Mighty Guides

Sponsored by

NISOS

# The Critical Value Outside Counsel Brings to Cyber Incident Response

# Table of Contents

# Introduction

When the CEO of Colonial Pipeline testified at a congressional hearing into the ransomware attack that shut down the nation's largest oil pipeline, he said his decision to pay the ransom was "the hardest decision I've made in my 39 years in the energy industry."

It's safe to say that the moment they were attacked, operations managers, cybersecurity teams, and corporate executives entered uncharted territory. Although companies develop cybersecurity protection and response strategies, rarely are they prepared for all the risks they face when a serious incident actually occurs.

These risks include business, legal, and regulatory liabilities that arise not only from the attack, but from how a company responds to the attack. They can damage the business and threaten its viability. Addressing those risks often far exceeds the costs of remediating the attack itself.

That is why an effective response to a serious cyber incident is not just a technical effort managed by an in-house response team. It must be a multi-faceted response overseen by an outside expert tasked with protecting the interests of the entire enterprise.

This ebook shows why an outside counsel with special expertise is the ideal entity to spearhead an attack response. It reveals the importance of establishing a relationship early, because when an attack occurs, risks to the business multiply at an alarming rate.

Anyone interested in improving their company's cyber response posture will find value in this ebook.

## Mighty Guides

Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

All the best,
**David Rogelberg**
Editor,
Mighty Guides Inc.

# Foreword

For those who work within the crosshairs of cybersecurity and law, there is a growing sense of urgency when it comes to security incidents and how to respond to them.

Today, security incidents are commonplace, and lawyers who are adept at the tough conversations (whether with boards, law enforcement, or security stakeholders) are the leaders who will help companies navigate to a better security stance. Let's face it, adversaries are not going away. If anything, they are growing increasingly sophisticated.

As lawyers, we are required to grow and adapt. A level of technical sophistication and subject matter expertise is required of us by the American Bar Association, or we must hire it and bring it onto our team. This book is a step forward. Keep in mind that this is not legal advice. Every incident is different and requires a varied approach. But the underlying expertise and principles can guide practitioners.

For many of us who practice law on the frontlines of cyber attacks, there is an understanding that companies don't get in trouble for having incidents; they get in trouble for how they respond. In many cases we need to step back from a security incident, open the umbrella of attorney-client privilege, and use outside counsel to get the entire team running the right plays. For most companies, the reputational risks of not having a coordinated and strategic approach are too great to attempt this in any other way.

Regards,
**Jennifer DeTrani**,
General Counsel,
Nisos

# Meet Our Experts

**Wynter Deagle**
Partner,
Sheppard Mullin

**Andrew Stanley**
Chief Information Security Officer,
Mars

**Aaron Charfoos**
Partner,
Paul Hastings

**Jennifer DeTrani**
General Counsel,
Nisos

**Justin Zeefe**
President and Co-Founder,
Nisos

**Evan Wolff**
Partner,
Crowell & Moring

**Jan Grzymala-Busse**
Security Manager,
Chicago Board Options Exchange

Chapter One

# The Critical Value Outside Counsel Brings to Cyber Incident Response

"We've experienced a cyber incident. We've got a big problem."

Those are words that no C-level executive wants to hear from the IT security team. Questions immediately arise: What happened? Is it still happening? What has been lost or damaged, and what's the business impact? How much is it going to cost us? Whom do we need to bring in or notify? How do we ensure that this is not going to happen again?

Those questions rarely have answers in the early stages of a serious incident. Security teams are working furiously to understand and contain whatever is happening. Business managers are scrambling to see how the attack is affecting normal operations and whether it is affecting partners and customers. Marketing and public relations people are already working to frame responses to questions they dread being asked. Tensions are rising. As the magnitude of the problem becomes apparent, the finger-pointing begins. The security team is working 24/7 to understand the attack, contain it, and restore systems as quickly as possible. IT and security executives are bombarded with questions from increasingly exasperated executives across the company who want to know the extent of the damage and how this security failure happened. Careers could be on the line.

"You can be in perfect compliance with every standard or regulation and still have a major incident."

Evan Wolff

Serious cyber incidents always begin as technical problems, but they quickly balloon into a great deal more. Beyond the costs of business disruption and damage to customers and brand, they often spawn penalties and lawsuits whose costs can far exceed the costs of technical remediation. A lot depends on the actions you take—or don't take—in the early stages of an incident. For instance, a breach in progress can actively expose information you are legally required to protect, a situation that puts you at risk of regulatory violation and lawsuits. Yet, shutting down a system to stop the data leak can disrupt a critical service that you are contractually obligated to deliver. What is the right course of action?

If you're not sure of the answer, you are not alone. The fact is, few organizations are equipped to handle all the collateral risk that comes with a serious cyber incident. They may have playbooks for dozens of attack scenarios, but at the end of the day, decisions must be made that have crucial business and legal consequences. Those decisions must be made quickly because the incident is still in progress. With every passing minute, the hole gets deeper.

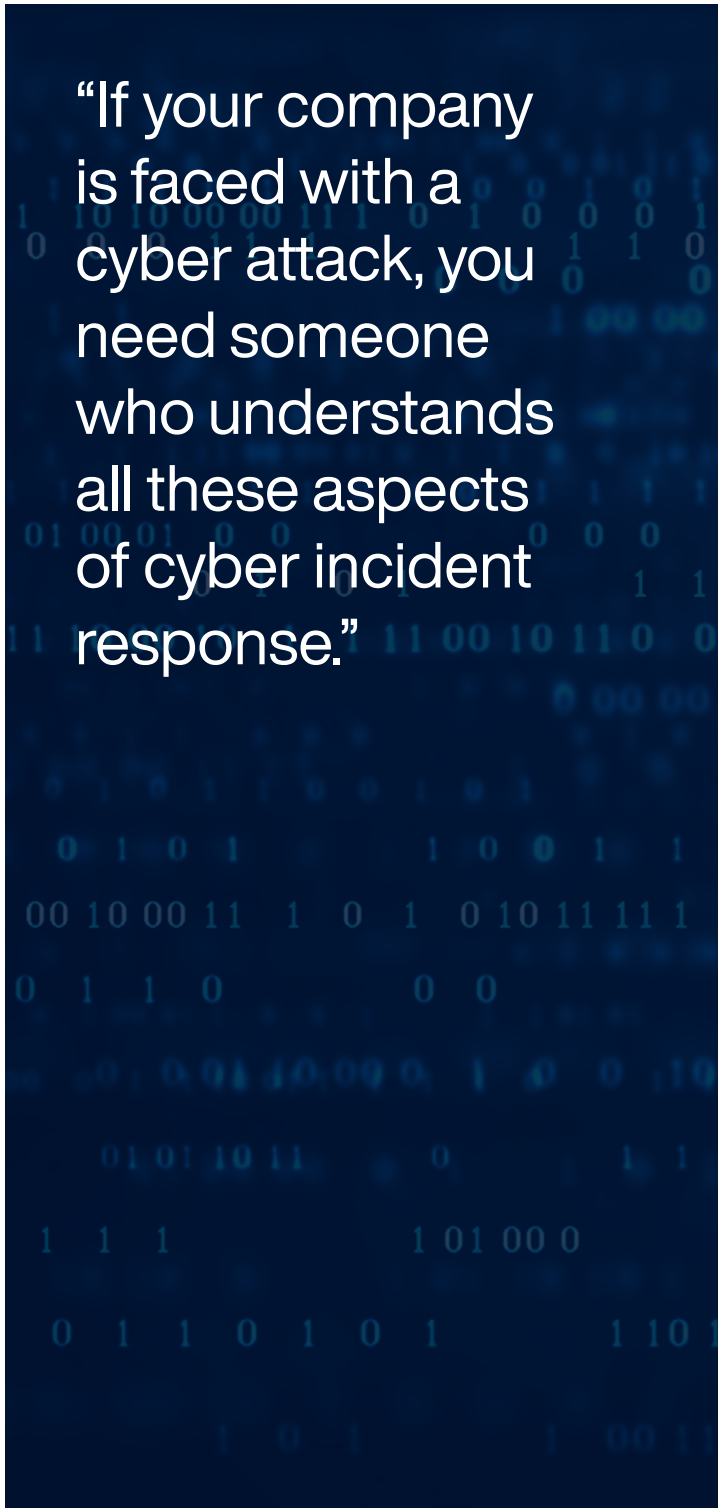
The smartest move any company can make when facing a serious cyber incident is immediately to contact an outside attorney who specializes in cybersecurity and breach management. The company should make this call even before it contacts law enforcement or on-call outside technical experts. Why is this so important? Major security incidents come with technical, business, and legal implications that pose a potentially existential risk to the business. If your company is faced with a cyber attack, you need someone who understands all these aspects of cyber incident response. That person will not be someone on staff—not your chief of security or IT, not your general counsel. You need outside counsel-people who have been down this road before and can oversee your incident response effort. They know when and how to bring in technical expertise

"You need outside council there because they've been down this road before."

Andrew Stanley

in a way that protects your interests; they can mediate between internal and external stakeholders during the stress of incident response, and they provide advice about which steps to take under a reasonable expectation of litigation. They work to protect the whole company from legal liability and brand deterioration.

What makes an outside counsel who specializes in incident response unique, and when should you call them in? Let's take a closer look.



# Key Points

- Serious cyber incidents always begin as technical problems, but they quickly balloon into a great deal more. They often spawn disruption, penalties, and lawsuits whose costs can far exceed the costs of technical remediation.

- When facing a serious cyber incident, you need an expert who has been down this road before and can oversee your incident response effort. That person will not be someone on your staff. It will not be your chief of security or IT, and it will not be your general counsel. It will be an outside counsel.

"They work to protect the whole company from legal liability and brand deterioration."

Chapter Two

# What Outside Counsel Brings to the Table

For purposes of security incident response, outside counsel must be more than an ordinary business lawyer.

Effective incident response requires someone who has deep knowledge of compliance and regulatory requirements and knows how to navigate legal liabilities that can have a significant impact on the business, which law enforcement and government agencies should become involved, when they should be called, and what they should be told. Outside counsel knows all this, and they know when it's in the company's best interest to bring in specialized technical expertise and how best to manage that relationship while preserving privilege.

> **"A data beach becomes a reputation injuring event that companies have to address properly or face long-term repercussions."**
>
> 
>
> **Jennifer DeTrani,**
> General Counsel, Nisos

"In addition to quickly assessing whether the environment is safe to use after an attack and understanding what happened, one of the first things you must do is determine if there are any regulatory risks that require disclosure."

Evan Wolff

This combination of skills gives the business several layers of legal protection:

- **Knowledge of legal and regulatory pitfalls.** Every cyber incident presents its own challenges and possible responses. Fully informed of an unfolding situation, when they understand the business needs and the actions being taken to mitigate an incident, they can direct actions that reduce overall risk to the business. For instance, in one case, a financial services company experienced a distributed denial-of-service attack on a public-facing website that seriously threatened normal transactional activity. The security team wanted to take down the website immediately until they contained the attack. Outside counsel recommended that the team not do that right away. In addition to being a public-facing site, the website served as a trading platform for partners. If the security team took down the site, they risked lawsuits from contract partners, who would not be able to conduct trades, and there would likely be a US Securities and Exchange Commission investigation. Outside counsel was able to hit the pause button on that action until they determined a less disruptive strategy. It was the right call, one that no one in the company could have made. The security team was unaware of the potential legal issues, and the company's general counsel was not tracking the technical details of the mitigation efforts. Outside counsel provides advice and coaching on the legal ramifications of technical fixes that could create bigger business issues than the security event itself.
- **Engaging with law enforcement.** Outside counsel knows when to engage with law enforcement, which agencies to engage with, and what information should be voluntarily disclosed. It is important to recognize that although you feel victimized when you suffer a cyber attack, law enforcement may not view you as the primary victim and may not necessarily be on your side in subsequent investigations or legal actions. This is true even if it's a law enforcement agency that notifies you that you have been attacked. Outside counsel will be able to better protect your interests while cooperating with law enforcement.

"When outside counsel is fully informed of an unfolding situation, when they understand the business needs and the actions being taken to mitigate an incident, they can direct actions that reduce overall risk to the business."

- **Protection of legal privilege.** If you manage an incident yourself, you may be required to disclose everything related to that incident in subsequent official investigations or legal discovery processes. This material can include proprietary business information and detailed information about the company's technical infrastructure and security practices. If you immediately contact outside counsel to manage incident response, however, key information related to the incident may be protected by legal privilege, giving you more control over what you are required to disclose.
- **Outside technical expertise.** Outside counsel that specializes in cyber incident response will have close relationships with highly skilled technical experts who specialize in forensics and security remediation. If you call in your own forensics expert, whatever that expert discovers, recommends, and reports is subject to disclosure in an investigation. If outside counsel calls in the expert for purposes of consultation, manages this relationship, and oversees the work, those findings can be protected by legal privilege. When your company experiences a cyber incident, you should never call in your own outside expert, even if incident forensics and remediation are part of an existing service agreement. Your first call should go to outside counsel.

As important as these skills and knowledge are, outside counsel brings something else that is critical to a company struggling with incident response. The fact that outside counsel are "outside" means that they are not coming in to take sides or find fault. They are there for the sole purpose of protecting the interests of the company, which puts them in a position to thoughtfully mediate competing interests and provide a voice of objective reason at a time when tensions are running high.

Having outside counsel take control of the response effort when a serious incident occurs clearly provides legal and operational benefits that reduce overall risk to the company. The big question is, then, When should you bring in outside counsel?

"The fact that outside counsel are "outside" means that they are not coming in to take sides or find fault."

# Key Points

- Outside counsel provides advice and coaching around legal ramifications of technical fixes that might create bigger business issues than the security event itself.
- Although you feel victimized when you suffer a cyber attack, law enforcement may not view you as the primary victim. They may not be on your side in subsequent investigations or legal actions. Outside counsel will protect your interests in all engagement with law enforcement.
- If you manage an incident yourself, you may be required to disclose everything related to that incident in subsequent official investigations or legal discovery processes. If outside counsel manages the entire incident response, key information may be protected by legal privilege.

"Outside counsel is there for the sole purpose of protecting the interests of the company, which puts them in a position to thoughtfully mediate competing interests and provide a voice of objective reason at a time when tensions are running high."

Chapter Three

# How to Choose and Call In Outside Counsel

Employing outside counsel to oversee your response to a serious cyber incident minimizes risk to the business by providing several layers of legal protection. To gain that protection, it is imperative that you bring outside counsel into the process as soon as possible after an incident has occurred.

Of course, you cannot do that if you have not already established a relationship with outside counsel before the incident. Establishing that trusted relationship takes time, and time is one thing you will not have in the midst of a heart-stopping cyber crisis.

When vetting outside counsel, you must determine whether the outside counsel candidate can work closely with key business, legal, and technical stakeholders in the organization. They need to be able to talk credibly to all the C-level executives and report directly to the board, as needed. You must be convinced that outside counsel understand your business and any unique aspects that would be relevant to incident response. In the example of the attack on a financial services company where outside counsel averted potentially serious legal and regulatory liability by preventing the shutdown of a compromised website, outside counsel could not have made that call if they did not have a good understanding of how the business worked.

Some companies prefer to keep the legal and technical teams separate as they ramp up an incident response. In that way, the technical team can focus on fixing the problem. But outside counsel who specialize in incident response want the security executives at the

"When you are alerted to the incident, that is not the time to start figuring out who your preferred vendors are. Incidents are fast moving, so you need someone working with you who has the right skill set, is responsive, and understands your work preferences."

Wynter Deagle

same table as the rest of the executive team. Outside counsel need to understand what is happening on the technical side so that they can consider the legal implications of actions the security team is taking. It's just as important for them to communicate with and be trusted by the security team as it is for them to be trusted by the rest of the executive team.

Trust and communications are critical. When a serious incident occurs, key members of the response team work around the clock, and decisions must be made day and night. Outside counsel will be available on short notice to help work through these decisions.

Many companies develop a working relationship with outside counsel as part of their overall preparedness strategy. That way, the attorneys are available to consult about whether an event actually requires their help; if the event is indeed serious, they can step in and hit the ground running. Establishing that relationship early gives outside counsel a chance to become familiar with the company and its key players.

It also gives them a chance to overcome common misconceptions about their role in the process. This is important because those unresolved misconceptions can interfere with an effective incident response. What are common misconceptions about the role of outside counsel, and how do you overcome them?

# Key Points

- To gain legal protections when an incident occurs, it's imperative that you bring outside counsel into the process as soon as possible. You cannot do that if you have not already established a relationship with outside counsel prior to the incident.

- When vetting outside counsel, you must determine if the candidate can work closely with key business, legal, and technical stakeholders in the organization. It's just as important for them to communicate with, and be trusted by, the security team as it is for them to be trusted by the rest of the executive team.

"Trust and communications are critical. When a serious incident occurs, key members of the response team work around the clock, and decisions must be made day and night.

Outside counsel will be available on short notice to help work through these decisions."

Chapter Four

# Overcoming Common Misconceptions

When outside counsel are given incident response oversight, the most common reaction within the company is, "Why do we have a lawyer working on this technical problem?" For those unfamiliar with the role of outside counsel, that is a perfectly reasonable question. Failure to answer it adequately can lead to reticence and a misconception that seriously hampers the response effort.

For instance, it is easy for business and technology executives to assume that outside counsel are not experts in the company's business and therefore cannot process all the detailed information about an incident. That assumption can lead to outside counsel receiving a filtered-down version of relevant facts that limits their ability to make critical judgments about what may not be on the horizon of business and technology managers.

Business leaders may question the need for outside counsel when they already have their own internal legal team. Yet, it is often the case that the company's general counsel makes the call to bring in outside counsel. There are good reasons for that. For one thing, general counsel will not have outside counsel's specialized knowledge about all the legal risks that come with a cyber incident. Also, general counsel know that their position in the company will make it more difficult to play an objective role that bridges competing interests that heat up under the pressures of a cyber attack. Finally, outside counsel will be highly sensitive to maintaining the privileged status of information related to the incident.

"My job is actually to mitigate your litigation risk and to make you look good."

Wynter Deagle

Internal technology teams may assume that outside counsel think they know everything, and by stepping into the process, they will attempt to tell internal technical experts how to do their jobs. Or, outside counsel are simply there to say "no" to everything the internal tech teams try to do. It's a dangerous assumption that can lead to security teams taking actions without first checking with outside counsel and, in doing so, incurring unintended legal risks.

For this reason, it is important to establish a trusted relationship with outside counsel before an incident occurs. It does more than give outside counsel an opportunity to become familiar with the business and its key people. It also gives outside counsel the opportunity to demonstrate through thoughtful questioning and understanding that they have the executive team's back. It is incumbent on outside counsel to show that they understand the business and the security event, and they are there to comply with legal and regulatory requirements. They must show that they are not there to assign blame or find fault. They are there to protect the enterprise.

Outside counsel can establish trust and overcome misconceptions by meeting with C-level executives, the corporate legal team, and key security team players. Outside counsel need to bring these people together and treat them as a team rather than as factions in the company.

Establishing that level of trust is essential if a company is to realize the full value that outside counsel bring to incident response. One area critical to outside counsel's goal of limiting legal risk is managing the flow of information about an incident, which brings us to the tricky question of legal privilege.

"Knowing the culture, the systems and the people that you're going to be dealing with is absolutely critical."

Aaron Charfoos

# Key Points

To gain legal protections when an incident occurs, it's imperative that you bring outside counsel into the process as soon as possible. You cannot do that if you have not already established a relationship with outside counsel prior to the incident.

When vetting outside counsel, you must determine if the candidate can work closely with key business, legal, and technical stakeholders in the organization. It's just as important for them to communicate with, and be trusted by, the security team as it is for them to be trusted by the rest of the executive team.

"It is important to establish a trusted relationship with outside counsel before an incident occurs."

Chapter Five

# The Importance of Legal Privilege in Protecting the Company

If your company experiences a cyber attack and you hire an outside security expert to determine what happened, that expert's work is not protected by legal privilege. Why does that matter?

It can matter in several ways. If the outside expert writes a report detailing the causes of an incident in a way that finds fault with actions your company did or did not take, that assessment can become evidence in a lawsuit filed against your company. In fact, all the forensics work would have to be disclosed in the event of a lawsuit.

Or, say that the outside expert writes a report that includes 150 recommendations your company should implement to improve its security posture. It's likely that you do not have the budget to implement all those recommendations. If you do not implement them all, that report could become evidence of negligence in any regulatory investigation or legal action arising from a subsequent security incident.

It has become common practice for companies to enter into long-term contracts with cybersecurity service providers. Those contracts often set aside a certain number of hours for cyber incident response. If an incident occurs and experts are quickly called in, whatever work they do will not be covered by legal privilege and can become evidence in legal and regulatory actions.

"The courts have said that if a company is going to hire a technical forensic response expert to deal with an incident, it generally is not going to be protected with privilege."

Aaron Charfoos

In contrast, if you call in outside counsel and outside counsel brings in a cybersecurity expert to provide advice about responding to the incident, much of that work may be protected by legal privilege, meaning that your company would not be required to disclose it. The key is that this specialized forensic work must be scoped closely to the work outside counsel requires that enables them to advise you on the incident.

Legal privilege is a tricky issue. Lawyers and judges often wrestle with it, and they often have differing viewpoints on whether legal privileges should apply to written findings and work products. Outside counsel is in an ideal position from which to scope and manage forensics work in ways that maximize the protections that legal privilege affords. It is not just the outside security experts who are important here, however. Internal communications are also a potential issue in any legal action.

You can take many actions to optimize legal privilege protections in a way that gives you more control over incident-related information you may be required to disclose:

- **Bring in outside counsel as early as possible after an incident occurs.** If possible, place the entire matter of assessing the incident under the purview of outside counsel.
- **Do not hire outside cyber forensics experts directly.** If you have a long-term service provider contract that includes forensics, there should be a clause that in the event of a security incident, all forensics work must be contracted through outside counsel.
- **Scope the forensics work carefully.** Separate out any proactive "fixes" from the statement of work and contracting that relates to assessment of the security incident.
- **Forensics should focus on determining what happened.** The forensics work should refrain from assigning fault or recommending fixes in relation to findings about what actually happened.

"If you want to protect what the third party consultant is doing or their report, outside counsel needs to retain that consultant, direct, and supervise their work."

Wynter Deagle

- **Avoid written forensics reports.** Whenever possible, oral updates and assessments are preferable to written reports or email discussions. Keep discovery disputes to a minimum. In cases where a forensics report is necessary, omit recommendations for improving cybersecurity practices. Limit the sharing of the report along with any materials used to create it.
- **Communicate on a need-to-know basis.** Limit incident-related communications to those who need to know for purposes of managing incident response. All incident-related communications with anyone outside the company, including regulators, lawyers, and law enforcement, should first be reviewed by and discussed with outside counsel. Under no circumstances should there be discussions about who may or may not have been at fault.
- **Defer to outside counsel's advice.** Seek advice from outside counsel about the legal implications of actions and responses under consideration. Be thorough in explaining the reasons for and consequences of response actions. Follow outside counsel's advice.

Legal privilege is an important tool in protecting the company against legal risk. Do not hesitate to take full advantage of this protection.

"Outside counsel is in an ideal position from which to scope and manage forensics work in ways that maximize the protections that legal privilege affords."

# Key Points

- If the outside expert writes a report detailing the causes of an incident in a way that finds fault with actions your company did or did not take, that assessment can become evidence in a lawsuit filed against your company.
- If outside counsel brings in a cybersecurity expert to provide advice about responding to the incident, much of that work may be protected by legal privilege, meaning your company would not be required to disclose it.
- If you have a long term-service provider contract that includes forensics, there should be a clause that in the event of a security incident, all forensics work must be contracted through outside counsel.

"Seek advice from outside counsel about the legal implications of actions and responses under consideration. Be thorough in explaining the reasons for and consequences of response actions. Follow outside counsel's advice."

# CONCLUSION

Any cyber incident that damages customers, partners, or investors incurs legal risks and liabilities that could be greater than the costs of remediating the incident itself.

Although organizations typically have incident response plans at the ready, most are ill-prepared to manage legal risks associated with the actions they take to fix the technical and business problems. Legal risks become especially critical in the midst of a cyber disaster as everyone frantically scrambles to understand and contain the event, restore normal operations, and save their careers.

Outside counsel with special expertise in cyber incident response should be the cornerstone of all efforts to mitigate a serious cyber incident. Their knowledge of the legal and regulatory pitfalls will prove invaluable when developing remediation plans that limit your legal risks with customers and partners. It is also essential when engaging with law enforcement so that you don't unintentionally incriminate yourself, in giving depositions to regulators, and in the way you manage incident forensics and internal communications so that you can further protect yourself through legal privilege.

Outside counsel can be most effective when brought in to oversee an incident response effort as early as possible. Ideally, you will establish a solid working relationship with an outside counsel before you become the victim of a serious cyber attack. This enables outside counsel to know your business, know your key people, and quickly understand what is at stake when an incident occurs.

It may seem counter intuitive to appoint an outside counsel to oversee the resolution of a technical issue. But that is just the point. A serious cyber incident is not only a technical problem. It is a complex event with technical, business, and legal implications that pose a potentially existential risk to the business. That is why the best strategy is to bring in outside expertise that can rationally balance all these interests and risks with the sole objective of protecting the entire enterprise.

# Key Points

- Although organizations typically have incident response plans at the ready, most are ill-prepared to manage legal risks associated with the actions they take to fix the technical and business problems.
- Outside counsel with special expertise in cyber incident response should be the cornerstone of efforts to mitigate a serious cyber incident. Their knowledge of the legal and regulatory pitfalls is invaluable in limiting your legal risks with customers and partners.

A serious cyber incident is not only a technical problem. It is a complex event with technical, business, and legal implications that pose a potentially existential risk to the business.

Bring in outside expertise that can rationally balance all these interests and risks with the sole objective of protecting the enterprise.

# Learn More About Our Experts

**Wynter Deagle,** Partner at Sheppard Mullin

Wynter Deagle is an experienced first-chair litigator who defends clients from privacy, cybersecurity, data protection, and technology-related individual and class actions, business disputes, regulatory investigations, and enforcement actions. Outside of the courtroom, she helps clients roll out data-driven products and services, respond to data security incidents, and make compliance decisions that balance business functionality with the requirements of privacy and data security laws and regulations.

**Andrew Stanley,** Chief Information Security Officer at Mars

A seasoned technology executive, Andrew Stanley has spent 20 years across multiple industries building strong teams, driving transformation programs, and delivering novel solutions to difficult technology problems. He is continuously recognized as a thought leader within the World Economic Forum, MIT on cybersecurity, government, and diplomatic groups. He is an advisor to Google's Enterprise Solutions and Xerox and is a CISO Ambassador for the FBI.

**Aaron Charfoos,** Partner at Paul Hastings

Aaron Charfoos, a partner in the Paul Hastings Data Privacy and Cybersecurity practice, serves as chair of the Firm's litigation practice in Chicago. He is an accomplished cybersecurity, privacy, class action, and data protection trial lawyer who has litigated data breach and trade secret theft cases and defended clients in regulatory investigations brought by U.S. and international regulatory bodies.

**Jennifer DeTrani,** General Counsel at Nisos

Jennifer DeTrani has a demonstrated history of mission-driven results in the cybersecurity, information technology, secure communications, and software industries. She provides a strong compliance, growth-focused infrastructure, and outreach to the legal community in her work as general counsel and EVP at Nisos. She has also managed the legal and human resources departments and privacy concerns for Wickr and had her own law firm in the San Diego area.

**Justin Zeefe,** President and Co-founder at Nisos

Justin Zeefe cofounded Nisos in 2015 and serves as its president. His vision delivers smart defense and effective response against advanced cyber attacks, disinformation, and abuse of digital platforms. He spent 10 years as the operations officer for the U.S. Government, including multiple warzone deployments and overseas postings. Zeefe is one of the twelve experts who contributed to the book *Cybersecurity in Our Digital Lives.*

**Evan Wolff,** Partner at Crowell & Moring

Evan Wolff is a partner at Crowell & Moring and the cochair of its Privacy & Cybersecurity Group. With a national reputation for understanding complex cybersecurity legal and policy issues, he develops legal, technical, and governance mechanisms to prepare companies with rapid, comprehensive responses to cybersecurity risks and threats. Wolff has conducted training and incident simulations, developed response plans, led privileged investigations, and advised on hundreds of data breaches.

**Jan Grzymala-Busse,** Security Manager at Chicago Board Options Exchange

A security researcher passionately chasing the security dragon, Jan Grzmala-Busse has been a software engineer and developer, an information security specialist and researcher, a security engineer/manager, and a senior information security consultant/contractor. Currently, he is serving as the director of data classification at BMO Financial Group. Fluent in Polish and English, he earned his bachelor's and his master's at the University of Kansas.

Expert-Driven, Cross-Functional Research & Analysis

# Managed Intelligence™

Nisos enables cybersecurity, corporate security, and trust and safety teams with world-class intelligence capabilities tailored to meet their needs.

Fusing robust data collection and a deep understanding of the adversarial mindset, we deliver smarter defense and more effective response against advanced cyber attacks, disinformation, and abuse of digital platforms. Contact us to learn more about our service offerings at www.nisos.com.

## Third Party Intelligence

Gain deep visibility into latent risks in your supply-chain or acquisition targets

## Reputation Intelligence

Defend your brand and reputation from external threats and disinformation

## Protective Intelligence

Identify, assess, and mitigate threats to your company's people, property, and assets

## Cyber Intelligence

Reveal digital threats outside your network, unmask insiders, and threat hunt on the dark web

## Platform Intelligence

Stop platform abuse that impacts your customer's experience and trust in your brand

## Fraud Intelligence

Stop fraud leveraging corporate environments, services, and systems for monetary gain

NISOS