THE LEVICK E-BOOK SERIES
VOLUME 5

Cybersecurity & Privacy

LEVICK FIXING THE IMPOSSIBLE™

Primerus
The World's Finest Law Firms

Table of Contents

Continued on next page

Continued on next page

BROADCAST HIGHLIGHTS

Krebs on Security

Biometric Privacy

The Bad Guys Have Changed

BROADCASTS

About LEVICK

LEVICK is a crisis communications and public affairs agency representing countries and companies in the highest profile matters worldwide. Comprised of attorneys, former journalists, intelligence officers, authors, and members of governments, we provide our clients with risk intelligence to anticipate forthcoming challenges; crisis remediation; rehabilitation, and reemergence.

On public affairs, we understand how ideas become movements and can inspire viral communications — or help to minimize it. From the Gulf oil spill, AIG, and Guantanamo Bay to the World Cup, multi-jurisdictional class actions, and nation-state kidnappings and ransom, we help our clients implement the strategies and communications on the most complex matters. For regulatory, litigation, financial, crisis, and public affairs matters, LEVICK is the firm of choice for the world's leading law firms and insurance companies.

About Primerus

Primerus
The World's Finest Law Firms

Primerus is a society of the world's finest independent, small to medium sized law firms. With over 3,000 of the world's finest attorneys, and 175 member firms in more than 50 countries, Primerus is available to assist in-house counsel, corporate executives and business owners with all of their legal needs worldwide. Connecting with Primerus firms, clients can expect responsive, partner-level service at reasonable rates.

Foreword

by Ian Lipner, Senior Vice President, LEVICK

Cybersecurity was once a technical conversation confined to the pages of trade magazines and left to the information technology community to decipher. It wasn't a business conversation unless it was a budget discussion, and cybersecurity was still seen by the typical CFO as an area in which cost-effectiveness was a bigger priority than effectiveness.

The mood began to change with the first big breaches, often those associated with credit cards or payment accounts. LEVICK is well-known for handling some of the industry's first and most severe incidents, such as the U.S. Office of Personnel Management cyberattack, the Target credit card data breach and the Heartland payment card breaches. By then it was becoming more real, and easier for a CFO to calculate the cost of a data security incident. In the meantime, the world moved more commerce, more business process online.

Cybercriminals playing a longer game with the aim of identity fraud made personally identifiable information (PII) their targets, and GDPR regulation followed, making cybersecurity more a priority for companies. Still, far too many brands waited to respond rather than prevent.

Ransomware groups then became more prominent — criminal groups targeting the actual operations and public facing services of companies. The cost of downtime is inarguable. The impact on brand is unmistakable. And in 2020, if your website and systems are all down, for that moment, you cease to exist.

As Fortune 500 CEOs watched malware shut down their competitors' day-to-day operations in a blink of an eye, they made cybersecurity a boardroom conversation. But laggards waited for the next shoe to drop. They didn't train their employees to avoid phishing; they didn't beef up their security; they didn't hire specialist teams.

Or worse, the cybercriminals may just be a step ahead of industry. Now, during the COVID-19 crisis, organized cybercriminal groups are launching two pronged attacks — using stolen data as further blackmail fodder while simultaneously paralyzing critical systems. And they're stealing new user credentials that will enable them to access more accounts for new attacks in the future. This happens as millions work from home on insecure cable routers and their children add new credentials to dozens of new websites on second-hand laptops for remote learning. The global pandemic has created a massive opportunity for cybercriminals.

The leader companies, especially in the regulated industries, already understand that doing business in this environment without proper cybersecurity posture could be fatal. They are installing next generation endpoint security products, engaging with forensic specialists for simulations, adding risk quantification capabilities, and even protecting their executives with concierge-based services.

In the interest of further informing leader companies, we explore in this eBook the myriad vectors for risk, the effects they have on our businesses, and the measures companies are putting in place to contend with the next wave of cybercrime.

section

02

The *Other* Russian Hacking Scandal: Don’t Palpitate – Prepare!

Almost lost amid the Watergate-level tsunami of media coverage over incriminating emails and what constitutes "collusion" is the U.S. government's 2017 revelation that Russian hackers were behind cyber-intrusions into the U.S. energy power grid. FBI and Department of Homeland Security (DHS) officials believe that the hackers' primary targets were nuclear power companies and other energy facilities.

To date, those officials say, there is no evidence that plant operating systems have been compromised or that public safety has been placed in jeopardy. Hackers have so far "only" succeeded in breaking into administrative systems, pilfering log-in and password information.

Still, it's a sobering development — one every bit as threatening to national security as the integrity of our election system. Chaos, it has long been said, is only an extended blackout away. It's been a matter of public record that nefarious Russian hackers have zeroed in on U.S. energy companies. The only thing more frightening than having a hostile nation proven capable of controlling your energy grid is the execution of that control.

It's also a matter of public record that Russian hackers deliberately disabled the Ukrainian electric system in December 2015, leaving a quarter of a million Ukrainians without power for hours on end. The Russians have since tested a cyberweapon capable, experts say, of upending power grids on every continent, with nuclear facilities at the top of their target list.

Information warfare expert Molly McKew of Fianna Strategies maintains that "Russia views these asymmetric means as critical tools to give them advantage in a shadow war against the West — and the development and deployment of these tools is escalating. One category of hybrid warfare is economic warfare, and targeting critical infrastructure as pressure, disruption, or leverage is a part of that. These threats and attacks from the Kremlin are part of a concerted campaign to weaken America."

CONTROL THE NARRATIVE BEFORE IT CONTROLS YOU

by Paul Ferrillo, Partner and Cyber Specialist, McDermott Will & Emery

Name your nation-state. Name your cybercriminal organization. Name your brand of malware or ransomware. Today's environment has never been more perilous for U.S. companies.

Literally, your company can be fine one day, and then an employee of yours actually "clicks on the link or attachment" and the black screen of death shows up on company computers announcing that your files have been encrypted.

It only takes one bad email to ruin your day.

The time to stop the cycle is here and now. A holistic defense composed of many parts, such as identity and access management, email filters, multi-factor authentication, and machine-learning anomaly detection, makes the most sense. No solution is perfect, but many solutions can help defeat an Advanced Persistent Threat (APT)-like menace.

Above all, have a battle-tested incident response, business continuity, and crisis communications plan, so you can control the narrative, *before* it controls you.

All of these activities can be conducted at the direction of counsel and subject to the attorney-client privilege. No organization wants its well-intentioned, proactive security engagements to result in the creation of a "smoking gun" in the event of litigation. Consider working with outside counsel on these activities to prevent your business from being penalized in litigation for its compliance activities. Tech-savvy counsel can also assist in developing employee trainings that help reinforce the responsibility all personnel share to help prevent security incidents.

Palpitations, anyone?

Mark Farley, of Farley & Partners LLP and crisis response counsel to some of the largest global energy companies and chemical manufacturers, also worries about the integrity of America's industrial infrastructure. "Chemical manufacturing facilities and oil refineries represent targets for terrorists or others committed to industrial sabotage," Farley says, pointing out that facilities that rely on automated process control systems could be especially vulnerable to intrusion.

Farley emphasizes that unsavory elements are hatching computer viruses that specifically attack industrial processes. "The emergence of the Stuxnet worm in 2010, which is believed to be the first malware created specifically to target such control systems, exposed their vulnerability to cyberattack, not just by terrorists, but by foreign governments," he says. A rogue command at a chemical or energy plant could cause a pipe to rupture or a storage tank to explode, endangering workers, the public, and the environment, warns Farley.

Hackers could foist similar chaos onto the control systems of the financial services industry or any sector they choose, experts say. McKew observes that such attacks, left unmolested, will surely weaken the U.S. economy and, with it, national security.

What can we do about it?

THE IMPORTANCE OF THREAT INTELLIGENCE IN CYBERSECURITY

by Adam Vincent, Chief Executive Officer, ThreatConnect

In today's cybersecurity environment, many security products perform some level of security automation and orchestration. These capabilities allow organizations to automate a greater variety of security tasks, freeing up humans to handle scenarios that require deeper thought. However, many of these technologies still leave security analysts with a glut of logs and events, many of which may lack vital information or are merely false positives. All of this tends to further feed into the known issues of overworked security teams, gaps in security, and poor organizational efficiency.

To account for these weaknesses, security software has begun to incorporate intelligence creation into the output of the workflow itself. These new platforms have begun to allow for not only aggregation, but analysis of external data feeds, creation of new internal intelligence, and connections between defensive products for the automation of detection and prevention with operational threat intelligence. This next generation of security platforms — Security Orchestration, Automation, and Response (SOAR) — pulls together these elements to create a more holistic and more actionable single source of truth.

Proper SOAR solutions combine threat intelligence with orchestration and automation, providing additional benefits:

- The ability to alert, block, and quarantine based upon multi-sourced, validated intelligence helps to ensure that you are alerting and blocking the right things.
- Intelligence allows your security team to act more decisively and proactively, eliminating false positives and validating events to increase the accuracy of actions taken.
- Through the usage of intelligence thresholds and consequent automation, security teams can strategically determine processes to provide greater improvements to security.
- By parsing gluts of information into more efficiently scaled channels, security analysts can use adaptable scoring and contextualization to more accurately determine what action, if any, needs to be taken.
- Integrating threat intelligence and incident management allows teams to capture their insights, artifacts and sightings, and refine them into new intelligence.
- Processes can be adjusted automatically as new threat capabilities, tactics, techniques, and infrastructure develop.

Along with the progression of technology, bad actors are becoming increasingly sophisticated. Incorporating intelligence management and analysis capabilities natively into our security platforms will be the next crucial step in the development of cybersecurity.

On a national level, McKew says, we need to harden our energy grid and gather better intelligence about foreign threats. Other critical U.S. infrastructure — including our communications grids, our fiber-optic transmission lines, and our water extraction and distribution systems — should also be strengthened.

On a corporate level, what remedies can facility owners and operators take to mitigate risk and strengthen their capacity to fend off cyberattacks? Mark Farley and I offer this quick prescription:

- Evaluate your site security by assessing overall plant vulnerability, particularly your control systems;
- Review your plant network architecture and assess the vulnerability of your Internet and corporate information networks;
- Update your employee crisis training to include a cyberattack scenario from a hostile foreign power and regularly conduct drills to ensure that everyone is on the lookout for telltale cyber intrusions and aware of their take-charge responsibilities should one occur;
- Have worst-case-scenario materials ready to go, from statements and tweets from the CEO to testimonials from third-party cybersecurity experts;
- Ensure that your communications people are expert at tapping social and digital media channels as well as conventional outlets — in a cyber crisis, you'll need to dispel myths and misinformation and get the facts out in a hurry; and
- Track adversarial online communications and examine its original source — look for patterns and things that don't seem to make sense. Most nation-state attacks leave footprints along the way that don't necessarily tell you what is about to happen but can point you in the right direction.

Cyberattacks have become an unfortunate reality for every business and institution, regardless of size or mission. Having your systems breached or blatantly assaulted is not a matter of if — it's a matter of when.

Companies in these perilous times have no choice but to ready themselves for the nightmare contingency that America's biggest adversary could be hell bent on disrupting their operations.

After the success of Russia's interference in the energy grids of its satellite countries, we have little doubt about either their intent or capability. We also have an early warning.

Don't palpitate. Prepare.

No Easy Solutions: Facebook's Response to Russian Hacking May Determine Tech's Regulatory Future

In many ways, Mark Zuckerberg is a talisman for the rest of Silicon Valley. The Facebook founder and social media pioneer has always embodied the Valley's swashbuckling entrepreneurship.

But Zuckerberg's buccaneering days are likely behind him as he has finally started to recognize the perils facing Facebook and his industry, not to mention owning up to his responsibility in cleaning up the Russian hacking of his company's services that tainted the 2016 election. The same holds true for the rest of the tech community, much of which (Twitter, DreamHost, and Disqus, to name but a few) was manipulated by cyber crooks working under the thumb and index finger of Vladimir Putin.

Suddenly Silicon Valley has become *the* front line in America's fight to keep hostile foreign powers from throttling our democratic institutions. Russia's thuggish behavior is especially thorny for the Big Five, the so-called FAANG companies — Facebook, Amazon, Apple, Netflix, and Google.

Robert Mueller's investigation revealed that Russia's military intelligence unit, the GRU, an offshoot of Putin's alma mater, the KGB secret police, targeted Facebook and other Web-hosting platforms to trumpet the emails it had stolen from Hillary Clinton's campaign and the Democratic National Committee. All this follows revelations that the Russians tapped phony Facebook accounts to spread malicious anti-minority and anti-immigrant messaging and to purchase at least $100,000 worth of anti-Clinton advertising.

Zuckerberg and Facebook were slow to recognize the gravity of the Russian threat. In the immediate wake of President Trump's surprise victory, Zuckerberg said it was "crazy" to believe that his company's platforms had been exploited by a foreign adversary. But after evidence of Russia's skullduggery mounted, Zuckerberg has acknowledged that Facebook has a responsibility to atone for its missteps.

Russia's depravity runs deep. The GRU's hacking division, the cyber thieves that experts suspect were behind the original DNC breach, goes by the obnoxious moniker Fancy Bear. Either Zuckerberg gets Fancy Bear to retreat to its cave or he runs the risk of watching his company and other tech giants get devoured by federal regulation — the scenario that Silicon Valley has managed to avert all these years.

Zuckerberg's tour of the country demonstrates that he and Facebook are beginning to understand the implications of Fancy Bear's mauling. They are publishers — not cowboys — who accept, it would seem, at least some of the responsibility of legacy media. Now the issue becomes: How much of a leadership role is Facebook willing to take in finding real solutions? And how far will it go in disclosing its own corrective actions? Without concerted disclosure and transparency, Zuckerberg could become, in the public's eye, just another robber baron. In 2011, Facebook argued before the Federal Election Commission that its ads were "small items," like campaign buttons, and should be exempt from campaign disclosure rules.

Facebook's public affairs and communications strategy is only now evolving. The phalanx of Washington lobbyists they've retained rivals Exxon-Mobil and dwarfs the big Wall Street firms. Yet so far, they've all stayed mum about Facebook's strategy.

The potential regulations faced by Facebook and others are not insignificant. In fact, these regulatory ideas have begun to percolate in policymaking circles:

- Web platforms with more than one million users would be compelled to publicly disclose the names of individuals and organizations that spend more than $10,000 on election-related advertisements.
- Providers would be required to establish a public database and display digital copies of all relevant ads.
- The database would also have to house all "electioneering communications," including a description of its targeted audiences, its view count, the exact timing of its placement, its price, and detailed contract information.

And that's just the beginning. The draconian antitrust fines and taxes that the European Union has begun to assess against the FAANG companies could find their way across the Atlantic. It's entirely plausible to suggest that Web companies could be looking at a regulatory regimen not unlike that imposed by the Federal

Communications Commission (FCC) on television and radio broadcasting in the 1950s and '60s: a "fairness doctrine," requirements for community service and public-spirited broadcasting, an insistence on children's educational programming, prohibitions against "obscene" or "indecent" material, et al.

Robert Corn-Revere, a partner at Davis Wright Tremaine who specializes in communication and information technology law, notes that, "People who worry about large, unaccountable tech companies should worry more about large tech companies subject to the control of politicians and regulators. In that regard, the experience of Europe – not to mention our own history with regulating communications technologies – should serve as a cautionary tale."

Veteran technology policy lobbyist Kim Koontz Bayliss of Perry Bayliss adds, "How tech companies respond to mounting Congressional criticism is extremely important and will dictate how policymakers treat them going forward on everything from antitrust to zero-rating. The more integral these companies become to the lives of average Americans, the more serious the threat. They must work harder to educate policymakers about how they are conducting their business."

The FAANG companies must also work harder at communicating the economic, educational, and cultural benefits that technology brings *every minute of every day* to American life — and not just to policymakers and opinion leaders, but *to everyone*. They need to enlist grassroots and grasstops allies that can take their message to those parts of America that feel left behind in the information revolution.

They need to ramp up their corporate social responsibility programs and rededicate themselves to bridging the Technology Divide that separates the upwardly mobile from those struggling to get ahead. Too often, that gap makes rural and less fortunate communities feel abused and forgotten. If technology has separated those with 20th century skills in a 21st century workplace, it must now help bridge that gap so that anger subsides and reason — and hope — return.

NEED FOR PRINCIPLE-BASED DATA REGULATION STANDARDS

by Bill Ide, Partner, Akerman, and co-chair of the Conference Board ESG Advisory Board

Data and its utilization have changed and will continue to change the way we live. The societal benefits of data utilization have been astounding, but with such advances also come significant potential harms.

Governmental regulation of data has largely been reactive and has failed to establish guiding principles that capitalize on the benefits while mitigating the harms. Issues such as surveillance, facial recognition, global data flow, and government access to data held by others without obtaining judicial approval need public debate and resolution by governmental action. The Conference Board ESG Center is examining the private sector issues surrounding the goal of transparent collection, securitization and utilization of data to achieve the maximum benefit of data utilization while assuring adherence to established principles of securitization, privacy and ethical norms.

To date, regulation in the United States has centered on data security. Every state currently has a data breach notification law; many have recently enacted data protection laws. These laws are inconsistent; from a national perspective, they appear to burden, more than benefit, the use of data. As privacy concerns have come to the forefront, it appears that privacy laws may arise from a similar balkanized regulatory framework. Self-regulation efforts, which have the potential to alleviate the need for government regulation, have not yet led to recognized standards, ethical or otherwise, on how data should be responsibly secured and utilized. It is time to leap ahead of where digital innovations are going, reform existing paradigms and create new ones to provide data governance that assures the greater good.

The Conference Board ESG Center believes that thought leadership and education are critical to resolving the many complex issues surrounding data and its usage. Data collection, securitization and utilization of data must be transparent and balanced to achieve the maximum benefit of data utilization while minimizing the potential for harm.

As technology will continue to evolve, principle-based data regulation that can evolve with the changing technology is needed. It can be implemented through legislation, regulation or adoption of self-regulation norms. The Conference Board ESG Center plans to present a white paper that facilitates a meaningful discussion about the principles that should govern data security and usage.

When Americans living along the East or West Coast hear "robotics" or the "Internet of Things" they look forward to the prospect of mastering new technology. When a rural or at-risk American hears about exotic breakthroughs, they fear their jobs and way of life are being threatened.

Beyond the specter of added taxation and regulation, there is another bête noire with which the Big Five must grapple. Part of it is a byproduct of the Technology Divide but in truth its roots run much deeper.

Trump's victory heralded a new kind of American populism — a contempt for big money and big institutions that is far more belligerent than its predecessor of a century ago.

The radical nationalist movement championed by former Trump Svengali Steve Bannon is not just anti-establishment; it's anti-*anything* that smacks of the ruling class, with Big Tech at the top of the list. Many Americans — and not just Trump voters living in small towns – resent tech's ubiquitous presence and prodigious money-making. They would applaud any leader slapping it down.

This anti-elite populism is likely to survive Trump's tempestuous presidency. Mark Zuckerberg and his Silicon Valley compatriots are facing some serious hurdles. It's not just Fancy Bear that lurks on their pathway.

"BEC" IS HUGE CYBER THREAT

by Christina Gagnier, Shareholder, Carlton Fields Los Angeles

What may seem benign in today's rapidly paced online communications is often not: a single email and the subsequent response from an employee could lead to a chain reaction of data breach and economic loss. Business email compromise (BEC) is emerging as an imminent, unforeseen cyber threat to businesses and is often overlooked as one of the largest risks in information security today.

In the wake of sweeping changes to data privacy and security regulations globally, many companies are focusing on wholesale shifts in the ways that they manage data. With all the attention to detail and sophistication that is being layered into global privacy compliance, one of the continually overlooked areas is that of simple human error; in the case of business email compromise, a harmless response to an email can turn out to be anything but. Also known as "phishing" or "spoofing," a third party creates a "mirror" email account that appears to come from someone internal to a company, but this account is being operated by an outside third party often looking for pecuniary gain.

Being proactive to prevent these attacks is essential. Several steps can be taken to jump-start better business email practices and safety.

- ***Start with the Right Email Technology***
  Authentication has become a cybersecurity buzzword over the past several years, and there is a good reason for it: it can be critical in stopping an employee from errantly sending out data. Make sure your email systems flag emails from accounts outside the company ecosystem. The use of multifactor authentication mechanisms can help avoid the success of external email compromise attacks.
- ***Train Your Team***
  Train your employees on how to recognize common scam attempts. Prepare resources for employees to reference should they have questions about an email or other communication received. Ensure your team knows that they should report anything suspicious.
- ***Have Clear Guidelines on Information Sharing***
  Make it a policy that no one shares sensitive information without verification. An "email from the CEO" asking for financial account information should immediately demand a phone call or other communication for verification of the request. It should be company policy that any sensitive information that is shared should be password protected. Clear guidelines lead to clear methods of response that can avert cyber threats.
- ***Make Sure IT Employs Preventative Measures***
  Your IT team should be constantly monitoring systems for cybersecurity threats. Engaging in routine audits and catching system issues can be critical to avoiding data loss. IT should be put out front and center not only as a resource for "fixing" computer and network problems but also as a front line of defense for helping to identify potential cyberattacks.

section

04

Averting IP Debacles: A "Lessons Learned" Checklist for Smart Companies

Intellectual property (IP) challenges for U.S. corporations can take many forms. Sometimes it can be failing to recognize the threat of a cyberbreach.

At other times, it can be ignoring copyright infringement litigation until it's too late, or neglecting to track down a competitor's patents, or foot-dragging while filing for trademark protection, or not being zealous enough in preserving trade secrets.

The ultimate lesson to learn? Few issues can injure an established corporation or bring down a promising venture more quickly than mishandled intellectual property (IP) concerns.

Look no farther than Apple, which in 2017 was forced by a Texas jury to pay $502.6 million in damages after it ruled that iMessage, FaceTime, and other Apple offerings infringed on VirnetX's patents in a dispute that took eight years to resolve.

Or look at Google, which recently lost its initial appeal on a multibillion-dollar copyright infringement case against Oracle that could have profound repercussions on the technology software industry if the ruling stands.

Staying on top of emerging IP trends, sidestepping IP potholes, and embracing proactive communications measures can determine a company's ultimate success. A company's CEO and board members have no choice but to accurately assess their IP risks — and take the necessary steps to mitigate them.

It's apparent from such recent studies as The 2017 Global Patent & IP Trends Indicator that IP activity has significantly increased worldwide, with most new filings coming from the U.S., Europe, and China.

It's also evident that corporate counsels are worried about the potential effect of the European Unitary Patent (UP) and its Unified Patent Court (UPC), both of which are aimed at streamlining patent filings. Officials are trying to create a single patent across the EU that can be administered by a single court, thereby saving money and aggravation.

The UP and its court affiliate were slated to go into effect in 2018. But both have been delayed, in part because of the U.K.'s Brexit vote and in part because of misgiving leveled by Germany's Federal Constitutional Court.

The EU controversy illustrates the tension surrounding patent rules and why IP remains such a big priority in corporate suites. Companies, even those in brick-and-mortar industries, have little choice but to exercise IP due diligence. Indeed, identifying IP assets and confirming their availability is part and parcel to any business transaction, maintains Gaston Kroub, a founding partner of Kroub, Silbersher & Kolmykov PLLC, an IP boutique firm in New York.

"Whether it's in the area of patents, trademarks, copyrights, or trade secrets, the evolving nature of IP law demands that companies of all sizes take a proactive approach to dealing with IP issues," says Kroub, the author of an *Above the Law* article on IP trends.

"Of special concern are the high costs of defending against intellectual property claims brought by others, both in terms of hard costs in the form of legal fees and the like, and soft costs in the form of unwanted business disruption and negative publicity. It is critical, therefore, for companies to work with internal or outside IP counsel to ensure that appropriate levels of attention are paid to IP issues in a timely manner, especially when it comes to assessing the risk of receiving an infringement claim because of a specific product or service offering.

"As with most things, being proactive when it comes to IP issues can help reduce the impact of potential business problems arising out of unforeseen events like an infringement claim," he says.

With Kroub's warning in mind, what communications lessons can companies implement to reduce their IP risks and create a smarter internal and external approach to IP?

- *Give IP the priority it deserves.* The higher the stakes, the more important the IP due diligence. Don't wait until the transaction is practically finished to identify competitive patents or begin considering the exposure of your proprietary offerings. Identify key risks and vulnerabilities on day one and constantly update the list.
- *Give every division a stake.* Given confidentiality, not every member of your executive team can be part of the IP exercise, but every *division* ought to be. Legal, marketing, communications, public affairs, and IT should all be part of your IP task force. With the potential of artificial intelligence (AI) to revolutionize labor-intensive IP administrative tasks, shorten decision-making processes, and increase the ability to analyze large amounts of data, companies now have the ability to put strategic decision-making first, without worrying that there are too many cooks in the kitchen.
- *Protect your own "state secrets" first.* If there isn't consensus on those patents, trademarks, service marks, et al., that are integral to your continued marketplace success, you need to develop it in a hurry. Your untouchables list — and the protection action that list demands — needs to be understood by every top- and junior-level staffer in the company. Look at the March 2018 suit filed by Match Group against dating app Bumble, which was founded by former employees of Match's Tinder dating service. Trade secret misappropriation allegations stand out, especially when you note that features of Bumble allegedly mirrored ideas developed for Tinder right before the employee severance agreements were up.

UNMASKING IDENTITIES OF CYBER ADVERSARIES

by Amyn Gilani, VP of Product, 4iQ

Uncertainty in identity attribution and plausible deniability has historically weighed in cybercriminals' favor. As security leaders shift their views, however — no longer playing defensive whack-a-mole — the likelihood of catching culprits has risen. Bad actors may attempt to obfuscate their online identities, but they are people, too. Many have left traces of their identities in social media apps and websites that were exposed in data breaches and leaks.

In 2007, I was deployed to Iraq as a U.S. Air Force intelligence analyst on the Joint Special Operations Command Task Force. My objective was to capture insurgents and disrupt terrorist activities. We constantly pursued the identities of al-Qaeda's mission-critical individuals, relentlessly tracking networks of the dangerous people who put democracy at risk. Correctly identifying targets was critical to ensuring the right people were taken out of the equation.

Now that the battlefield has shifted largely in the digital realm, the same can be said for attributing and uncovering identities of cyber adversaries.

Today, there are tools that leverage breached data, open-source intelligence and other data sources, making identity attribution possible, reliable and efficient. By uncovering the identity of its adversaries, your organization can use this five-step approach to disrupt and prevent future attacks:

1. **Make the data obsolete:** Resetting passwords of employee and customer accounts to prevent takeovers will reduce the value of exfiltrated data on the black market.
2. **Move quickly:** The more swiftly you take action on the compromised data, the better. This will lead to less disruption and fewer financial losses for your organization.
3. **Report it**: File suspicious activity reports and inform law enforcement. Call the Department of Homeland Security's National Cybersecurity and Communications Integration Center or an established contact from the local FBI cyber unit.
4. **Identify threat vectors**: Analyze when and where. Patch up weaknesses and vet your partners' and vendors' security postures, as they may represent possible avenues of attack.
5. **Collaborate:** Given the interconnected nature of our networks, collaboration is crucial in the arsenal of law-abiding organizations. If you find leaked or exposed data from another company, inform them so they can quickly notify customers, reset passwords and perform remediation. For anti-phishing, contribute to the Anti-Phishing Working Group. For identity attribution support, invest in a credible identity intelligence monitoring service.

- *Get some credit for your own IP.* If it would further your business objectives to give wider visibility to your trade- and service marks and other intellectual property, then engage marketing, communications, and advertising in some smart outreach. Such visibility could pay dividends for a deal down the road or just now in the planning stages.

- *Make sure you know what's going on overseas.* If going global in any way is part of your business plan, then your company needs to adopt a global approach to IP strategy. If your company applies for single patent protection in many different countries, then you need to be advised on country-specific processes and challenges. As the EU's current confusion demonstrates, the IP field requires constant monitoring. Regulatory and litigation risks vary from locale to locale.

- *Keep it simple.* There are few issues more complicated than IP law. You will be wise to remember Proverbs 17:28: "Even a fool is thought wise if he keeps silent, and discerning if he holds his tongue." Most non-IP lawyers on your team will nod in agreement with your strategy rather than risk asking what they fear is a stupid question. Don't be afraid to "dumb down" the issues so that you are certain everyone on the team gets them. Remember, IP is traditionally the combination of legal and scientific training. But IP litigation is fought in the worlds of business, law, politics, and communications.

In today's hyper-competitive business climate, no company can afford to fall behind the IP curve. Better to take to heart Benjamin Franklin's adage that "By failing to prepare you are preparing to fail."

PREPARING FOR THE (CALIFORNIA) CCPA'S PRIVATE RIGHT OF ACTION

by Jon Frankel, Shareholder and Cyber Specialist, ZwillGen

With the California Consumer Privacy Act, or CCPA, going into effect January 1, businesses were primarily focused in 2019 on ensuring their ability to comply with the law's transparency, contracting, and access/deletion request requirements. But now that the CCPA is in effect, it's time to refocus on another key aspect of the law — namely, its private right of action (PRA) for data breaches that are the result of a business's failure to implement and maintain reasonable security procedures and practices. While not the first data breach-related PRA under California law, the CCPA PRA is notable for offering statutory damages of $100 – $750 per consumer per incident, which in a class-action lawsuit could quickly add up.

In anticipation of a torrent of consumer lawsuits following data breaches, businesses subject to the CCPA may want to consider several activities to prepare for 2020 and beyond. Performing an assessment of the maturity of your organization's information security program may help to identify "gaps" that should be addressed to counteract allegations of unreasonable security practices following a data breach. Engaging a vendor to perform a penetration test or vulnerability assessment can likewise provide significant value, especially if your organization has not done one before. Standing up a vendor risk management program to shore up security risks created by service providers or supply chain components is also increasingly viewed as an essential component of reasonable security.

Implementing a new incident response plan or strengthening an existing one can further mitigate litigation risk by helping to ensure that inevitable security incidents are quickly detected and handled efficiently and professionally.

Finally, conducting a tabletop exercise is a highly effective way to pressure test your incident responders and make sure that the response to "live" incidents is consistent and predictable.

section

05

Keeping Board Members Apprised of Risks of Cyberbreaches & “Disrupted” Communications

The onus of managing risk in every corporation ultimately falls on the CEO and the board of directors. Few events pose more sudden and systemic risks to corporate leadership than a significant cyber event. And the threat is only growing.

If reputations are gained by the teaspoon and lost by the gallon, cyber is exponentially more threatening. Effective CEOs, therefore, are thoroughly plugged into cybersecurity operations, those systems and procedures that, in today's lexicon, are aimed at mitigating the risk of company communications being "disrupted."

I know from conversations with CEOs and general counsels across the country that, besides being impugned on social media, their biggest fear is having their cyber systems hacked — and their "state secrets" exposed and exploited, or worse, their external and internal communications operations dismantled or gutted. When you can't tell the world you've been hacked because your email system is completely down, you're in trouble.

A cybersecurity breach or collapse can take a corporation down or dent its reputation with key constituencies almost as fast as you can say "GDPR," the acronym for General Data Protection Regulation, the European Union's (EU) new data regulatory regimen that — for good reason — is causing angst in C-suites and boardrooms across the world.

Many board members don't necessarily live in the world of disrupted communications, cyber ambushes, NGO assaults, blow-ups on Twitter, and all the rest. So, what's the appropriate role for board members these days on issues such as GDPR compliance?

The board's responsibility revolves around recognizing risk — and ensuring that the company is taking appropriate action and installing sufficient back-up systems to minimize that risk.

GDPR is a classic example: hundreds, if not thousands of American corporations are operating under the mistaken impression that they don't have to comply with the EU's new privacy regulations. Yet if companies depend on the creation or processing of data (and these days, what company doesn't?), there's a strong chance that they'll be subject to GDPR and the ongoing efforts of the EU and other government entities around the world to crack down on hacking and privacy violations.

Under GDPR, every data-driven company must appoint a designated data protection officer. Data protection best practices, moreover, now point to the creation of a board-level cyber risk committee, as well as toward the assurance of personal employee-level cybersecurity discipline among board officers themselves, since they're often the target of phishing. Finally, board members should keep in mind that the U.S. Cybersecurity Disclosure Act of 2017 requires board-level cybersecurity expertise.

The "European model" for antihacking and privacy protection is the way the world is going. Smart companies and board members need to stay a step ahead.

Athletic apparel retailer Under Armour's recent experience is sobering. When hackers breached Under Armour's MyFitnessPal app, it took the company some four weeks to detect the magnitude of it and another week beyond that to disclose it — a fairly quick response, compared to a lot of cyber hacks. Under Armour's data protection systems, all in all, held together quite well; the hackers failed to access such valuable user information as location, birth dates, and credit card numbers.

Still, Under Armour's board members were no doubt surprised to learn that a big chunk of the company's passwords were protected by a relatively antiquated — and knowingly flawed — hashing scheme. As *WIRED* put it, "This means that attackers likely cracked some portion of the stolen passwords without much trouble to sell or use in other online scams."

Imagine the scene in Under Armour's boardroom when the IT executives tried to explain why certain passwords were rigorously protected and others weren't. "The situation, while not an all-time-worst data breach, was a frustrating reminder of the unreliable state of security on corporate networks," reported *WIRED*.

A GDPR CHECKLIST FROM THE LONDON PERSPECTIVE

by Jonathan Armstrong, Partner, Cordery

There's been lots of talk about how GDPR has upped the game with data breaches. The basic obligation to keep data secure has not changed much from pre-GDPR days. What has changed is reporting, enforcement and consequences — the much talked-about fines of 4% of global revenue or €20m. In fact, for security breaches where there's a failure to report in time the fine can be 6% or €30m. Enforcement is on the rise, too, with more than 2,500 actions in the EU to date.

What does GDPR say about data security?

Most of the GDPR requirements relating to data security are contained in three articles of the GDPR: Article 32, which deals with the security of processing; and Articles 33 and 34, which deal with breach notification.

Making sure that data is secure is one of the cornerstones of the new rules. To do this, GDPR introduced two new security breach reporting requirements — reports to the regulator and to those affected. There is wide definition of data breach under the GDPR — it includes destroying the data, losing it, altering it or improperly disclosing it. A data breach can include data in transit or data at rest.

GDPR requires an organization to put adequate technical and organizational measures (TOMs) in place to protect data. Some of these TOMs could include:

- Systems and processes to make sure the data stays confidential;
- Systems and processes to make sure that the data can be restored if there is an incident; and
- A process for regularly testing and assessing the measures you have put in place.

GDPR has also made it easier for civil actions in the EU, too. We've seen some interesting cases issued since GDPR came in and this, too, is likely to be a real point of pain for corporations going forward.

What type of data breaches are we seeing since GDPR came in?

It's pretty clear that most (if not all) organizations in the EU have seen a data breach since GDPR came in. Not all data breaches have to be reported but even some that are fairly small, do. At Cordery we've seen breaches of all shapes and sizes. There's been a real trend for vulnerabilities in some systems, particularly in Office365, to be exploited on an industrial scale usually to dupe corporations or their debtors out of money. The greatest cause of data breaches, however, is still human error. For example, in Ireland in the first year of GDPR, some 83% of data breaches involved some form of unauthorized disclosure. Seven percent involved data lost or stolen — whether on a device or hard copy — the same percentage as the number of cyberattacks. So, while much of a corporation's effort is aimed at the "enemy outside," it's the "enemy within" — whether that be poor training, poor awareness or disgruntled employees — that's responsible for by far the majority of data breaches reported.

What do organizations need to do?

Institutions need to have in place a system to triage data breaches at pace and in volume. They'll need to make sure that everyone in the organization knows the need to report a breach quickly and they'll need to have a way of asking the right questions at the right time to determine severity. For the most serious breaches, they'll need to get the team together to respond – that will include the technical team, legal and compliance and PR experts to manage external relations.

They'll need to consider reporting obligations quickly — in less than 72 hours if GDPR is in play. And they'll need to invest in remediation and mitigation whether or not a regulator is involved. Technology can be part of the answer — systems like Cordery Breach Navigator can take some of the pain away but practice is key, too. We know that organizations that rehearse a data breach fare better when one happens. Breaches are a "when not if" so invest the time to get prepared.

Former Department of Homeland Security Secretary Tom Ridge, now chair of Ridge Global Cybersecurity Institute, argues that protecting against cyber incidents is *everyone's* responsibility, from the people in the boardroom to entry-level employees. "Board members who are not as experienced with cybersecurity need to see it at the forefront of financial risks that could impact their bottom line," says Ridge. "We need to have more information-sharing and more conversations about cyber risk at the board level, and not just within companies' IT departments."

How can companies keep their board members attuned to the risks inherent in disruptive communications without intimidating or depressing them?

The answers aren't easy, but there *are* constructive steps that perceptive companies can take to keep board members plugged in.

First and foremost is to ***provide board members with a steady diet of articles and expert commentaries on the changing cyber climate***. Don't saddle them every other day with a 100-page treatise on the latest cyber hack nightmare. That will turn them off. Instead, e-mail or text them quick and easily-digested news summaries and samples of how a nasty hack was averted, or on the flip side, how company X was hurt by a sluggish response to a cybercrime.

INCREASING FOCUS ON CYBERSECURITY AND DATA PRIVACY AND THE HODGEPODGE OF REGULATORY SCHEMES

by Marcus Asner & Junghyun Baek, Partners, Arnold & Porter

Regulators in the United States increasingly are focusing their efforts on cybersecurity and data privacy issues. But, somewhat surprisingly in this day and age, we still do not have a comprehensive federal regulatory regime covering cybersecurity and data privacy, so each agency is left to come up with its own regulations and guidance. To make matters worse, most of the 50 states also have their own unique set of relevant laws. All of this creates a mind-boggling challenge for companies, as they struggle to navigate the complex and confusing hodgepodge of regulatory schemes.

The Federal Trade Commission (FTC), as a de facto privacy regulator, continues to actively exercise its enforcement authority. The FTC's role continues to evolve. In 2019, for example, the FTC changed some of its practices relating to enforcement orders, increasing third-party assessor accountability and requiring data security considerations to be elevated to the board level.

Other federal agencies also are jumping into cybersecurity. The Securities Exchange Commission (SEC) and other financial regulators are also focusing on cybersecurity issues, zeroing in on cloud services during company audits. The SEC recently published a report containing staff observations on cybersecurity, while the National Security Agency (NSA) published a guidance on mitigating vulnerabilities in cloud services.

There also is an increasing focus on data privacy and national security. Under a final rule adopted in January 2020, certain foreign investments in a U.S. business that deals with sensitive personal data of U.S. persons trigger a mandatory declaration requirement. And the Committee on Foreign Investments in the United States may block and has blocked certain transactions relating to sensitive personal data when it sees a national security threat. Similarly, in late 2019, the Department of Commerce issued a proposed rule on Information and Communications Technology and Services (ICTS) Supply Chain that would allow the Department to assess certain ICTS transactions and potentially block a transaction for national security reasons.

Adding to the jumble, states — in particular, California and New York, but also many others – are increasingly active in cybersecurity and data privacy space, which adds another layer of complexity for companies trying to comply with the law.

All of this creates a dizzying mix for companies working hard to comply with the various regulatory schemes. But data and computers pervade the modern-day business world. So, unless or until Congress passes some sort of nationwide regulatory fix, companies have no choice but to stay on top of the legal landscape, and learn how to navigate the confusing hodgepodge of regulations that may apply.

When a respected business outlet runs a story about the dangers inherent in disrupted communications, make sure your board members see it — with key passages highlighted. That way they'll be less shocked if and when the hazards hit *you*. And perhaps they'll be more inclined to help you undertake preventive measures *now*, during peacetime, and not wait until it's too late.

Second, ***consider adding board members to internal task forces on your areas of greatest vulnerability***. They'll see first-hand how seriously risk management is being handled by the company. And they'll develop a greater appreciation for how rugged the real world of disrupted communications can be these days.

Third, ***show your board members the efforts you're making to strike down the silos***. When a disrupted communications crisis hits, you're going to need everyone on board right away: from the general counsel's office and public affairs to the folks in information technology and human resources. If they haven't worked together in a crisis environment — even a simulated one — it could lead to a lack of trust and backbiting.

Managing risk these days is managing disrupted communications — and the way-too-easily disrupted world that comes with it.

section

06

Should We Empower Companies to Retaliate Against Hackers? Here’s What Experts Are Saying

Reflecting on the past decade, this much should be obvious: Regulation cannot keep up with the pace of technological change. This makes cybersecurity — the thin wall that protects everything from our identity and intellectual property to our financial capital — an exceedingly crucial protective barrier in our society and economy.

As a communications strategist who advises companies besieged by cybercrime, I can attest that those protective walls are getting violated far too often. Since 2017, the rate of identity breaches has increased more than 400%. On top of their often-disabling impact on brand reputation, data breaches exact painful financial costs. Equifax's infamous breach cost the company more than a half-billion dollars. Cybersecurity costs financial services companies, on average, some $2,300 per employee, a number that has tripled over the last four years.

But can companies and their board members be too zealous in fighting cybercrime?

A recent bipartisan bill, the Active Cyber Defense Certainty Act (ACDCA), offers to "allow use of limited defensive measures that exceed the boundaries of one's network," giving authorized entities the legal authority to "retrieve and destroy stolen files," "monitor the behavior of an attacker" and "disrupt cyberattacks without damaging others' computers," among other things. Is the ACDCA a realistic antidote to cyber fraud? Or, by empowering companies to retaliate against hackers, is ACDCA's solution potentially as corrosive as the problem? A walkthrough of what the experts have been saying on this subject may prove instructive.

The debate over how far to go in strengthening cybersecurity is likely to roil corporate boardrooms and legislative chambers.

Argues Paul Ferrillo, a Greenberg Traurig partner and the author of *Navigating the Cybersecurity Storm: A Guide for Directors and Officers*, "ACDCA's term of art, 'active cyber defense,' is in the eye of the beholder. Does it mean that under ACDCA a company is entitled to install a purely defensive measure such as a 'honeypot' to figure out who is attacking its network — and from where? Or, as some observers say, does active cyber defense enable a company to 'hack back' against an attacker's computer system? Or does it depend on certain contingencies? In my view, ACDCA as presently constituted is not explicitly clear on this point."

Still, Ferrillo believes that a properly conceived ACDCA has the potential to become a constructive instrument in the battle against cybercrime. Active defensive measures like honeypots and machine-learning solutions, if correctly deployed, can be critically important tools, he notes. Still, before any institution seeks to hack back against an adversary, it would be wise to consult with experts and attorneys.

Cybersecurity expert George de Urioste, the chief financial officer of 4iQ, likens a company's efforts to protect its cyber assets to a property owner using video surveillance technology to safeguard their possessions.

"It is generally accepted in our society that a property owner has the right to 'see' anyone on their premises and seek identification," de Urioste says. "Should a crime occur, video is often used to establish attribution of criminal activity to share with law enforcement. I would strongly advocate for the ACDCA, at a minimum, to affirm a property owner's right to unmask the cybercriminal via 'identity threat intelligence.'" This aligns with the explanation of the bill offered by lawmakers, who wrote in a FAQ document that it would allow entities to "establish attribution of an attack" and "monitor the behavior of an attacker."

"Every cybercriminal knows the effectiveness of surreptitious activity revolves around masking their identity," explains de Urioste. "If we can fight back by bringing some sunshine onto the dark web, a major first step of proactive defense will be established."

The impetus behind ACDCA, de Urioste says, points to "meta issues about economics and safety. Digital criminal activity grows exponentially; it will be with us forever.

Private leaders see the economic impact; they constantly need to increase their cyber defense spending. Public leaders increasingly hear the outcry from consumers who are harmed by digital breaches. They want private leaders to assume greater responsibility and accountability. It all adds up to an urgent moment for greater empowerment, as intended by ACDCA principles."

Given the enormity of these risks, notes risk management expert Kenneth J. Peterson, the Founder and CEO of Churchill & Harriman, Inc., companies have an obligation to explore a range of aggressive options and contingencies as contemplated by the ACDCA.

"All offensive tactics meant to collect actionable threat intelligence executed within the law and in accordance with regulations should be on the table and considered," Peterson says. "Boards are frustrated that the investments they've made to improve their enterprise risk posture have not wholly protected them."

Jon Frankel, a cybersecurity attorney and shareholder at the tech and privacy law firm ZwillGen, contends that the authority embodied in those ACDCA principles "is only as great as a company's ability to accurately attribute an attack and avoid damaging other computers. Companies must understand that they cannot deploy active cyber defense measures without correctly attributing the attack. It seems unlikely a company will know without any doubt who the perpetrator is, especially because hackers are good at concealing their identities by attacking through proxy servers or a series of compromised computers that belong to innocent third parties. Companies must ensure that they have accurately attributed an attack to avoid targeting innocent third parties and/or violating international law."

RANSOMWARE INCIDENTS REQUIRE NEW COMMUNICATION STRATEGIES

by Craig Hoffman, Partner, BakerHostetler

Just as organizations started to get a handle on how to communicate about a data breach, ransomware changed the landscape. Response communication strategies now have to address the substantive content and the logistics of disseminating a message without the availability of the computer network. Just like the early days of communications about incidents involving theft of data, you can look back at early responses to ransomware incidents to find lessons to improve your preparedness.

The surge in ransomware attacks started in late 2018; organizations were forced to learn how to communicate about a security incident that caused business continuity impacts. Effective ransomware attacks simultaneously encrypt most of the devices across an organization. The attack shuts down email, phone systems, point-of-sale devices, machines that run manufacturing, ERP systems, file shares, individual devices, and backups. It is equivalent to all of an organization's devices disappearing. Organizations, without warning, are forced to figure out how to communicate to employees, customers, and other key stakeholders about when operations will be restored, sometimes without being able to use their email system. And often the timing of restoration is uncertain. Organizations can be resilient and resourceful, and individual and business customers can be understanding, in the short term. But the outages and service disruption can last for days or weeks. Internal and external patience wears thin. If misleading ("Our website is down for routine maintenance") or overly ambitious ("Service will be restored in two hours") statements are part of the picture, maintaining relationships after the incident can be challenging.

In late 2019, some threat actors decided to up the ante by adding an extortion demand to the ransom note — before we encrypted data on your devices we took some of your data and will release it unless you pay — to increase pressure on organizations to pay the ransom. The one-two punch of a business continuity impact and potential theft of data with a threat to release the data publicly if the ransom is not paid is forcing organizations to adapt again.

There are steps you can take to reduce the likelihood of a ransomware incident. Building an incident response plan that accounts for a business continuity incident, doing tabletop exercises to test and improve response capabilities, and identifying in advance the third parties you will engage to work with you in the event of an incident are all good steps to take to improve your ability to effectively respond. And if an incident does occur, leverage those advisors to take advantage of the "compromise response intelligence" they have gained to get the right outcome for your organization.

A muscular undertaking demands a paradigm shift in approach. De Urioste advocates cyber vigor, a commitment by companies to stay a step ahead of bad actors. In my view, cyber vigor means worse-case scenario planning on the front end, and an equally smart range of tactics following an actual attack.

In a blog post outlining the tenets of cyber vigor, de Urioste offers a three-point prescription. First, know your adversary. What are your company's digital "greatest hits," and who would profit from pilfering them? "If you don't know," he writes, "you are flying blind." Do your homework and don't be afraid to let your imagination — and your crisis contingency scenarios — run wild. Second, determine your compromised data, including that which has been stolen or leaked from your suppliers and vendors. Third, establish the vulnerability of your employee attack surface. It's the consumer data breaches that grab headlines and cause the most handwringing, but less-publicized employee password breaches often trigger the biggest headaches for companies.

Company accounts hold the potential to "unlock valuable corporate data, leaving the door wide open for adversaries to walk out with whatever trade secrets they want," de Urioste warns.

RANSOMWARE: REWARDS OR RESOLUTIONS?

by Mark Singer, Cyber and Tech E&O Claims Manager, Beazley-London

Cyber and ransomware attacks are proliferating, disabling computer systems of corporations, municipalities, schools and police departments and causing significant associated costs to recover from attacks.

Since 2014, we have seen an exponential rise in ransomware attacks, jumping from 11 in 2014 to 336 in 2018 and 775 in 2019. We continue to see a steady stream in terms of volume in 2020.

In recent years, cyber insurance sold by domestic and foreign companies has grown into a $7 billion-plus annual market in the U.S. alone. With the rise in the frequency of attacks, the sums that are being demanded by cybercriminals have also expanded exponentially, with seven- or even eight-figure demands not being unusual.

Basic cyber hygiene is key to avoiding a ransomware incident, although no organization can be entirely safe. Organizations should focus on incident response, disaster recovery and business continuity. In particular:

- Ensuring that backups are segregated from the rest of the network to shield them from an attack's path of destruction.
- Regularly testing the organization's recovery from backups to ensure they are viable should they need to restore the organization's data following an attack.
- Knowing how long the restoration process will take so their stakeholders are able to make informed decisions about whether to pay a ransom and how best to mitigate a potential loss.

It is critical to have the right measures in place such that, if disaster does strike, the organization is well placed to respond.

Beazley helps policyholders struck by ransomware to address their incident response, cyber extortion, and data recovery. Our Beazley Breach Response (BBR) insurance policy has been specifically designed to minimize overall business disruption that can come from such incidents. BBR vendors are vetted industry leaders with an excellent track record of understanding complex cyber events, addressing ransom demands, helping with disaster recovery and working with insureds to make the big decisions, quickly. Ultimately, the decision making is in the hands of our insureds. We make sure they have access to the vendors to assist making the best decision for them and in line with regulatory compliance.

Beazley aims to help its insureds achieve their main objective; to mitigate risk and get their businesses back online. Moreover, while many notable, high-profile cyberattacks predate the cyber insurance market, we have seen a rise in indiscriminate attacks that are growing in technical sophistication. At Beazley, we are committed to delivering on our promises to help our cyber policyholders avoid and respond to these situations through education and access to our expert network.

In peacetime the solutions are more mundane. Among the strategic communications elements that institutions should prepare in advance of any cyberbreach or cybercrime are:

- Sophisticated holding statements approved by the counsel's office;
- A compelling protocol to respond to earned media inquiries;
- A detailed social media response strategy, based on sample scenarios, "conversations," and responses;
- Talking points to address customers, employees, investors, media, and other key constituencies;
- A responsive email to general customers and business partners;
- Comprehensive instructions for identity theft monitoring service enrollment; and
- A website FAQ page.

In the future, a more proactive approach will likely become the norm — and legislative prescriptions are starting to move in that direction. Playing "whack-a-mole" in the wake of an attack won't sufficiently protect the brand or business operations.

Critical Technologies: Your Company's Surprising Supply Chain Exposure on Huawei

U.S. corporate leaders who believe that the firestorm surrounding Huawei won't singe their companies might want to think again. Remember: the Trump Administration, articulating national security concerns, has imposed a trade blacklist on Huawei and *all* its subsidiaries, a maze of networks that spreads across 170 countries and reaches a third of the world's population.

Your company may not be directly engaged with Huawei or its affiliates — *but there's a strong likelihood your supply chain is.*

As they say (phonetically at least) in Mandarin, *zhù nĭ hăo yùn.* It means "good luck." If your subsidiaries and affiliates have Huawei entanglements, you may need it.

So will the rest of us. In its zeal to defend national security (and gain political leverage on the escalating trade war), the Administration has already inflamed global trade tensions and is potentially ceding American leadership in critical technologies. We can all appreciate both the political calculus and significant risks of trade wars, particularly this one with China, but even more serious is the acute and long-term concern of a critical technologies gap. The former risks recession and has already caused a draconian investment decline by Chinese companies in the U.S.; the latter risks a second-place or worse finish in the current technology race, on which hinges global hegemony, defense, and business leadership. We cannot even begin to imagine a world where America is not at the forefront of technological innovation.

Like it or not, U.S. companies and their supply chains are thoroughly dependent on Huawei and its leviathan supply chain — and vice versa. Motorola Solutions (which a decade ago contemplated acquiring Huawei) and its subsidiaries do an immense amount of business with Huawei and its subsidiaries. Those relationships cannot be ended overnight.

The Administration's action puts Motorola and a host of other companies in an uncomfortable and potentially untenable position. What's the current state of play for U.S. companies vis a vis Huawei? It's a bit murky — and it's not likely to get clearer anytime soon.

The Administration in May 2019 declared that U.S. companies were forbidden to supply hardware or software to the many devices manufactured or distributed by Huawei. In late spring, Google announced that it would comply with the White House's decree — a move that was soon followed by a Commerce Department ruling that softened the prohibition against trade with Huawei.

Commerce determined that Google and other U.S. tech companies could offer software updates for current Huawei products but would be proscribed from engaging in similar trade with *future* Huawei products, including the Mate X, a foldable phone that the Chinese behemoth has been developing for years in direct competition with South Korea's Samsung.

Confused? You're not alone. And the confusion has gone global.

"The rules governing trade sanctions often are extremely confusing, and that can pose significant challenges for clients who are trying hard to comply," contends Marcus Asner, a former assistant U.S. attorney in the Southern District of New York who co-chairs Arnold & Porter's Anti-Corruption Practice Group.

"To add to the mix, we're also seeing a ramped-up enforcement environment in the trade sanctions area, with a whole slew of regulators focused on these issues. All of this increases the risk and can lead to a great deal of anxiety among clients engaged in cross-border trade," he says.

Certain foreign-based tech providers that rely on "U.S.-origin technology" for their products and services aren't sure but suspect they could be affected by the

Administration's Huawei ban. British chip designer ARM is now owned by the Japanese telecom giant Softbank, which, not surprisingly, does considerable work with Huawei. Without divulging details, ARM announced this summer its desire to comply with "all of the latest regulations set forth by the U.S. government."

At least ARM appears to have the semblance of a plan. Careful monitoring and contingency planning are precisely what companies seeking to reduce their exposure on Huawei need to embrace, argues Mark D. Cowan, a veteran of several White Houses and the CEO of Potomac International Partners.

"It is vital for companies to remain aware of the behind-the-scenes actions that Commerce is taking on Huawei, as well as the motivations behind them," Cowan says. "Companies must understand how the government defines national security in such cases to effectively argue that there is *not* a national security threat in using Huawei in their supply chain. To avoid getting caught in the anti-Huawei web companies must show themselves to be cooperating with the government, being transparent about where Huawei does fall in their supply chains and communicating clearly about what kind of risk this might pose to U.S. national security."

CYBER DISSONANCE — TACTICAL MANAGEMENT OF A STRATEGIC RISK

by Lynne Burns, Global Head of Marketing Communications, Cyber, Marsh JLT Specialty

Cyber threats are now viewed as a critical risk by most organizations, but many still pursue a tactical approach rather than adopt a formal risk management strategy.

In the 2019 Global Cyber Risk Perception Survey conducted by Marsh and Microsoft, 80% of organizations surveyed ranked cyber threats as a top-five risk, a large increase from 67% in 2017. Notably, however, confidence in cyber resilience — the ability to understand, prevent, and respond to cyberattacks – fell across the board, with one in five saying they are "not at all confident" in their cyber management capabilities.

The decline in confidence may stem in part from the fact that, despite soaring corporate cybersecurity budgets, the economic impact of cybercrime continues to rise.

This concern/confidence gap may also reflect another key finding: most firms are *not* applying a rigorous, disciplined risk management framework to cyber threats as they would for other critical business risks. Many struggle to create a strong cybersecurity culture with appropriate governance, prioritization, management focus, and resources. This places organizations at a disadvantage in building cyber resilience and in confronting the increasingly complex cyber risk landscape.

For example, for most firms, information technology and information security functions continue to be viewed as the primary owners of cyber risk management versus broader ownership shared across other key functions such as risk management, C-suite leaders, and the board. In 2019, 88% of companies named IT/InfoSec as a main owner of cyber risk. Only 49% of organizations cited risk management as a primary owner of cyber risk — a dissonant response given the functional name.

The fact that IT is named as a primary owner nearly twice as often as risk management points to a mistaken view of cyber risk as primarily a technology issue, rather than an enterprise risk with potential to inflict potentially significant financial and operational damage.

The question of who leads cyber risk management is just one area in which there is dissonance between an organization's perceptions and actions.

Another area is time: despite the high level of concern about cyber risk, only 17% of executives spent more than a few days over the past year focusing on it. Even among IT respondents, 30% said they spent only a few days or less on cyber risk.

Investment decisions are another area that reflect a reactive approach to cyber risk. Only 30% of organizations employ quantitative methods to measure and express their cyber exposures — so the large majority use vague, descriptive methods, which don't yield reliable data. Moreover, 26% say they have no assessment method at all!

While the range and type of actions necessary for effective cyber risk management varies by company, the best practice for all organizations, regardless of industry or size, is to apply a rigorous risk management framework to cyber risk as they do for other strategic risks, incorporating planning, training, risk transfer, and response rehearsal.

Sage advice, but companies also need to factor both the Administration's political machinations and Huawei's persistent tone-deafness into their calculus. William Plummer, a former vice president in Huawei's Washington office, said that "when substantive and informed experts suggested something that should be done, it filtered way up into some Mandarin star chamber and came back as something we didn't recognize."

For Huawei, with its historical ties to the Chinese government and military, the breakdown in U.S.-Chinese relations, and the leaked documents of its potential involvement with North Korea in violation of U.S. export controls, the challenges are significant.

Huawei has strong cyber security, economic, legal, and political arguments to make, and they have many allies who would echo them, but so far, they aren't making them or letting their American surrogates chime in. Economically, Huawei may not need the American market, but politically, it can't run the risk of permitting one foreign government to undermine its global expansion.

Zhù nǐ hǎo yùn. All the protagonists in this convoluted debate could use some good luck. And some careful thinking before they do something we'll all regret.

section

08

For Smart Companies, There Is Business Life After Cyberattacks

It is, perhaps, a sobering sign of our times that cyberattacks — data breaches or ransomware assaults — don't automatically undermine a company's value as either a business or as a partner.

While studies suggest that, on balance, the share value of breached companies underperform the market, corporations with strong fundamentals have not only recovered from cyber muggings but flourished. JP Morgan Chase and Home Depot are just two examples of corporations that were victimized by lethal cybercrime and gone on to realize even greater success.

The market tends to discount high-profile cyberattacks, perhaps because the business community sees companies that have weathered such assaults as zealously determined *not* to let them happen again. In advising corporate CEOs and general counsels, I often point out there are only two kinds of companies: those that have been hacked — and those that are going to be hacked.

It's not unlike the old saw about the brakemen that coupled and decoupled rail cars a century ago. It wasn't hard to pick out the wizened veterans; they only had eight or nine fingers. Their (literal) hands-on experience may have left them permanently scarred — but also wise and cautious. They made for the best brakemen because *they understood the cost*. Their less experienced colleagues may have had all their fingers intact, but they weren't trusted the way the seasoned men were.

No one who's tried to plug a cyberbreach is missing fingers, but — take it from someone who's counseled companies through hundreds of cyber assaults — they've probably missed a few nights' sleep. Since cyberattacks often affect huge swaths of customers, vendors, suppliers, and other stakeholders (not to mention attract tough media coverage), they're exhausting to quell. But the quelling must be done the right way — aggressively and forthrightly.

Ask Charles Kallenbach, an attorney who earned his cyber spurs as counsel to Heartland Payment Systems during HPS' notorious 2009 hack, one of the most malevolent data breaches in history. If the TJX hack of 2005 compromising some 45 million records was the first significant cyberattack, then Heartland marked the start of Cyber 2.0.

"We felt we were well prepared for an attack, and we had a number of important defenses in place. But the hackers were able to exploit a very small weakness — and wreak havoc. Heartland's stock price per share plummeted from the high teens to $3.50, and I was hyperventilating into a paper bag," says Kallenbach.

Heartland was targeted a decade ago by sinister hackers who knew what they were doing and who infiltrated dozens of other publicly traded companies. After the attack, the company went on the offensive, instituting a range of safeguards to deter future assaults. Heartland was sold to a payments industry competitor in 2016 — for a healthy $100 per share.

"For companies that use and guard valuable personal data, best practices should include expanding information security capabilities, such as plugging their vulnerabilities, expanding their data loss prevention program, increasing their data breach insurance coverage, all while retaining crises communications experts, as well as attorneys who specialize in data security before being attacked. Companies can start with an audit by an information security firm that can point to the most obvious data security lapses. It's also a good idea to make sure that outside counsel retains the data firm to protect attorney-client privilege for their report," Kallenbach prescribes.

Adds Jonathan Armstrong, a data security expert at London-based Cordery, "Cybercrime, like war and taxes, is an inevitable fact of life. We need to prepare for *when* not *if*. That's harder than it used to be as the attacks are more sophisticated but also since today's corporations aren't islands — they rely on vendors and partners to do what they do. You need to try and control your data – whether it's on your systems or a third parties – but you also need to prepare for the inevitable. That means proper war gaming so you're battle-ready when the next breach happens."

Publicly traded companies (and their stock prices) naturally get the most attention during and after cyber assaults, but privately held companies that bounce back from

NEXT GENERATION ENTERPRISE RISK MANAGEMENT DUE DILIGENCE

Kenneth J. Peterson, Founder and CEO, Churchill & Harriman

Across industries, governments, and the regulatory landscape, required levels of enterprise risk governance are increasingly critical at a global level. Industries have frequently looked to the financial services industry for emerging risk management models to produce broader, deeper levels of due diligence evidence to test and validate their own resilience and those of their business partners.

For all interested parties, there is good news. A new tool is now available to help all, from small organizations to the largest multinationals whose infrastructure is designated as "critical" to test and report on their resilience.

The Financial Services Sector Coordinating Council (FSSCC) has developed and now released a tool they call the FSSCC Cybersecurity Profile. It was devised in response to a survey of chief information security officers from financial institutions that indicated nearly 40% of their time was spent on compliance and reconciling competing, duplicative, redundant, and inefficient cybersecurity supervisory examinations.

The Profile is aimed at saving time and aggravation. It provides a framework that integrates widely used standards and supervisory expectations to help guide financial institutions in developing and maintaining cybersecurity risk management programs. It is the result of two years' work and collaboration among financial institutions, trade groups, and government agencies.

Spearheading the effort was FSSCC, buttressed by the American Bankers Association, Bank Policy Institute's technology policy subdivision BITS, Futures Industry Association, Global Financial Markets Association (and its member associations, the Association for Financial Markets in Europe, the Asia Securities Industry & Financial Markets Association, and the Securities Industry and Financial Markets Association), as well as the Institute of International Bankers.

COMBATING BEC, EAC AND APP SCAMS

Peter Yapp, Partner, Schillings

Business Email Compromise (BEC), Email Account Compromise (EAC) or Authorized Push Payment (APP) scams (sometimes also known as "CEO fraud") are the scourge of boardrooms around the world. If there was ever a type of fraud to engender angst, this was it. While Ransomware has got all the column inches in the press, BEC/EAC and APP scams have netted the most amount of money for cyber criminals. And the figure is rising year on year. In the UK alone the value of APP frauds has risen from £354m in 2018 (over 84,000 cases) to £413m (over 108,000 cases) for the rolling year ending June 2019 (figures from UK Finance).

In September 2019, the FBI, based upon victim notifications between June 2016 and July 2019, reported the value of domestic and international incidents as $26bn (over 166,000 cases).

AIG released their own statistics in July 2019 showing that in 2018, BEC accounted for 23% of cyber insurance claims received from Europe, the Middle East and Asia. Ransomware stood at 18%.

In simple terms, an example of a BEC is when you receive a spoofed email asking you to urgently pay money to a new bank account.

There are two main ways that the fraudsters get a foothold in your system: Brute-force password attacks (often helped by previous breaches, reported at https://haveibeenpwned.com) and phishing attacks that entice the user to disclose their username and password.

Schillings recommends the following to avoid falling victim to a BEC/EAC or APP scam:

- Use two-factor or multi-level authentication for your main personal / critical business email accounts
- Be suspicious of any emails requesting fast actions, especially if not following your normal procedures
- Make a phone call to check changes of bank account
- Monitor bank accounts on a regular basis for irregularities e.g. missing deposits
- Verify the email address used to send emails, especially when using a mobile device, ensuring the senders email address matches who it is coming from

attacks deserve credit, too. One of them is InsynQ, a Washington State-based cloud-hosting service that partners with accounting and other professional service firms.

InsynQ was hit by a withering ransomware attack from anonymous sources in July of 2019. To contain the spread of malware, InsynQ essentially shut down its network, a move that precluded customers from accessing their accounting data for three days. It wasn't an easy decision, but by taking down its network, InsynQ may well have stopped a contagion from destroying the company — and damaging its clients, too.

The cybercrime containment lessons that InsynQ learned on the fly, and the technology and business solutions it devised may stand them in good stead. In early September, the company announced it was adding a heavy hitter as chief information security officer, Michael Marrano, author of *The Human Firewall Builder: Weakest Link to Human Firewall in Seven Days*. Marrano's addition could make them a safer and more reliable partner than, say, a competitor that has never experienced an attack.

No one wants to lose their fingers or be forced to hyperventilate into a paper bag to get through a crisis. Smart companies that gets bruised in a cyber fight may end up being stronger for it. But only if they learn their lessons and take steps to minimize the prospects of it happening again.

LITIGATION RISKS LURKING WITHIN THE CALIFORNIA CONSUMER PRIVACY ACT

by Donna Wilson and Scott Lashway, Co-Leaders, Privacy and Data Security, and Matthew Stein, Special Counsel, Privacy and Data Security, Manatt, Phelps & Phillips, LLP

The California Consumer Privacy Act (CCPA) has been the most notable development in privacy and data security law in the U.S. in recent years. While various provisions of the act continue to be debated by legal counsel, companies can be sure that more litigation is coming to California.

CCPA's applicability and consumer rights make it a top priority for anyone doing business with California consumers; companies rightfully have been focused on their proactive compliance initiatives. Today, in-house counsel must remember that the CCPA also demands, as a part of these proactive efforts, a qualitative and quantitative evaluation of litigation and regulatory risks — including both open and hidden litigation risk — requiring immediate attention.

Clear litigation risks are written directly into the CCPA — most obviously, the private right of action for individuals when a business suffers a data breach. Under CCPA, a consumer must show that his or her unencrypted or nonredacted personal information was subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the company's failure to maintain reasonable security procedures. Interestingly, plaintiffs may argue that the statutory language of the CCPA addressing the civil action presents a "duty to implement and maintain reasonable security procedures and practices." Of course, data breaches have always sparked litigation risk, but they have been limited by the need to show actual injury and damages.

Under the CCPA, plaintiffs will attempt to pursue statutory damages ($100 to $750 per incident, per customer) or actual damages (if greater), and injunctive relief in case of breach. There will be litigation surrounding whether a plaintiff can pursue statutory damages alone, which state courts in other jurisdictions (under other privacy statutes) have rejected. Given this, expected damages sought by plaintiffs potentially could be staggering. In 2016, one company was accused of exposing personal information of more than 20 million individuals and ultimately reached a national settlement with state attorneys general for $148 million; the California user share was approximately $18 million of that. Accounting only for California users, the company could have faced between $240 million and $1.8 billion under the CCPA.

Companies should expect the plaintiff's bar to be aggressive in testing different statutes — related or not — to assert CCPA rights violations. Indeed, if the California attorney general's draft regulations become law without significant changes, companies' potential exposure to these types of second-order claims may only increase: The draft regulations arguably increase disclosures that companies may be required to make.

Ready or not, the CCPA and an eager plaintiff's bar are here. Companies should be qualifying, quantifying and minimizing their litigation and regulatory risks immediately and keeping an eye on early cases brought under the act in 2020.

Companies Must Strengthen Cybersecurity Amid WFH/COVID-19 Crisis

By Phyllis Sumner and Richard Levick

As tens of millions of workers transition to remote work environments in the wake of the COVID-19 pandemic, the cybersecurity weaknesses of America's current remote work ecosystem have become apparent. Criminals and nation-state actors have been presented with an exponential growth in access points to pressure and penetrate corporate systems, and the scramble to secure systems from a menagerie of devices, networks, and enterprise networks leaves many companies vulnerable to attack, theft, or exploitation.

The FBI has stated that cyberattacks have drastically increased this spring; ransomware, malware, general email scams, and malicious phishing expeditions abound — some cybercriminals have even taken to providing fraudulent COVID-19 resources via apps or other downloads to target both individual and corporate systems. While these assaults have happened in an astonishing variety of industries and against a diverse array of targets, areas hit hardest by COVID-19 are the most vulnerable. These crimes can be extremely profitable, often lack sophistication to execute certain techniques, require a remarkably low financial commitment, and are difficult to attribute to any particular parties.

Considering this combination, it becomes clear that this threat will be a persistent one. As corporations build out the interoperability of their corporate systems with personal technology — via either increased compatibility with personal mobile devices or other methods of accessing company databases through home computing networks — the probability of inadvertently introducing vulnerabilities into corporate systems increases. The ability to rapidly identify vulnerabilities and detect breaches will become paramount to the successful operation of any company.

The longer this remote work period persists, the more sophisticated and targeted the actions of criminals and bad actors will become. Considering these technical vulnerabilities in conjunction with the increased ease of exploiting human vulnerabilities (i.e., it is more difficult to exert direct control over how employees use their computer systems in a remote work environment), it is critically important to increase vigilance in adopting and maintaining proper cybersecurity hygiene.

Despite the increased risks and the uncertainty of security protocols constructed on an ad hoc basis, working remotely is a mandatory aspect of life for tens of millions of Americans. Corporations must find a way to protect the safety and security of both their employees and the public writ large by ensuring that remote work systems are secure enough to operate for as long as needed until a significant portion of the American workforce can return to work safely. This effort requires vigilance, flexibility, and a keen awareness of the threat landscape, but corporations that can create and foster a secure working environment now will be far better situated to protect themselves from cybersecurity threats in a post-COVID working environment.

A starting point for any organization must be a thorough review of data storage — storage hardware, storage methods, and access control. As myriad new devices are granted access to corporate systems, the need for the careful curation of access lists and data logs recording the time and manner of access grows. Monitoring and controlling access will allow organizations to reintegrate the vulnerable and potentially compromised assets that have been out of their direct control for extended periods of time.

Institutions also need to assess their cybersecurity insurance policies to ensure adequate coverage, as well as seeking to mitigate their third-party and supply-chain vendor risks. Increased utilization of remote work technologies and outside support systems will also require corporations to revisit and revise their vendor and supply chain risk management programs. As the web of contact with outside systems and vendors grows, existing cybersecurity procedures may also need to be overhauled. These may include Incident Response Plans, remote work and employee privacy policies, data privacy and security training materials, bring-your-own-device (BYOD) rules, data/record retention schedules, information security and acceptable use policies, and email and messaging standards.

Given the radical nature of the changes that are likely to take place, communication and education efforts are a necessary pillar of a successful transition. A combination of intensive contingency planning and aggressive outreach to employees, vendors, suppliers and stakeholders is recommended. Employees who have been working from home need to make their shared platforms, devices and databases less vulnerable to attack. It's not just the organization's cybersecurity that's at risk, but the privacy interests of the individual at stake in maintaining their personal and financial security from criminals and other bad actors.

Internal messaging related to cybersecurity must be clear, compelling, and consistent — whether in writing, in person, online, in a virtual training session, or in a video. After employees receive training, each should be required to pass a test to ensure they understand their new cybersecurity responsibilities. An ongoing Return to Work task

DATA EVENT DETECTION AND INVESTIGATION IN A REMOTE WORLD – WHAT ORGANIZATIONS CAN DO NOW TO ENSURE PREPAREDNESS

by Jim Prendergast, Esq., John Mullen, Esq., and Jennifer Coughlin, Esq., Mullen Coughlin

While it's a given that cyber criminals, human error, and reliance on data and information systems are here to stay, organizations are now facing the unanticipated possibility that remote work will be a long-term or permanent part of operations. Below are four steps organizations should take to best position themselves to investigate and respond to a data privacy event in a remote-work world.

1. ***Ensure your Incident Response Plan is realistic.*** Your Incident Response Plan should be short, responsive to cyber events, updated on at least an annual basis and contain business and personal contact information for the incident response team (and their backups), including contact information for your cyber insurance carrier and broker. It should allow for immediate alert of suspicious activity to technology, risk, and legal departments. It should NOT direct the engagement of, or reliance on previously engaged IT providers or the direct engagement of external incident response support vendors (other than counsel). It must be flexible enough to address varying cyber risks – which are constantly evolving — but inflexible enough to always provide for rapid response, data preservation, and engagement of appropriate incident response support providers at the earliest point of suspicious activity detection.
2. ***Understand the risks of remote work and operations unique to the organization.*** Remote operations create unique risks to the security of an organization's data and information systems. Some organizations seamlessly transitioned from in-person to remote operations. But we've heard plenty of stories of staff being told to purchase laptops or portable devices as the company wasn't able to provide prior to going remote. The introduction of new devices and new work environments are red flags for organizations. They should: (1) confirm access and audit rights to all devices connecting to the system or housing the organization's data; (2) conduct a review of new technical and legal risks to information and system security, including the heightened risk of phishing attacks, ransomware and social engineering; and (3) conduct additional employee training on device, information, and system access, use and security.
3. ***Understand challenges the organization will face regarding remote coordination of incident detection and response.*** If you've not conducted employee training since moving to a remote work environment, you must. Detection and reporting of suspicious activity and the ability to monitor systems usage while users are connected remotely are different from pre-COVID operations. Incident Response Plans often depended on staff gathering in a central location or conducting in-person investigations. Today, this ability to swiftly detect and immediately respond to suspicious activity is challenged.
4. ***Conduct remote tabletop exercises to ensure your Incident Response Plan is flexible enough to handle all types of events.*** Tabletop Exercises are important if you want to efficiently execute your Incident Response Plan. The key to successful and swift execution is practice. Employ several fact patterns — based upon recent cyber trends and risks unique to the organization. At the conclusion of the Tabletop Exercise, reflect on opportunities for improvement and effectuate them.

While we long for pre-COVID normalcy, there is no denying the immediate impact of COVID on organizations and operations. The long-term impact is unclear. Organizations will be best prepared to detect, investigate, and respond to data privacy events if they implement and repeat nos. 1 through 4 going forward.

force should be established — with input from a variety of institutional stakeholders, from communication and human resources to the general counsel's office and information technology. The communications elements of all cyber crisis response plans must be thoroughly overhauled to reflect current exigencies, then incorporated into drills and table-top exercises that engage everyone in the organization.

Supply-chain constituencies also need to be built out and tested in conjunction with the latest cybersecurity procedures. Once an organization's internal priorities have been addressed, it can begin reaching out to assure local and industry media, elected officials, and community leaders that it is thoroughly committed to identifying and mitigating cybersecurity assaults in this unpredictable and evolving environment.

The nature of the newly established remote work ecosystem means that cybercriminals have more access points and security vulnerabilities to exploit than ever before. To adequately address these emerging threats, corporations and institutional stakeholders must bring to bear a suite of innovative methods and tools to prevent compromise when possible and mitigate damage when necessary. While cybercriminal activity is inevitable, and emerging national security paradigms result in more sophisticated attacks than in the past, organizations which use this opportunity to implement strong, secure, and flexible cybersecurity practices will find themselves on solid footing to face the known threats of today, and the unknown threats of the post-COVID world.

Phyllis Sumner chairs King & Spalding's Data, Privacy, and Security Practice and is the firm's Chief Privacy Officer. Richard Levick, Esq., @richardlevick, is Chairman and CEO of LEVICK.

WHAT'S WORKING IN WASHINGTON PODCAST

Increase in Hacks on Businesses Force New Strategies

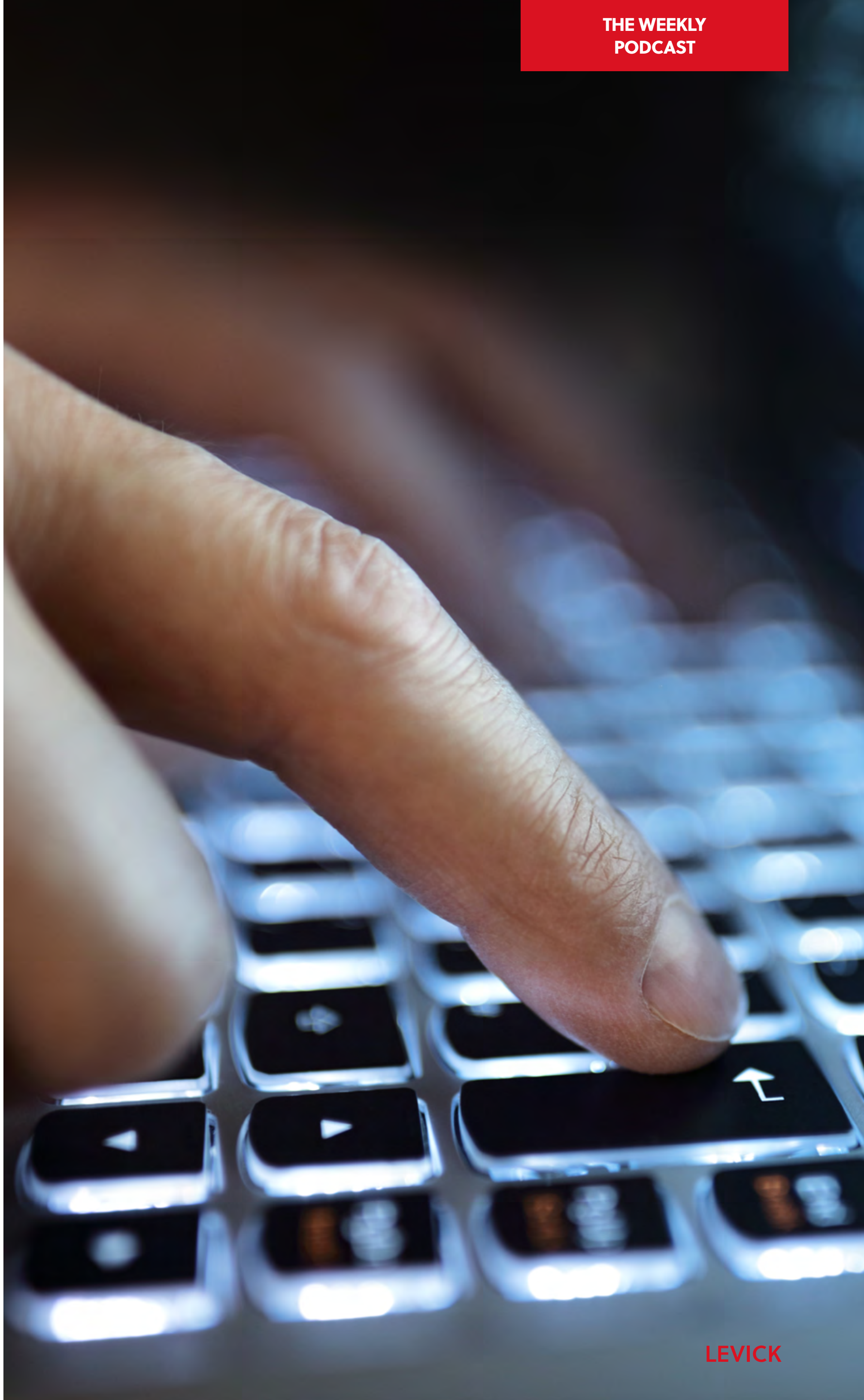
It's no longer a question of whether a company will be hacked, it's when. Richard Levick, founder and CEO of LEVICK, joined *What's Working in Washington* to discuss what companies should be doing during peacetime to prepare for a cyberattack.

READ>>

Digital Tools for the General Counsel

In this podcast episode of *The Weekly*, Carl Watson, General Counsel, Asia for Arcadis, discusses with Richard Levick the digital tools he has used at Arcadis to make them more efficient, release brain power and cut costs, all at the same time.

LISTEN >>



THE WEEKLY PODCAST

IN HOUSE WARRIOR PODCAST

The Changing Digital Economy and Cyber Risks

From Noise to Signal: Alberto Yepez, Managing Director of ForgePoint Capital and Chairman of the Board of 4iQ provides his view of upcoming cyber risks and challenges including the evolution of cyber criminal activity, the unique challenges of emerging markets, the impact of Covid-19 and how the digital economy is changing. Ian Lipner, chair of LEVICK's cyber practice joins the show with his own insights.

LISTEN >>

Resiliency

Resiliency with Paul Ferrillo, a partner at McDermott, Will & Emery and Ian Lipner, head of LEVICK's cyber practice. Paul addresses the need to think differently, build redundancies and plan for resilience in an age when what can happen will happen.

LISTEN >>

Cyber Breach

John Mullen, partner and co-founder of Mullen Coughlin — a law firm that handles more than 2,500 breaches a year — joins host Richard Levick and Ian Lipner, the head of LEVICK's cyber practice, to provide insight into what general counsels and others need to know about cyber hygiene and response.

LISTEN >>

Contact Tracing, Surveillance Software & Privacy

Ken Rashbaum, a partner with Barton LLP who heads the firm’s privacy and cyber practice, and host Richard Levick discuss the evolution of privacy in the workplace when the workplace for everyone is home.

LISTEN >>

Navigating Blockchain

Huhnsik Chung, a partner with Carlton Fields and CEO of SQrBlock, explores blockchain as a business solution with host Richard Levick.

LISTEN >>

Ransomware

Kim Peretti, a partner at Alston & Bird and co-chair of the firm's cyber security practice, discusses ransomware with host Richard Levick.

LISTEN >>

IN HOUSE WARRIOR PODCAST

Cyber Security and Privacy for High Net Worth Individuals

Cyber criminals spend less and less time trying to break through the cyber protections of companies and instead go after the homes and vacation homes of the perfect targets. Dr. Chris Pierson, CEO and Founder of BlackCloak, joins host Richard Levick and Ian Lipner, the head of LEVICK's cyber practice, to examine how high net worth individuals and companies can protect themselves from the hack that has already come or will soon.

LISTEN >>

IN HOUSE WARRIOR PODCAST

Krebs on Security

Global cyber security thought leader and journalist Brian Krebs joins co-hosts Richard Levick and Ian Lipner on a tour de force on growing cyber threats and what companies can do. It is not a question of if but when with particular challenges for small and mid-sized companies, particularly in the area of ransomware.

LISTEN >>

IN HOUSE WARRIOR PODCAST

Biometric Privacy

The Future Is Now: As part of the series on technology and the law, Blank Rome Biometric Privacy Team chair Jeffrey Rosenthal discusses the growing promise, threats and challenges of biometrics – from fingerprints to facial recognition — and how companies and their counsel should prepare, with co-hosts Richard Levick and Ian Lipner.

LISTEN >>

IN HOUSE WARRIOR PODCAST

Weaponizing Cyberspace

Mark Mermelstein, a partner with Orrick, discusses what happens when a business competitor teams up with a foreign mercenary in cyberspace, with hosts Richard Levick and Ian Lipner.

LISTEN >>

connect to address 192.168.1.10
username: **********
password: ***********
Access granted...
exited after 0.006146 seconds with return value
any key to continue . . .

The Bad Guys Have Changed

Beazley Claims Team Leader of Cyber & Tech, Marcello Antonucci speaks with cohosts Richard Levick and Ian Lipner on seeing around the next cyber corner, cyber-hygiene, disaster response and risk management.

LISTEN >>

Have We Reached Peak Tech?

Trust in tech companies is at an all-time low after a long series of privacy mishaps and worries about job automation. Which begs the question: have we reached peak tech? Is the bubble going to burst, and finally lead to a reasonable amount of regulation? To understand what's on the horizon, and what could change, *What's Working in Washington* spoke with James Moore, founder and CEO of the Washington Institute for Business, Government, and Society; Kandi Parsons, shareholder at ZwillGen; and Richard Levick, founder and CEO of LEVICK.

LISTEN >>

WHAT'S WORKING IN WASHINGTON PODCAST

Understanding What Regulation the Tech Industry Needs

On *What's Working in Washington*, Phil Bond, president of government affairs for Potomac International Partners, Elizabeth Rogers, regulatory expert and partner at Michael Best, and Richard Levick, CEO of LEVICK, discuss the myriad of problems facing future regulations for the tech industry, and how regulations might take shape in the near future.

LISTEN >>

WHAT'S WORKING IN WASHINGTON PODCAST

WHAT'S WORKING IN WASHINGTON PODCAST

True Costs of Hacking

Andres Franzetti, chief executive officer and founding member of the Risk Cooperative and Brian Finch, partner of Pillsbury Winthrop Shaw Pittman, spoke with host Richard Levick on *What's Working in Washington* about the real impact of hacking, collateral damage, the integrity of information, and the real costs of cybersecurity.

LISTEN >>

Protecting Small Businesses from Social Media Attacks

On *What's Working in Washington*, Richard Levick, CEO of LEVICK, provides recommendations on what small businesses should be doing to protect their brands following attacks on social media.

LISTEN >>

WHAT'S WORKING IN WASHINGTON PODCAST

Russian Cyber Attacks Show Emerging Threats to Companies

The FBI says it agrees with the CIA that Russia hacked the Democratic National Committee to influence the 2016 U.S. presidential election. Hacking emails is a relatively simple attack, but it shows the influence cyberattacks can have. Weekly contributor Richard Levick, CEO of LEVICK, explains how he expects cyber threats to grow in the coming years and how companies need to protect themselves. Levick talks about the increasing threat to U.S. infrastructure, banks and hospitals as cyber criminals develop more advanced attacks.

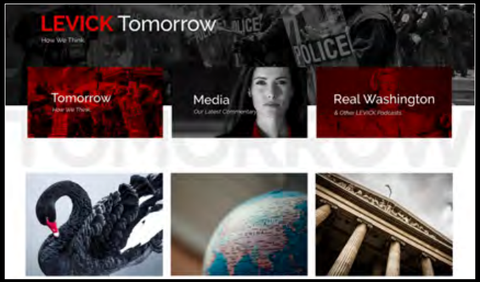
LISTEN >>

LEVICK Resources

Learn More: For the latest insights on breaking events, industry trends, and global development…

Subscribe to LEVICK's newsletter Today…

Visit the LEVICK blog…



Read LEVICK's e-books

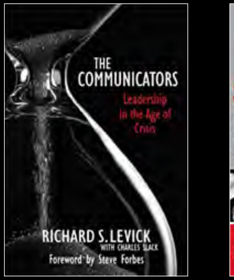
Litigation Communications in the Information Age:
What Every Lawyer, General Counsel, Communications Officer, and Board Member Should Know
LEVICK

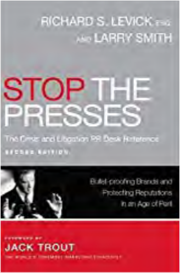
Criminalizing the Boardroom:
A Communications Guidebook for Prosecutorial Targets
LEVICK

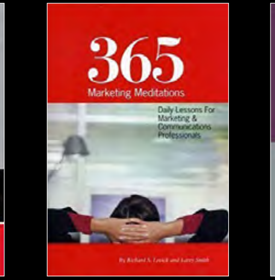
Navigating U.S. Regulatory, Legal & Communications Hurdles
A Guidebook for Foreign Companies
LEVICK

CONTINUED ON NEXT PAGE

Read LEVICK's books




RICHARD S. LEVICK ESQ.
AND LARRY SMITH
STOP THE PRESSES
The Crisis and Litigation PR Desk Reference
SECOND EDITION
Bullet-proofing Brands and Protecting Reputations in an Age of Peril
FOREWORD BY
JACK TROUT


365
Marketing Meditations
Daily Lessons For Marketing & Communications Professionals
By Richard S. Levick and Larry Smith

inside
outside
Larry Smith
How Businesses Buy Legal Services
With a Foreword by Richard S. Levick

Listen to LEVICK…

IN HOUSE
WARRIOR
A DAILY BROADCAST IN COURAGEOUS LEADERSHIP
hosted by Richard Levick | presented by CCBJ

Watch LEVICK…

Read LEVICK

DC
1900 M Street, NW
Washington, DC 20036
P 202.973.1300

NY
122 East 42nd Street
New York, NY 10168
P 917.612.8419

LEVICK

FIXING THE IMPOSSIBLE™