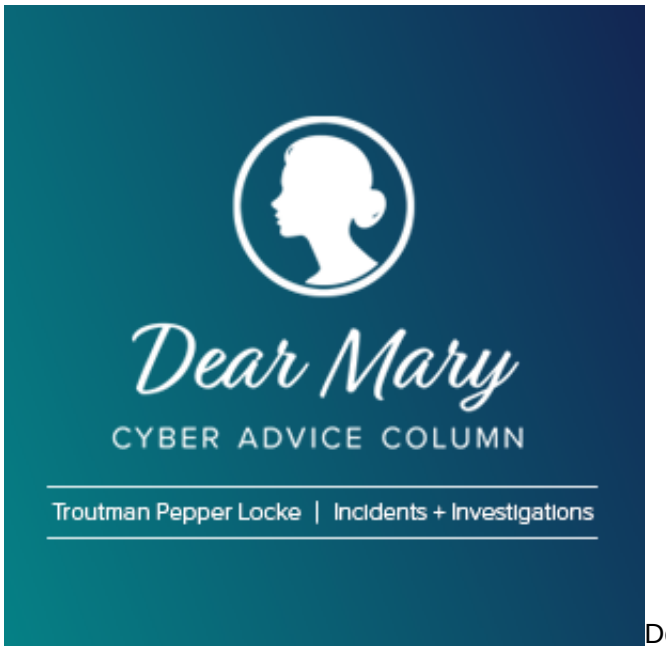
Articles + Publications | 2024-2025

Dear Mary — Incidents + Investigations Cybersecurity Advice Column

CONTACTS

Kaitlin J. Clemens | Sadia Mirza | Ronald Raether, Jr. | Stephen C. Piepgrass | Ashley L. Taylor, Jr. | Samuel E. "Gene" Fishel | Karla Ballesteros | Robyn W. Lin | Whitney L. Shephard | Edgar Vargas | Casselle A.E. Smith | Daniel Waltz



Dearest Reader,

Welcome to 'Dear Mary,' Troutman Pepper's cybersecurity advice column brought to you by its Incidents + Investigations team. Through this column, "Mary" responds directly to her readers' questions, covering all things related to incident response, data breach, and cybersecurity.

Have a question about security incidents, forensic investigations, data breaches, or preventing/managing the legal and regulatory challenges that follow? Reach out to have your question answered. Of course, answers provided will be general in nature and should not be considered legal advice. Always consult with an attorney (preferably one of ours) before acting on what you read here.

Happy reading.

2025

Dear Mary,

Our company experienced a cybersecurity incident. It seemed pretty minor — just a few suspicious emails and an employee's account being locked. To my dismay, we're now hearing from our IT team that the issue is more serious. We have cyber insurance, but we didn't notify our carrier right away. Did we make a mistake? When should I reach out to our insurance provider?

– Unsure Insured of San Francisco

March 18, 2025

Dear Unsure Insured,

Your questions are ones that many entities wrestle with during an active incident. Cyber insurance policies are designed to help businesses respond to incidents effectively, but coverage may depend on timely notification according to the insurance carriers' requirements. Waiting too long — or failing to notify at all — could put your ability to recover costs at risk.

Early notification is key. Most policies require notification within a specific timeframe. If an incident later escalates into something more serious — like data theft or system downtime — and you haven't informed your carrier, you may be setting yourself up for some difficult conversations concerning coverage.

Beyond policy requirements, notifying your carrier early has some practical benefits. For instance, cyber insurers maintain a network of specialized resources to assist their insureds respond effectively to cybersecurity incidents. These resources (often called on-panel vendors) may include legal counsel, forensic firms, data mining services, threat actor negotiation firms, and public relations support. If you notify promptly, you may be able to leverage these experts to assess the situation, contain the threat, recover systems, and comply with legal obligations — often at reduced or even no cost to your organization beyond the policy deductible. This can significantly reduce the impact of the incident on your business.

To avoid scrambling during an incident, take these steps now:

1. Review your policy to understand notice requirements and coverage triggers.

2. Establish an incident response plan that includes when and how to notify your carrier.
3. Connect with pre-approved vendors ahead of time to ensure agreements are in place before an incident occurs. Many insurers require use of specific legal, forensic, and recovery firms; establishing these relationships before an incident can speed up response time. Incidentally, Troutman Pepper Locke is a pre-approved law firm for certain insurance carriers.

Cyber insurance is a great tool to have in your arsenal, but like any tool, its effectiveness depends on knowing how to use it properly.

Signing off,

– Mary

2024

SEC Cybersecurity Incidents Disclosures: Materiality, Decryptors, and Ransom Payments

Dear Mary,

I work for a public company that recently experienced a ransomware attack. Fortunately, we were able to restore our business operations quickly by obtaining a decryption key from the threat actor. Given that we managed to get back up and running so swiftly, do we still need to determine whether the incident is material and report it?

Sincerely,

– Concerned Executive

September 11, 2024

Dear Concerned Executive,

Yes, your company is still required to determine whether the incident is material, even if you managed to restore operations quickly. One of the primary objectives following a ransomware attack is to get the business back up and running safely and securely. Every day the business is not operational translates to financial loss, reputational harm, and other negative impacts.

Achieving this often requires significant effort, including assistance from third-party restoration firms, rebuilding systems from scratch, and sometimes even negotiating with the threat actor for a decryption key in exchange for a ransom payment. Once the business is operational again, it is considered a significant win.

However, returning to normal business operations does not absolve a company from the requirement to make materiality determinations. Even if the company manages to restore operations in record time, it must still assess the materiality of the cybersecurity incident and report the incident under Item 1.05 of Form 8-K within four business days after the company determines that it has experienced a material cybersecurity incident.

On a positive note, if operations are restored quickly, it may indicate that the financial impact was minimal, which is a factor to consider when determining materiality. The key point is that in assessing the materiality of the incident, a company should determine whether "there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision, or if it would have significantly altered the total mix of information made available," regardless of the resolution of an incident, including if such resolution occurred because the company ultimately paid a ransom demand or otherwise obtained a decryptor.

It sounds like your company has some decisions to make. If you are uncertain whether the incident is material, you may want to consider using Item 8.01 to disclose the cybersecurity incident. Keep in mind, however, that if a company discloses a nonmaterial incident, or one for which it has not yet made a materiality determination, under Item 8.01 and then later determines that the incident is material, the company should file an Item 1.05 within four business days of such subsequent materiality determination. This later notice may reference the Item 8.01 initial notice but should still satisfy the disclosure requirements of an Item 1.05 filing.

Sincerely,

Notifying Law Enforcement of Security Incidents

Dear Mary,

I recently experienced a security incident at my company and am considering whether to report it to law enforcement. While I want to cooperate and help catch the cybercriminals responsible, I am worried that law enforcement might come after my company for… I am not exactly sure what.

What should I do?

– Not Guilty

August 21, 2024

Dear Mr. Guilty — pardon me — Not Guilty,

Your hesitancy to engage law enforcement is not uncommon. Many businesses are intimidated by the thought of interacting with law enforcement, especially during an active security incident. Let me provide some clarity to hopefully give your not-guilty conscience some peace of mind.

Law enforcement's primary interest in security incidents is to pursue the threat actors or cybercriminals responsible. Typically, the client or victim is not the target of their investigation efforts. However, because the cybercriminal may have been lurking in your systems, you may have valuable information to share. This includes indicators of compromise (IOCs), information pertaining to the threat actor's techniques, tactics, and procedures (TTPs), and the like. Therefore, law enforcement may be interested in speaking with you.

If you decide to notify law enforcement, here are a few tips to keep in mind:

1. **Law Enforcement's Capacity:** Law enforcement agencies are often busy and may not get involved in every case. It's not uncommon to report an incident and never hear back. However, if your incident involves a specific threat actor gang or issue that law enforcement has shown interest in, you may be fortunate enough (is that the right phrase?) to receive a response.
2. **Optics:** Notifying law enforcement can be beneficial from an optics perspective. It may demonstrate to affected stakeholders that you are taking the matter seriously and are committed to addressing the issue.
3. **Nonprivileged Communications:** Remember that your communications with law enforcement are not privileged. Where possible, leverage your cybersecurity counsel to navigate these conversations for you. They likely have significant experience in interacting with law enforcement and may have valuable contacts within the agencies to facilitate reporting.
4. **Confidentiality Concerns:** Based on law enforcement's prior history, it's not guaranteed that your report will

remain confidential. The information could be shared with regulators and even the public, so craft any notice you intend to submit with this in mind.

5. **Cooperation:** Should you have valuable information or forensic artifacts to share, law enforcement may request a certain level of assistance and cooperation from you as part of their investigation. Depending on their needs, this could require a significant commitment of time and resources on your part. You may also need to consider whether the requested cooperation involves disclosing any confidential or proprietary information. For example, if you're asked to turn over certain systems or machines involved in the security incident, consider the types of data stored within those machines and what steps you may need to take to ensure that the disclosure is permitted.
6. **Report to the Right Agency:** Consult with your cybersecurity counsel to determine which law enforcement agency is most appropriate to notify. For example, ransomware attacks are typically reported to the FBI, while the Secret Service is particularly skilled in handling wire fraud and business email compromise (BEC) incidents. Ensure you report to the right agency to maximize the effectiveness of your response.
7. **Law Enforcement Delay:** While we're jumping ahead a bit, discuss with your counsel what a "law enforcement delay" entails. In the context of breach notification, law enforcement agencies may request that you delay sending any breach notification letters if issuing such letters would impede a related investigation. Naturally, they can only make this request if they are aware of the incident, which may be a reason to consider notifying them.

Also keep in mind that while many businesses choose to notify law enforcement out of an abundance of caution, there are circumstances where notifying law enforcement is strongly encouraged or even legally required. This includes situations where businesses are paying a ransom or are subject to certain regulatory frameworks that mandate notification.

Overall, coordinating and cooperating with law enforcement can be a positive and friendly experience, given their primary objective of taking down the cybercriminal. Just ensure you consider the points mentioned above as you navigate reporting and any subsequent discussions.

Yours truly,

Ensuring Proper Legal Involvement in the Incident Response Process

Dear Mary,

I'm the general counsel of an organization and have recently started getting involved in the cybersecurity side of things. As I'm getting my bearings, I've noticed that our security team doesn't always involve the legal department when an incident is suspected. While I understand that not every incident requires our involvement, I'm concerned that we're being left out of matters that do need legal oversight, and when we are involved, it's often too late. What can I do to help address this?

– Living in FOMO

August 14, 2024

Dearest L. FOMO,

Your concern is both valid and common among legal teams everywhere. But worry not, for there is a solution, and it begins with understanding your security team's formalized triage process. Here's what you need to know:

1. **Understand the Triage Process:** Security teams typically use a triage process to determine how to escalate and respond to each detected incident. They might assign a severity level to incidents on a scale from 1 to 4 — Level 1 being routine incidents that internal IT can handle, and Level 4 being major incidents requiring a response. This triage process usually dictates which matters require legal involvement and which do not. For example, the triage process may dictate that only Level 3 and 4 incidents need to be escalated to Legal, meaning Legal will not be notified of Level 1 and 2 incidents.

2. **Define Legal's Role:** Your mission is to ensure that the triage process clearly dictates which incidents need to be escalated to Legal and when. As you correctly noted, not all cybersecurity incidents require the same response or lead to the same outcomes. Historically, however, security teams have struggled to identify which incidents will have legal implications, often skipping critical steps needed to mitigate potential legal exposure. Consequently, you should work closely with them to define the matters Legal should be involved in from the outset and ensure there is a protocol in place to provide such notification. This might include incidents that could potentially implicate sensitive or confidential data, affect many individuals, involve certain types of attacks (*e.g.*, ransomware or other network intrusions), or are likely to result in consumer/customer harm or otherwise trigger regulatory scrutiny. Incident response is not always black and white, so if the security team is ever uncertain about whether an incident meets a certain classification level, encourage them to view Legal as a partner in this process and to reach out for discussion.

3. **Periodic Review:** Once you have reviewed and are comfortable with the documented triage process, implement an internal audit system to ensure that security incidents are being classified correctly and that those requiring legal involvement are being escalated appropriately. While some misclassifications are inevitable, if you notice recurring errors, it may be necessary to revisit the triage process to determine what adjustments are needed or what additional training should be provided to address potential gaps.

By understanding, refining, and auditing the triage process, you can alleviate your fear of missing out on critical incidents or being involved too late. With that worry off your plate, the only thing left to ponder is … what does Legal do once notified?

Yours truly,

– Mary

Restrictions on Paying a Ransom Demand

Dear Mary,

Which states now have statutory laws prohibiting payment of ransom following a data security breach? Are there others working on such legislation, to your knowledge?

– Dick Clarke (But Not the New Year's Eve Guy)

July 31, 2024

Dearest Dick,

While the phrases "ransomware" and "good news" rarely find themselves in harmonious company, private

businesses may find solace in the knowledge that, generally, U.S. law does not restrict private entities from paying a ransom in the unfortunate event of a ransomware attack. Alas, the same cannot be said for our public sector counterparts. Legislation in states such as North Carolina, Florida, and Tennessee imposes restrictions on public sector entities from paying a ransom, with North Carolina even forbidding any communication with the threat actor altogether. Last I heard, other states such as Arizona, New York, Pennsylvania, Illinois, Iowa, Massachusetts, and Texas have been contemplating similar and possibly even more expansive laws. Additionally, laws have been introduced at the federal level that could potentially restrict ransom payments for certain types of entities, such as financial institutions, so that is most certainly something to look out for.

For private entities, although paying the ransom is not currently prohibited, there are steps that should be taken prior to making such a payment. These include notifying law enforcement and conducting a sanctions check, among others. If these steps are satisfactorily completed, the entity may be at liberty to proceed with the payment. Additionally, the entity should consider whether any regulatory authorities, such as CISA, need to be notified once payment is made.

Yours sincerely,

Understanding Access vs. Acquisition

Dear Mary,

Each of the 50 states has its own definition of what constitutes a reportable data breach. For some, it requires “unauthorized access” to personal information. For others, it requires “unauthorized acquisition.” And then, some states have further qualifications to their definition, such as whether that unauthorized access or acquisition “compromises” or “materially compromises” the integrity, security, or confidentiality of the data. No states (apart from New York) define access or acquisition, and no state defines compromise vs. material compromise. How would you suggest analyzing all these varying terms?

– Patchwork

July 25, 2024

Dear Patchwork,

Excellent question. The first step is determining if there is “access” or “acquisition.” Let’s begin there.

The question of access versus acquisition focuses on how the threat actor interacted with the protected information.

Imagine a burglar enters your house, rifles through important documents on your desk, and reads them trying to find information they can steal. However, whether because of time constraints or lack of interest, after reading the documents, the burglar didn’t take them with him. This would be a form of “access.” The burglar gained access to the documents and viewed them, but never took them out of your house.

Now imagine a scenario where the burglar enters the house, and even if he didn’t rifle through the documents *in* your house, he threw them in a box and took them with him. He has removed the documents from your house. That’s a form of acquisition.

Now let’s apply this metaphor to a security incident. Let’s say there is evidence that a threat actor gained access to your system and clicked and opened a file. That would likely be a form of access. If a threat actor exfiltrated the files — meaning they copied, downloaded, or otherwise removed the information from your environment — that would be acquisition.

Your question about “compromise” or “material compromise” generally concerns the impact on the data from a security, confidentiality, or integrity standpoint. With some exceptions (*e.g.*, where data may have been removed from the environment but remains unreadable), usually, if there is unauthorized access to or acquisition of data, it is considered compromised, whether “material” or not.

So, our next step is typically to see if the law allows for a risk of harm analysis, which focuses not on the impact to the data, but on the potential impact to the consumer. For example, is the consumer now at risk of identity theft or fraud?

It’s worth noting that some of the factors you may consider when evaluating the risk of harm to consumers are the same factors you would use to determine whether the security, confidentiality, or integrity of the data has been compromised. For instance, if the data was encrypted and the threat actor did not gain access to the decryption key, we might conclude that the confidentiality, security, or integrity of the data has not been compromised. Consequently, the incident is unlikely to result in harm to the consumer since the threat actor cannot view or use the data.

As you noted, many states don’t qualify what they consider to be access, acquisition, compromise, or even a material risk of harm. When in doubt, however, use the *patchwork* to your advantage (see what I did there?). Despite their differences, all these laws are grounded in the same fundamental principles and aim to protect

consumers. Therefore, if one statute is silent on a particular issue, it may be reasonable to look to other laws or legal opinions for guidance. By doing so, you can draw on a broader range of interpretations and best practices to inform your approach and ensure compliance with the overarching goal of consumer protection.

Cheers,

Understanding Breach Notification Obligations Under California Law: What Does the CCPA Require?

Dear Mary,

I am the privacy compliance officer at a cloud-based software company. We recently experienced an incident where, although none of our client's data was compromised, it appears that our employees' information may have been copied and removed from our environment. This information includes employees' full names, salaries, and salary schedules. All of our employees reside in California, and given the CCPA's broad definition of personal information, I am assuming notification will be required?

– Frowning in Fresno

July 17, 2024

Dear Frowning,

I have been patiently waiting for this question, so thank you for this. There has been a lot of confusion surrounding the California Consumer Privacy Act (CCPA) and its implications for breach notification obligations.

First, it's important to clarify that the CCPA is primarily a privacy statute designed to provide consumers with

certain rights over their “personal information” and to ensure transparency from businesses regarding their information practices. While the CCPA does broadly define “personal information,” California has a separate breach notification statute, Cal. Civ. Code § 1798.82, which specifies when businesses must notify individuals of security incidents. The CCPA does not change the breach notification obligations outlined in this statute. In other words, the CCPA does not dictate whether you need to notify individuals or regulators of a breach. You should refer to California’s breach notification statute for that information.

The good news is that while the CCPA broadly defines personal information, the breach notification statute uses the term “personally identifiable information,” which is more narrowly defined. Based on the details you’ve provided, an individual’s salary or salary schedule is not considered a protected data element under this statute, so there’s a chance this incident may not trigger notification. I do want to note that while the CCPA doesn’t change whether notice will be required, the CCPA does allow consumers to bring an action for statutory damages in the event of a data breach due to a business’s failure to implement reasonable security procedures (sidenote: I think this is the provision that may have led some to mistakenly believe that the CCPA changes breach notification obligations in California, but it does not). Before seeking these statutory damages, the consumer must provide a 30-days’ written notice identifying the specific CCPA violation (*i.e.*, the business’s failure to implement reasonable security procedures). My point in sharing this information is to emphasize that if you ever need to issue a breach notice under California law, you should be mindful of this provision when drafting your notification letter or responding to any potential cure notices. The language used in these communications could come back to bite you later on.

I hope this information helps turn that frown upside down.

Cheers,

Preserving Forensic Artifacts Following Incident Detection

Dear Mary,

One of our employees recently fell victim to a phishing attack, allowing unauthorized access to their email account for a brief period. To be safe, we reset everyone's passwords and terminated all active sessions. We're now in the process of hiring a law firm to determine if we need to notify anyone about the incident. It's taking a little longer to get them engaged, but I'm hoping to have this done soon. In the meantime, is there anything else we should be considering?

– Not Entirely Clueless in Connecticut

July 10, 2024

Dear Not Entirely Clueless,

It sounds like you're on the right track with containment (i.e., securing your environment) and seeking legal counsel. The law firm will likely recommend hiring a forensic firm to assess the extent of the incident (e.g., whether any data was accessed or taken). One critical step is to ensure your team preserves any relevant logs or artifacts, as these will be critical for the forensic analysis. Different logs provide varied information and have different retention periods, so it's important to halt any rollover or deletion processes. By maintaining comprehensive logs, you can better determine the scope of the compromise, potentially reducing the number of notifications required. Without such logs, you may face uncertainty and difficulty in deciding who to notify and on what basis.

Can Vendors Notify Affected Individuals on Behalf of Businesses After a Data Breach?

Dear Mary,

We were recently impacted by a vendor incident, and the vendor is offering to provide notice to the

impacted individuals on our behalf. That sounds like great news to us, but is this something we can and should consider?

– Potentially Optimistic in Miami

July 3, 2024

Dear Potentially Optimistic,

Yes, this is certainly an option worth considering, and many businesses have taken this route before. Your contract with the vendor may even address notification obligations in the event of a security incident and whether they will provide notice to the impacted individuals on your behalf. However, here are a few things to keep in mind.

1. **Is the Notice Legally Compliant?** Ensure your team reviews the content of the notice to confirm it complies with any potential legal obligations (*e.g.*, if social security numbers are impacted, is the vendor providing consumers with any required credit monitoring?). Some breach notification laws have notice content requirements, so be sure to review the notice from that perspective.
2. **Does the Notice Explain Why the Vendor Has the Consumers' Information?** A common issue with vendor notices is that they might not explain why the vendor has the consumer's information, which can confuse people. Make sure the notice explains this clearly. Data owners, such as yourself, sometimes request to be named specifically in the notice or that the notice include sufficient context to explain the relationship between the vendor and business, even if in general terms.
3. **Verify the Recipients and Process for Notification.** Verify who will receive the notice and how it will be sent. If mailing, consider whether you need to review the addresses being leveraged or if the vendor already has the most up-to-date information.
4. **Call Center Scripts.** If the vendor sets up a call center, ask to review the script to see what information will be given to consumers who call in.
5. **Proactive Notification.** Even though your vendor may ultimately provide the formal breach notification letter, consider whether a proactive notification to affected individuals should be sent. Doing so may help alleviate concerns or questions as to the legitimacy of the notice and show that you're involved and on top of the situation.

Remember, while the responsibility to notify usually lies with the data owner, you can still likely leverage a vendor to handle this. Just make sure you do your due diligence to ensure the notice complies with legal requirements and doesn't create additional exposure for your company.

How to Respond When Your Service Provider Suffers a Cyberattack

Dear Mary,

One of our critical service providers recently suffered a cyberattack. It's all over the news, and our business operations are severely impacted. We're losing money every day, and we have no idea how long this will last. Do you have any suggestions on what to do? The lack of information from our service provider is incredibly frustrating.

– Frustrated in Dallas

June 26, 2024

Dear Frustrated,

You are not alone in facing this challenge. Many businesses have encountered similar issues, and if they haven't yet, they should brace themselves because they likely will in the future. Here are some steps to consider:

1. **Ensure Your Environment is Secure:** If there's any chance the cyberattack could have spread from your service provider to your own systems, take immediate action to secure your environment. This might include hiring a forensic investigation firm to thoroughly check your systems, just to be safe.
2. **Hire a Forensic Accountant:** Consider bringing in a forensic accountant to help your team determine and document any potential business losses. This could be crucial if you plan to file an insurance claim to recover some of these losses. It's better to address this now rather than scrambling to figure it out later.
3. **Business Continuity Options**: Consider whether there are any business continuity options to mitigate the potential disruption. This could include looking into alternate service providers (even if just temporary) to ensure continuous operations.
4. **Review Legal Notification Obligations:** If your service provider handles personal information on your behalf, you need to consider any legal notification requirements that may be triggered (*e.g.*, your company may have a legal obligation to notify others about the incident). Consult with legal counsel to understand what obligations you may have if any of your data has been compromised. With that said, you may not even know at this point what data of yours, if any, is involved. This takes me to my next point.
5. **Extend Some Grace to Your Service Provider:** This might be difficult, but try to be patient with your service provider. Cyberattacks are increasingly common, and thorough investigations and recovery efforts take time. Ensure they are taking appropriate steps, but once confirmed, give them some space to manage the situation. Pressuring them for immediate information may result in inaccurate updates or a faulty timeline. Your legal counsel can help you determine how much time is reasonable and when it might be necessary to apply more pressure.

Good luck to your team. Seems like every day we hear about a new vendor incident. Breach notification laws need to catch up in this regard, but that's a discussion for another day…

– Mary

Understanding Regulatory Response Times Following a Cybersecurity Incident

Dear Mary,

We received a data request from Health and Human Services, Office for Civil Rights, today. It was in connection with a data security incident that happened almost a year ago. Is this normal? Should this impact how we respond?

– Not Forgotten in New Orleans

June 20, 2024

Dear Not Forgotten,

Don’t let the one-year delay throw you off; it’s not completely out of the ordinary. There are many factors beyond the incident itself that can influence how regulators approach a potential investigation. This includes things like the staffing levels at the regulators’ offices. I’ve heard whispers of a backlog at OCR, so this delay might just be a result of that.

My advice? Have your counsel reach out immediately and figure out where the potential investigation is heading. Maintaining an open line of communication and determining regulators’ goals early is important. If done right, you may be able to defuse the situation before it snowballs into something more.

My friends at Troutman Pepper wrote a whole series on regulatory investigations following cybersecurity incidents. Probably worth a read. It can be accessed here.

– Mary

Does Every Incident Require a Forensic Report?

Dear Mary,

We had a security incident a few weeks backs that luckily turned out to be nothing. I'll tell you, tension was high around here while the investigation was ongoing because there was a possibility that it was going to be bad. The forensic firm (hired by our outside counsel) figured out that the incident resulted from a misconfiguration in our MFA. We fixed that and now I'm wondering whether we really need a forensic report given the limited impact. I am not sure I understand the need.

– Uncertain in Atlanta

June 12, 2024

Dear Uncertain,

This is certainly one of those topics that gets people chatting. But if you ask me (which you did), I'd say seriously consider getting the forensic report, especially if it may be covered by attorney-client privilege. However, you need to remember two things: (i) even if you believe the report is privileged, assume that it will be part of litigation later; and (ii) the report needs to purely factual. The fact that there was a hiccup with the MFA configuration isn't something that is privileged. So, documenting it in a forensic report doesn't necessarily worsen your position (again, depends on how it is documented). You just need to make sure the forensic report is limited to the facts. There is no room for imagination, opinions, or speculations. Think nonfiction. Like this letter.

It's also worth noting that the forensic report could come in handy later if any issues related to the incident pop up. It demonstrates the company was diligent in investigating the incident and took the right steps from an incident response perspective.

Glad to hear the incident turned out to be small. I guess the saying is true—MFA isn't bulletproof.

– Mary

Should Companies Conduct Their Own Forensic Investigations?

Dear Mary,

I work in the IT department of a mid-sized company that recently detected a security incident. Everyone is freaking out – minus me. My manager asked our IT team to investigate the incident. But the incident is already contained, and business is back to normal. Why do we need to investigate further? Like seriously, why? And if we do need to investigate further, should I be doing this? I've been in IT for a while, and I have never been in this situation before.

– Forensic Forgoer in Florida

June 3, 2024

Dear Forensic Forgoer,

I am happy to hear the incident has been contained. Containment is a critical step in the incident response process, but it is not the only one.

Do You Need to Investigate?

Your first question is do you need to investigate the incident? Y-E-S!

You most certainly do need to investigate. Here's why. A forensic investigation goes beyond containment – you should figure out the nature, size, and scope of the incident because: (1) the business should know; and (2) there may be legal things that the business needs to be thinking about (*e.g.*, notifying people that their data may have been impacted). And when I say "you" – I don't mean you. I mean a third-party forensic investigator. I could recommend a few if you need suggestions but you may also want to consider reaching out to your insurance carrier (assuming the business has cyber insurance – more about that later).

So, why a forensic investigation? Forensic investigators try to answer questions like:

1. Whether your network has been accessed by a bad guy (or girl) – let's say bad girl.

2. How the bad girl gained access to the network (commonly referred to as the “root cause”).
3. What the bad girl did while in the network, *e.g.*, did she move around (laterally) in your environment, and if so, where did she go?
4. Did the bad girl access or exfiltrate (remove) data? And if so, what kind of data?
5. And if the incident has really been contained. I know you said it has but there’s no harm in having a second pair of eyes confirm. To the contrary, there’s a lot of good reasons for doing so (*e.g.*, it eliminates the appearance of bias and reduces privilege concerns if the forensic firm is engaged through the proper channels).

Why do these questions matter? There are legal reasons why they matter. The law requires businesses to notify individuals in the event of a “data breach” (a legally defined term which means there was unauthorized “access” or “acquisition” of certain types of protected information). And trust me, it’s not a good idea to ignore those obligations.

There are business reasons too. Some of your customers may have questions about the incident—like what steps you took to make sure it doesn’t happen again, and if their data what impacted. If you don’t know how the incident occurred and what data was impacted, it’s going to be tough to answer those questions with certainty.

Should You Do the Investigation Yourself?

Now, turning to your next question, should you be doing this investigation?

Earlier I mentioned the use of a forensic investigator. The truth is, it’s usually in a business’s best interest to bring in a third party. Businesses sometimes shy away from third-party forensic investigations for one simple reason – like everything else these days, they cost money. In my experience, this happens most often when a business honestly believes that its employees can perform the same investigation without spending any extra money.

It’s important to mention that sometimes there will be instances when a third-party forensic firm is not needed. BUT, before making that decision, businesses should really think about the legal and business ramifications of doing so. Usually, third-party forensic firms are engaged by outside counsel (lawyers at law firms) on behalf of the business that experienced the security incident. This allows businesses to claim privilege and work-product protection over the investigation and related communications. The law isn’t super clear in this area, but recent cases have made clear that establishing these legal protections involves a fact-sensitive inquiry.

So, if you do the investigation yourself, you might have a tough time arguing that the investigation is privileged. Why? Because courts may view it as something that was done for business reasons, as opposed to legal. Because privilege is meant to allow open communications without fear of them being used against the company, conducting a privileged forensic investigation that is intended to also stop a criminal from further harming the company is likely in every company’s best interest.

You may also want to bring in a third party for optics. Being able to tell regulators and people affected by the incident that a “specialized third-party forensic firm was engaged to determine the nature and scope of the incident” may give those parties comfort, and honestly, it might just be expected these days. I say this because when reporting a data security incident to regulators, several of them make businesses indicate whether a forensic investigation was performed. If you can’t answer yes to that question – there’s a good chance you may get additional questions about the investigation, including whether it was thorough and complete.

Engaging a third-party to perform the investigation could also remove the appearance of bias. While certain in-house security professionals may be in the best position to investigate the cause and scope of a cybersecurity incident given their familiarity with the network, this could create obstacles — like can a company's own investigation of how an incident occurred be trusted — that could otherwise be avoided if a third party is used. Now do you see why optics are important.

Lastly, because you mentioned that you work in IT, I want to at least flag the difference between IT (short for "information technology") and information security. Put simply, IT professionals make stuff happen. They ensure networks, systems, and devices are working and running smoothly. In contrast, information security professionals stop bad things from happening. They focus on protecting data and assets and monitor emerging risks and cyberattacks. Thus, while a majority of security work is handled by IT professionals, understanding the distinction between the two is important.

Ok, to wrap up here, I wanted to share the following takeaways. Keep these handy – they'll come in handy now and for any other incidents that may come up.

1. Don't skip doing a forensic investigation just because you believe the incident has been contained. You need to figure out the nature, scope, and size of the incident for business and legal reasons.
2. When investigating an incident, always consider hiring, through outside counsel, a third-party firm to do the investigation for you. You may not need to take this step for every incident, but it's important to at least consider this step before doing the investigation yourself.
3. Privilege is an important issue that businesses need to be thinking about in the context of responding to security incidents. For IT and security professionals not familiar with this concept – reach out to your legal team and start the discussion.
4. Don't have a legal team or know of any forensic vendors? If your business has cyber insurance, your broker or carrier likely has a preferred panel of vendors that are ready to help with your response. So, if you have insurance, contacting your broker or carrier in the event of an incident may be one of the first steps you take.

Good luck with the incident, Forensic Forgoer. Perhaps you've had a change of heart (and name).

RELATED INDUSTRIES + PRACTICES

- Incidents + Investigations
- Privacy + Cyber