

REPRINT

CD corporate
disputes

DATA PROTECTION AND CYBER SECURITY LITIGATION

REPRINTED FROM:
CORPORATE DISPUTES MAGAZINE
OCT-DEC 2015 ISSUE



www.corporatedisputesmagazine.com

Visit the website to request
a free copy of the full e-magazine

EPSTEIN
BECKER
GREEN



EDITORIAL PARTNER

www.ebglaw.com

Epstein Becker & Green, P.C.

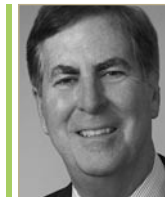
Epstein Becker & Green, P.C., is a national law firm with a primary focus on health care and life sciences; employment, labour, and workforce management; and litigation and business disputes. Founded in 1973 as an industry-focused firm, Epstein Becker Green has decades of experience serving clients in health care, financial services, retail, hospitality, and technology, among other industries, representing entities from startups to Fortune 100 companies. Operating in offices throughout the US and supporting clients in the US and abroad, the firm’s attorneys are committed to uncompromising client service and legal excellence.

KEY CONTACTS



Patricia M. Wagner

Member & Chief Privacy Officer
 Washington, DC, US
 T: +1 (202) 861 4182
 E: pwagner@ebglaw.com



Stuart M. Gerson

Member
 Washington, DC, US
 T: +1 (202) 861 4180
 E: sgerson@ebglaw.com



Adam C. Solander

Member
 Washington, DC, US
 T: +1 (202) 861 1884
 E: asolander@ebglaw.com

EXPERT FORUM

DATA PROTECTION AND CYBER SECURITY LITIGATION



PANEL EXPERTS

**Glen A. Kopp**

Partner
 Bracewell & Giuliani LLP
 T: +1 (212) 508 6123
 E: glen.kopp@bgllp.com

Glen A. Kopp, former Assistant United States Attorney in the Southern District of New York, is a partner in Bracewell & Giuliani's white-collar, internal investigations and regulatory enforcement practice in New York. Prior to joining the firm, he served for five years in the US Department of Justice, handling all phases of the federal criminal process. In private practice and at DOJ, he has handled regulatory enforcement matters, criminal proceedings, litigation and internal investigations relating to financial institutions, corporate, accounting, wire and bank fraud, insider trading, money laundering, options back-dating, securities, export control and other matters.

**Joseph M. Burton**

Partner
 Duane Morris LLP
 T: +1 (415) 957 3014
 E: jmburton@duanemorris.com

Joseph M. Burton is a partner in, and a former managing partner of, the San Francisco Office of Duane Morris LLP. He is a nationally recognised legal expert in the areas of cyber security and cyber fraud. He provides advice concerning all aspects of the prevention, detection, and response to data breach and other cyber fraud incidents; as well as advice regarding compliance with statutory, regulatory, and contractual cyber security and privacy requirements. His practice also involves criminal defence and civil litigation of cyber crime and cyber security matters.

**Patricia M. Wagner**

Member & Chief Privacy Officer
 Epstein Becker & Green, P.C.
 T: +1 (202) 861 4182
 E: pwagner@ebglaw.com

Patricia M. Wagner is a member and chief privacy officer at Epstein Becker & Green, P.C. Ms Wagner's experience includes representing a wide range of health care clients in all aspects of general and more highly nuanced privacy and security issues and concerns. She works with clients to develop practical strategies to help those clients meet state and federal privacy and security requirements, as well as helping clients respond to and evaluate potential security breaches and litigation. Ms Wagner regularly speaks and writes on privacy and security compliance issues. She was selected to the Washington DC Super Lawyers list in the area of healthcare.

**Andrew Moir**

Partner
 Herbert Smith Freehills LLP
 T: +44 (0)20 7466 2773
 E: andrew.moir@hsf.com

Before qualifying as a solicitor, **Andrew Moir** gained hands-on experience in the electronics, IT and software engineering fields, and now specialises in matters which require an understanding of scientific and technical issues. In relation to cyber security and data protection, this has included both advising clients before the event in order to improve their cyber-readiness and resilience, as well as after the event in relation to incident response, including dealing with regulators such as the UK Information Commissioner's Office, managing communications to the affected data subjects, protection of intellectual property, damage limitation and containing the breach.

**Jeremy Batterman**

Associate Director
 Navigant
 T: +1 (303) 437 7227
 E: jeremy.batterman@navigant.com

Jeremy Batterman has been in the cyber security field for over 15 years and has worked on hundreds of information security incident response, theft of trade secret and data forensics matters as well numerous enterprise risk assessments. Mr Batterman advises and educates audit committees, boards, counsel, management and security engineers in business issues pertaining to cyber security. He has earned industry certifications, such as EnCE, GREM, GCFE and has an M.B.A. from the University of Maryland University College. Mr Batterman is a well-known panellist, speaker and educator on cyber-crime, strategy/operations, incident response, cyber intelligence, APT and investigations.

CD: Reflecting on the last 18 months or so, how would you describe recent litigation trends arising from data protection and cyber security issues?

Kopp: As data breaches and the exposure of sensitive consumer information continue to dominate the news cycle, it is clear that companies must seriously examine their own exposure to liability in the unfortunate event of a 'hack' or other cyber intrusion. In the last year and a half, we have seen affected companies, already under extreme pressure to mitigate damage to business operations, become the targets of multiple legal proceedings. Not only are companies now on clear notice that they may expect action by federal and state regulators, consumer class action suits, and shareholder derivative suits brought against directors and officers, but companies must also be prepared to defend against these potentially conflicting proceedings simultaneously. A comprehensive legal approach that includes both pre-and post-breach strategies is essential.

Burton: If it were the weather, I would describe the trend as rainy with a small chance of sunshine. Historically, the vast majority of data breach cases have been dismissed because of the plaintiff's inability to establish legally cognisable harm. While appearing in several forms, the courts' early

reluctance was principally based on the fact that unauthorised access and acquisition of personally identifiable information (PII) does not always result in the misuse of that PII. Plaintiffs have had an extremely difficult time establishing actual use and resultant adverse consequences. Early defences to these suits were based on an asserted failure to state cognisable claims under applicable state laws. Such defences were largely successful. However, recent defences have been premised on attacking plaintiffs lack of standing because of the absence of existing redressable harm. These defences have also been successful, but several courts have been more supportive of these kinds of suit and have developed legal theories which find actionable harm even without evidence of actual identity theft, or other misuse of the PII.

Wagner: The last 18 months have not seen any decline in the number of cases brought arising out of data protection and cyber security issues. Indeed, in the healthcare arena we have seen an increase in these cases, particularly cases seeking class certification. However, there have been a number of positive cases where courts are realising that the plaintiffs bringing such actions have suffered no harm and therefore have no valid claim against the defendant organisation. Similarly, the US federal and state governmental authorities continue to conduct vigorous reviews of such incidents, and in some cases to bring regulatory actions.

Moir: So far, in England & Wales at least, litigation relating to data protection and cyber security has been comparatively rare, partly due to the high cost of UK litigation, and the difficulty in establishing financial loss. The recent case of *Google vs. Vidal-Hall* may lead to a growth of litigation in this area. By contrast, regulatory action, for example taken by the Information Commissioner's Office and the Financial Conduct Authority (FCA), is frequent and on the rise. Some examples of FCA fines for loss of customer data include a £2.275m fine for Zurich UK and a £3.185m fine for HSBC. The ICO levied a £250,000 fine against Sony Computer Entertainment Europe Limited in relation to the PlayStation Network data breach.

Batterman: Looking at compound annual growth rates, year-over-year there has been a sharp increase in the number of class action lawsuits related to these issues being filed. With more regulatory actions being taken and the Attorney General taking a closer look at cyber security issues, the drive to protect people's privacy has now become a kind of lightning rod for litigation. This is a pretty dramatic trend.

CD: How would you characterise the potential risks, liabilities and penalties facing organisations whose cyber security and sensitive data has been compromised?

Moir: There are many different ways in which organisations can incur liability as a result of cyber security incidents. While the risks from litigation and regulatory fines are significant, they are not the only ones. Liability can take various forms. Companies can be left open to blackmail if sensitive information is threatened to be released, or to ransomware if critical information is left inaccessible. Trade secrets or other intellectual property could be compromised by a competitor. Funds could be transferred out directly as happened in, for example, the Citigroup hack in 2011. Also, in the event of customer data being compromised, for example, companies may end up making ex-gratia goodwill payments or offers to its customers in order to mitigate any damage to the customer relationship resulting from the breach. All of these can result in significant losses, but do not necessarily relate to litigation or regulatory issues. Regulatory liability can arise where organisations have failed to comply with applicable data security laws. For example, data protection legislation in the UK allows for the imposition of fines of up to £500,000 on organisations which have failed to comply with the regulatory regime. Liability for cyber security breaches can also be incurred in litigation for breach of statutory obligations, breach of contract, breach of equitable duties and negligence. Directors could also, in theory, be personally liable through breach of directors' duties.

Wagner: Every organisation that holds consumer data, particularly sensitive consumer data, is facing a risk that the data will be compromised. The goal is to be able to manage that risk, through appropriate safeguards, constant assessment of the environment, appropriate policies and procedures and oversight. In that way, in the event a breach does occur, an organisation that is able to demonstrate that it took reasonable and appropriate steps to secure the information it held mitigates the risk of a fine or penalty being issued by a regulatory agency. While private civil litigation may be, at this point, inevitable in any substantial breach, organisations that have response plans in place prior to the breach can mitigate and minimise the likelihood that the breach will cause harm to individuals. While that may not avert litigation being filed, it provides the organisation with strong defences in the litigation.

Batterman: With the emphasis being on the side of regulators and the Attorney General, the risks and penalties facing organisations are increasing. Target recently settled with Visa and paid a very hefty fine, and we are seeing a lot of these types of disputes. This is also taking place in the healthcare arena. In addition, the Federal Trade Commission (FTC) is now increasing its 'branding' and telling consumers that 'the FTC is on their side'.

In the same breath, the FTC is giving corporations fair warning that they are going to start coming after them.

Burton: There are three primary areas where a business must be prepared to deal with the consequences of a data compromise. First, any business will have to contend with the costs of remediation. This involves fully discovering, containing and eradicating the threat; and future-

"While the risks from litigation and regulatory fines are significant, they are not the only ones. Liability can take various forms."

*Andrew Moir,
Herbert Smith Freehills LLP*

proofing your data and systems from future similar attacks. This can be expensive. If you work in a regulated industry, such as finance or healthcare, you face the virtual certainty of investigation and likely imposition of penalties from increasingly aggressive agencies. Even if you don't work in a specifically regulated industry, the FTC in particular, and state Attorneys General have shown an increasing and

expanding interest in pursuing businesses. The third area of concern is addressing potential damage to your company's brand and reputation. The Sony Pictures, Ashley-Madison, and Target cases demonstrate the dangers here. Of least consequence is the threat of civil litigation. The fact is that most cases of this kind are dismissed, some have settled and none have gone to verdict.

Kopp: There are numerous avenues of litigation that these companies may face. First, they may be exposed to civil suits by the consumers who have had their information exposed. While the available common law causes of action will depend on the facts of the case, negligence and breach of contract claims are common. These plaintiffs can also attempt to avail themselves of a number of federal statutes, such as the Stored Communications Act, the Wiretap Act and the Fair Credit Reporting Act. Companies should also be prepared to deal with investigations by governmental agencies, such as the FTC, the Federal Communications Commission and the Securities and Exchange Commission. Additionally, another line of litigation may come from a company's shareholders, such as a breach of fiduciary duty claim premised on the company's lack of security measures or on the way the aftermath of the breach was handled. Finally, while criminal charges are

unlikely, the possibility should not be ruled out in particularly egregious cases. The scope of penalties a company will face is fact-specific and also somewhat unclear since many cyber breach cases

"While the available common law causes of action will depend on the facts of the case, negligence and breach of contract claims are common."

*Glen A. Kopp,
Bracewell & Giuliani LLP*

have not yet been resolved. Such penalties can range from compensatory damages to an injunction requiring the company to implement certain security measures.

CD: Have any class action lawsuits and civil litigation cases involving cyber breach and data loss gained your attention recently? Could you outline the key points we can draw from the outcome of such cases?

Batterman: One case that we have followed was the litigation resulting from the Sony breach.

Not only did the attackers steal sensitive data, but they also used the attack for political reasons. In the end, the organisation was brought to its knees but continued to incur additional jabs by way of the attacker publishing internal executive emails and releasing sensitive employee information. While the judge tossed out many of the plaintiffs' claims, the claim that Sony failed to protect the former employees' sensitive information survived. The claim for damages focused on the fact that former employees' information was being used to send threatening emails to the company and others; furthermore, some employees were implicated by the press as being the one's responsible for the attack. In addition, they cited that all of their HR records and PII were publicly released to sites such as Wikileaks. There should be a few key takeaways from cases such as these. First of all, the former employees were able to convince the judge that the release of their PII caused them direct or impending harm. Secondly, although Sony is an entertainment company, there is still an expectation that the company would protect the sensitive data of its employees and customers. Finally, although the attack was considered to be government sponsored and most companies would not be able to properly defend against this type of targeted advanced threat, the judge still allowed for the claim regarding the former employees' sensitive information exposure and just recently, Sony announced it is settling this claim.

Kopp: One notable case is a recent decision in which the Seventh Circuit held that a data breach case may proceed based on the 'substantial risk' of future injury. This decision lowers the bar for plaintiffs trying to allege damages in any kind of cyber breach case, and could play a particularly interesting role in lawsuits like the ones filed against the parent company of Ashley Madison, Avid Life Media, where plaintiffs may try to highlight potential personal harms, such as a divorce or the loss of a job. In Delaware, after unsuccessful shareholder derivative lawsuits filed in the wake of the Target and Wyndham breaches, a shareholder recently brought a Section 220 action to inspect the books and records of Home Depot following that company's data breach. In the right circumstances, a shareholder Section 220 action could even force a company to make public privileged communications between its officers and its counsel regarding preparation for, and responses to, a data breach.

Burton: The most important data breach case has to be the recently decided Neiman Marcus appeal. This is one of a small handful of breach cases decided by a federal appellate court. Relying on recent case law in the unrelated area of national security, the court found that in the context of a data breach there is a reasonable likelihood that future injury will occur and as such the plaintiffs had the substantial risk of harm necessary for standing. If other courts follow this reasoning it will be much

more difficult to dispose of these lawsuits short of trial. Secondly, the recent federal appeals court opinion in the Wyndham Hotels litigation strongly supports the FTC's asserted and increasingly expansive authority to police the data security practices of businesses in general. Perhaps more importantly, the opinion points to a heretofore non-existent formulation of the minimum standard of care owed to customers by businesses handling their sensitive information.

Wagner: There are two lines of cases that are drawing attention. The first are the cases that are arising out of actions being brought by the FTC against companies that have experienced a cyber security incident. These cases are important, as they are providing the framework for the FTC's jurisdiction over such matters. That legal framework could have important implications. The second line of cases includes the class actions that are being filed that include the organisation's chief information officer or chief information security officer as a named defendant. The impact of this second line of cases, should the trend continue, will reach beyond any particular litigation. Even when indemnified for such actions, individuals may be reluctant to take on the role as a security officer or information officer. Similarly, individuals may be reluctant to work at organisations that are building, but don't yet have a robust security culture.

Moir: Class action lawsuits are not a feature of English litigation. There are group litigation orders, which have some similarities, but these are rarely made in comparison to class action lawsuits in the US. Part of the reason for the lack of cyber related litigation in the UK to date is that the courts have traditionally required some form of tangible loss on the part of the claimant. For example, as drafted, the Data Protection Act 1998 in the UK gives an individual the right to compensation for distress occasioned by contraventions of the Act, but only if they have additionally suffered 'damage', which has been interpreted to mean pecuniary loss. However, the recent case of *Google vs. Vidal-Hall* threatens to change this. A number of claimants sought damages for distress, despite being unable to demonstrate financial loss. The Court of Appeal found that this bar to a successful claim was incompatible with European law, thus allowing the claim. Google has received permission to appeal to the Supreme Court. However, if the judgment stands it will make it significantly easier to claim damages for cyber breaches, such as where usernames and passwords are compromised, even though financial loss has not necessarily been suffered.

CD: In your opinion, what factors should parties consider when assessing potential damages related to cyber related litigation?

Wagner: In terms of damages related to the plaintiffs in the litigation, there should be actual demonstrated harm. Theoretical or potential for harm is not sufficient. However, as organisations evaluate the costs of cyber related litigation, in addition to damages, should there be any, and costs of litigation, organisations should be aware of the reputational cost to the organisation. On the other hand, those costs may ultimately be less than the costs that might be incurred for settling such litigation, as settlement could send a message that is counterproductive to the organisation's strong security posture.

Moir: Broadly, the starting point in the UK when assessing damages is to put the aggrieved party back into the position they would have been had the breach not occurred, subject to ensuring that the damage is a result of the breach and is not too remote. It is quite possible to see in this context how a claim for damages could arise if, for example, a bank was hacked and an individual's savings were lost as a result. A claimant would, of course, still have to show the bank had done something wrong – for example, through negligence, breach of contract and so on. Damages under DPA for contraventions of the Act itself so far have been quite low. For example, the damages were just £751 in *Halliday vs. Creation Consumer Finance Ltd* and £2250 in *AB vs. Ministry*

of Justice. The opt-in nature of group litigation in the UK discourages large classes of claimants from coming together, which also reduces the scope of liability.


Kopp: In assessing potential damages in cyber security litigation, the nature of the company's business and the sensitivity of the information at issue are significant factors. Certain industries face

“In terms of damages related to the plaintiffs in the litigation, there should be actual demonstrated harm. Theoretical or potential for harm is not sufficient.”

*Patricia M. Wagner,
Epstein Becker & Green, P.C.*

higher potential damages in cyber security litigation. For example, across all industries, after a breach occurs, the average cost per record lost or stolen is \$154, but certain high-risk industries, such as the healthcare industry, have valuable private consumer information. In the healthcare industry, lost or stolen records result in \$363 in damages, over double the all-sector average. These costs include legal fees incurred in the resulting lawsuits. The scale of





the suit is also important in determining potential damages, as evidenced by the rise of class action law suits in cyber security and data privacy cases. In the absence of easily demonstrated monetary damages, class action plaintiffs have begun to allege statutory damages under the Stored Communication Act, the Electronic Communication and Privacy Act, and the Computer Fraud and Abuse Act. In one case upheld by the Seventh Circuit Court of Appeals, the district court, in certifying a class alleging the improper sale of consumer data to third parties, noted that the lack of known damages was not relevant because statutory damages are allowed under the ECPA and SCA claims. As a result, the defendants faced the largest class ever certified in an internet privacy suit, and ultimately settled the case for \$14m.

Batterman: When considering potential damages, you have to look at the situation holistically from the company's perspective. If a company has suffered a cyber attack – for example, a breach where an attacker was able to steal sensitive data – how extensive was the damage? What was the associated business loss? Was it related to a cyber attack, or something else? Taking this holistic approach is very important as there are forensics costs associated with the event, regulatory considerations, and so on.

Burton: There are four factors that must be thoroughly considered and understood by the

parties and their counsel: actuality, causation, redressability and proportionality. The first three are the constitutionally required elements for standing to sue discussed in the Neiman Marcus decision and elsewhere. The fourth is an often overlooked consideration. Actuality asks whether or not the allegedly injured party has in fact been harmed. It is closely related to redressability. Causation asks if the defendant's actions brought about the complained of injury. This factor is little discussed because of the difficulties plaintiffs have had in first establishing actuality. Proportionality asks what's at stake and what it will cost to obtain it. It balances the actual or reasonably anticipated costs of the litigation against the redressable harm. If the redressable damages do not significantly exceed the costs to attain them, then perhaps a different course of action, however distasteful, is appropriate.

CD: What impact is the recent legislative and regulatory response – such as the National Institute for Standards and Technology's (NIST) cyber security framework – likely to have on the data protection landscape? What are the specific implications for companies, as far as avoiding litigation is concerned?

Burton: Legislative progress regarding cyber security in the United States has been shamefully deficient. For over two years a hodge-podge of

conflicting and often confusing bills in various houses of Congress have failed to progress to a final vote in both houses. Moreover, even if passed, the proposed bills will have little or no impact on present or future security litigation. The regulatory agencies have done much better through the promulgation of a number of comprehensive guidelines, such as the NIST Framework and the Presidential Directive, and specific worthwhile agency regulations, including the FFIEC, SEC and OCC. However, the proliferation of all of these regulations, and the ever changing state measures make up an ever growing 'jungle gym' of requirements which the average business executive and consumer must attempt to traverse in order to achieve 'compliance', albeit not necessarily better security. All of this activity, or lack of it, has had and will continue to have little or no impact on security litigation.

Batterman: From an information governance perspective, the NIST framework is a good reference point for companies, but it is not a 'one size fits all' framework. Just because you have a NIST policy in place doesn't mean you are going to be able to avoid a cyber attack. If a company has some sort of framework in place, and there are all different types out there, such as NIST, ISO, COIT, Kill Chain or the OCTAVE model, they will be in a better position. As attack vectors change, updating the framework is key. A company should not think 'we have a framework in place' and just let it sit on the shelf.

Constant vigilance is needed. A framework is just a structure to help organise and call out areas that need to be addressed. However, it always comes down to people, technology and process. The most important being the right people. In our experience, many companies have expressed confusion over the NIST standards. They are asking ‘How do we implement it?’ and ‘Does it fit our business model?’ This is a disconnect we are seeing with respect to the NIST framework in particular. It is important to remember that frameworks are really just a small piece of an overall strategy. Adopting and implementing a framework will help a company secure its networks but if the organisation is breached it won’t help prove the company did everything it could to secure sensitive information.

Moir: In the UK and EU, there are two major regulatory developments on the horizon which will have a significant impact on organisations with respect to data protection and cyber security. The proposed new General Data Protection Regulation in Europe includes a mandatory obligation for organisations across all sectors to inform their relevant data protection authority of any security breaches, including the facts surrounding the breach, its effects and any remedial actions taken by the organisation. Under the current regime, there is a system of self-reporting of data protection breaches, with no formal obligation to inform the regulator. The Regulation also could increase the maximum fine

for failing to comply with applicable data security laws to 100m or 5 percent of annual global turnover, whichever is the greater. The EU is also proposing a new Directive on Network and Information Security – otherwise known as the Cyber Security Directive – which would include a requirement for ‘market operators’, such as banks, utility companies and so on, to adopt ‘appropriate and proportionate’ measures to manage cyber risks, and to notify incidents affecting continuity of services. It also proposes ‘effective, proportionate and dissuasive’ sanctions for failure to comply.

Kopp: Though participation in the NIST Framework is voluntary, it does provide a useful benchmark for companies to determine whether their cyber security programs are considered best practices or up to industry standards. Therefore, while non-compliance with the NIST Framework can subject a company to a higher risk of a cyber security breach, potential plaintiffs may also argue that the company breached the applicable standard of care by not following such standards. Other regulatory regimes will continue to provide much needed guidance to organisations looking to meet best practices, and potentially serve as roadmaps for plaintiffs arguing that companies – or their management – failed to sufficiently protect personal identifiable information. On the other hand, compliance with regulatory frameworks allows companies that have suffered a breach to argue that they met standards

of reasonableness in their efforts to guard against cyber attacks.

Wagner: It would be most helpful to organisations if meeting certain standards, such as those set out by NIST, would be deemed to be prima facie evidence of a robust security program, and therefore an affirmative defence that could be utilised more effectively in litigation. The standards would have to be attainable by a broad cross-section of industry, both large and small. Of course, even if such standards are met, there can never be a guarantee that a breach will not occur, although it may make the organisation less of a target.

CD: How do you expect the data protection and cyber security litigation landscape to develop over the next 12 months? Are we likely to see a continued escalation of disputes in this area, and increasing risk for companies?

Moir: Given the increasing focus on cyber security and data protection issues in recent years – not to mention the increasing prevalence of cyber-attacks themselves – it seems inevitable that there will be an accompanying escalation of disputes in this area. Whilst most of the litigation we have seen to date has taken place in the US, it is perhaps only a matter of time before we see a significant test case in the

UK where a cyber security breach has resulted in tangible losses for large numbers of individuals.

Kopp: More robust data privacy legislation, and the growth of novel enforcement strategies, may lead to a significant uptick in government cases against companies that have exposed their customers' data to a security breach. Agencies like the Food and Drug Administration, the Securities and Exchange Commission, and the Department of Energy have issued guidance on cyber security procedures and a recent federal appellate court decision confirmed the FTC's jurisdiction to pursue unfair trade practices claims against a company that did not provide adequate safeguards over its customers' data. In addition to federal agencies, state attorneys general have developed novel enforcement theories just as state legislatures are considering new and enhanced laws governing the cyber realm. Together, these efforts all forecast a greater level of litigation and enforcement over the next 12 months aimed at companies that have not done enough to prevent data breaches.

Batterman: We are expecting to see the amount of litigation increase, which generally results in increased risk for all organisations. We are already seeing numerous class action lawsuits being filed, but many have been thrown out. From a judicial perspective, you need a valid argument that asks 'What are my damages?' Can you quantify what

those are? A recent example is the Ashley Madison attack. There are potentially a lot of people doing things that their partners didn't know about, so we could see an uptick in litigation associated with that fallout. This is one business industry that was infiltrated and sensitive information was exposed.

Wagner: I would anticipate that data protection and cyber security litigation will continue to grow over the next 12 months, as the current cases continue to work through the judicial framework. As a result, the threat of litigation will continue to pose a risk for companies that hold consumer data. Companies should continue to implement processes to decrease the risk of a breach occurring – while having a robust incident response plan in place in order to be able to respond quickly and effectively in the event a breach occurs.

Burton: We are already seeing a significant shortening of the time within which breach lawsuits are being filed after they are first reported or otherwise become publicly known. This is occurring despite a continuing inability to adequately plead or prove the requisite damages. With few exceptions data security litigation has concerned breaches involving unauthorised access to PII usually in the form of credit card or other financially important information. There has been

very little litigation involving different kinds of data security incidents such as ransomware, destruction of data, denial of service and indiscriminate release of confidential information. Given the continuing difficulties in establishing PII related harm, these other forms of cyber attack may begin to attract the attention of plaintiffs. Also the coming proliferation of 'intelligent devices' such as lights, doors, refrigerators, TVs and cars brings with it a

“We are already seeing a significant shortening of the time within which breach lawsuits are being filed after they are first reported or otherwise become publicly known.”

*Joseph M. Burton,
Duane Morris LLP*

demonstrated likelihood of malfunction and the certainty of product liability litigation. We should expect to see several early and perhaps primitive steps in this regard over the next year.

CD: What final piece of advice would you offer to companies, in terms of establishing effective policies and

procedures to protect their data and mitigate cyber related litigation?

Wagner: An organisation should focus on ensuring that it has a robust privacy and security program in place. A robust program would include policies and procedures that dictate the acquisition, use and securing of consumer information. In addition, a robust program would have a response team and action plan in place, before a breach occurs. In developing that response action plan, organisations should review the limits and requirements of their current cyber security policies. In addition, the organisation should consider whether there are preferred vendors that the organisation would prefer to utilise in a breach event. If so, the organisation may want to work with those preferred vendors to have contracts in place prior to the breach, or alternatively the organisation may want to work with its insurance carrier to ensure that preferred vendors can be utilised in the event of a breach. When a breach occurs, it is better if the organisation can focus its efforts on immediate remediation, rather than having to negotiate contracts or wait on approval of vendors.

Burton: Currently, most data security litigation is premised and dependent upon there having been an unauthorised access to or use of sensitive data. Protection of the data itself significantly reduces or completely eliminates the risk of litigation. If the data cannot be accessed, changed or used, there is no litigation injury. It's that simple. The best and the most effective means of protecting sensitive

“Having effective policies and procedures in place all starts with the tone from the top. Once the philosophy is established by the organisation, you then look at the people, the processes and the technology.”

*Jeremy Batterman,
Navigant*

information is to encrypt it. While there are various forms and means of encrypting data to evaluate and choose from, what is imperative is that every business must have a data security policy which mandates the establishment and implementation of technical solutions and administrative processes for the encryption of sensitive data within the businesses custody or control, and whether the data is in motion or at rest. It is that simple. Anything less amounts to a roll of the dice in the litigation game.

Moir: In today's modern environment where every single organisation is reliant to a greater or lesser extent upon technology and telecommunications, it is not a case of 'if' a cyber security breach occurs, but rather a case of 'when'. Organisations need to put data protection and cyber security issues on the board agenda sooner rather than later, and before a cyber breach occurs rather than as a result of one. Then they can take steps to prepare themselves by assessing the specific risks and impacts to the business of a cyber attack, devising a cyber risk management strategy and embedding cyber risk management within the organisation at every level. Cyber security is not just an 'IT issue'; it is also a people and processes issue, requiring companies to embrace education and awareness of cyber issues among their workforce.

Kopp: Cyber security protections are best viewed as part of a company-wide risk management plan, rather than as a narrow IT best practice. In the same spirit of embracing cyber security procedures as a business imperative, companies should identify best-practices and then follow through with executing those procedures. In a recent government action against a company for inadequate cyber security safeguards, the government noted that the company advertised its use of sophisticated data protection measures but the company had not, in fact, implemented those procedures. Lapses like that one – and even less serious oversights

– can expose individual officers and employees to personal liability in government investigations, class action lawsuits, and shareholder derivative actions. Developing a robust cyber security plan and then fully implementing that plan can help a company avoid data breaches in the first instance and mitigate the effects of a breach when one occurs.

Batterman: Having effective policies and procedures in place all starts with the tone from the top. Once the philosophy is established by the organisation, you then look at the people, the processes and the technology. What we have seen out in the marketplace is that if companies don't have the philosophy and leadership on the issue correct, everything else falls short. The second macro point is that some CEOs are still in denial that they are a cyber target. They say things like, 'My company doesn't store high value information like credit cards or Social Security numbers,' or 'We are not processing people's personally identifiable information', or 'We are a manufacturing company, so why would we be a target?' This is not the mindset to adopt. From an information security perspective, think about all the other things that a malicious individual could do with a foothold in your network. They could shut down your plant or hold vital information hostage. If you are conducting an M&A deal, they could potentially be reading emails, transferring information related to different vendors, siphoning bank information, or blackmailing

employees. There is a whole cadre of threat vectors, outside of intellectual property and PII, which, unfortunately, a lot of executives fail to consider. In a recent example, a CEO received a message which said 'Pay us X amount of dollars or we are going to release all of the data regarding your organisation'. That potential data consisted of intellectual property such as design schematics. The hacker did not

go after the PII; they went after the organisation's 'secret sauce'. Other companies have been used as malware farms, or as launching points for attacks on a third-party organisation. In response, companies need to set the philosophy at the top, ensure they have adequate risk coverage, and understand how to mitigate those risks. If companies do that, they will be in a better position. 