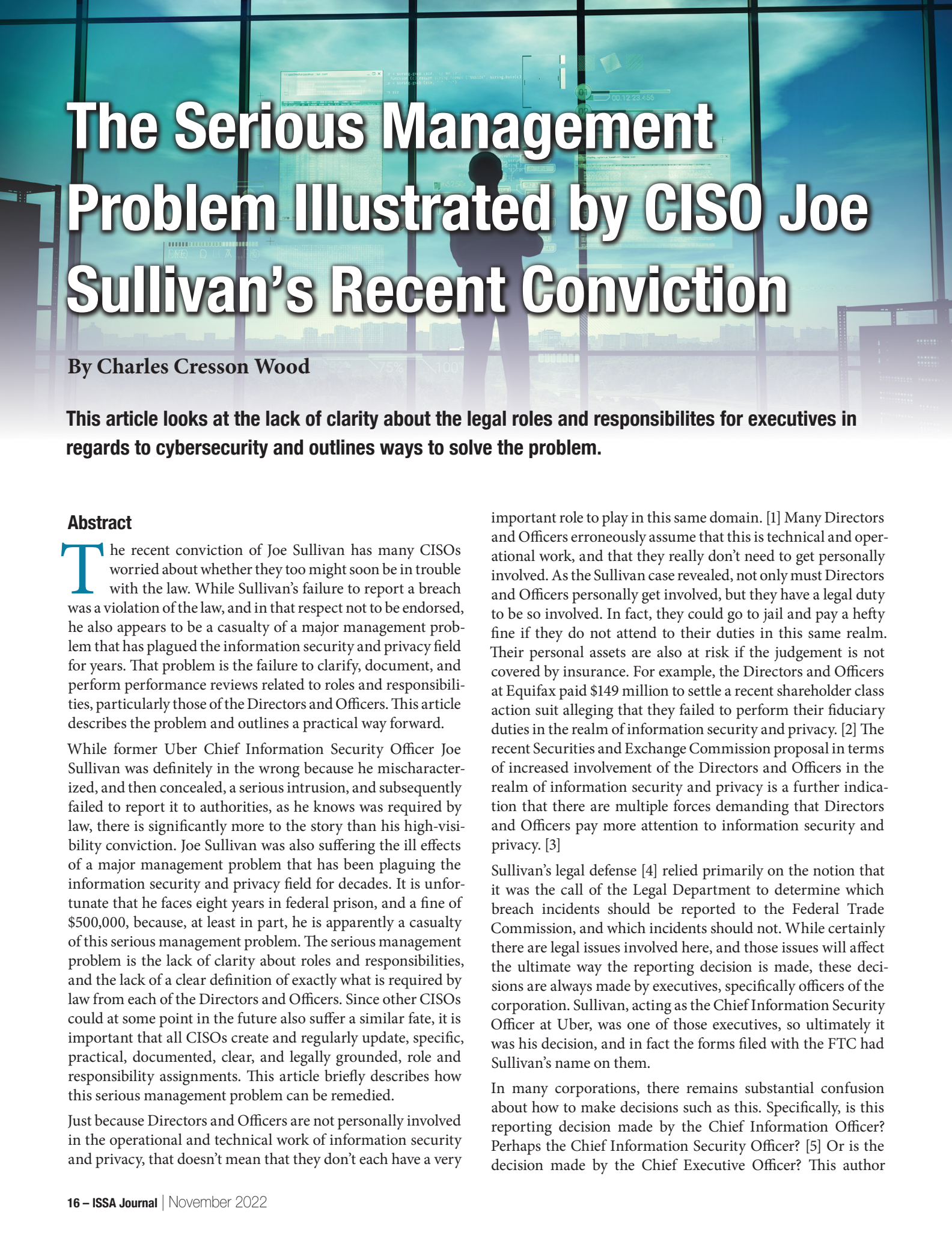




The Serious Management Problem Illustrated by CISO Joe Sullivan's Recent Conviction

By Charles Cresson Wood

This article looks at the lack of clarity about the legal roles and responsibilities for executives in regards to cybersecurity and outlines ways to solve the problem.

Abstract

The recent conviction of Joe Sullivan has many CISOs worried about whether they too might soon be in trouble with the law. While Sullivan's failure to report a breach was a violation of the law, and in that respect not to be endorsed, he also appears to be a casualty of a major management problem that has plagued the information security and privacy field for years. That problem is the failure to clarify, document, and perform performance reviews related to roles and responsibilities, particularly those of the Directors and Officers. This article describes the problem and outlines a practical way forward.

While former Uber Chief Information Security Officer Joe Sullivan was definitely in the wrong because he mischaracterized, and then concealed, a serious intrusion, and subsequently failed to report it to authorities, as he knows was required by law, there is significantly more to the story than his high-visibility conviction. Joe Sullivan was also suffering the ill effects of a major management problem that has been plaguing the information security and privacy field for decades. It is unfortunate that he faces eight years in federal prison, and a fine of \$500,000, because, at least in part, he is apparently a casualty of this serious management problem. The serious management problem is the lack of clarity about roles and responsibilities, and the lack of a clear definition of exactly what is required by law from each of the Directors and Officers. Since other CISOs could at some point in the future also suffer a similar fate, it is important that all CISOs create and regularly update, specific, practical, documented, clear, and legally grounded, role and responsibility assignments. This article briefly describes how this serious management problem can be remedied.

Just because Directors and Officers are not personally involved in the operational and technical work of information security and privacy, that doesn't mean that they don't each have a very

important role to play in this same domain. [1] Many Directors and Officers erroneously assume that this is technical and operational work, and that they really don't need to get personally involved. As the Sullivan case revealed, not only must Directors and Officers personally get involved, but they have a legal duty to be so involved. In fact, they could go to jail and pay a hefty fine if they do not attend to their duties in this same realm. Their personal assets are also at risk if the judgement is not covered by insurance. For example, the Directors and Officers at Equifax paid \$149 million to settle a recent shareholder class action suit alleging that they failed to perform their fiduciary duties in the realm of information security and privacy. [2] The recent Securities and Exchange Commission proposal in terms of increased involvement of the Directors and Officers in the realm of information security and privacy is a further indication that there are multiple forces demanding that Directors and Officers pay more attention to information security and privacy. [3]

Sullivan's legal defense [4] relied primarily on the notion that it was the call of the Legal Department to determine which breach incidents should be reported to the Federal Trade Commission, and which incidents should not. While certainly there are legal issues involved here, and those issues will affect the ultimate way the reporting decision is made, these decisions are always made by executives, specifically officers of the corporation. Sullivan, acting as the Chief Information Security Officer at Uber, was one of those executives, so ultimately it was his decision, and in fact the forms filed with the FTC had Sullivan's name on them.

In many corporations, there remains substantial confusion about how to make decisions such as this. Specifically, is this reporting decision made by the Chief Information Officer? Perhaps the Chief Information Security Officer? [5] Or is the decision made by the Chief Executive Officer? This author

contends that it should be the latter, but in this particular instance, according to what we know about what happened at Uber during Sullivan's tenure there, the CEO didn't know about the intrusion. In more general terms, is this matter something that is handled by lower-level management only, or is it something that needs to be brought to the highest level of executive management? If there is to be a tiered approach, where only serious intrusions are reported to executive management, then what is the cut-off and is that cut-off indeed justifiable?

Beyond the requirements of the law, each organization will make these and related information security and privacy decisions a bit differently. The management keys needed for success in this area are: (a) reaching an internal consensus of clarity about the necessary roles, (b) orchestration of the coordination of roles across multiple departments, and third parties as well, (c) assignment of duties to specific roles with individual accountability, (d) regular review and update of these duties and roles (to reflect changes in both the law and new business relationships), (e) clear documentation in job descriptions, committee mission statements, and departmental mission statements, (f) regular checking to make sure essential duties are being performed (for example via performance reviews), and (g) usage of penalties/rewards based on adherence to the duties assigned (alignment of incentive systems). All this is not rocket science, but it is generally used for lower-level employees only in the domain of information security and privacy. These same generally accepted management practices need to be applied to executive management, and the board of directors as well.

As a bit of background to the Joe Sullivan case, by all published accounts that this author was able to locate, Sullivan was an exemplary Chief Information Security Officer, serving at Facebook, Cloudflare, as well as Uber. Before that, he worked for the US Department of Justice as an attorney prosecuting information security cases. He was generally known as one of the best practitioners in the field. One would not expect him to be convicted of criminal obstruction related to a breach that took place in 2016. Instead of doing what was required by law, i.e., reporting the breach to the federal government, under Sullivan's guidance, the company categorized the breach, and a related \$100,000 bitcoin payment to the involved hackers, as a bug bounty matter. Supposedly, that made the incident not reportable. Sullivan claimed (but the jury did not agree) that it was not his job to report the breach, that it was instead the job of the legal department to handle this work. If an attorney who specializes in this same field (Sullivan), who has many years of prior experience in this same field, still can't get this right, then it is not surprising that other CISOs are wrestling with these matters too. [6] While there are other aspects to the story, the crux of problem here is that there was confusion about what the minimum legal obligations are, and who should be doing what, in the realm of information security and privacy.

The excuse that information security and privacy is a new field, and that we are still trying to understand it, still trying to appreciate what is required, is no longer going to be credible in a court of law, as the Sullivan conviction clearly shows. This

field has been in existence for several decades now, and it's now clear what must be done, although the financial resources to do those things are often not budgeted. One of the most significant reasons why these resources aren't in the budget at many organizations, is that financial incentives push decision-makers to make decisions which favor low costs, high profits, high stock prices, high quarterly bonuses, etc. [7] When the Directors and Officers are directly and explicitly confronted with their legal duties in this realm, through the process described in this article, the resources are understandably much more likely to be forthcoming. Likewise, if their performance bonus or some other significant incentives are tied to having a successful information security and privacy effort, then too the necessary resources will be forthcoming much more readily. And having specific statements of roles and responsibilities for all involved Directors and Officers, and doing compliance auditing against that, will also go a long way towards getting an adequate budget.

Another excuse that is often raised when there has been no substantive action in the domain of information security and privacy roles and responsibilities, is that the field is still in flux, and that the legal and regulatory requirements have not yet been definitively clarified, and that this situation supposedly justifies a lack of action within a particular user organization. While it is true that the field is evolving rapidly, and that there are many changes on a regular basis, it is also clear that we have enough publicly accessible information on which to readily develop a definitive collection of laws, regulations, contracts, consent decrees, and other legal obligations to which a particular firm, and its Directors and Officers, are required to adhere. The fact that this definitive collection of legal obligations now exists enables many other related activities, such as use of compliance checks of the Directors and Officers by insurance companies as an application-related hurdle that must be cleared prior to the issuance/renewal of Directors and Officers liability insurance policies. Still another useful application of third-party independent compliance checking involving the Directors and Officers is as a due diligence process prior to the completion of a merger or acquisition.

The path to clarity of roles and responsibilities begins with a custom evaluation of the requirements dictated by laws, regulations, contracts, etc. The results of this effort will of course vary from firm to firm. For example, this unique collection of legal requirements depends on the industry, the jurisdiction (e.g., the state where the corporation is incorporated), types of information handled, types of technology deployed, contracts in force, litigation now in process, etc. After this minimum legally dictated level of roles and responsibilities is explicitly defined, it can then be used by the Compliance Department, or the Internal Audit Department, to periodically perform a compliance review, to determine whether the Directors and Officers are doing all that the law requires. Yes, Directors and Officers should be the subject of compliance reviews in the domain of information security and privacy, just like lower-level employees, and third parties as well. In fact, when the Directors and Officers go through something like this process on a regular basis, and they get a third-party lawyer auditor to perform an

independent audit, the resulting professional opinion letter can be an important document helping to establish trust with third parties. And, on a related note, after the minimum required by law has been defined, then the organization can and should add additional roles and responsibilities, to achieve competitive advantage, to facilitate the operational activities related to certain products and services, etc.

In summary, a major problem that has caused Joe Sullivan, and so many other CISOs as well, so much trouble is the widespread failure of American corporations to adequately clarify and document the roles and responsibilities related to information security and privacy. The first factor that must be considered when attempting to remedy this major problem is to know the minimum required by law. All allocations of roles and responsibilities must cover the fundamental points found in the minimum required by law. If organizations don't even have clarity about the minimum required by law, then they aren't going to do a good job when it comes to allocating roles and responsibilities. And if roles and responsibilities are poorly defined, then important tasks are likely to fall between the cracks, and intrusions and other problems (as Joe Sullivan experienced) are the likely result.

In terms of the action steps to make substantial improvements in this area, organizations need to clarify and document what exactly the Directors and Officers are required to do by law. Then an internal compliance checking process can be undertaken. Using the traditional risk assessment process (as found in the ISO 27000 standards), an institutionalized internal compliance review process should be created and followed. After full compliance has been demonstrated, third party lawyer auditors should be retained to verify the correctness of the internal compliance review's conclusions. Not only can this third-party review generate documentation that could legally protect the corporation, as well as the Directors and Officers, in a future court case, but this documentation can be an important motivational tool, much like annual performance reviews.

Furthermore, when Directors and Officers have their compliance with the minimum required by law reviewed by an independent third-party lawyer auditor, and when their incentive systems incorporate consideration of information security and privacy, that sends a very serious message. That message indicates the "tone at the top," and that tone will flow down to the rest of the organization, and then on out to third parties as well. In that way the Directors and Officers communicate to all employees, and related third parties too, that internal controls, like information security and privacy, are important, and must be a part of business as usual.

About the Author

Charles Cresson Wood, Esq., JD, MBA, MSE, CISSP, CISM, CISA, CGEIT, CIPP/US, is a compliance-related attorney and management consultant specializing information security and privacy. He is based in Lakebay, Washington. His latest book is entitled "Corporate Directors and Officers Legal Duties for Information Security and Privacy: A Turn-Key Compliance Audit Process." He can be reached via his web site www.dutiesaudit.com.

NOTES

1. See Charles Cresson Wood, "The Rules Have Now Been Clarified – The Minimum Legal Duties for Directors and Officers Are Both Established and Readily Determined," *ISSA Journal*, vol. 20, issue 5, May 2022.
2. For a high-level summary of this case, see Molly Stubbs, "Equifax Agrees to \$149 Million Settlement for Infamous 2017 Data Breach," *Expert Institute*, June 25, 2020. As an aside, it is unclear how much of this was paid by Directors and Officers liability insurance. There are also other recent high-visibility legal cases where the Directors and Officers paid a heavy price for failing to address information security and privacy. For example, as a result of a series of data breaches going back to 2013, the Yahoo! Directors and Officers several years ago settled with shareholders to the tune of \$80 million. For the details, see Kevin LaCroix, "Yahoo Settles Data Breach-Related Securities Suit for \$80 Million," March 5, 2018.
3. See "SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," March 9, 2022, U.S. Securities and Exchange Commission (www.sec.gov/news/press-release/2022-39)
4. For more background about the case, see Lily Hay Newman, "The Uber Data Breach Conviction Shows Security Execs What Not to Do," *Wired*, October 7, 2022.
5. Fully 36% of Chief Information Security Officers are not reporting breaches because they fear that they will lose their jobs as a result. This statistic is from a UK survey performed by Keeper Security, entitled 2021 Cybersecurity Census Report. If CISOs don't have the budget to do the job that needs to be done, there will be serious breaches, and the cover-ups will only conceal how the system is seriously broken, until the truth comes out some other way, such as in the mass media or in a lawsuit. Being clear about the minimum duties that are required by law sets a floor below which budgets must not go, and that process of gaining clarity can serve as starting point for rationalizing, harmonizing, and aligning the broken incentive systems at many organizations.
6. The Sullivan case, specifically the part of the case involving misprision of a felony (not reporting a breach when one has a duty to report), also makes ransomware negotiations and payments still more pressured, difficult, and complicated than they already are.
7. For a wide-ranging discussion of the effects of incentives on information security decisions, see Charles Cresson Wood, "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.