CYBERSECURITY, DATA & PRIVACY

Cybersecurity is your business

A practical guide for executives in the battle against the $8 trillion threat to your company, customers and employees

BRUNSWICK

Written by

Glenn Hall
Executive Editor

Based on insights from Brunswick's Cybersecurity, Data & Privacy experts:

Yasmin Brooks
Partner in London

Katharine Crallé
Partner in New York

Siobhan Gorman
Partner in Washington, D.C.

Nicola Hudson
Partner in London

George Little
Partner in Washington, D.C.

Paddy McGuinness
Senior Advisor in London

Admiral Mike Rogers, USN, Ret.
Senior Advisor in Washington, D.C.

Mark Seifert
Partner in Washington, D.C.

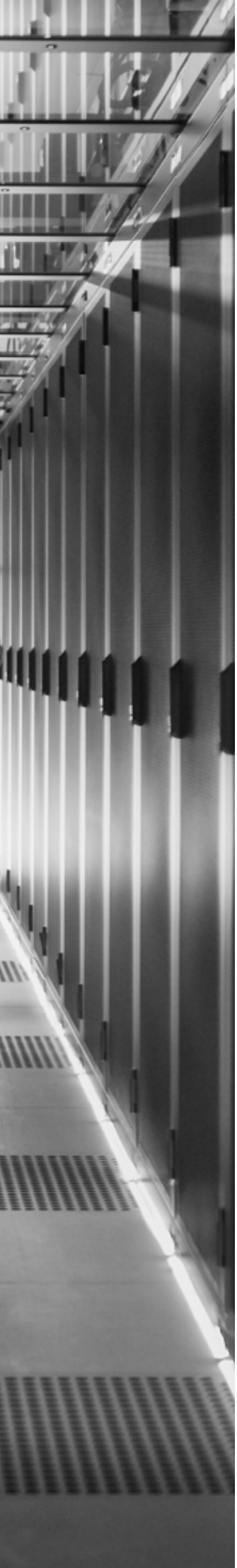
Design by

Victoria Robinson
UK Design Manager

Data visualisation by

Karoline Von Tschurtschenthaler
Data Visualization Analyst

RJ Andrews
Data Visualizer



Contents

Is your company ready for the next cyberattack?

The risk your company faces from digital attacks is growing in scale and complexity. We are witnessing a cybercrime explosion, an increase in state actor attacks and a proliferation of cyber tools which will syphon an estimated $8 trillion from global businesses and society this year alone.

This guide shares best practices from companies that successfully mitigated a breach and lessons from those that struggled. These are real-world insights based on an analysis of hundreds of cyber and data security incidents that Brunswick's global cybersecurity experts helped resolve.

We've distilled that analysis into this booklet, which outlines how board directors, chief executive officers and C-suite leaders across multiple functions should prepare for – and respond to – an almost inevitable cybersecurity breach.

We hope that these insights will help you defend, and even enhance, your company's reputation.

Know the Rules of Engagement

Chapter takeaways: The most successful responses to a data breach start with an integrated crisis team led by a C-suite that understands their individual roles and works together seamlessly. Putting your stakeholders at the heart of the decision-making process will help build trust and protect your business and brand.

When cybercriminals break through your company's digital walls – and statistics show that they inevitably will – corporate weaknesses will be laid bare.

If your C-suite executives aren't clear about their roles in a crisis, you'll squander the chance to prevent harm to your company's reputation. If you don't have a cross-functional and battle-tested crisis team, you'll put revenue at risk. And if you don't have a stakeholder-centric communication plan, you'll incur the wrath of customers, investors, regulators and your board.

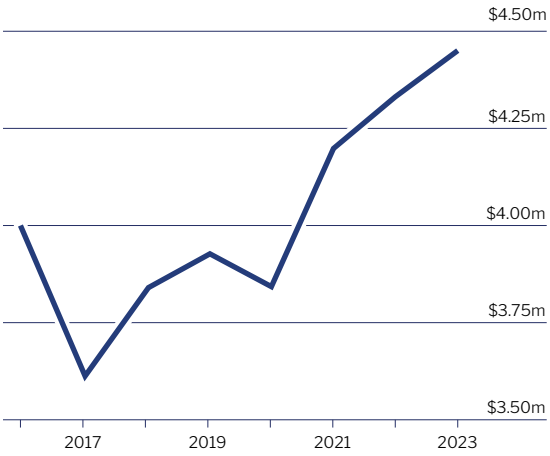
Companies that have successfully navigated a cyber incident had these elements in place before the crisis hit: an engaged C-suite, an integrated crisis team and a targeted communications strategy. Yet these elements commonly take a back seat when it comes to a company's ever-growing list of cybersecurity priorities.

"How you respond to a cyberattack is often more important than the attack itself," says **George Little**, a Brunswick partner in Washington, DC, who works with the **Cybersecurity, Data & Privacy practice** and previously worked at the US Department of Defense and the CIA. "Having the right team in place and having people know each other before they have to go into the cyber foxhole is really important."

Getting it wrong is expensive. The cost of a mega breach can reach more than $300 million, according to estimates from IBM in its 2023 Cost of a Data Breach report. Many companies will fall victim to multiple data breaches, with a separate IBM report showing that 83 percent of 550 global organizations studied had more than one data breach between March 2021 and March 2022.

Figure 1: Cost per Data Breach Rose 23% Since 2017

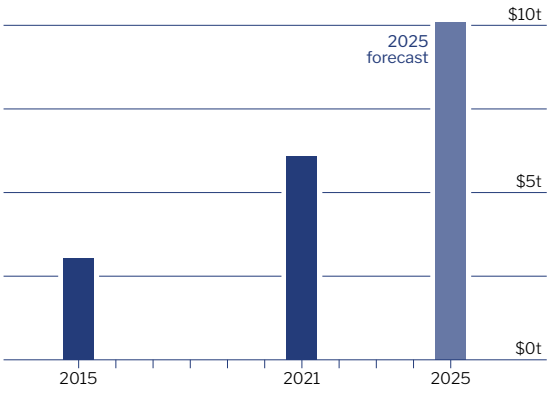
Average total cost of a data breach 2016–2023 in USD millions



Source: Cost of a Data Breach Report 2023, IBM

Figure 2: Global Cybercrime Expected to Soar

Estimated total damage of cybercrime wordwide in USD trillions



Source: Cybercrime Report 2022, Cybersecurity Ventures

"Cybersecurity is a forever problem for corporate executives," says **Mark Seifert**, a Brunswick partner in Washington, DC, who works with the Cybersecurity, Data & Privacy practice and previously held senior corporate and US government roles in telecommunications. "This is a business risk that needs to be constantly monitored."

The companies who do it best challenge themselves by tackling the tough questions and worst-case scenarios with their C-suite regularly and capturing that decision-making process. Those decisions and processes should then be reflected in the materials team members utilize across the entire organization, says **Katharine Crallé**, a New York-based partner with Brunswick's Cybersecurity, Data & Privacy practice who specializes in communications strategy.

"You want your top executives to zero in on the most strategic questions and agree on what would trigger those tough calls now, not in the heat of the moment," Crallé explains. "Anything but the most critical decisions are then delegated to your core crisis response team, who have been practicing regularly and in line with guidance from the top."

Every company should have a crisis management team (CMT) and captain in place at all times. The team should be cross-functional with representation from legal, finance, communications, operations and other key parts of the business. Given the intensity and complexity of many cybersecurity incidents, companies often bring in external advisors to support the response team from a technical, legal and reputational perspective on both planning and response. External advisors – whether they are forensic experts, outside legal counsel or communications firms – need to learn the ins and outs of your business before a real crisis strikes, so they can jump in immediately and operate as an extension of your team.

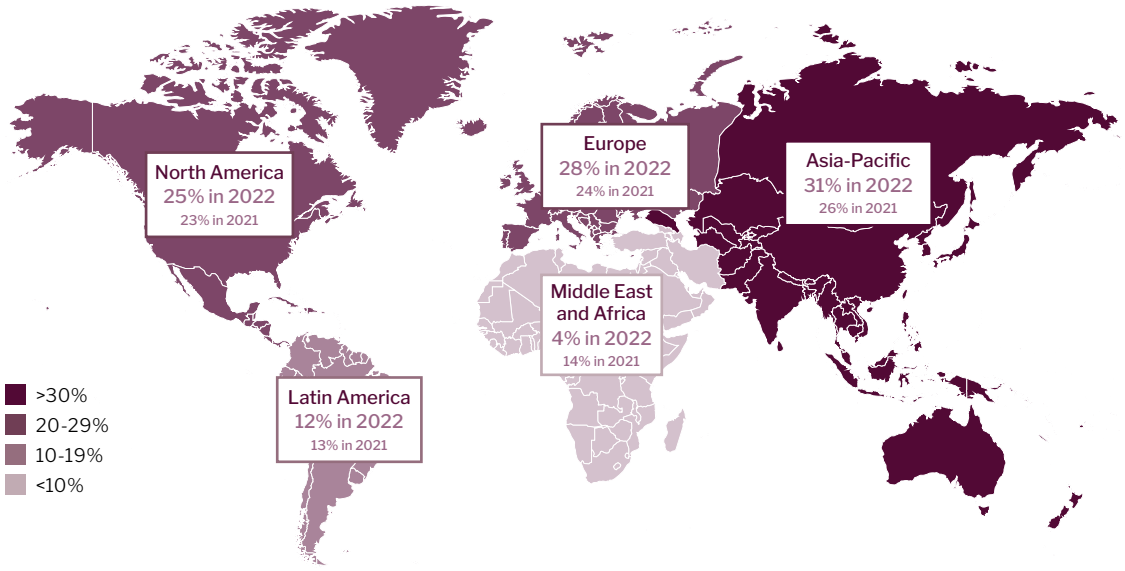
Any business change – such as staffing moves, new product launches or regulatory developments – alters the risk equation and should trigger a reassessment of cybersecurity readiness. It is critical to identify stress points and potential gaps in your cyber crisis plans that emerge as cybercriminals continuously evolve their tactics, says **Nicola Hudson**, a Brunswick partner with the Cybersecurity, Data & Privacy practice in London who previously served on the executive board of the National Cyber Security Centre (NCSC) and as Head of News at No. 10 Downing Street.

These plans should be modeled on the most likely scenarios, with the goal of ensuring processes are in place that will allow for a rapid response and recovery, Hudson says.

It is almost inevitable that every company will face a cyberattack at some point, and a quick and effective response can enhance a company's reputation, says **Admiral Mike Rogers**, USN, Ret., a senior advisor at Brunswick who previously simultaneously led the US Cyber Command and the National Security Agency.

"Cyber can become a differentiator," Rogers says.

Figure 3: Cybercrimes Know No Borders, it is a Global Threat
Incidents* per region 2022 vs. 2021



Source: X-Force Threat Intelligence Index 2023, IBM.
**Share of incident response cases by region to which IBM X-Force responded from 2020–2022*

C-Suite Roles and Responsibilities

Cyber incidents can cascade through your entire organization and affect important stakeholder relationships, including those with customers, investors and regulators.

That's why every member of the C-suite has a role to play when it comes to strengthening your company's cybersecurity posture and resilience. It's not just a matter for chief technology officers and chief information security officers.

A best practice is to make cybersecurity a highly collaborative effort and create multiple layers of defense. For example, human resources has a role to play in terms of employee education and training, and the legal team will step in when it comes to reviewing contracts and approving third-party vendors. When this work is siloed and emerging issues are not escalated to the right parts of the business, cybercriminals are likely to slip through the cracks.

Ultimately, the CEO and the board are responsible for making sure that all teams are working together harmoniously and that there is an overall program in place for mitigating cyber risks to the business.

In general, C-suite members assume the following roles and responsibilities:

CEO

- Leads and participates in regular crisis preparedness exercises with other C-suite members and business leaders across different functions. Reports to the board of directors.
- Makes strategic decisions during a live incident, such as deciding whether to engage with cybercriminals or pay ransom demands, as well as reviewing key communications to employees, customers, partners, investors and other critical audiences.
- In edge cases: Serves as a spokesperson during a live incident if the company is in the cybersecurity industry or if the company is summoned to appear before government authorities, for example.

Finance

- Reviews proposed investments in cybersecurity, including the company's cybersecurity insurance and cybersecurity risk management and preparedness programs.
- Assesses the materiality of a cybersecurity incident in coordination with the legal team and evaluates potential implications for cash flow and financial stability.
- Leads investor engagement during and after an incident, including filing relevant disclosure forms and communicating with investors and analysts.

Technology & Security

- Evaluates and manages cybersecurity risks across the company, escalating critical issues for the attention of the C-suite and board of directors.
- Leads the technical investigation, response and recovery during a live incident. Provides regular updates from the investigation to inform key business decisions and communications.
- Builds resilience by developing and implementing incident response procedures, disaster recovery protocols and business continuity plans.

Legal

- Evaluates cybersecurity risks and ensures compliance with cybersecurity risk management protocols and procedures.
- Reviews and fulfills legal, regulatory and contractual obligations to report cybersecurity incidents, including assessing the materiality of an incident in coordination with finance and other functions.
- Leads crisis management planning and often plays a central role during a live incident, often serving as the crisis captain.

Human Resources

- Ensures employees receive regular cybersecurity training and are familiar with company policies such as incident response plans and social media use.
- Advises on employee-related matters during a live incident, for example, when employee data or payroll processing may be affected.
- Maintains a feedback loop with employees to address questions about the company's cybersecurity risk management and preparedness programs as well as gather feedback during and after a live incident.

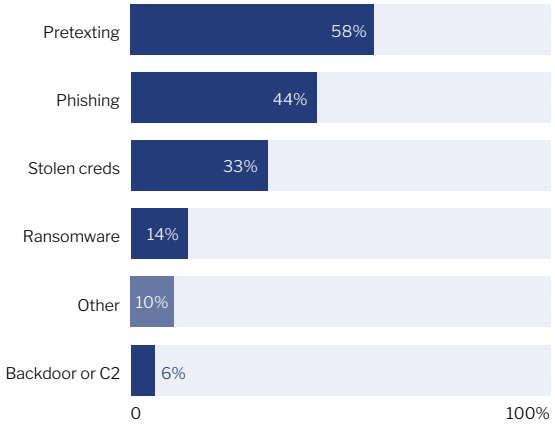
Communications

- Develops a crisis communications framework and drives communications strategy during a live incident. Creates and maintains channels for communication, including backup channels if all or part of corporate systems are affected.
- Coordinates across different business functions such as legal, human resources and finance to ensure the needs of internal and external audiences are reflected in the company's communications.
- Leads media engagement during an incident, including conducting background meetings and sharing statements with reporters, if needed.

Get Your Digital House in Order

Chapter takeaways: It's critical to have a holistic view of your systems, the data you hold and the third parties you interact with. If you experience a cyber incident and it takes months to figure out who and what was affected, your company's reputation will take a hit, and you will lose trust with customers, investors, employees and other critical audiences.

Figure 4: Pretexting Occurred Often in 2022
Action varieties in 1,696 social engineering incidents



Source: Data Breach Investigations Report 2023, Verizon

Cyberattacks often reveal flaws in corporate infrastructure that was built for cost and efficiency but not security. That's why it is essential to have a holistic view of your company's systems and who has access to them.

Companies have been seduced by the efficiency and speed of the online world, and security slows things down, Seifert says, adding that one of the challenges now is getting people to accept the time it takes to maintain security.

"The amount of digital interconnectivity around the world serves as fertilizer for digital crime, allowing it to proliferate at scale," Seifert warns.

Executives need to know exactly how their most sensitive and important data is protected. They need to know what data is in the cloud and what is connected to shared services, and they should understand the interdependencies across their organization's infrastructure to be prepared for a shutdown of one system that is vital to others.

Critically, executives should reassess risks frequently as their businesses change, such as through acquisitions, staff movements or switching suppliers. This requires centralized data management across the entire organization, including subsidiaries, joint ventures and vendors, especially those operating in other countries.

"A problem we often see in companies is that if you ask who's in charge of data, there is no single person who controls all the decisions," Seifert says. "If no one is accountable, people are going to make decisions that don't take in the full range of the risk involved."

Your business can lose weeks or even months of revenue after a breach if you don't have a complete view of your technology infrastructure in advance, Crallé says. "Even if your company's systems are not significantly compromised by an incident, you need to be prepared to explain your potential exposure," she says.

"The time and resources needed to come to an acceptable answer increases exponentially if you don't start with a clear understanding of your systems and how you use information," Crallé says.

Evaluating the access granted down through a company's supply chain needs to be part of every cyber risk assessment, no matter the size of the business: More incidents and confirmed data breaches are reported at small and medium-sized businesses (those with fewer than 1,000 employees) than at larger firms, according to **Verizon's 2023 Data Breach Investigation Report**. Executives should evaluate what data is the most sensitive or significant to their operations and reputation, and consider keeping that data under stricter internal controls, says Rogers.

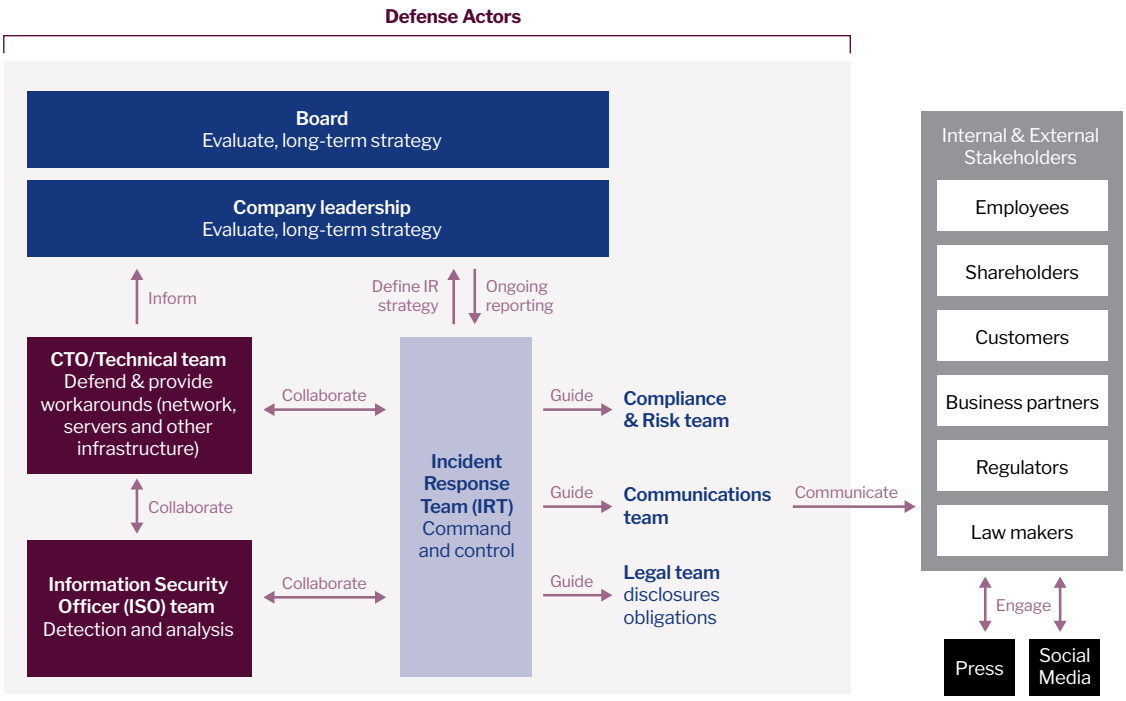
"It is a danger to treat all data the same way," he explains. "If this data is your true competitive advantage, are you really comfortable with it being on an external server?"

For less-sensitive data, the cloud often is the best solution both in terms of cost and security, Rogers says, adding that it is important to carefully assess cloud vendors. The best ones offer a high degree of transparency about the security systems protecting your data and what they'll do if anything is compromised. Even if you are satisfied with your current vendor, Rogers advises, it is a good idea to review the contract language and add specific requirements on security, disclosures and the right to audit how they protect data.

Implementing state-of-the-art security protocols across your technology platforms won't protect you from an attack that gains access to your data through a less-sophisticated supplier that is connected to those systems, says **Yasmin Brooks**, a Brunswick partner in London who works with the Cybersecurity, Data & Privacy practice and also serves on the UK government's National Cyber Advisory Board.

"It's not enough to have your own house in order – if you're trusting anything to a third-party vendor, that's something you need to take seriously," Brooks says.

Figure 5: Company Ecosystem in an Incident

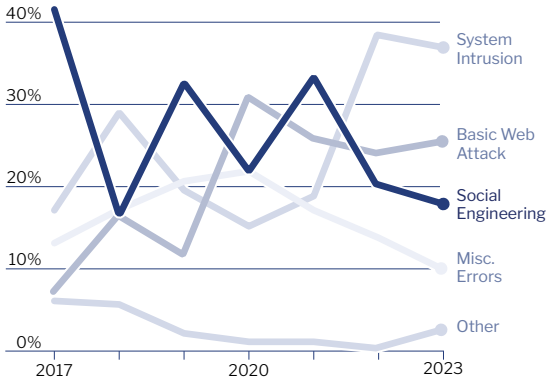


Keep Up With the Criminals

Chapter takeaways: You need to know what's out there and what's coming next – because you will be judged on how well you prepare for and respond to these evolving threats.

Figure 6: Social Engineering's Ups and Downs

Breach incident classification since 2017



Source: Data Breach Investigations Report 2023, Verizon

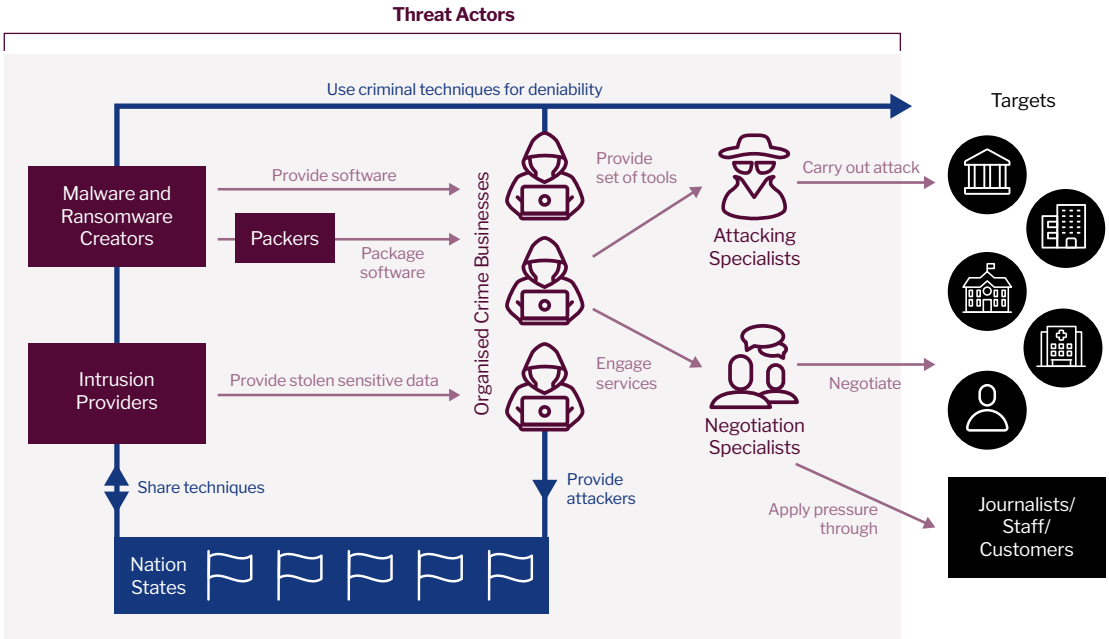
A data breach at a commonly used file transfer service in early 2023 threatened at least a thousand companies and government agencies around the world with a single attack, signaling the evolution of malware into a threat capable of stealing data at a previously unimaginable scale.

The ability of cybercriminals to identify and exploit supply chain vulnerabilities in this way underscores the growing sophistication of a maturing cybercrime industrial complex, supported by state actors and specialized distributors of malware that can quickly adapt to new security tactics implemented by their targets.

While criminals are constantly updating their technology and approach, exploiting human vulnerabilities remains their primary tactic. Over the past decade, stolen credentials have been responsible for most data breaches, according to Verizon's annual Data Breach Investigation Report. The 2023 report found some kind of human involvement in 74% of breaches.

Figure 7: How the Cybercrime Industrial Complex Operates

The level of sophistication, organization and coordination among cybercriminals rivals that of many of the global businesses they attack



"The threat is always there, it's just evolving," says Brooks. "No company is immune, no matter how much they have done in the past to protect their systems."

A good example is "phishing," typically an email trying to trick the recipient into clicking on a malicious link or attachment. The latest twist is "pretexting," a specialized phishing approach that often targets company employees via spoofed corporate email that use a false pretext, such as the boss urgently needing data.

More frequent updates to cyber education programs are needed as phishing gets more elaborate and targeted, says Little, whose experience includes top roles in the national security and defense community as well as the private sector.

Once criminals gain access to company systems, they typically use time-tested ransomware to lock up a company's data and then demand payment for the digital keys.

"Ransomware and extortion are still reigning supreme because it makes a lot of money for criminals," says **Siobhan Gorman**, a Brunswick partner in Washington, DC, who works with the Cybersecurity, Data & Privacy practice and has led a range of cybersecurity, public affairs, litigation and corporate reputation projects in the financial, retail, airline and technology sectors.

Companies will consider paying large sums of money to keep their data from being exposed, Gorman says. The trend among companies is increasingly to pay, at least in part, to minimize damage to their reputations.

Sometimes It Makes Sense to Engage

When cybercriminals infiltrate your company's data, talking to them may be the best option

As counterintuitive as negotiating with criminals may sound, it could be the best way to understand the scope of the threat, says Gorman, who advises executives on crisis management and media relations.

"Executives may need to negotiate in order to learn everything they can about what the criminals think they have," says Gorman. "Sometimes it makes sense to negotiate, and other times it doesn't."

Gorman outlines three key reasons companies can benefit from negotiating:

- Identifying the actors and the technology they used
- Getting details on the data they claim to have breached
- Buying time for crisis management

Trying to negotiate doesn't mean paying them, Gorman emphasizes. You may find out that the people behind the ransomware or extortion aren't interested in talking, or you may buy enough time to get your systems running without needing to pay.

When companies refuse to engage, criminal groups are starting to target the leadership of the firm and their families, says Rogers, adding that this remains a new and relatively infrequent tactic. "If the company doesn't pay, the criminals try to make the executives pay," Rogers says.

One thing to always bear in mind is that you are dealing with criminals. Most of the time, they are "criminal capitalists," and all they want is money. They are good at getting into your system and finding a way to extort you, but they are not always good about fulfilling the terms of the settlement.

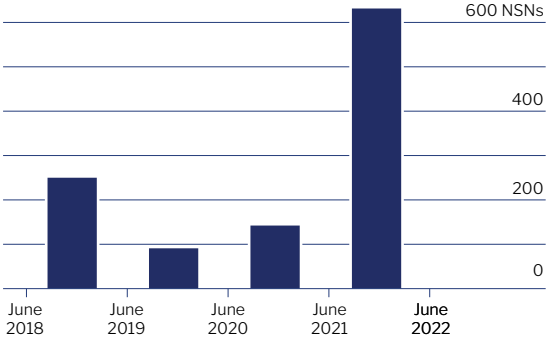
Figure 8: Internal Competence Saves Cash

Average cost of a cloud-based data breach by responsibility in USD millions

Source: Cost of a Data Breach Report 2022, IBM

Figure 9: Critical Infrastructure Under Attack

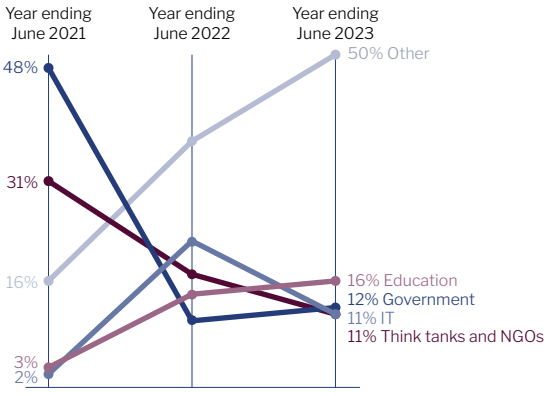
Annual critical infrastructure nation state notifications* by Microsoft



Source: Digital Defense Report 2022, Microsoft
**When Microsoft observes a customer targeted by nation state activities, they deliver a "nation state notification" (NSN) alert.*

Figure 10: Espionage Targets Changing Fast

Share of total incidents by sector as tracked by Microsoft



Source: Digital Defense Report 2021, 2022 and 2023, Microsoft

It can be disruptive for a company's systems to be down for even a few minutes, let alone a few days, Little explains. Ransom payments have been growing along with the increase in large-scale attacks in recent years, he adds.

In some cases, threat actors aren't even bothering to deploy ransomware. Instead, they steal data and threaten to expose it if companies don't pay up, says Gorman. The approach has evolved to operationally impair companies rather than spend the time to figure out which data would command the highest ransom.

"Data is still the goal, they just monetize it in new ways beyond ransomware," Gorman adds.

Criminals are finding more ways to exploit each breach, frequently double-dipping and sometimes triple-dipping, according to Brooks.

Here's how the triple-dip works:

1. Encrypt company data, then demand a ransom for the decryption key.
2. Steal data from the same target, then extort payment to get the data back.
3. Threaten to reveal the breach to high-profile clients unless hush money is paid.

The growing sophistication of the cybercrime industrial complex is further underwritten by adversarial countries that have the means to develop the most advanced technology to infiltrate data and computing systems. Nation-states are collaborating with criminals as they expand beyond espionage into economic destabilization, according to Seifert.

A significant technology transfer is underway as nation-states sell their sophisticated malware and ransomware technology to modern-day digital privateers. The hackers, ever in pursuit of more money, have been reselling the nation-state technology and fueling the globalization of cybercrime.

State actors allow criminals to run short-term data heists for profit so long as they don't interfere with the long-term nation-state objective of collecting intelligence on other governments, the military-industrial complex or other critical industries.

Rogers points out that the espionage work of nefarious nation-states continues to expand as they seek intelligence about the critical infrastructure of rival nations by clandestinely infiltrating the data systems of companies involved with the supply of electricity, water and technology.

More recently, nation-states have targeted academic research at colleges and universities, especially those involved in artificial intelligence, industrial processes, chemical engineering and other areas of economic significance.

Rogers says that puts academia at greater risk for attacks, especially as universities form private companies to capitalize on the intellectual property their research creates. This risk extends to any company that works with universities.

As technology advances, in particular with artificial intelligence, and as bad actors get more sophisticated, the next criminal wave may be data manipulation attacks, Little warns. This new threat will involve criminals corrupting or altering data that remains inside a company's systems and then demanding payment to return the unaltered data.

While noting that data manipulation isn't currently being seen at a significant scale, Little says this threat could potentially be more disruptive than data breaches or operational attacks. Data manipulation could become a tactic used by nation-states to disrupt entire societies, he says.

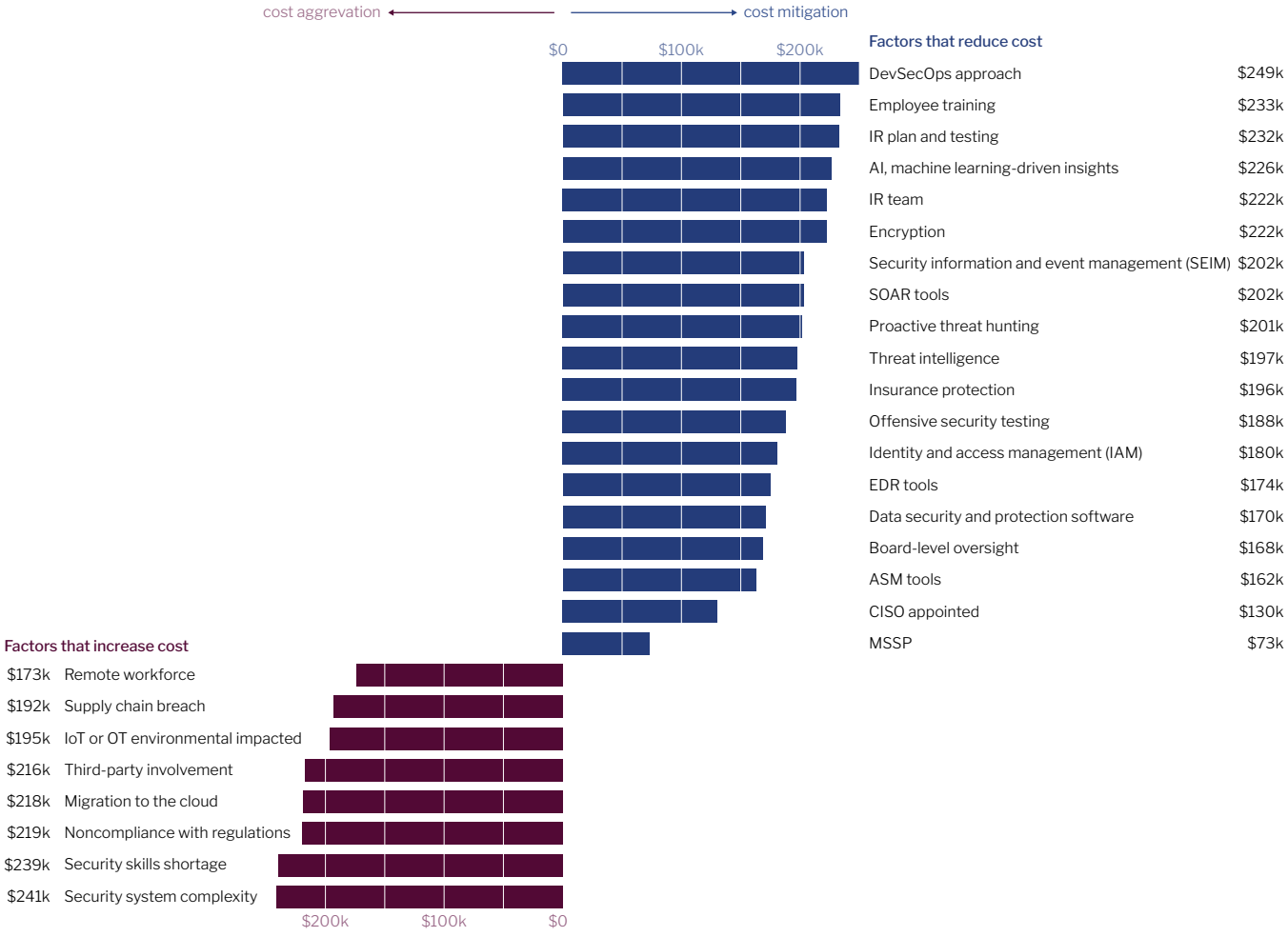
Similarly, generative artificial intelligence, which can be eerily effective at blurring the lines between machine and human communication, may power the next wave of phishing and pretexting.

Cybercriminals are very adaptive, says **Paddy McGuinness**, a senior advisor at Brunswick who previously served as the UK's deputy national security advisor for intelligence, security and resilience. The shift by cybercriminals to extortion tactics is a result of companies getting better at preventing malware attacks. There is a half-life for defensive measures; they will all eventually be outdated.

"Information security work has a Darwinian effect on the attackers," McGuinness says. "As we improve, so they change to be able to still make their money."

Figure 11: Incident Response (IR) Approaches Reduce Damage

Monetary impact of key factors on the average total cost of a data breach in USD thousands



Source: Cost of a Data Breach Report 2023, IBM

The First 72 Hours After a Breach: What to Expect

Chapter Takeaways: What you do in the first hours after a breach is discovered sets the tone for the entire response. Still, a cyber crisis can last for months, and you need to protect your business and your people throughout the investigation and recovery.

The immediate hours after discovering a cyberattack are critical but complex – you are operating under significant uncertainty and with a lack of information yet often expected to communicate quickly and transparently.

Unlike other types of crises, you may not know:

- How long the incident will last **(Longevity)**
- Who is behind it and what they will do next **(Threat Actor)**
- What the full scope and impact are **(Facts)**

The inherent uncertainty in a cyber incident makes it one of the most difficult crises to manage. Most incidents drag on for weeks and it can take months before the forensic investigation concludes. In some cases, the impact is felt for years when companies are tied up in litigation relating to an attack.

How you respond to a cyberattack will depend on the nature of the incident, but there are common stages and key decision points that companies will go through in the first 72 hours.

Hour 0–2

Inevitably, when cybercriminals attack, they will do so on a Friday afternoon or a public holiday when your full crisis management team won't be in place, so make sure deputies have been appointed and have been part of planning and testing exercises. It will be an intense and grueling 72 hours.

In the first few hours of a cyber incident, the technical team will be looking to ascertain the nature of the attack and, importantly, focused on containing it. This is the top priority to mitigate the impact to the business.

Hour 2–6

As part of its investigation, the technical team will gather information about the incident, such as whether data has been exfiltrated, systems disrupted or a ransom note received. This creates an initial understanding of what has happened and will inform your response, including how you classify the incident and which escalation protocol you trigger.

Your CMT should be up and running soon after and external advisors brought onboard, with a clear understanding of roles and responsibilities. At this stage – when little is known and there is the greatest potential for miscommunication – it is key that the team remains small and the work confidential to minimize the risk of leaks.

Hour 6–12

The CMT should be meeting regularly, two or three times a day, to determine the impact and what needs to be done, who should be informed and what workarounds may be needed. In some cases, new communication channels will have to be established if existing ones – like email or phones – were compromised in the attack.

At this point you will start to shape what you say about the incident, based on what you know with certainty about the attack and the steps you are taking to protect the business and your stakeholders.

Hour 12–24

Your legal team will be working against the clock – many regulators require notification of a potential data breach within 72 hours, and some, especially in critical infrastructure sectors, will need to be notified within mere hours of discovering an incident. Legal will be working through which jurisdictions are affected for regulatory purposes and whether to alert law enforcement.

You may also have other legal obligations, such as commercial agreements with suppliers or other third parties that require you to notify them of a cyber incident or even allow them to be involved in the investigation.

Hour 24–36

If the news hasn't leaked by now, you will need to make a decision about whether to proactively announce that you have suffered a cyberattack or whether to take a reactive approach. You need to consider a multitude of factors, but this will be one of the most important decisions you make that will have a long-term impact on your reputation.

Based on your strategy, your communications team will prepare messaging to your staff, customers, clients, shareholders and all other stakeholders – all of which should be aligned with any legal communications and consistent across markets, as well as internally and externally.

The order also matters: You shouldn't be disclosing a lot of detail before you have engaged with the relevant regulators. Balancing what to say when so much will be unknown is always the trickiest part.

Hour 36–48

Once you are through the first few days, your crisis team should be having daily meetings, updates from all work streams and a clear direction.

The technical teams will be working to either restore or rebuild systems, and investigations will continue to determine scale and impact. Operations will be looking at workarounds if the impact on operations is severe.

A cyber crisis is never linear, and you may need to continuously update your scenario planning and communications materials as new findings emerge from the ongoing investigation.

Beyond the First 72 Hours

By day four, your crisis team may be exhausted and struggling to maintain pace. Your technical team will have been working around the clock trying to identify, isolate and contain the incident, beginning what will be a long investigation into what happened. Your legal team will have informed the regulators as required, but this will usually be just the first of many updates. For some companies, this process can take over a year.

While it may feel like things are quieting down, it is usually at this point that matters can take a significantly different turn very quickly; the threat actors may decide to exert pressure on you by dumping troves of data or speaking directly to the media. Be ready with communications to those impacted to explain what happened, if any data was taken, how to stay safe and whether any type of fraud monitoring is available.

Three Months Out

Communications during the first three months post-incident will move through many phases, from the initial realization that there is a problem to addressing what has happened and identifying actions to take.

The most critical thing is consistency of message to all stakeholders and focusing on the facts. Those in your organization who are on the front lines dealing with customers and suppliers will need a script approved by legal and technical teams about what is known to have happened and what they need to do or not do about it. This will need to be continually updated as more information comes to light.

Four to Six Months Out

Finally, you are on your way back to business as usual. You will want to move on. However, this is exactly the time when leadership needs to maintain vigilance.

Companies that have been breached are likely to be targeted by criminals again. Most attacks on businesses still come through a phishing attack, exploiting poor password controls and a sloppy grip of admin rights. There is no better time than after a cyber incident to roll out an internal cybersecurity campaign about how you want staff to be more secure in the workplace.

It is also a good time to do a quick pulse survey for staff to see how they are feeling. They are usually the ones that feel the impact of a cyber incident the most. Many will have been working long hours to help fix the problem and provide workarounds. They may have also been the ones whose data has been stolen.

Once the survey is complete, it is important to put in place new measures to remedy what issues are uncovered and to reflect on the lessons learned from the cyber crisis more broadly. This will help strengthen your cyber resilience and crisis management capabilities going forward.

Written by Nicola Hudson, Brunswick partner with the Cybersecurity, Data & Privacy practice in London.

10 Lessons from 100 Breaches

After assessing more than 100 recent cybersecurity incidents, Brunswick's Global Cybersecurity, Data & Privacy practice group offers the following lessons learned and advice for business leaders.

01 Look at reputational risks across the business

When the incident response process begins, it's critical to step back and look at the entire organization and what's on the horizon. A cybersecurity incident is not just a matter for CISOs and CIOs. Among other things, you'll need to consider the implications for deals and announcements in the pipeline, review planned marketing and advertising activities, and prepare for tough questions during media engagements or events where company executives are speaking.

02 Assemble a team that will facilitate real-time decision-making

Technology and process have a role to play in a successful response strategy, but the best responses maximize the expertise, insights and relationships of your people and partners. Keeping the circle small will streamline decision-making, but it's equally important to stay flexible – pulling in subject-matter experts and leaders from different business units where needed. When you're assembling your team, determine what, if any, additional resources are needed to supplement your in-house capabilities.

03 Get comfortable making decisions with limited information

While you should never speculate or put out information that isn't vetted by your legal team and forensics experts, you will almost always be making decisions with limited information during a cybersecurity incident. Critically, you must not allow this dynamic to stop your team from moving forward. Successful incident response teams commonly schedule regular check-ins to share updates and come to a consensus on business decisions.

04 Use time and threat intelligence to your advantage

During a cybersecurity incident, you're often operating against the clock – be it regulatory requirements, contractual obligations or deadlines set by threat actors. In ransomware situations, working with forensics experts and negotiators makes it possible to learn about the *modus operandi* of cybercriminal groups and engage with them to buy time, regardless of your payment decision.

05 Plan for the worst and play out potential scenarios

We've seen company operations freeze up overnight for weeks or months at a time. Consider merging your cybersecurity and business continuity planning to ensure you have alternative channels for communications and operational workarounds if backup systems aren't adequate. Company executives and board members should also review a range of likely scenarios and possible courses of action in advance, especially when it comes to ransomware and supply chain attacks, which can bring global operations to a standstill.

06 Develop messaging that is clear and authentic to your values

In your communications, use language that reflects your company values and acknowledges the needs of your key stakeholders. Be careful not to overcomplicate the messaging or blame others as it can sow mistrust.

07 Align on the channels and sequencing for communicating with key stakeholders

It's critical to think about not only what you should be communicating but also through which channels and in what order. For instance: Prior to deploying your initial communications, you may need to brief your frontline workers or relationship managers and equip them with materials to handle what comes their way.

08 Consider the full lifecycle of inquiry management

You will likely get an influx of messages from stakeholders after you deploy your initial communications. Make sure you're not only thinking about how information goes out, but also how it comes back in. Set up a procedure to track and address these inquiries quickly and use a consistent approach to maintain trust over time.

09 Prepare for sustained pressure from multiple directions

While the initial incident response may unfold quickly, the investigation and recovery process is generally measured in months, not days. Prepare yourself and your team for the long haul including sustained pressure from well-briefed cyber reporters, regulatory agencies and customers or partners demanding regular updates. Think about how you will need to manage your team and look for opportunities to ease the burden of their usual responsibilities.

10 Own your mistakes and use the opportunity to build a stronger system

Even if you think you have responded to the incident effectively, there will always be areas you can improve upon. In today's cybersecurity landscape, everyone is vulnerable. Invest in increasing your resiliency to future threats.

How Brunswick Can Accelerate Your Response

Brunswick's Cybersecurity, Data & Privacy Practice Group

Brunswick's global Cybersecurity, Data & Privacy practice group advises corporate leaders on effective strategies to prepare for, respond to and lead on cyber challenges and opportunities.

We look at the risk landscape using a 360-degree approach, and our global team's capabilities reflect this focus. We offer three overarching types of support to our clients: 1 Preparedness, 2 Response & Recovery and 3 Leadership.

1 Preparedness

In today's cyber threat landscape, everyone is vulnerable. What sets organizations apart is their ability to withstand major disruptions to normal operations, share information and timely updates with their key audiences, and recover and evolve capabilities to counter future threats. We work with corporate leaders to prepare for cybersecurity incidents and strengthen their overall organizational resilience. Our support includes:

- Risk analysis
- Playbook development and alignment
- Crisis simulations and training
- Education and culture change
- Disinformation resilience planning

2 Response & Recovery

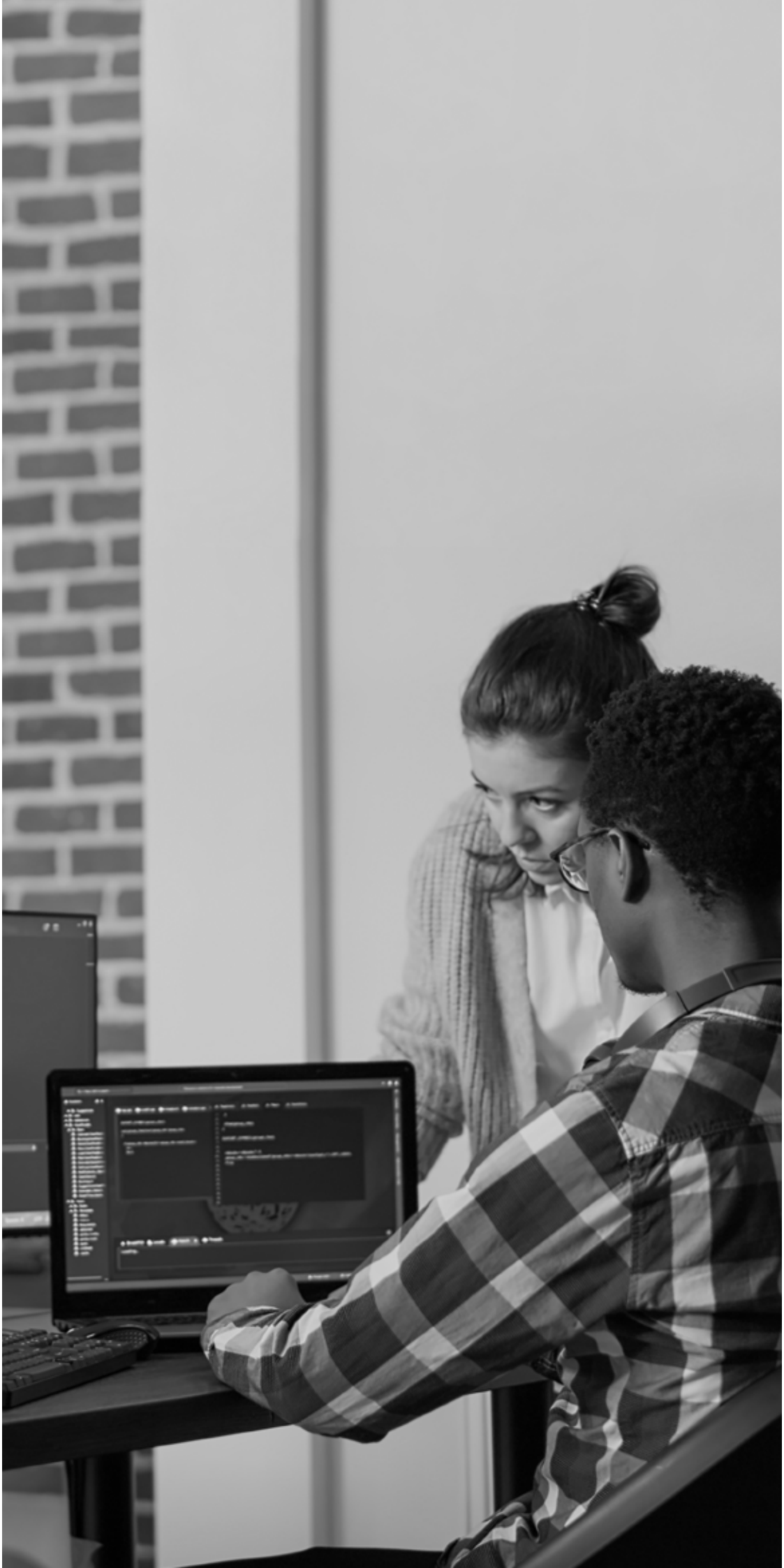
During a cyber incident, we provide ongoing support on all critical issues – from strategy development to stakeholder engagement and media handling. No two incidents are the same, but our breadth of experience allows us to apply best practices to each situation. Our support includes:

- C-suite and Board advice
- Stakeholder mapping and assessment
- Incident response strategy and scenario planning
- Rapid-response campaign generation
- On-the-ground support
- Real-time monitoring and analysis

3 Leadership

In addition to preparing for and responding to cyber incidents, Brunswick helps companies anticipate potential legal and regulatory issues, communicate about their data governance practices and ultimately lead the conversation in their industry. Our support includes:

- Narrative building and platform development
- Leadership positioning
- Public affairs advocacy
- Issues management



Meet the Global Brunswick Cybersecurity, Data & Privacy Team

Yasmin Brooks

Partner, London

Email
Add vCard
+44 207 404 5959

Yasmin specializes in crisis response, resilience and data privacy. She supports clients across multiple sectors and geographies as they navigate a range of cyber risks. Yasmin spent nearly two decades in UK Government where she led on a number of cyber issues, including a national cyber strategy, the formation of the National Cyber Security Centre and a range of data and cyber legislation. She has worked in both Government and industry on some of the most significant cyberattacks that have affected companies across the globe.

Katharine Crallé

Partner, New York

Email
Add vCard
+1 212 333 3810

Katharine has spent more than 15 years advising clients around the world as they navigate crises and significant periods of change. She has specific expertise in cyber security and data privacy matters, and helps clients take a full stakeholder approach in their communications around today's complex security environment. Katharine worked in Brunswick's London, Dubai and Hong Kong offices prior to her return to New York, which has informed the counsel she provides to multinational companies on their most critical issues.

Siobhan Gorman

Partner, Washington, D.C.

Email
Add vCard
+1 202 374 9781

Siobhan has worked on corporate crisis across a range of industries, including financial services, healthcare, defense, entertainment, technology, and automotive. Tapping her longtime journalism experience, she regularly advises clients on media relations issues and conducts media training for executives.

Siobhan is a member of the Senior Advisory Group for Harvard University's Defending Digital Democracy Project and the Advisory Committee for Brown University's Executive Master in Cybersecurity.

Nicola Hudson

Partner, London

Email
Add vCard
+44 20 7404 5959

Nicola is a former Board member of the UK's Government Communications Headquarters and a founding Board Director at the UK's National Cyber Security Centre. She previously managed the UK Prime Minister's press office and was head of the Government Olympic Communications during the 2012 London Olympics. She has extensive experience in strategic and crisis communications across FTSE 100, and government and national security departments.

George Little

Partner, Washington, D.C.

Email
Add vCard
+1 202 393 7337

George brings extensive expertise from the highest levels of the national security and defense community, as well as the private sector. Prior to joining Brunswick, he was head of Marketing and Communications at Booz Allen Hamilton. George served as Assistant to the US Secretary of Defense for Public Affairs and Pentagon Press Secretary, and as Director of Public Affairs and Chief of Media Relations for the US Central Intelligence Agency (CIA). In these roles, he worked closely with counterparts from other governments to address the full range of security challenges facing the US, its allies and partners around the world. George also spent five years at IBM advising corporate and government clients on business and technology strategy.

Paddy McGuinness

Senior Advisor, London

Email
Add vCard
+44 207 404 5959

Paddy McGuinness is a Senior Advisor at Brunswick Group, supporting clients on crisis and resilience and the interplay between geopolitics, national security and their transactions. He works closely with the firm's regional and specialist leads across Technology, Cyber, Litigation, Geopolitical, Activism and Competition and Regulatory Affairs. From 2014 to 2018, Paddy was the UK's Deputy National Security Advisor for Intelligence, Security and Resilience, advising two successive British Prime Ministers on UK Homeland Security policy, capabilities and related legislation. Paddy works with governments advising on their resilience and with private equity on emerging technologies and advises the UK Parliament's Joint Committee on the National Security Strategy.

Mike Rogers

Senior Advisor, Washington, D.C.

Email
Add vCard
+1 202 393 7337

Admiral Rogers joined Brunswick following a 37-year career in the US Navy after rising to the rank of four star admiral, and is a senior advisor to the firm in the areas of cyber security, privacy, geopolitics, technology and intelligence.

He culminated his career with a four-plus-year stint serving simultaneously as commander of the US Cyber Command and director of the National Security Agency – creating the US Department of Defense's then-newest large war fighting organization and leading the US government's largest intelligence organization. In those roles he worked extensively with the leadership of the US government, the DoD, and the US Intelligence community as well as their international counterparts in the conduct of cyber and intelligence activity across the globe.

Mark Seifert

Partner, Washington, D.C.

Email
Add vCard
+1 202 393 7337

A certified privacy professional and a former regulatory attorney, Mark offers insights and practical advice to clients addressing complex privacy issues. Mark has extensive experience within the US government, including 16 years with the Federal Communications Commission as well as service in all three branches of government. Mark also served as counsel to the House Committee on Energy and Commerce on telecommunications and technology matters. He is a board member for the Center for Democracy and Technology.

BRUNSWICK