CYBERSECURITY

An Advertising Supplement to the Orange County Business Journal • June 20, 2016

Presented by

ABACUS DATA SYSTEMS™

CHASE

CYLANCE®

THERE IS NO TURNING YOUR BACK ON CYBER TERRORISM

"There are only two types of companies:
those that have been hacked and those that will be"

- Robert Mueller, Former FBI Director

Abacus Private Cloud is a compliance ready, fully managed Desktop-as-a-Service (DaaS) engineered to safeguard your business against cyber threats.

ABACUS DATA SYSTEMS
Fully Managed Technology Solutions

abacuslaw.com/ocbj
888-592-2044

Cybersecurity Strategies for Small and Middle-Market Companies

By Mike Hornak, Partner, and Marc Boiron, Associate, Rutan & Tucker

The rise of cyber incidents has resulted in a focus on best practices to prevent, plan for and respond to those incidents. Large companies are able to implement most of those best practices; however, the limited resources of small and middle-market companies require that those companies rely on practices which, albeit not best practices, nonetheless will help protect the companies and their boards of directors from liability, and protect company assets and third party assets from cyber events.

Many small and middle-market companies ignore even the most basic cybersecurity, relying on the mistaken notion that only larger companies are the targets of cyberattacks. The available data is to the contrary. As large companies implement best practices in cybersecurity, cybercriminals increasingly target smaller companies that have not implemented adequate security practices. When cyber data is stolen, those companies may ultimately be subject to litigation based on theories of negligence, breach of contract, and breach of federal or state statutes, among others claims.

Any cybersecurity strategy for small and middle-market companies must consider the consequences of the inevitable cybersecurity event, including litigation risk, lost cyber assets, disruption of the business, and lost customers and clients. The governing body and senior management should be involved in determining the company's cybersecurity strategy, including the resources that will be allocated to cybersecurity.

Small and middle-market companies can take a few inexpensive steps to decrease the likelihood that those companies will face a data breach, or at least mitigate the consequences of a breach. Below are but a few of those inexpensive steps.

Training

There are limited cybersecurity measures that are as cost-effective as employee training to prevent a broad range of breaches that result from or are contributed to by employee error. Employee-related data breaches can be reduced through a mandatory training program that can be inexpensive to establish and maintain and can be carried out internally, combined with web-based training programs. A good training program should be updated from time to time, incorporated into the employee onboarding process and provided to existing employees no less than annually.

Although a good training program has many facets and will differ by industry, key aspects include (i) making employees aware of the various types of cybersecurity threats, (ii) informing employees on how and when to report cybersecurity threats, and (iii) instructing employees on key points of access to the company's data (such as unauthorized software installation, accessing public Wi-Fi, inserting removable media, downloading or uploading corporate data to mobile devices, and phishing emails). In-person cybersecurity training should be considered because employees typically pay more attention and ask more questions than when training is provided online; however, online updates or reminders regarding cybersecurity are a useful supplement to in-person training programs.

Passwords and Multi-Factor Authentication

All companies should require that strong passwords be used on all systems and networks on which their data is accessible, though it is preferable for companies to require multi-factor authentication on those systems and networks. If passwords are used, then the company should require that all passwords be of a minimum length; include capitalized letters and special characters or numbers; be changed no less than every 90 days; and be different from any password the employee uses for personal emails, website access, or online shopping.

Multi-factor authentication, which generally requires that a password and a pin number generated on a cell phone or password token be entered to gain access to a system or network, provides greater security than passwords without adding significant costs. Cybercriminals are unlikely to be able to access a system or network with multi-factor authentication unless they have access to all of the pieces required for authentication, which (unlike passwords) protects the system from information obtained by keyloggers.

Notwithstanding the benefits of multi-factor authentication over passwords and their importance in a cybersecurity strategy, cyber data remains vulnerable to, among other things, spoofing, spyware, trojan horses and worms; therefore, multi-factor authentication cannot, alone, protect a company's cyber data.

Encryption

Data encryption is generally considered to be the backbone of any cybersecurity strategy and should be part of the cybersecurity strategy of all small and middle-market companies. Encrypting data is a process that makes data previously readable and usable by people unreadable and unusable by people. Therefore, unless a cybercriminal is able to decrypt encrypted data, obtaining access to the encrypted data is not valuable to the criminal.

In addition to protecting company and customer data, a meaningful benefit of encryption is that encryption of data may eliminate, or substantially reduce, the persons and governmental entities to whom formal notice of a data breach is required under the existing web of conflicting federal and state statutes and regulations.

Different quality encryption software exists. Companies with larger cyber budgets should consider high-end encryption software but, for some small and middle-market companies that do not have sufficient resources to pay for higher-end encryption software, free encryption software is available. Before relying on free encryption software, companies should ensure that the software meets any regulatory and other compliance standards applicable to them.

Insurance

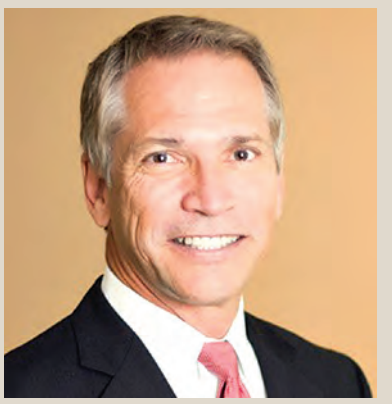
As with commercial general liability insurance, cybersecurity insurance is becoming a virtual necessity. Depending on the policy, cybersecurity insurance may provide broad coverage, including for costs related to: legal defense, obtaining legal advice on notification and regulatory requirements, sending notifications, settlements, judgments, regulatory penalties and fines, public relations, lost profits (but not lost intellectual property), credit monitoring services, and forensic discovery. Companies will need to decide the appropriate type of coverage based on the costs and risks they face.

Notwithstanding the recent decision of the United States Court of Appeals for the Fourth Circuit, which found that the commercial general liability policy at issue required an insurer to defend a company in a class-action lawsuit that arose out of the inadvertent posting of patients' medical records online, small and middle-market companies should not rely on general liability policies to provide protection against cybercrimes. Most modern general liability insurance policies specifically exclude cybersecurity coverage, though some providers permit cybersecurity coverage to be added to its general liability insurance policies.

Small and middle-market companies that consider obtaining cybersecurity insurance should recognize that policies are far from uniform. Given the broad range of available coverage and the relative novelty of cyber insurance policies, the costs of, and coverage and exclusions in, those policies range drastically. The cost of cyber insurance can range from approximately $1,000 annually for $1,000,000 of coverage to $40,000 or more annually for the same amount of coverage.

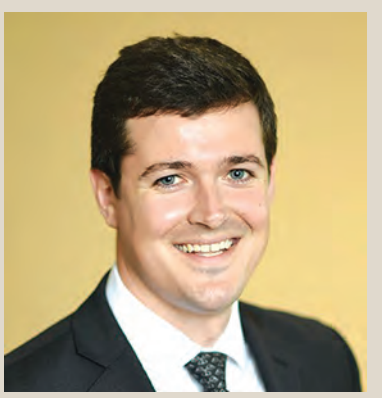
The uncertainty of cybersecurity liability policies should not deter small and middle-market companies from obtaining cybersecurity coverage because it provides important protection to those companies when firewalls, anti-spyware, passwords, multi-factor authentication, encryption and/or other cybersecurity measures fail.

Mike Hornak



Mike Hornak is co-chair of Rutan & Tucker's Cybersecurity, Privacy, and Corporate Governance practice group. His expertise extends to intellectual property disputes (including cybersecurity), shareholder and partner governance, the defense of consumer and shareholder class actions, and commercial litigation. He also advises clients on data protection schemes and the practical and legal responses to data breaches. Mr. Hornak is a frequent speaker and panelist on cybersecurity and privacy issues. He can be reached at mhornak@rutan.com or 714.641.3472.

Marc Boiron



Marc Boiron is a member of the Cybersecurity, Privacy and Corporate Governance Practice Group and focuses his practice on advising boards of directors and companies on cybersecurity matters and emerging and mid-market companies in the areas of California and Delaware corporate laws, securities laws, mergers and acquisitions, restructurings, recapitalizations, leveraged buyouts and strategic alliances. Marc can be reached at mboiron@rutan.com or 714.338.1861.

How to Defend Against Cyberthreats

We recently surveyed our Executive Advisory Board to find out how executives view the cybersecurity environment and their own vulnerability within it. Their responses prompted a conversation with Mike Kelly, Chase Commercial Banking's Head of Cybersecurity and Technology Controls, about how businesses can protect themselves against cyberthreats and what they need to know about the current fraud landscape.

Eighty-five percent of executives surveyed said their organizations require complex passwords for applications with sensitive data or critical operations, and 41 percent use multifactor authentication. What are some other tactics businesses can use to help protect confidential information?

There are generally three distinct areas within data security that companies should make sure they're thinking about when developing security protocols:

1. Access. Things like requiring complex passwords and implementing multifactor authentication are important ways to protect against unauthorized access to your data—but they can be made stronger if businesses have certain complementary measures in place, such as requiring that passwords have a robust history and are changed frequently. A robust password history will prevent your employees from reusing old passwords—best practices say that you should require employees to update their password at least 15 times before they're able to reuse an old one—and frequently updating passwords helps ensure that passwords are changed before they can be compromised.

2. Encryption. The encryption process converts sensitive data into a coded form that's typically undecipherable without the right decryption tools. However, it's worth noting that if access is compromised, encryption is basically useless—it only works if credentials remain uncompromised.

3. Monitoring. This one is pretty simple, but it's essential: You need to know what people are doing on your servers, even authorized people.

A number of organizations outsource their tech support to third-party vendors (44 percent) or freelance specialists (18 percent). What are some precautions businesses should take when outsourcing something as vital as data security?

There's not a right or wrong answer in terms of what you should outsource—in many cases, it depends on a business's size and industry. That said, one rule that applies to businesses of all sizes and across all industries is that any controls you have or standards you set internally should be applied to your vendors, too—the expectations have to be the same. You aren't absolved from managing your data security when you outsource it to a vendor—it's still your responsibility.

In terms of risk, concentration is always something to watch. If you give one vendor the keys to your kingdom—for example, if they have the ability to manage all your wire account data, as well as the ability to change it—you're putting your business at risk. Of course, sometimes it can be hard to break apart your tech support functions, in which case, you just have to be transparent with your board and have the proper audit rights in place. But in a perfect world, you'd be able to segment your data security so that you're not completely dependent on one vendor.

Thirteen percent of survey respondents said their businesses had experienced cyberfraud that led to stolen money. Of that 13 percent, 19 percent said the fraud was a result of malware, and 19 percent cited social engineering (which occurs when criminals create fake situations that trick businesses into quickly sending funds). What are some steps that companies can take to guard against social engineering attacks? And are there other fraud trends businesses need to know about?

Social engineering, which some call phishing, is huge. This is where I see the majority of data compromises arise. It's important to educate your employees to be vigilant about properly screening emails, phone calls and even website popups for fraud.

Generally, there are a number of steps you can implement that can help prevent social engineering attempts to gain access to your funds:

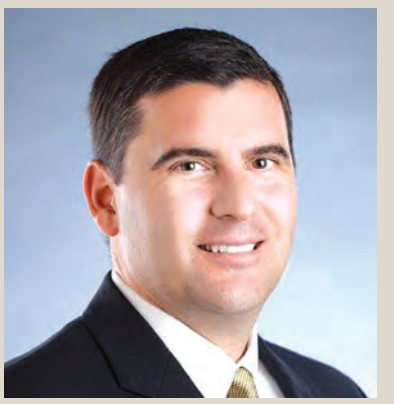
1. Validate new or updated payment instructions—even if they were received via internal email.
2. Speak with—or contact directly—anyone who's requesting a funds transfer or a change to payment instructions so you can validate that the changes are legitimate before processing.
3. Examine all payments before they're issued, and ensure that all correspondence is validated and documented across your entire business.

There's also always the threat of the malicious insider—someone within the company who has bad intentions and perpetrates fraud on your business—but if you're properly monitoring employee activity, you have a good chance of reducing this risk.

Survey respondents cited a number of actions their businesses are taking to prevent cybersecurity breaches, including conducting external penetration tests, implementing ongoing training and education for employees, and continuing to invest in software and systems to block attacks. What are some other ways you would advise organizations to protect themselves?

The best advice I have is to promote awareness of cyberthreats—particularly via ongoing training and education, which tends to be undervalued—and to create a culture where escalation is encouraged. If employees know they won't be penalized or made to look foolish for following the steps above, you can drastically reduce your risk for things like wire transfer fraud, which is on the rise.

Rick Nogueira



Rick is the Region Manager of Chase's Middle Market Banking group serving Orange County and Inland Empire. In this capacity, he provides leadership and financial solutions to companies with revenues between $20 million and $500 million. A 25-year banking veteran in Southern California, Rick has spent more than 17 years of that time dedicated to Middle Market Banking. He joined Chase as a Senior Banker in 2009 and was promoted to the position of Region Manager in January 2012. For additional information, please contact Rick at rick.l.nogueira@chase.com.

About Chase

Chase Commercial Banking has a long history of providing comprehensive solutions, including lending and treasury services, to corporations, municipalities, financial institutions and not-for-profit entities with annual revenues generally ranging from $20 million to $2 billion, as well as real estate investors and owners. Please visit us at www.jpmorganchase.com/commercial.

CYBERSECURITY, PRIVACY & CORPORATE GOVERNANCE

RUTAN PROTECTS YOUR DATA

RUTAN

RUTAN & TUCKER, LLP

GUIDING CLIENTS TO SUCCESS

rutan.com

BUSINESS LITIGATION | CORPORATE / SECURITIES / TAX | EMPLOYMENT / LABOR | GOVERNMENT & REGULATORY LAW | INTELLECTUAL PROPERTY | REAL ESTATE

611 Anton Boulevard, Suite 1400 • Costa Mesa, CA 92626 • 714.641.5100
3000 El Camino Real, Suite 200, Building 5 • Palo Alto, CA 94306 • 650.320.1500

TROUTMAN SANDERS

Lessons in Commercially Reasonable Data Security

by Ronald I. Raether, Partner, and Megan Nicholls, Associate, Troutman Sanders LLP

Information security presents a real problem for many companies and the issue is increasing in importance and complexity. Many businesses are in denial that they could ever suffer a breach; unwilling to address security for fear that doing so will impede profitability. What is the net value to the bottom line if criminals are permitted to steal the identity of your valued customers, your intellectual property and diminish your goodwill?

Ronald L. Raether

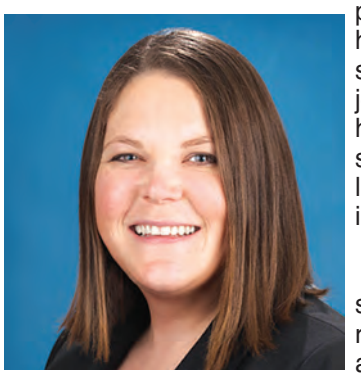
So, how do you prevent your company name from headlining the next data breach notification story? The simple answer: Maintain a robust information security program by understanding how information is received, used, stored and transmitted both inside and outside the organization. At the core of many information security laws is a layered approach to data security involving sound technology, administrative controls and a well-thought out data governance plan.

Creative use of Technology

Companies should employ a layered security approach in accordance with industry standards that addresses any issues unique to its business. This can include perimeter security, intrusion detection systems, egression device monitoring, oversight and surveillance technologies and the like. With this layered approach, when one security element fails, there are several others in place to mitigate, if not prevent, the resulting harm. Mobile devices, wireless networks, and remote company server access all play a key part in the ever-expanding virtual 'office' space increasing efficiency and flexibility, but they may also increase a company's risk of breach. Companies must balance the benefits of technology with appropriate enterprise risk management to isolate and minimize security threats, as well as mitigate resulting harms. Centralized control is essential.

Administrative Controls and Data Governance

Information should be managed according to sensitivity of the information and the risks posed if the information is stolen. A company must look at how each category of information is accessed or transmitted, by whom and for what purpose. Employees and third-party contractors have access to data and systems that can impact security well beyond their office space or assigned job responsibility. Ultimately, more sensitive, or high-risk/high-injury, information should be segregated from and guarded more securely than less sensitive, or lower-risk/lower-injury, information.



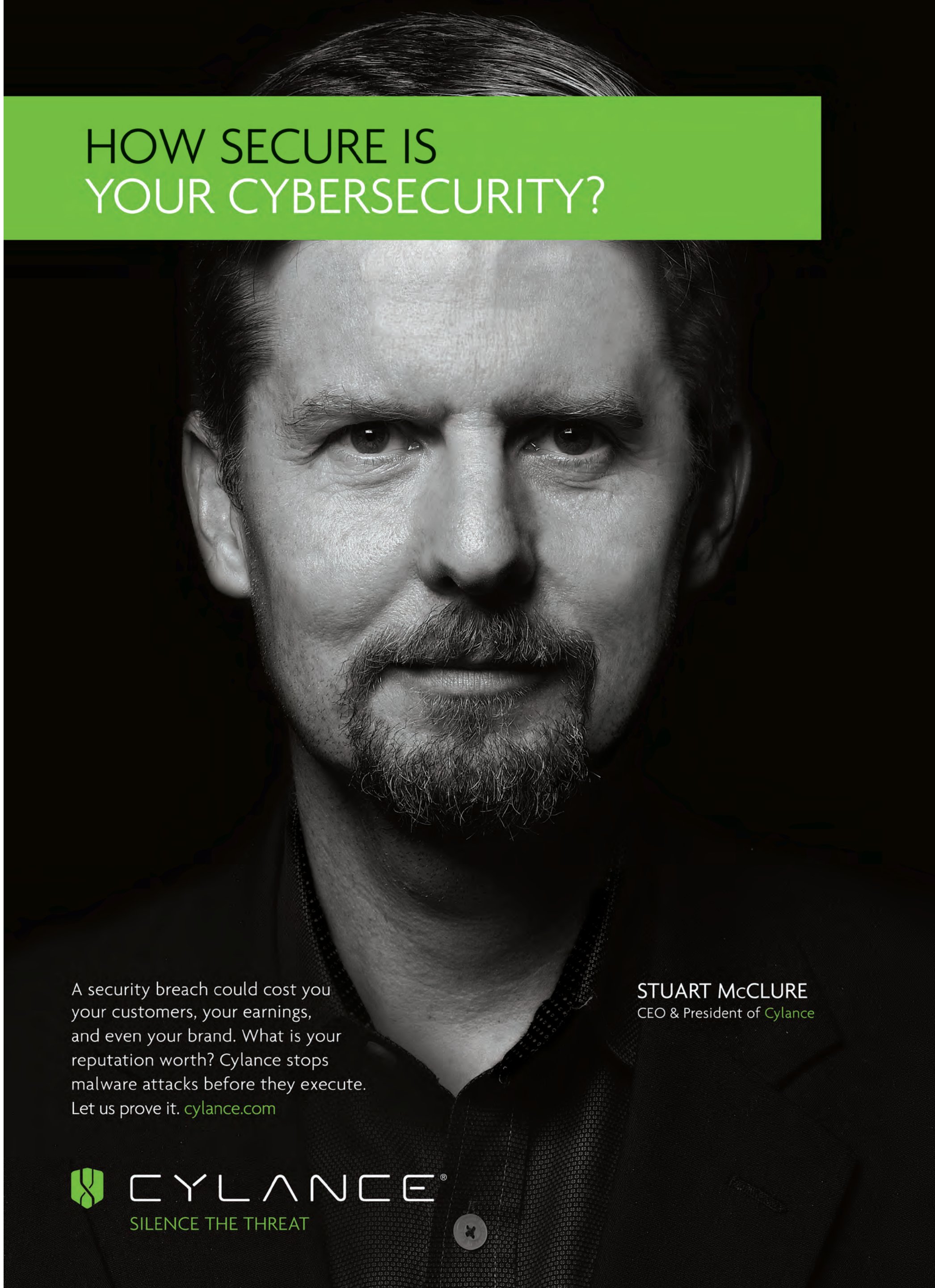
Megan Nicholls

A company's written policies and procedures should set forth clear, comprehensive and repeatable controls to restrict and audit access to and use of sensitive information. Regulators and law enforcement will have an easier time understanding a company's efforts if written policy and procedures are in place. But that is not enough. Employees must be trained regularly on their information security role and companies must audit for compliance with these policies and procedures.

Companies can ultimately limit the risk posed by creating a culture where every employee is empowered to take an active role in information security, regardless of hierarchy, through education and accountability. The most effective information security regimes have some relation with general counsel or another individual that can take concerns to the board and help achieve the proper balance between business functionality, privacy and information security.

For more information, contact Ronald I. Raether at 949.622.2722 or ronald.raether@troutmansanders.com. Contact Megan C. Nicholls at 949.622.2789 or megan.nicholls@troutmansanders.com.

HOW SECURE IS YOUR CYBERSECURITY?



A security breach could cost you your customers, your earnings, and even your brand. What is your reputation worth? Cylance stops malware attacks before they execute. Let us prove it. cylance.com

STUART McCLURE
CEO & President of Cylance

CYLANCE®
SILENCE THE THREAT

Effective Data Security Means Responsible Risk Management. *How is Your Company Doing?*

The frequency and size of data breaches and related litigation in the headlines has heightened "cyber anxiety" in corporate America. The challenge for any company is to channel that anxiety into smart action that enhances security of personal information or other sensitive data without harming operations or the bottom line. Misperception of risk is one of the biggest threats to succeeding in this endeavor. If a company fails to understand its risk profile, efforts to implement a poorly fitted security program may introduce new vulnerabilities or unnecessarily interfere with business operations. Here are three concepts to keep in mind to avoid succumbing to cyber anxiety.

Data security begins and ends with your company's unique risk profile. The patchwork of laws and regulations governing data security may create an urge to secure everything as though it were personal or other sensitive information, a practice some call "boiling the ocean." This urge must be resisted. Data security is another component of risk management, and therefore requires defining the risks to be managed. Taking the time to understand what types of data your company collects, how it makes such collection, what it does with that data, and where different types of data reside is indispensable. Indeed, in April 2016, the acting general counsel of the Federal Trade Commission—the federal agency that has taken much of the enforcement action relating to security of personal information—stated: "You can't secure your information unless you know what you have."

Knowing what you have is half of the equation. The other half is understanding the different ways in which your operations pose risks to your data. The technical innovations that have presented opportunities for new products, markets, and distribution channels are the same ones that have dramatically increased risk profiles for companies of all sizes and across all industry segments. With support from experienced legal counsel and qualified cybersecurity experts, the goal is to develop an actionable roadmap for managing risk without boiling the ocean.

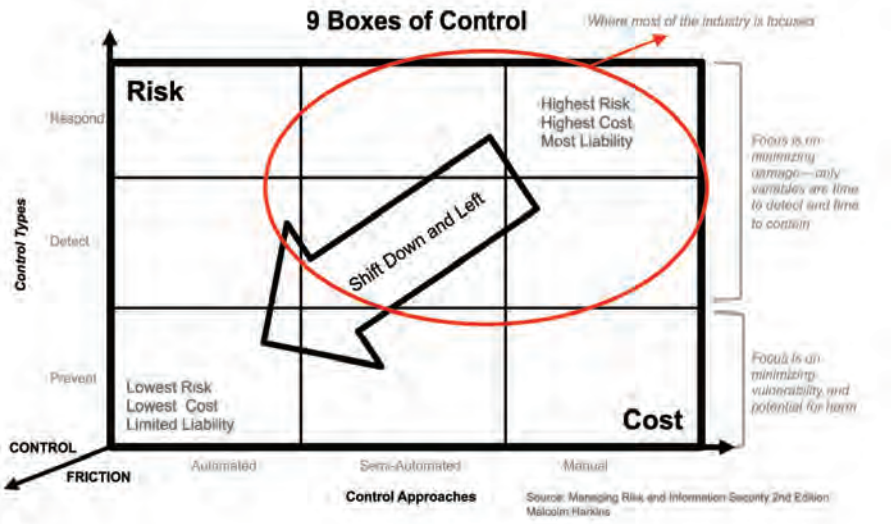
A "top down" approach to data security is necessary and attainable. Execution of a data security roadmap must be initiated at the Board level and overseen by the Board or a dedicated committee. Many regulators—including the FTC and the Securities and Exchange Commission—have made clear that effective data security requires an active mindset that starts with the Board and pervades every level of the organization. As some recent court decisions have shown, directors and officers who do not have a record of actually managing data security may lose the protection of the business judgment rule in shareholder suits arising from data breaches. However, these contributors to cyber anxiety need not be unduly burdensome.

Directors should, and can, balance their data security responsibilities with the duty to ensure the company's operational and financial health. Indeed, the key for Board members is not necessarily to become cybersecurity experts, but to examine how cyber-related risks contribute to broader enterprise risks driving corporate governance. Their most important contribution at the outset is to frame and start answering questions that are already on their minds: What could cause an "extinction event" for my company? What could impact the entire industry? What does the future look like? What types of data are most significant to the business and how may they be vulnerable? Through collaboration with legal and technical experts, the Board and senior management can begin to identify the right mix of data security controls that minimize business interruption.

Invest in data security controls that minimize both legal exposure and operational "friction." An effective data security policy will, among other things, clearly identify roles and responsibilities of relevant people, including directors, members of management, legal counsel, employees, vendors and other contractors with access to personal or otherwise sensitive data, cybersecurity professionals, and in many cases, a dedicated Chief Information Security Officer. These individuals must combine to implement three primary types of controls: prevention, detection, and response. Prevention occurs when an action or control prevents a risk before it affects users or the environment. Detection is identifying the presence of something malicious that has already entered the environment. Response is a reaction. From a risk perspective, prevention focuses on minimizing vulnerability and the potential for harm, while detection and response focus on minimizing damage.

Control implementation can be automated, semi-automated, manual, or some combination of all three. Automated control occurs entirely through machines. Semi-automated involves some level of human intervention. Manual controls are managed entirely by hand. The combination of control types and automation levels comprise the cells of the "9 Box" figure below. Risk increases as we move from prevention to detection to response. Cost increases as we move from automated to semi-automated to manual controls.

However, there is a third dimension to the 9 Box: control friction. Like a force that causes a moving object to slow down, controls can impose a "drag coefficient" on business velocity—they can slow the user or a business process. But this friction need not be an immutable force. A company can determine how much control friction to apply. Apply too much control friction, and users may go around IT and its security controls. This adds cost: The security team lacks visibility into user "work arounds," meaning it is less likely to prevent compromises, detection is difficult, and in many cases response after the fact becomes the only option. If a business adheres to high-friction controls, the effect can be to generate systemic business risk and hinder business velocity. The organization may lose time to market and the ability to innovate, and over the long term it may even lose market leadership. The size of a company's potential "drag coefficient" depends significantly on its culture, which is another reason that anything resembling a "one size fits all" approach to data security is misguided.



Again, everything begins and ends with a company's unique risks. In implementing an appropriate data security program, any company would do well to start by focusing on the following areas:

- Adopt good system "hygiene," including an inventory of connected devices.
- Use multi-factor authentication.
- Use encryption and/or rights management for sensitive data.
- Isolate critical functions.
- Backup critical systems.
- Consider using the cloud for reliable and scalable security.
- Consider a managed security service provider and regular penetration testing.
- Consider adding in-house or outside legal counsel with experience in privacy and data security compliance and litigation.
- Consider cyber insurance.
- Maintain an internal data security policy implemented through regular employee education and training.
- Maintain an incident response plan that can be deployed quickly and efficiently.
- Make data security a regular agenda item for Board meetings.

Maclom Harkins
Global CISO
Cylance Inc.

Marc J. Schneider
Litigation Shareholder, Stradling
(949) 725-4137
mschneider@sycr.com

Travis P. Brennan
Litigation Shareholder, Stradling
(949) 725-4271
tbrennan@sycr.com

Your Business Is Unique. Are Your Financial Solutions Built to Match?

We're dedicated to fostering growth in Orange County's communities. Let's start with your business. You can count on our full range of best-in-class products and services to position your business for long-term success, and seamless access to our firmwide network of experts means you'll receive customized financial solutions—along with the latest industry insights—to help meet your growing needs.

To learn more about how we can help you gain a competitive edge, please contact:

Rick Nogueira
Orange County and Inland Empire Region Manager
Chase Commercial Banking
(949) 833-4888
rick.l.nogueira@chase.com

CHASE

PAUL HASTINGS

From Life-Saving to Lethal: Product Liability After a Cyberattack

A hacker breaking into your email and stealing your passwords is bad. A hacker delivering a fatal dose through your insulin pump or remotely disabling your car's braking system is far worse. The Internet of Things presents significant challenges for cybersecurity, and exposes innovative manufacturers to untested claims for product liability. Although case law is virtually nonexistent, manufacturers' legal vulnerabilities are not. The historic framework for strict liability and negligence claims will inevitably be grafted onto claims for physical harm resulting from cybercrime directed toward connected devices. Regardless of the legal nuances courts ultimately apply, manufacturers can limit their potential liability with five proactive steps.

Product liability claims are traditionally based on a theory of strict liability or negligence. For example, the manufacturer of an insulin syringe that fails due to a manufacturing defect faces strict liability for resulting physical harm. However, if the insulin syringe fails due to a design flaw, a manufacturer is strictly liable only where the syringe's design was unreasonable. Software flaws could qualify as manufacturing or design defects, depending on the case. In an era where "security by design" is the evolving standard, injuries from products caused by cyberattacks on the products' software are likely to be approached under a design defect theory.

Yet current case law offers almost no guidance on what liability may attach when a connected device causes injury because its software was hacked. Industry standards (and, therefore, the legal standards of care) for cybersecurity are uneven and evolving every day, and no software is completely secure from malicious cyber intrusions. When should manufacturers be liable for intervening criminal acts of hackers? Courts will likely have a difficult time assessing whether a security gap was unreasonable, whether a standard of care was breached, or whether an intervening criminal act should absolve the manufacturer of liability. Nonetheless, companies can apply standards of reasonableness and industry norms to their businesses now, and reduce their risk of liability in five ways:

1. Prioritize security. Prioritizing software security not only reduces the risk of a successful attack, it demonstrates the reasonableness of the security measures in place, potentially eliminating tort liability.

2. Hire a cybersecurity advisor. A cybersecurity advisor can help assess the risk of products and their software, and recommend safeguards.

3. Document security efforts. Once implemented, companies should record all steps taken to secure the software, and put mechanisms in place to ensure long-term vigilance.

4. Have a plan for response and containment. Planning for containment of and a rapid internal and external response to an attack is an effective way to minimize damages.

5. Know the standards in your industry. Companies should know evolving security standards in their industry and join the conversation to ensure they are not left behind.

Although few, if any, cyberattacks have resulted in deadly damages, benign hackers have proven that lethal hacks are possible. Courts may hold manufacturers responsible for harm caused by unreasonable vulnerabilities. Given the exposure at stake, manufacturers cannot afford to wait for hackers or the law to catch up before taking action.


Christopher McGrath


Thomas Counts


Beau Stockstill


Danielle Decker

Chris McGrath, Tom Counts, Beau Stockstill and Danielle Decker

Chris McGrath and Tom Counts are partners, and Beau Stockstill and Danielle Decker are associates, in the litigation department of Paul Hastings LLP, with a practice focus on privacy and cybersecurity. Chris McGrath and Beau Stockstill are based in the Firm's Costa Mesa office. Tom Counts and Danielle Decker are in the Firm's San Francisco office. For additional information, please call 714.668.6200 or visit www.paulhastings.com.

ELLS CERTIFIED PUBLIC ACCOUNTANTS & BUSINESS ADVISORS

Cybersecurity: Keeping Taxpayer Data Secure

by Pamela Bustos, Principal, ELLS CPAs & Business Advisors

In this day and age, you can never be too careful regarding your cybersecurity precautions, as they are of the utmost importance in the effort to keep your financial and other personal data secure. As a full-service tax and accounting firm, ELLS CPAs and Business Advisors knows this all too well, as we are constantly entrusted with the private and personal financial data of our clients, including their businesses and family members.

ELLS has numerous systems in place to protect our clients' financial data, including secure email and client portals. Clients may occasionally complain about the added steps that are put in place by using secure email, but they are critical protections that benefit the client in the long term.

Additionally, with the increase in online access to various taxing agencies, including the IRS and California Franchise Tax Board (FTB), both agencies have been forced to acknowledge that there have been recent breaches of their online systems by hackers who have somehow gained access to taxpayer accounts without the appropriate permissions.

As a result, the FTB recently announced changes to their MyFTB site, which can be accessed by both taxpayers and tax professionals, after the determination that certain taxpayer accounts were added to the MyFTB accounts of tax preparers who had no affiliation with the taxpayer or their accounting firm. These changes involve the implementation of a 10-business-day waiting period before a taxpayer's account can be added to the MyFTB access of a tax preparer or a Power of Attorney will be processed. The taxpayer is mailed a letter notifying them of the request for access by the tax preparer. The taxpayer will be given the opportunity to call and prevent access to their account. If the taxpayer does nothing, the access will be granted.

While all this may seem like overkill, the added online access has actually created a window of opportunity for hackers to gain access to a taxpayer's private data, such as estimated tax payments and wage withholding paid during the year.

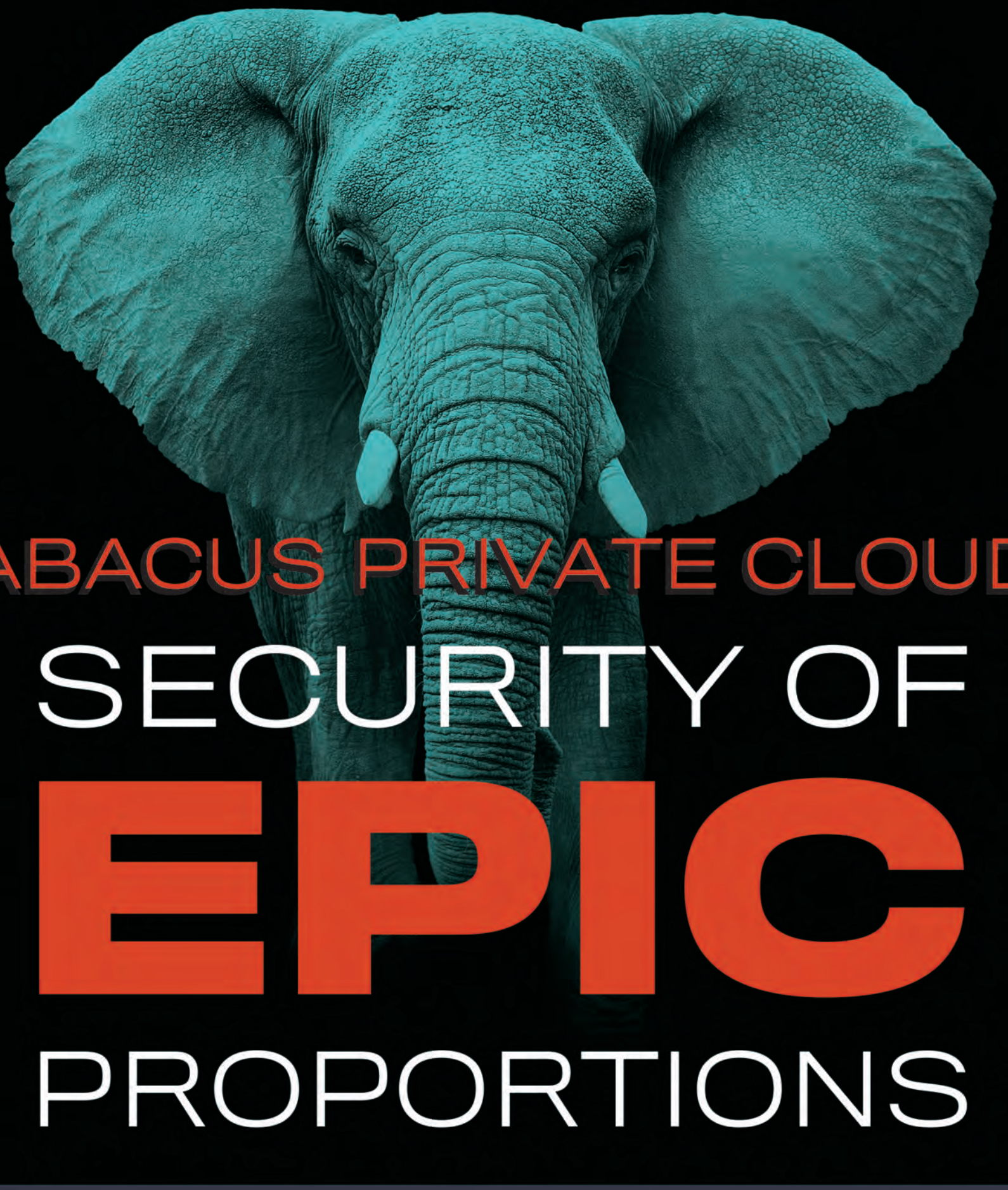
The FTB has already been sending these notification letters to taxpayers that a tax preparer is requesting access, but now with the 10-day waiting period about to be put in place, this will strengthen the controls surrounding the FTB's online access portal called MyFTB. Though the waiting period may be inconvenient, it is a necessary requirement to stop hackers in their tracks from gaining access to your sensitive financial data.

For more information, contact Pamela Bustos, Principal at 714.569.1000 or pbustos@ellscpas.com or visit us at www.ellscpas.com.

Pamela Bustos

Pamela Bustos joined the ELLS team in 2013, bringing with her more than 20 years of experience in taxation and consulting. Pam's areas of expertise include tax compliance for complex high net worth individuals and pass-through entities including partnerships, limited liability companies, S corporations and C corporations. She has extensive experience in providing tax planning for multi-state high net worth individuals and their closely held businesses. She also has significant experience in handling federal and state tax audits. Pam has worked with companies in a variety of industries including real estate, professional services and wholesale manufacturing. She manages manufacturing, distributing, real estate, high net worth individuals and professional services clients.

FACE IT
YOUR DATA IS EXPOSED



ABACUS PRIVATE CLOUD

SECURITY OF EPIC PROPORTIONS

- Ownership of Data
- Full IT Management & Maintenance
- Geographically Diverse U.S. Data Centers
- Uptime Guarantee
- Flexible & Scalable Environment
- Fully Integrated Backup & Disaster Recovery
- Compliance Ready
- Software & Industry Agnostic
- Use on Any Device, Any Time, Anywhere

ABACUS DATA SYSTEMS
Fully Managed Technology Solutions

abacuslaw.com/ocbj
888-592-2044