Ten Steps to Protect Privilege in the Event of Data Breach

Technology, Privacy, and eCommerce

CHEAT SHEET

- ***Spot the vulnerabilities.*** Before a breach occurs, general counsel should prepare a Vulnerabilities Report to assess the company's exposed areas and other concerns.
- ***Privileged communications.*** After a breach occurs, the general counsel should implement a manual or electronic privileged reporting channel, through which all communications related to the breach should be directed.
- ***First response.*** The incident response team should be included in the PRC protocols and be comprised of company officers, directors, employees, and internal or external experts.
- ***Notification requirements.*** Breach notification requirements depend on the magnitude of the breach, the type, the industry involved, and the jurisdiction(s) impacted.

On August 18, 2018, US President Trump announced the creation of a national Cyber Command on the same level as the Army, Air Force, Navy, and Marines. "The elevation of United States Cyber Command demonstrates our increased resolve against cyberspace threats and will help reassure our allies and partners and deter our adversaries," he declared.

With American commerce ever more dependent on digital information, data, and commerce, experts have also been ringing the alarm bells of inadequate cybersecurity louder and louder. Virtually every company has now suffered a cyberattack of some kind or another. Malware, ransomware, denial of service (DoS) attacks, phishing, password grabs, man-in-the-middle (MITM) schemes, malvertising, so-called drive-by-downloads, and plain rogue software — all have crippled companies and spawned tens of millions of dollars in liability, litigation, and legal fees, lost profits, and reputational damage.

Whether as a matter of national security or as a threat to critical business infrastructure and operations, cybercrime today poses one of the greatest risks to any organization's survival and bottom line. And when a cyberattack strikes, nothing could be more important to the office of the general counsel than executing the company's Critical Data Breach Checklist. But long before the breach occurs, steps should be taken to establish a privileged reporting channel (PRC) for all communications and information transmission.

1. Privileged communications

In the context of cyberbreach and its response and notifications, the primary privilege involved is the attorney-client privilege (along with its corollary, the work-product doctrine). These are the confidential communications and work transmitted between attorney and client on matters of legal versus operational interest and/or in anticipation of or involving litigation.

General counsel often walk a fine line, moving between the dual roles of providing regular, non-privileged business advice and engaging in the highly-protected attorney-client communications that can withstand forced disclosure. As a result, in-house counsel face a two-fold challenge of privilege protection: (1) shielding confidential information and advice by clearly defining privileged communications, and (2) waiving privilege by sharing or disclosing confidential information and

communications with non-clients and third parties.

Accordingly, for the GC, being ever-vigilant in the creation and protection of this privilege is of vital concern in the caustic arena that is cybersecurity.

2. Investigating and diagnosing cyber weaknesses and vulnerabilities

As with any disaster scenario — whether earthquake, hurricane, or cyberattack — the GC must commence preparations long before the event occurs. This begins with the investigation (which should be ongoing) of any vulnerabilities that may exist in the company's info security, privacy, and data retention systems. Generally headed by internal or external IT or cybersecurity teams, this investigation will result in a Vulnerabilities Report that details a lengthy list of concerns and problem areas.

In an ideal world, where money is no object and affordable manpower is limitless, all the vulnerabilities identified in this report would be instantly patched and permanently corrected. However, in the real world, it is far more likely that the weaknesses identified in the report will be addressed in a practical manner, in some order of priority. Certain remedies will be affordable, well within existing budgets, and capable of being corrected immediately. Others will have to wait to a later time, leaving an explicit, written record of unaddressed, known breach potentials.

If not properly protected, the Vulnerabilities Report, together with comments and remedial measures taken and not taken, could easily become Exhibit "A" in a plaintiff attorney's trial exhibit notebook during a post-breach lawsuit to demonstrate the company knew about vulnerabilities and deliberately chose not to address them. This entire hub of communications therefore takes on great significance, with the prospect of litigation always looming.

3. Establishing a privileged reporting channel to protect communications

At the first possible moment after breach notification, general counsel should implement a secure PRC for all related communications. With federal and state legal requirements ongoing, all communications related to the breach or potential breach should be directed through the PRC. This includes the Vulnerabilities Report, comments, and remedial steps taken, internal communications between company officers, directors, internal IT experts, employees, as well as external communications with outside counsel, outsourced contractors, and outside IT experts.

In-house counsel have two ways to establish a PRC: manually or electronically. Doing it manually, the old-fashioned way, involves time-consuming redactions, whiteouts and blackouts, and carefully controlled distribution to prevent inadvertent disclosure and consequent privilege waiver. Or, alternatively, a PRC can be accomplished with robust software that provides differential security protection, defined and limited access to privileged material, and cradle-to-grave monitoring and tracking.

Diligent GCs will have thoroughly considered these options well in advance of any breach notice.

4. Notify incident response team consisting of pre-designated executives, department heads, and technology experts

As with the PRC, the Incident Response Team (IRT) should be created as early as possible, and well in advance of the breach, because the truth is a critical data breach could occur any day. **Back on March 2, 2012, then-FBI Director Robert Mueller stated, "There are only two types of companies: those that been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again."** If it was prophetic then, it is passé today.

The IRT is a specific group of company officers, directors, employees, and experts (internal and/or external) who are pre-designated and assigned the responsibility of responding to a data breach. The IRT is in-house counsel's nexus for coordinating and responding to an incident when it occurs, for determining whether the incident is major or minor, and for managing the breach if it remains ongoing. At a minimum, this is also the team that must define the breach, repair the vulnerability, and respond to the incident by interfacing confidentially with all relevant team members and parties.

When communicating with the IRT, in-house counsel must ensure that communications take place in a privileged environment and within the confidential channel. This means the IRT must be fully onboarded to the PRC, taught how to label and mark communications to remain within the channel, and fully oriented to the need to protect communications from waiver through improper sharing or disclosure. Finally, the IRT must implement procedures for monitoring and tracking privileged materials, so that a complete and accurate file of privileged material is built from the outset.

5. Contacting outside counsel and forensic experts

In the event of a major breach, the first PRC communication by in-house counsel should be to pre-designated outside counsel, with whom all communications will be privileged. In the pre-designation process, outside counsel should be included in the PRC process, designated as a member of the IRT, and confirm they are capable of offering immediate counsel in the event of a breach. This is not a time when the general counsel wants to be interviewing law firms or broaching the subject with outside counsel for the first time.

With the PRC firmly in place, the in-house team should fully and frankly share, discuss, and analyze the incident with outside counsel, review the Incident Response Plan (IRP) as it applies to the minimal information known, and come to agreement on a preliminary plan, thus lending strength to the widest possible claims of attorney-client privilege and work product. While a strong argument can be made that "anticipation of litigation" is always assumed with a breach, it is always much easier to convince a skeptical judge if the confidential communications are run through outside counsel.

Topics of importance to be included in the initial and early discussions between in-house and external teams are evidence preservation, chain-of-custody, differentially-secured sharing of information with different levels of security, need-to-know permissions, optimal recipient designations, privilege protection considerations, and monitoring. Establishing a working forensic strategy going forward and operating within a system that technically and confidentially addresses the breach is primary.

One of the key delegations from in-house to outside counsel is the retention of appropriate experts. For in-house counsel to retain outside experts and consultants risks a court later concluding that none of the communications are privileged. On the other hand, when funneled through outside counsel via the PRC, outside consultants and experts more clearly fall under the privilege and work product umbrella. This is especially so if Vulnerability Reports are mixed with litigation assessments. And if these consultants are asked to make vulnerability assessments and reports, those reports are

even more sensitive. Unprotected communications can easily be deemed unprivileged later, with devastating results.

6. Breach notifications

A critical component of every IRP is notification of breach. Notification requirements depend on a variety of factors, including the magnitude of the breach (whether it's a "major incident" or not), the type of breach, the industry involved, and the jurisdiction(s) impacted. In 2003, California authored SB 1386 for Golden State companies, with 10 general compliance requirements. Many of these were adopted by the European Union in its landmark General Data Protection Regulation 2016/679, which took effect in May 2018. But every jurisdiction affected (international, federal, state, and local) must be examined carefully for unique breach notice requirements.

The office of the general counsel will be integral to the process of defining the level of the breach and the legal requirements triggered. Unfortunately, breach notification requirements are becoming increasingly complicated and overlapping. Today, it is not uncommon for differences to exist between different federal departments, different states, and different countries. For companies doing business nationally or internationally, this can be taxing, and mistakes can be made without very careful research and attention to detail.

7. Press and PR — Develop proactive strategies

How your company communicates with the public about a breach shapes the narrative that follows. In a world of 24/7 social media and news coverage, public scrutiny has never been higher or more intense. There are things your company must do independently, and those that are better outsourced, depending on the magnitude and type of breach.

Focusing on the company's proactive solutions should dominate in-house counsel's considerations, beginning with the issuance of a Holding Statement that relates the basic facts of the breach. How this is crafted has potentially enormous implications, not just for consumer relations, but for regulatory compliance and criminal and civil litigation.

Therefore, including a vetted PR individual or company on the IRT is highly recommended.

8. Contact law enforcement

For smaller breaches and in unique circumstances, reporting cyberattacks to law enforcement is not always a good idea. However, best practices dictate that in-house counsel notify law enforcement promptly of most serious data breaches (with criminal implications). Law enforcement is not a substitute for taking reasonable company responsive measures, but it can bring important resources to bear on the breach, follow the cyber-evidence off the company's network, and employ the power of warrants.

From a PR viewpoint, the involvement of law enforcement can also be reassuring. While on the one hand it highlights the seriousness of the problem, on the other it shows that the company is diligently seeking to catch the wrongdoer and correct the problem. This can be reassuring to investors and shareholders, as well as third parties and customers. This said, what can be expected from law enforcement must be tempered in terms of recovering funds and information lost, given law enforcement's limited resources.

Also, because law enforcement interaction makes certain evidence public, careful consideration must be given to preserving privileges and confidential information once the police become involved.

9. Breach documentation and evidence preservation

A natural tendency in any emergency is to dash in and try to fix the breach without thinking about the long-term consequences. Caution must be exercised to ensure this does not happen in the event of a cyberbreach whose causes and implications are not visible to the naked or untrained eye. In this haste, important evidence may be lost, compromised, or destroyed, preventing cyber investigators and law enforcement from doing their jobs, such as learning how malware entered a zero-day vulnerability.

A maxim for general counsel to live by could be: Breach response depends on the quality of the evidence preserved. Cybercriminals often do their best to erase their tracks, delete files, and create red herrings that muddy the waters of the digital crime scene, causing misdirection. Great initial caution must be exercised so evidence is not inadvertently or intentionally cleaned, swept away, or adulterated. In other words, treat the digital crime scene like you might a physical crime scene.

With close IT advice and monitoring, turning off servers, swapping out hard drives, creating forensically valid images, and basic backup all go a long way in preserving essential evidence. Again, imagine the law enforcement forensic squad wearing latex gloves and carefully bagging evidence after a major crime. In-house counsel should approach the data breach the same way, carefully monitoring and preserving evidence as an integral part of the IRP.

Evidence preservation also bears on the litigation that may follow. In-house counsel must be cognizant of the federal rule that whenever litigation is “reasonably anticipated,” all parties involved have an affirmative legal duty to preserve all potentially relevant evidence. In honoring this rule, of course, it iS crucial to funnel all communications through your PRC, preferably with the guiding hand of outside counsel to maximize privilege recognition.

10. Anticipating regulatory issues

The regulatory landscape for cybersecurity has never been so murky or complex. Certainly, part of this phenomenon is the delayed regulatory response to a world that’s become digital. For general counsel in this environment, however, many unique regulatory challenges have emerged.

Putting a magnifying glass on the Federal Trade Commission (FTC) sheds light on the rapid growth of affirmative agency action, and consequent challenges to in-house counsel. In the last 15 years, the FTC has initiated and resolved over 70 significant matters involving data security, most often following a major data breach or information security attack. Invariably these actions stemmed from the company’s failure to reasonably protect the private financial information of its customers and clients from cyberattack.

The FTC, of course, is not alone in this. Numerous other federal agencies have become active in investigating data breaches for regulatory violations. Among them are the FTC, the Securities and Exchange Commission, the Health and Human Resources Department, the Consumer Financial Protection Bureau, and even the Department of Defense. Any domain with digital repercussions could trigger an investigation and consequent legal implications.

In light of this, the office of general counsel is advised once again to keep all communications well within the PRC, involving qualified outside counsel from the outset.

Conclusion

It is the age of cybersecurity. On any given Monday, you could access your daily news — whether by newspaper or online push notice — and find the next major data breach incident stealing the headlines:

On April 3, 2018, the JokerStash hacker syndicate put five million credit and debit cards up for sale, all hacked from Saks Fifth Avenue and related companies.

On June 4, 2018, a security researcher creating a Vulnerabilities Report contacted the chief technology officer of MyHeritage, the genealogy site, indicating he had located a file entitled “myheritage” on a private server unrelated to the company. The result: 92 million records breached.

On June 27, 2018, the Sacramento Bee disclosed that 19.5 million records had been breached back in February 2018. Because it managed a database of voters, those records included voter registration data maintained by the California Secretary of State.

And of course, there were the 87 million records breached on Facebook.

Point being, one day that headline could feature your company. Given the inevitability of a breach occurring, the time for in-house counsel to become highly trained in cybersecurity response is now. Creating a secure PRC, with an established IRT, was yesterday’s task. Get your cyber-house in order, and rest more easily at night.

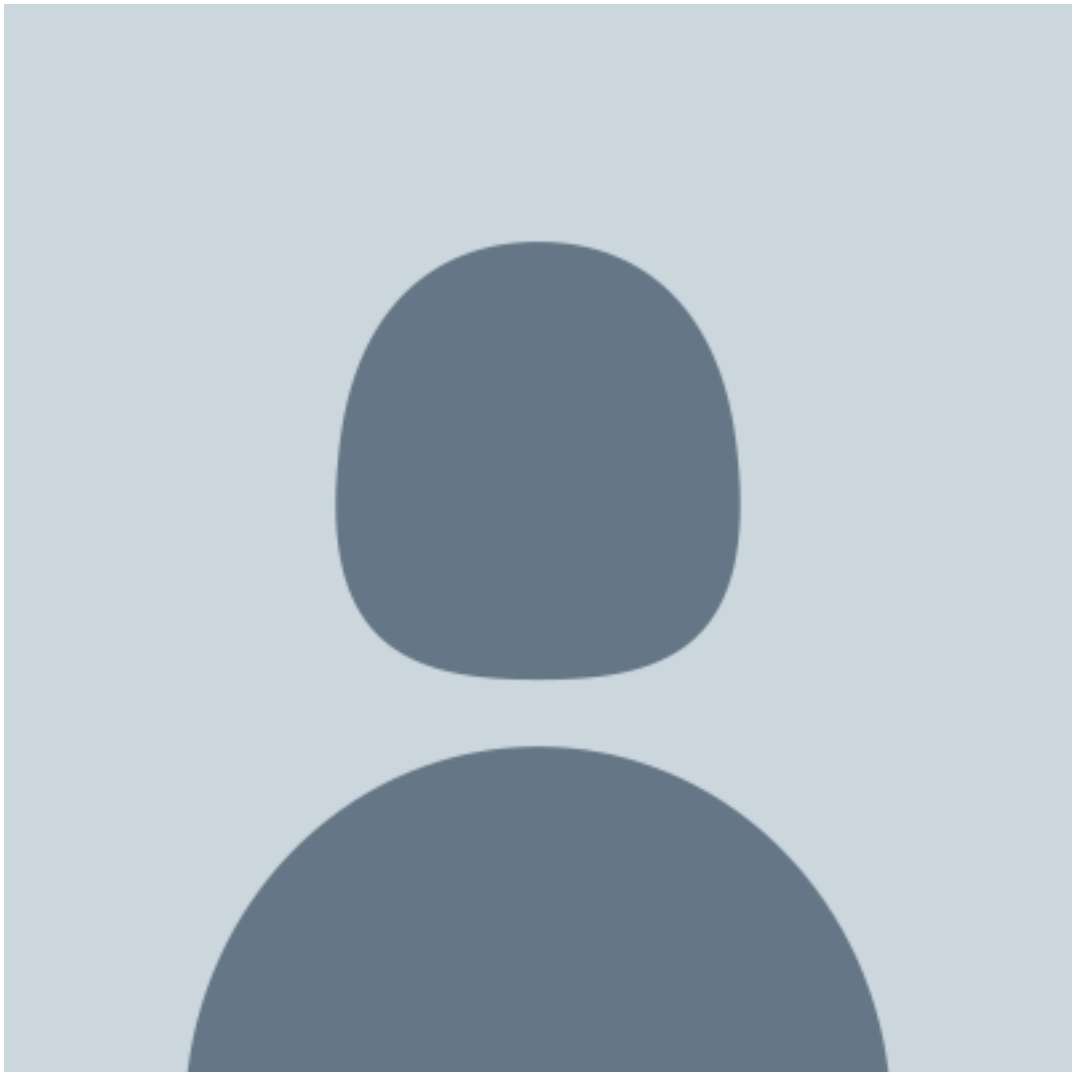
Pat Linden

General Counsel

WindTalker, Inc

He is a business and transactional attorney with more than 15 years of prior experience working in large law firms. He is instrumental in supporting WindTalker’s capital raising and acquisition strategies.

Christopher C. Combs



CEO

WindTalker, Inc

WindTalker, Inc. are developers of Privileged Reporting Channel and Distributed Sharing software that protects sensitive and privileged content for the lifecycle of the document. WindTalker's patented technology provides one central place to manage document, data, and content security. The company was founded in 2016 and is based in Atlanta, Georgia.