Cyber Resilience: Turning your enterprise into a phoenix rising from the virtual ashes

WOODS
ROGERS
VANDEVENTER
BLACK
ATTORNEYS AT LAW

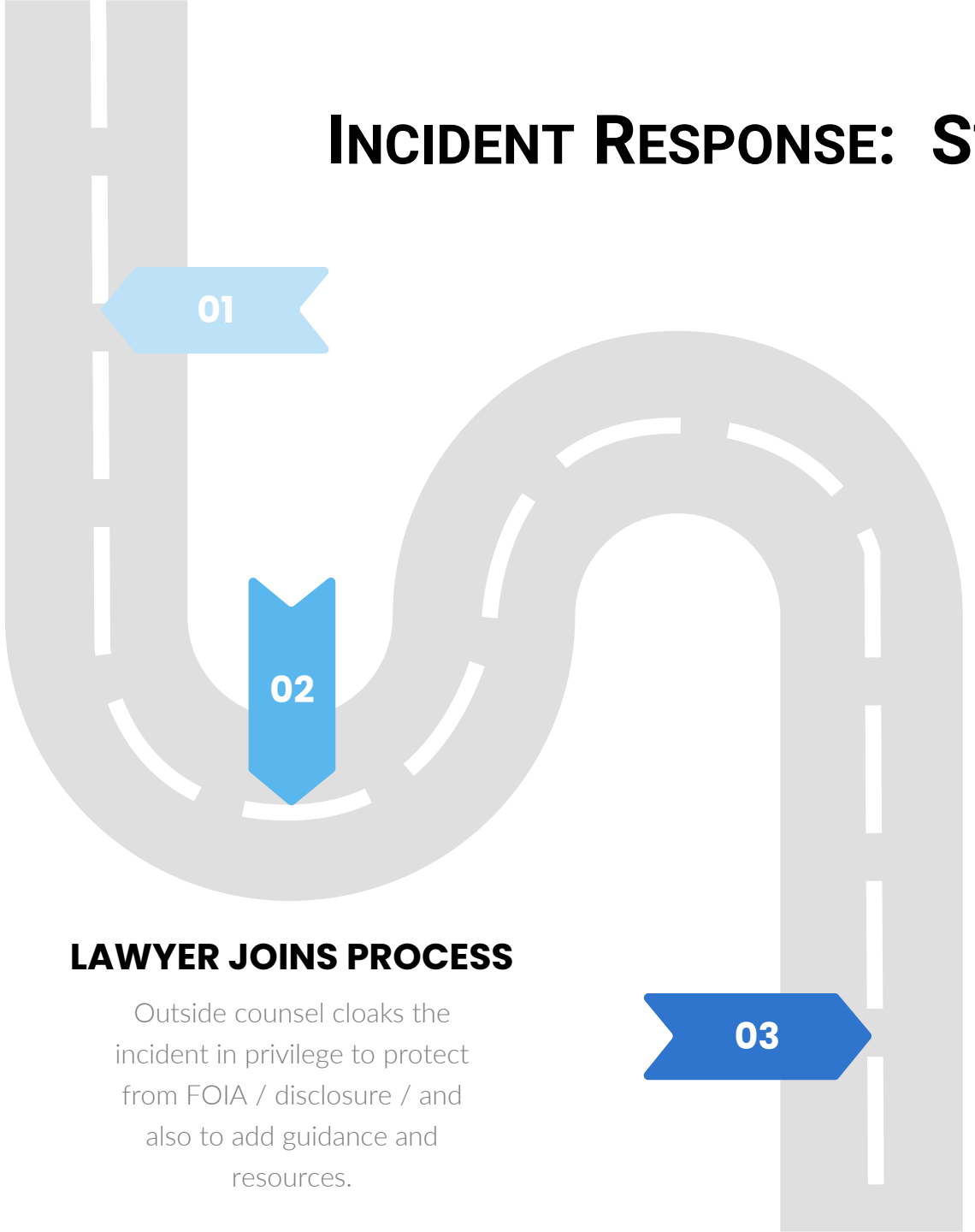
Working Backwards: The Incident

WOODS
ROGERS
VANDEVENTER
BLACK
ATTORNEYS AT LAW


PYSA
Hi Company,
Every byte on any types of your devices was encrypted.
Don't try to use backups because it were encrypted too.
To get all your data back contact us:
DonnaFoster@onionmail.org
MonicaSurface@onionmail.org
Also, be aware that we downloaded files from your servers and in case of non-
them on our website, and if necessary, we will
dates for our partners: http://
ad.onion/

RANSOMWARE

Incident Response: Step by Step



CALL CYBER INSURANCE

Call your cyber insurance contact to get immediate access to help.

LAWYER JOINS PROCESS

Outside counsel cloaks the incident in privilege to protect from FOIA / disclosure / and also to add guidance and resources.

TOGETHER FILE REPORTS

Work together to file the report to the Fusion Center under new Virginia law. Determine together whether legally this is a reportable event.

§ 2.2-5514. Prohibited products and services and required incident reporting.

A. For the purposes of this section, "public body" means any legislative body; any court of the Commonwealth; any authority, board, bureau, commission, district, or agency of the Commonwealth; any political subdivision of the Commonwealth, including counties, cities, and towns, city councils, boards of supervisors, school boards, planning commissions, and governing boards of institutions of higher education; and other organizations, corporations, or agencies in the Commonwealth supported wholly or principally by public funds. "Public body" includes any committee, subcommittee, or other entity however designated of the public body or formed to advise the public body, including those with private sector or citizen members and corporations organized by the Virginia Retirement System.

B. No public body may use, whether directly or through work with or on behalf of another public body, any hardware, software, or services that have been prohibited by the U.S. Department of Homeland Security for use on federal systems.

C. Every public body shall report all (i) known incidents that threaten the security of the Commonwealth's data or communications or result in exposure of data protected by federal or state laws and (ii) other incidents compromising the security of the public body's information technology systems with the potential to cause major disruption to normal activities of the public body or other public bodies. Such reports shall be made to the Virginia Fusion Intelligence Center within 24 hours from when the incident was discovered. The Virginia Fusion Intelligence Center shall share such reports with the Chief Information Officer, as described in § 2.2-2005, or his designee at the Virginia Information Technologies Agency, promptly upon receipt.

2019, c. 302; 2022, cc. 626, 627.

Report a Cyber Incident Commonwealth of Virginia

C. Every public body shall report all (i) known incidents that threaten the security of the Commonwealth's data or communications or result in exposure of data protected by federal or state laws and (ii) other incidents compromising the security of the public body's information technology systems with the potential to cause major disruption to normal activities of the public body or other public bodies. Such reports shall be made to the Virginia Fusion Intelligence Center within 24 hours from when the incident was discovered. The Virginia Fusion Intelligence Center shall share such reports with the Chief Information Officer, as described in § 2.2-2005, or his designee at the Virginia Information Technologies Agency, promptly upon receipt.

Incident Response: Parallel Tracks

RANSOMWARE IN 2022

OLD SCHOOL RANSOMWARE

Encrypt in place and do not exfil data off the network. Usual recovery method is to look to backups and hopefully move forward.

VS

RANSOMWARE 2.0

Encrypt in place and also take data off the network. Use the data on a shame website or to directly contact impacted businesses/individuals.

Road Ahead with Threat Actors

2022 Tactics

Welcome again! We are ready to help you.

01:11:12 AM | September 11

Hello, our network was encrypted. What do we need to do to unlock our files and keep more data from being released?

02:08:54 AM | September 11

Hello, let me ask my boss

Like Comment Share

6

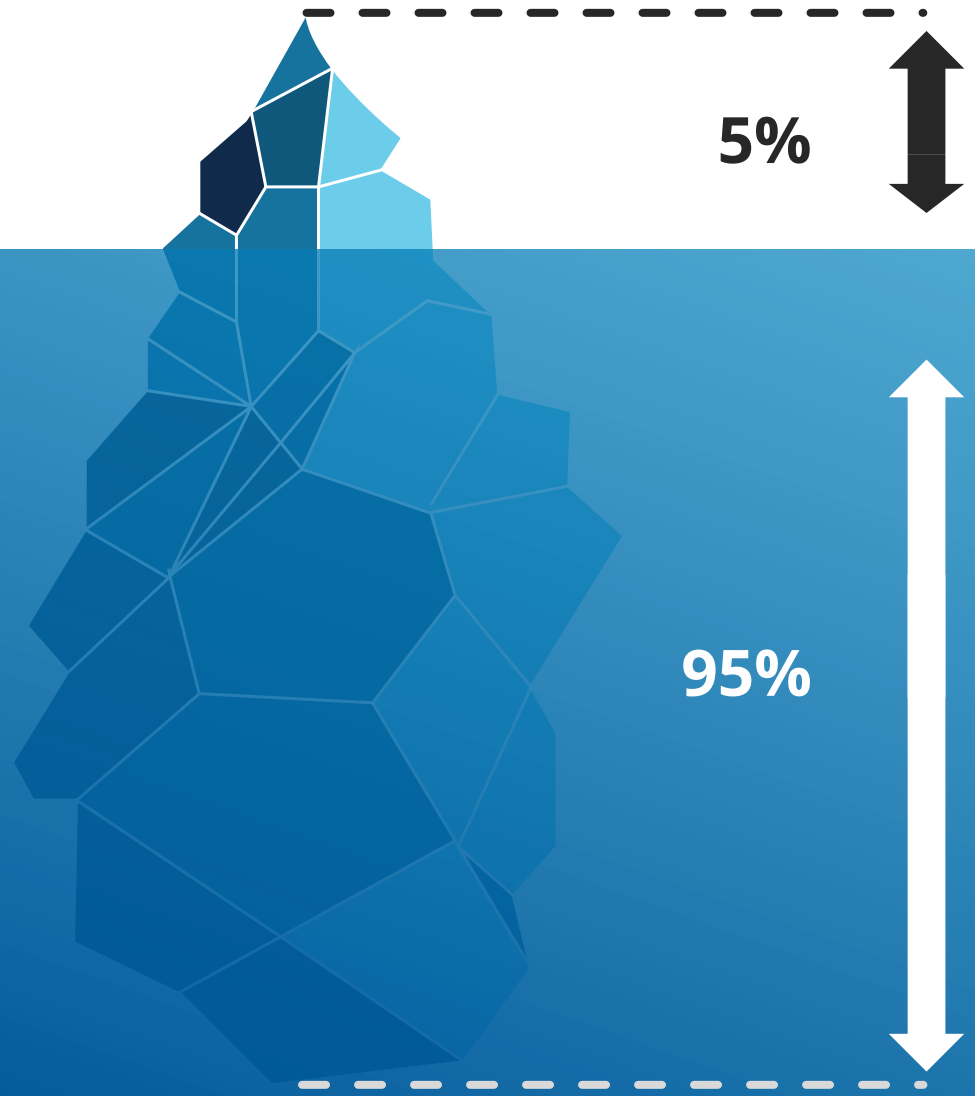
Most relevant

[redacted]

Great Job

Building the Restore Plan

The (un)likelihood of backups



5%

Backups Operational

Majority of the time, the backups (whether onsite / in the cloud / outsourced / internal) are not functional. It is rare to have a functional backup.

95%

No Backups - All Backups Corrupted / Non-Functioning

The common issues include: threat actor is able to utilize the same credentials to access the backup array and is thus able to encrypt the backups as part of its overall strategy.

In other tragic circumstances, the backups fail due to configuration error that is not discovered until after the incident.

The Incident Response

"Outside Team"
Incident Response Team Actions

Gathering evidence, preserving evidence, review of any data exfiltration and health of network.

Communications with TA + Notification Issues

Communicating to learn more about the data stolen / not to pay.

This bucket also includes law enforcement / Fusion Center / managing notice strategy.

The "Audience"

Managing public relations for both internal and external stakeholders (executive team / media / law enforcement).

The Rebuild / Restore

Buried in the dark waters, this is the critical piece that often we are unprepared for.

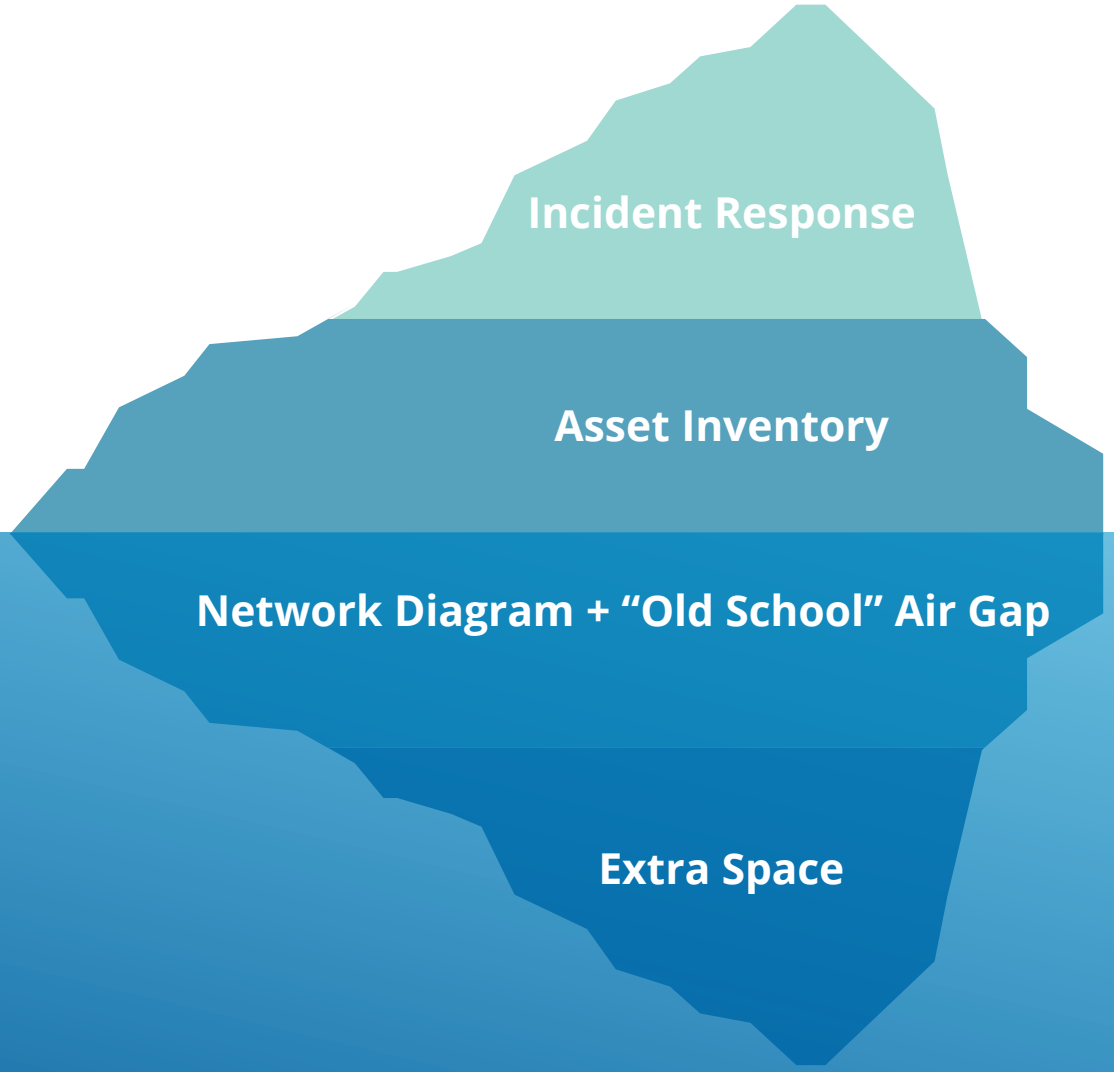
Managing the Rebuild: A Strategy

Current Focus: Above the Water

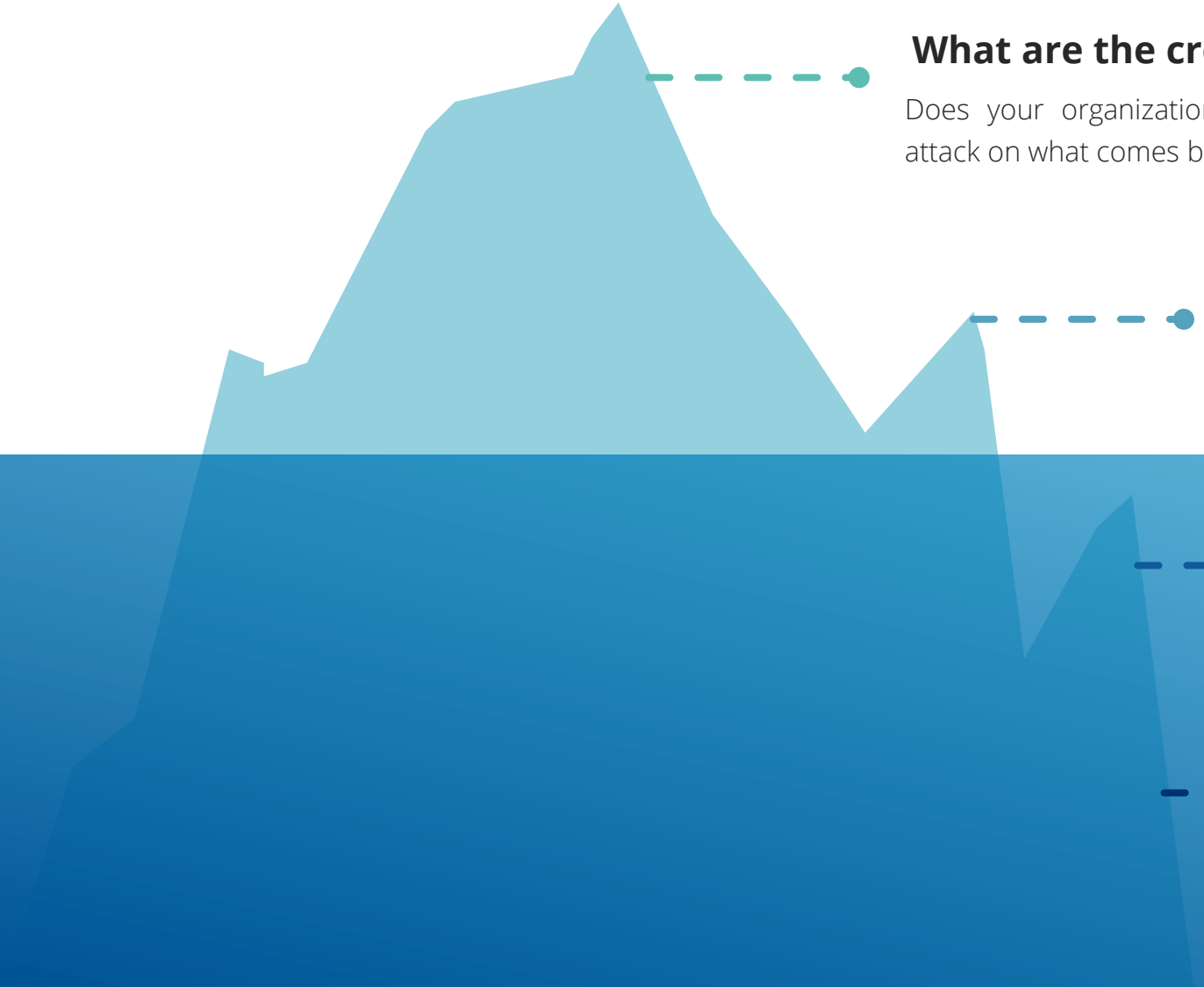
Focus is often on the surface level issues: having an up-to-date incident response plan.

True Need: Below the Surface

The real effort should be spent here: thinking through what could happen if the backups all fail. Do we have an old school air gapped drive with critical info / applications locked away? Do we have extra slack space to rebuild into if we had to stand up a parallel network?



Common Issues



What are the crown jewels that need to be stood up, first?

Does your organization have a common plan of attack on what comes back online, first?

Resources

In a rebuild scenario, do we have enough resources to stand up imaging servers, new switches, a clean network?

Moving the enterprise

All of a sudden, the cloud may look like a safe bet. Could you move to a new gov tenant quickly?

Team Burnout

Is your on-site team prepared to run the marathon and the sprint at the same time? Have you built an environment where everyone will pitch in?

Building the Audience Plan

WOODS
ROGERS
VANDEVENTER
BLACK
ATTORNEYS AT LAW

Knowing Your Audience

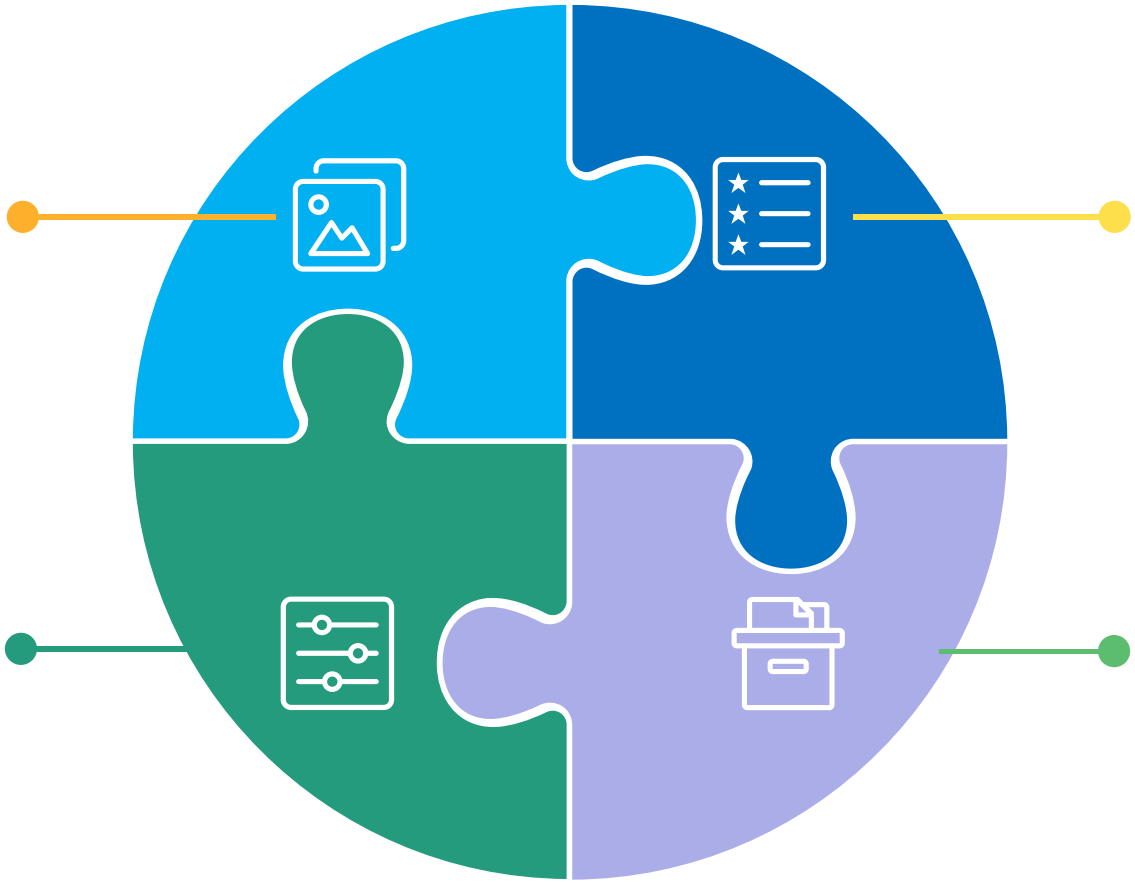
After an Incident Hits

Internal Team Stakeholders

Your team, your boss, Executive Leadership, the Board.

The “Commonwealth”

In a catastrophe, you attract a lot of attention.



Constituents You Serve

The Public.

Media

Local and potentially national.

The Puzzle

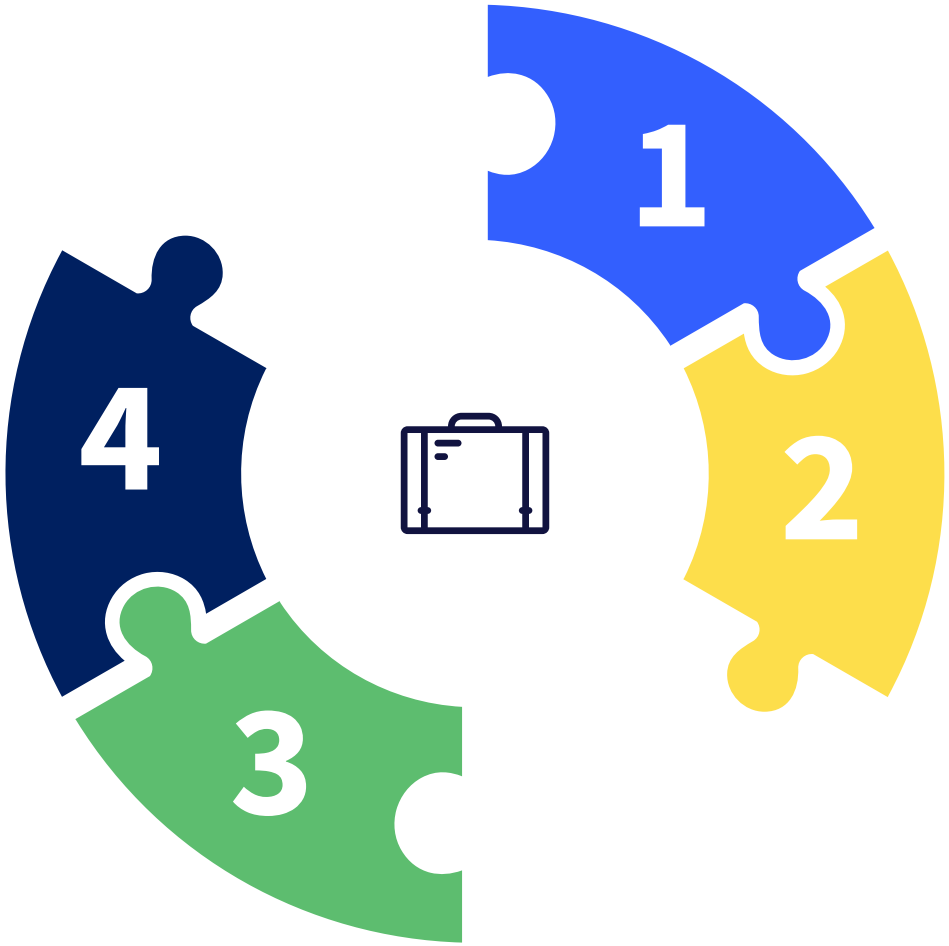
Communications Post-Incident Aren’t Easy

Identify

Identify what needs to be said, when, with Counsel.

Build

Have a strategy for building on the message from the outset. Save room on the runway.



Let go

The process needs to be focused on legal, internal and external media management.

Message

Stick to the message.

The Paybook

Everyone else

Think of all the various groups that need to be updated on a consistent message. Hire cyber PR teams to assist (covered by cyber insurance if hired through policy protocols)

Privileged & Confidential
Prepared at the Request of Counsel

Communications Playbook
Last update May 27 @ 3:00 pm EST.

Table of Contents

The Message

To Impacted Stakeholders

Impacted Stakeholders

Figuring out impacted stakeholders is a potentially slow process. Are you ready to pull the trigger on a pre-emptive notice to all?

[NAME]
[ADDRESS 1]
[ADDRESS 2]
[ADDRESS 3]

Dear [NAME],

We are contacting you about an issue that we have encountered that could possibly increase your risk for identity theft or constitute an unauthorized access of your health information.

On February 15, 2022, _____during a review of its e-mail system discovered that a single e-mail account was accessed by someone outside of _____. We are writing to notify you that some of your child's personal health information may have been affected by this incident. In particular, information, including personal health information consisting of **your child's name,** may have been in the e-mail box of the account accessed by someone outside _____.

Although we have no evidence to show that this information was actually accessed or used outside of our systems (nor do we believe that your child's name alone would necessarily give rise to any identity theft) we are notifying you of this event and the steps you can take to protect your child out of an abundance of caution. In addition, we have arranged to offer credit monitoring and identity restoration services from Experian at no cost to you.

What Happened

WOODS
ROGERS
VANDEVENTER
BLACK

ATTORNEYS AT LAW

Beth Burgin Waller
Chair, Cybersecurity & Data Privacy
bwaller@woodsrogers.com
P (540) 983-7625 | (804) 343-5039