BRP
CYBER CENTER OF EXCELLENCE

AHT
INSURANCE
A BALDWIN RISK PARTNER

REVELATIONS, REGULATIONS, & RISKS

CYBER EXPERTS WEIGH IN

Part Three: Regulatory

SARAH SARGENT

ATTORNEY
GODFREY & KAHN LAW

GODFREY & KAHN LAW

Sarah Sargent is a member of the Data Privacy, Cybersecurity & Technology practice. She holds the CIPP/US, CIPP/E and CIPM certifications from the International Association of Privacy Professionals, allowing her to draw from both domestic and international best practices when it comes to questions of data privacy.

Sarah's practice focuses on assisting clients in implementing innovative technology and finding practical business solutions for privacy compliance. She counsels clients on privacy compliance with a variety of state, federal and international laws, including the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and the New York Department of Financial Services Cybersecurity Regulation. Sarah's understanding of these regulations allows her to advise companies seeking to implement entity-wide privacy programs, walking them through each step necessary to prepare for the next emergent privacy law.

She also advises clients on a variety of technology issues, including software licensing,vendor management, data breach prevention and SaaS and software development contracting. Additionally, Sarah assists in cybersecurity and privacy due diligence in mergers and acquisitions. Beyond preventative efforts, Sarah's focus also includes data breach remediation and litigation in various industries, including healthcare,financial, non-profit, manufacturing and retail. She routinely works with opposing counsels, forensics experts, insurers and government regulators to resolve security incidents promptly and efficiently.

DO NOT USE THE B WORD (BREACH). MAKE SURE TO CALL IT A SECURITY INCIDENT.
A BREACH IS A LEGAL DETERMINATION THAT A LAWYER HELPS YOU REACH AFTER YOU'VE ANALYZED THE FORENSIC EVIDENCE.

WE ASKED, SARAH ANSWERED

Q: CAN YOU GIVE US AN OVERVIEW ON THE MOST RELEVANT POINTS IN THE REGULATORY ENVIRONMENT?

There have been a lot of changes happening in the last six months to a year in the cybersecurity world. The main reason for that is regulators are starting to require more disclosures about security incidents. A big update is that the SEC adapted a new rule for public companies that will require disclosure of material cybersecurity incidents and disclosure related to how companies handle cyber risks, cyber strategy, and governance. The incident disclosure must be filed within 4 days of determining the cyber incident was material.

There are a number of new state privacy laws, now 12 in different states. Some new privacy laws require companies to protect personal information with reasonable security measures. View Enacted Laws Here

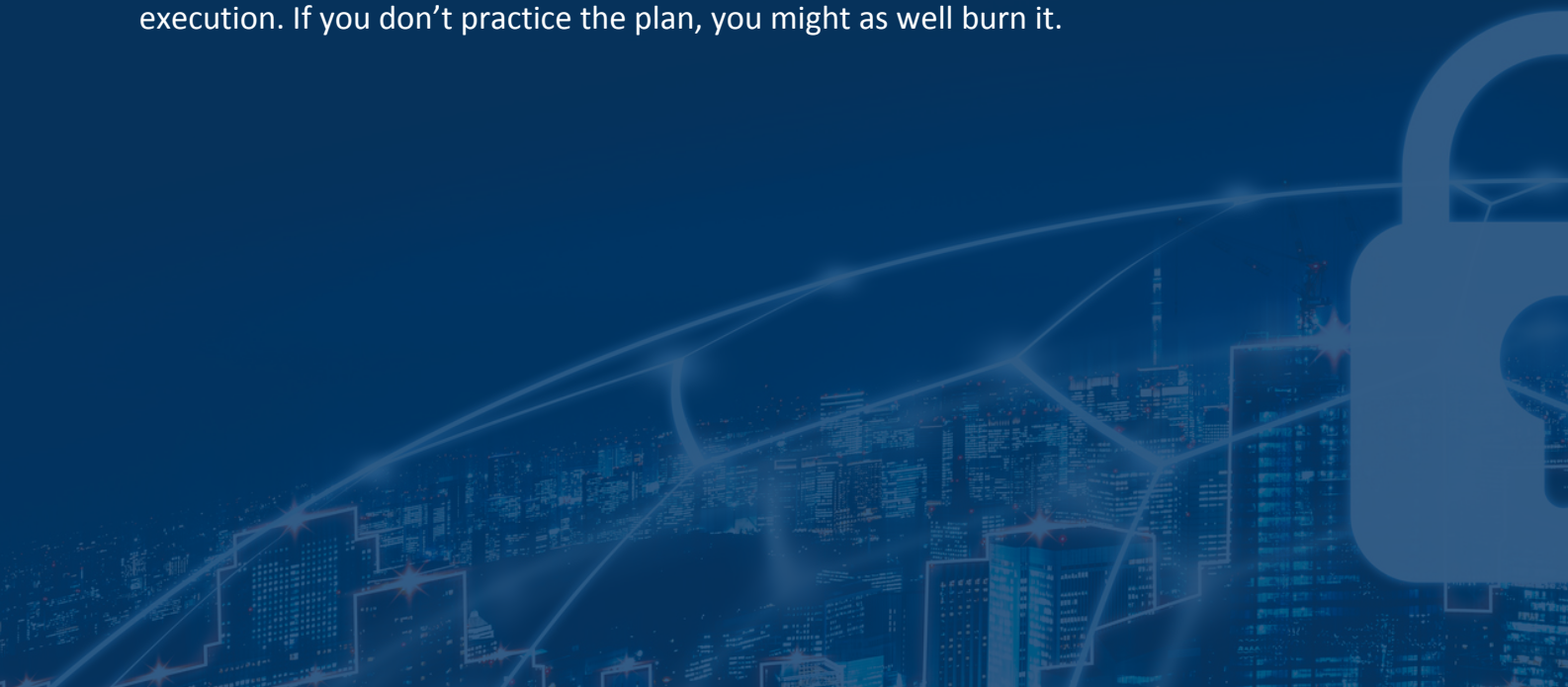
Q: HOW DO YOU SEE THESE NEW REQUIREMENTS CHANGING THE PROCESS WHEN YOU GET INVOLVED WITH A CLIENT WHO'S HAD SOME SORT OF CYBERSECURITY OR PRIVACY INCIDENT?

A lot of disclosure requirements and tightening deadlines are going to force companies to move more quickly, making it critical for companies to be prepared to handle incidents and have their group of people identified to aid in the incident. Examples in this group are an attorney or data breach coach to walk you through the legal aspects and a forensic provider who analyzes the forensic evidence on the system to make sure you've contained the incident. Having these providers identified beforehand and approved through your insurance policy, if your policy requires that, is all going to help you move quickly to meet these disclosure deadlines.

Q: WHAT ARE BASE THINGS THAT NEED TO BE INVOLVED IN AN INCIDENT RESPONSE PLAN?

An incident response plan should identify key players internally and externally, including HR, marketing, and those with risk decision-making authority. Ensure you have all their contact details, including personal contact information in case the office emails or phones go down.

The plan should outline incident evaluation based on severity levels (e.g., low, medium, high, emergency) and how to engage the appropriate team. For high-level emergencies impacting the entire company, an all-hands meeting should be held promptly. The plan should cover incident investigation, forensic evidence collection, remediation, return to normal operations, and post-incident analysis for continuous improvement. Regular practice and training are essential for ensuring everyone is familiar with the plan's execution. If you don’t practice the plan, you might as well burn it.



Q: WHAT ADVICE DO YOU HAVE FOR INSUREDS WHO SUSPECT THEY MAY HAVE AN INCIDENT?

If you think you have an incident, you need to do containment. Once you feel like you've gotten to a place where you're contained, call your broker, insurance company, and attorney or data breach coach. This allows you to kickstart the process to preserve a claim if you choose to file one, or if you need to notify your broker to get access to third-party vendors who will help you along the way.

Something I would not recommend is trying to handle a complex incident without outside help. This does not go well because you eventually need outside help, and you have to undo what you've already done. Make sure to utilize your resources like your data breach coach or your broker.

Sometimes I see clients not using a secure communication channel. If you think email has been compromised, get off email, get on the phone or some sort of secured channel, like Teams.

Do NOT use the B word (breach). Make sure to call it a security incident. A breach is a legal determination that a lawyer helps you reach after you've analyzed the forensic evidence

Also avoid making broad public statements before you've conducted a thorough investigation. Making a big statement can cause issues rather than just collecting facts. The easiest way to make people mad is to make them panic when you don't have all the facts or tell them something that ends up being wrong. Avoid making quick statements.

Q: WHAT CAN WE EXPECT TO COME DOWN THE PIPE FROM A REGULATORY STANDPOINT?

Vendor due diligence is going to be a key piece of what regulators want to see companies handling. With all the MOVEIT-related matters, there were a number of vendors impacted by that vulnerability and multiple levels down the supply chain. The regulators' reaction, especially in the financial space, is to remind institutions that they must have good vendor due diligence and solid contracts in place.

I also think that regulators are going to want to see companies preparing for incidents and handling incidents that require notification to individuals in a timely manner. The state attorney general's offices understand some of these investigations just take time. As long as you're showing that you are moving the ball forward and trying to be a good steward of the data you have, they are largely comfortable with that. But if you ignore things or aren't moving at a reasonable pace, that's when we'll be seeing regulators coming in more often or even investigating people.

Q: WHAT ARE SOME SUCCESS STORIES WITH CLIENTS THAT HAVE HAD A CYBER INSURANCE POLICY IN PLACE?

The biggest difference I've seen between those who have insurance and those who don't is the response time. When you have cyber liability insurance, it forces you to think through the incident response plan and the process a little more thoroughly. Any time we talk about incident response, time is money. If your company is down, it's all time you're losing on revenue, so the time component is always a lot quicker when you've identified those players.

I'm also seeing a lot of insurers requiring additional technical measures to qualify for cyber insurance. I think the reason they recommend those controls is because they hope it mitigates risk and helps an incident be contained. Those features really help shrink the incident and ultimately cut down the impact to the business.

Q: WHAT KEEPS YOU UP AT NIGHT WHEN YOU THINK ABOUT MANAGING YOUR CLIENT'S RISK?

Unstructured data that you have no idea what's in it and you don't have a good understanding of the personal information it contains. There are so many times you discover Social Security numbers or driver's license numbers that someone just happened to be storing in their email for no good reason other than it was easy. That always creates a big risk and it's a hard risk to mitigate, especially as your company grows in size because it's hard to understand your risk profile. Unstructured data makes an incident tougher especially when you have ransomware or data exfiltration and you're trying to figure out what was taken and what was exposed.

The other piece is really aggressive threat actors. Some ransomware groups are starting to contact customers, leadership, c-suite, and board members. They find employees on LinkedIn and message them or even impersonate them. Aggressive threat actors make it so much harder because you're already trying to figure out what happened in your system and then you have to deal with robo calls coming into your business saying they have your data and they're going to expose it. It makes everything more panicky and difficult to deal with. Sadly, this is not unusual these days for that reach-out if they aren't getting a reaction from you.

SEE OUR KEY TAKEAWAYS:

"What NOT to Do During a Cyber Incident"

Read it Here

Collaboration is critical to mitigating cyber exposure. Evolving cyber risk requires companies to coordinate preventive measures companywide, utilize the best security controls, and work closely with trusted partners in the cyber security community.

The BRP Cyber Center of Excellence provides more than expertise in placing cyber insurance coverage. We offer a broad range of integrated solutions and services that provide value to our customers by limiting the potential financial and operational impacts of cyber incidents. We work closely with companies across every industry to identify their specific vulnerabilities, mitigate current cyber risks, and stay ahead of new risks emerging on the horizon.

BRP
CYBER CENTER OF EXCELLENCE

AHT
INSURANCE
A BALDWIN RISK PARTNER

CONTACT US TO HELP PROTECT YOU AND YOUR BUSINESS.

BRP
CYBER CENTER OF EXCELLENCE

AHT
INSURANCE
A BALDWIN RISK PARTNER