

Protecting Privilege in Practice: Cyber Incidents

Security incidents are unplanned events that can involve theft of data and impact business continuity. They present immediate and significant business and legal risks, driving the need for business solutions and legal advice. Using Cygnvs [a secure collaboration platform], organizations that prepare for incidents can set up work streams to obtain information needed to solve the business issues and get legal advice. This will establish and preserve attorney-client privilege and work product without slowing down the response.

The purpose of this white paper is to describe the three primary steps for successfully asserting that communications regarding the investigation of a security incident are covered by the attorney-client privilege. The application of privilege is not absolute and multiple factors affect a court's decision; this discussion does not guarantee an outcome. This paper also addresses the use of the Cygnvs platform as related to privilege. It should not be viewed as an endorsement or promotion of this or any other similar platform.

Cygnvs:

- Provides a secure, hassle-free and cloud-based interface to communicate and store documents both prior to and during a cyber incident.
- Can be used for out-of-band communications to discuss sensitive topics like containment and ransom negotiation strategy, or as an alternate communication channel if the incident has shut down email.
- Allows your contacts, documents and communications with insurance, legal counsel and vendors to be accessible anywhere and anytime via browser or mobile app.

Cygnvs Supports Incident Response Preparedness

You are encouraged to use Cygnvs before an incident occurs. Organizations are able to load their incident response plan and key contacts directly into the platform when they first receive access. Subsequently, they can configure an incident response room tailored to their incident response plan, which can include establishing connections with key third parties (e.g., insurance broker, external legal counsel, forensics). Organizations can simulate an incident in order to test and modify their plans. For example, an organization can simulate the compromising of its corporate networks and the need to move to an out-of-band communication channel to initiate its incident response plan. You can access the Cygnvs Mobile Application and ensure that everyone who needs to be involved

in the response is preregistered into the platform and has access to the documents they need. Another unique feature is the direct connectivity during the policy term to the insurance carrier and broker, where organizations can access news about the cyber-risk landscape and the pre-breach services that are available to policyholders (often at no cost).

Privilege Within Cyber Incidents and Breach Response

The attorney-client privilege generally protects communications made in confidence for the predominant purpose of obtaining legal advice. Confidential communications between corporate employees and counsel are privileged if the communications are for the predominant purpose of assisting counsel in rendering legal advice to the company. Attorney-client privilege can be extended to include a company's in-house counsel's communications with any corporate employee as long as the communication relates to the subject matter for which the company is seeking legal representation. Communications with independent contractors who are the "functional equivalent" of an employee can also be protected by this privilege.

The attorney-client privilege will also extend to the work and communications of third-party experts who were hired for the predominant purpose of obtaining confidential legal advice from the lawyer. Simply copying an attorney is not enough to make a communication privileged. Additionally, where the purpose of the communication is primarily for a business purpose or is unclear, it may also not be privileged.

Privilege in Practice: Establish, Preserve and Prove

With Cygnvs, organizations can manage incidents seamlessly with their counsel, vendors and insurance teams. An incident response room template can be utilized, so the business avoids the need to scramble during an incident.

Protecting Privilege in Practice: Cyber Incidents

Rooms can be tailored to specific subjects, and permissions can be assigned to restrict users to specific rooms. There can be multiple workstreams for different purposes, such as a work stream related to facts that may not be privileged, one for general communication or scheduling, and another workstream related to specific legal advice. Organizations (and counsel if granted permission) can control access to each workstream.

Attorney-client privilege and work product are important components of incident response strategy. Sometimes the “privilege” issue gets more attention than is warranted based on the number of incidents that occur, the number of times a lawsuit is filed in connection with an incident, and the number of times the issue of privilege is actually tested and results in a ruling by a court during litigation. To illustrate this, we note that BakerHostetler advised clients regarding 1,270 incidents in 2021. Among those 1,270 incidents, notifications were provided to individuals 525 times. Of those 525 instances in which notice was provided, 23 of the companies each had at least one lawsuit filed against it. As those 23 lawsuits are defended, it is likely that assertions of privilege and work product will be tested in only a few of them. The challenge is that a business often does not know at the start of the incident whether notification will be required or whether the incident will result in a lawsuit. If you do not establish the basis for privilege at the start, it may be challenging to claim later.

There are three components to effectively managing the issue of privilege and work product. You must establish the basis for its application, you have to preserve (and not waive) it during the incident, and then, if it is tested, you must have the ability to prove it.

Establish:

To establish privilege, forensic firms should be engaged by counsel for the purpose of providing legal advice. Subsequent communications with engaged firms and experts related to this work should be marked as privileged in order to support the application and make identification and collection of privileged communications easier. This may not include consultants who may be hired for purely business functions. An example would be a “helping hands” firm that is only carrying out work to restore operations, such as setting up a new device or cleaning affected devices. If the same company is retained for both forensic investigation and helping hands, there should be two separate and distinct scope of work agreements defined, the first to be executed with counsel and the second to be with just the organization. Within Cygnvs, a privileged room including forensics, legal teams and the client can be established along with a separate room for the IT and helping hands vendor, which would not necessarily be privileged.

Preserve:

Use of Cygnvs can assist with preservation. By restricting access and limiting various types of communication to certain rooms, organizations lessen the risk of waiver of privilege due to the potential

of sharing of information with third parties outside the privilege umbrella. A room assigned for IT workstream communication should only be used for carrying out work to restore operations, not for forensic findings and requests. The helping hands vendor should not be included in forensic status communications and calls. The restricted permissions feature allows organizations to think critically about what third parties may access, which allows them to protect and preserve privileged communications and documents. This also ensures that the right parties are in the appropriate place, which avoids waiver of privilege. Organizations should focus on maintaining consistency for the purpose of the provision of legal advice. In practice, this does not require every document or communication to be marked privileged. In fact, overextending the scope of confidentiality may undermine the claim of privilege. Rather, communications with regard to scope of work, recommendations and reporting should all come at the request of counsel. Use of Cygnvs’ rooms and permissions for access make consistency an easy task. All individuals necessary to maintain privilege are granted access to the room. There is no need to constantly ensure counsel is included in a certain communication. Individuals are added once and have access until their permissions are removed.

Prove¹:

In circumstances where privilege is challenged, external counsel and the internal legal team may need to provide declarations demonstrating the rationale behind the assertion for privilege and a showing that the predominant purpose is to obtain legal advice. There may need to be communications shown to the court in camera to demonstrate the purpose of the work as related to legal advice. Cygnvs’ technology enables clients to grant access solely to employees involved in the incident and provides fine-grained access to external providers – like law firms and cyber-incident response vendors – setting up specific workstreams where communication rules of engagement are defined and purposeful. With Cygnvs, there is no need to search through email inboxes or document management systems to find items relevant to the incident or communications to support a claim of privilege. When it is necessary to prove communications are privileged, organizations are required to make a “clear showing” that such communications were made for a legal, rather than a business purpose. There may be additional scrutiny given to in-house counsel communications because they may play multiple roles within an organization. The courts have found declarations from participating parties of the privileged communications to be persuasive. Therefore, it is important to keep lines clear and communications organized. Cygnvs databases can be archived and exported so that in the event of litigation or regulatory inquiries post-incident, documents to support privilege can be easily obtained.

¹ See Appendix for examples of cases where privilege was at issue following a cyber incident.

A View of Cygnvs:

CYGNVS

Marc Smith

Acme Llc.

Home

Notifications

Westside Health

Ransomware

Overview

Team

Workstreams

News

Analytics

Profile

Help Center

Sign Out

Acme Llc.

Search...

Policy Number: 0034TG564289 | Affected Entity - | Claim Id: - | Date of Incident: - |

Workstreams

Create Workstream

Carrier communication

1/6

Open

In Progress

Privilege space

1

8

Restricted

Complete

Broker communication

Open

Not Started

Risk management

Open

Not Started

Details

Add Detail

Name	Detail
Broker name	Demo Broker
Broker emergency contact information	cyber@demobroker.com
Insurer name	iDemo
Insurer emergency contact information	1-888-567-3645

Noticeboard

Leave a comment

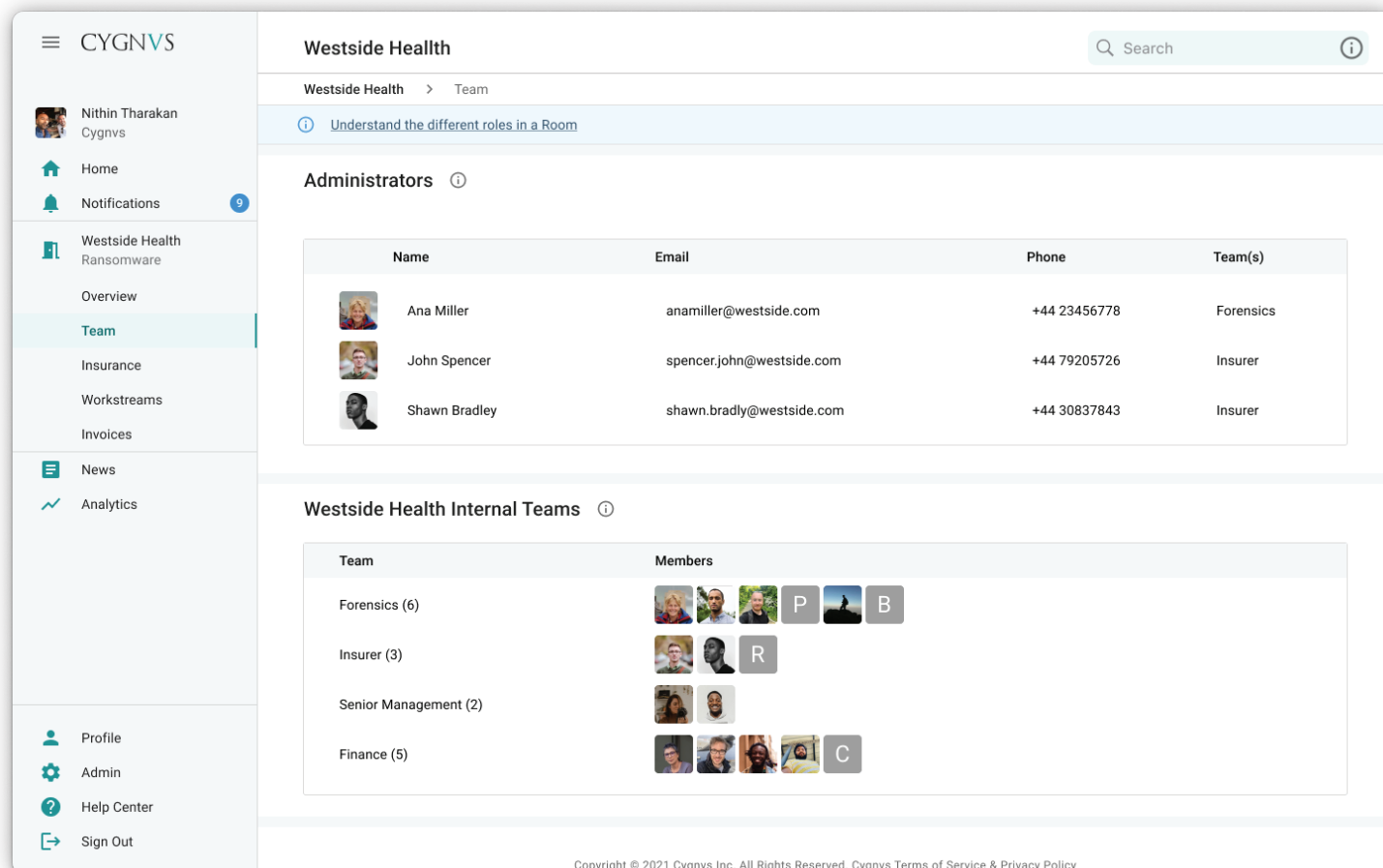
@

Copyright © 2021 Cygnvs Inc. All Rights Reserved. [Cygnvs Terms of Service](#) & [Privacy Policy](#)

View workstreams, connect with insurance contacts and quickly access policy documents.

3

A View of Cygnvs: *(Continued)*






Westside Health Search ⓘ













Westside Health > Team

ⓘ Understand the different roles in a Room

Administrators ⓘ

Name	Email	Phone	Team(s)
 Ana Miller	anamiller@westside.com	+44 23456778	Forensics
 John Spencer	spencer.john@westside.com	+44 79205726	Insurer
 Shawn Bradley	shawn.bradly@westside.com	+44 30837843	Insurer

Westside Health Internal Teams ⓘ

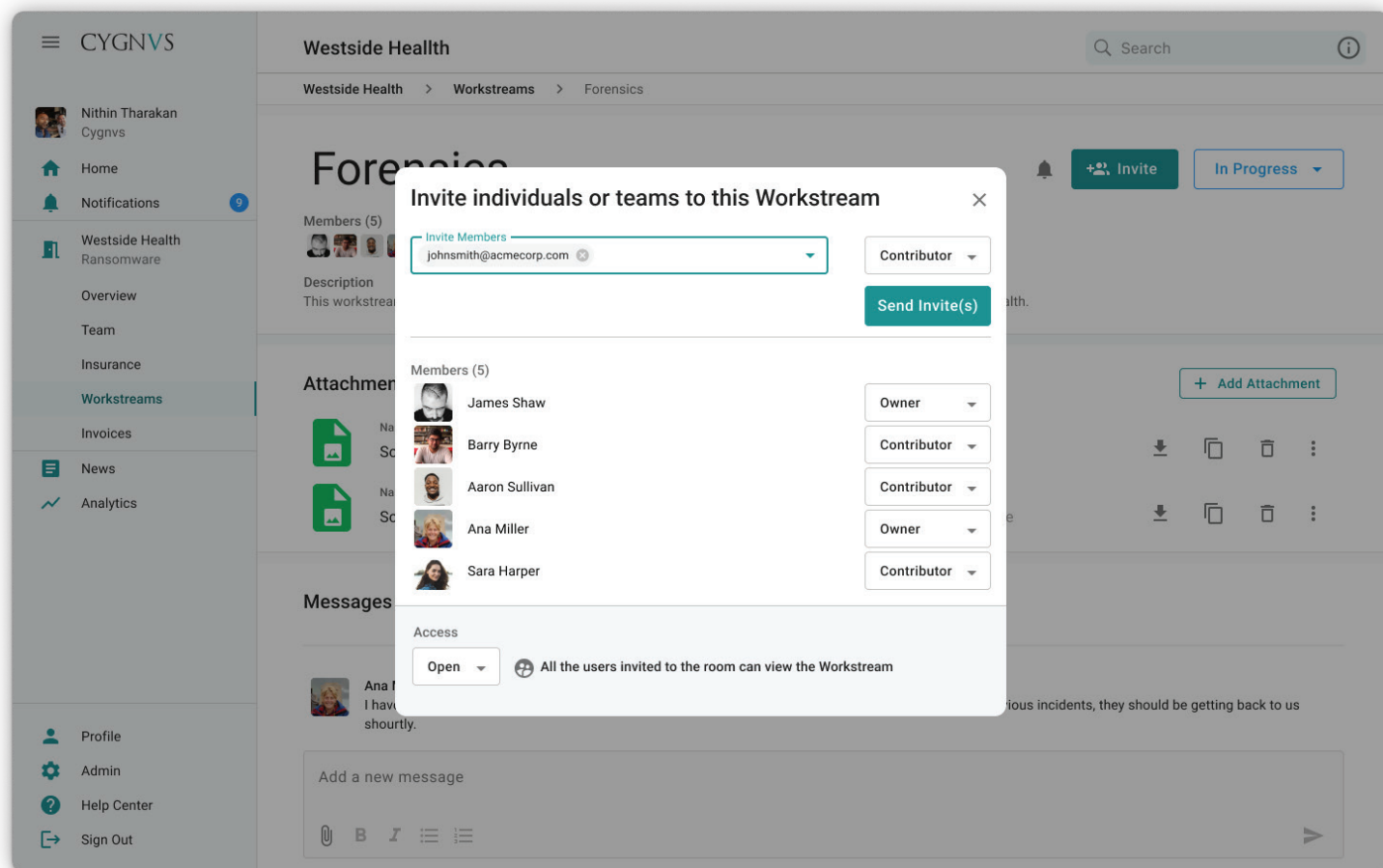
Team	Members
Forensics (6)	   P  B
Insurer (3)	  R
Senior Management (2)	 
Finance (5)	    C

Copyright © 2021 Cygnvs Inc. All Rights Reserved. Cygnvs Terms of Service & Privacy Policy

Teams are simple to create. An organization can establish counsel as an administrator, and responsibilities in assigning individuals to rooms and providing privileges can be managed by either counsel or the client.

While the organization is working on business priorities and restoration, counsel can easily establish privileged spaces for protected communication.

A View of Cygnvs: *(Continued)*



Clients can establish various levels of access permissions per each participant.

A View of Cygnvs: *(Continued)*

The screenshot displays the Cygnvs application interface. On the left is a sidebar with the 'CYGNVS' logo and a navigation menu including Home, Notifications (with a badge), Westside Health Ransomware (with sub-items Overview, Team, Insurance, and Workstreams), Invoices, News, and Analytics. At the bottom of the sidebar are links for Profile, Admin, Help Center, and Sign Out. The main content area is titled 'Westside Health' and shows a breadcrumb trail: 'Westside Health > Workstreams > Forensics'. A search bar is in the top right. The 'Forensics' workspace header includes an 'Invite' button and an 'In Progress' status dropdown. Below the header, it shows 'Members (5)' with five avatars and a description: 'This workstream is for members of the forensic team that are involved in the ransomware room within Westside Health.' The 'Attachments' section features a table with two entries: 'Screenshot_01_01_2022.jpg' (Image after the incident took place) and 'Screenshot_02_01_2022.jpg' (Image before the incident took place). Each row has icons for download, copy, delete, and a menu. An 'Add Attachment' button is at the top right of this section. The 'Messages' section shows a date separator for 'Wed 2 Jan 2022' and a message from 'Ana Miller' at 15:14 stating: 'I have reached out to the insurance provider and anked for more information about the policy holder's previous incidents, they should be getting back to us shourtly.' Below the message is a text input field with a placeholder 'Add a new message' and a rich text toolbar with icons for attachments, bold, italic, bulleted list, and numbered list.

Each workstream identifies the specific participants, documents and messages relevant to that workstream.

A View of Cygnvs: (Continued)

CYGNVS

Marc Smith

Acme Llc.

Home

Notifications

Westside Health Ransomware

Overview

Team

Workstreams

News

Analytics

Profile

Help Center

Sign Out

Acme Llc.

Search...

Policy Number: 0034TG564289 | Affected Entity: | Claim Id: | Date of Incident: |

Incident Response Demo

Complete

Description

Interactive Ransomware Room

Workstreams

+ Create Workstream

Broker communication channel

Open

Not Started

Carrier communication channel

1/6

+3

Open

In Progress

Client - Attorney communication channel

1

8

Restricted

Complete

Initial steps

Open

Not Started

Investigation

1

3/12

+4

Open

Not Started

Response planning

3/12

8

Open

Not Started

Details

+ Add Detail

Name

Detail

Broker name

Demo Broker

Broker emergency contact information

cyber@demobroker.com

Insurer name

iDemo

Insurer emergency contact information

1-888-567-3645

Noticeboard

Leave a comment

B I

@

Copyright © 2021 Cygnvs Inc. All Rights Reserved. [Cygnvs Terms of Service & Privacy Policy](#)

Post-incident rooms can be archived and stored, allowing easy access to documents and communications relevant to subsequent regulatory or litigation matters.

7

Appendix

1. Post Incident Report marked privileged. *In re Experian Data Breach Litigation*, No. SACV 15-01592 AG (DFMx), (C.D. Cal. May 18, 2017).
2. Third-party expert post incident report protected. *Genesco, Inc. v. Visa U.S.A., Inc.*, 302 F.R.D. 168, 190–91 (M.D. Tenn. 2014).
3. Report including business functions requested by attorneys was not protected because it was not shown that the report was created in anticipation of litigation. *Premera I*, 296 F. Supp. 3d 1230, 1240-47 (D. Or. 2017).
4. Narratives drafted to help prepare responses to regulatory inquiries were entitled to work-product protection. *Premera II*, 2019 WL 464963, at *7 (D. Or. Feb. 6, 2019).
5. In camera inspection leads to finding of no privilege. *Fero v. Excellus Health Plan, Inc.*, 15-CV-06569(EAW)(JJM), (W.D.N.Y. Aug. 3, 2020).
6. Forensic report not protected; SOW contracts were unclear as to work performed for provision of legal advice. *In re: Capital One Customer Data Security Breach Litigation* (E.D. Va., No. 1:19-md-02915).

KEY CONTACTS

Theodore J. Kobus III

T: +1. 212.271.1504

tkobus@bakerlaw.com

Craig A. Hoffman

T: +1.513.929.3491

cahoffman@bakerlaw.com

Cygnvs

info@cygnvs.com