November 30, 2017

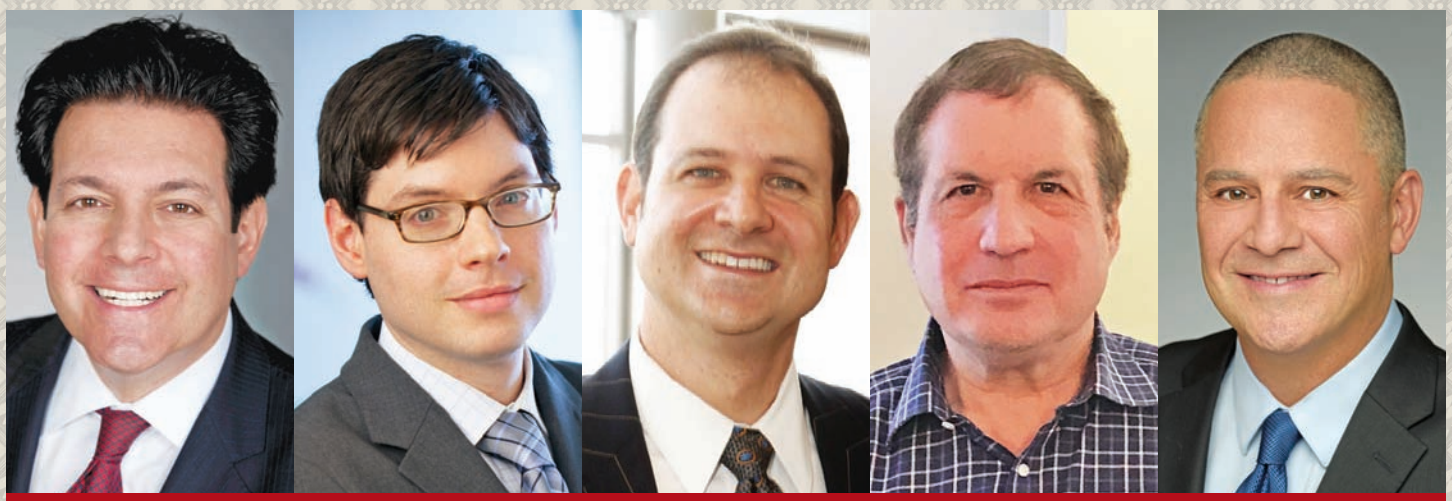
Daily Journal • California LAWYER

Roundtable Series

ADVERTISING SUPPLEMENT TO THE LOS ANGELES AND SAN FRANCISCO DAILY JOURNALS

Cybersecurity

Experts weigh on this year's top data security trends



IAN BALLON
Greenberg Traurig

JONATHAN BLAVIN
Munger, Tolles & Olson

SERGEANT JUSTIN FEFFER
Los Angeles County District Attorney's Office

PETER SELVIN
TroyGould PC

DAVE WATTS
NetFusion

Discussion includes an update on cyber threats, security breach litigation, risk mitigation, and cyber insurance.

"It takes a lifetime to build your reputation. Don't lose it in a second to a data breach."

Your business is at risk.
Call NetFusion today to schedule a complimentary risk assessment.

323.606.7608

NETFUSION

Cybersecurity

Cybersecurity practice is evolving rapidly to keep up with an increasingly sophisticated cyber threat environment. Practitioners are advising clients on emerging threats and litigation over data breaches, on how to improve and implement cyber risk mitigation policies, and on how to navigate the robust cyber insurance market. Meanwhile, statutes and precedents surrounding data security are mounting in jurisdictions across the country, putting conflicting pressures on businesses and their attorneys.

California Lawyer moderated a conversation on these and related issues among Ian Ballon of Greenberg Traurig, Jonathan Blavin of Munger, Tolles & Olson, Sergeant Justin Feffer of the Los Angeles County District Attorney's Office, Peter Selvin of TroyGould, and Dave Watts of NetFusion.

Participants

IAN BALLON
Greenberg Traurig

JONATHAN BLAVIN
Munger, Tolles & Olson LLP

SERGEANT JUSTIN FEFFER
Los Angeles County
District Attorney's Office

PETER SELVIN
TroyGould PC

DAVE WATTS
NetFusion

Moderated by
CALLAWYER.COM

DISCUSSION

MODERATOR: What are the most common cyber threats and techniques you are seeing currently?

JUSTIN FEFFER: The main threat and attack we see are password-oriented attacks—phishing attacks attempting to steal credentials, the use of stolen credentials to log into accounts and further compromise information. And, in fact, we have some very good information from Verizon's 2017 Data Breach Investigations Report, which has good statistics about cybercrimes and trends. 81 percent of the attacks documented in the report involved password attacks in one way or another. Business e-mail compromise is also a huge attack vector, and it's very significant in terms of dollar amount losses—billions of dollars are lost per year to business e-mail compromise attacks. Malware remains a very big problem in the cyber threat arena. And, in particular, ransomware has emerged as one of the dominant forms of malware that suspects are using to monetize the distribution of malware.

DAVE WATTS: To echo what Justin [Feffer] was talking about, I'm seeing a rise in the sophistication and specialization of threats. For example, there are new, advanced, and targeted ransomware threats. First, the cybercriminals perform sophisticated reconnaissance. They will use social engineering to identify which users have the highest-level access at a particular company—such as an administrator or a top executive. They spearfish that person, compromise their machine to gain network access, and then operate with that person's permissions to get in to the systems and data they are targeting. This allows the cybercriminals to find the highest value data or critical business systems on the network so you will pay the highest ransom. And before they start encrypting, they disable or obfuscate backup settings and alerts

IAN BALLON defends data privacy, security breach, and TCPA class action suits. He authored the four-volume legal treatise, *E-Commerce and Internet Law: Treatise with Forms 2d edition* (West), and books on security breach notification laws and the CAN-SPAM Act. A Chambers-recognized lawyer, Mr. Ballon was recognized by *The Daily Journal* both as one of the Top 75 IP litigators in California (2009 through 2017) and as one of the Top 100 lawyers in California.

Ballon@gtlaw.com

gtlaw.com

so you think you're getting good backups when you're not. These criminals are not looking for $300 or $400. This year, a South Korean web hosting company, Nayana, paid a $1 million ransom to decrypt 153 web servers and 3,400 business websites. This was a well-planned, sophisticated attack that paid off for the cybercriminals.

PETER SELVIN: My focus is on insurance, so I'm going to talk about some of the cyber insurance aspects of it. From my own reading, ransomware attacks are on a very steep trajectory upward. So companies who are shopping for cyber insurance need to make sure that that coverage is part of the package that they're buying. There are conditions that trigger coverage, but ransomware is a covered risk now, and that's important.

Another interesting problem for civil lawyers is when companies get what are called spoofing e-mails—e-mails that have been engineered to look unbelievably authentic, but they're frauds.

FEFFER: Business e-mail compromise—the label we attach to that type of attack vector—is unbelievably successful.

WATTS: From an insurance perspective, they haven't technically been hacked.

SELVIN: Exactly. *Medidata Solutions v. Federal Insurance*, 2017 WL 3268529 (S.D.N.Y. July 21, 2017), which is now on appeal, addressed that very point, which is that the impersonation of a client or a customer is not necessarily use or manipulation of the computer. The issue was whether this type of attack fits within the coverage requirement of use or manipulation. *Medidata* says yes, because of manipulation of the "from" and "to" fields. There's a more recent case that goes the other way. So, the issue is open.

JONATHAN BLAVIN: A trend that I'm seeing are intrusions directed not at our client, but at their vendors. Someone is in the system observing the relationship between the parties to understand past practices and courses of business, and then, you see a spoofed e-mail address sent to the vendors who think it's from the client. Unfortunately, it's a successful way that accounts are compromised, particularly with vendors that may not have defenses as sophisticated as a larger corporation may have.

I've also seen a recent trend of botnet attacks, which control a distributed network of computers through software. It's distributed across potentially thousands or tens of thousands of machines. Usually, an individual has no idea that the software is even running on his or her computer. Figuring out the source of the attack can be very difficult. Usually, through civil discovery, you can serve subpoenas, and try to go to the ISPs, but it's very difficult to trace it back to the original bad actor, which makes it hard from both a criminal perspective but, also, in civil litigation, if you want to go after the person, to try to figure out who your defendant is. In the cases that we've handled, we've, at times, brought Doe actions, and then, we've subsequently served subpoenas and sought early discovery to try to figure out, ultimately, who the bad actor is.

WATTS: In botnet attacks, the attacking machines are usually infected for quite a while before they are activated. So, it's an advanced, persistent threat which means it goes undetected for a long period of time. I'm seeing more of these affecting organizations of all sizes. We came across a CPA firm recently that was breached in February but saw no evidence of breach until May. In May, post-tax season, the cybercriminals accessed the CPA firm's tax preparation software and ran a list of all clients that had filed tax extensions. Then they electronically filed the returns using the same software. They knew enough to duplicate the clients, adjust the deductions to beef up the refunds, send the refunds electronically to prepaid debit cards, and then delete the duplicated accounts to eliminate future notifications on the refunds. It was a very sophisticated and specialized attack on a twelve-person CPA firm.

There's this false sense of security that, "I haven't seen any evidence of a breach so I haven't been breached." Right? Wrong! In most cases, advanced persistent threats exist in your network undetected for an average of eight months. Usually by the time you notice them, the reconnaissance is complete and the attack is in full swing.

MODERATOR: As the Internet of Things

TroyGould
ATTORNEYS

Our job is to **solve problems.**

CYBERSECURITY
ROUNDTABLE

TroyGould is an innovative, mid-sized firm that uses creative and cost-effective means to achieve its clients business goals. From start-ups to middle-market and Fortune 500 companies, the firm's attorneys represent clients in a variety of industries, including:

- Consumer Products
- Entertainment
- Financial Services
- Health Care
- Life Sciences
- Manufacturing
- Media
- Natural Resources
- Real Estate
- Technology

310.553.4441

1801 Century Park East
Suite 1600
Los Angeles, California 90067

JONATHAN BLAVIN is a litigation partner with Munger, Tolles & Olson. Mr. Blavin has substantial experience in Internet and privacy-related litigation involving the Electronic Communications Privacy Act, Section 230 of the Communications Decency Act, the Children's Online Privacy Protection Act and the Computer Fraud and Abuse Act. He also has significant experience in high-technology intellectual property disputes, including claims brought under the Copyright and Digital Millennium Copyright Acts, the Lanham Act and other statutes. His clients include Airbnb, LinkedIn and Facebook.

jonathan.blavin@mto.com

mto.com

continues to grow, what potential cybersecurity challenges do such devices present?

FEFFER: The critical factor has been that most of these enterprise-type devices are inexpensive, and because they're inexpensive, they lack the security controls that you would expect. When consumers are buying Internet devices, their key factor is cost. They pick the least expensive baby monitor or home security camera. Those are not going to be equipped with the ability to upgrade them and patch them. The fact that we have now literally billions of these low-cost devices attached to the Internet, with low abilities for upgrading to patch security flaws that may be inherent in them, makes them very vulnerable to exploitation by cyber criminals.

What I've seen in my work very often involves medical devices—medical devices now are largely IoT devices. When a hospital buys an X-ray imager or a diagnostic machine, the capital outlay for that machine does not accommodate upgrades and constant IT attention. Instead, hospitals look at it, like, "It's an X-ray imager; it should last ten years." Those devices are very vulnerable, and that's also very scary.

So, this is the type of threat that you see from the Internet of Things. It's a threat that comes up when you don't think about security of the device, itself.

IAN BALLON: When dealing with the Internet of Things, it is important to do due diligence about the privacy and security employed by different companies that may access information or which could create security vulnerabilities for a company's own network. Maintaining good internal practices may not be sufficient.

The Internet of Things can also make it more challenging for a company to be transparent about its practices or obtain contractual liability limitations or agreements to arbitrate disputes with consumers if there isn't privity of contract. Where a consumer must access an app or a website to activate a product, it can be easier to establish privity of contract for an IoT offering.

WATTS: When something looks like an appliance, people adopt a psychological viewpoint of set-it-and-forget-it. That's not the case anymore. Everything's connected to the Internet in an office: Your HVAC systems; key card systems; projectors and video equipment; even your electronic postage meter. As Justin [Feffer] said, they are rarely designed with security in mind.

My recommendation is to put all IoT devices on a separate network segmented away from your production data.

MODERATOR: Does the Internet of Things raise unique liability issues?

BLAVIN: There was a toy that was surreptitiously recording children's voices who were using it. It was connected to the Internet, and that information was transmitted back to the company that made the doll. People filed complaints with the FTC and consumer groups, saying that this violated the Children's Online Privacy Protection Act. There was some ambiguity as to whether or not an online service within the meaning of COPPA would apply to an IoT device, like a toy. The FTC issued further guidance and said, yes, a toy that is connected to the Internet does constitute an online service within the meaning of COPPA and would be subject to COPPA's requirements, which include getting informed parental consent. So, in terms of how this could affect the cost of devices and what companies would need to do if, now, all children-related devices that are connected to the Internet are subject to COPPA and the parental consent requirements, I think that does have a significant impact from both the consumer's perspective and from the company's perspective in terms of getting those devices to market and complying with the law. That, to me, seems a pretty significant development in terms of how existing law, such as COPPA, is being applied to these new devices.

MODERATOR: More generally, what are the latest trends in data security litigation and regulation?

SELVIN: From a liability insurance perspective, there are two hot topics right now.

The first is the liability of directors and officers in connection with security breaches. From a D&O perspective, suits against directors and officers have generally not stuck,

although that may change as the regulatory environment gets more robust. There is a securities class action pending now in connection with the Equifax breach, claiming that the company had not benchmarked its financials to take into account material risks arising from cyber intrusion. So, that's one area that's significant.

The other topic involves the Target breach. Target reached a $39.4 million settlement with a class of banks that, in the wake of the data breach, had to cover all of the expenses to fix the credit reporting and identity theft of the Target customers whose personal information had been compromised. So, the zone of potential claimants included not only customers, employees, and vendors, but also banks that had to clean up after the data breach. It's significant because the banks were not in privity with the party that suffered the breach.

BALLON: When we met last year, I predicted that other circuits would reject the liberal test for standing in security breach cases adopted by the Seventh Circuit based on district court cases in California, as inconsistent with *Clapper v. Amnesty Int'l*, 133 S. Ct. 1138 (2013). That is what in fact has happened in the past year. There is now a clear division among the circuits over what level of harm is sufficient to confer standing in a case where a person's information has been compromised but the individual has not been the victim of identity theft or otherwise incurred economic harm. As a consequence, where a company is sued may be outcome-determinative.

While many standing disputes implicate the Supreme Court's more recent decision in *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016), *Clapper* actually deals more directly with standing based on the threat of future harm, which is typically what is asserted in most security breach cases. Before *Clapper*, there was already a split among the circuits over whether apprehension of future harm was sufficient to confer standing in a security breach case. The Ninth and Seventh Circuits took a very liberal approach to whether the "risk" of future harm was sufficient, while other circuits, such as the Third Circuit, held that individuals that had been victims of identity theft had standing, but, short of that, merely because information had been compromised did not justify standing based on the risk of future harm.

Prior to this year, post-*Clapper* circuit-level cases took a liberal approach. Those cases are *Remijas v. Neiman Marcus*, 794 F.3d 688 (7th Cir. 2015) and *Lewert v. P.F. Chang's China Bistro*, 819 F.3d 963 (7th Cir. 2016) from the Seventh Circuit; and *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384 (6th Cir. 2016), an unreported 2-1 opinion from the Sixth Circuit.

In 2017, we have seen a number of other circuits weighing in.

In *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017), the Fourth Circuit took a much more reasonable approach, which is more consistent with *Clapper*. In *Beck*, the court rejected the argument that plaintiffs had standing where there was no actual financial injury, but merely a fear of future harm. The appellate panel rejected the argument that offering credit monitoring underscored that the breach was serious. That is important because the Seventh Circuit has said that if a company offers credit monitoring it may evidence that a breach is severe, which really is not a fair inference. Many companies offer credit monitoring because it is a good way to allay consumer concerns and strengthen the integrity of a brand or because it is required (for example, under state laws in Connecticut or Delaware)—not because it evidences that there is an imminent risk of identity theft.

Beck also rejected the argument, based on statistical evidence, that 33 percent of health-related data breaches resulted in identify theft, which plaintiffs urged meant there was a heightened risk of harm sufficient to confer standing.

The Second Circuit in *Whalen v. Michaels Stores*, 689 F. App'x 89 (2d Cir. 2017) followed the same approach, taking a narrower view of standing based on the fear of future harm as a result of security breach, as did the Eighth Circuit in *In re SuperValu*, 870 F.3d 763 (8th Cir. 2017).

These circuits follow a stricter view. I think that is the right approach. If in the future a person whose information was compromised becomes a victim of identity theft, then he or she would have standing to sue at that time.

Meanwhile, the D.C. Circuit followed the Sixth and Seventh Circuits in adopting a very liberal view of standing in *Attias v. Carefirst*, 865 F.3d 620 (D.C. Cir. 2017). So there is a

From a D&O perspective, suits against directors and officers have generally not stuck, although that may change as the regulatory environment gets more robust. There is a securities class action pending now in connection with the Equifax breach, claiming that the company had not benchmarked its financials to take into account material risks arising from cyber intrusion. So, that's one area that's significant.

– PETER SELVIN, TroyGould PC

SERGEANT JUSTIN FEFFER supervises the Los Angeles County District Attorney's Bureau of Investigation Cyber Investigation Response Team (CIRT). He has worked as a task force officer for federal cyber crime task forces since 2004. He has instructed thousands of law enforcement officers, prosecutors and public officials throughout the United States and internationally in cyber security, cyber crime and high technology threats. Mr. Feffer has been a sworn law enforcement officer in Southern California since 1988, and a California attorney since 1994.

da.co.la.ca.us

significant split, which can make a difference in whether or not your case may end at the very outset of the case based on standing.

BLAVIN: Given the split on the *Clapper* issue, I wouldn't be surprised if the Supreme Court takes up this issue, maybe not this term, but, perhaps, next term because you do have quite a divergence between the courts of appeal on this question.

One trend that we've seen is that plaintiffs now facing standing questions are often just filing in state court. Decisions from the Ninth Circuit have indicated that just because a case gets dismissed on Article III grounds, that doesn't mean that the plaintiffs can't go and refile their claims in state court. So, you always have to be mindful that when you're going to make an Article III standing argument, that just might mean that you push the plaintiffs into state court, and you may ultimately prefer to be in federal court to resolve these cases.

If we get further Supreme Court guidance in privacy litigation as to what it means to actually suffer cognizable injury for purposes of Article III, that might not mean the elimination of class action litigation; it just might mean more class action litigation in state courts.

The difficulty with that position is, what's the difference between Article III standing and the harm requirement that you will need to meet under state common law? Plaintiffs would have to say, "We may not have Article III standing, but we've still suffered enough injury or harm for purposes of asserting our common law state claims."

BALLON: That's very insightful. The flip side is that because in many of these cases there has been no economic loss, even where standing can be established it may be difficult for a plaintiff to state a claim. Damage is an element of many claims, including the common law claims most frequently asserted in cybersecurity putative class action suits, such as breach of contract and breach of implied contract. Even a section 17200 claim in California requires actual economic harm. If plaintiffs can get past the issue of standing, they often can't get past Rule 12 motions, or, if they have pled their claims artfully and can state a claim, they may not get past a motion for summary judgment.

BLAVIN: Another issue I've seen concerning the question of the risk of future harm is that many times, there will be a data breach, but the company doesn't quite know the full extent or scope of it. What we've seen over the years are situations where there's a breach which initially the company thought may have affected a million customers; when, in fact, it is discovered a couple years later, on some part of the dark Web, that there's actually 50 million accounts that were affected by that. So, in thinking about the scope of potential harm, companies' expectations can change pretty drastically as it's discovered that more data, in fact, was taken or affected than what was originally perceived by the company at the time. That's something to think about in terms of standing and how this could affect both litigation and regulatory investigations.

BALLON: Every person's information has been compromised—for most of us multiple times—but only a small percentage of us have actually been victims of identity theft. I don't mean to minimize the consequences, but if everyone who has had their information compromised had standing to sue it would mean that virtually everyone in the United States would have a claim to bring—or even multiple claims.

I do think that the Supreme Court will resolve this issue because there is a circuit split and Chief Justice Roberts is very focused on questions of federal jurisdiction. There is now probably a 5-4 majority that would view the stricter approach to standing in security breach cases as the better one.

WATTS: If there is a more narrow definition for standing established, then how do you hold companies with large amounts of personally identifiable information accountable to adopt better security practices? Without liability, it seems less likely that they will be held accountable.

BALLON: That is a public policy question. My personal preference would be to create safe harbors to encourage good practices, rather than enacting more punitive measures. Class action litigation is not a very good way to shape public policy. These cases end up

Munger, Tolles & Olson's

PRIVACY & DATA SECURITY GROUP

OUR LAWYERS REPRESENT **HIGH-PROFILE** CLIENTS IN **CUTTING-EDGE** PRIVACY AND DATA SECURITY CASES THAT ARE SHAPING BUSINESS AND SOCIETY.

MUNGER TOLLES & OLSON LLP

LOS ANGELES | SAN FRANCISCO | WASHINGTON, D.C. | MTO.COM

GT GreenbergTraurig | 50TH ANNIVERSARY

2000 ATTORNEYS | 38 LOCATIONS WORLDWIDE* | 5 IN CALIFORNIA

On the Cutting Edge of Global Privacy and Cybersecurity, Including the Defense of Data Privacy, Security Breach and TCPA Class Action Suits

We develop innovative strategies to counsel and defend industry-leading clients in data privacy, data security and data breach, and information management matters.

This issue's Privacy Roundtable includes Ian Ballon, co-chair of Greenberg Traurig's Global Intellectual Property & Technology Practice Group and the author of the leading Internet law treatise, *E-Commerce & Internet Law 2d edition* (West, www.IanBallon.net). Ian defends data privacy, security breach and TCPA class action suits. He is listed in *Chambers & Partners* in the area of data privacy and in the *Best Lawyers in America* as the 2018 Lawyer of the Year in Technology Law. Ian received *The National Law Journal*, 2017 "Trailblazer" Award in Intellectual Property. He also holds the CIPP/US certification from the IAPP.

IAN BALLON | ballon@gtlaw.com | 650.289.7881 | 310.586.6575 | Silicon Valley & Los Angeles

GREENBERG TRAURIG | CALIFORNIA

LOS ANGELES | ORANGE COUNTY | SACRAMENTO | SAN FRANCISCO | SILICON VALLEY

GREENBERG TRAURIG, LLP | ATTORNEYS AT LAW | WWW.GTLAW.COM

benefitting a very small number of people—mostly class action lawyers, not consumers.

FEFFER: Along those lines, I saw an interesting development in California with regard to Civil Code Section 1798.81.5(b), which requires entities that collect personal identifying information of consumers to use reasonable security procedures and practices to protect that information. Kamala Harris, when she was Attorney General of California, published a data breach investigation report from the California Department of Justice, and she said in there something that I thought was very useful, on what a minimum security practice is. She tied it to the Center for Internet Security's Top 20 Critical Security Controls, and said that businesses should adopt those top 20 controls as a minimum threshold for meeting reasonable security practices.

So, in terms of a safe harbor approach that you mentioned, businesses could use something along these lines where you develop an actual standard. In my experience, in responding to many, many breaches and criminal incidents against businesses, small and large, and also government agencies as well, security tends to be, more or less, ad hoc without any real standardization. So, everyone basically is ending up reinventing the wheel at their own company, and that's not a good position to be in.

WATTS: I would love to see everyone adopt the CIS Top 20.

FEFFER: What's great about the CIS's Top 20 Critical Security Controls is that they're prioritized. So, item number one is the most important thing to do. In my experience, unfortunately, I have rarely seen businesses that actually have even met the first security control.

WATTS: I agree with Justin [Feffer] on both points. Because they're prioritized, the SANS Institute says if you implement the first five controls, you can effectively protect yourself against 85 percent of the most common cyberattacks. Implementing all 20 increases this to 94 percent. Yet when we come in and do an assessment for a new client, I rarely see any of the top five implemented.

MODERATOR: It sounds like proactive risk mitigation is key. What steps can companies take to mitigate security and liability risks?

SELVIN: In the insurance area, what you're trying to do is anticipate the liability risks, and ensure that they're covered. Importantly, a major component of cyber insurance is to provide coverage for the defense of regulatory actions and some of the remediation steps that may be required in the wake of a data breach. Products have come to the marketplace that drop down and provide coverage for things that, in the ordinary insurance world, you wouldn't think would be covered because the standard insurance exclusion relates to fines and penalties and regulatory investigations. But now, in the cybersecurity area, those are core liability and expense concerns.

WATTS: The bottom line for risk mitigation is businesses must be willing to change. What used to work doesn't work anymore. Security needs to be part of your corporate culture from the top down. It's amazing how often the top executives or partners are not engaged in the process. They'll say, "Oh, IT is going to handle it." That brings me to my next point: security cannot be managed by IT. There's a difference between delegation and abdication. You can't just hand it off and be done with it. Cybersecurity does not work that way. Choose to align your organization with information security controls like the CIS Top 20. Regularly audit your alignment with these controls. And add advanced security incident and event management (SIEM) to identify and respond to compromises that have slipped past your perimeter defenses.

FEFFER: A defense in depth strategy is key because vulnerabilities abound and they are unpredictable. You can't predict when a safe product becomes unsafe, so a defense in depth strategy with redundant controls and layers of security is best. If any one defense fails, then there are others behind it to back it up. Think of it like a castle. You have multiple rings of security around the castle: a moat, a wall, a parapet, a sally port. Even if you get through all those things, in the center, there's a fortress. That's the way to think of cybersecurity.

We know that 81 percent of attacks involve

PETER SELVIN is a member of TroyGould PC where he practices in the firm's litigation department. Peter has been listed since 2007 in "Best Lawyers in America"® for both insurance law and commercial litigation. Peter has published numerous articles and has lectured on various aspects of insurance coverage, including cyber-insurance and insurance recovery for data breaches and other cyber-related losses. Prior to joining TroyGould, Peter was a litigation partner with Loeb & Loeb, LLP.

pselvin@troygould.com

troygould.com

DAVE WATTS is president of NetFusion. Watts and his team design, implement and manage stable, scalable and secure IT networks for professional services firms and small-to-medium sized businesses throughout California. Recognized by the *Los Angeles Business Journa*l as a finalist for CIO of the year for five consecutive years, Dave uses a proprietary approach to network architecture, designed to bolster an organization's productivity and network accessibility while increasing data privacy and security.

dwatts@netfusion.com

netfusion.com

the theft or exploitation of weak passwords. A good defense in depth strategy is multifactor authentication, so that users need something in addition to a password to get access to their accounts, data, or machines. Many companies will use a token. You need a username and the password and, then, also, a code from a token that changes every 30 seconds. For risk mitigation, a defense in depth-type strategy is really the key to effective cybersecurity.

WATTS: As part of your defense in depth strategy, it is a very bad practice to have a Web server of any type (database, client access, etc.) sitting on your production network talking to the Internet. There needs to be segmentation so that if you compromise the Web server you still have some extra hoops you have to jump through to get to the production network. Again, you have to assume the external-facing Web server will be compromised. It will be. Having the proper segmentation in place will help protect your data.

FEFFER: I also want to react to something Dave [Watts] said about the culture of security. I have friends who are chief information security officers. In some ways, they're hired to be the sacrificial lamb that gets fired when things go wrong. They get hired; they have all these ideas about security; the business does not implement any of them; then, there's a disastrous breach; and they fire the security guy. It is a cultural problem. Sometimes the most senior executives are the least interested in security. I have friends who have done phishing tests on their own organizations. Do you know who does the worst and is most likely to fall for a phishing e-mail? Senior employees and executives.

MODERATOR: Are companies showing more interest in cybersecurity?

WATTS: Large organizations seem to be more concerned about it, but they often fall down when it comes to the ongoing vigilance it requires. You can't just hire the security officer, and consider it done. You have to implement process-based change and process-based checks and balances. That's where you get some resistance. With smaller businesses and firms, I see a resistance to budgeting for ongoing security above and beyond traditional IT. They think, "Oh, it's not going to happen to me." They bury their heads in the sand. It's hard to get them to take it seriously until it happens to them.

BALLON: Even for bigger companies that do take data security seriously, it is important to continually revisit policies and procedures and to do tabletop exercises to plan for a breach. This is an area where the technology changes very quickly, and the attackers are several steps ahead of the industry. Companies need to continually reevaluate their level of protection.

WATTS: You're exactly right. I recommend that you audit your alignment with those controls, and then, have a quarterly sit-down with someone other than the person who's doing the auditing. And, hopefully, it's someone at a high level.

BALLON: That's a great suggestion.

BLAVIN: In terms of liability, there is this critical question: were vulnerabilities addressed in a prompt manner? There's always this issue when you knew of the vulnerability at some point, you were going to do something, it was scheduled for next quarter, it didn't happen, and there was a breach in the interim. That can create a dangerous situation for a company because it shows that internally they knew they had to do something about this, but they delayed in doing it.

There's a prioritization of time and resources that a company needs to consider when they've identified vulnerabilities. Many times, there's a question of, "Does this really constitute a best standard industry practice, or is this more optional in nature?" or "We don't have to have the gold standard—we just need to do enough."

Another liability risk concerns privacy policies. Often, in their privacy policies, companies will say certain things about practices that they will undertake. That can get folks in trouble because then, you may have a breach of contract claim: you said that you would undertake "X" type of precautions, you don't do it, and then, you get stuck with a claim for a breach of the privacy policy.

MODERATOR: Would it be helpful for the

government to take a more active role in setting guidelines and policies for risk mitigation?

BALLON: I'm a fan of self-regulation. The government can be helpful in providing safe harbors, or guiding principles. But excessive regulation can impede business in ways that don't necessarily enhance security.

WATTS: I agree. And I would like to see them say it has to be "reasonable security" as defined by standard frameworks of controls like the CIS Top 20 or specific NIST controls because they're all process based. If companies complied with those, they would be way ahead of the game.

FEFFER: I think there's a role for regulation. Recently, there's been ransomware in the health care context concerning health records. For example, there was a recent news story that Hollywood Presbyterian Medical Center paid a ransom in Bitcoin to attackers in order to decrypt the data the hackers had encrypted. Do hospitals have to notify the patients that their information was put at risk? The Department of Health and Human Services recently said that if ransomware has encrypted your data, that's considered a breach because if the attacker is able to manipulate the data by encrypting it, then the attacker has control of the data. The fact that the attacker could have exfiltrated the data, for example, is definitely a realistic conclusion from the circumstances.

Before this recent HHS guidance, many health providers did not think that ransomware triggered a data breach notification requirement. So, that's an example of when the government's role is appropriate because patients should know that their protected health information has been put at risk. Before that, most health care providers were not notifying patients whose records were encrypted because they just considered it ransomware and not data exfiltration.

MODERATOR: What insurance products are you seeing on the market to guard against a data breach?

SELVIN: The normal forms of insurance, like D&O and CGL, have been around for a long time, and the policy forms have been standardized.

Cyber insurance is still evolving, and the offerings from different companies are quite varied. You get different forms of coverage. There are premium differences. But the language is not standardized. Therefore, it is exceptionally important, when companies are looking for cyber insurance, to be very mindful of the differences in language and policy coverage.

In general, the covered risks are the disclosure and dissemination of covered materials. So, information in your database that gets sent out on the Internet is a risk. There is often defined a trigger of coverage in a very technical sense—just as the word "securities claim" may be defined in a D&O policy, a "network security event" or a similar phrase may be the triggering event in a cyber policy.

In the insurance world, there is first-party risk and third-party risk. For first-party risk, you think of your property policy. In cybersecurity, it would be things like security breach remediation, crisis management expenses, or PR expenses. Then, you have third-party coverage, which covers the risk that companies face from third parties asserting liability claims against them, such as employees, customers, or clients.

The key issue is exclusions. Any company that relies on traditional insurance products to handle cyber exposure is playing with fire because the world has really changed, and those exclusions are now being written into more traditional products. But D&O may drop down if the directors and officers are sued or if the company has entity coverage in a D&O policy. And, in some cases, a crime policy may also drop down.

Major companies, and even mid-sized companies, must prioritize insurance, just as a matter of prudence. Breaches are inevitable, so there's got to be a way to offload that risk.

> Security cannot be managed by IT. There's a difference between delegation and abdication. You can't just hand it off and be done with it. Cybersecurity does not work that way. Choose to align your organization with information security controls like the CIS Top 20. Regularly audit your alignment with these controls. And add advanced security incident and event management (SIEM) to identify and respond to compromises that have slipped past your perimeter defenses.
>
> **– DAVE WATTS, NetFusion**

> Even for bigger companies that do take data security seriously, it is important to continually revisit policies and procedures and to do tabletop exercises to plan for a breach. This is an area where the technology changes very quickly, and the attackers are several steps ahead of the industry. Companies need to continually reevaluate their level of protection.
>
> **– IAN BALLON, Greenberg Traurig**

BLAVIN: One question is whether the insurance limits are sufficient in terms of the overall coverage for breaches. I know there's been a lot of discussion relating to whether Equifax's insurance policy could potentially cover the total scope of damage from its breach. It is not clear whether these insurance policies are sufficient or whether the limits have to go up quite a bit higher.

SELVIN: That raises two questions: one on limits, and one on the type of coverage. The question of appropriate limits has to be assessed on a company-by-company basis. The second question is what pieces a company wants from the various menus of coverage. That should depend on the likelihood of a particular risk that may develop, but I suspect that selections are driven largely by price. Dave [Watts] talked about companies being reluctant to spend money. Where the risk is more difficult to monetize or forecast, the price tends to be higher to take into account that additional risk. But the damages or the potential damages can often be catastrophic. But, it's not a lawyer who answers those questions; it's an insurance broker or a risk manager—somebody who really understands the marketplace and pricing.

WATTS: I see a huge discrepancy in the amount of knowledge some of these insurance brokers have about what policy you should get, because it largely falls under property and casualty. Those brokers are accustomed to insuring tangible things, not the intangible risk of a breach.

SELVIN: Brokers who have a deep practice in this area know the options and are sophisticated. But you mentioned property and casualty; that is a straightforward commodity. Cyber insurance is not so simple. Companies with any significant exposure should deal with brokers that do this all day, every day, and have their own group to do it because they know the marketplace.

WATTS: That's good advice. I meet people who think their insurance is going to be a cure-all for their breach. But it won't cover everything. For example, there's no coverage of lost time, right?

SELVIN: There is a business interruption element to most cyber policies. So, for example, if there's been a denial of service attack that causes the company to stop operating. Now, there are all kinds of caps and qualifications on coverage, but if the company is disabled and is unable to resume its normal operations for the period of time set forth in the policy, that is a covered risk. But supervisors and people running around dealing with outside consultants, that's just part of your internal overhead.

WATTS: Will insurance cover any loss of your brand or reputation?

SELVIN: No. But one important element of first-party coverage is PR and crisis management. That has become an indispensable part now in terms of addressing reputational damage post hoc.

MODERATOR: What cybersecurity issues are on the horizon in 2018?

BALLON: I think we are going to continue to see an increase in litigation. But because of circuit splits—not only on standing, but also under a number of different statutes such as the Computer Fraud and Abuse Act and Video Privacy Protection Act, where the law in one circuit is more favorable than the law in others—we're going to see more litigation brought strategically in particular venues where the law is perceived to be more favorable, until these circuit splits are resolved.

WATTS: From a technical side, I think there's going to be much more emphasis on the assumption that you're going to be breached. So, rather than focus only on prevention, I think there will be additional focus on how we identify and contain advanced persistent threats. More companies will implement systems and response processes that will identify and contain those breaches before they can access or remove data.

FEFFER: I've been dealing with cybercrime full-time for fourteen years now, and, unfortunately, my prediction is things will continue to get worse. The first case I investigated was the defacement of the D.A.R.E. website, literally. It was done by what we would now call a hacktivist. That was a big case back then, and now, it's nothing. The takeaway is attackers are

growing more sophisticated.

For example, the Nigerian prince e-mail scheme to get an inheritance has now led to the business e-mail compromise technique, which is extremely effective and has resulted in businesses, large and small, and government agencies, frankly, as well, losing billions of dollars. My prediction is things will not improve, and we'll see the attackers growing in their sophistication and specialization. Targets will become more and more vulnerable, unfortunately.

SELVIN: The insurance area that is closely watched is the extent to which officers and directors are going to be tagged for breaches. As I said earlier, so far, there has not been much traction. But cybersecurity is now so closely tied into the company's overall financial condition that it's got to be, at some point in time, either the basis for a derivative or federal securities fraud suit. That's going to change the pricing of D&O coverage, or there may be exclusions to D&O coverage. As regulators continue to ramp up and impose on officers and directors these additional obligations, it's inevitable, I think, that there will be claims that follow on to a data breach and the consequent drops in stock price. It's just inevitable that that will eventually happen.

BLAVIN: I am interested to see how the regulatory environment changes, if at all, under the new administration. I think in the next year, we will see whether or not the FTC and other federal agencies are taking a different approach than they may have taken under the Obama administration. Also, it's very interesting to see state regulatory agencies and state enforcement ramping up. After the Equifax breach, we heard immediately from the New York Attorney General and the California Attorney General. To the extent there are any vacuums in the federal space, you're certainly going to see the states jump into them quickly.

Due to many of these recent high-profile breaches, the FTC's actions are going to be in the spotlight. I think we can expect states to be just as active as they've been in the past, and potentially more so, if they perceive a vacuum in federal enforcement.

WATTS: In the private sector, I think it's going to become much more common that when a company is looking to acquire or merge with another business, they will assess the company's cybersecurity posture and protections. I think that will be on the rise.