March, 2016

Making Sure BYOD Does Not Stand for "Breach Your Organization's Data"

Allyson Haynes Stuart

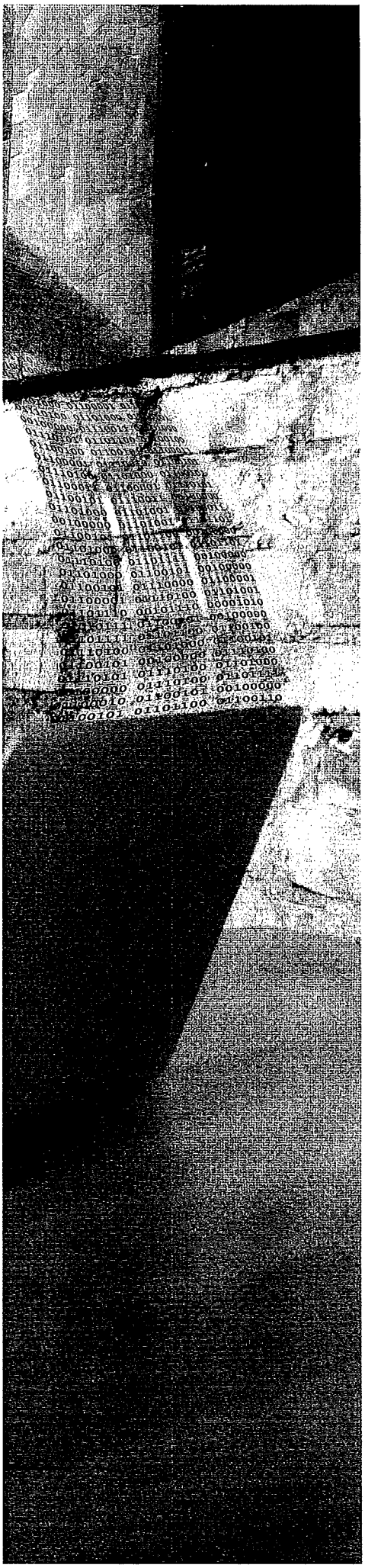


PHOTO BY GEORGE FULTON

Making Sure BYOD Does Not Stand for "Breach Your Organization's Data"

By Allyson Haynes Stuart

It is the modern employer's dilemma: do you allow employees to bring their personal smartphones, laptops and tablets to work for business purposes? Do you purchase work devices for them, duplicating what they have? Or do you simply ban use of any personal device for work purposes?

Approximately 80 percent of full-time U.S. workers have a smartphone with Internet access, 87 percent have a laptop or desktop computer and 49 percent have a tablet computer.[1] In all, 96 percent of full-time American employees say they use at least one of these types of devices.[2] In addition, more and more employees are working from outside the office, which often increases productivity.[3] Outright bans on use of personal devices for work may be impractical or, worse, not followed. And it is economically beneficial for employers not to have to duplicate these devices. For these reasons, many employers are incorporating employee-owned devices into their policies. Reportedly, more than half of North American and European companies are developing a bring-your-own-device (BYOD) policy.[4] But with the benefits of BYOD come many challenges. This article explores the risks associated with BYOD and offers practical solutions for employers seeking to maintain a secure corporate network.

The risks of BYOD

First, what are the risks of allowing employees to use their own devices for work? Obviously, risks vary greatly depending on the type of employer. There will be

more risk for employees who deal with confidential information, such as in the health care or legal sectors. One recent survey found that 72 percent of consumers text for work purposes, and that 25 percent of those messages contain confidential information.[5] But some risks apply even to non-confidential communications.

Loss of control over employer data

Many employers are required as part of compliance obligations to retain certain data or communications. If that data resides on a device over which the employer has no control, the employer may face regulatory or other problems.

Compliance and confidentiality

In the financial services industry, a variety of federal regulations require broker-dealers, investment advisers and investment companies to retain copies of all communications relating to their business and to produce such records upon request.[6] E-mails, text messages and instant messages are "communications" and brokerage firms, therefore, have to retain such records related to their business and be able to produce them promptly at the request of the Securities and Exchange Commission (SEC). In 2013, the top source of fines by the Financial Industry Regulatory Authority (FINRA) was noncompliance with electronic messaging laws.[7] Barclays Capital Inc. was fined $3.75 million for systemic failures to properly preserve electronic records and certain e-mails and instant messages.[8] Audio communications, a key component of smartphones, are also increasingly critical, as the volume of audio data recorded and analyzed by banks multiplies.[9]

In the health care sector, the Health Insurance Portability and Accountability Act (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act, requires health care providers and other covered entities to safeguard the privacy of patient information and protect its security.[10] The Freedom of Information Act and similar state open records laws require government agencies to maintain and disclose information requested by the public.[11]

Finally, law firms are a prime repository of confidential information—and unfortunately a frequent target for cybercriminals.[12] Lawyers are the stewards of their clients' files and are required to do a reasonable job of securing data. Rule 1.1 of the Model Rules of Professional Conduct requires a lawyer to provide competent representation, which includes keeping track of "the benefits and risks associated with relevant technology."[13] Model Rule 1.6 requires attorneys to maintain the confidentiality of information relating to the representation of a client, including "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to

the representation of a client."[14] Ethics opinions in Arizona, New Jersey, Nevada and Virginia emphasize that law firms must take competent and reasonable steps to protect client data from hackers and viruses, and to assure that the client's electronic information is not lost or destroyed.[15]

In addition to ethical requirements, attorneys also face common law duties of confidentiality, breach of which can result in a malpractice action, as well as various state and federal statutes and regulations that require protection of defined categories of personal information.[16]

Litigation hold

There are instances in which an employer may need access to communications or data on an employee's device whether or not those communications can be labeled "confidential." When an entity reasonably anticipates litigation, it must identify and preserve electronically stored information (ESI) in addition to other evidence likely to be relevant to the litigation.[17] Courts have imposed sanctions from the minor to the severe for spoliation, or failure to preserve ESI. For example, in *Qualcomm Inc. v. Broadcom Corp.*, a district court in California awarded Broadcom attorneys fees and costs in the amount of $8.5 million, and referred six outside counsel to the state bar, after finding Qualcomm had hidden over 46 thousand e-mails.[18] More recently, courts have fined parties and their counsel for deletion of social media postings.[19] Importantly, the law does not differentiate among types of media—a litigation hold should include potentially relevant information in the form of instant messages, Skype chats, social media and text messages in addition to the now-familiar e-mail.

These relevant communications may exist on an employee-owned device. Employers need to know ahead of time what kinds of ESI are created and retained on the device, and ensure that business-related information is subject to a document retention policy. They should have mechanisms in place to ensure that, if a litigation hold is entered, employees understand their obligations to maintain and not delete such data. In addition, employers can use software solutions discussed later to control that information themselves.

The risk of data breach

Data breaches are seemingly ubiquitous these days. According to PwC, there were 42.8 million cyber incidents in 2014.[20] One-third of in-house counsel report having experienced a corporate data breach.[21] There are many sources of legal obligations that require employers to use reasonable security measures to try to prevent data breach, including state law,[22] federal law with Federal Trade Commission (FTC) enforcement,[23] public disclosures and contractual obligations. How does BYOD affect the security of the employer network?

One issue is simply the mobility of the device itself. Paul Ihme, Senior Security Consultant for Soteria, a cybersecurity firm in Charleston, says one of the greatest vulnerabilities comes from employees' use of an outside network, where they may pick up malware or other intrusive software that may not be able to penetrate the security controls protecting a company's infrastructure. That malware can then be transferred to the company's network when the employee comes back to work. The vulnerable network could be anything from a public WiFi hotspot to a home network, neither of which typically has the security infrastructure in place to prevent anything but the most basic attacks.

Another risk is in the intermingling of data on the device, sometimes leaving sensitive business information at risk of loss. Despite headline-grabbing hacker-related incidents, the most common reason for a data breach is "employee error"[24]—where the breach occurred as the result of a mistake the employee made, such as accidentally sending an e-mail with sensitive information to someone outside the company. Information leaks committed using mobile devices—intentionally or accidentally—constitute one of the main internal threats that companies are concerned about for the future.[25]

In addition to unintended disclosure and hacking, other common sources of data breach are spam, phishing, malware, and a lost, discarded or stolen device.[26] Again, employee-owned mobile devices increase the possibility of these risks.

How can companies control these risks?

Technological risk control

One solution that Soteria recommends is the use of mobile device management (MDM). MDM is a type of security software used by an organization to monitor, manage and secure employees' mobile devices.[27] Brad Warneck, co-founder of Soteria and President of Consulting Services, says that MDM allows the employer a certain amount of control over the employee's device, including basic administration and policy enforcement, such as control over the downloading of applications. MDM can also be very helpful where the company handles sensitive information, because some MDM solutions act as an encrypted sandbox where that information is unable to be read by other processes resident on the device. Finally, MDM can allow the employer to remotely wipe a device should it get in the wrong hands.

Use of such software on employee-owned devices is challenging because those devices usually include personal photos, messages and other data. For reasons like the privacy concerns discussed in a later section, employees may not want their personal text messages, calls, e-mails and photos accessed, archived or remotely wiped along with corporate information. To address these chal-

lenges, organizations are increasingly selecting secure mobile apps that are integrated with MDM platforms that use a "persona" architecture, which separates business and personal calls and data.[28] K Royal, Vice President and Assistant General Counsel of CellTrust Corporation, notes: "This design enables organizations to apply policies—such as data erasure and archiving—that impact the business persona only. This greatly increases the likelihood that more employees will feel comfortable using their personal device at work, which means the business will benefit more from BYOD as a result of increased participation."[29]

In addition to MDM, these are general recommendations for ensuring security of corporate data on BYOD devices:

- Require strong passwords. A recent survey[30] found that 2015's most commonly used password was "123456"—that is not acceptable! Also problematic is the use of pet or children's names that are readily available on social media.
- Use multiple factors of identification, like a text-message passcode in addition to a password.
- Encrypt data or individual folders in the device, or encrypt the device itself.[31]
- Limit access to confidential information, including screening individuals who can access certain data, or segregation of sensitive data.[32]
- Screen outside vendors and ensure they undergo periodic security audits.
- Remote control: Enable remote wiping of a device should it get in the wrong hands, find-my-device features that track its location, and remote backup of information on the device.

Data breach response plan

The second primary way for an organization to protect itself against BYOD challenges is to establish, maintain and practice a data breach response plan. Despite the obvious risks, many U.S. companies do not have a written cyber breach response plan, and fewer still actually practice them. In fact, according to data recently reported by the Ponemon Institute, nearly half of the companies with a breach response plan have either never practiced the plan, or regularly wait more than two years to practice the plan.[33] Having such a plan can help not only in limiting data loss but also in limiting liability: the number one question asked by regulators after a data breach is whether the target company has an established breach response plan, and, if so, whether the plan was ever practiced in advance of the breach.[34]

A data breach response plan should address immediate responses—who should be notified internally if any suspicious activity is discovered, who should be on the response team, and what initial steps they should take. It should cover notification of others, including the board, inside or outside counsel, insurance carriers, law enforcement or regulators, and customers (keeping in mind any applicable breach notification laws). Finally, the plan should address documentation of actions and how to maintain confidentiality and privilege, and it should address the implementation of a litigation hold if litigation is reasonably anticipated.

Once the plan is in place, the organization should test it—by a full simulation, or simple table top exercise. Testing the plan is critical to ensuring the appropriate people take ownership and are well trained; to identifying and correcting any errors or deficiencies in the plan; and to updating the plan to ensure it stays effective as threats and vulnerabilities evolve.[35]

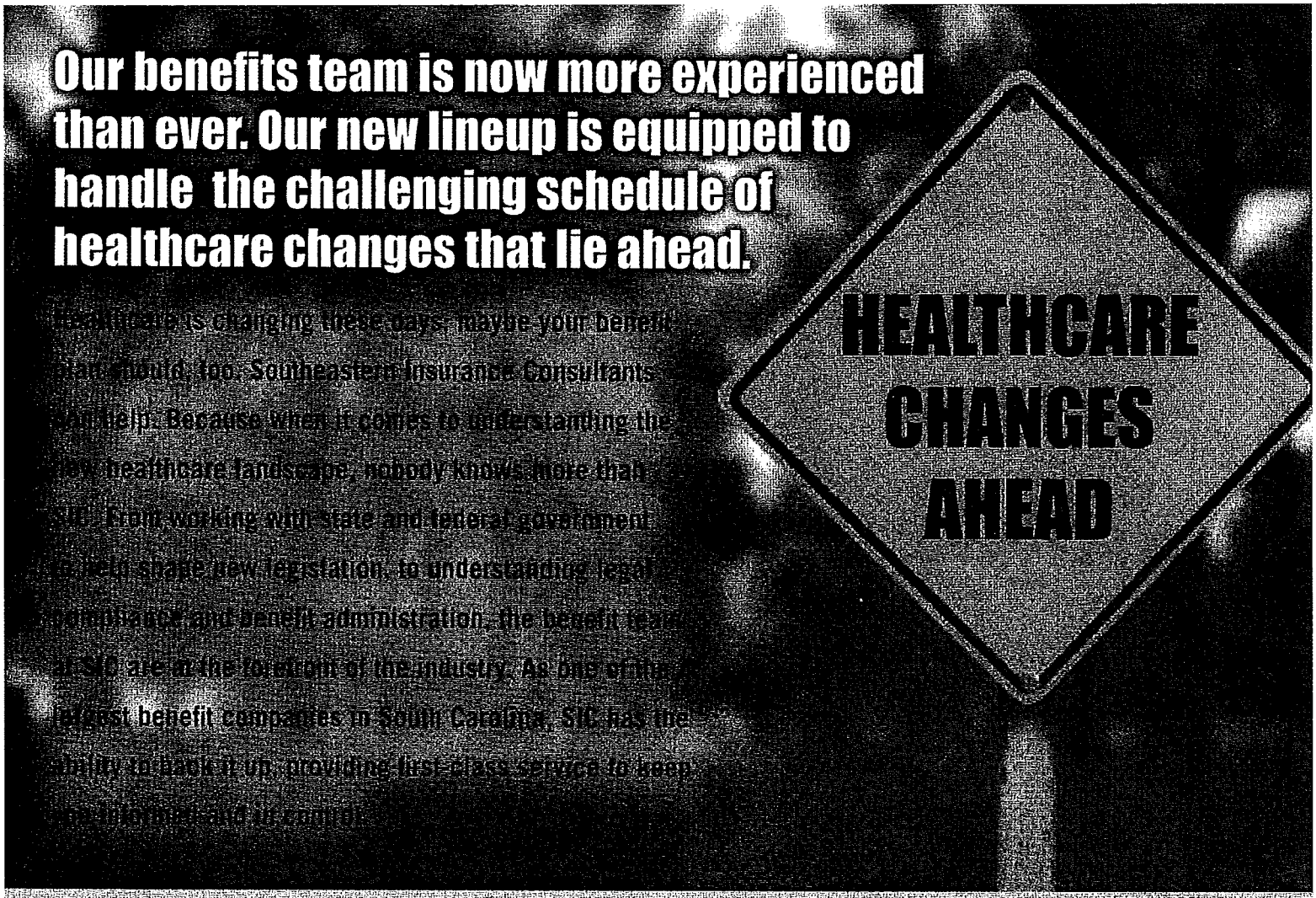
Communication with employees and respect for their privacy

A final aspect of BYOD that an employer should keep in mind is the employee's right to privacy. A recent survey found that a majority of mobile workers trust their employer to keep personal information private on their mobile devices.[36] Whether or not that expectation is reasonable, employers need to be careful with their monitoring of employee communications and with their tracking of the location of employee devices to ensure employers do not infringe on employee privacy. The Supreme Court has assumed, without deciding, that a government employee can have a reasonable expectation of privacy in personal communications exchanged on an *employer-provided* device (and privacy would arguably be higher on the employee's own device).[37] And some state laws require that employers give prior notice to employees of any electronic monitoring.[38]

Because the question of reasonable expectation of privacy will turn on the specific facts, employers need to make very clear in their policies and communications to employees what information is not private, and what is acceptable use of business data and networks. What data may employees access on their devices, and are there specific applications they should or should not use? Can the employer access e-mail, Word files, social media, personal photos or applications on the employee-owned device? Does the employer intend to track the device? Clarity and consistency in the employer's policy are key to maintaining appropriate parameters.

Best practices include the following:

- Establish transparent, easily-understood policies on BYOD, privacy, document retention and acceptable use, and follow them;
- Delineate the personal from the business uses of the device, and set parameters on monitoring, tracking, archiving and remote wiping;
- Share those policies with employees as early as possible, having each employee sign a statement stating that they have received and understand the policy; and
- Train employees on how to maintain privacy on the device, on security best practices and on



SIC

Southeastern Insurance Consultants, LLC

Our Knowledge, Your Benefit!

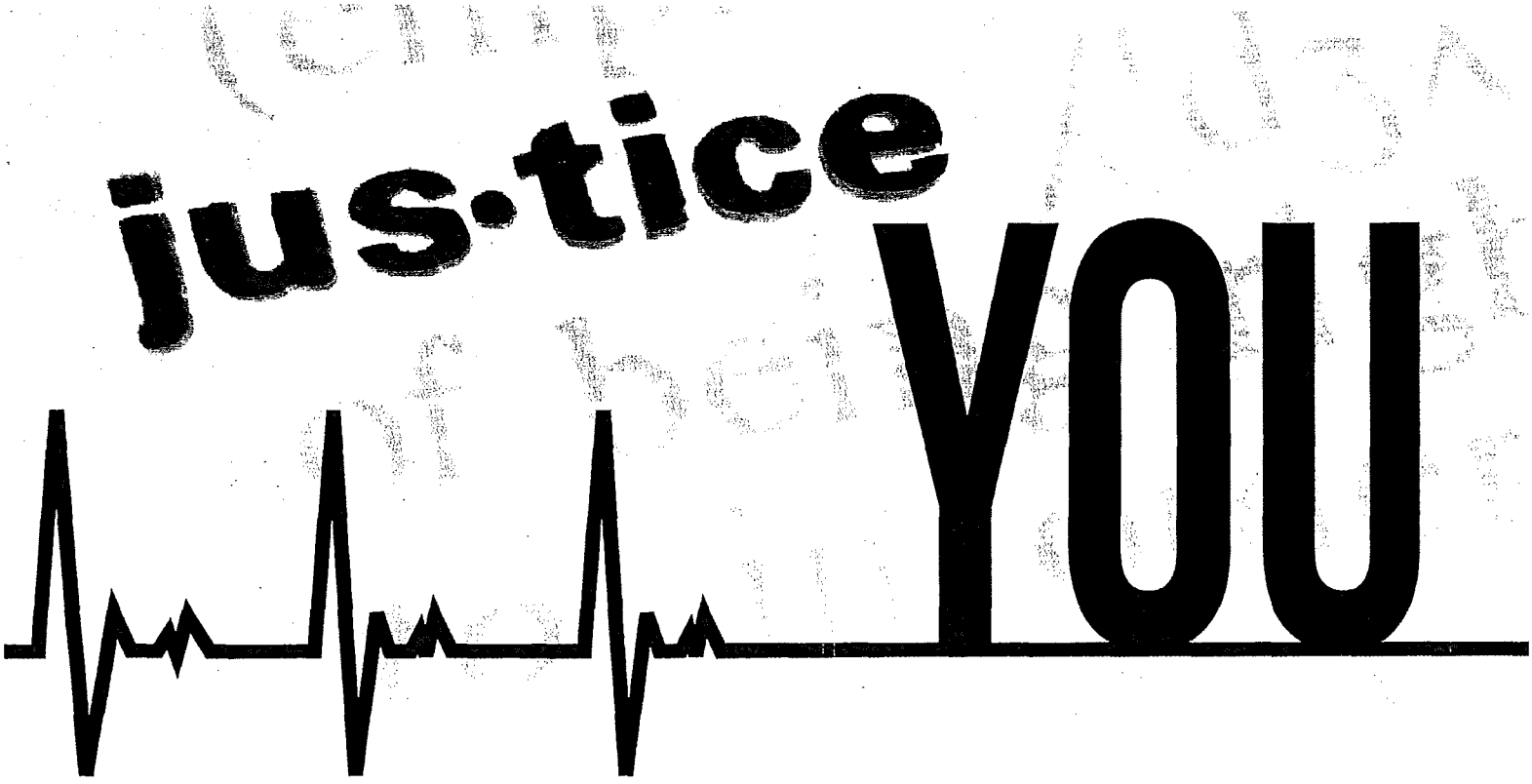
- **Health Plan Options** —Individual, Small Group, Large Group, Managed Care, Self-Funded, Level-Funded
- **Dental Insurance**
- **Life Insurance** —Group or Individual Life Plans
- **SIC Also Offers** —Short/Long Term Disability, Retirement Plans (401k, SEP, etc.), Wellness Plans, Benefit Counseling, Supplemental Benefits, Individual/Child Plans, Home, Auto, Watercraft and Professional Liability

Contact one of our team members today to see how we can help you prepare the best game plan for your team.

- Eric Wells – *Irmo*
  803-730-9200
  ewells@siconsultants.com
- Ed Byrd – *Columbia*
  803-600-6719
  ebyrd@siconsultants.com
- George Routon – *Newberry*
  803-730-0505
  grouton@siconsultants.com
- Steve Brown – *Greenville*
  864-268-5717
  sbrown@siconsultants.com
- Sam Plexico – *Barnwell*
  800-617-1001
  splexico@siconsultants.com

877-244-0481

www.SIConsultants.com



CAN MAKE IT HAPPEN...

The South Carolina Bar Foundation's mission to fund the advancement of justice by improving access, education and accountability can't be achieved without donors like you!

We ask you to join us as a Foundation supporter. We rely on members of our legal profession to keep building and growing, especially in times of financial stress and low IOLTA revenues. Your participation through giving not only serves your communities but also serves your colleagues and profession.

The Pledge of Allegiance closes with the words "justice for all." With your help, the SC Bar Foundation and its grantees can continue working toward making this true for all South Carolina citizens, not just those who can afford it. Together, we can make it happen.

To donate, contact the Foundation:
Phone: 803-765-0517
Email: foundation@scbar.org
Website: www.scbarfoundation.org

South Carolina
BAR FOUNDATION
Lawyers Sustaining Justice

data breach response.

Conclusion

BYOD does not have to be a death knell to an organization's data maintenance and security. With the right policies, precautions and communications with employees, organizations can control the risks associated with outside networks. Implementation of a data breach response plan, as well as testing and training for the plan, will both lessen likely data loss as well as protect against regulatory fines and litigation. The organization and its employees can all benefit from BYOD's upside: increased flexibility and productivity, better client services and cost efficiencies.

Allyson Haynes Stuart practices with Crystal & Giannoni-Crystal LLC in Charleston.

Endnotes

[1] Jim Harter, Sangeeta Agrawal, and Susan Sorenson, *Most U.S. Workers See Upside to Staying Connected to Work*, Gallup (Apr. 30,2014), www.gallup.com/poll/168794/workers-upside-staying-connected-work.aspx#!mn-world.

[2] *Id.*

[3] Regular work at home, among the non-self-employed population, has grown by 103% since 2005 and 6.5% in 2014. *See* Global Workplace Analytics, *Latest Telecommuting Statistics* (Sep. 29,2015), http://globalworkplaceanalytics.com/telecommuting-statistics.

[4] K. Royal, *Balancing Security and Privacy in BYOD*, TelecomReseller (Dec. 14, 2015), http://telecomreseller.com/2015/12/14/balancing-security-and-privacy-in-byod.

[5] Kristin Tinsley, *Survey Reveals Most Employees Text Using Unsecure Channels*, TigerText (Feb. 12, 2015), www.tigertext.com/survey-reveals-employees-text-using-unsecure-channels.

[6] *See* Gramm-Leach-Bliley Act of 1999 §§12 U.S.C. 6801-6809 (2012).; SEC Rule 17a-4(b)(4), 17 C.F.R. 240.17a-4(b)(4); *see* Jon Eisenberg, *K&L Gates 2014 SEC and FINRA Enforcement Actions Against Broker-Dealers and Investment Advisers.*

[7] Ken Anderson, *2013 FINRA Disciplinary Actions from Electronic Communications Transgressions*, Smarsh (Feb. 27, 2014), www.smarsh.com/blog/2013-finra-disciplinary-actions-electronic-communications-transgressions.

[8] *FINRA Fines Barclays $3.75 Millions for Systemic Record and Email Retention Failure*, FINRA (Dec. 26, 2013), www.finra.org/newsroom/2013/finra-fines-barclays-375-million-systemic-record-and-email-retention-failures

[9] *See* Royal *supra* note 4, ("We have seen a 100 percent increase in the volume of audio data recorded and analyzed by banks," quoting Brandon Daniels, Clutch Group).

[10] *See* Health Insurance Portability and Accountability Act (HIPPA) of 1996, 42 U.S.C. §201 (2012); Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, 42 U.S.C. §201 (2012).

[11] *See* 5 U.S.C. § 552 (2012); *See also* state law statutes include Florida, Fla. Stat. § 119.01 – 119.15 (1995); Georgia, O.C.G.A. §§ 50-18-70 – 50-18-77 (2007); North Carolina, N.C.G.S. §§ 132-1 – 132-10 (2014); New York, N.Y. Pub. Off. Law § 84 – 90 (Supp. 2009); and South Carolina, S.C. Code Ann. §§ 30-4-10 – 30-4-165 (1976).

[12] Cybersecurity firm Mandiant says at least 80 of the 100 biggest firms in the country, by revenue, have been hacked since 2011. Susan Hansen, *Cyber Attacks Upend Attorney-Client Privilege*, Bloomberg Businessweek (Mar. 19, 2015), www.bloomberg.com/news/articles/2015-03-19/cyber-attacks-force-law-firms-to-improve-data-security.

[13] ABA Model Rule 1.1 comment 8 (2012).

[14] ABA Model Rule 1.6 (c).

[15] *See* State Bar of Ariz. Op. No. 05-04, July 2005; Ariz. Bar Op. No. 09-04, Dec. 2009; N.J. Comm. on Prof. Ethics Op. 701 (Apr. 24, 2006), Nev. Standing Comm. on Ethics and Prof. Resp. Formal Op. 33 (Feb. 9, 2006) and Va. Standing Comm. on Legal Ethics Op. 1818 (Sept. 3, 2005).

[16] David G. Ries, *Safeguarding Confidential Data: Your Ethical and Legal Obligations*, ABA Law Practice (July/Aug. 2010), www.americanbar.org/publications/law_practice_home/law_practice_archive/lpm_magazine_articles_v36_is4_pg49.html.

[17] *See generally Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422 (S.D.N.Y. 2004).

[18] *Qualcomm Inc. v. Broadcom Corp.*, 2010 WL 1336937 (S.D. Cal.). The new F.R.C.P. 37(e) requires that courts find "intent to deprive another party of the information's use in the litigation" before ordering an adverse inference instruction or other severe sanction, while lesser sanctions will depend upon prejudice to the other party. Fed. R. Civ. P. 37(e).

[19] *See Painter v. Atwood*, No. 2:12-CV-01215-JCM, 2014 WL 1089694, at (D. Nev. Mar. 18, 2014); *Lester v. Allied Concrete Co.*, Nos. CL08-150, CL09-223 (Va. Cir. Ct. Sept. 1, 2011).

[20] Daniel L. Farris, *The Preparedness Gap: Why You Should Treat Data Security and Cyber Readiness Like a Fire Drill*, Law Technology Today (Dec. 14, 2015), www.lawtechnologytoday.org/2015/12/preparedness-gap-treat-cyber-readiness-like-fire-drill.

[21] *One-Third of In-house Counsel Have Experienced a Corporate Data Breach, ACC Foundation: The State of Cybersecurity Report Finds*, Association of Corporate Counsel (Dec. 9, 2015), www.acc.com/aboutacc/newsroom/pressreleases/accfoundationstateofcybersecurityreportrelease.cfm.

[22] Companies experiencing data breaches have been sued for negligence, breach of contract based on company privacy policies, and breach of state consumer protection and data security or breach notification statutes. *See In re Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig.*, 834 F. Supp. 2d 566 (S.D. Tex. 2011). ; Doe v. Avid Life Media, No. Case 2:15-cv-06405 (C.D. Ca. Aug. 21, 2015).

[23] The Federal Trade Commission ("FTC") Act prohibits "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a). The FTC brings actions against compromised entities for failure to use "readily available security measures." The FTC "Red Flags Rule" requires banks and financial services companies to establish an identity theft prevention program and requires action by covered entities that experience a "red flag", which is "a pattern, practice, or specific activity that indicates the possible existence of identity theft." 16 CFR 681.1.

[24] *See supra* note 21.

[25] *Kaspersky Labs Global Corporate IT Security Risks: 2013*, Kaspersky lab,(May2013)

[26] *See* Jonathan I. Ezor, *Privacy and Data Protection in Business: Laws and Practices* 260 (2012).

[27] Vangie Beal, *MDM-Mobile Device Management*, Webopedia.com www.webopedia.com/TERM/M/mobile_device_management.html (last visited Feb. 10, 2016).

[28] *See supra* note 4.

[29] *Id.*

[30] Morgan, *Announcing Our Worst Passwords of 2015*, TeamsID (Jan. 19, 2016), www.teamsid.com/worst-passwords-2015.

[31] *See* Andrew Cunningham, *Phone and laptop encryption guide: Protect your stuff and yourself*, ars technica (Aug. 23.2015 1:00pm), http://arstechnica.com/gadgets/2015/08/phone-and-laptop-encryption-guide-protect-your-stuff-and-yourself.

[32] This tip is even more important in light of the recent decision by the Second Circuit, where the court found that an employee could only be held liable under the Computer Fraud and Abuse Act for theft and other misuse of company data if that employee lacked authorization AND bypassed a technological barrier to access the information. *United States v. Valle*, 807 F.3d 508 (2d Cir. 2015).

[33] *Supra* note 18.

[34] *Id.*

[35] *Supra* note 4.

[36] *61% of Mobile Workers Trust Their Employer to Keep Personal Information Private on Their Mobile Devices*, MobileIron (July 15, 2015), www.mobileiron.com/en/company/press-room/press-releases/trust-gap-2015.

[37] *City of Ontario v. Quon*, 130 S. Ct. 2619 (2011).

[38] *See* Conn. Gen. Stat. Ann. § 31-48d; 19 Del. C. § 705 (2008). Similar legislation is pending in Massachusetts, Pennsylvania and New York. *See* Mark W. Robertson and Anthony DiLello, O'Melveny, & Meyers LLP, *State By State Employee Monitoring Laws*, Law360 (2008), www.omm.com/files/upload/Employee%20Monitoring%20Laws.pdf.