Data Security and Privacy:

More than I.T.

By Drake Mann
Christopher L. Travis and
Don Lloyd Cook

One day, you click a link.

Your screen goes dark. After a few seconds, a skull with glowing red eyes emerges from the darkness next to a message: "Your files are now encrypted...pay $1,500 for the key or the key will be destroyed when the countdown clock gets to zero."

A clock beneath the message is counting down.

The statistics are attention-getting: 40% of all targeted cyber-attacks are directed at companies with fewer than 500 employees; almost two-thirds of victimized companies are forced out of business within six months of an attack; 83 percent of small businesses have no formal cyber-security plan, even though 71 percent are dependent on the internet for daily operations. Yet most business managers think hacks are isolated incidents that won't have an impact on their business.[1]

It's Too Late

There's a running gag among data security presenters:

"How many here work at an organization that has never been hacked?"

The novices' hands shoot up. The crowd snickers.

The presenter smirks: "There are two kinds of companies, those that have been hacked and those that have, but don't know it yet."

It's funny (to them) because it's true. In 99% of all payment card data security breaches—regardless of victim size or attack method—"someone else told the victim they had suffered a breach." And in 85% of those cases, it took an average of *178 weeks* to discover the problem.[2]

Data security is no longer something simply to hand off to the IT guy. A culture of data security diligence and awareness must permeate every organization, large and small.

"Humans are the weak link."

Organizations can't leave data security and privacy to IT professionals because the IT folks cannot manage the problem alone. A firewall and some antivirus software are inadequate protections these days.

Thieves frequently send emails designed to look trustworthy—"phishing" emails—that install malicious software ("malware") when the victim clicks a link in the phishing email. The malware infiltrates the victim's network, and can steal information, log key strokes to capture usernames and passwords, spread more malware, encrypt files for ransom, or other nefarious actions. The malware agent sometimes hides for weeks before it goes to work.

Drake Mann, CIPM, CIPT
Christopher L. Travis and
Don Lloyd Cook, Ph.D., CIPP/US, CIPP/C
are members of the Data Security and Privacy Group at Gill Ragon Owen, P.A. They can be reached at (501) 376-3800 or by email at mann@gill-law.com, travis@gill-law.com, or cook@gill-law.com.

Consider the Target breach. The Target breach appeared "to have begun with a malware-laced email phishing attack sent to employees at a heating and air conditioning firm that did business with the nationwide retailer."[3] Target had provided the HVAC firm network credentials to access Target's computer network for electronic billing, contract submission, and project management.[4] The thieves stole the HVAC firm's credentials at least two months before they stole any data from Target. Before the attack, the HVAC firm probably did not consider itself a likely hacking target.

Yes, Target's own technical security failures ultimately enabled the thieves to steal Target's data.[5] But the initial breach could have been avoided if the HVAC firm had had a data security culture that included not only good network security, but also policies and practices that included training employees to identify phishing emails and to respond appropriately.[6] Adequate data security measures these days should include enterprise-wide policies and practices that support a security-conscious culture.

Parisa Tabriz, self-titled Security Princess at Google, Inc., proclaims that a company's greatest data security weakness is not technical: "For better or worse, humans are the weak link in security."[7] And, as a "60 Minutes" reported, "there's no shortage of weaknesses. Most company employees are allowed to browse online or visit Facebook on corporate computers and many take them home for personal use. All it takes to contaminate a network is for one person to unwittingly access an infected file that looks realistic ... like an Adobe Flash Player update or an email that pretends to be from Apple Support."[8]

These points of human vulnerability can be managed. Similarly to complying with state and federal employment laws, companies can survey their operations and establish operational standards that provide supervisory controls for employee behavior. Businesses should regard their privacy and data security landscape and address it enterprise-wide.

Several frameworks are available to assist in the process of assessing data security and developing reasonable and appropriate controls. The Federal Trade Commission publishes a guide with practical tips on creating a plan for safeguarding personal information.[9] The AICPA publishes Generally Accepted Privacy Principles[10] and the ISACA publishes Control Objectives for Information and related Technology (known as COBIT).[11] In general, the frameworks show that achieving and maintaining strong data security is an ongoing process that touches every aspect of company operations.

Even if statistics or anecdotes do not persuade businesses (including law firms) to address data security, they may soon find their hands forced. Trends in regulation and in standards of care forecast that broad changes in privacy and data security practices are on their way.

It is already nearly impossible for a business to avoid some form of external data security oversight, whether by contract or regulation. The Payment Card Industry requires that all businesses that accept payment cards meet the PCI Data Security Standard (PCI DSS). And federal regulatory regimes provide baseline data security guidance in banking and healthcare. However, even businesses that don't accept payment cards and are not in banking or healthcare should add data security controls for at least two reasons: 1) healthcare and banking regulations are incrementally extending data security obligations to businesses that serve healthcare and banking institutions and 2) negligence standards of care evolve.

PCI Compliance

Every enterprise that accepts payment cards has contracted with a payment card processor and, as a necessary component of that contract, has certified that it is PCI-compliant, meaning its computer network and operations comply with the PCI DSS. Low-transaction-volume businesses, such as law firms, usually provide self-assessments of their PCI compliance. Often an office manager or billing staff member completes a self-assessment questionnaire (SAQ)[12] on behalf of the organization. However, businesses may not appreciate the implications of simple, innocuous-looking SAQ questions, such as whether the computer utilized to conduct payment card transactions is connected to the company's network. If it is, the entire network typically must be PCI-compliant. If a breach occurs, a business's contract with its payment processor allows the payment processor, and through it card brands such as VISA, to levy (potentially crippling) fines.[13] Every business accepting payment card payments should ensure that it is, in fact, PCI-compliant. (*Editor's Note:* See page 28 of this magazine for a more detailed article on PCI Compliance).

Regulatory Creep—HIPAA & GLB

Healthcare and banking regulations protect non-public, personal information—information that technology has increasingly made faster, easier, and cheaper to move. In healthcare, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is widely known for its concern for protecting patient privacy. But the banking sector may have the most mature regulation of all information security regulatory regimes. The Gramm-Leach-Bliley Act (GLB) includes the latest additions to the banking regulatory regime; among other things, GLB addresses the collection, disclosure, and safeguarding of customers' personal financial information.

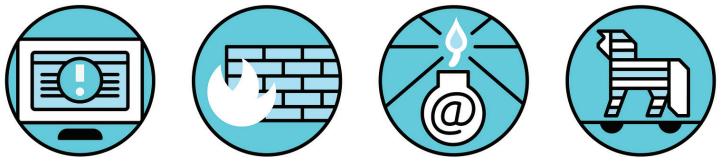
Recent amendments to both HIPAA and GLB have extended their reach and influence beyond the business sectors those laws initially regulated. For example, under HIPAA, covered entities have for some time asked third-party service providers (e.g., lawyers, data processors, storage warehouses) who handle Protected Health Information (PHI) to enter into "business associate"[14] contracts requiring those third parties to

acknowledge their commitment to ensuring the privacy and security of PHI they receive and to promise to notify the covered entity in the event of a data breach. But changes in 2009 (and related regulatory changes in 2013)[15] made HIPAA directly applicable to the "business associates" of covered entities.[16]

One of the core requirements of HIPAA's Security Rule (one that *must be documented*)[17] is that business associates must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) it holds. The business associate must implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level and must sanction employees who fail to comply. And, the business associate must regularly review records of information system activity such as audit logs, access reports, and security incident tracking reports.[18] These formal, structured, entity-wide requirements, long familiar to health care providers, now must become routine business practices of business associates of covered entities.

In a similar manner, GLB's protections are also spreading beyond the walls of financial institutions. In late 2013, the Office of the Comptroller of the Currency issued guidance to national banks and federal savings associations regarding how those entities should manage the risks associated with the third parties to which the institutions outsource significant banking functions.[19] While those relationships have long been the subject of regulatory concern, banking regulators are beginning to take a closer, and broader, view of banks' oversight of their third-party vendor relationships.

One example of this spread exists in the title industry. The American Land Title Association, the title industry's main trade group, adopted a voluntary set of "best practices" that it strongly encourages its members to follow. These "best practices" include a wide range of written privacy and information security plans, controls, and documentation practices. Some speculate that, as data breaches of title companies increase, as they inevitably will, banks will tend to rely less on those title companies that cannot certify that they have implemented ALTA's best practices regime.



"DATA SECURITY IS NO LONGER SOMETHING SIMPLY TO HAND OFF TO THE IT GUY. A CULTURE OF DATA SECURITY DILIGENCE AND AWARENESS MUST PERMEATE EVERY ORGANIZATION, LARGE AND SMALL. 'HUMANS ARE THE WEAK LINK.'"

GLB's regulatory extensions are also impacting law firms. Lawyers who handle bank-customer financial information in the course of their representation of banks are finding that banks are beginning to require their outside counsel to verify that the outside counsel has a coherent, comprehensive set of information-security policies and practices. Some banks even require their outside counsel to agree to subject themselves to periodic data security assessments.

Weak Data Security Provokes[20] Civil Liability

Beyond banking and healthcare, not protecting sensitive information is increasingly the subject of civil litigation. While there is no private right of action for HIPAA violations and proving damages or causation from most privacy breaches is at best a challenging proposition, there are emerging trends that prefigure a broad sea change in data security and privacy litigation.

In *Acosta v. Byrum*,[21] the North Carolina Court of Appeals considered the claim of a psychiatric patient who brought a claim for negligent infliction of emotional distress when the psychiatrist allegedly allowed a clinic employee to access her electronic health records. The employee allegedly "had severe personal animus towards plaintiff," and he provided information from those records to third parties, causing the plaintiff severe emotional distress. In reversing the lower court's dismissal for failure to state facts on which relief can be granted, the North Carolina Court of Appeals held that, while HIPAA does not provide a private cause of action, HIPAA could provide evidence of the duty of care owed by the psychiatrist with regard to the privacy of plaintiff's medical records.

Acosta was not unique.[22] Since *Acosta*, cases in West Virginia[23] and Connecticut,[24] among others, have held that HIPAA's requirements are relevant to the standard of care in negligence cases. The Connecticut Supreme Court held that "to the extent it has become the common practice for Connecticut health care providers to follow the procedures required under HIPAA in rendering services to their patients, HIPAA and its implementing regulations may be utilized to inform the standard of care applicable to such claims arising from allegations of negligence in the disclosure of patients' medical records pursuant to a subpoena."[25]

The FTC offers free on-line resources for businesses, including tips for creating and implementing a comprehensive plan for safeguarding personal information.[26] The very fact that these sorts of tips are readily available and easy to implement implies a shift in the burden businesses bear.

What To Do Now

Attacks happen every day. Blindly trusting that "the IT people have it covered" is no longer a responsible option. Any business should inventory the data it holds, develop policies and procedures that are reasonably related to its risks, minimize its data footprint, oversee third parties entrusted with handling sensitive data, educate employees and punish policy violations, and periodically reassess its policies and operations. IT

professionals have a role to play, but that role is only one part of a larger whole.

Before the recent onslaught of computer viruses and data breaches, perhaps no one could be faulted for not having anti-virus software or paying much attention to data security. But now, malware, worms, and Trojan horses are universally recognized as harmful, and their appearance on any computer is increasingly foreseeable. Standards of care change, and a reasonable person holding others' personal information must do more than install anti-virus software, dust his or her hands, and walk blithely away from further data security concerns.

The countdown clock is running.

Endnotes:

1. http://smallbusiness.house.gov/uploadedfiles/kaiser_testimony.pdf; *see also*, John Patrick Pullen, *How to Protect Your Small Business Against a Cyber Attack*, Entrepreneur, http://www.entrepreneur.com/article/225468.
2. Verizon 2014 Data Breach Investigations Report.
3. http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/.
4. http://faziomechanical.com/Target-Breach-Statement.pdf.
5. http://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412.
6. Some good responses include not clicking on any link, reporting the attempted phish, or forwarding the email to the company it appears to be from so that the company can take defensive steps, and then deleting it. http://www.antiphishing.org/; https://www.paypal.com/us/cgi-bin/webscr?cmd=xpt/cps/general/Spoof-outside.
7. http://www.cbsnews.com/news/google-hacker-security-princess-parisa-tabriz-female-star-tech-industry/.
8. Steve Kroft, "60 Minutes" report "The Attack on Sony" broadcast April 12, 2015. http://www.cbsnews.com/news/north-korean-cyberattack-on-sony-60-minutes/.
9. https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.
10. http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/GAPP_BUS_%200909.pdf.
11. http://www.isaca.org/cobit/pages/faqs.aspx.
12. https://www.pcisecuritystandards.org/security_standards/documents.php?association=saqs.
13. PCI compliance will become even more important after October 1, 2015. To encourage businesses to shift to new payment card technology—chip-and-PIN cards—VISA and other card brands will shift liability for fraud to the party to the transaction with less-secure technology. For example, if the merchant has chip-and-PIN card readers but the issuing bank has not provided the customer with a chip-and-PIN card, the bank must absorb the loss. http://usa.visa.com/download/merchants/bulletin-us-participation-liability-shift-080911.pdf.
14. 45 C.F.R. §§ 164.502(e), 164.504(e), 164.532(d) and (e).
15. 45 C.F.R. Parts 160 and 164, available at http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.
16. Bryan Looney and Amy Wilbourn, New HITECH Requirements and How They Impact Your Practice, The Arkansas Lawyer, Summer 2011, at 26.
17. *See* § 164.316 for policies and procedures for Security Rule documentation requirements; note that business associates will have to maintain documentation for six years and be able to produce it, if requested.
18. 78 Fed. Reg. 5590, HIPAA Section 164.308—Administrative Safeguards.
19. OCC Bulletin 2013-29. http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html
20. "Weakness is provocative." Donald Rumsfeld.
21. 180 N.C. App. 562, 638 S.E.2d 246 (2006).
22. *See*, *generally*, Martha Tucker Ayres, *Confidentiality and Disclosure of Health Information in Arkansas*, 64 Ark. L. Rev. 969 (2011).
23. *Tabata v. Charleston Area Medical Center*, 759 S.E.2d 459 (W. Va. 2014).
24. *Byrne v. Avery Ctr. for Obstetrics & Gynecology, P.C.*, 314 Conn. 433, 102 A.3d 32 (2014).
25. *Byrne*, 314 Conn. at 459, 102 A.3d at 49.
26. http://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security. ■