the US State of New York Department of Financial Services Cybersecurity Regulation requires a Certificate of Compliance that must be filed annually and signed by a board member or senior officer stating that they have reviewed all relevant documents and certify that the organization is in compliance with the regulation.

### Designation of Roles

The roles of the key individuals across an organization who are responsible for information security and privacy must be explicitly assigned. This includes the BoD's audit and risk committees, the executives responsible for the overall management of the organization (i.e., chief executive officer [CEO], chief operating officer [COO], chief financial officer [CFO], general counsel or chief legal officer [CLO], chief compliance officer [CCO], CIO, CISO, DPO or CPO), business unit managers, head of human resources (HR), risk manager, head of communications and head of procurement. If the organization is large enough to engage in government relations at the state or federal level or participate in the work of standards-setting bodies, public-private committees or multinational fora, the roles of these individuals should also be clearly defined.

Far too many organizations assign information security and privacy responsibility to the CIO or a person on the IT staff and stop there. That is not good enough. Each of the roles stated are generally performed by someone. Organizations need to analyze who in their organization is filling key management functions and assign those persons a specific role for the information security and privacy areas. In smaller organizations, a person may serve in more than one of these roles, in which case their responsibilities will be expanded. It should be noted that information security and privacy responsibilities should not be assigned to the same person, as this can create segregation-of-duties issues (the objectives of security in some areas are in opposition to and in competition to those of privacy). Clear designation of each role lays the foundation for the creation of a cross-organizational team that can, and should, communicate and coordinate with other members of the team throughout the year.

### Specification of Responsibilities

The responsibilities for each role should be clearly defined, including specific duties, reporting relationships, decision-making powers, performance reviews, key performance indicators (KPIs) and required tasks. Ideally, these should be included in the person's job description. The purpose of the clarification of responsibilities is to ensure that key actions are performed and eliminate confusion or disputes regarding each role.

Similarly, the responsibilities of BoD committees with respect to privacy and information security often are not well understood. Although audit committees previously were assigned the responsibility of information security and privacy

compliance and the related risk management, it is now more common that a separate board risk committee handles these issues as part of its management of enterprise risk.

BoD responsibilities should include a review of cyberrisk insurance coverage to ensure that risk is appropriately transferred, mitigated, avoided and accepted. For example, many cyberrisk insurance policies are not clear about whether cyberattacks that may be attributed to a nation-state will be covered or deemed an "act of war" (*force majeure*). Organizations must be clear about the different types of risk they are facing and whether the related financial risk has been transferred to insurance companies or not.

**Agreement to Designated Roles and Responsibilities**

Those who have been assigned a designated role and responsibilities for information security and privacy must formally (in writing) agree to accept these responsibilities. Detailing the responsibilities in a job description is one way to have implied agreement. Otherwise, the responsibilities should be set forth in writing and a written acceptance of those responsibilities should be obtained (in a contract in the case of a third party).

A formal written acceptance of responsibilities means that the parties not only understand their role but that they also take the matter seriously and understand their responsibilities and that they are accountable for them. Alternative avenues for the acceptance of roles and responsibilities can be achieved with employment contracts, departmental mission statements, committee charters, policy and guideline statements, codes of conduct, outsourcing contracts and similar documents. Some organizations even go one step further, requiring individuals to attend specialized training programs, which include an acknowledgment that they understand the material by passing a test.

In addition to the specific roles and responsibilities for privacy and cybersecurity, the protection of an organization's data and IT systems is a shared responsibility that should be clearly set forth in an organization's code of conduct, employee handbook and top-level policy.

> "A CULTURE EMBRACING CLEARLY DEFINED ROLES AND RESPONSIBILITIES, SUPPORT FOR THE RULE OF LAW AND GROUP MUTUAL SUPPORT, THAT IS COUPLED WITH WILLING AND VOLUNTARY COMPLIANCE WITH ASSIGNED ROLES, IS ABSOLUTELY CRITICAL."

**Enforcement of Designated Roles and Responsibilities**

Both the private and public sectors need to regularly measure performance according to the designated roles and responsibilities, particularly for key roles. It is important that the responsibility for information security and privacy thereafter be enforced. Many organizations fail to ensure that responsibilities are performed, take steps to determine whether related policies and procedures are complied with, or review the effectiveness of existing incentives encouraging consistent compliance. It is important that employee handbooks, codes of conduct, and information security and privacy policies state that compliance is mandatory and violations of policies may result in disciplinary action up to and including termination. Organizations that conduct annual performance reviews could easily include this effort in the annual review process. When employees know that being responsible for information security and privacy will be part of their performance review, they are more likely to take these matters seriously and refrain from skirting these duties.

**Testing of Designated Roles**

All too often, after a breach or serious information security or privacy problem, the responses undertaken are chaotic, and those actions indicate that the response team did not understand clearly who was responsible for certain critical tasks, activities and projects. This often occurs when external players, such as outside counsel, forensic investigators, crisis communication firms or law enforcement are brought in to assist with a response. It is important that the management of specific external players be assigned to an internal person. For example, the general counsel or chief legal officer manages outside counsel and the forensic investigation, coordinating with the CISO and DPO/CPO.

Internal and external roles should be clearly specified in the incident response plan and regularly reviewed and maintained. The problem in too many cases is that incident response plans are not tested, or perhaps are tested only with a few of the players, such as the technical team and legal counsel, but such testing leaves many other key players out of the test. In addition, incident response plan tests are often not performed annually, thus the people with assigned roles and responsibilities get rusty, take other jobs, or may not be up-to-speed with either the threat environment or the current information systems.

**Culture in Support of Roles**

One of the most important responsibilities of senior management and the BoD is to establish a culture of integrity and compliance that is supportive of information security and privacy. This begins by setting the tone from the top that is conveyed in codes of conduct, high-level policies, and the visible undertaking of their responsibilities with respect to information security and privacy programs.[33] Such an enterprise culture underpins and accelerates the success of all information security and privacy programs.

A culture embracing clearly defined roles and responsibilities, support for the rule of law and group mutual support, that is coupled with willing and voluntary compliance with assigned roles, is absolutely critical. The culture also needs to have incentive systems, reinforcements, and rewards that encourage adherence to these roles and responsibilities.

## The Future Will Not Be an Extrapolation of What Is Current

As the coronavirus (COVID-19) pandemic revealed, the future will not be a simple linear extrapolation of trends that have occurred in the past. The coronavirus is not just another version of the flu; it is something unique and novel and much more serious than anything the world has ever experienced. The same is true with the information security and privacy threat environment: The attacks and methods employed can and will be unique, and the consequences will be devastating. Although rapid change characterizes both domains (e.g., mutations and innovations), the latter realm is much more challenging because the adversaries are using dynamically mobilizing advanced technologies, such as artificial intelligence (AI), to exploit weaknesses in information security and privacy. The latter is much more challenging because constantly shifting human ingenuity is brought to bear by human attackers.

> "HACKING AND CRACKING HAS BEEN AUTOMATED SO THAT THE THREAT HAS BEEN MARKEDLY MAGNIFIED."

For example, the 2017 WannaCry and NotPetya attacks caused the largest disruption of computer systems and cyberbusiness interruption losses the world had ever seen.[34] Attackers are now deploying artificial intelligence (AI) and machine learning to identify weaknesses in the protection systems that have been deployed. Attackers are exploiting the billions of unsecure Internet of Things (IoT) devices to gain entry to enterprise and government systems. Hacking and cracking has been automated so that the threat has been markedly magnified.

Every successful approach to counter the rising tide of cybercrime, system outages and related losses must begin with the assignment of clear roles and responsibilities for privacy and information security that are performed by the board, down to every employee, and also to all involved third parties. Such a successful effort requires a commitment to develop and maintain information security and privacy programs that are aligned not only with best management practices but also with best technical practices. Six specific ways in which those two domains can and should now be combined have been outlined herein.

This means that BoDs and senior management need to assume the roles they have been skirting, including getting personally involved in reviewing budgets for information security and privacy programs, evaluating the performance of others working in this same area, ensuring that the

organization has a strong culture supportive of information security and privacy, and participating in the regular testing of contingency plans.

## Endnotes


1 Warren Buffett made these remarks during the 2017 annual Berkshire Hathaway shareholders' meeting. Buffett indicated that cyberattacks and related problems were a bigger threat to humanity than nuclear weapons. Had he made these remarks in late 2020, he probably would have placed pandemics first and cyberattacks second. In full disclosure of Buffett's position, it should be mentioned that some of the companies Berkshire Hathaway owns, such as American International Group, offer insurance against cyberattacks and related problems such as cyberbullying.

2 IBM, *2019 Cost of a Data Breach Report*, USA, 2019, *https://www.ibm.com/security/data-breach*

3 Wood, C. C.; W. S. Rogers, Jr.; R. S. Poore; "Why It's Now Time for an Internationally-Harmonized Regime for Information Security and Privacy," *Sci-Tech Lawyer* (American Bar Association), April 2018, *https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2018/spring/why-its-now-time-an-internationally-harmonized-legal-regime-information-security-and-privacy/*

4 For a broader discussion about restructuring incentive systems to work in a manner that supports information security and privacy, see Wood, C. C.; "Solving the Information Security and Privacy Crisis by Expanding the Scope of Top Management Personal Liability," *Journal of Legislation*, vol. 43, no. 1, December 2016

5 Council of Europe, Convention on Cybercrime, ETS No. 185, 2001, *https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185*

6 *Op cit* Wood, Rogers, Poore

7 Westby, J. W.; "US Companies Unaware of EU Cybersecurity Regulations," *Forbes*, 7 October 2019, *https://www.forbes.com/sites/jodywestby/2019/10/07/us-companies-unaware-of-eu-cybersecurity-regulations/#4faab60d7174*

8 Westby, J. R.; "EU Cybersecurity Certification Schemes Will Surprise US Businesses," *Forbes*, 21 October 2019, *https://www.forbes.com/sites/jodywestby/2019/10/21/eu-cybersecurity-certification-schemes-will-surprise-us-businesses/#743da8853802*

9 Westby, J. R.; "Why the EU Is About to Seize the Global Lead on Cybersecurity," *Forbes*, 31 October 2019, *https://www.forbes.com/sites/jodywestby/2019/10/31/why-the-eu-is-about-to-seize-the-global-lead-on-cybersecurity/#1699d7b22938*

10 Westby, J. R.; "Don't Make Dangerous Decisions," Leader's Edge, 16 August 2019, *https://www.leadersedge.com/p-c/dont-make-dangerous-decisions*

11 Westby, J. R.; "The Insider Threat," Leader's Edge, June 2019, *https://www.leadersedge.com/p-c/the-insider-threat*

12 Federal Trade Commission, "Privacy and Security Enforcement," USA, *https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement*

13 Brewster, T.; "Equifax Just Got Fined Up to $700 Million for That Massive 2017 Hack," *Forbes*, 22 July 2019, *https://www.forbes.com/sites/thomasbrewster/2019/07/22/equifax-just-got-fined-up-to-700-million-for-that-massive-2017-hack/?sh=3b85794e3e96*

14 Federal Trade Commission v. Equifax, Inc., USA, 2019, *https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_complaint_7-22-19.pdf*

15 Federal Trade Commission, "Equifax to Pay $575 Million as Part of Settlement With FTC, CFPB, and States Related to 2017 Data Breach," USA, 22 July 2019, *https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related*

16 Federal Trade Commission, "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook," USA, 24 July 2019, *https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions*


## Enjoying this article?

- Read *State of Cybersecurity 2020, Part 2: Threat Landscape and Security Practices. www.isaca.org/state-of-cybersecurity-2020*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

17 Smith, A.; "New and Improved FTC Data Security Orders: Better Guidance for Companies, Better Protection for Consumers," Federal Trade Commission, USA, 6 January 2020, *https://www.ftc.gov/news-events/blogs/business-blog/2020/01/new-improved-ftc-data-security-orders-better-guidance*
18 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27014 *Information technology—Security techniques—Governance of information security*, Switzerland, 2013, *https://www.iso.org/obp/ui/#iso:std:iso-iec:27014:ed-1:v1:en*
19 *Marchand v. Barnhill*, 212 A. 3d 805 (Del. 2019) (the board has a duty to establish an information system that informs them of risks, and then to monitor the information that the system produces); Francis v. United Jersey Bank, 432 A.2d 814, 821-822 (N.J. 1981) (directors have a duty to monitor the affairs of the corporation and to remain informed about the affairs of the corporation) (hereinafter "Marchand"); *In re Caremark Int'l Inc. Deriv. Litig.,* 698 A.2d 959 (Del. Ch. 1996) (the board has a duty to exercise good faith judgment when determining that the corporation's information and reporting system is in concept and design adequate to assure the board that the appropriate information will come to its attention in a timely manner as a result of ordinary operations) (hereinafter "Caremark").
20 Hill, M.; "90% of UK Data Breaches Due to Human Error in 2019," *Infosecurity Magazine*, 6 February 2020, *https://www.infosecurity-magazine.com/news/90-data-breaches-human-error/*
21 Kelley, D.; S. Kathuria; "Spear Phishing Campaigns—They're Sharper Than You Think," Microsoft, 20 December 2019, *https://www.microsoft.com/security/blog/2019/12/02/spear-phishing-campaigns-sharper-than-you-think/?ranMID=24542&ranEAID=TnL5HPStwNw&ranSiteID=TnL5HPStwNw-bRsRfeHe81NZA.dztxVNkA&epi=TnL5HPStwNw-bRsRfeHe81NZA.dztxVNkA&irgwc=1&OCID=AID2000142_aff_7593_1243925&tduid=%28ir__d1l1yfr9kokftwhakk0sohznxu2xny0awxwc2vuc00%29%287593%29%281243925%29%28TnL5HPStwNw-bRsRfeHe81NZA.dztxVNkA%29%28%29&irclickid=_d1l1yfr9kokftwhakk0sohznxu2xny0awxwc2vuc00*
22 American National Standards Institute (ANSI), *2018 Uniform Plumbing Code*, IAPMO/ANSI UPC 1—2018, p. iv–v
23 Wood, C. C.; "Solving the Information Security and Privacy Crisis by Expanding the Scope of Top Management Personal Liability," *Journal of Legislation*, vol. 43, issue 1, December 2016, *https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1661&context=jleg*
24 US Department of Justice Criminal Division, Evaluation of Corporate Compliance Programs, June 2020, *https://www.justice.gov/criminal-fraud/page/file/937501/download*
25 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27001:2013 *Information technology—Security techniques—Information security management systems—Requirements*, Switzerland, 2013, *https://www.iso.org/standard/54534.html*
26 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27014: 2013 *Information technology—Security techniques—Governance of information security,* Switzerland, 2013, *https://www.iso.org/standard/43754.html*
27 Sostrin, J.; "To Be a Great Leader, You Have to Delegate Well," *Harvard Business Review*, 10 October 2017, *https://hbr.org/2017/10/to-be-a-great-leader-you-have-to-learn-how-to-delegate-well*
28 See, e.g., US Sarbanes-Oxley Act (SOX) § 404 (2002), which requires that certain members of the top management team make representations about the adequacy of a publicly listed firm's financial internal controls, and of course information security and privacy are a significant part of every organization's internal controls. Numerous other laws contain requirements that are specific to privacy and cybersecurity, such as the US Health Insurance Portability and Accountability Act (HIPAA), the US Federal Information Security Modernization Act (FISMA), and the US State of New York Department of Financial Services Cybersecurity Regulation.
29 *Lobato v. Pay Less Drug Stores*, 261 F.2d 406 (10th Cir. 1958). A director or officer can be held personally liable for damages caused to third parties when he/she reasonably should have known that failure to act would lead to a hazardous condition or an injury to a third party.

30 Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Concerning the Conduct of Certain Former Officers and Directors of W.R. Grace & Co., 65 SEC Docket 1240, Release Document No. 34-39157 (Sep. 30, 1997). Corporate directors have a duty to protect shareholder interests and that includes the use of compliance systems to both monitor management and subordinate employees, so that they are shown to be in compliance with the law.

31 *Op cit* Marchand and Caremark

32 Just as businesses were able to find new customers through the new transcontinental railway system, it also enabled new markets to develop. The transcontinental railway system helped to unify the United States and made wagon trains obsolete. Through this transcontinental railway system, goods from Asia were shipped to the West Coast of the United States and, similarly, goods from Europe were shipped to the East Coast. Although the original intent was to develop and populate the interior of the United States, the transcontinental railroad system also created faster routes between Europe and China. By 1900, 30 percent of the world's goods were manufactured by the United States, and the transcontinental railroad system had a big part to play in that success. When a single reliable standardized system is built, and it responds to a major need, it markedly facilitates commerce and innovation. Just as most people do not appreciate how significant the transcontinental railway was to US history, most people today do not appreciate how important clarified and agreed-upon roles and responsibilities are to information security and privacy.

33 Wood, C. C.; "Integrated Role Clarification and Performance Evaluation: Key to a Successful Information Security and Privacy Effort," *ISSA Journal,* August 2020

34 Greenberg, A.; "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, 22 August 2018, *https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/*