CHAPTER 13

# BUSINESS REALITIES OF COMPLIANCE PENALTIES FROM DATA BREACH

BY KEVIN FREAM

*It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently.*
~ Warren Buffet

In the 2011 movie "Moneyball", General Manager Billy Beane provides an insightful lesson showing how to release players in a succinct straight-forward manner. Just like that illustrative scene, you need to know there is no silver bullet answer for preventing data breach – much less avoiding the corresponding compliance penalties affecting virtually every business. Unlike releasing a player as in the movie, publicized data breaches are guaranteed to have severe backlash including damaged reputation.

Business owners and management teams should literally take a lesson from the approach and title of the book Moneyball: The Art of Winning an Unfair Game. Whether you lean politically toward the left or right, no one can deny that government compliance programs and taxes continue to rise. In spite of the U.S. Small Business Administration 2006 re-launch of Business.USA.Gov, small and medium-sized businesses are especially easy targets and largely unaware of compliance penalties.

Aristotle put forth the concept that ignorance of the law is no excuse in approximately 340 B.C. His words still ring true today, as common unawareness does not remove your liability for violating the law. Compliance penalties can be shockingly devastating by delivering hefty fines and potential prison time, instead of the misguided myth of simply paying a nominal fine when you get caught.

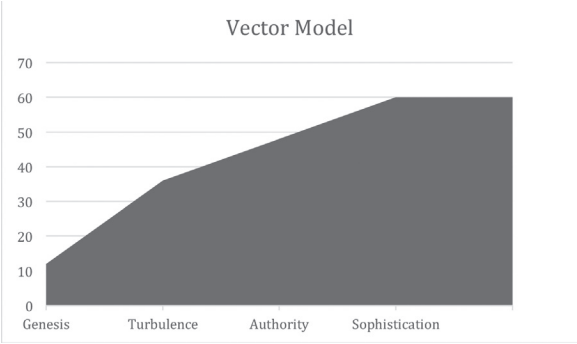
You can blindly copy your competition by taking a cost-of-doing-business approach toward government compliance, or leverage smart ideas and build a better product/service for customers. Savvy organizations will primarily focus upon a vector approach to reducing complexity and avoiding risk, as well as the true costs of compliance violations explained in the following sections.

## VECTOR GROWTH APPROACH TO TECHNOLOGY

In 1973, the Harvard Business Review published an evolution of Information Technology (IT) presented by Richard Nolan as the stages of a technology growth model. Although enhanced from four to six stages a decade later, the Nolan Growth Model is a dated premise based upon the fallacy of economic growth rather than practical business need.

Generally, all organizations today utilize and can afford necessary technology. It's extremely rare that IT Managers have any significant budget authority. Further, startup companies regularly disrupt all industries, dispelling a widely-perpetuated marketing pitch that the more you spend on technology, the more competitive your company.

Ask yourself who benefits from an IT department focused solely on growing its own fiefdom? Who gains from having a costly patchwork of layers of hardware and software from various vendors for significant complexity? The answer is definitely not owners, shareholders, or customers – which is why discerning leaders and management teams implement the Vector Model as shown below.




Source: streamliningtechnology.com

Genesis is the beginning stage in implementing technology solutions based upon reduced complexity, rather than by the budget of technical features. The concept starts with an initial understanding that some services are recommended to be outsourced at a far less cost with greater productivity and security than any do-it-yourself approaches, which may misleadingly seem more cost effective.

Turbulence is the following step wherein management begins to take a lead role in fully understanding technology strategy and implementation, as opposed to abdicating leadership to the accounting or technology personnel within a company. The result is old paradigms of support and purchasing are both challenged and streamlined.

*70% of companies fail to transition from Turbulence to Authority.*

Next is Authority, in which critical services are consolidated and therefore the risk is distributed across a smaller number of products and services. The organization then begins publishing intellectual property as a differentiator in being both more trustworthy than their competitors and offering more value for customers.

The last phase is called Sophistication which entails the organization evaluating their return on investment, while

continuing to focus on better customer experience. Special emphasis by management is taken in reviewing processes for any business improvement with the consideration of new technology. Once you identify the current operational stage of technology within your organization, you have a better understanding of weaknesses. Therefore, you can begin to evaluate a breakeven between technology costs and business improvement versus the risk of compliance penalties. Unfortunately, an estimated seventy percent of businesses are so resistant to change that they never make it past the Turbulence stage. As evidenced by research every few years by Forbes and Bloomberg, this obstinate lot eventually fails in their endeavors. Industry forces like unexpected compliance penalties just hasten their demise.

## STATURE DAMAGE MODEL: REAL COST OF COMPLIANCE VIOLATIONS

In most businesses employees and owners think of compliance penalties like a traffic fine. You had the bad luck to get caught and you pay the fee and move on. However, unlike a mere traffic ticket, the highest cost of compliance penalties from data breach is actually your damaged reputation. The reason why is twofold: you are legally required to publicize a breach for the protection of current and future customers, and then there is the overstated, yet true notion, that nothing on the Internet ever really goes away.

Until relatively recently, many organizations could simply shun or ignore compliance risk without the Internet as a factor. What's the cost of doing nothing? Who's going to know? Well, the cost of doing nothing is often zero, but only until some catastrophic event like exorbitant compliance penalties and related lost revenue materialize. While Fox Business reported in 2014 that the odds of the IRS auditing a business with $1 million or more in sales is just 12.1%, the odds of a data breach penalty are nearly 25%.

The Office of Civil Rights (Division of U.S. Department of Health and Human Services) actively audits health-related organizations

for privacy violations. Also, banks and related financial institutions review merchant data security standards annually to protect cardholder payment information. Finally, the Federal Trade Commission is scheduled to aggressively investigate all types of businesses for proper disposal of customer and employee information because of widespread identify theft.

Not only are government agencies reviewing compliance, but practically anyone can be a whistle-blower for privacy and data breach concerns. Employee, vendors, customers, and competitors can all report compliance violations and trigger audits and penalties as stated in the publically viewable sites below:

HIPAA: http://www.hhs.gov/hipaa/filing-a-complaint
PCI-DSS: https://www.mastercard.us/en-us/consumers/get-support/report-problem-shopping.html
FACTA: https://www.ftccomplaintassistant.gov/

The true cost of compliance violations is worsened by lost revenue and productivity, purchase of additional security products and services, lost future income due to negative publicity, and then penalties with on-going audit often required afterward.

**Reputation Damage Calculator**

Top Concerns: security breach reasons, penalties, security costs, and future prevention.

| Scenarios | Value | Units |
|---|---|---|
| Outage Duration | 8 | Hours |
| Employeess Affected | 12 | Employees |
| | | |
| Productivity Loss | 100% | Percentage |
| Revenue non-recoverable | 100% | Percentage |
| | | |
| Average Employee Cost | $22 | Hourly |
| Average Employee Reveneue | $104 | Hourly |
| Intagible Cost | $11 | Hourly |
| | | |
| Productivity Loss | $3,168 | Violation |
| Revenue Loss | $9,984 | Violation |
| Intangible Loss | $0 | Violation |
| | | |
| Compliance Penalties | $10,000 | Incident |
| Added Security Products/Services | $12,000 | Incident |
| **Total Loss** | **$35,152** | |

Source: cyberprey.com

The worst part is not only regulatory authorities publicizing penalty violations and your own data breach notice, but the realization that such negative publicity is saved with easy access at archive.org. Years after a publicized data breach notice is removed from any web site, prospective customers or cunning competitors may search for old breach pages. Using common search tools like Ahrefs.com, anyone can view broken links to an old non-existent web page and copy the exact address to search on "Wayback Machine" (https://archive.org/web/).

Medical and health data breaches are regularly listed at: www.cdph.ca.gov/programs/Pages/LnCBreachConfidential.aspx. Large business data breaches are also listed at sec.gov.

## TOP THREE COMPLIANCE PENALTY CONCERNS

The amount of potential taxes and other compliance liabilities for business owners seems to grow each year, as evidenced with new legislation like the Affordable Care Act. Large publicly-traded organizations also have their own unique set of compliance challenges with Sarbanes Oxley. For most other businesses, there are three major compliance concerns all generally focused on privacy issues: Health Insurance Portability and Accounting Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), and Fair and Accurate Credit Transactions Act (FACTA).

President Bill Clinton signed the infamous HIPAA into law in 1996. The portion that affects all employers (not just medical and insurance entities) is the policies, procedures, and guidelines for maintaining the privacy and security of individually identifiable health information. Unauthorized disclosure (printed or digital documents) of individually identifiable health information may be reported to the Office of Civil Rights for investigation and penalty assessment.

| HIPAA Violation | Minimum Penalty | Maximum Penalty |
|---|---|---|
| **Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA** | $100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation) | $50,000 per violation, with an annual maximum of $1.5 million |
| **HIPAA violation due to reasonable cause and not due to willful neglect** | $1,000 per violation, with an annual maximum of $100,000 for repeat violations | $50,000 per violation, with an annual maximum of $1.5 million |
| **HIPAA violation due to willful neglect but violation is corrected within the required time period** | $10,000 per violation, with an annual maximum of $250,000 for repeat violations | $50,000 per violation, with an annual maximum of $1.5 million |
| **HIPAA violation is due to willful neglect and is not corrected** | $50,000 per violation, with an annual maximum of $1.5 million | $50,000 per violation, with an annual maximum of $1.5 million |

The "Payment Card Industry Security Standards Council" was formed on December 15, 2004 for policies between the major credit card brands of Visa, MasterCard, American Express, Discover, and JCB. PCI-DSS is a proprietary information security standard aimed at reducing fraud and identity theft for the many organizations that handle major credit cards. Violations primarily involve data breach by hackers due to inadequate security processes and systems or disclosing more than the last

four digits of a card in digital or printed form.

| PCI Penalties |
| --- |
| **Fines up to $500,000 per data security incident** |
| **Fines up to $50,000 per day for non-compliance with published standards** |
| **Liability for all fraud losses incurred from compromised account numbers** |
| **Liability for the cost of re-issuing cards associated with the compromise** |
| **Suspension of merchant accounts** |

President George W. Bush signed FACTA into law in 2003. Most people understand that FACTA allows individuals access to a free credit report annually, but what is not commonly known is that it requires secure disposal of employee and customer information for businesses. The Federal Trade Commission announced that in 2016 it will begin randomly auditing organizations of all sizes due to the rampant problem of identity theft. Common violations for FACTA are failure to shred or delete employee or customer documents or inadequate digital security: https://www.ftc.gov/tips-advice/business-center/guidance/disposing-consumer-report-information-rule-tells-how

| FACTA |
| --- |
| Federal Trade Commission has not published a defined schedule to date, but will likely pattern after HIPAA penalties. Fines up to $500,000 per data security incident |
| Violators may also face state fines and possible civil action. |

Organizations are required to publicly publish anything that constitutes as major violations and contact customers in writing concerning breach or potential breach of private information, potentially ruining a company's reputation. A poor but common practice is a single form or database which includes complete

employee information including medical claims. Any business or organization that follows this practices and takes credit card payments, may then be in violation and penalized for all three compliance areas above.

## REGULAR EXAMINATION OF RISK AND IMPROVEMENT

While your competition takes an apathetic or cost-of-doing-business approach, the best advice to avoid compliance penalties is taking a business improvement approach. A regular Cyber Security Exam is cheap insurance and any improvement in business process or security is a differentiator to publicize to customers.

A Cyber Security Exam is the purview of qualified IT security firms and not accountants or lawyers. Legitimate firms follow the Vector Model to try and eliminate complexity and costs. Exams should be performed by degreed and certified professionals with more than 10 years' experience in technology security. Most exams will cost between $3,000 and $7,000 depending upon the size and complexity of the customer organization and may include an Acceptable Use Policy (AUP). Qualified firms may also act as a defense for government compliance audit like a CPA or an attorney representing a client. In the process, your existing IT staff gains some accountability while you gain peace of mind.

Good marketing builds trust with a preponderance of evidence for prospective customers. Press releases, blog posts, videos, and compliance logos are all important to provide a positive impression and your continual commitment to improvement for existing customers. In all businesses there is a human element. If you do suffer a breach and compliance penalty, you have a basis to evaluate failures from the last exam and more importantly, you have many positive listings to push anything negative down in Google search results.

## About Kevin

As the CEO of Matrixforce Corporation, Kevin Fream brings twenty-five years of experience as a cyber-security advisor to prospective customers. He specializes in helping business owners and leadership teams reduce technological complexity and avoid risk, with an emphasis on highlighting current compliance penalties that impact the viability of nearly every business.

While Kevin was completing his Bachelor of Science in Management Information Systems degree from the University of Tulsa, he landed a paid internship with DuPont. That early experience with one of the most security conscious organizations in the nation allowed him to go on to work nationwide with a number of other Fortune 500 firms.

Along the way, he noted that the local marketplace was riddled with suspect competencies, rude behavior, and relentless hourly billing. Mid-sized businesses of $5 million to $150 million in revenue seem to be particularly under-served and mistreated. As a result, Kevin formulated a distinct customer service strategy:

1) Assume the risk for customers by offering flat cost and demonstrating business justification. No one would be compensated for billable hours or selling products.
2) Train staff on rules of engagement and how to talk with customers in simple language, so that they can understand and control outcomes for Information Technology.
3) Specialize in Microsoft productivity and security solutions for annually-audited expertise.

Today, Matrixforce has saved clients collectively over $500 million on technology services and products and is a top 100 Microsoft Gold Cloud Partner.

More cyber-security insights, tools, and downloads may be accessed at Cyberprey.com.

Look for Kevin's next book being published soon: *Revealing Secrets to Streamlining Technology.*

Contact information:

- kfream@matrixforce.com
- http://www.linkedin.com/in/kevinfream